Elastic Network Interface

Operation Guide

Product Documentation

Contents

Operation Guide

Operations Overview

Last updated：2024-07-05 16:45:03

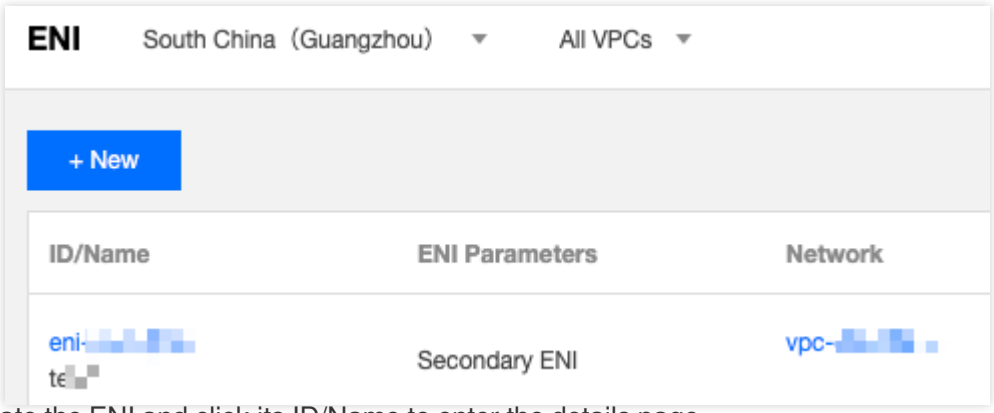
When using ENIs, you may have some questions about how to create and query ENIs, bind ENIs to and unbind ENIs from CVMs, and modify primary private IPs. This document describes some common operations for using ENIs and related products.

Common Operations

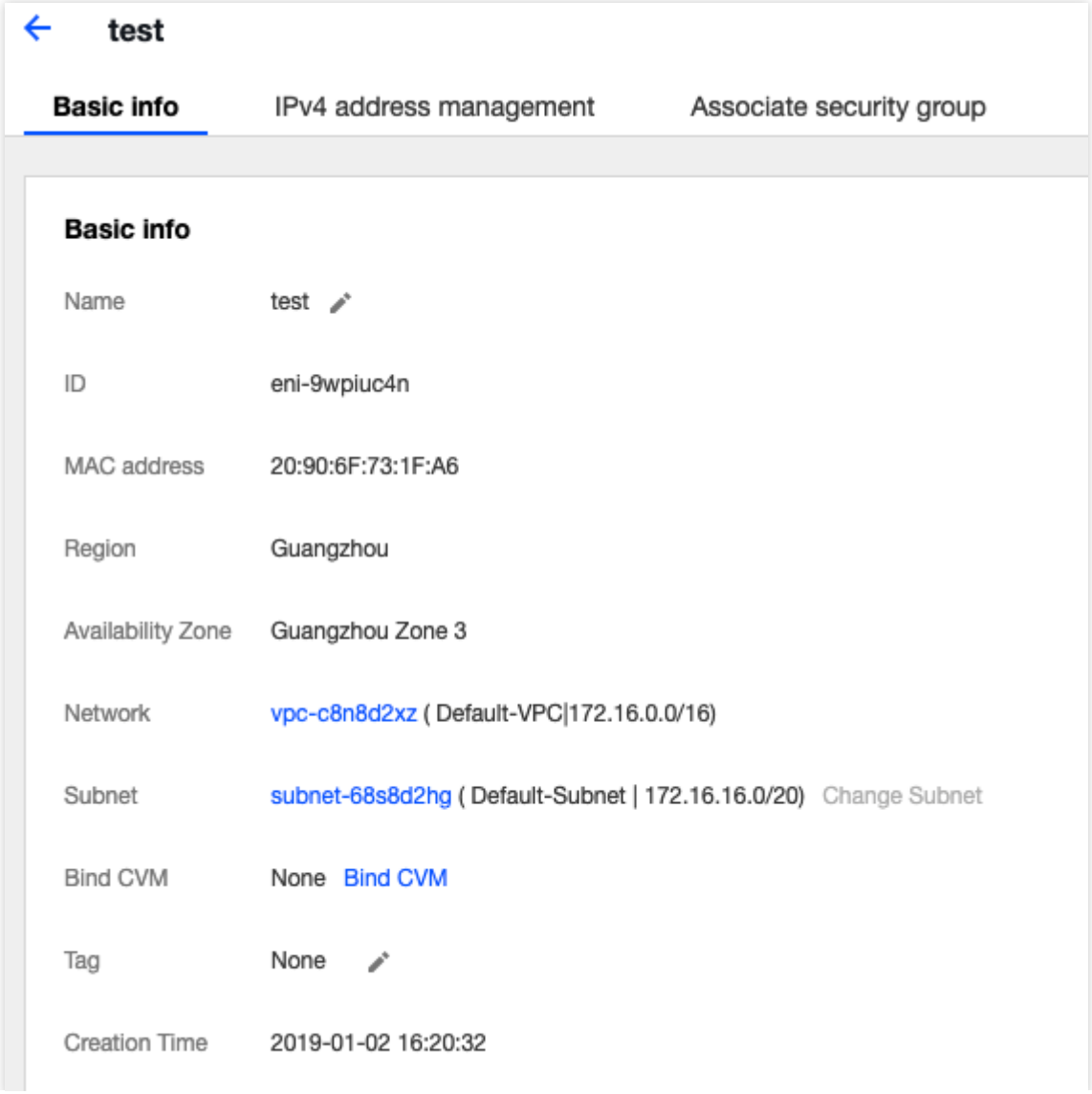
Viewing ENI Information

Last updated：2024-01-11 16:04:31

1. Log in to the VPC Console.
2. Choose **IP and ENI** -> **ENI** in the left sidebar to go to the ENI list page.



3. Locate the ENI and click its ID/Name to enter the details page.



Creating an ENI

Last updated：2024-01-11 16:04:31

1. Log in to the VPC console.
2. Choose **IP and ENI** > **ENI** in the left sidebar to go to the ENI list page.
3. Select a region and a VPC, and click **+ New**.
4. In the pop-up window, enter an ENI name, select the VPC and subnet to which the secondary ENI belongs, and assign a private IP to the ENI. To add a tag, click **Advanced options**.

Note:

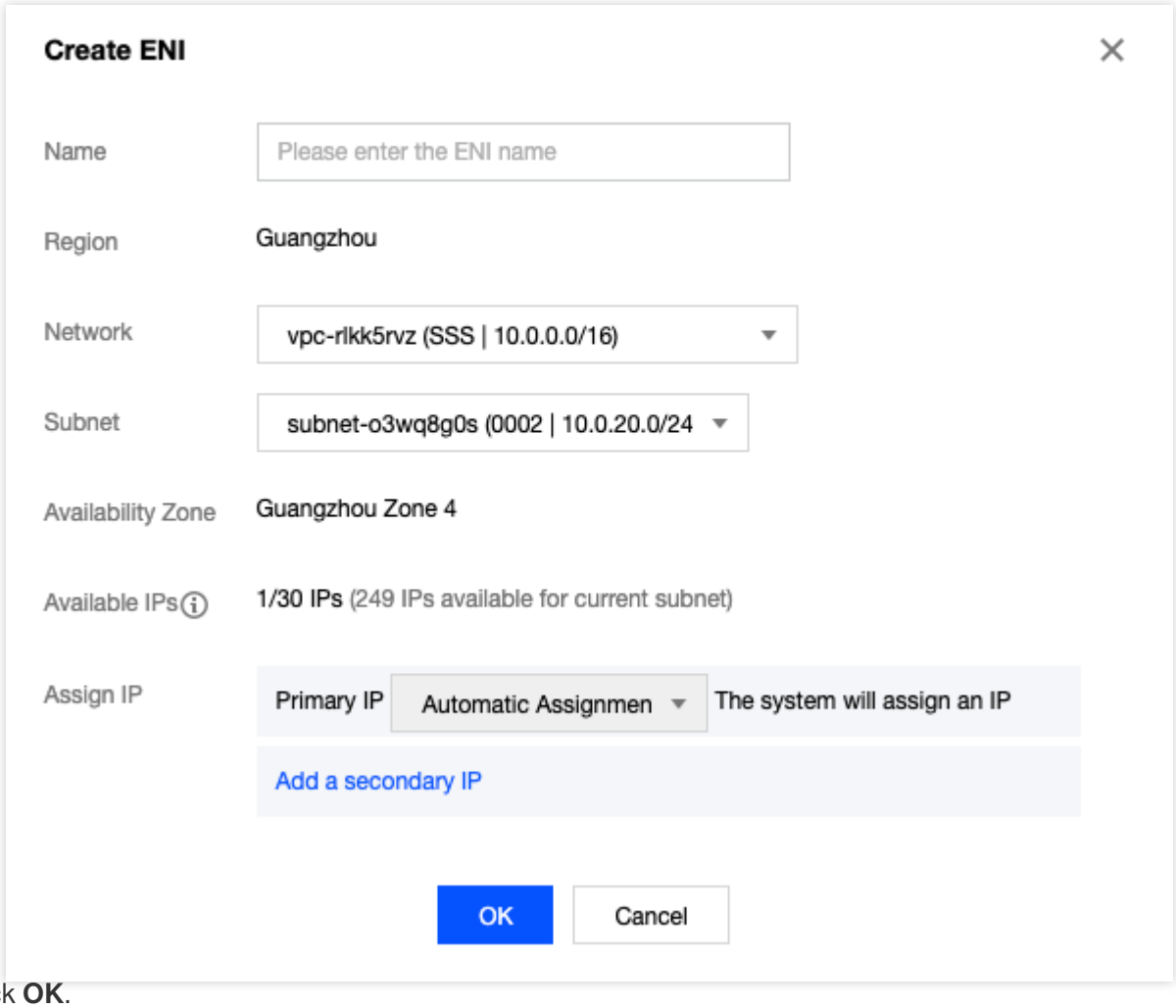
You need to configure the security group for the secondary ENI separately. After creating the secondary ENI, please determine the security policy of the ENI based on your business situation and bind the security group to it. For details, see binding security groups.

"Automatic" and "Manual" are supported for IP assignment:

Automatic: The system will automatically assign a private IP available in the subnet CIDR block to the ENI.

Manual: You need to enter a private IP available in the subnet CIDR block.

A secondary ENI is configured with a primary IP by default. If you need multiple IPs, click **Add a secondary IP** to configure them.



5. Click **OK**.

Configuring Security Groups

Last updated：2024-01-11 16:04:31

The secondary ENI can be bound with one or more security groups, which implement access control on the in/outbound traffic of the ENI. You need to bind the security group to the created secondary ENI according to your business situation. The ENI can be bound with the same security groups as or different ones from the CVM instances. This document describes how to bind a security group to or unbind it from the secondary ENI.

Binding security groups

Prerequisites

You've created the security group(s) as instructed in Creating a security group.

Operation Guide

1. Log in to the ENI console.
2. Click the ID of the ENI to which the security group needs to be bound.
3. Click **Bind** in the **Associate security group** tab.
4. In the **Configure security group** pop-up interface, check your created security group(s), and click **OK**. When multiple security groups are bound, the higher the security group is, the higher its priority will be, and it will be matched earlier.

Unbinding security groups

Note:
It is recommended that you reserve at least one security group for an ENI.

Operation Guide

1. Log in to the ENI console.
2. Click the ID of the ENI from which the security group needs to be unbound.
3. In the ENI details page, click **Associate security group** tab, and then click **Unbind** in the **operation** column of the **Bound security groups** list.
4. In the pop-up window, click **OK**.

Binding and Configuring an ENI
Binding an ENI to a CVM

Last updated：2024-01-11 16:04:31

This document describes how to bind a secondary ENI to a CVM.

Note:

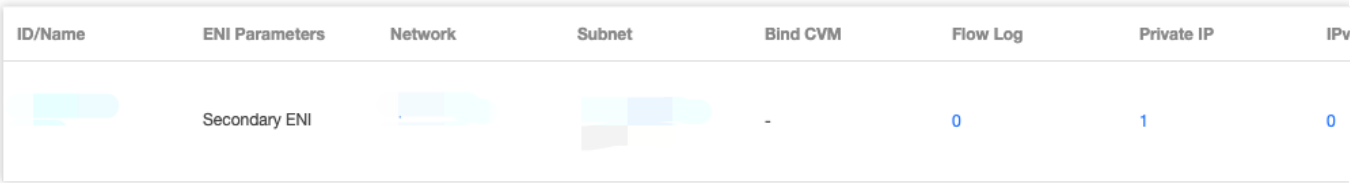
You need to configure the security group for the secondary ENI separately based on your business situation. With no security group bound, the ENI does not have access control on in/outbound traffic by default. To bind the security groups, see binding security groups.

For CVMs using CentOS 8.0, 7.8, 7.6, 7.5 or 7.4 images, install a tool before binding an ENI. The ENI information is automatically configured in the ENI file, and the routing policy is automatically delivered. For more details, see Configuring an ENI on a Linux CVM.

For CVMs using other images, bind an ENI to the CVM as instructed below. Then complete the ENI configuration by referring to Configuring an ENI on a Linux CVM or Configuring an ENI on a Windows CVM.

Binding to a CVM

1. Log in to the VPC console.
2. Click **IP and ENI** > **ENI** in the left sidebar.
3. Locate the row of the desired ENI, and click **More** > **Bind CVM** in the **Operation** column.

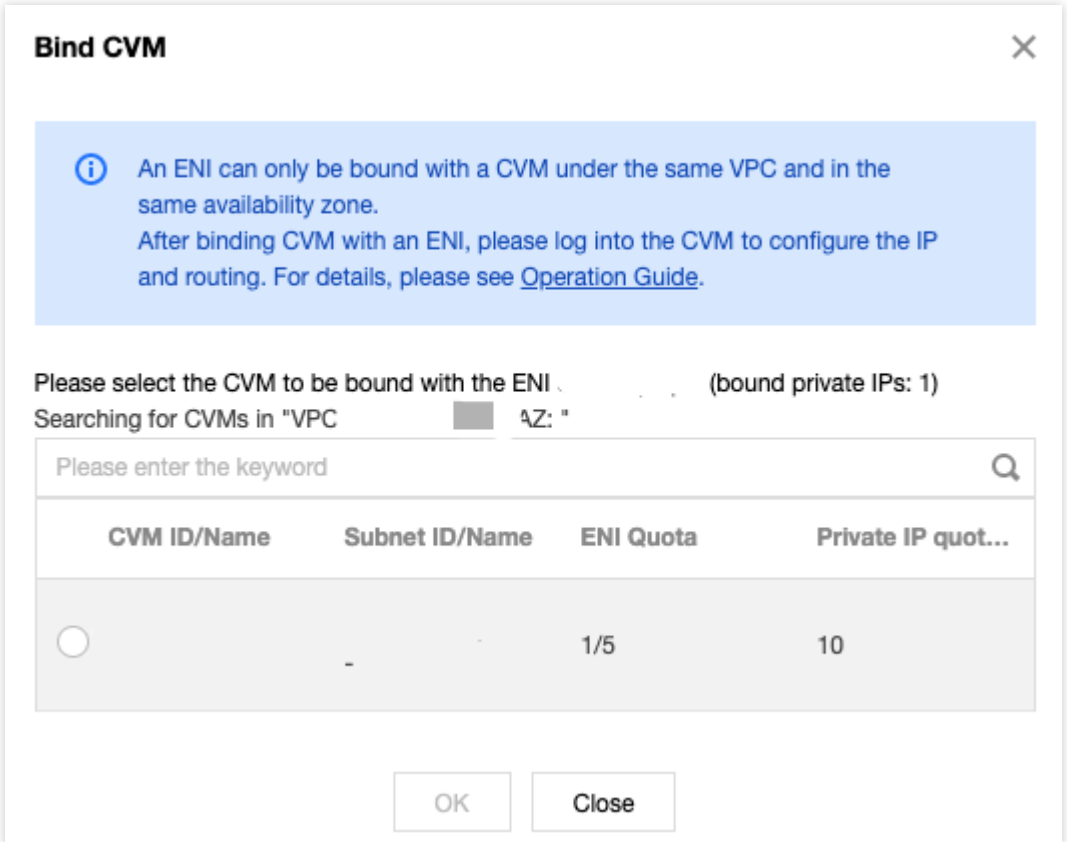


Note:

You can also click the ENI ID to go to the details page, and click **Bind CVM**.

The ENI can be bound to the CVMs in the same availability zone as the ENI. For more model limits, see Use Limits.

4. In the pop-up window, select the target CVM and click **OK**.



Configuring an ENI on a Linux CVM

Last updated：2024-01-11 16:04:31

This document guides you to configure an ENI on a Linux CVM.
This document provides instructions on how to configure an ENI on two common server images: CentOS and Ubuntu.
Configuring an ENI on a CentOS CVM
Configuring an ENI on an Ubuntu CVM

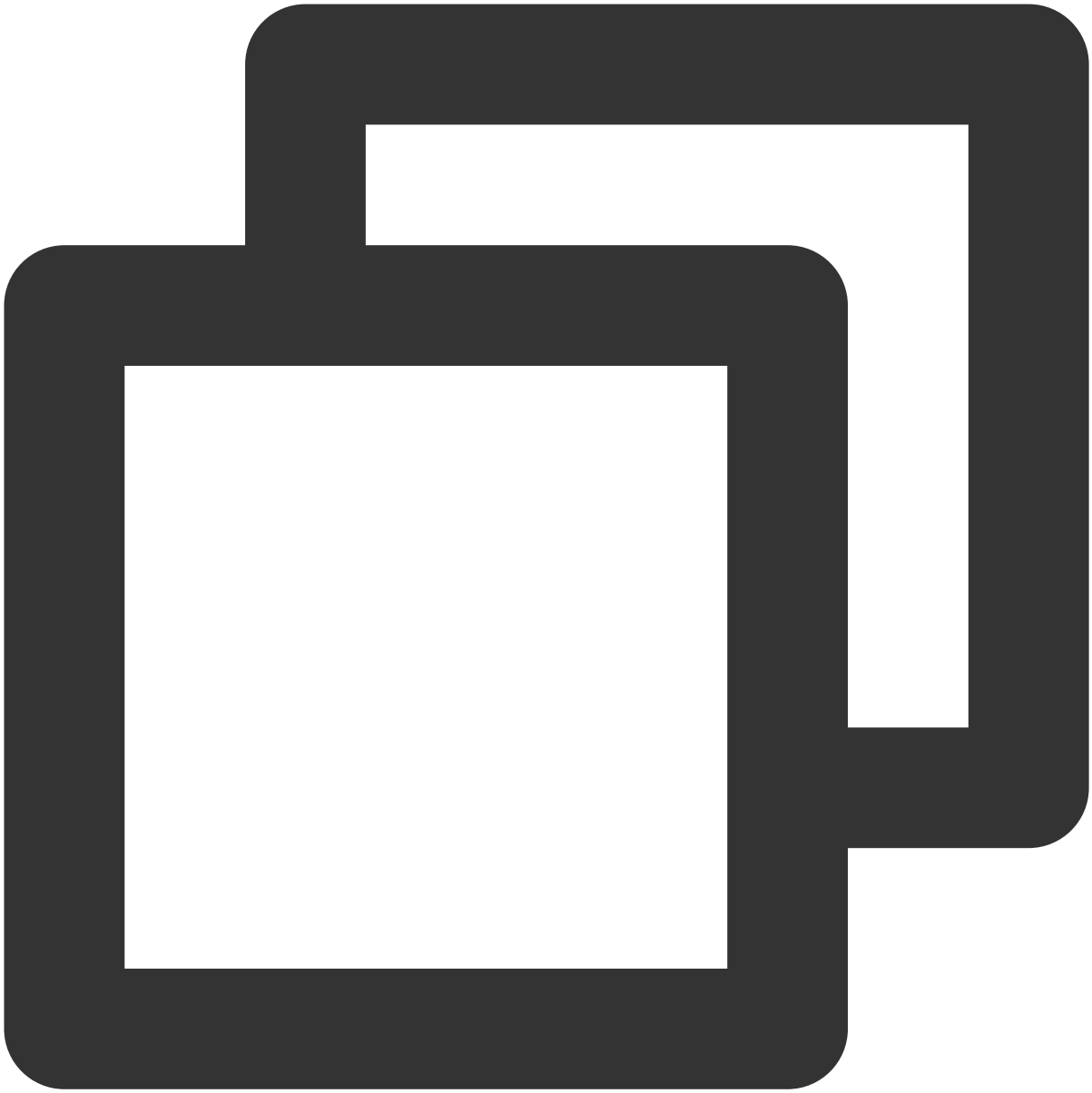
Configuring an ENI on a CentOS CVM

Method 1: Tool-based configuration

Note:
This method is applicable to CentOS versions 8.0, 7.8, 7.6, 7.5, 7.4 and 7.2.
The nic-hotplug.tgz tool automatically creates the ENI configuration file and distributes the ENI route when an ENI is bound or the CVM is restarted.
If the CVM has already configured with ENIs, ensure that the routes of existing ENIs have been correctly configured before using the tool to configure a new one. If restart is acceptable to your business, you can restart the CVM as instructed in the step 5 for the tool configuration to take effect on all ENIs.

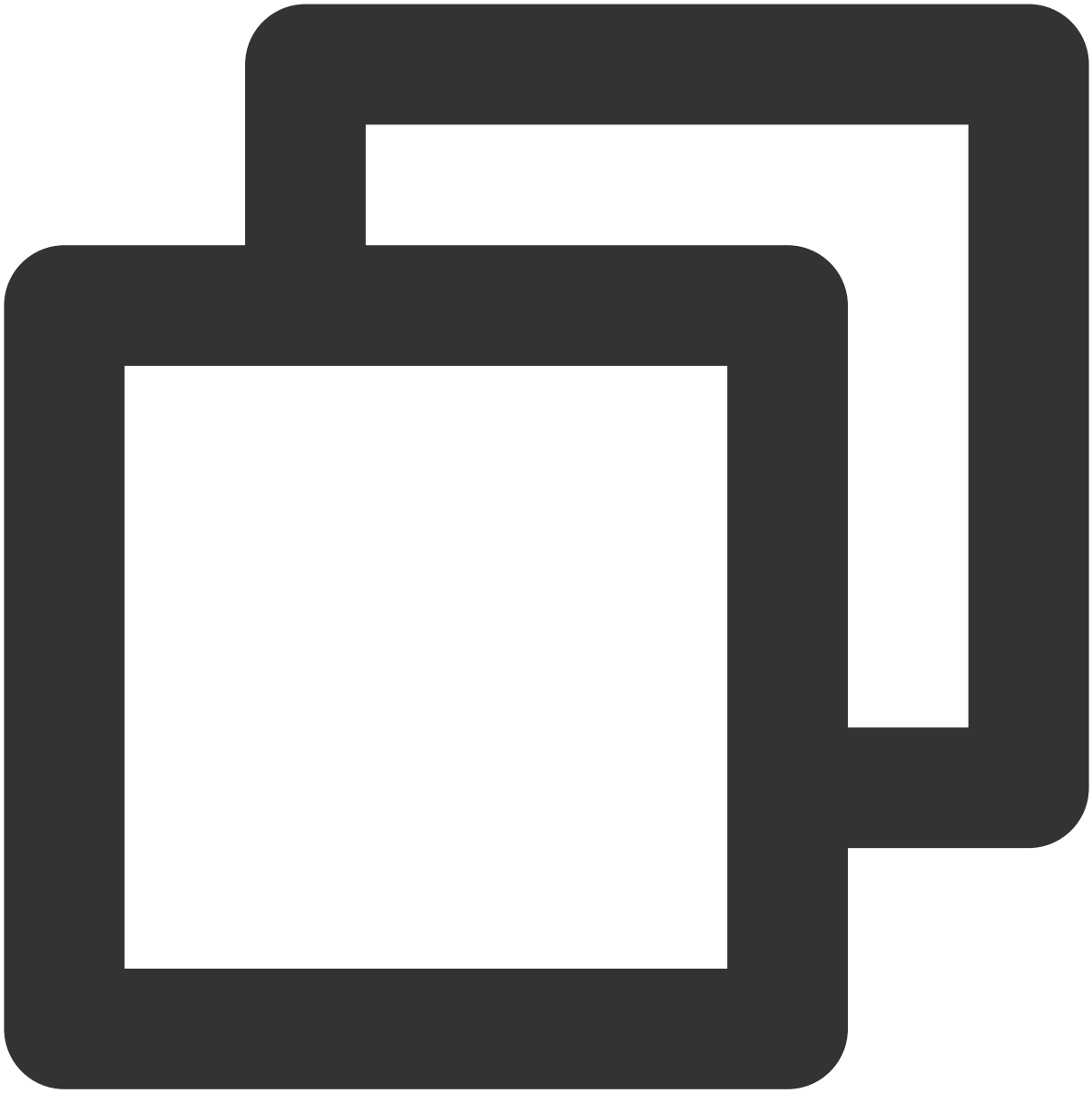
Directions

1. Log in to the CVM and run the following command to download the nic-hotplug.tgz tool.



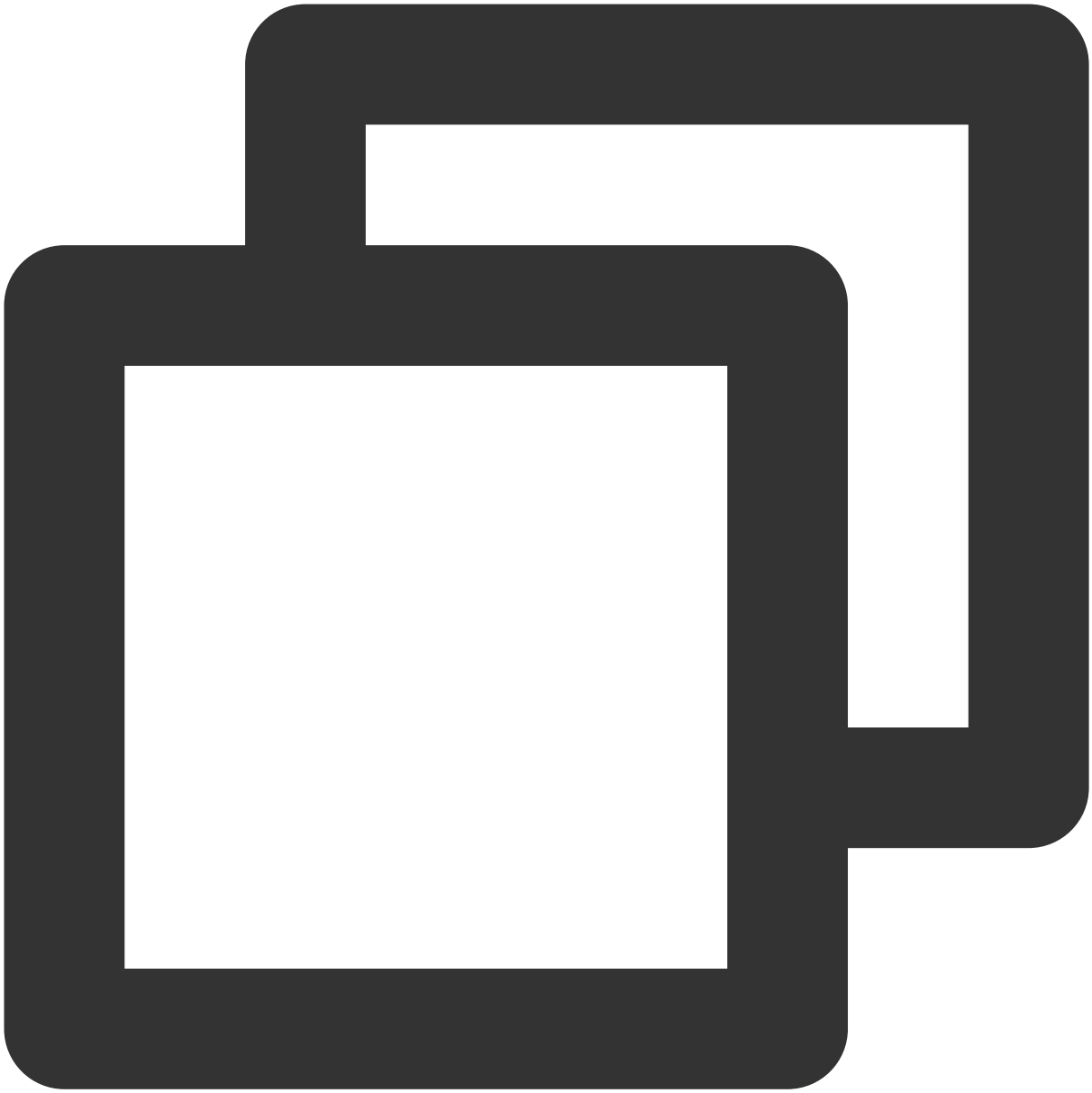
```
wget https://iso-1255486055.cos.ap-guangzhou.myqcloud.com/nic-hotplug.tgz
```

2. Run the following command to decompress the file.



```
tar -zxvf nic-hotplug.tgz
```

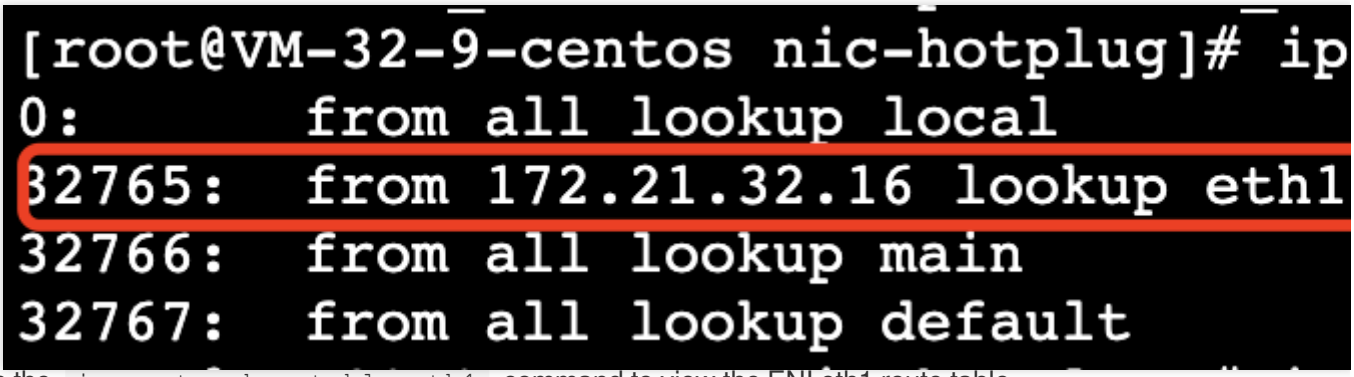
3. Run the following commands to grant the execute permission and install the tool.



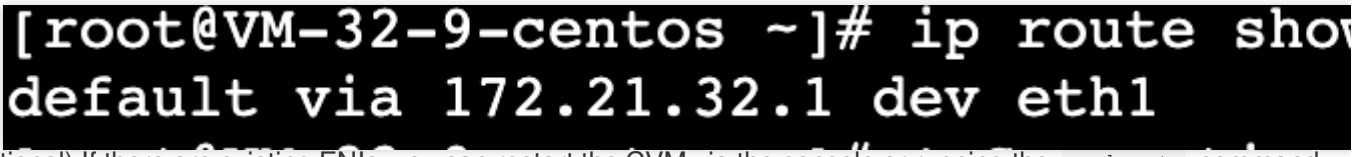
```
cd nic-hotplug
chmod +x ./install.sh
./install.sh
```

4. Bind an ENI, and then verify that the route of the new ENI eth1 has been distributed.

i. Run the `ip rule show` command. You can see that the policy-based route of the ENI eth1 has been added.



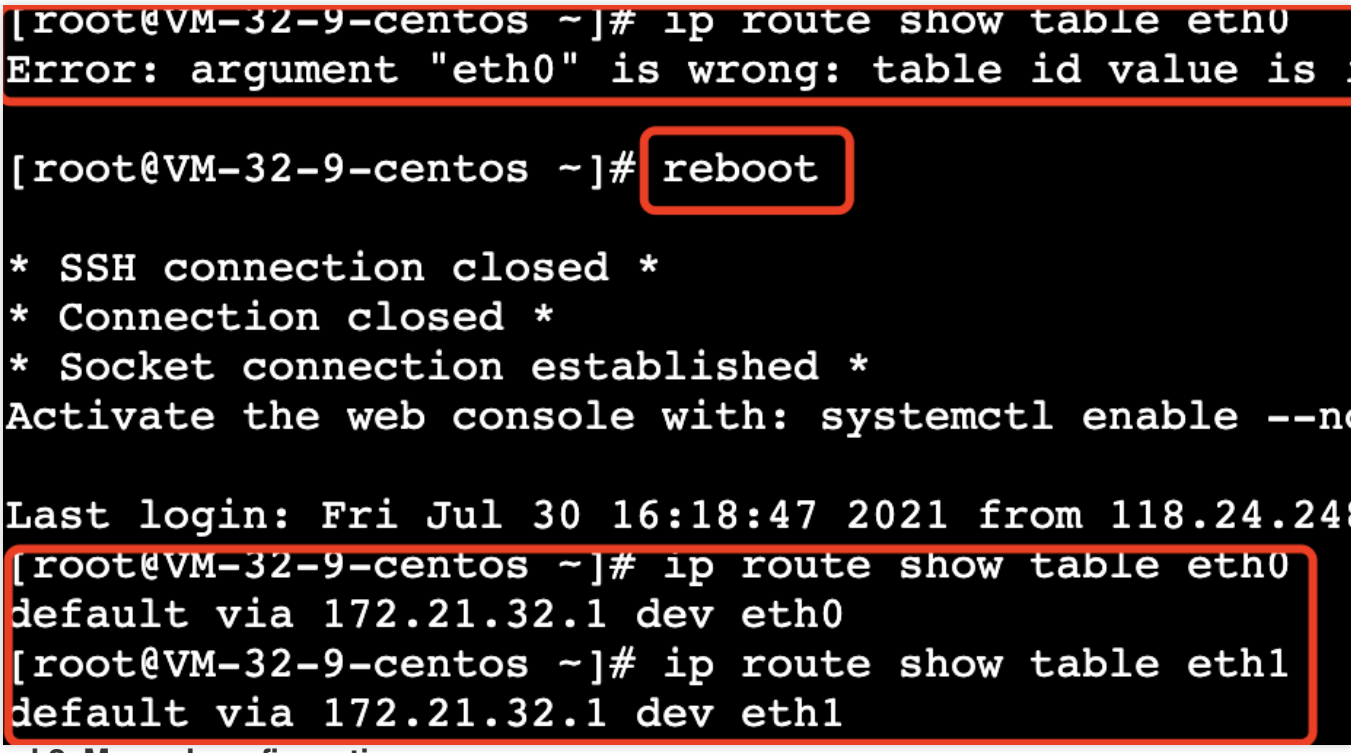
ii. Run the `ip route show table eth1` command to view the ENI eth1 route table.



5. (Optional) If there are existing ENIs, you can restart the CVM via the console or running the `reboot` command.

Then, the routes of all ENIs will be automatically distributed.

Restart CVM by running the command:



Method 2: Manual configuration

Note:

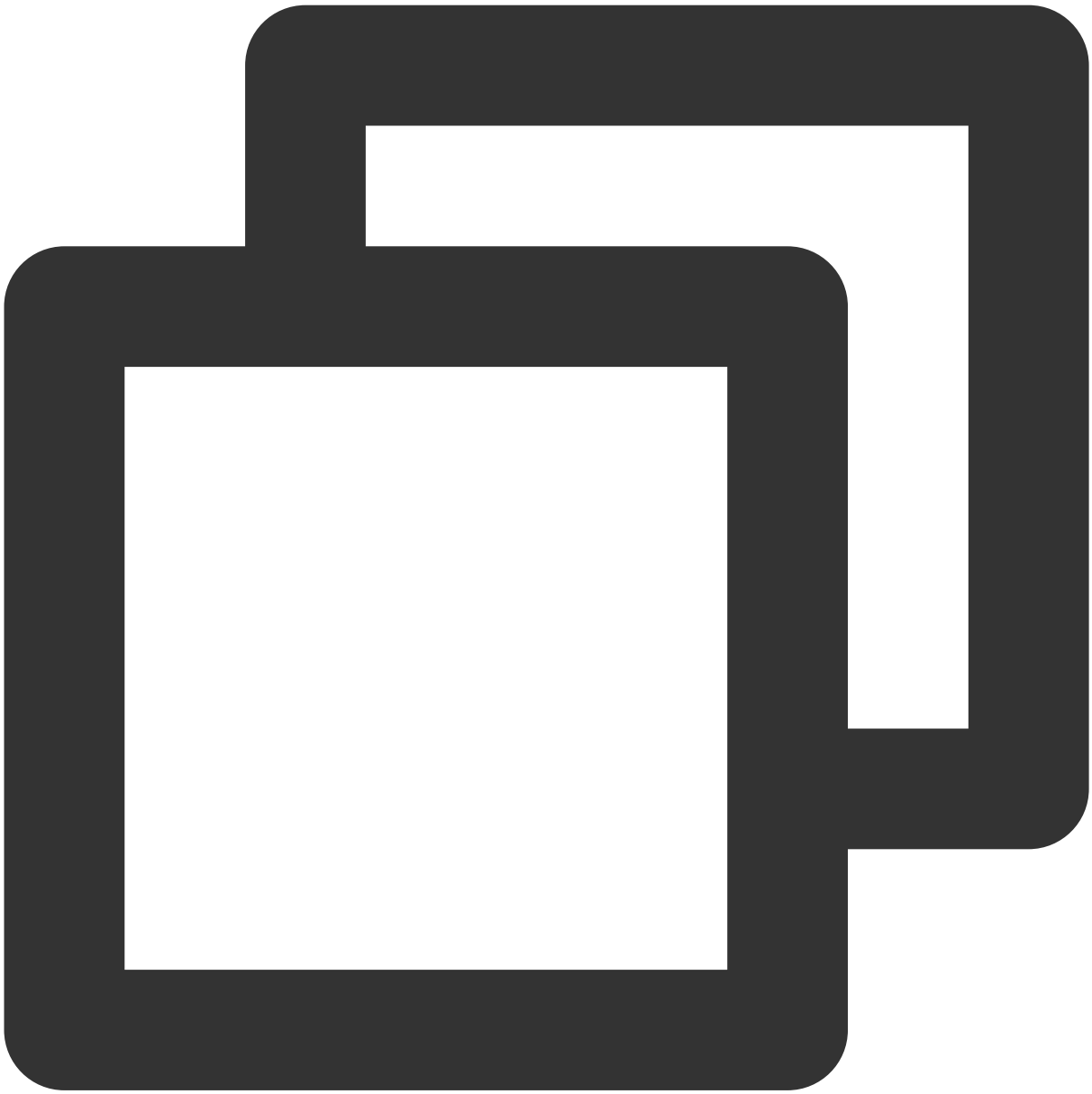
The following operations use CentOS 7.8 as an example.

Prerequisites

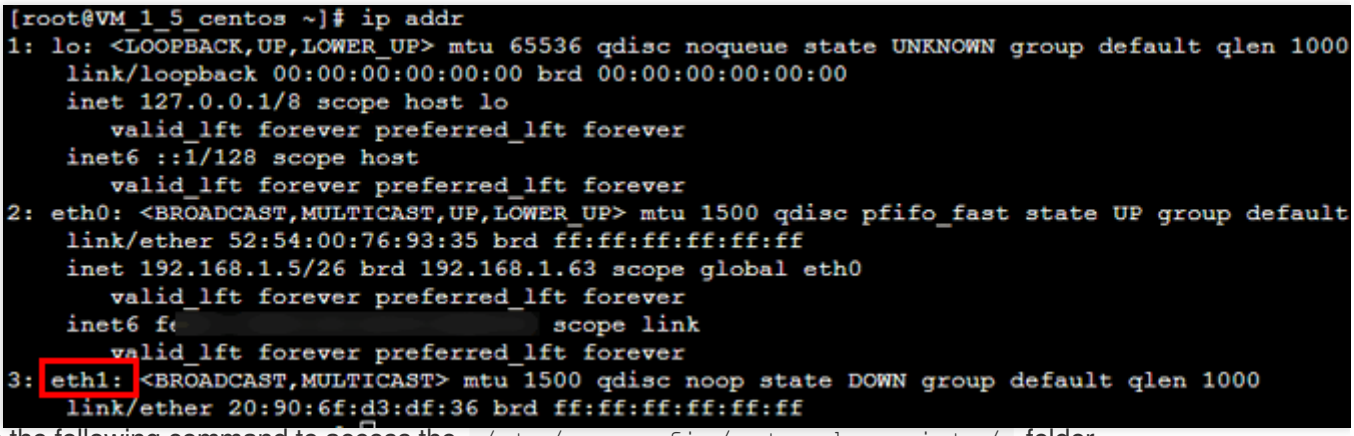
You have bound an ENI to the CVM. For detailed directions, see Binding ENI to CVM.

Directions

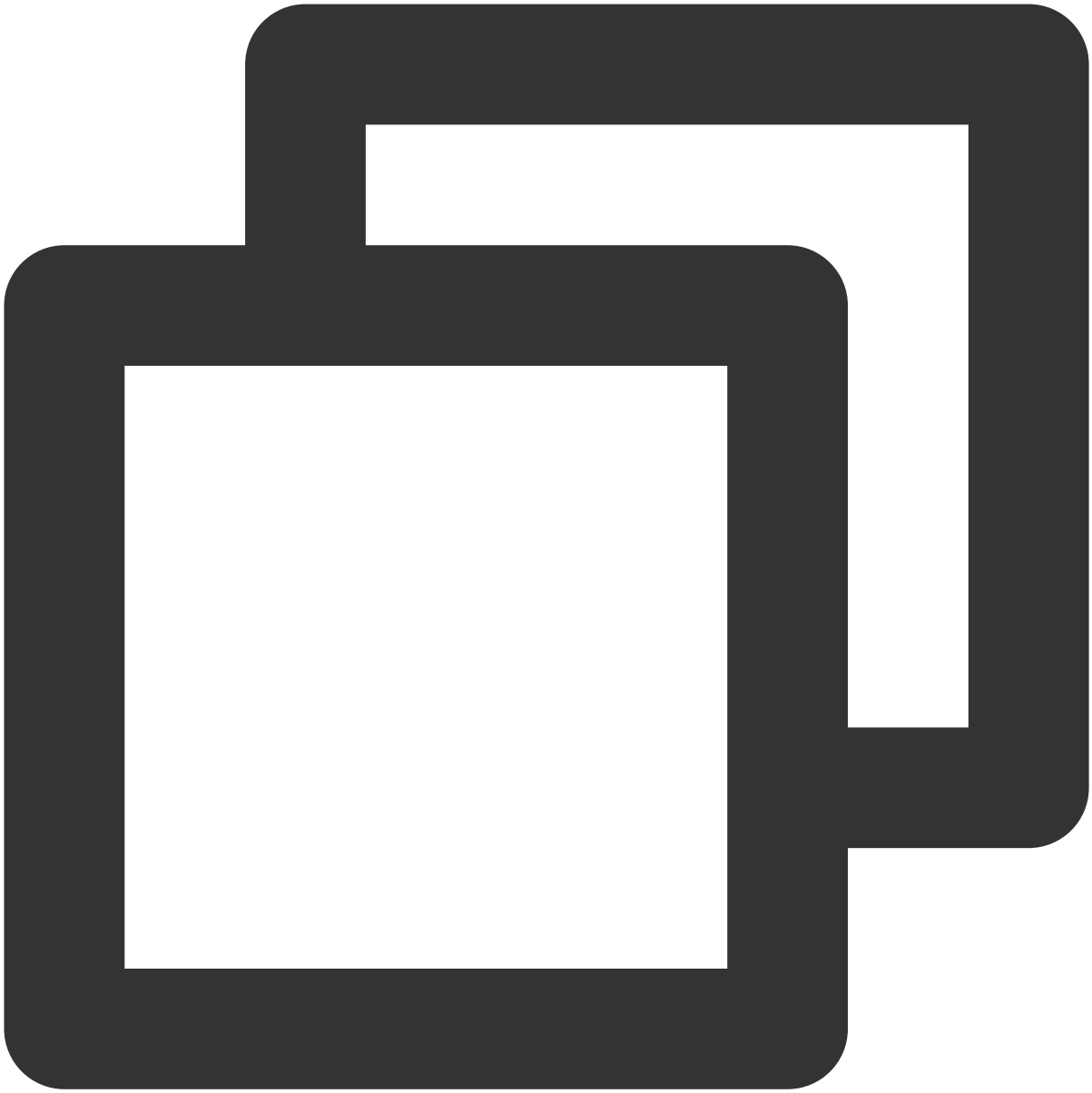
1. Log in to the CVM as the administrator and run the following command to locate the ENI to be configured (IP not shown). As shown in the figure, the ENI to be configured is `eth1`.



```
ip addr
```



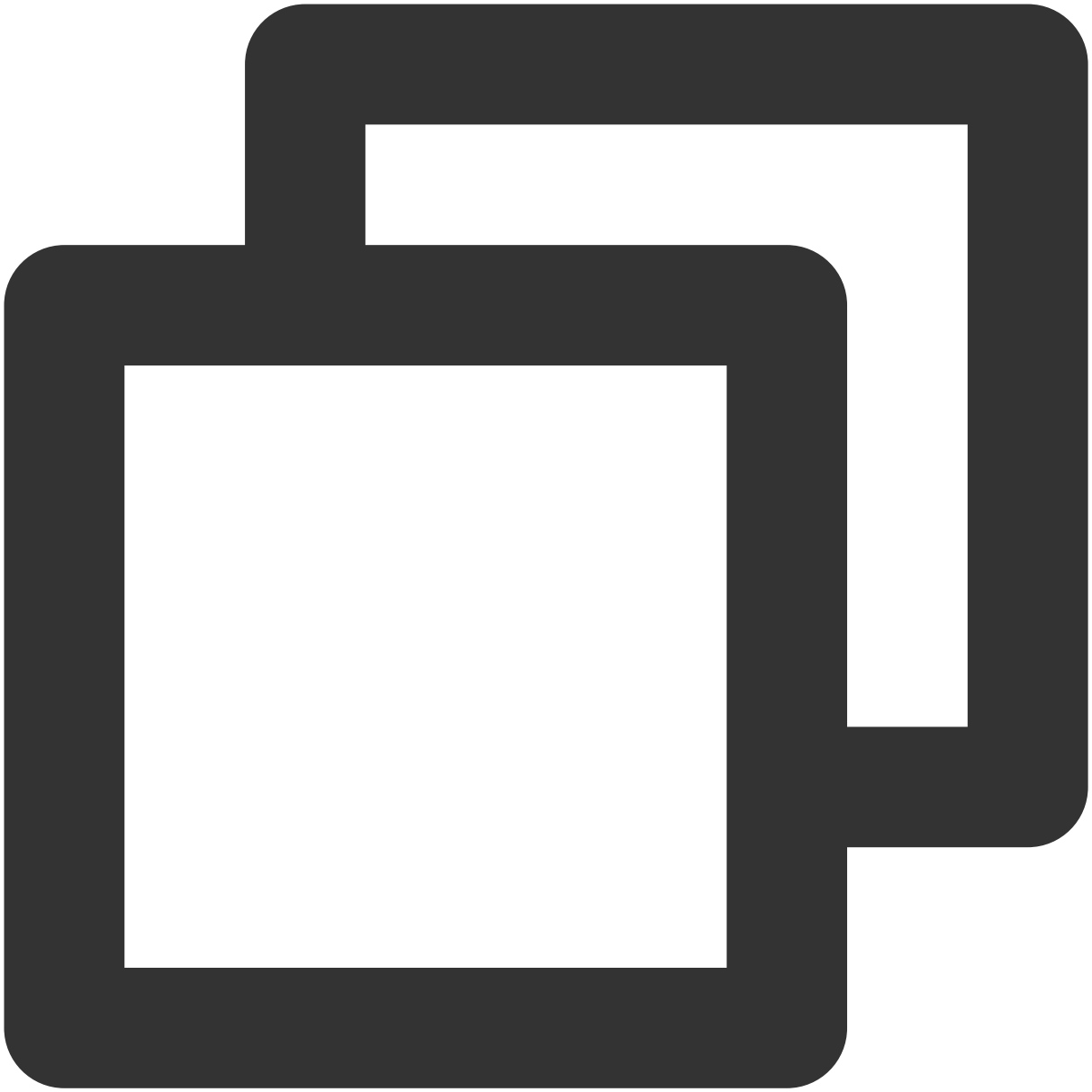
2. Run the following command to access the `/etc/sysconfig/network-scripts/` folder.



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

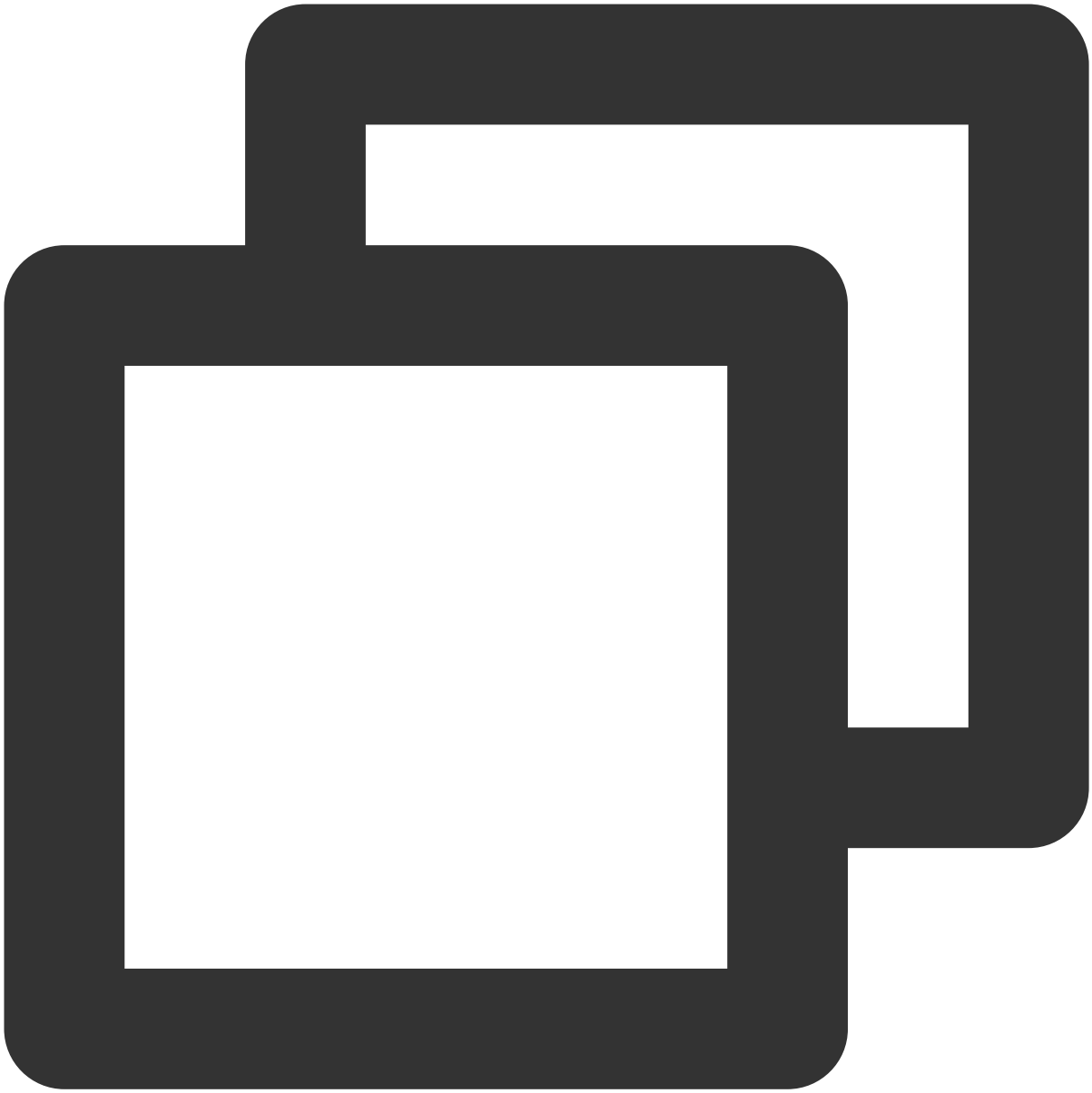
3. Create a configuration file such as `ifcfg-eth1` for the new ENI.

i. Run the following command.



```
cp ifcfg-eth0 ifcfg-eth1
```

ii. Run the following command to modify the configuration file.



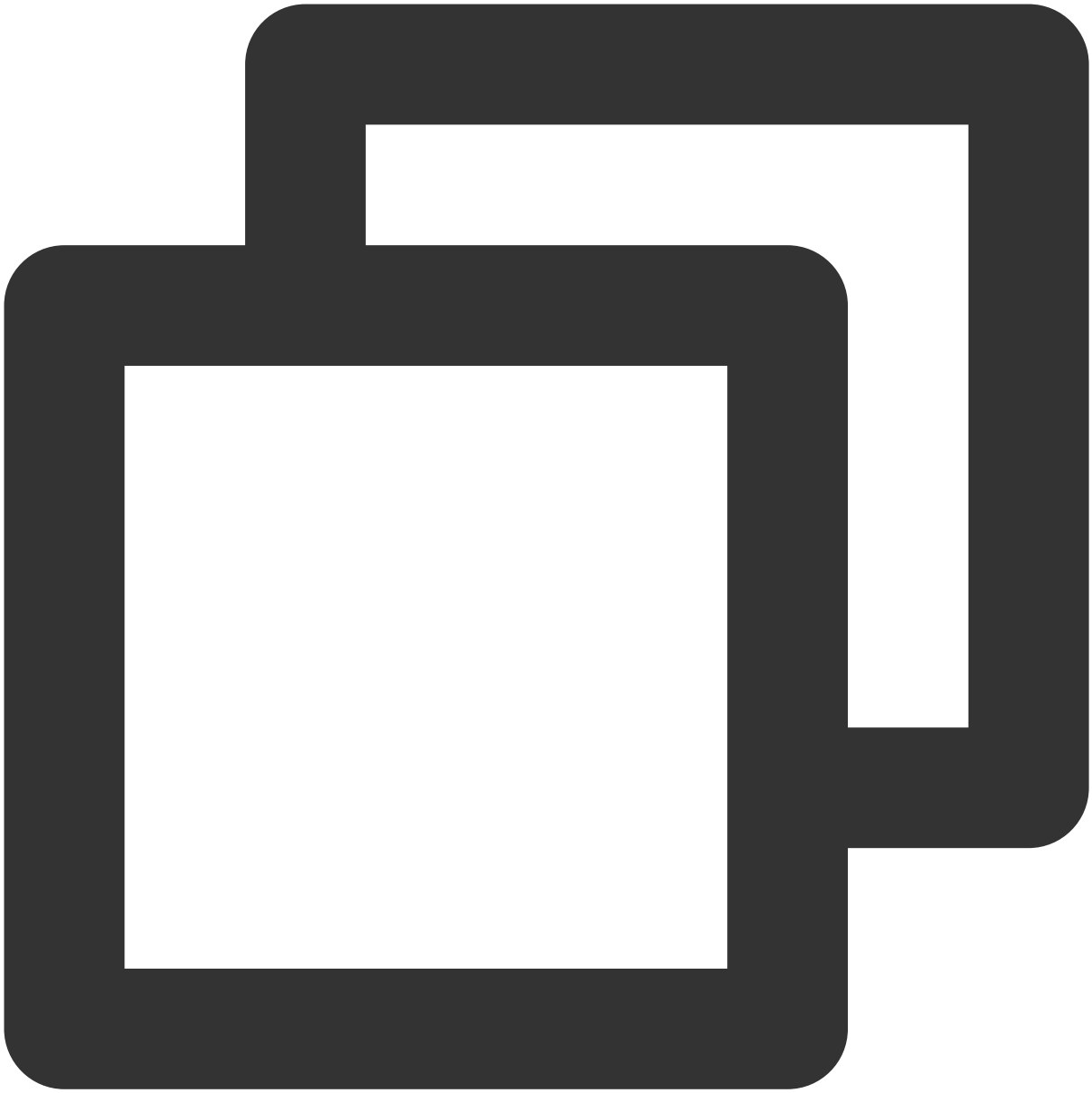
```
vim ifcfg-eth1
```

iii. Press **i** to switch to the edit mode and modify the configuration file as follows:

Note:

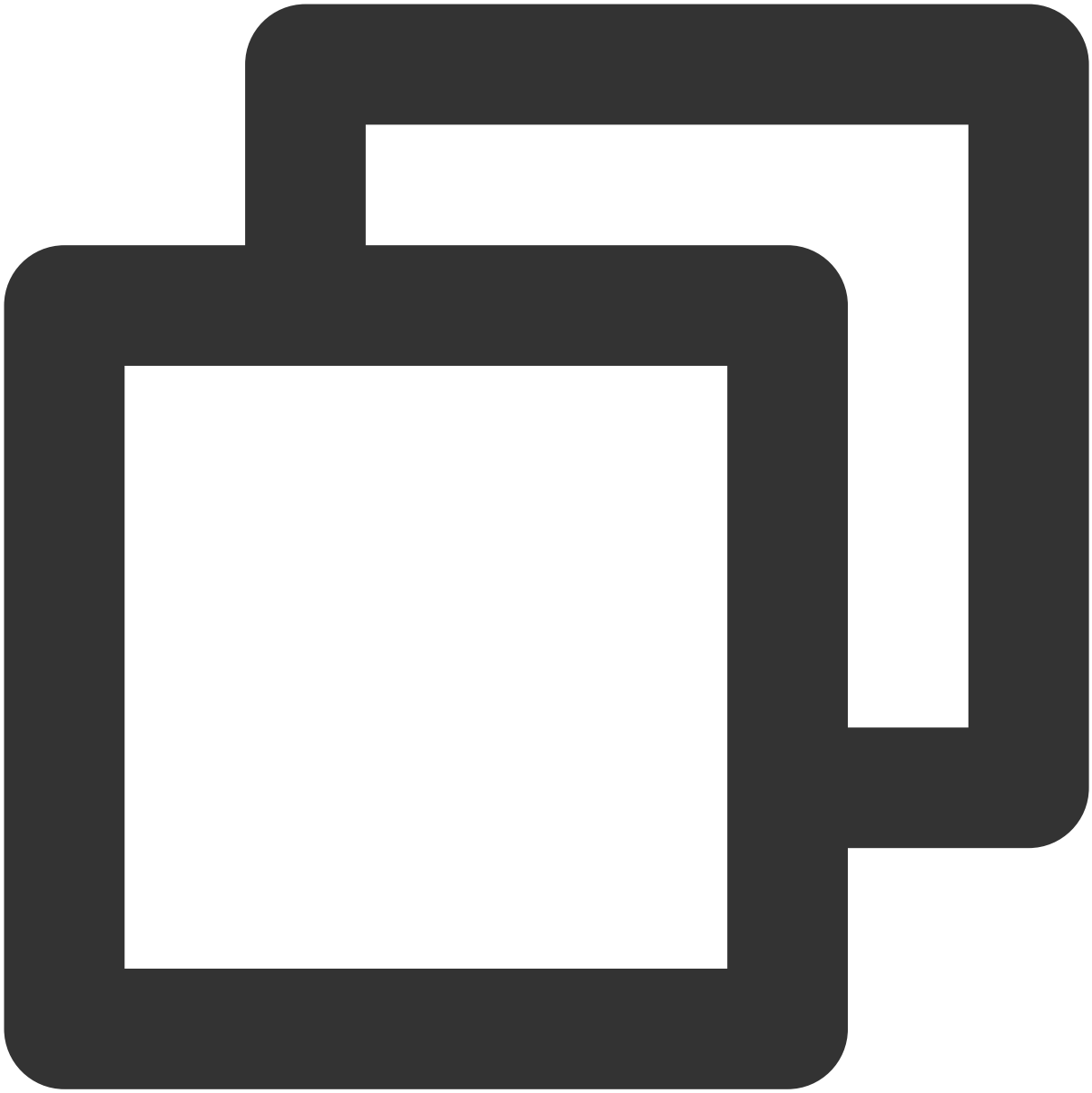
For the methods to view the IP address and subnet mask of the ENI, see the Appendix.

Mode 1: Statically manual IP configuration



```
DEVICE='eth1' # Enter the actual ENI name obtained in step 1.
NM_CONTROLLED='yes'
ONBOOT='yes'
IPADDR='192.168.1.62'  # Enter the actual IP address of the ENI.
NETMASK='255.255.255.192'  # Enter the actual subnet mask.
#GATEWAY='192.168.1.1'  # Enter the actual IP address of the gateway of the subnet
```

Mode 2: Dynamically acquire IP address



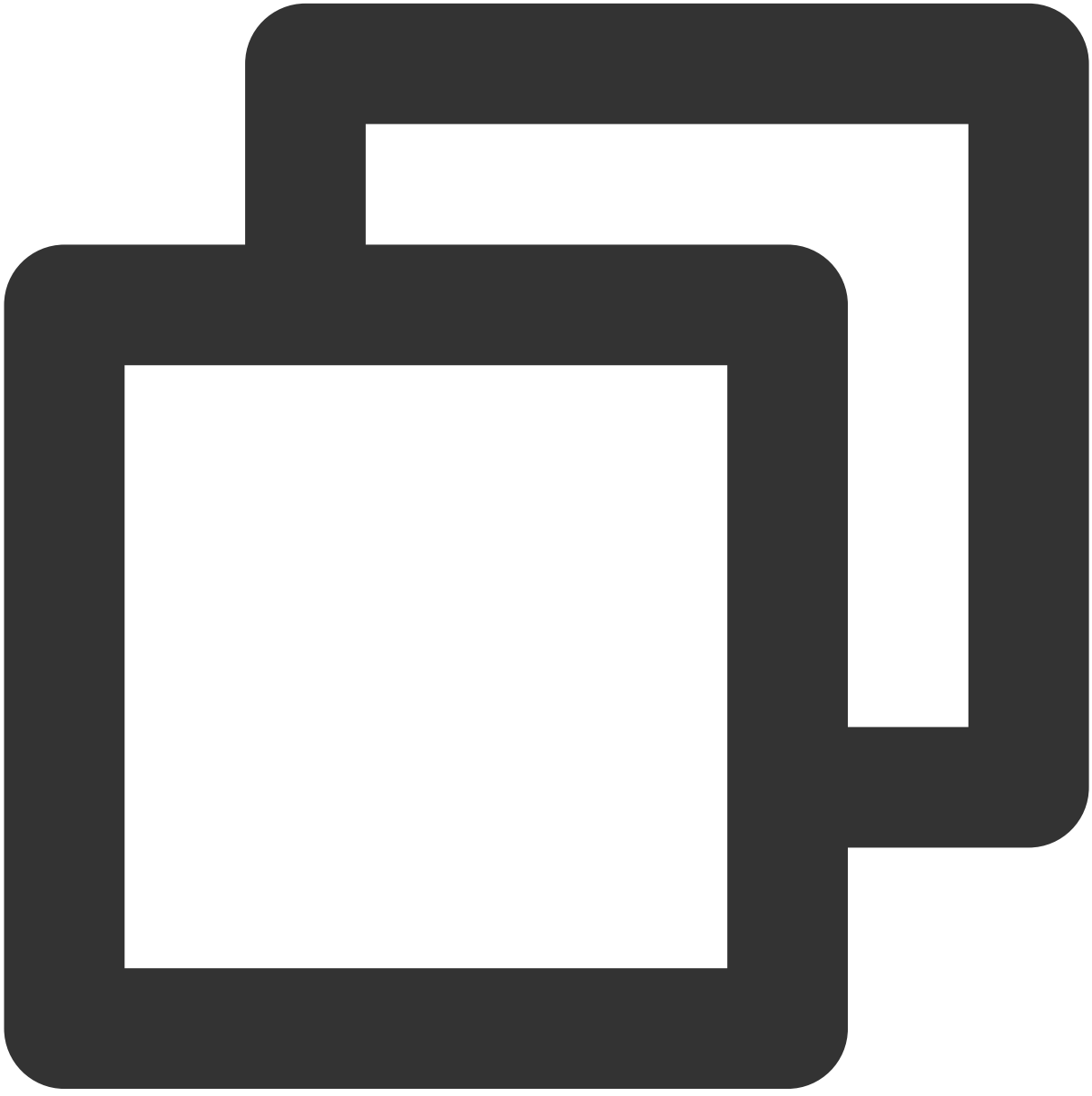
```
BOOTPROTO=dhcp     #Automatically acquire IP address
DEVICE=eth1        # Enter the name of the ENI to be configured
HWADDR=20:90:6F:63:98:CC    # Please replace it with the actual MAC address of the
ONBOOT=yes
PERSISTENT_DHCLIENT=yes
TYPE=Ethernet
USERCTL=no
PEERDNS=no
DEFROUTE=no    # Determine whether to set the ENI as the default route. Do not set
```

3.1 Press **Esc** when you get to the last line of vim, enter **wq!**, and then press **Enter** to save and close the configuration file.

4. Run the following command to restart the network service for the configuration to take effect.

Note:

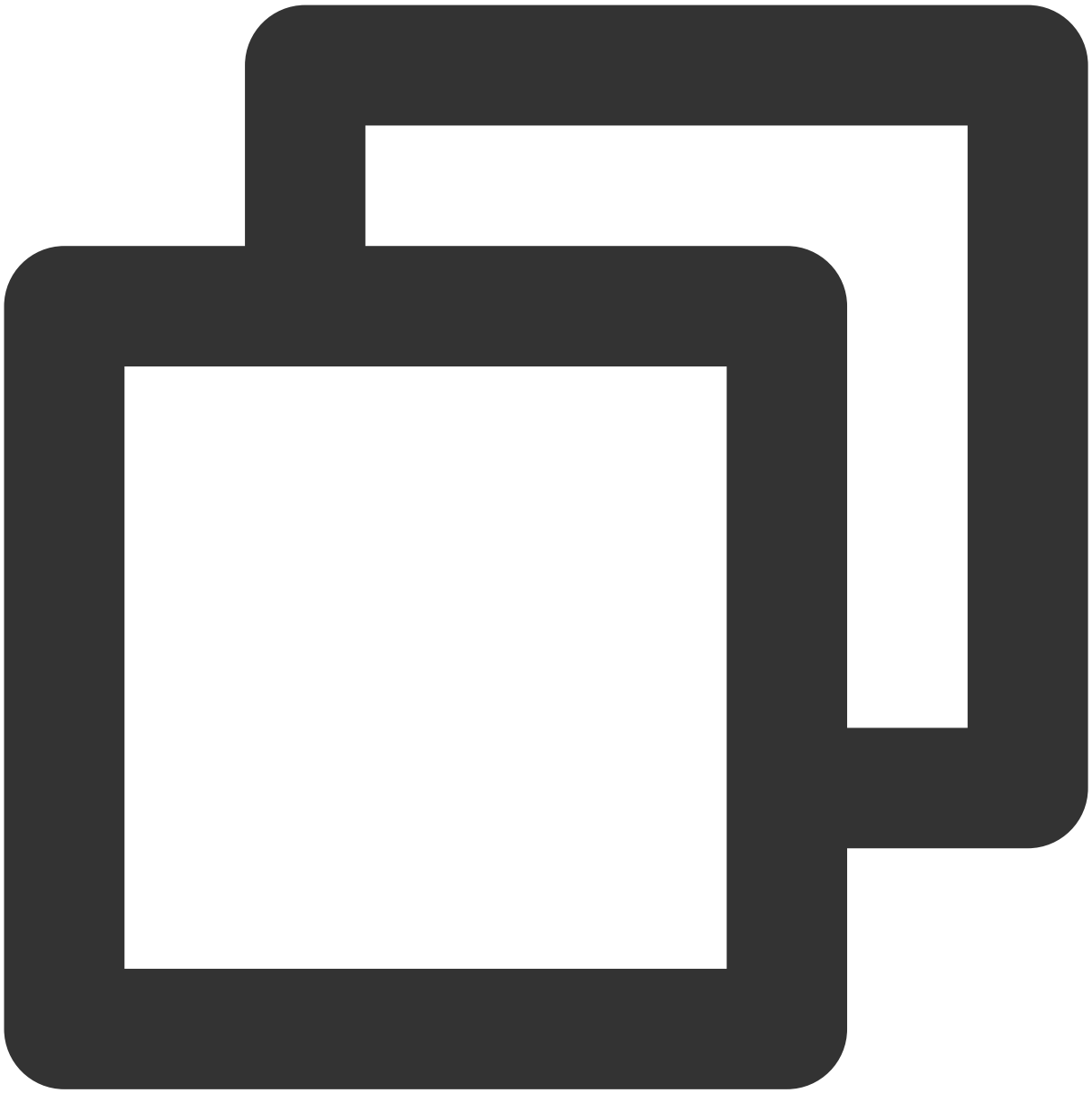
If you have configured DNS, the resolv.conf file may be reset after the network is restarted, and the DNS resolution may be affected.



```
systemctl restart network
```

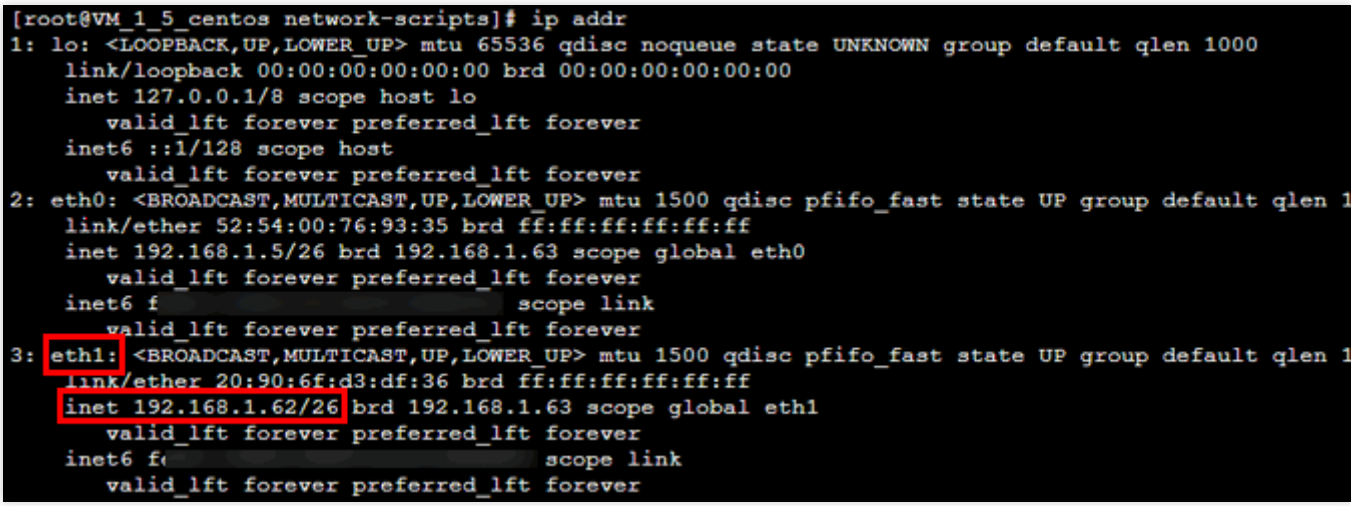
5. Check and verify the IP configuration.

5.1 Run the following command to check the IP address.



```
ip addr
```

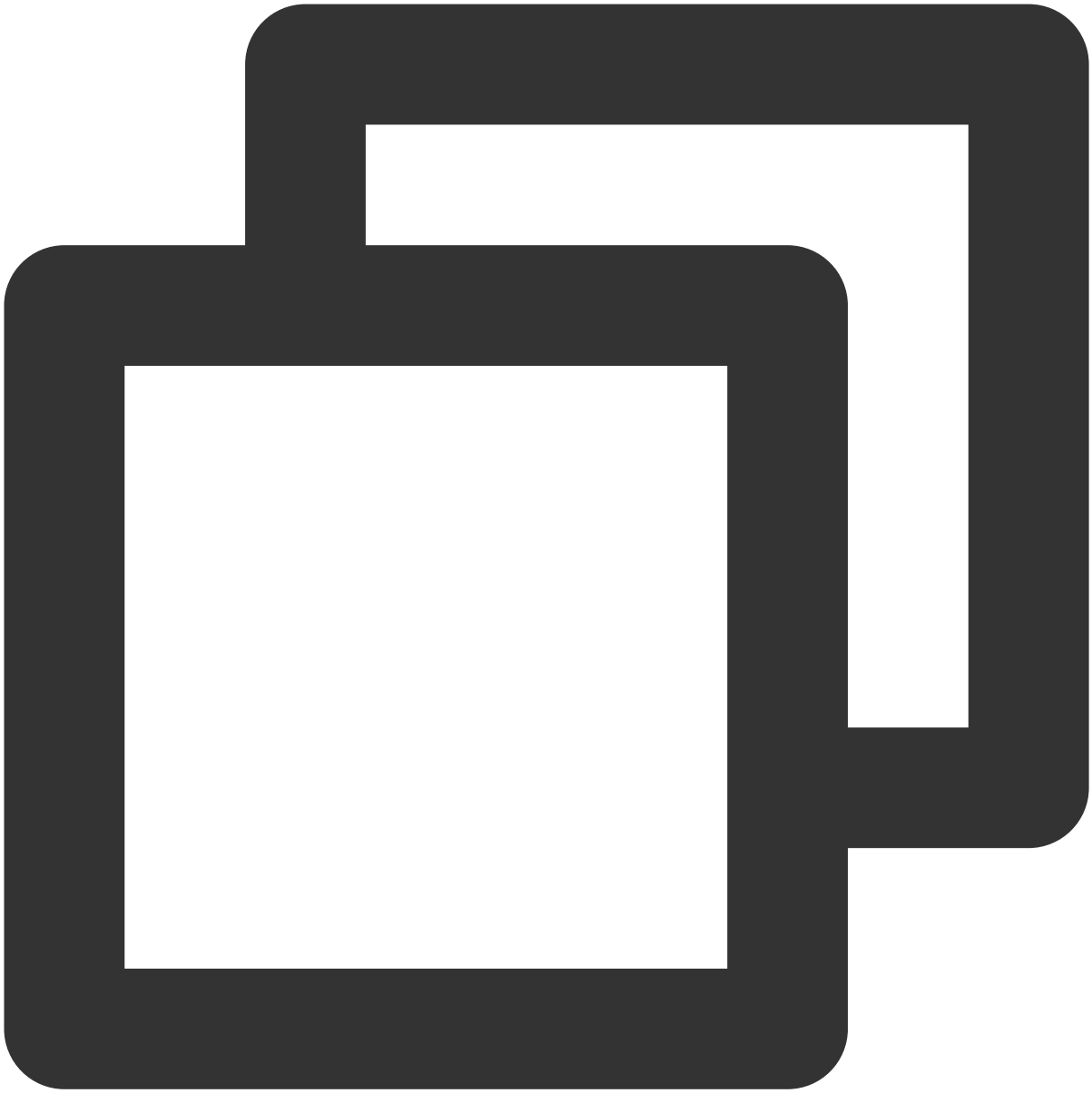
5.2 Confirm that the secondary ENI and its IP are visible, as shown below:



If the IP address is incorrectly configured, perform the following checks:

5.2.1 Verify the configuration file. Reconfigure the file if needed.

5.2.2 Confirm whether the network service has restarted. You can run the following command to restart the network for the configuration to take effect.



```
systemctl restart network
```

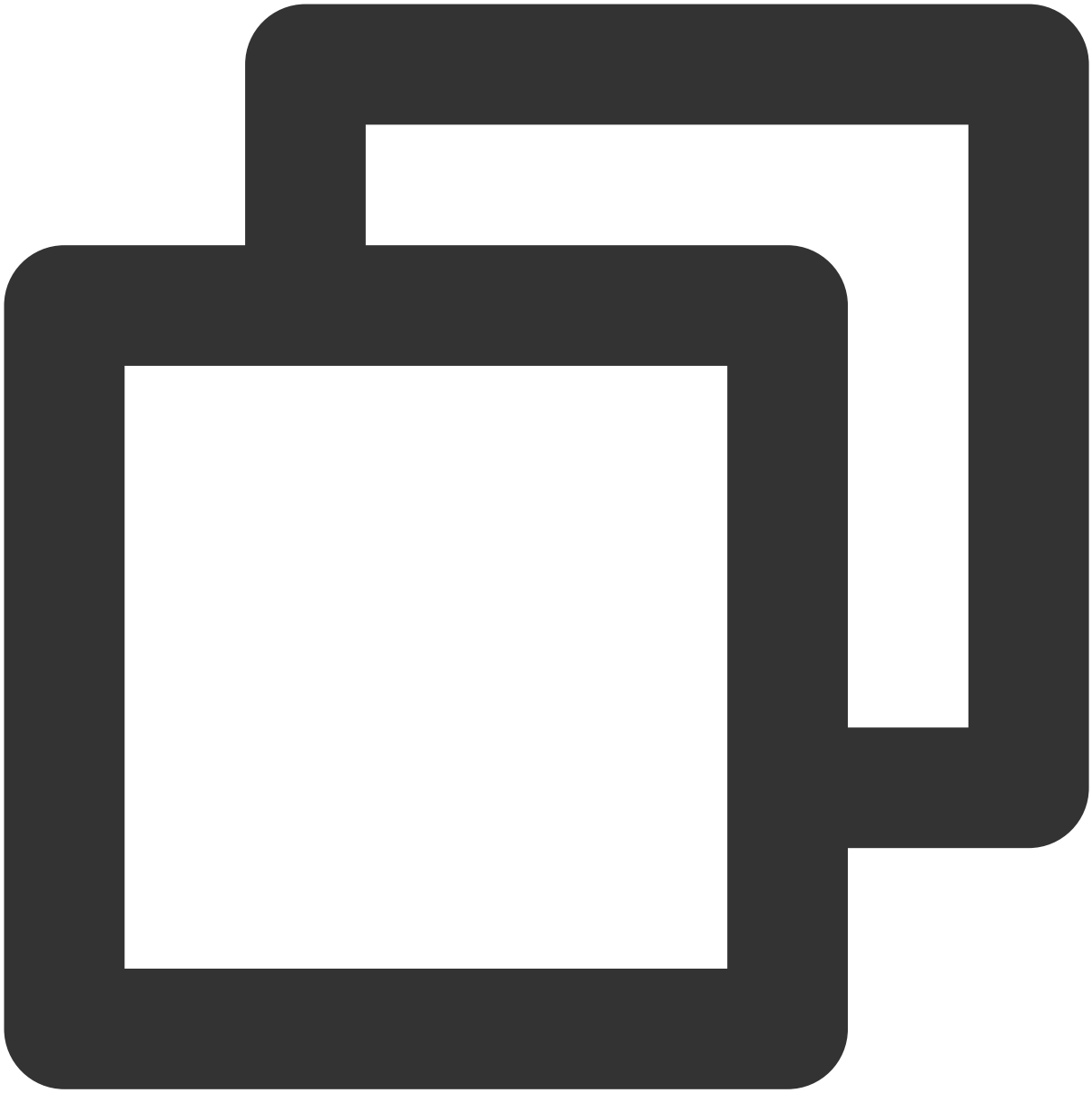
6. Configure the routing policy based on actual needs.

After the preceding configuration, the Linux image still sends packets from the primary ENI by default. In this case, you can configure policy-based routing to specify the ENI through which packets are sent and returned.

6.1 Creat

e two route

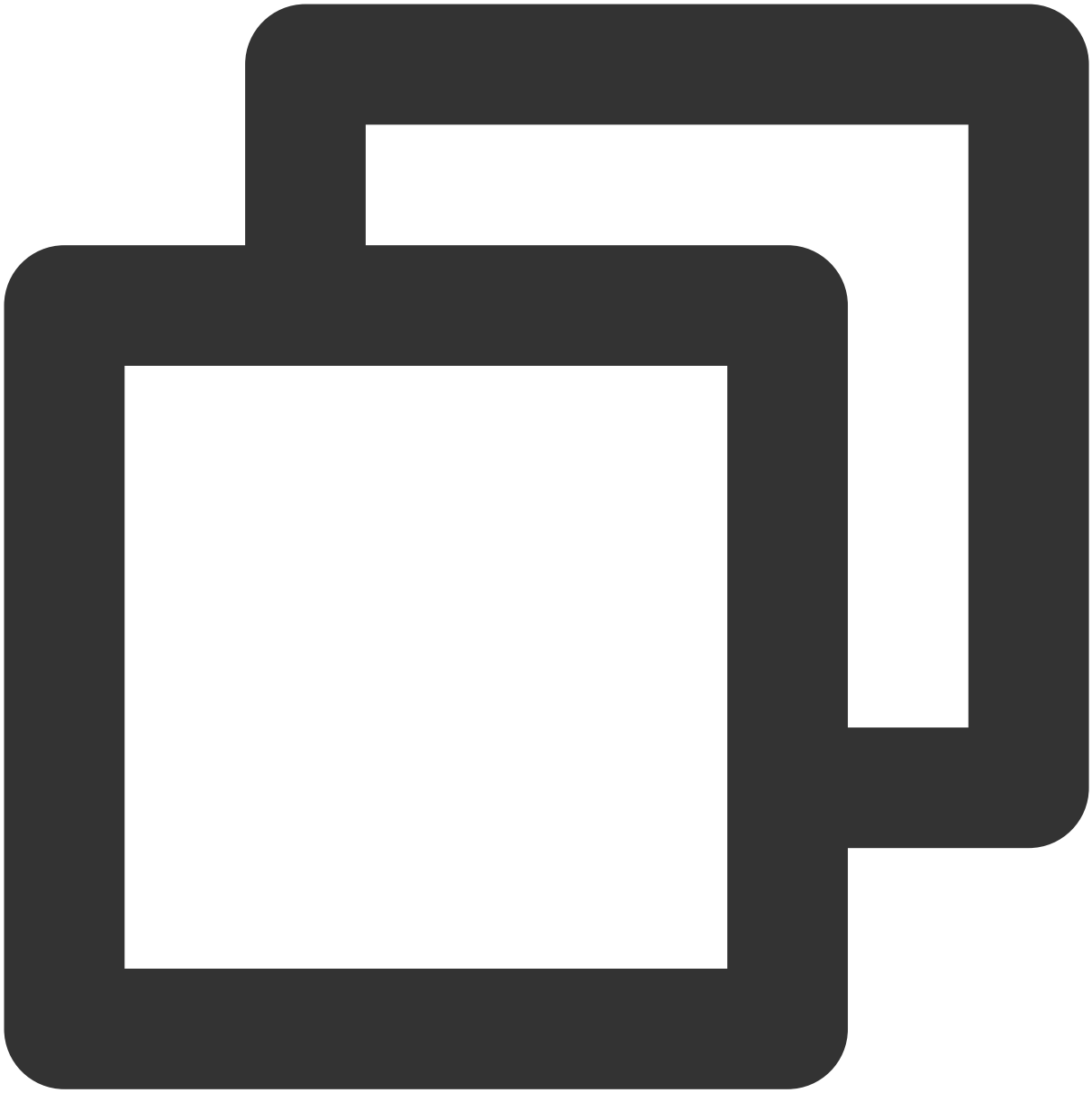
tables.



```
echo "10 t1" >> /etc/iproute2/rt_tables    #Replace “10” with the actual route ID a
echo "20 t2" >> /etc/iproute2/rt_tables   #Replace “20” with the actual route ID an
```

6.2 Add default routes for both route tables in the following two ways.

Configure a temporary policy-based route, which needs to be re-configured after restarting the network). Run the following command.



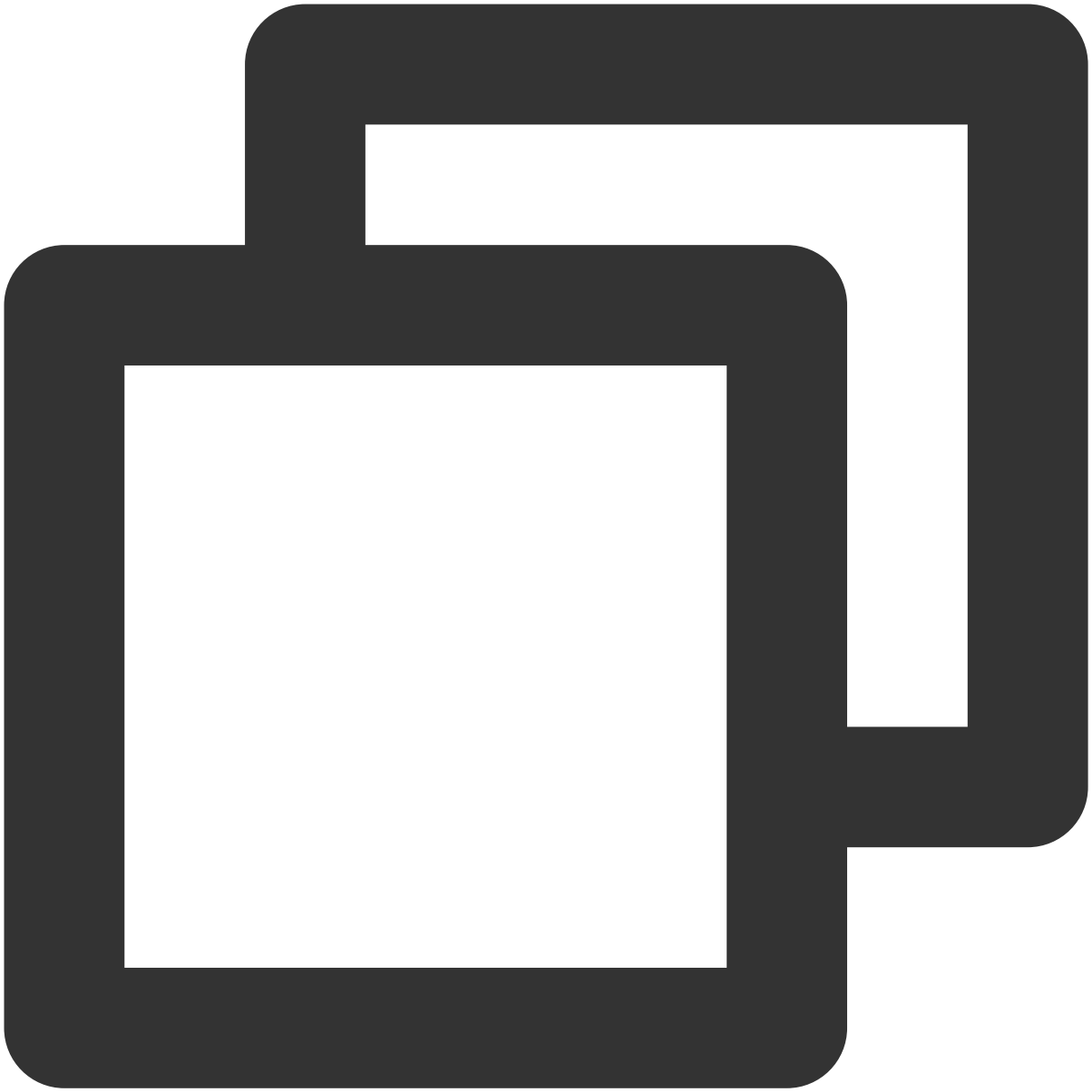
```
ip route add default dev eth0 via 192.168.1.1 table 10   #Replace “192.168.1.1” wit
ip route add default dev eth1 via 192.168.1.1 table 20   #Replace “192.168.1.1” wit
```

Note:

For gateway details, see [Viewing the gateway] (#.E6.9F.A5.E7.9C.8B.E7.BD.91.E5.85.B3) .

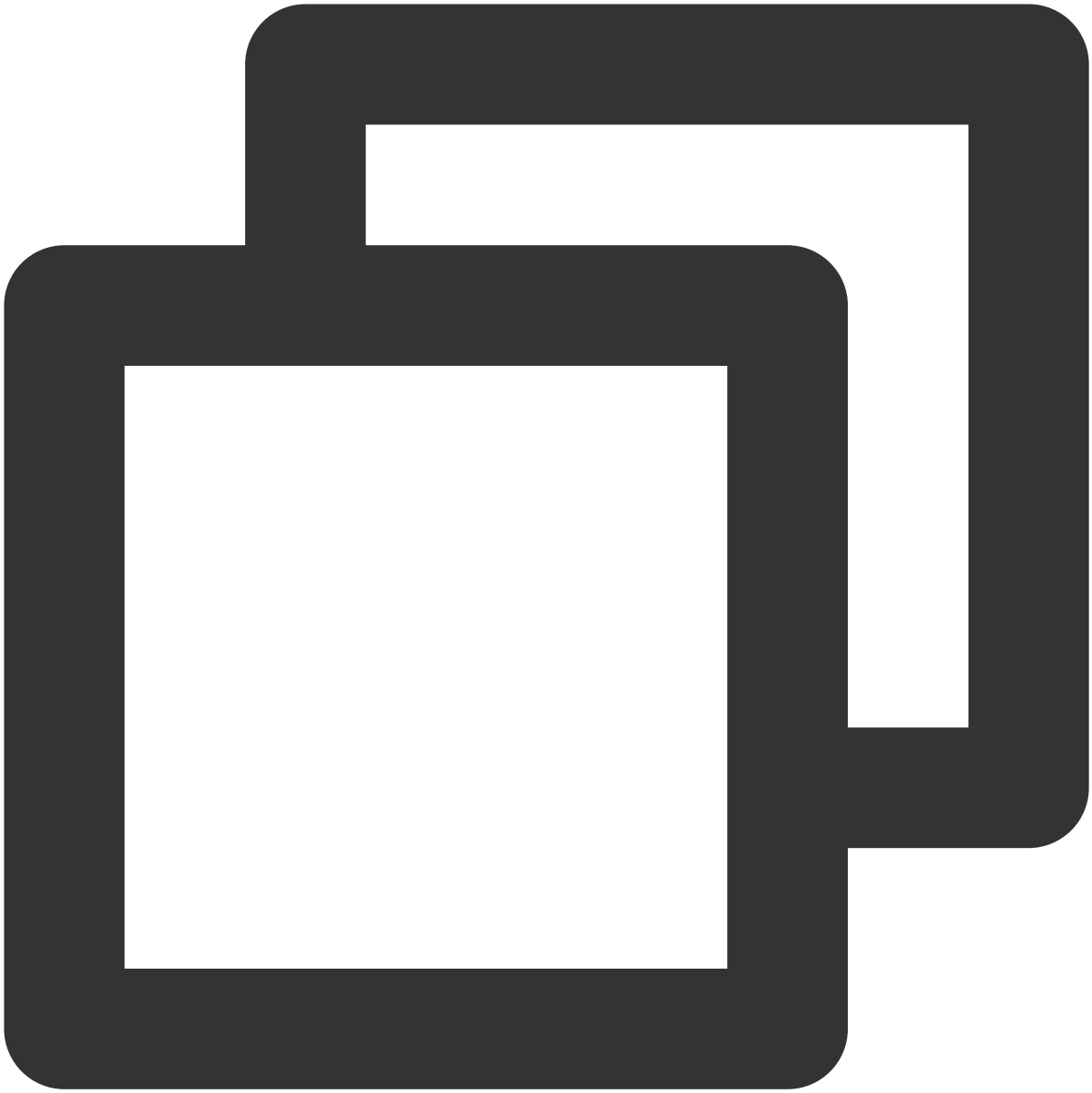
Configure a permanent policy-based route, which can be saved in the configuration file. The following operations use CentOS 7.8 as an example.

6.2.1 Edit the configuration file "route-ENI name" (such as route-eth0) under the directory "/etc/sysconfig/network-scripts/".



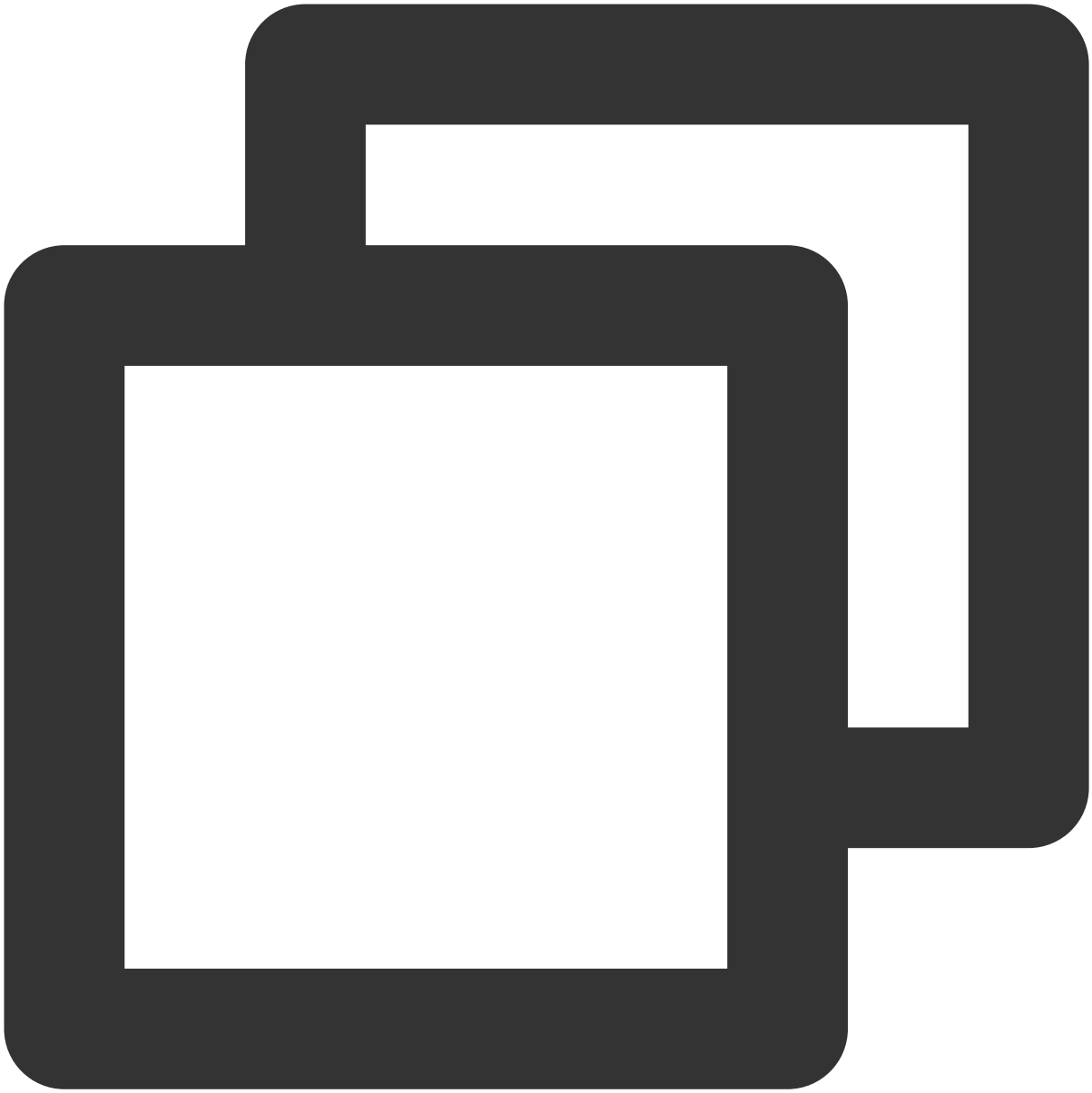
```
vim /etc/sysconfig/network-scripts/route-eth0    # Edit the route-eth0 file
```

6.2.2 Add a line of command: `default dev [ENI name, such as eth0] via [the gateway of the ENI, such as 192.168.1.1] table [code of the policy-based route table, such as 10]`. For example,



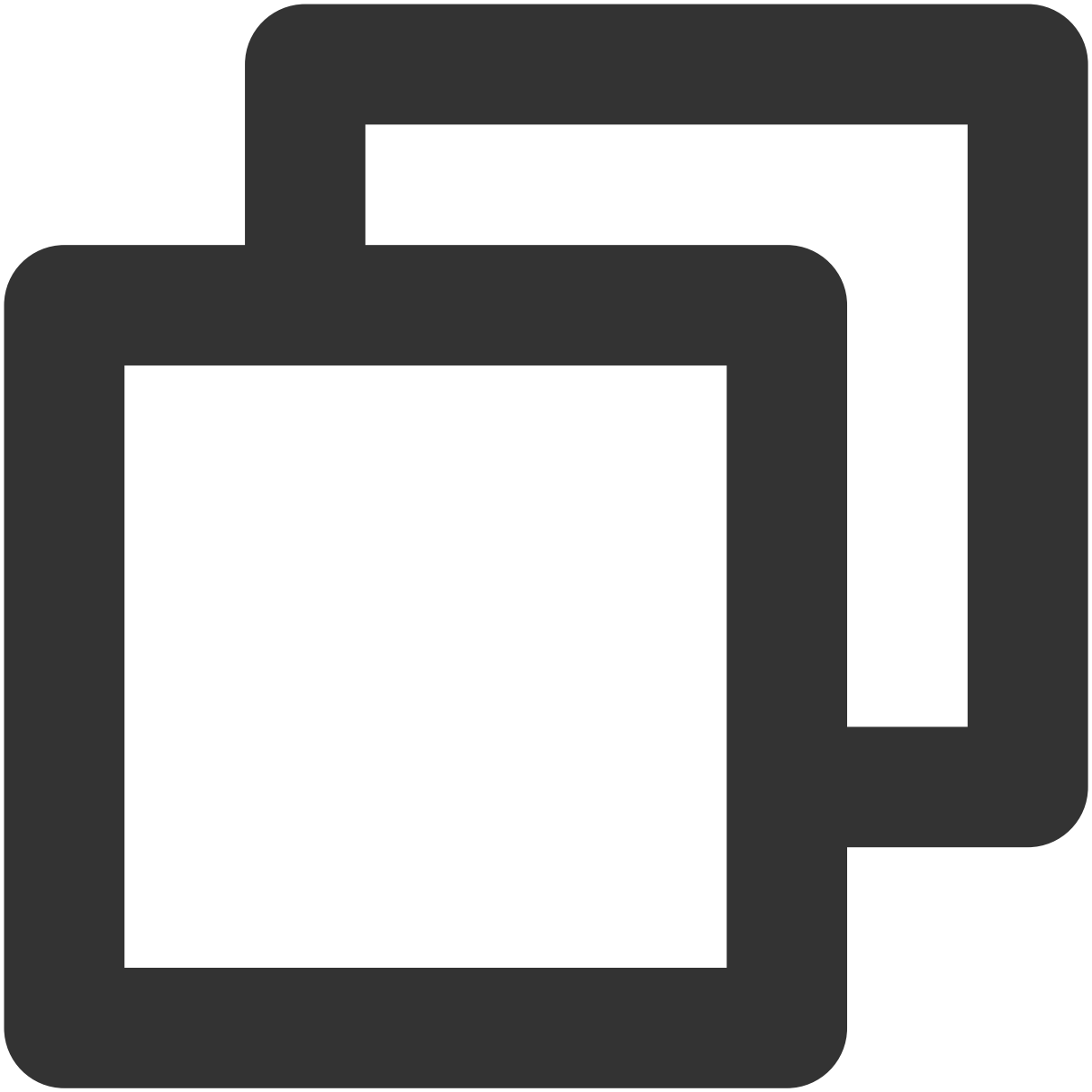
```
default dev eth0 via 192.168.1.1 table 10        # Add a default gateway for route
```

6.2.3 Press "ESC", and enter " wq!" to save and exit. Then follow the same operation to configure the route-eth1 file.



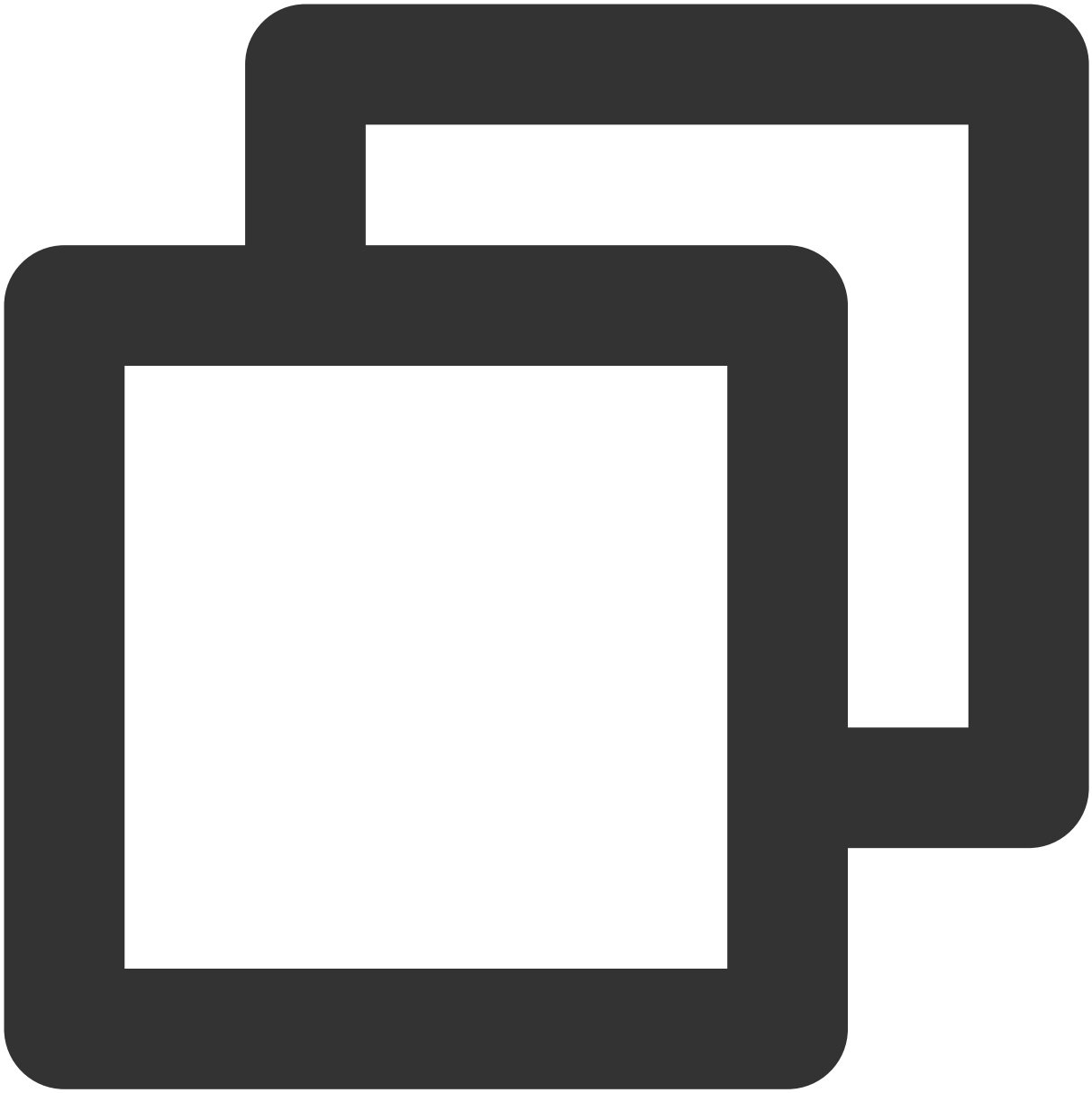
```
vim /etc/sysconfig/network-scripts/route-eth0    # Edit the route-eth1 file
default dev eth0 via 192.168.1.1 table 20        # Add a default gateway for route
```

6.2.4 Restart the network for the configuration to take effect.



```
systemctl restart network
```

6.3 Configure a policy-based routing policy.

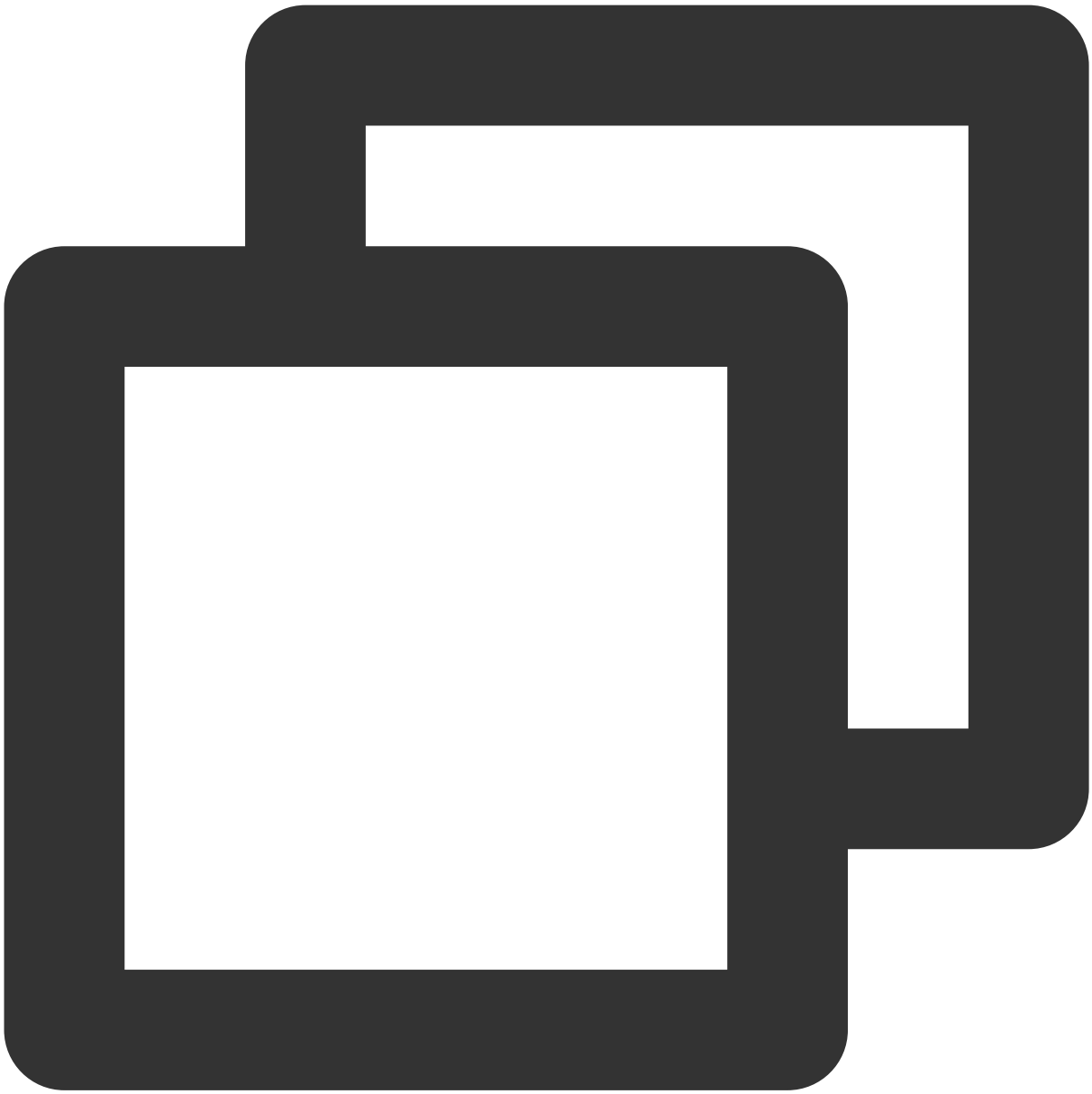


```
ip rule add from 192.168.1.5 table 10     #Enter the actual IP address of the prima
ip rule add from 192.168.1.62 table 20     #Enter the actual IP address of the seco
```

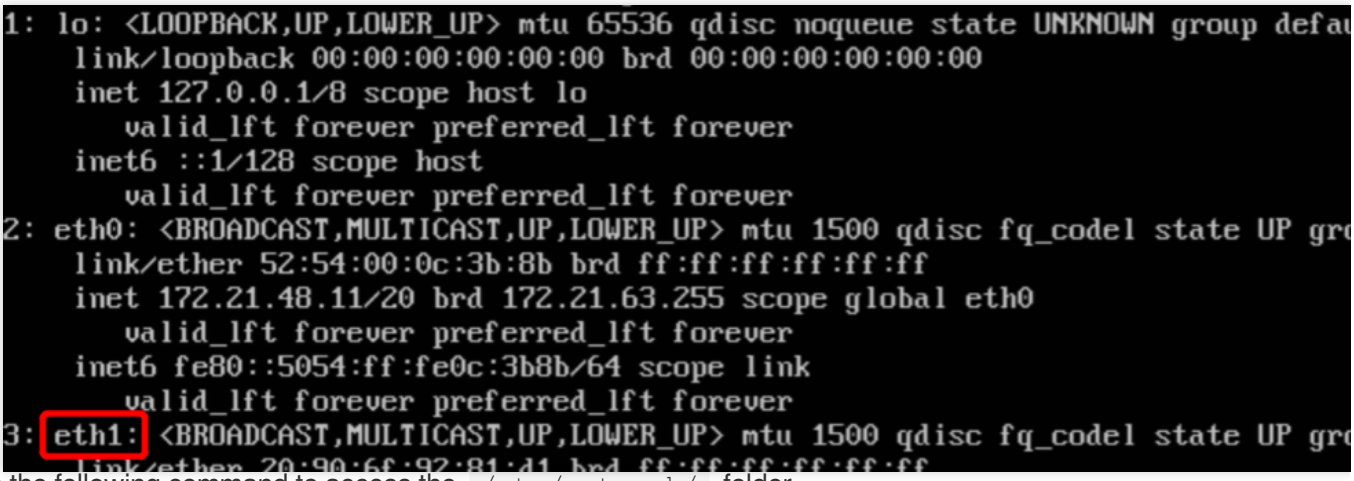
7. After completing the configuration, you can ping the private IP of a CVM that is in the same subnet. If the pinging succeeds, the configuration is correct. If no other CVM exists, you can bind the private IP of the secondary ENI to a public IP and then ping the public IP.

Configuring ENI on an Ubuntu CVM

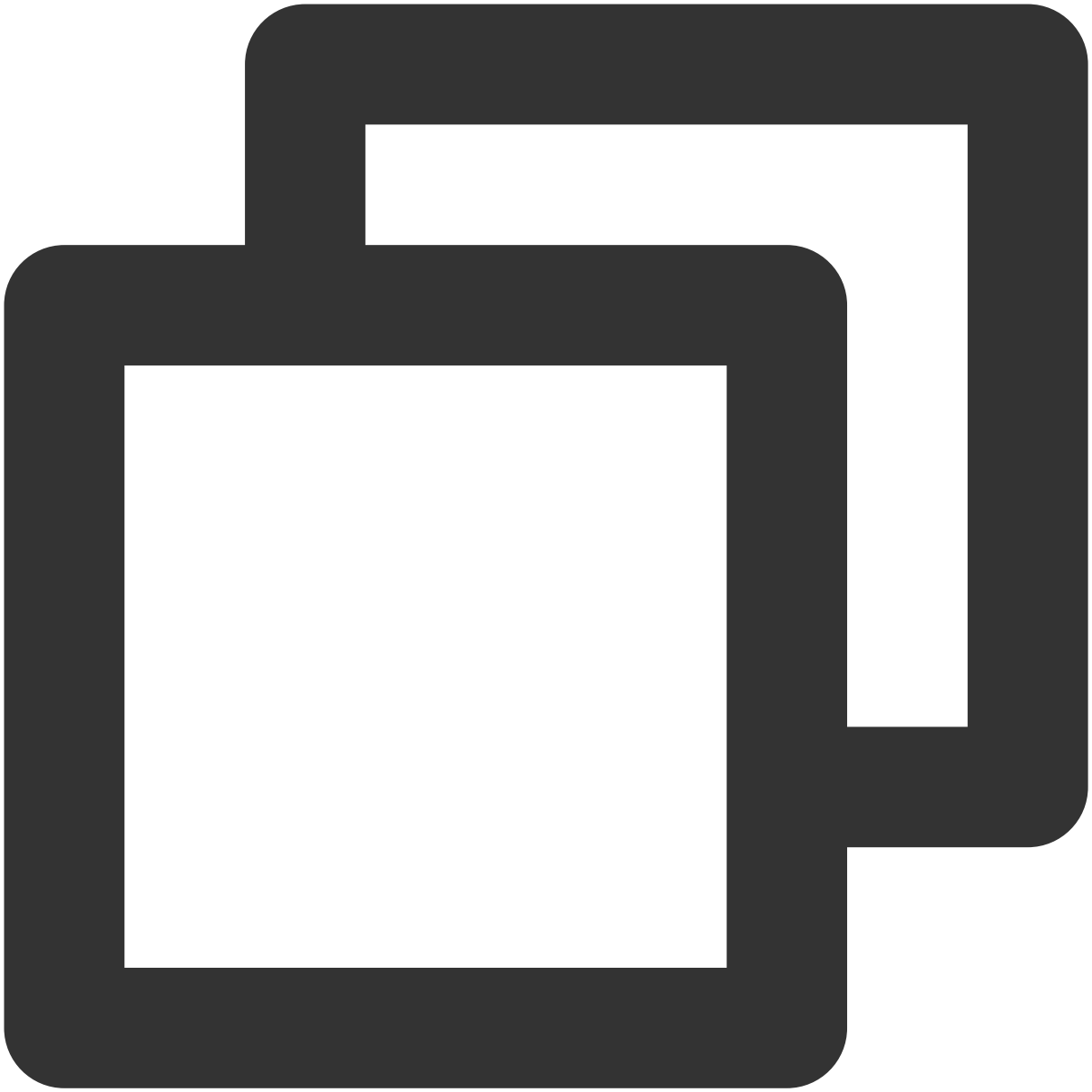
1. Log in to the CVM as the administrator and run the following command to locate the ENI to be configured (IP not shown). As shown in the figure, the ENI to be configured is `eth1`.



```
ip addr
```



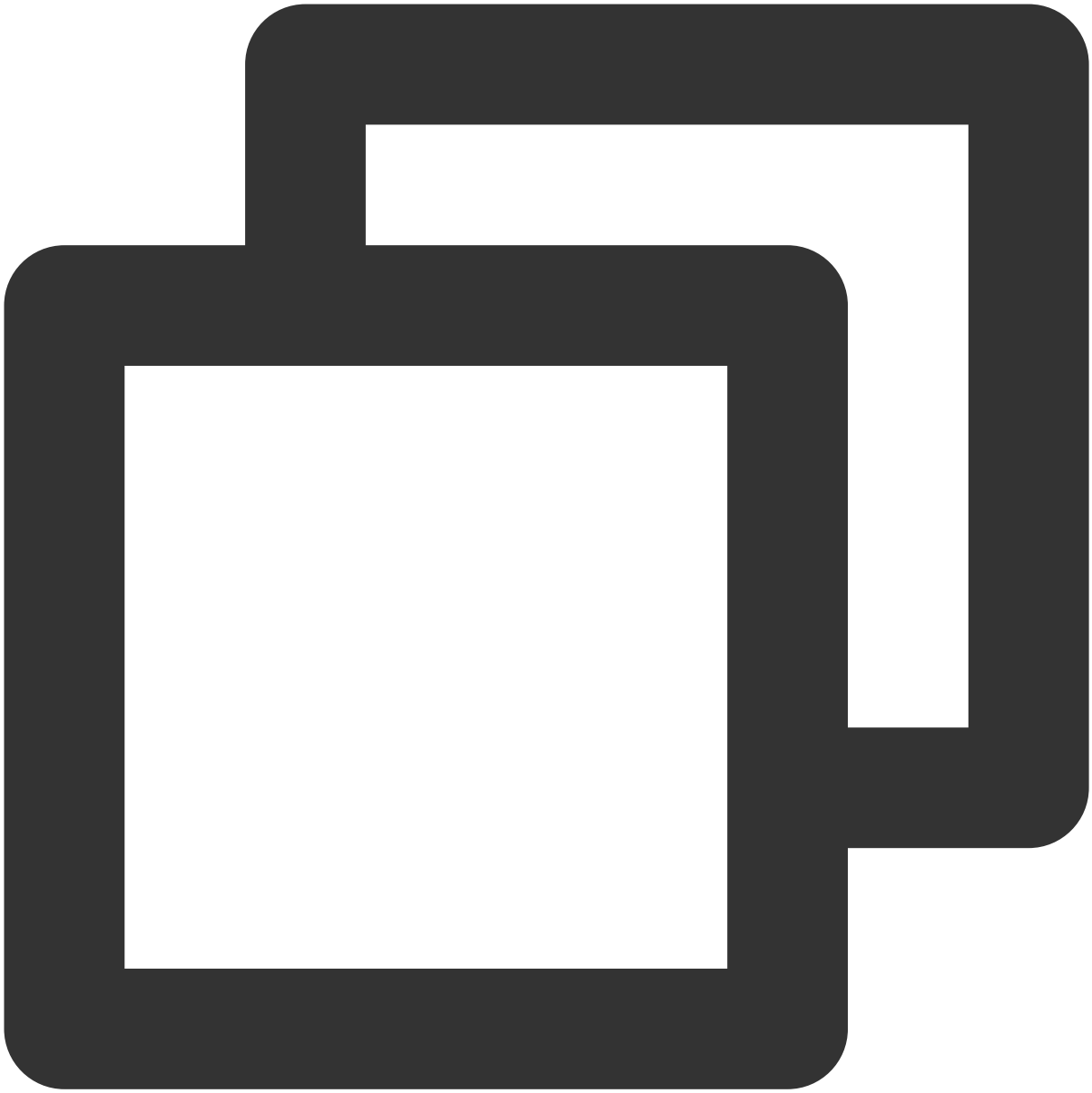
2. Run the following command to access the `/etc/network/` folder.



```
cd /etc/network/
```

3. Modify the configuration file “interfaces”.

3.1 Run the following command to switch to the "root" account and modify the configuration file.

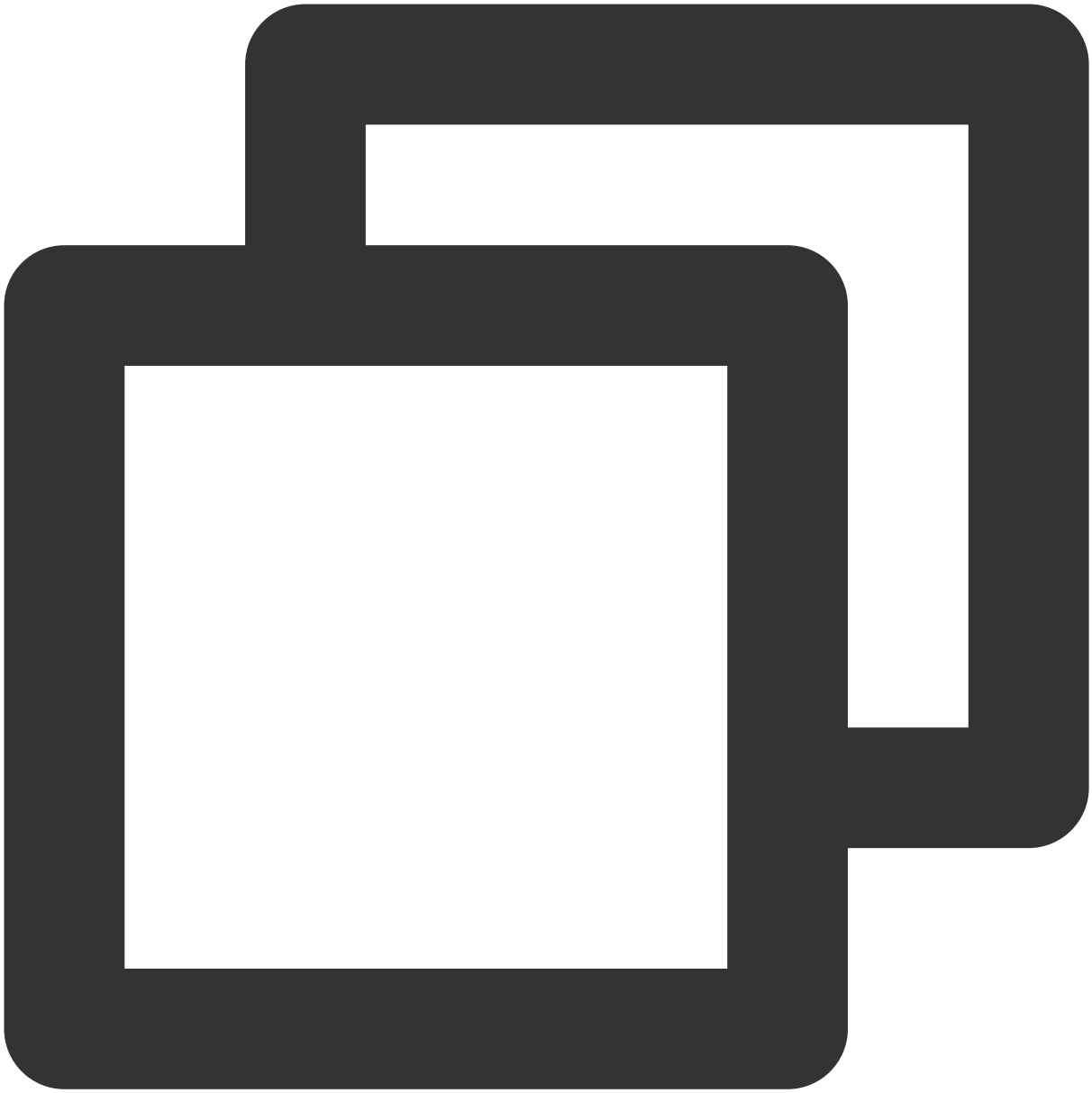


```
sudo su
vim interfaces
```

3.2 Press **i** to switch to the edit mode and add the following content to the configuration file.

Note:

For the methods to view the IP address and subnet mask of the ENI, see the Appendix.

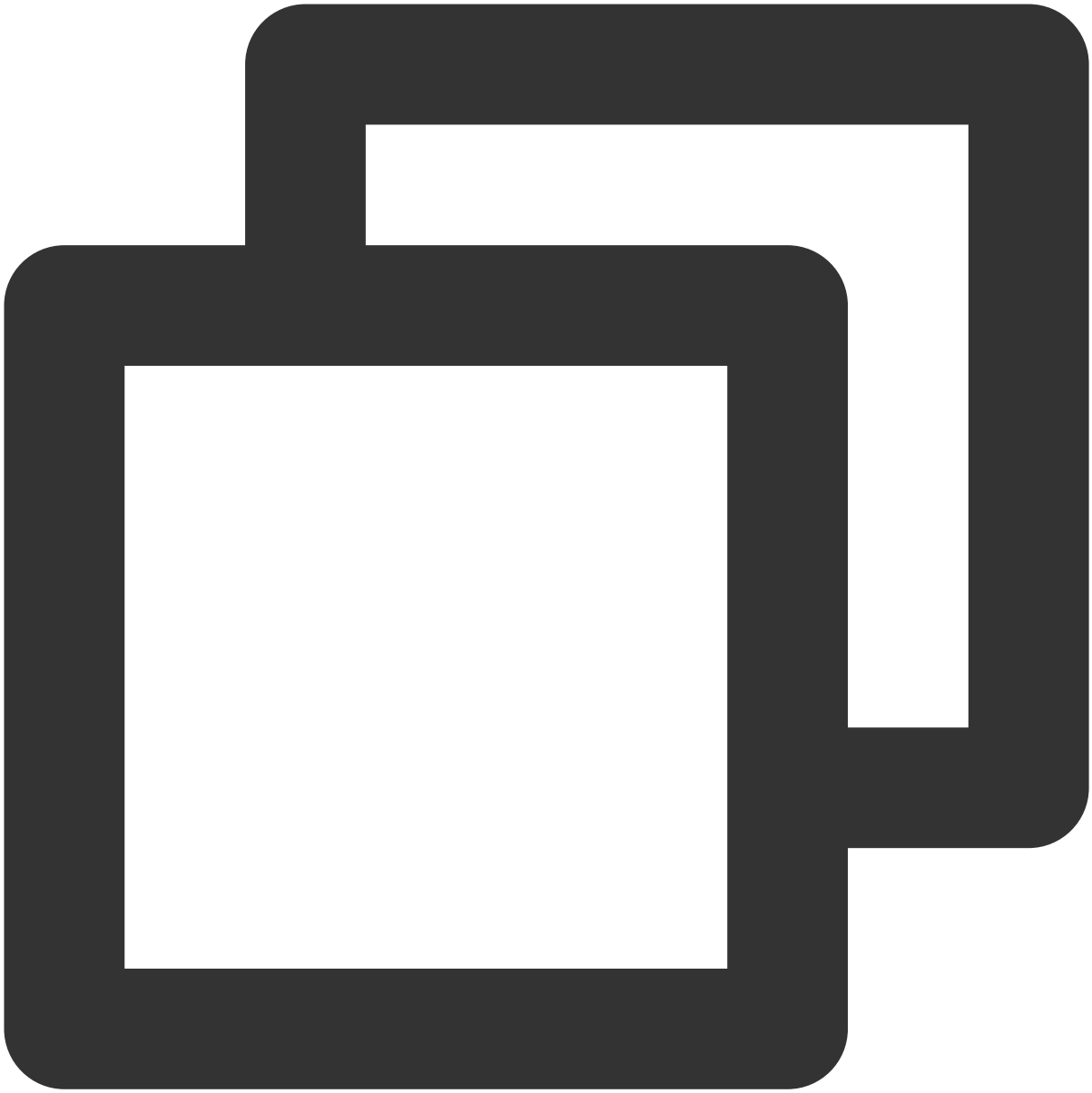


```
auto eth1 # Enter the actual ENI name obtained in step 1.
iface eth1 inet static # Enter the actual ENI name obtained in step 1.
address 172.21.48.3 # Enter the actual IP address of the ENI.
netmask 255.255.240.0 # Enter the actual subnet mask.
```

3.3 Press **Esc** when you come to the last line of vim, enter **wq!**, and then press **Enter** to save and close the configuration file.

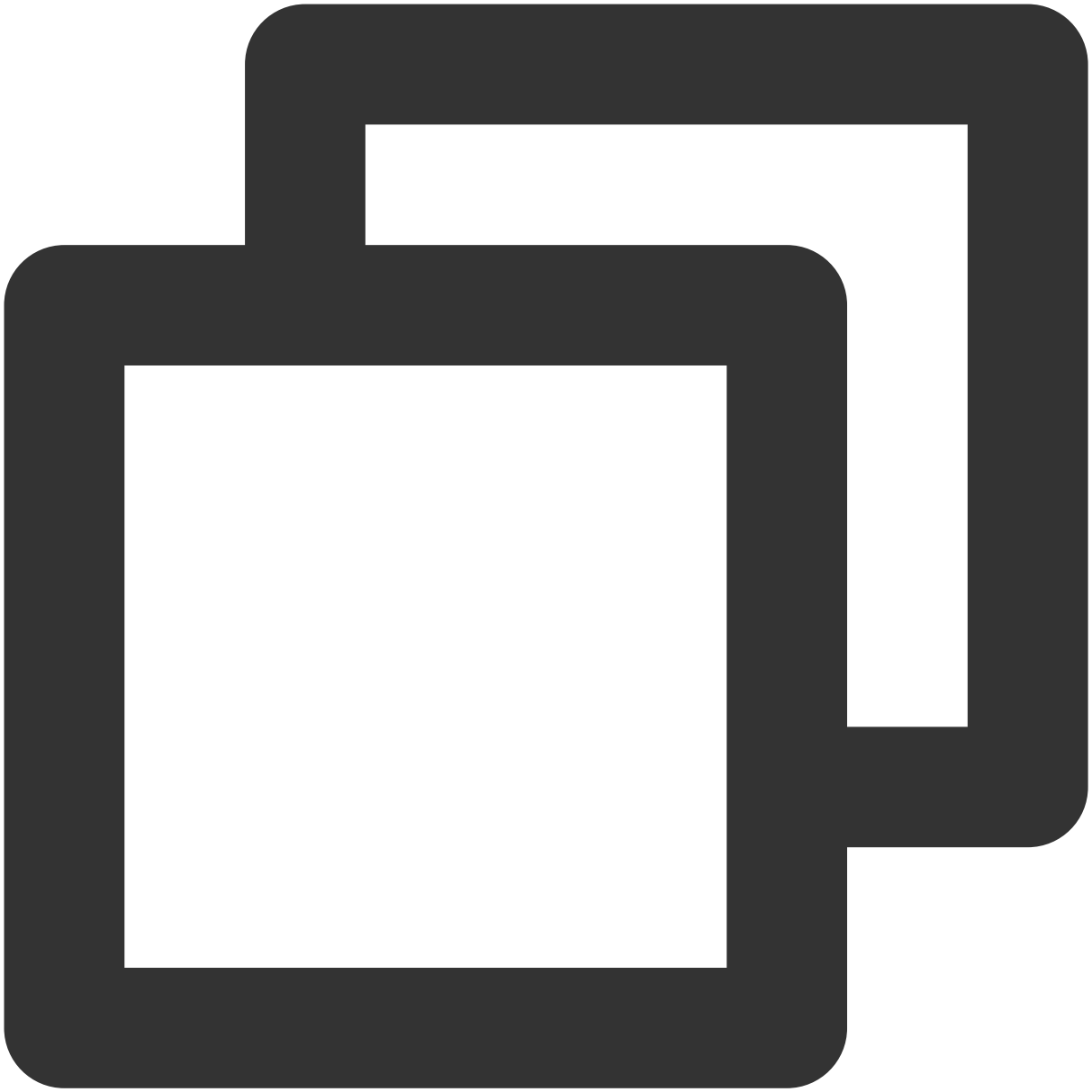
4. Restart the ENI eth1.

4.1 Run the following commands to switch to the “root” account and install ifupdown.



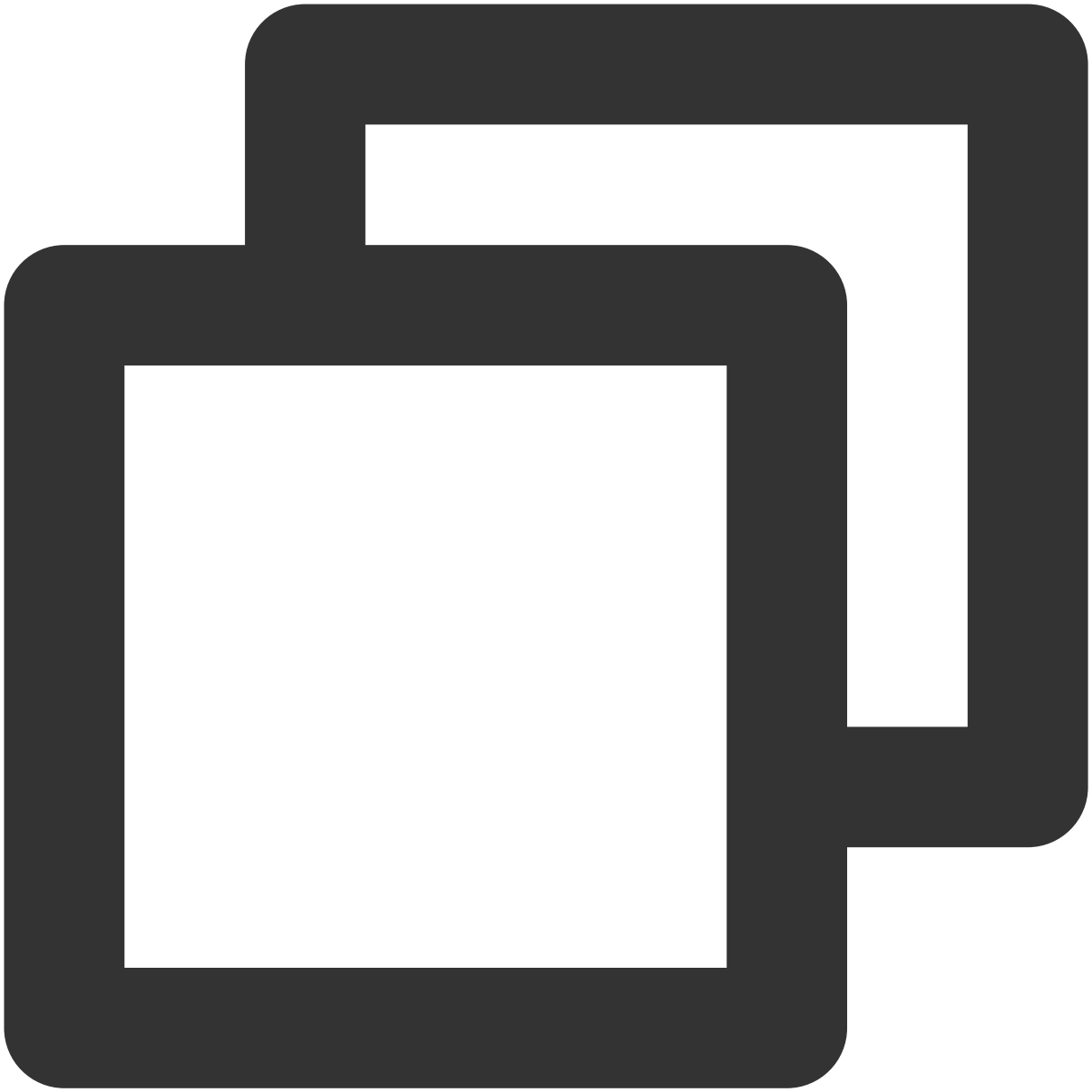
```
sudo su
apt install ifupdown
```

4.2 Turn off the ENI eth1.



```
ifdown eth1
```

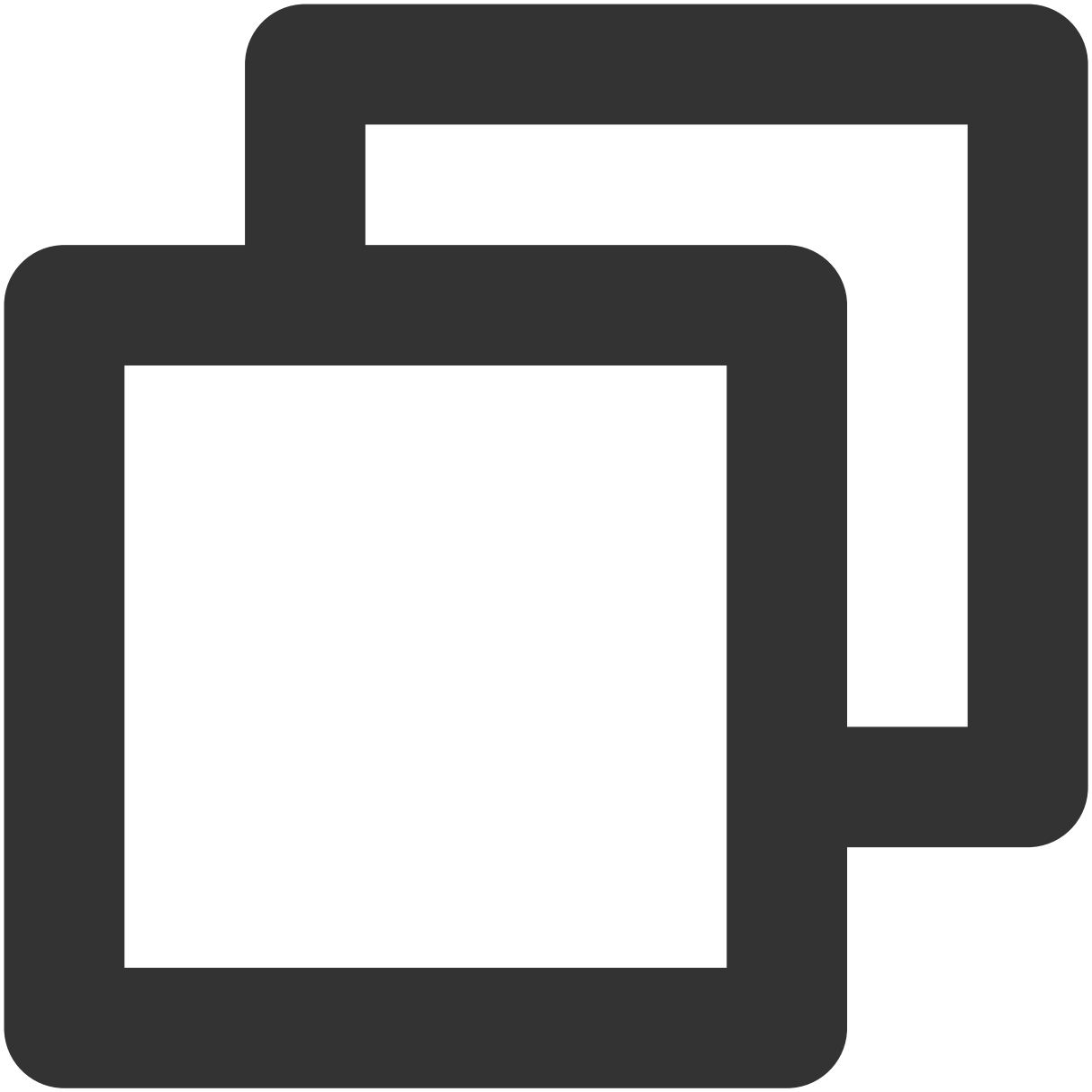
4.3 Start the ENI eth1.



```
ifup eth1
```

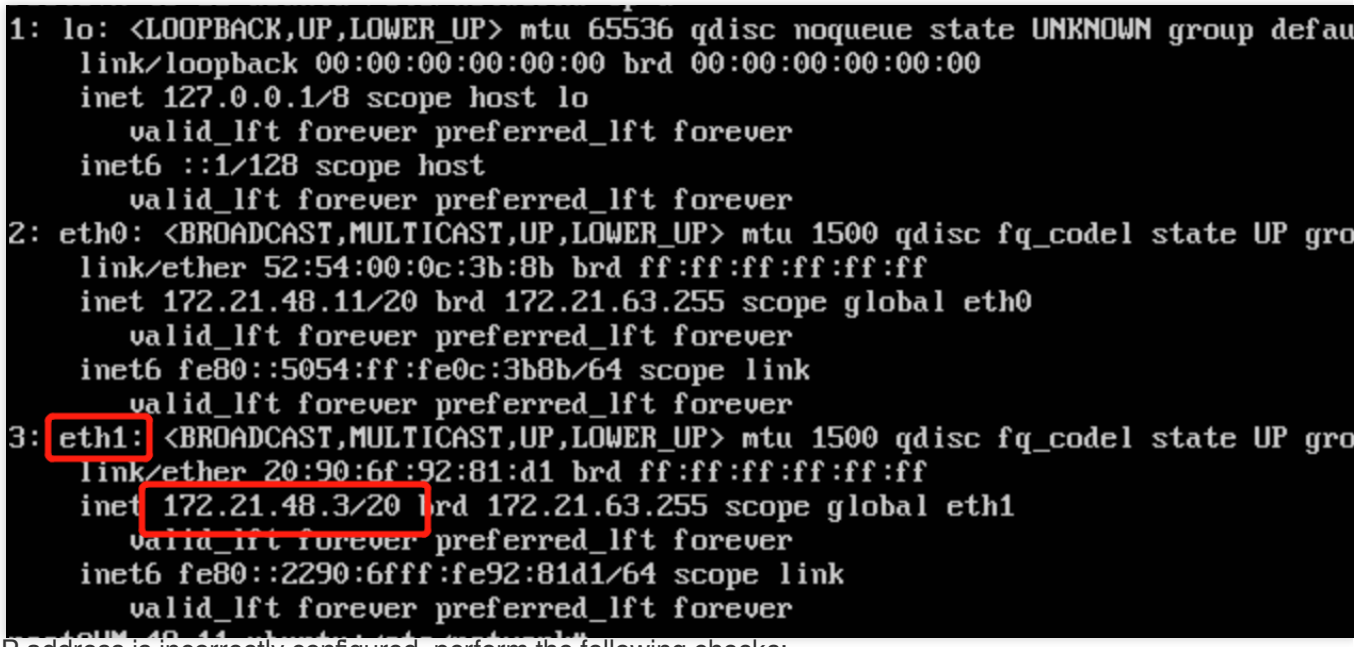
5. Check and verify the IP configuration.

5.1 Run the following command to check the IP address.



```
ip addr
```

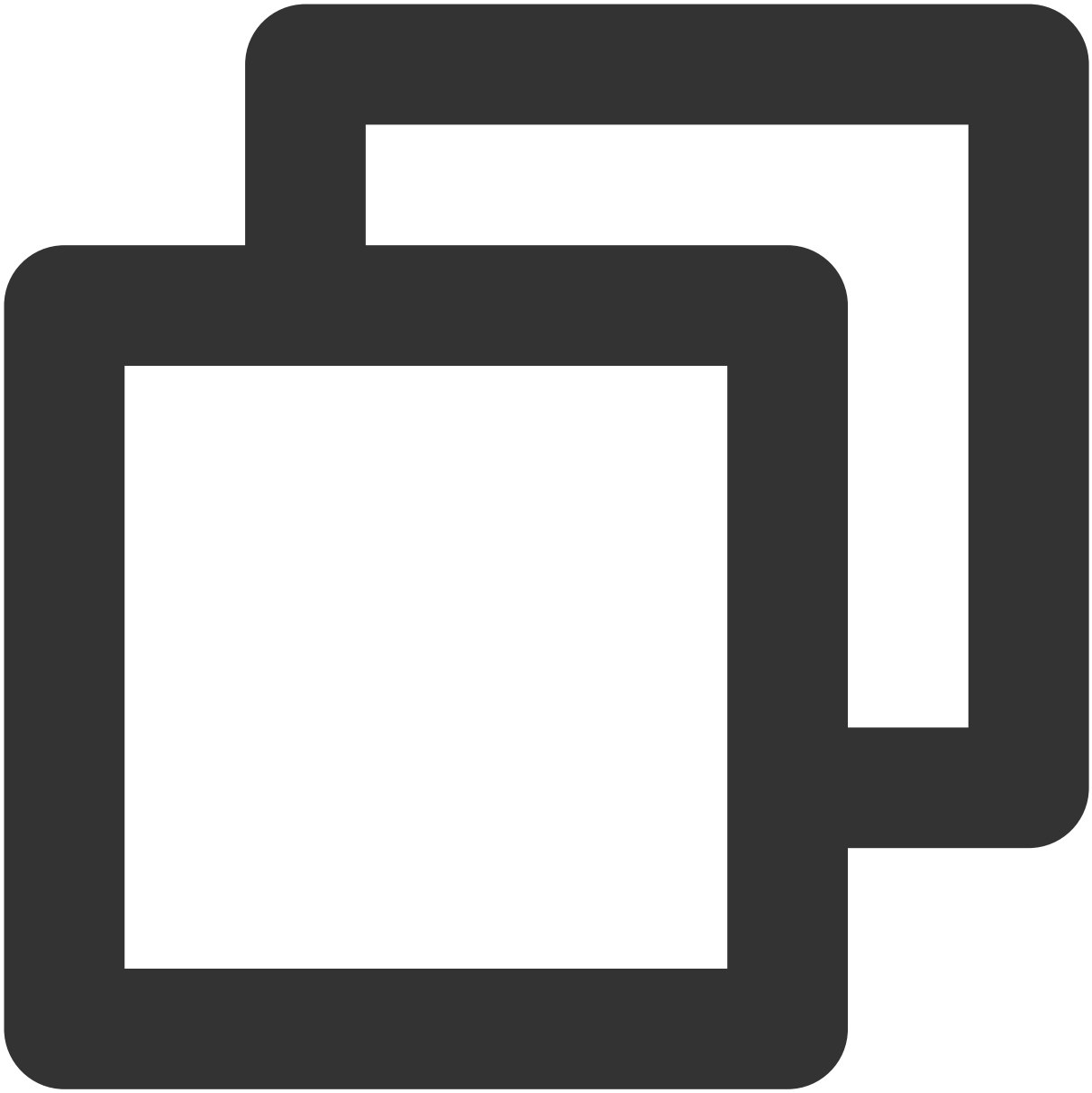
5.2 Confirm that the secondary ENI and its IP are visible, as shown below:



If the IP address is incorrectly configured, perform the following checks:

5.3 Verify the configuration file. Reconfigure the file if needed.

5.4 Confirm whether the ENI has restarted. You can run the following commands to restart ENI for the configuration to take effect.



```
ifdown eth1
ifup eth1
```

6. Configure the routing policy based on actual needs.

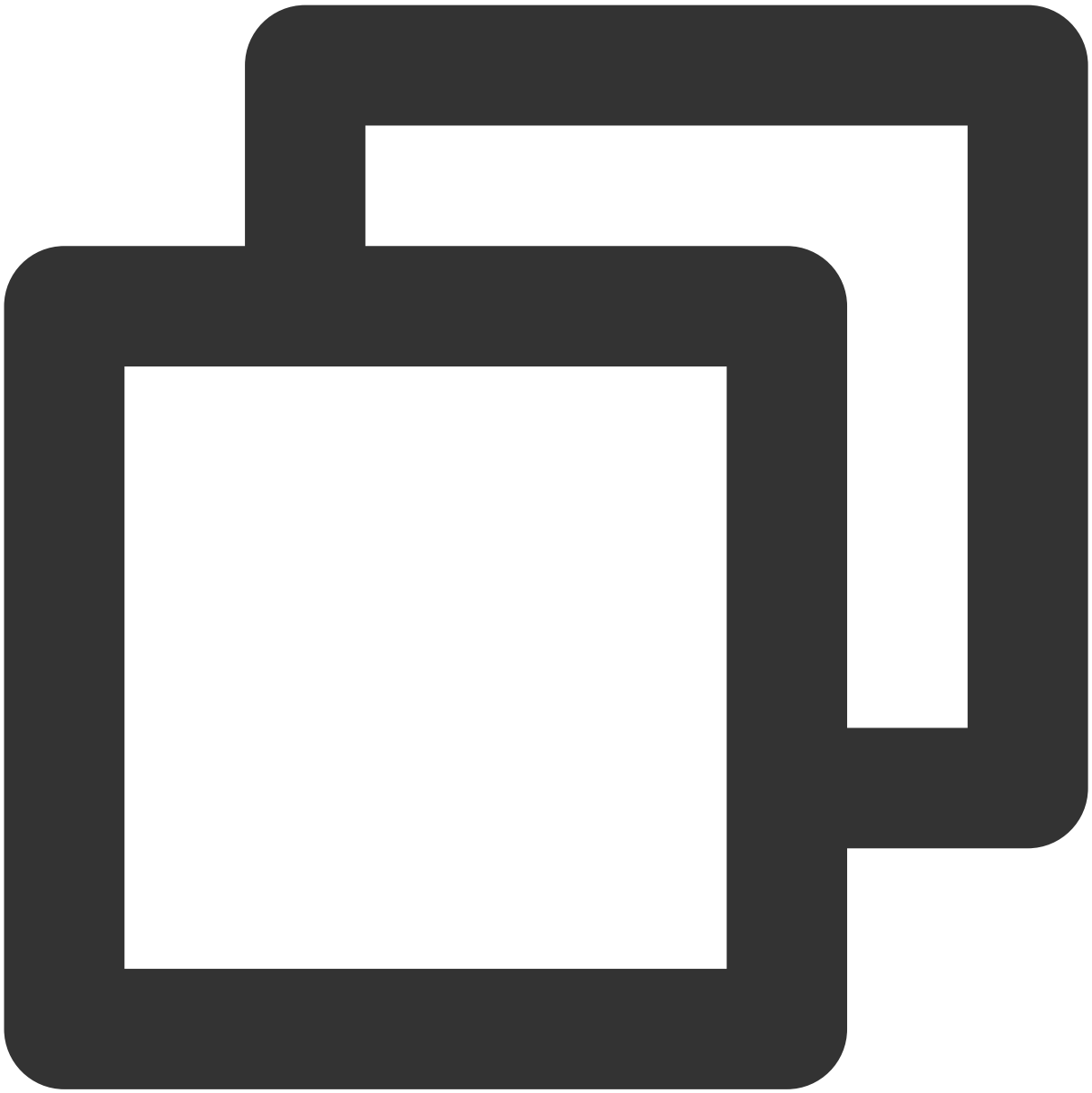
Note:

After the preceding configuration, the Linux image still sends packets from the primary ENI by default. In this case, you can configure policy-based routing to specify the ENI through which packets are sent and returned. A temporary static route is configured accordingly. You need to reconfigure a route after restarting the network.

6.1 Run the following c

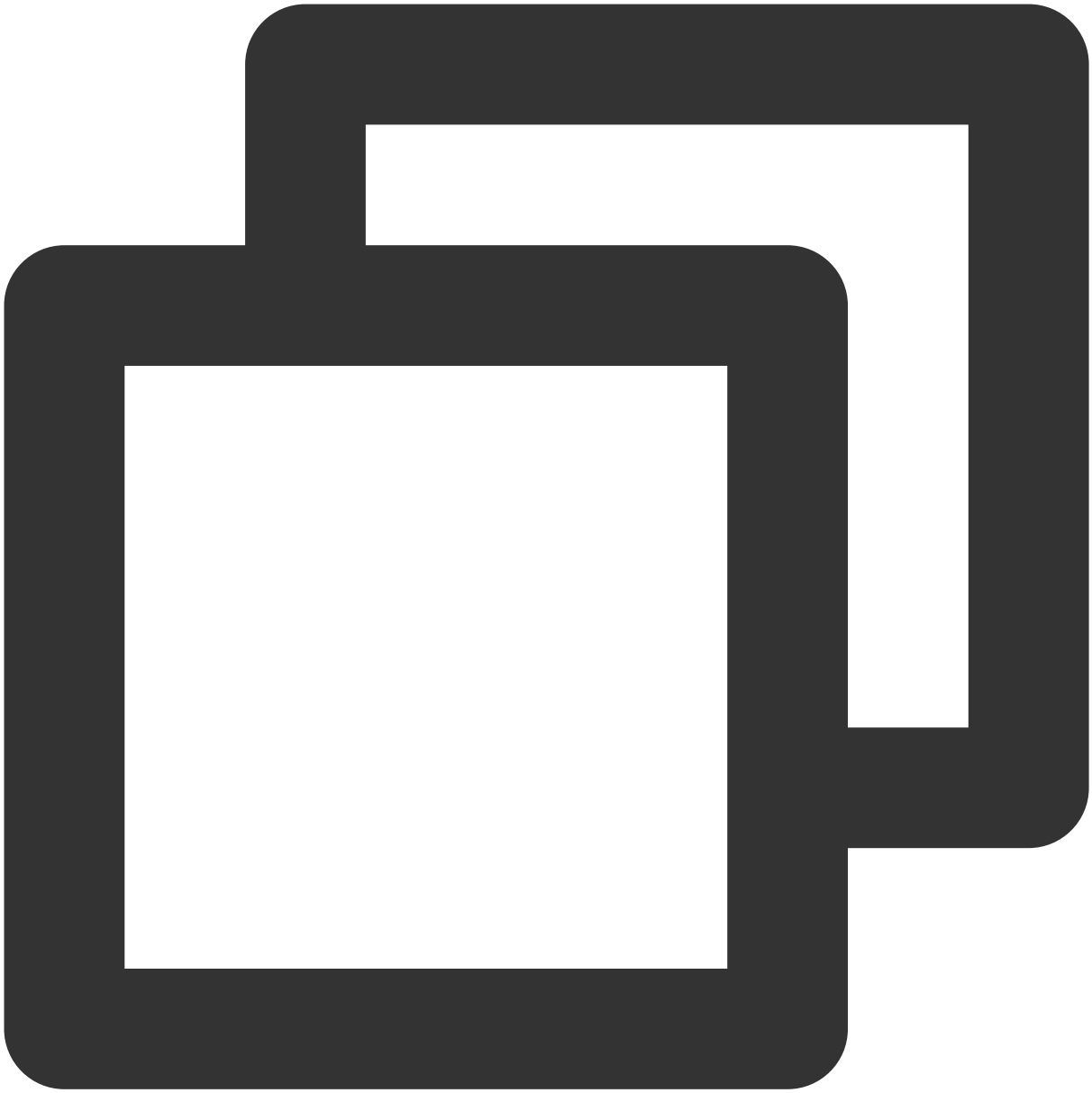
ommands to c

reate two route tables.



```
echo "10 t1" >> /etc/iproute2/rt_tables   #Replace “10” with the actual route ID an
echo "20 t2" >> /etc/iproute2/rt_tables  #Replace “20” with the actual route ID and
```

6.2 Run the following commands to add default routes for both route tables.

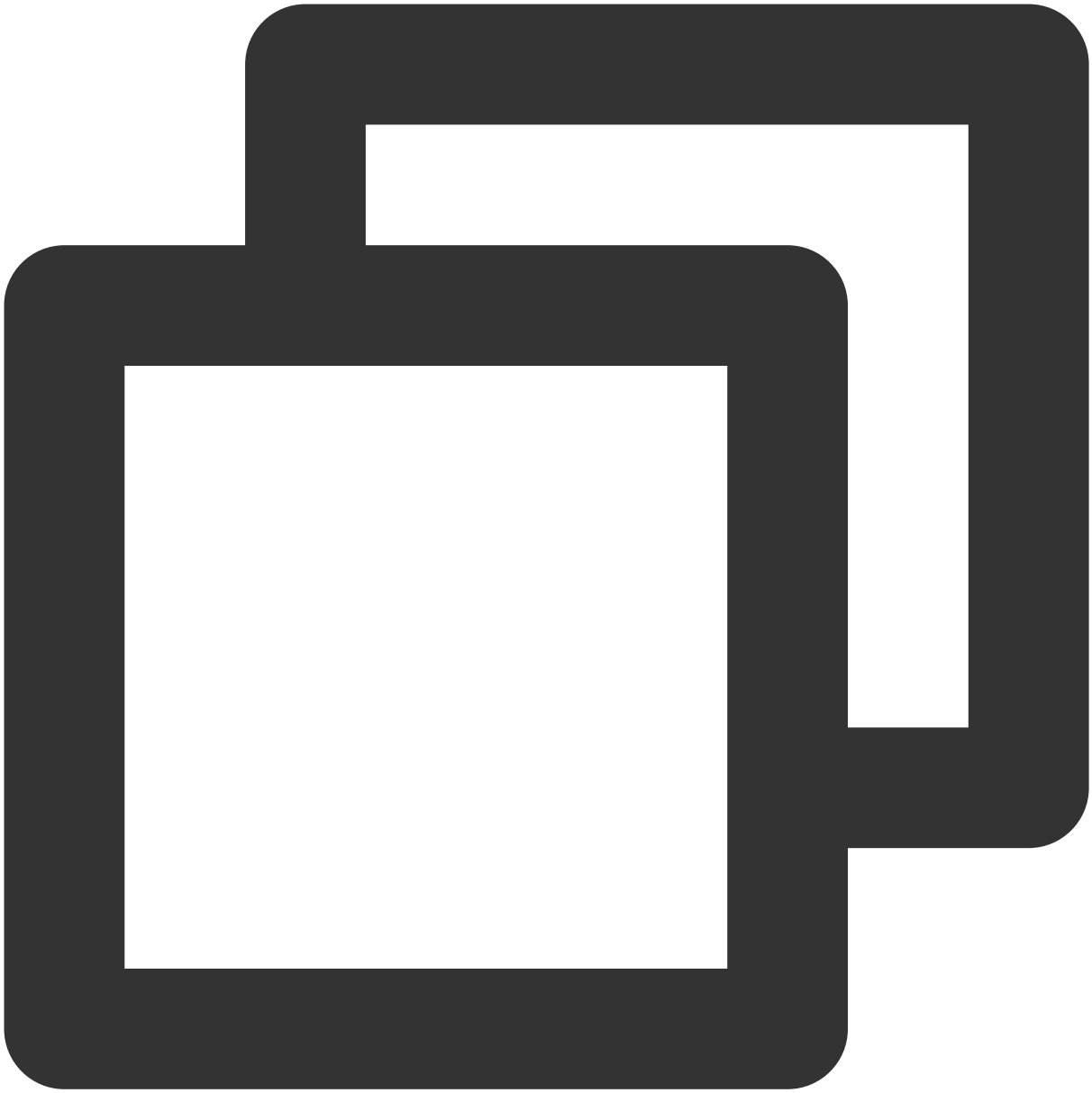


```
ip route add default dev eth0 via 172.21.48.1 table 10   #Replace “172.21.48.1” wit
ip route add default dev eth1 via 172.21.48.1 table 20   #Replace “172.21.48.1” wit
```

Note:

For gateway details, see Viewing the gateway.

6.3 Run the following commands to configure policy-based routing.



```
ip rule add from 172.21.48.11 table 10   #Enter the actual IP address of the primar
ip rule add from 172.21.48.3 table 20    #Enter the actual IP address of the second
```

7. After completing the configuration, you can ping the private IP of a CVM that is in the same subnet. If the pinging succeeds, the configuration is correct. If no other CVM exists, you can bind the private IP of the secondary ENI to a public IP and then ping the public IP.

Appendix

Viewing the IP address of an ENI

1. Log in to the VPC console.
2. Choose **IP and ENI** > **ENI** in the left sidebar to go to the ENI list page.
3. Click the ID of the target ENI to go to its details page.
4. Select the **IPv4 address management** tab to view the IP address of the ENI, which is the private IP.

Viewing the subnet mask of an ENI

1. Log in to the VPC console.
2. Choose **IP and ENI** > **ENI** in the left sidebar to go to the ENI list page.
3. Click the ID of the target ENI to go to its details page, where you can view the subnet mask of the ENI.

As shown in the following figure, the CIDR bits of the subnet are /20, which means that the subnet mask of the ENI is `255.255.240.0` .

The relationship between the CIDR bits and the subnet mask is described in the following table:

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 the gateway

If you haven't made any changes, the gateway is the first IP address in the subnet IP range. For example, if the subnet IP range is `192.168.0.0/24`, the gateway is `192.168.0.1`.

If you are not sure about the subnet IP range of the ENI, please follow the steps below:

1. Log in to the VPC console.
2. Choose **IP and ENI** > **ENI** in the left sidebar to go to the ENI list page.
3. Click the ID of the target ENI to go to its details page, where you can view the subnet where the ENI resides. As shown in the figure below, the first IP address in the subnet IP range is `10.200.16.17`.

Configuring an ENI on a Windows CVM

Last updated：2024-01-11 16:04:31

Note:

The following operations use Windows 2012 as an example.

Directions

Windows provided with DHCP

If the CVM is provided with DHCP, you can view its secondary ENI and IP by following steps below without any further configuration:

1. Log in to the CVM, and select **Control Panel** -> **Network and Internet** -> **Network and Sharing Center** to check the secondary ENI that has been automatically obtained.
2. Click the “Ethernet 2” secondary ENI to view its information.
3. In the **Ethernet 2 Status** pop-up window, click **Properties**.
4. In the **Ethernet 2 Properties** pop-up window, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
5. In the **Internet Protocol Version 4 (TCP/IPv4)** pop-up window, you can see **Obtain an IP address automatically** is selected, so there is no need to enter one.
6. Return to the **Ethernet 2 Status** pop-up window and click **Details**. As shown in the figure below, DHCP is enabled and the IP automatically obtained is displayed.

DHCP not set

If the CVM is not provided with DHCP, you need to configure the private IP by following the steps below:

1. Log in to the ENI console and bind the ENI to a CVM.
2. Log in to the CVM and select **Control Panel** -> **Network and Internet** -> **Network and Sharing Center**.
3. Click to edit the “Ethernet 2” secondary ENI.
4. In the **Ethernet 2 Status** pop-up window, click **Properties**.
5. In the **Ethernet 2 Properties** pop-up window, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
6. In the **Internet Protocol Version 4 (TCP/IPv4)** pop-up window, enter the actual IP and click **OK**.
7. In the **Ethernet 2 Properties** pop-up window, click **OK** to complete the configuration.
8. In the **Ethernet 2 Status** pop-up window, click **Details**. As shown in the figure below, DHCP is disabled and the IP manually entered is displayed.
9. Ping the private address of a CVM that is in the same subnet. If the pinging succeeds, the configuration is correct. If no other CVM exists, you can bind the private IP address of the secondary ENI to a public IP address and then ping the public IP address.

Setting Service Level

Last updated：2024-01-11 16:04:31

You can specify different service level for different ENIs. When bandwidth congestion occurs, this can ensure that the key services with high priority be forwarded first.
There are four service levels, Gold, Silver, Bronze and Default, ranking by priority for traffic forwarding. You can keep it as Default for general usage.
Note:
The service level defaults to "Default".
ENI is a private network resource. The service level is only applied to underlying traffic service and is irrelevant to the billing.

Directions

1. Log in to the VPC console.
2. Choose **IP and ENI** > **ENI** in the left sidebar to go to the ENI list page.
3. Locate the target ENI. Click **More** > **Set service level** in the **Operation** column.
4. Choose a service level from the drop-down list. Click **OK**.
5. To set the same service level for multiple ENIs, you can select multiple ENIs and click **Set service level** at the top.
6. Click **OK**.

Deleting an ENI

Last updated：2024-01-11 16:04:31

You can delete an ENI that is not bound to a CVM.

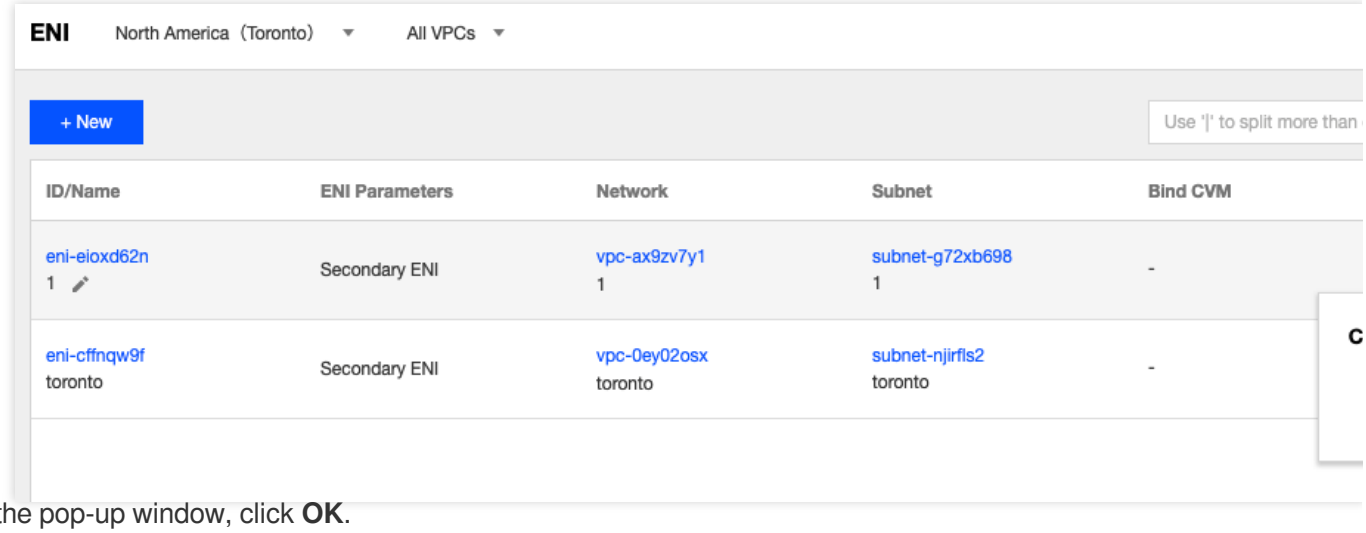
Note:

When an ENI is deleted, its associated private IPs, EIPs, and security groups are automatically unbound.

You can only delete ENIs that are not associated with CVMs.

The primary ENI is deleted when the CVM is deleted.

1. Log in to the VPC console.
2. Choose **IP and ENI** > **ENI** in the left sidebar to go to the ENI list page.
3. Locate the row of the desired ENI and click **Delete** in the "Operation" column.



4. In the pop-up window, click **OK**.

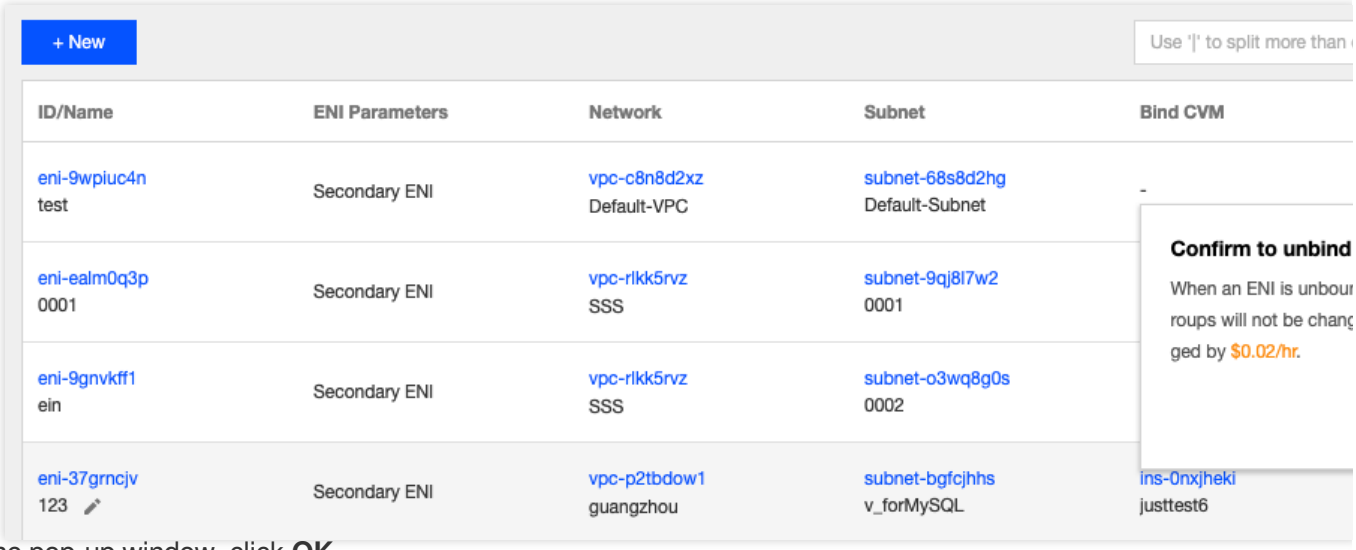
Unbinding from a CVM

Last updated：2024-01-11 16:04:31

1. Log in to the VPC console.
2. Choose **IP and ENI** > **ENI** in the left sidebar to go to the ENI list page.
3. Locate the target ENI, and click **More** > **Unbind from the CVM** in the **Operation** column.

Note:

You can also click the ENI ID to go to the details page, and click **Unbind from the CVM**.



4. In the pop-up window, click **OK**.

Note:

When an EIP is unbound, an idle is incurred. Release unused EIPs to avoid unnecessary costs.

Binding Secondary Private IP Addresses

Last updated：2024-01-11 16:04:31

To bind multiple IP addresses to a single ENI, you can apply for secondary private IP addresses for the ENI as follows:

Step 1. Assign a Private IP

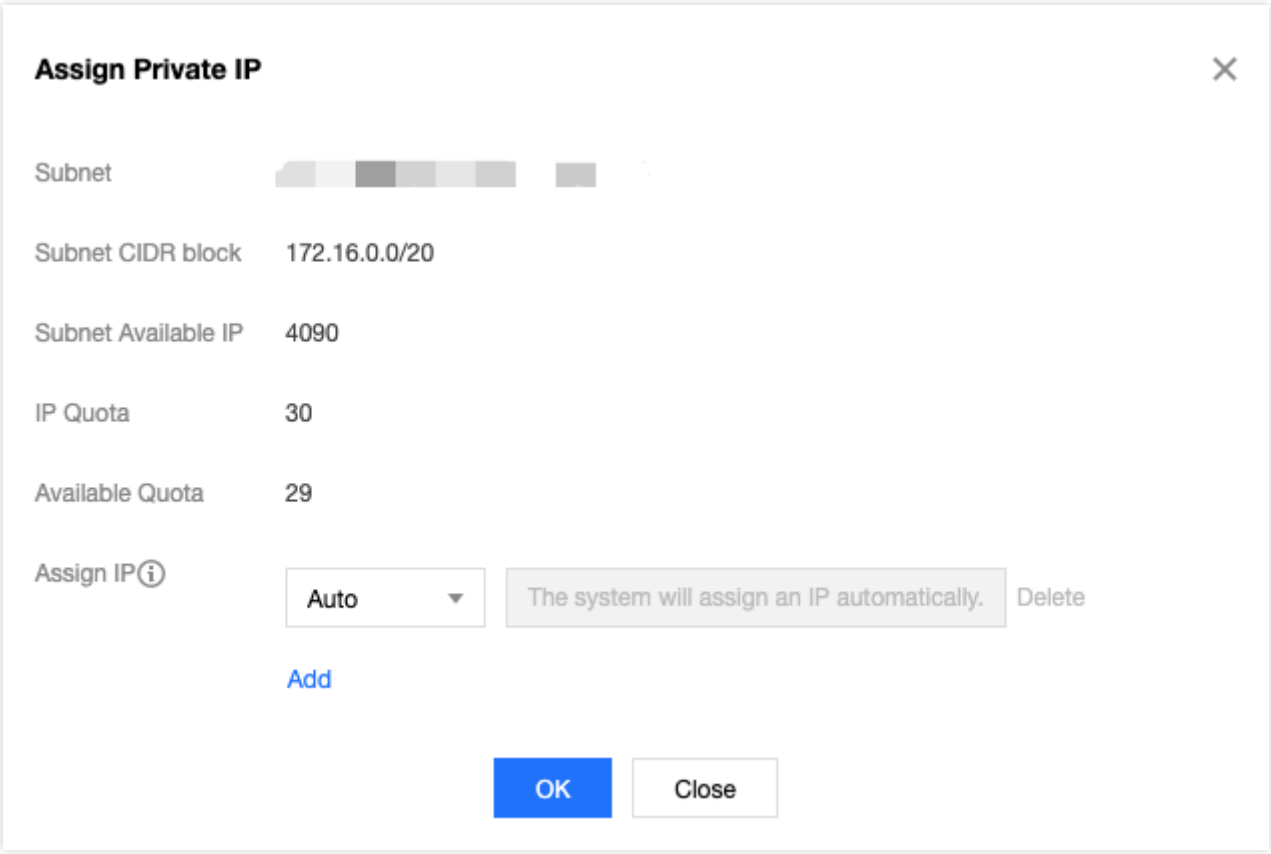
1. Log in to the VPC console.
2. Choose **IP and ENI** > **ENI** in the left sidebar to go to the ENI list page.
3. Locate the ENI instance for which you want to request a secondary private IP, and then click on its **ID/Name** to go to its details page.
4. Click the **IPv4 Address Management** tab, and check the primary private IPs that have been bound.

5. Click **Assign Private IP** and select **Auto** or **Enter manually** for **Assign IP** in the pop-up window.

Note:

If you select **Enter manually**, make sure that the private IP address you enter is within the subnet IP range and is not a reserved IP address of the system.

For example, if the subnet IP range is `10.0.0.0/24`, the entered private IP address should be within `10.0.0.2 - 10.0.0.254`.

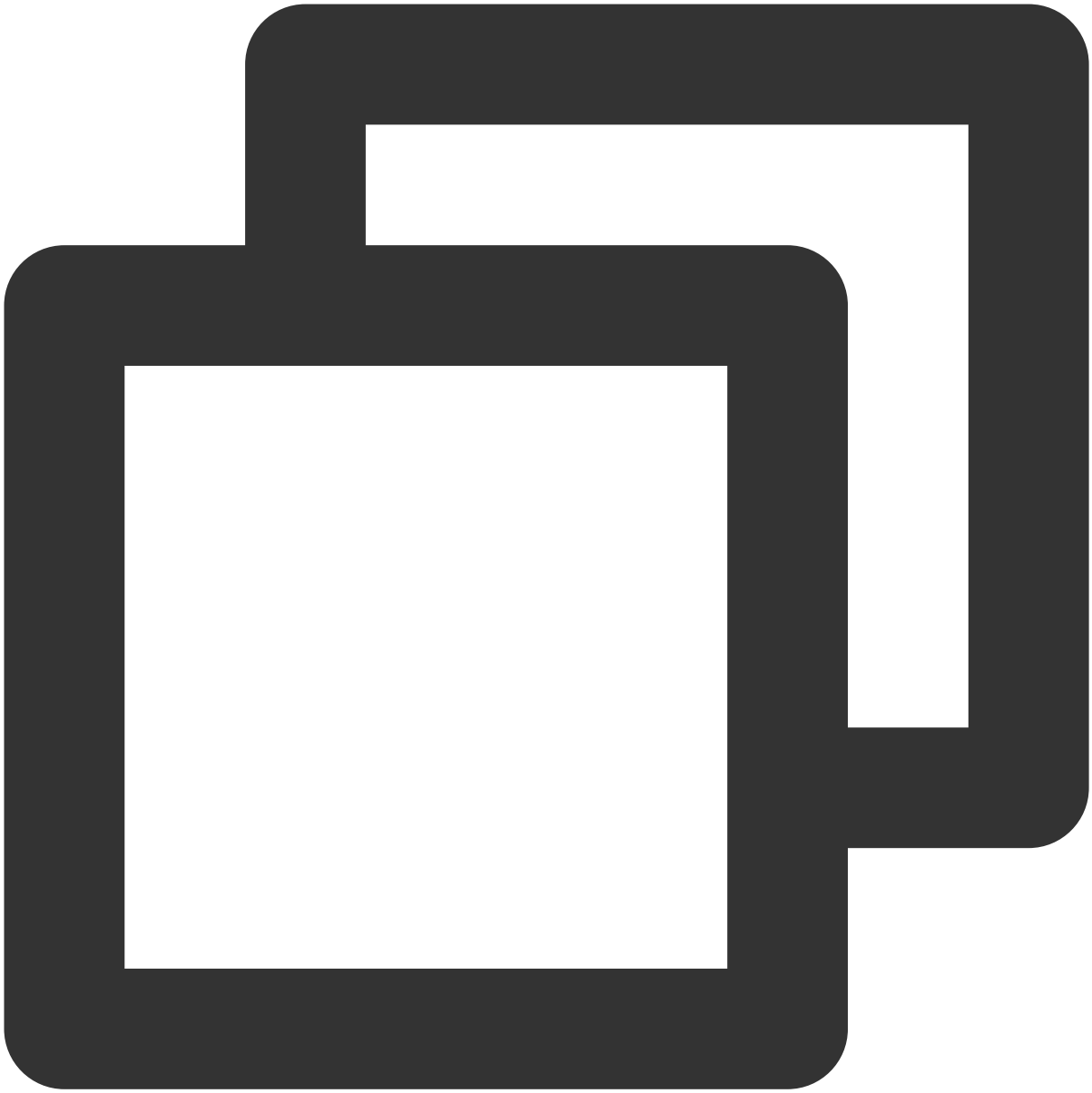


Step 2. Configure the Secondary Private IP

Follow the steps below to log in to the CVM that is bound with the ENI and configure the secondary private IP to make it effective:

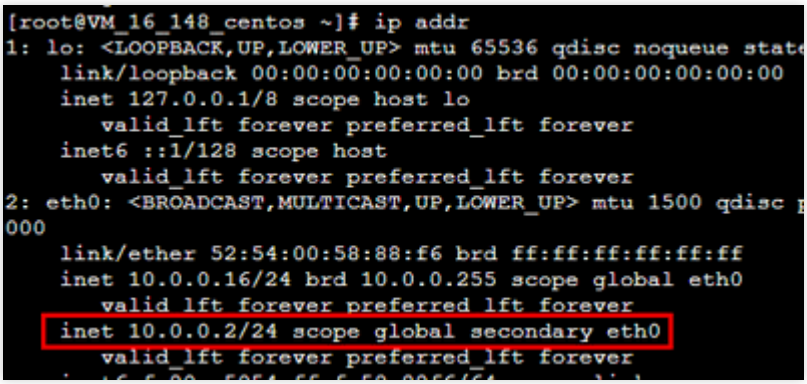
Linux CVM instances

1. Run the following command to configure the secondary private IP.



```
# For example, `ip addr add 10.0.0.2/24 dev eth0`
ip addr add Secondary private IP/CIDR bits dev eth0
```

2. Run the `ip addr` command to view the configured IPs, as shown below.



Windows CVM instances

1. Perform the f

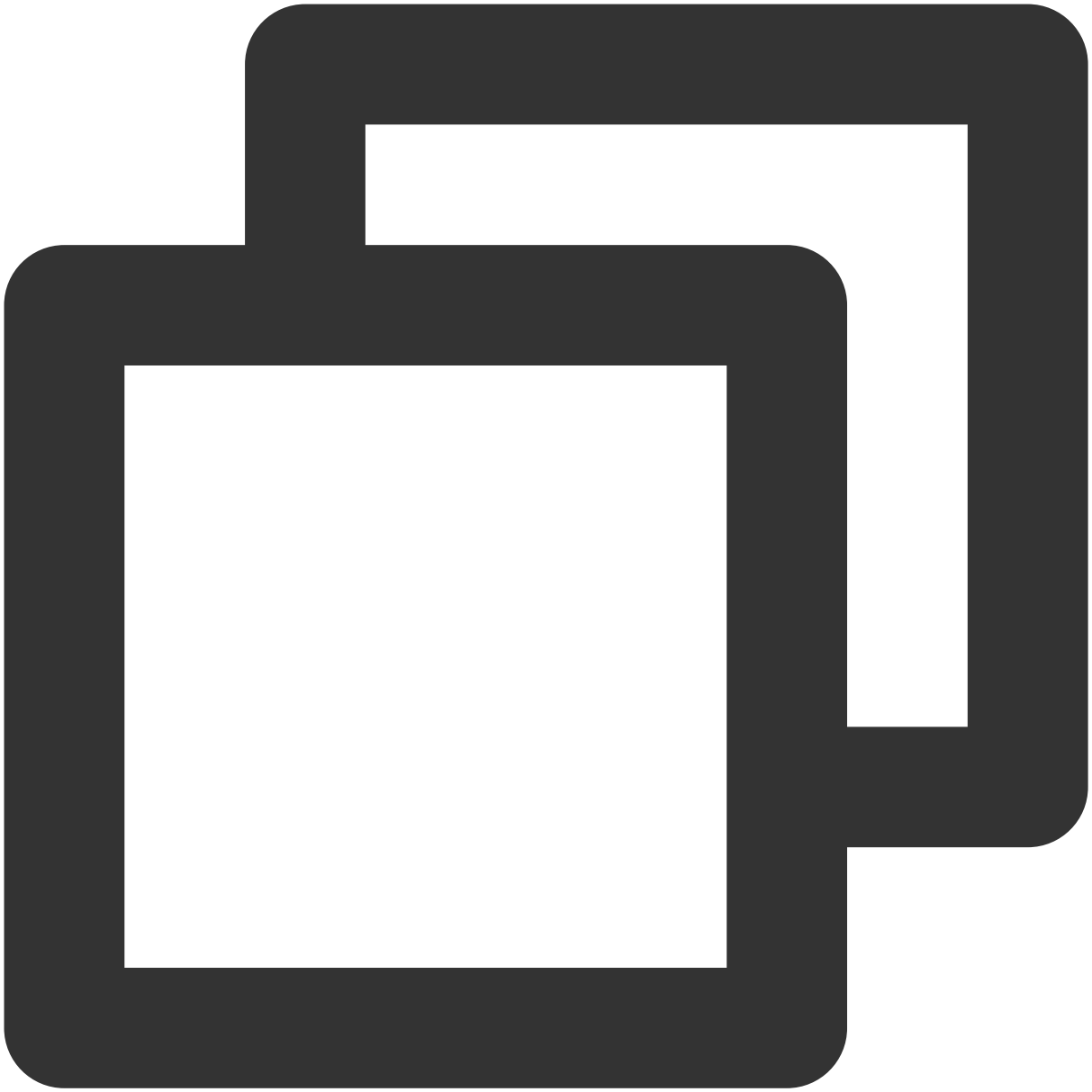
ollowing steps t

o view the IP address, subnet mask, default gateway, and DNS server of the CVM instance.

2. On the desktop, select


in the lower-left corner and click


to open the **Windows PowerShell** window.



```
ipconfig /all
```

3. Record the IPv4 address, subnet mask, default gateway, and DNS server values that are displayed.

4. Select **Control Panel** > **Network and Internet** > **Network and Sharing Center**. Click **Ethernet** to modify its information.

5. In the **Ethernet Status** pop-up window, click **Properties**.

6. In the **Ethernet Properties** pop-up window, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

7. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** pop-up window, specify the following information:

Parameter Name	Parameter Value
IP address	The IPv4 address obtained in step 1
Subnet mask	The subnet mask obtained in step 1
Default gateway	The default gateway obtained in step 1
Preferred DNS server	The DNS server obtained in step 1
Alternate DNS server	The alternate DNS server obtained in step 1. If the alternate DNS server is not given, ignore this parameter

8. Click **Advanced** to configure the secondary private IP address.
9. In the **Advanced TCP/IP Settings** pop-up window, click **Add** under the **IP Addresses** section.
10. In the **TCP/IP Address** pop-up window, enter the secondary private IP and the subnet mask obtained in step 1, and click **Add**.
11. In the **Internet Protocol Version 4 (TCP/IPv4)** pop-up window, click **OK**.
12. In the **Ethernet Properties** pop-up window, click **OK** to complete the configuration.
13. In the **Ethernet Status** pop-up window, click **Details** to view the configured IP addresses.

Releasing Secondary Private IP Addresses

Last updated：2024-01-11 16:04:31

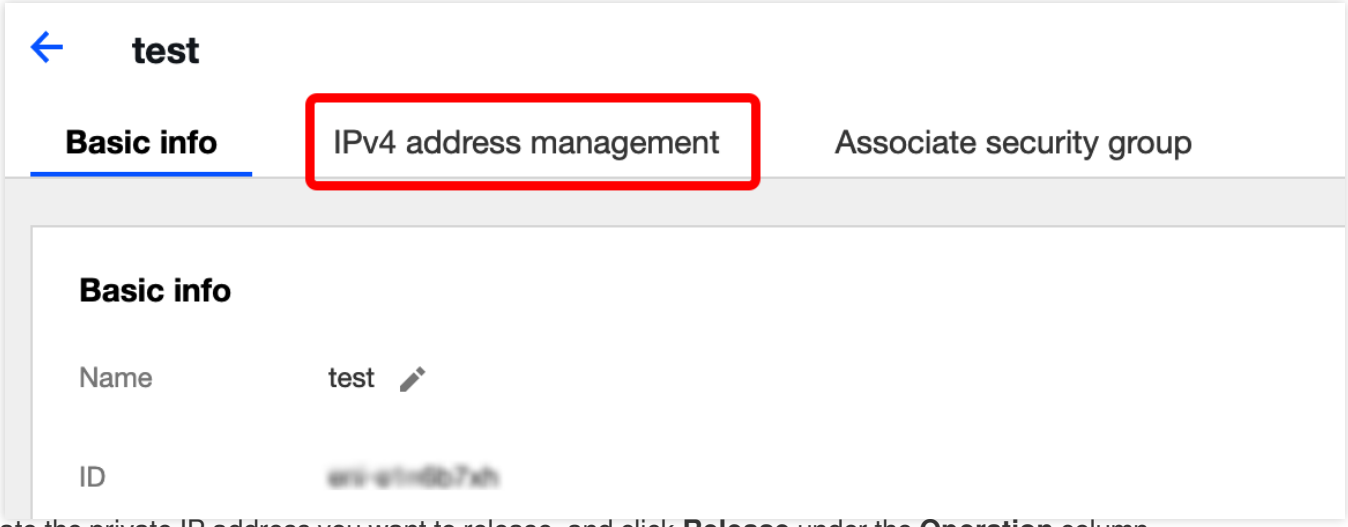
Note:

Only a secondary IP address can be released from an ENI. The primary IP address cannot be released.

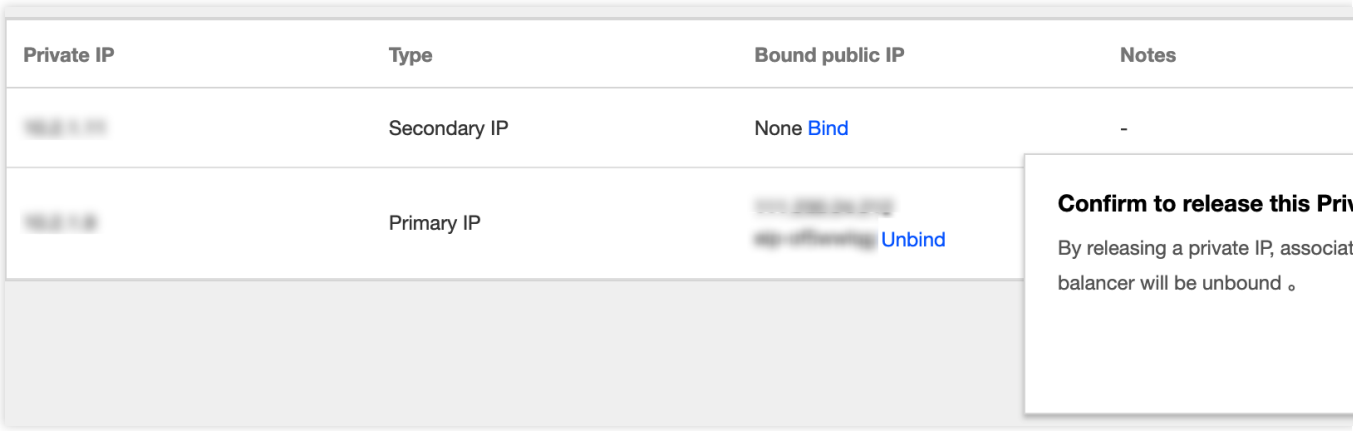
After a private IP address is unbound, the associated EIP will be unbound automatically.

Directions

1. Log in to the VPC Console.
2. Choose **IP and ENI** -> **ENI** in the left sidebar to go to the ENI list page.
3. Locate the ENI you want to release secondary private IPs, and click its ID/Name to go to the details page.
4. Click the **IPv4 address management** tab to view private IP addresses and EIPs that have been bound.



5. Locate the private IP address you want to release, and click **Release** under the **Operation** column.
6. Click **OK** in the pop-up window.

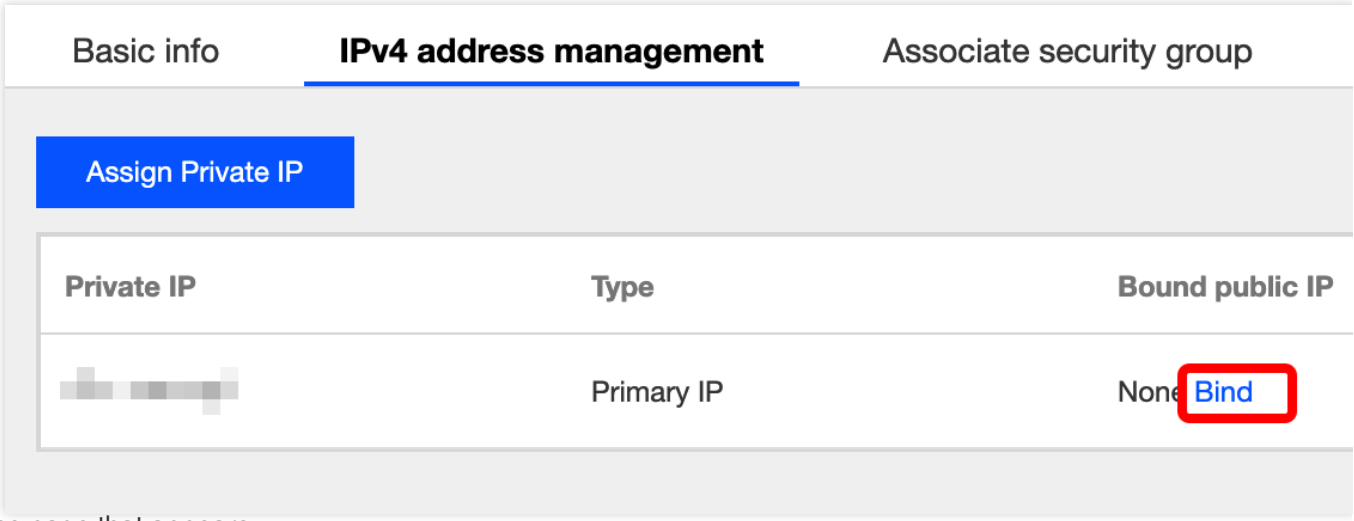


Binding EIPs

Last updated：2024-01-11 16:04:31

1. Log in to Virtual Private Cloud Console.
2. Choose **IP and ENI** > **ENI** in the left sidebar to go to the ENI list page.
3. Click the ID of the desired instance to enter its details page.
4. Click **IPv4 Address Management** in the tab to check existing private IPs.

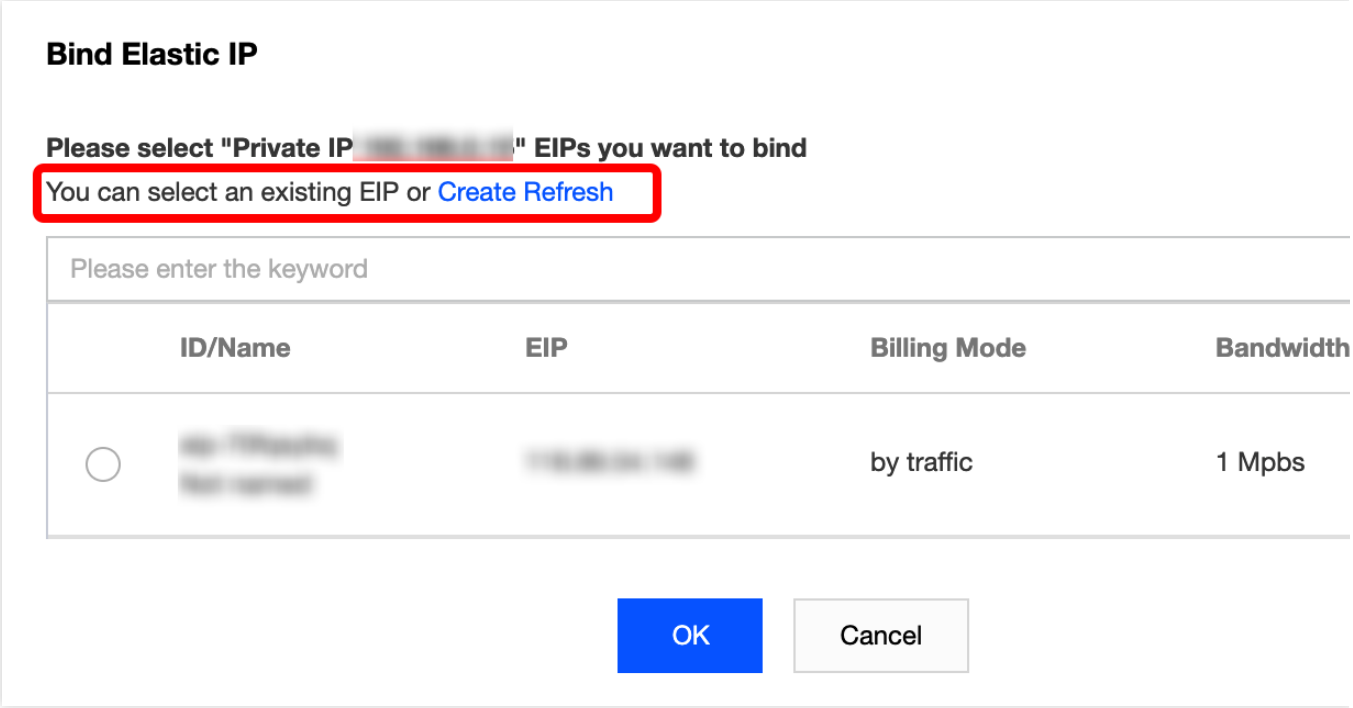
5. Click **Bind** in the **Bound Public IP** column.



6. In the page that appears:

Select the desired EIP and click **OK**.

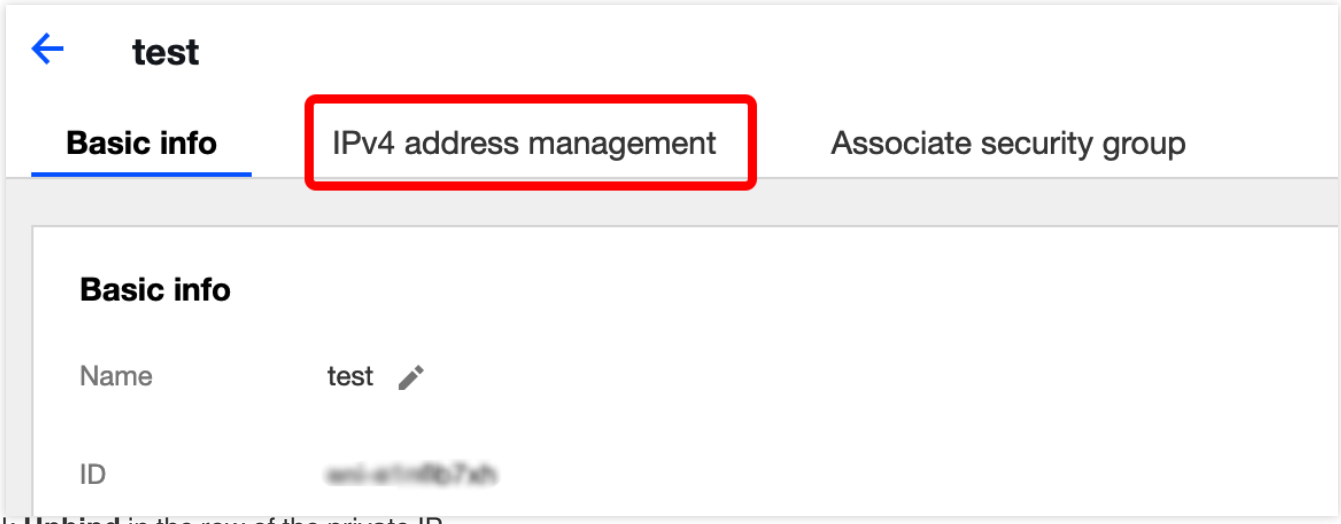
If no EIP is available, click **Create** at the top of the pop-up box to apply for one. For more information, refer to Applying for EIPs. After your application is approved, return to the page and click **Refresh**. You should see the EIP you applied for. Select it and click **OK**.



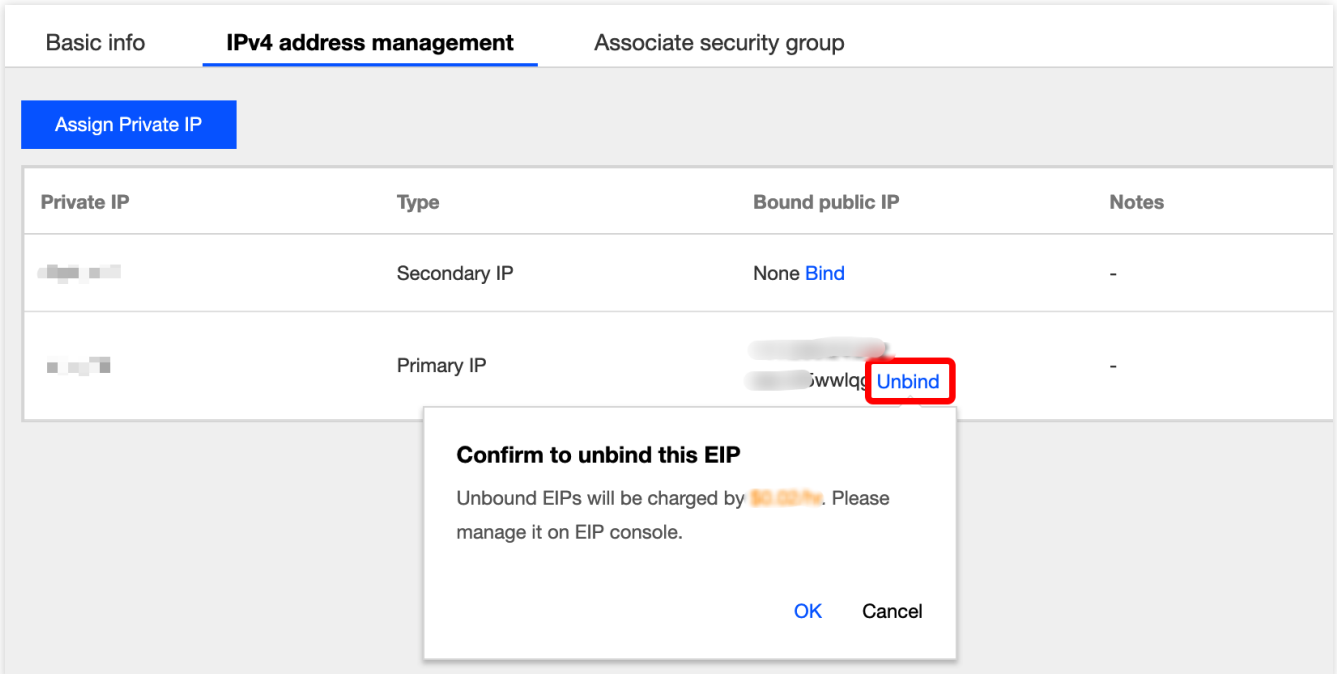
Unbinding EIPs

Last updated：2024-01-11 16:04:31

1. Log in to the VPC Console.
2. Click **ENI** in the left sidebar to enter the ENI list page.
3. Click the instance ID to enter the details page.
4. Click **IPv4 Address Management** in the tab to view private IPs and EIPs that have been bound.



5. Click **Unbind** in the row of the private IP.



6. Click **OK** in the pop-up window.

Modifying Primary Private IPs

Last updated：2024-01-11 16:04:31

This document describes how to modify the primary private IP of a CVM instance on the ENI console.

Note:

You can modify the primary private IP of the primary ENI, but not that of secondary ENIs.

Note that modifying the primary IP of the primary ENI will automatically restart the associated instance and cause business interruption for about 30 seconds.

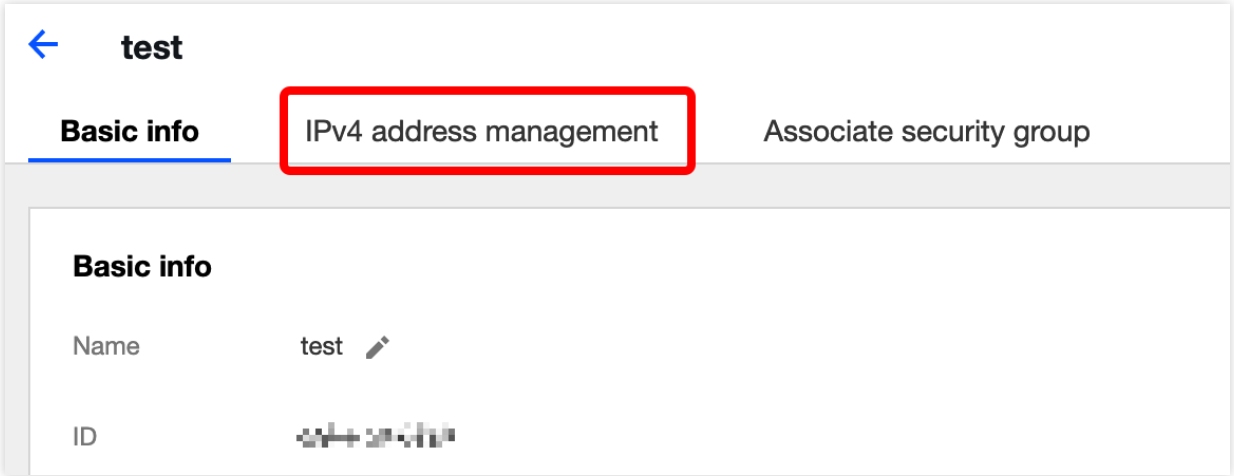
The private IP can also be modified on the CVM console as instructed in Modifying Private IP Addresses.

Prerequisites

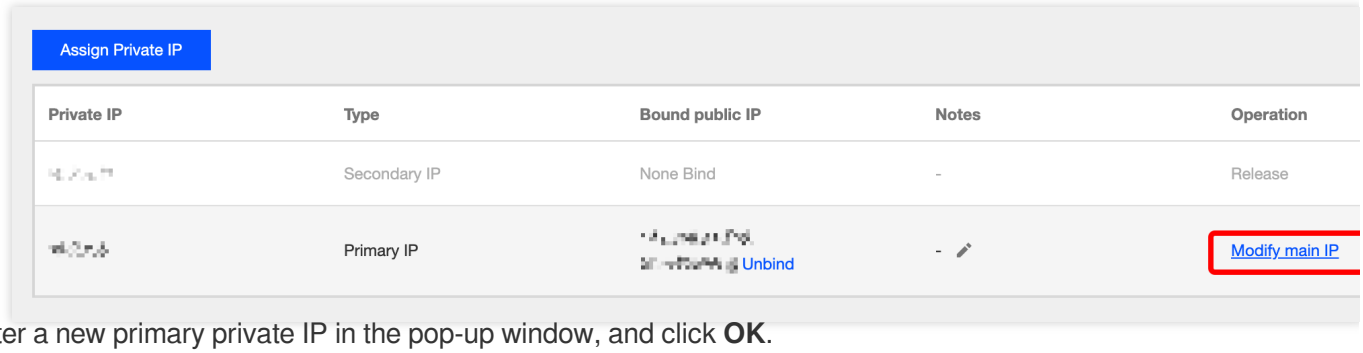
The primary ENI ID of the CVM instance has been obtained on the CVM console. For more information, see Query Instance Info.

Directions

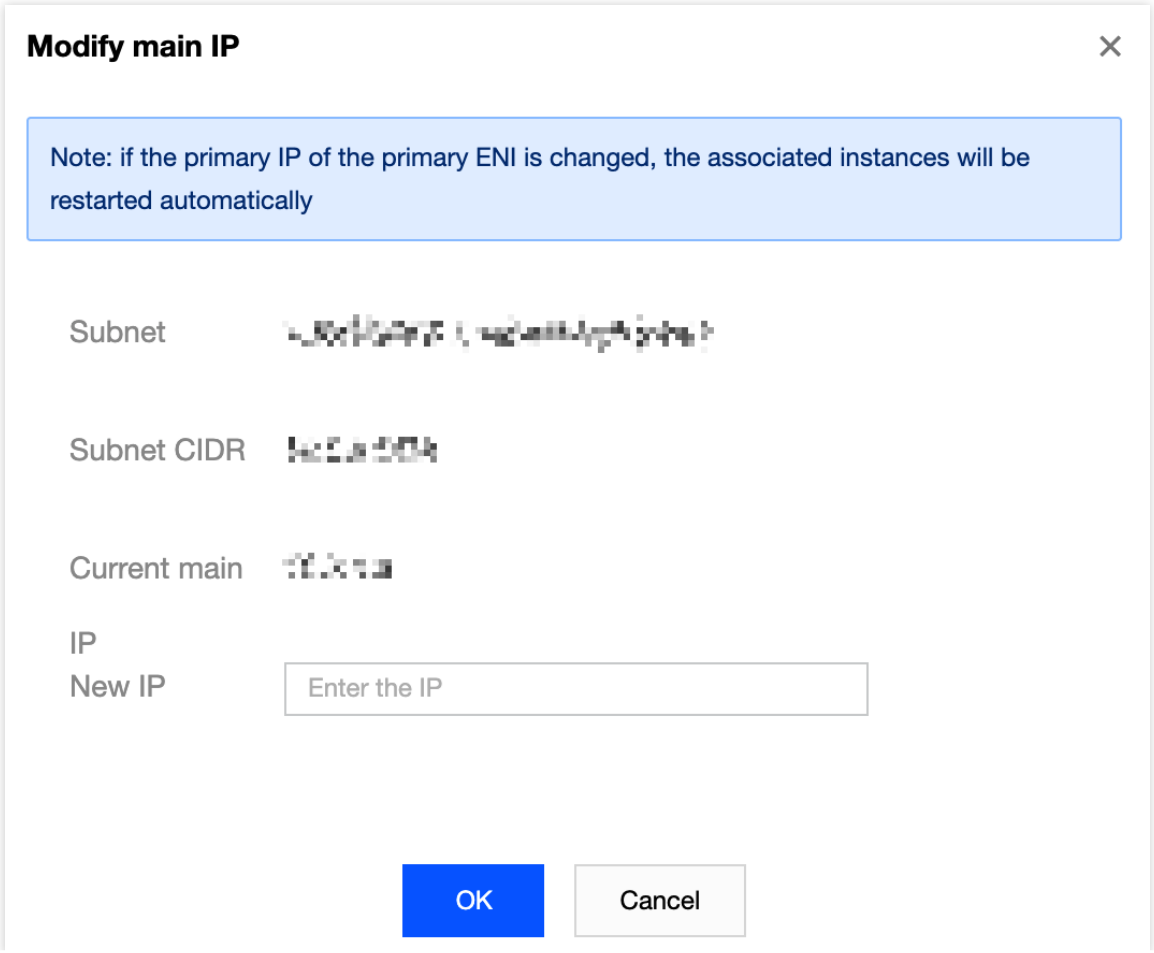
1. Log in to the VPC console.
2. Choose **IP and ENI** > **ENI** in the left sidebar to go to the ENI list page.
3. Locate the ENI you want to modify the primary IP, and click its **ID**/**Name** to enter the details page.
4. Click the **IPv4 address management** tab, and check the primary private IPs that have been bound.



5. Locate the primary private IP you want to change, and click **Modify Primary IP* under the **Operation** column.



6. Enter a new primary private IP in the pop-up window, and click **OK**.



Cloud Access Management
CAM Overview

Last updated：2024-01-11 16:04:31

If you have activated several Tencent Cloud services, such as VPC, CVM and TencentDB, and you let other users to manage these services by sharing your cloud account key, the following problems may arise:
The possibility of your key being compromised is high because it is shared by several users.
The access of other users is not under control. They can introduce security risks caused by misoperations.
To avoid the above problems, you can create sub-accounts for other users to manage different services. By default, a sub-account can not work with VPCs. Therefore, you need to create a policy to grant VPC-related permissions to them.
Note:
VPC supports access control on the resource level, such as an ENI.
Skip this chapter if you don't need to manage the access permission of sub-accounts for VPC resources.

Overview

Tencent Cloud's Cloud Access Management (CAM) is a web service that helps you manage the access permissions for resources under your Tencent Cloud accounts. With CAM, you can create, manage, or terminate users (user groups), and manage identities and policies to allow specific users to access and use specific Tencent Cloud resources.
You can use CAM to bind a user or user group to a policy which allows or denies them access to specified resources to complete specified tasks.
For more information on CAM policy elements, see Element Reference.
For more information on how to use CAM policies, see Policy.

Getting Started

A CAM policy allows or denies one or more VPC operations. You need to specify the target of the operation. The policy can also include some custom conditions.
Some APIs do not support resource-level permissions, which means that you cannot specify resources when using those APIs.

Content	Reference
Basic policy structure	Authorization Policy Syntax

Defining operations in a policy	ENI Operations
Defining resources in a policy	ENI Resource Path
Resource-level permissions supported by ENI	Resource-level Permissions Supported by ENI
CAM examples	CAM Examples

Authorizable Resource Types

Last updated：2024-01-11 16:04:31

ENI supports resource-level permission control, which means you can specify when a user is allowed for an operation, and what resource can a user get access to.
Cloud Access Management (CAM) allows you to grant access permissions to the following resources.

Resource Type	Resource Description Method in Authorization Policies
ENI APIs	`qcs::vpc:$region:$account:eni/$networkInterfaceId`

ENI APIs describes ENI API operations that currently support resource-level permissions as well as resources and condition keys supported by each operation. **When configuring the resource path,** you need to replace variable parameters such as `$region` and `$account` with your actual parameters. You can also use the `*` wildcard in the path. For more information, see CAM Examples.

Note:

ENI API operations not listed in the table do not support resource-level permissions. You can still authorize users to perform these operations, but the resource element of the policy statement must be specified as `*` .

ENI APIs

API Operation	Resource Path
Requesting a private IP for an ENIAssignPrivateIpAddresses	ENI resourceqcs::vpc:$region:$account:eni/*qcs::vpc:$region:$account:
Binding an ENI to a CVMAttachNetworkInterface	ENI resourceqcs::vpc:$region:$account:eni/*qcs::vpc:$region:$account:
Creating an ENI and binding it to a CVMCreateAndAttachNetworkInterface	VPC resourceqcs::vpc:$region:$account:vpc/*qcs::vpc:$region:$accour
	CVM resourceqcs::cvm:$region:$account:instance/*qcs::cvm:$region:$a
	ENI resourceqcs::vpc:$region:$account:eni/*
Creating an ENICreateNetworkInterface	VPC resourceqcs::vpc:$region:$account:vpc/*qcs::vpc:$region:$accour
	Subnet resourceqcs::vpc:$region:$account:subnet/*qcs::vpc:$region:$a
	ENI resourceqcs::vpc:$region:$account:eni/*
Deleting an ENIDeleteNetworkInterface	ENI resourceqcs::vpc:$region:$account:eni/*qcs::vpc:$region:$account:
Unbinding an ENI from a	CVM resourceqcs::cvm:$region:$account:instance/*qcs::cvm:$region:$a

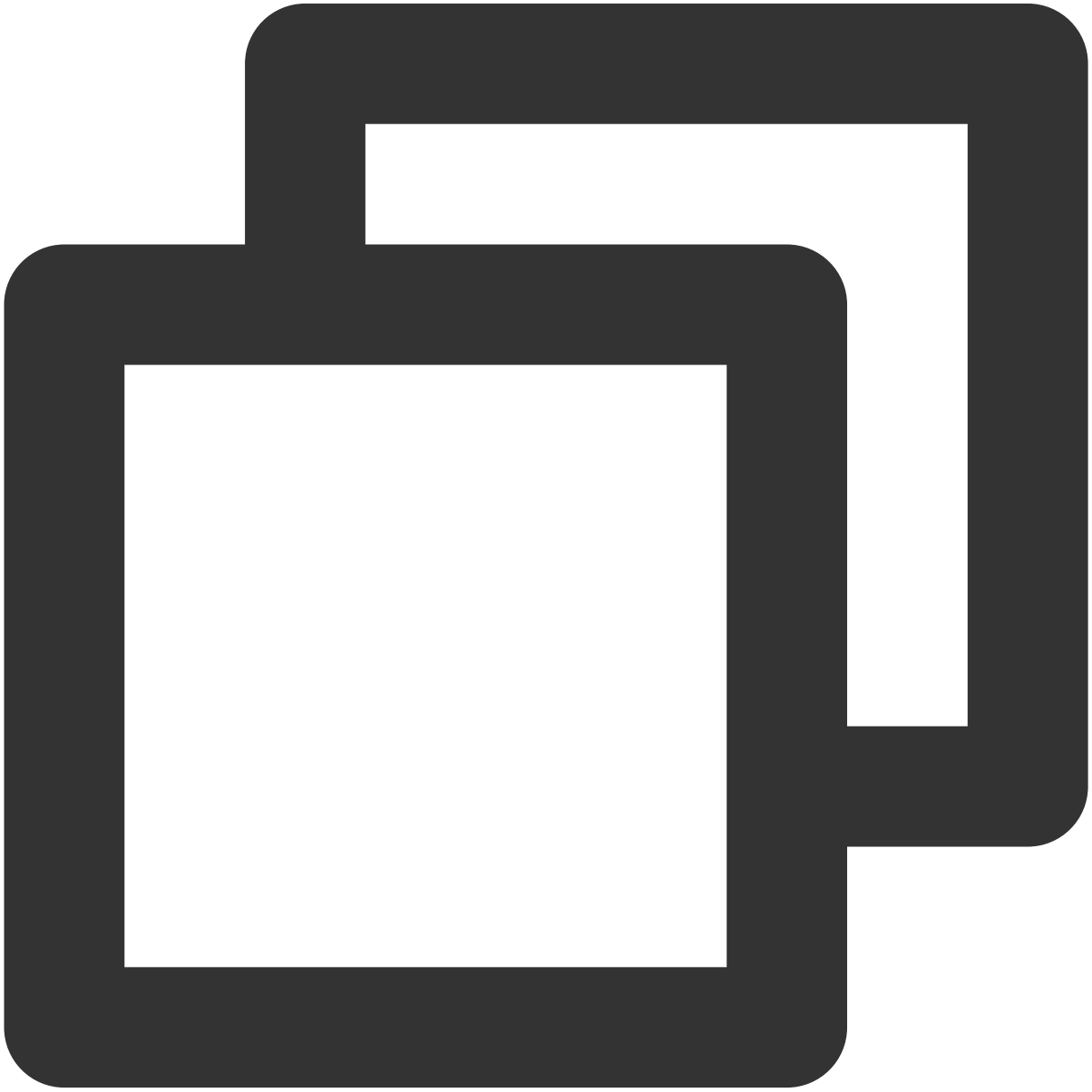
CVMDetachNetworkInterface	ENI resourceqcs::vpc:$region:$account:eni/*qcs::vpc:$region:$account:
Migrating an ENIMigrateNetworkInterface	CVM Resourceqcs::cvm:$region:$account:instance/*qcs::cvm:$region:$accou is required before and after the migration)
	ENI resourceqcs::vpc:$region:$account:eni/*qcs::vpc:$region:$account:
Migrating a private IP of an ENIMigratePrivateIpAddress	ENI resourceqcs::vpc:$region:$account:eni/*qcs::vpc:$region:$account:
Modifying an ENIModifyNetworkInterfaceAttribute	ENI resourceqcs::vpc:$region:$account:eni/*qcs::vpc:$region:$account:
Modifying the private IP Information of an ENIModifyPrivateIpAddressesAttribute	ENI resourceqcs::vpc:$region:$account:eni/*qcs::vpc:$region:$account:
Returning a private IP of an ENIUnassignPrivateIpAddresses	ENI resourceqcs::vpc:$region:$account:eni/*qcs::vpc:$region:$account:

Authorization Policy Syntax

Last updated：2024-01-11 16:04:31

Policy Syntax

CAM policy:



```
{
```

```
          "version":"2.0",
          "statement":
          [
              {
                  "effect":"effect",
                  "action":["action"],
                  "resource":["resource"],
                   "condition": {"key":{"value"}}
              }
          ]
}
```

`version` : (Required) It must be `2.0` for now.

`statement` : It describes the details of one or more permissions. It contains `effect` , `action` , `resource` , and `condition` . One policy can have only one `statement` .

1.1 `action` : (Required) It specifies whether to allow or deny the operation. The operation can be an API (prefixed with `name`) or a feature set (a group of APIs, prefixed with `permid`).

1.2 `resource` : (Required) It describes the details of an authorization. A resource is described in a six-part format. Detailed resource definitions vary by product. For more information on how to specify a resource, see the corresponding documentation for the product for which you want to write a resource statement.

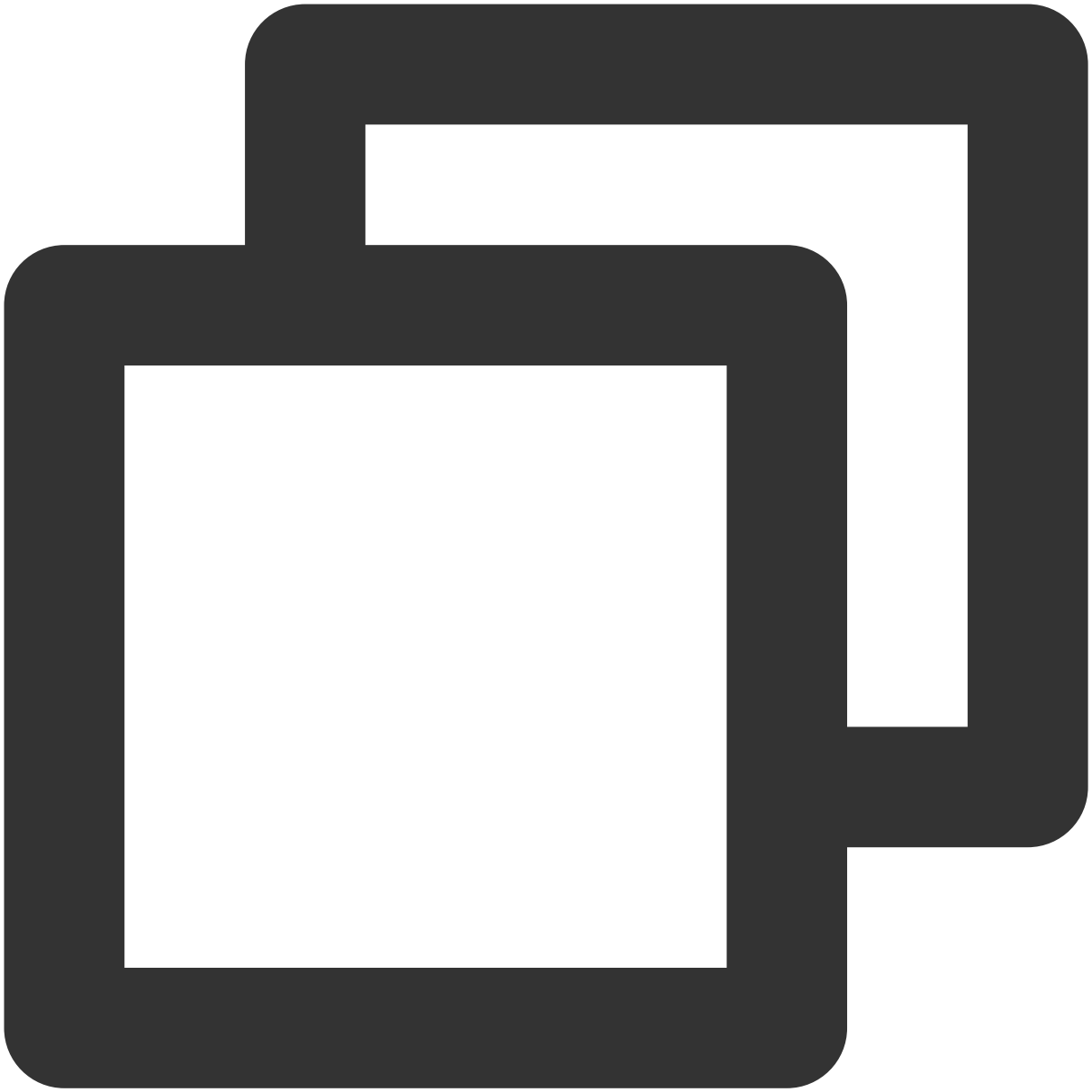
1.3 `condition` : (Optional) It describes the condition for the policy to take effect. A condition consists of an operator, an action key, and an action value. A condition value may contain information such as time and IP address. Some services allow you to specify additional values in a condition.

1.4 `effect` : (Required) It describes whether the statement result is `allow` or `deny` .

ENI Operations

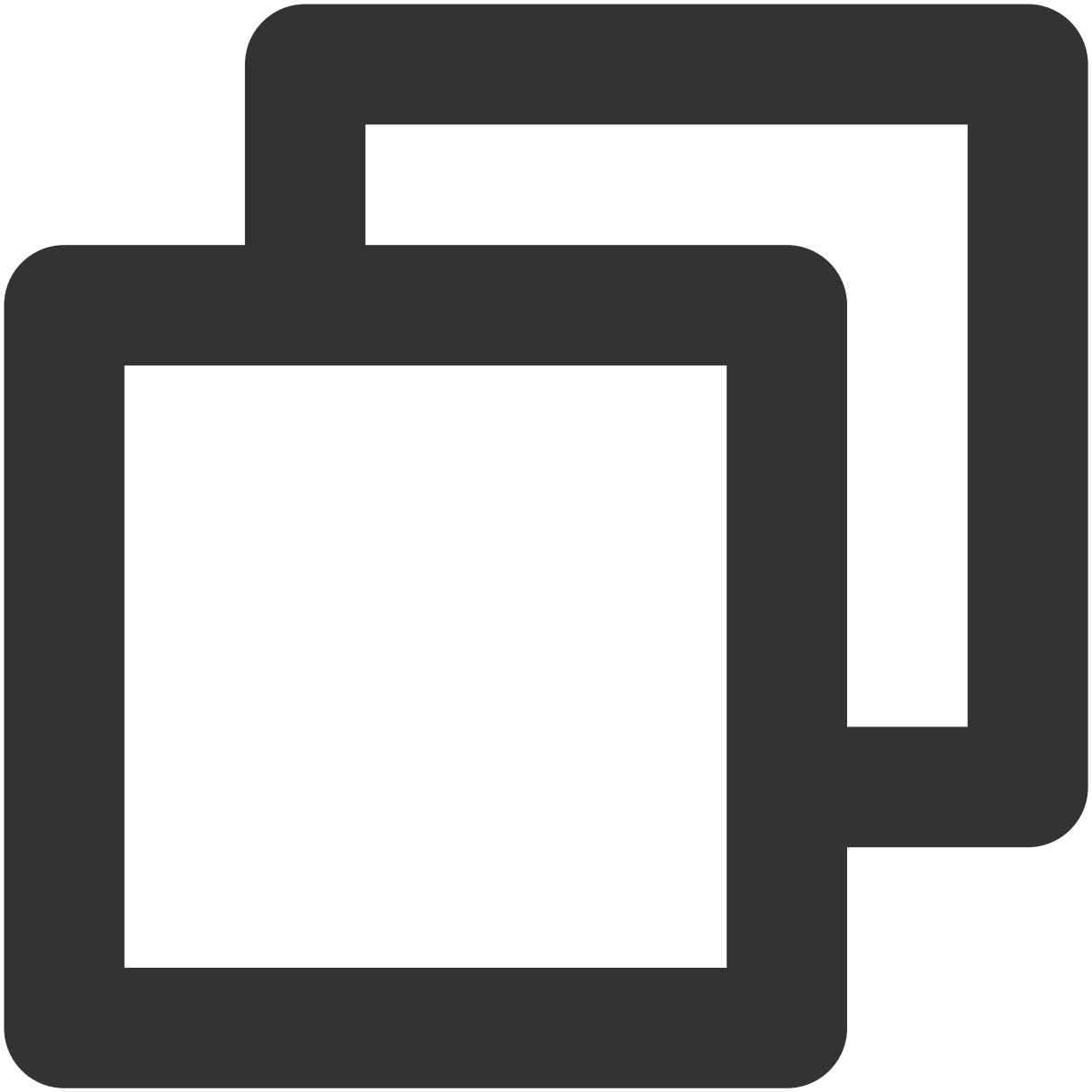
In the statement of a CAM policy, you can specify any API operation from any service that supports CAM. For VPC, use APIs with the prefix `name/vpc:` , for example, `name/vpc:Modify` , or `name/vpc:CreateNetworkInterface` .

To specify multiple operations in a single statement, separate them with commas, as shown below:



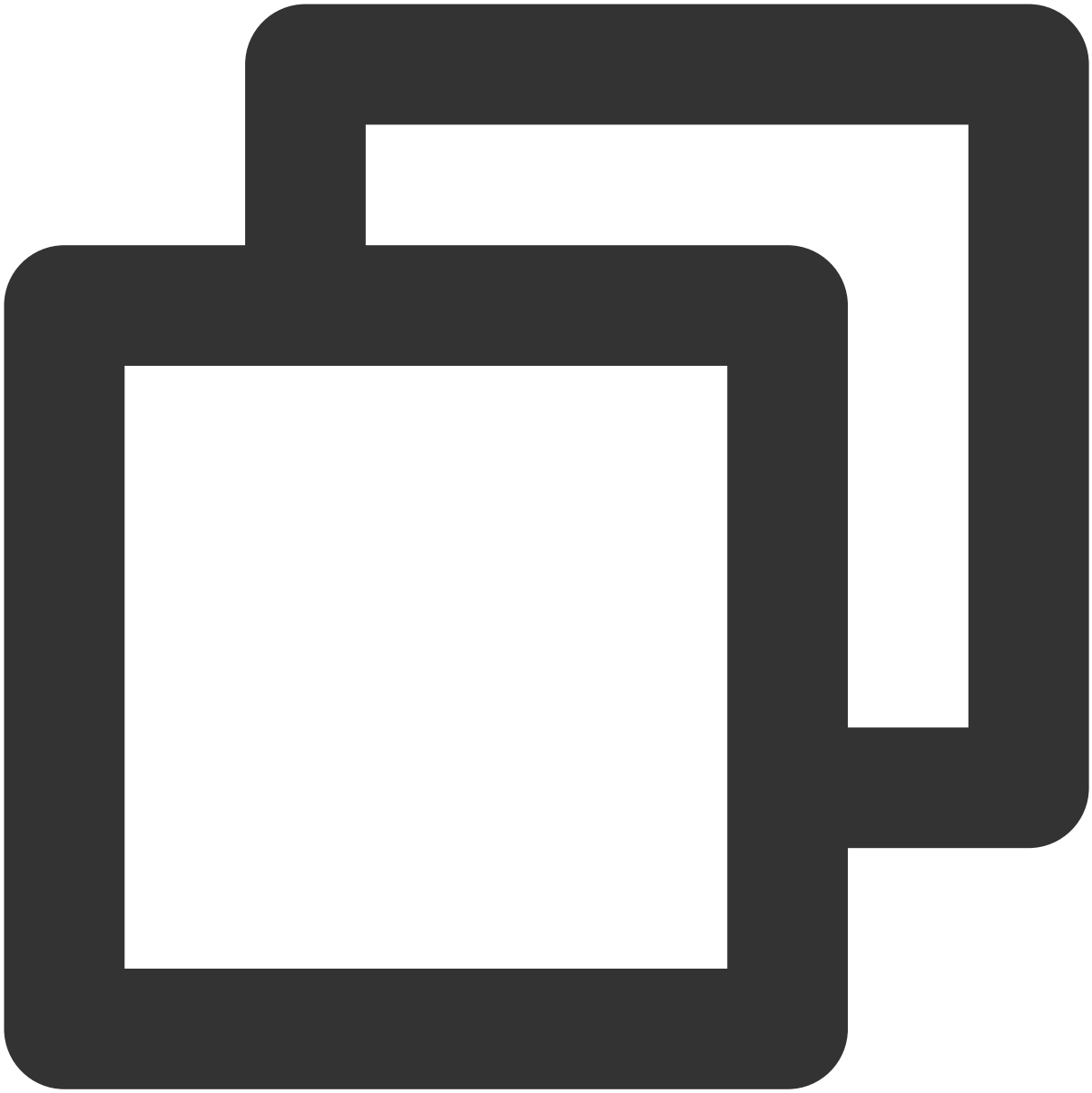
```
"action":["name/vpc:action1","name/vpc:action2"]
```

You can also specify multiple operations by using a wildcard, such as all operations that start with "Modify" as shown below:



```
"action":["name/vpc:Modify*"]
```

To specify all operations in a VPC, use a wildcard (*) as follows:

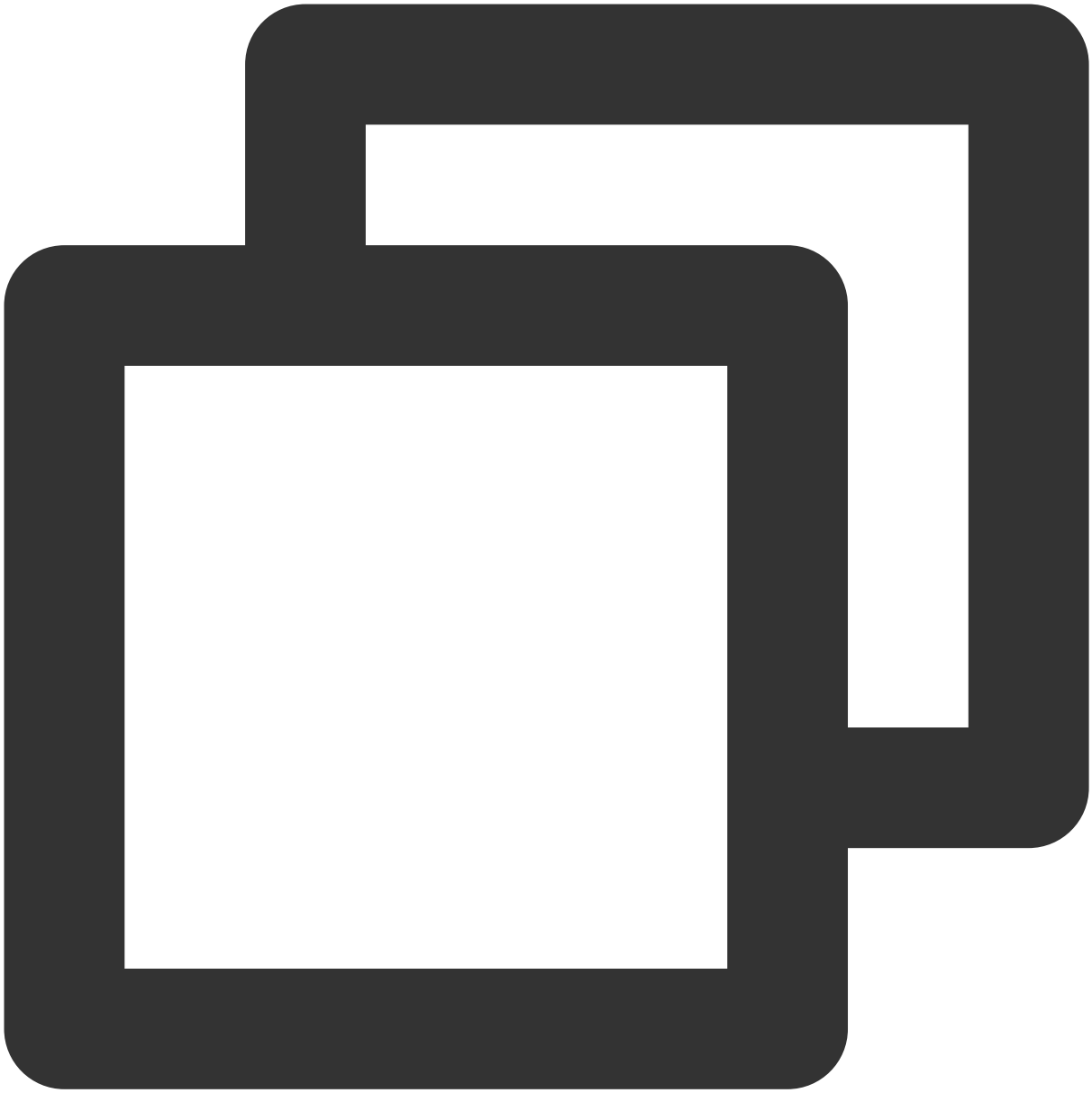


```
"action"：["name/vpc:*"]
```

ENI Resource Path

Each CAM policy statement has its own applicable resources.

The general format of resource paths is as follows:



```
qcs:project_id:service_type:region:account:resource
```

project_id: Describes the project information, which is only used to enable compatibility with legacy CAM logic and can be left empty.

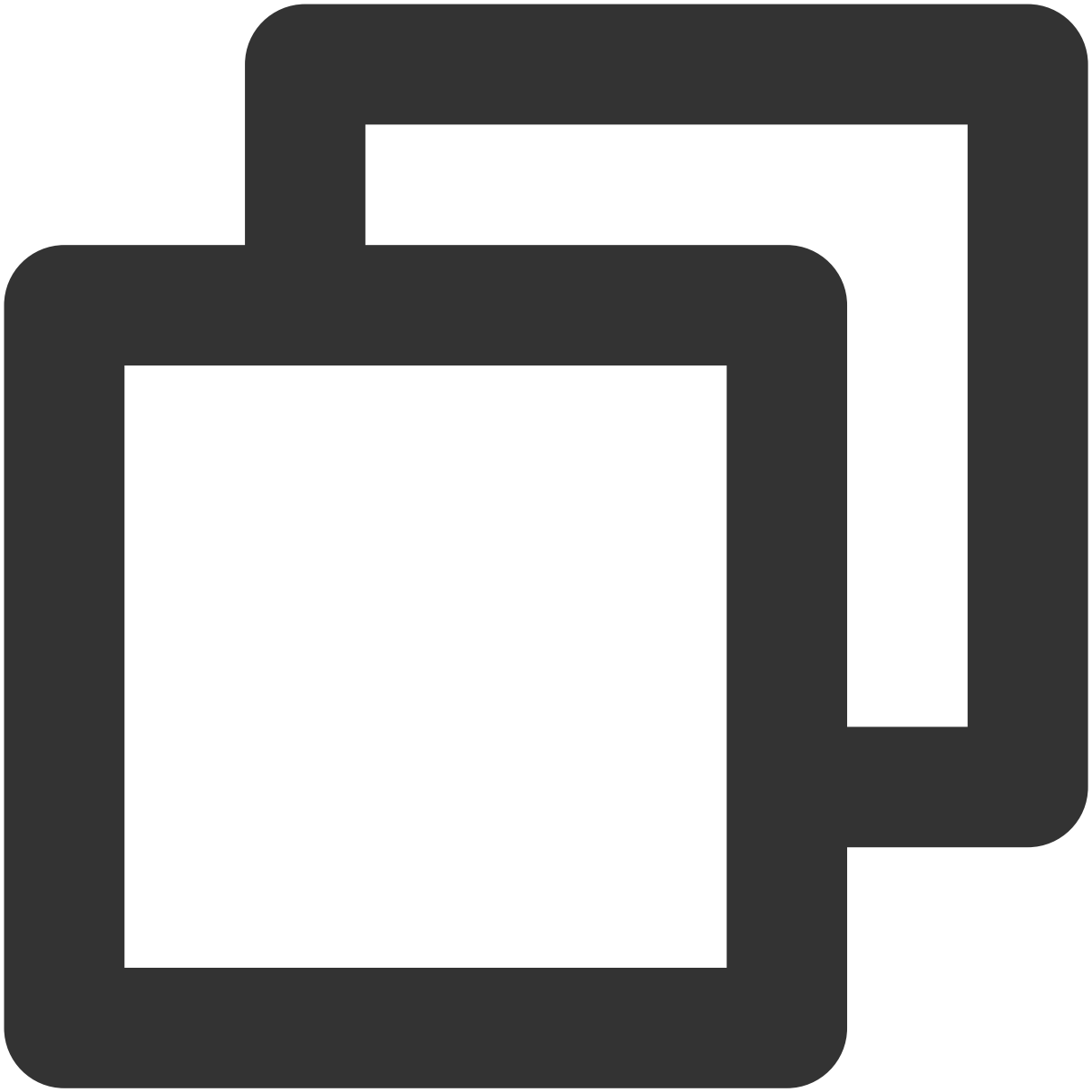
service_type: Abbreviation of the Tencent Cloud service, such as `VPC`.

region: Region of the resource, for example, `bj`.

account: Root account of the resource owner, such as `uin/164256472`.

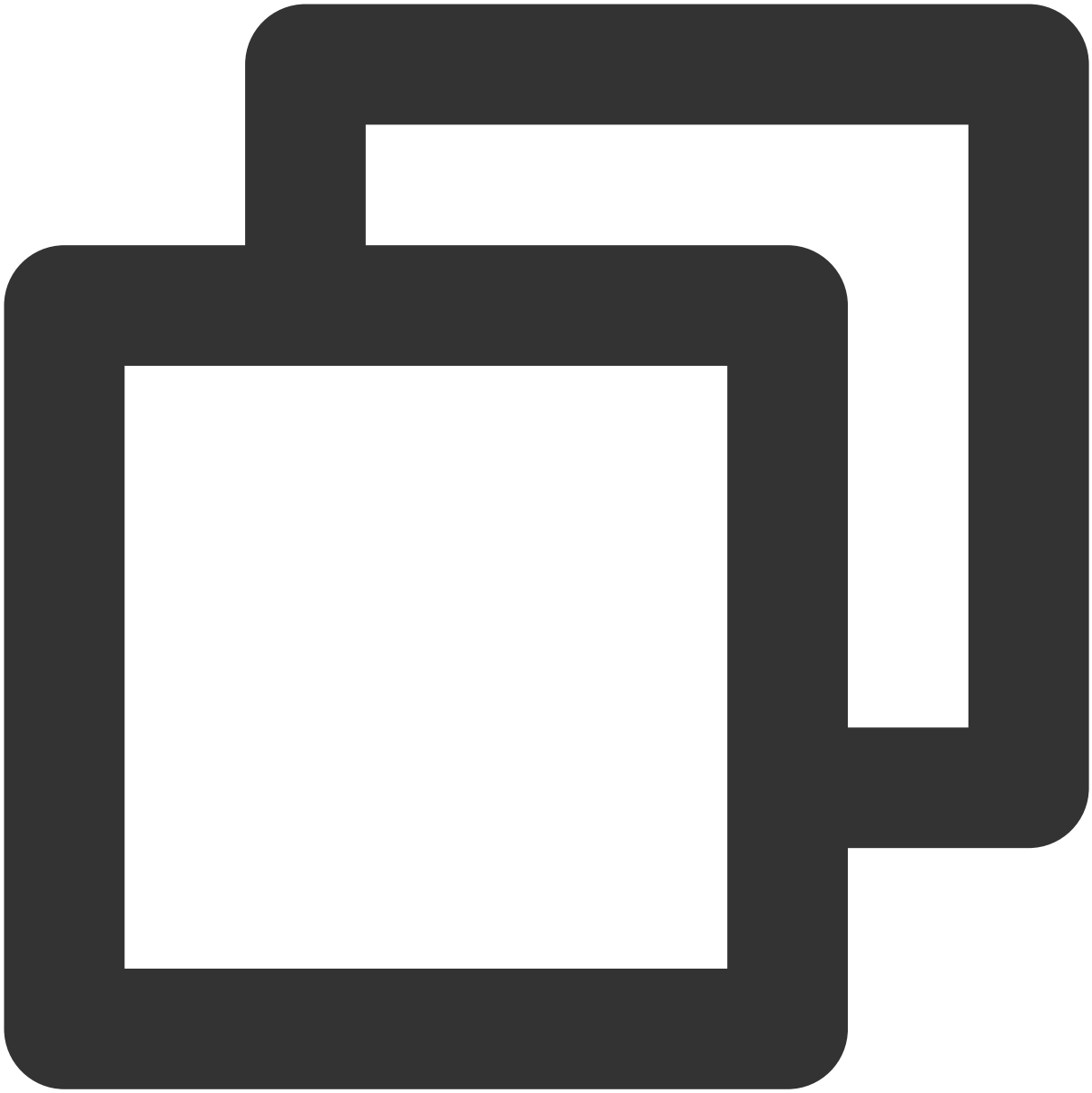
resource: Describes the resource details of each product, such as `eni/eni_id1` or `eni/*`.

For example, you can specify a specific instance (eni-abcdefgh) in the statement as follows:



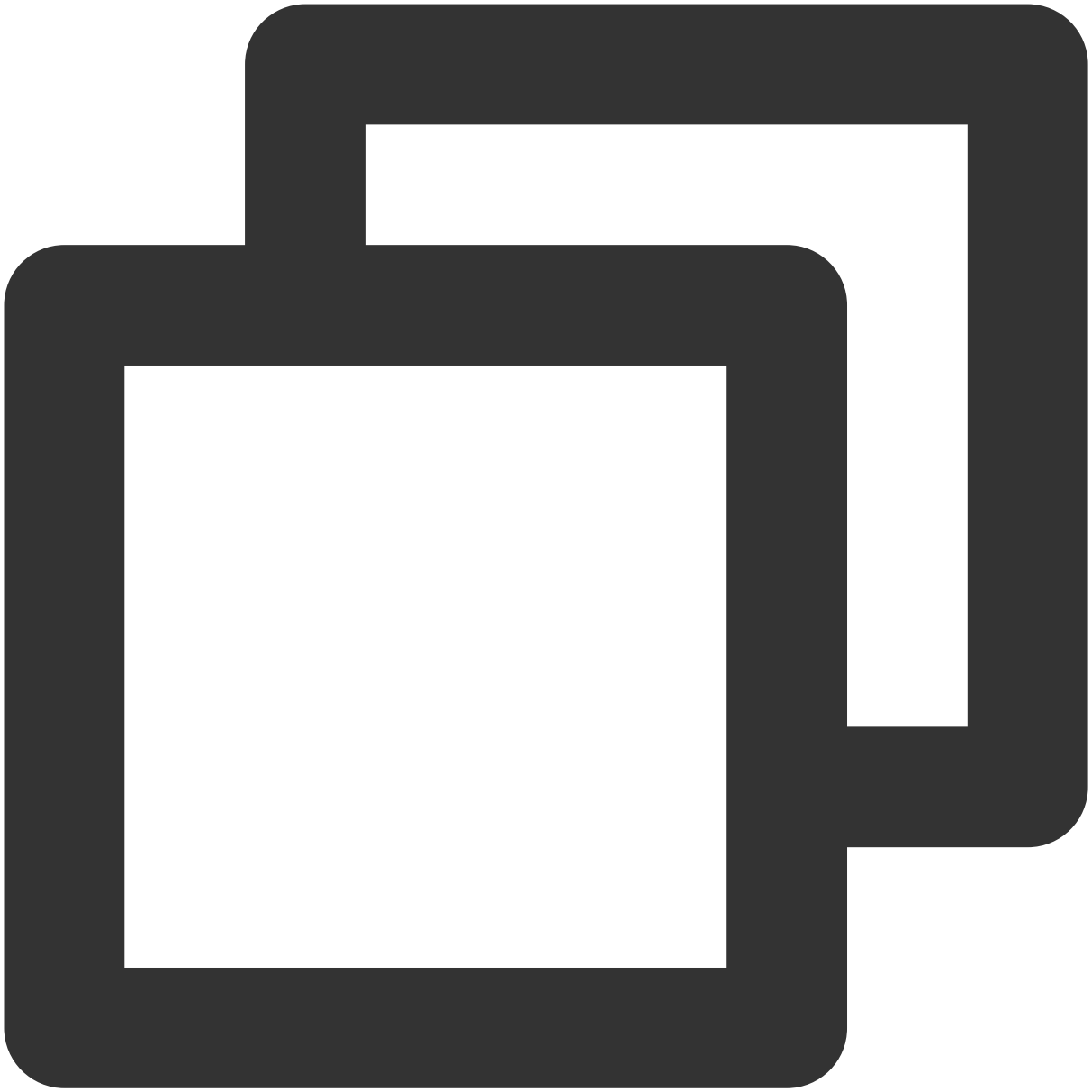
```
"resource":[ "qcs::vpc:bj:uin/164256472:eni/eni-abcdefgh"]
```

You can also use the wildcard (*) to specify all instances that belong to a specific account as shown in the following:



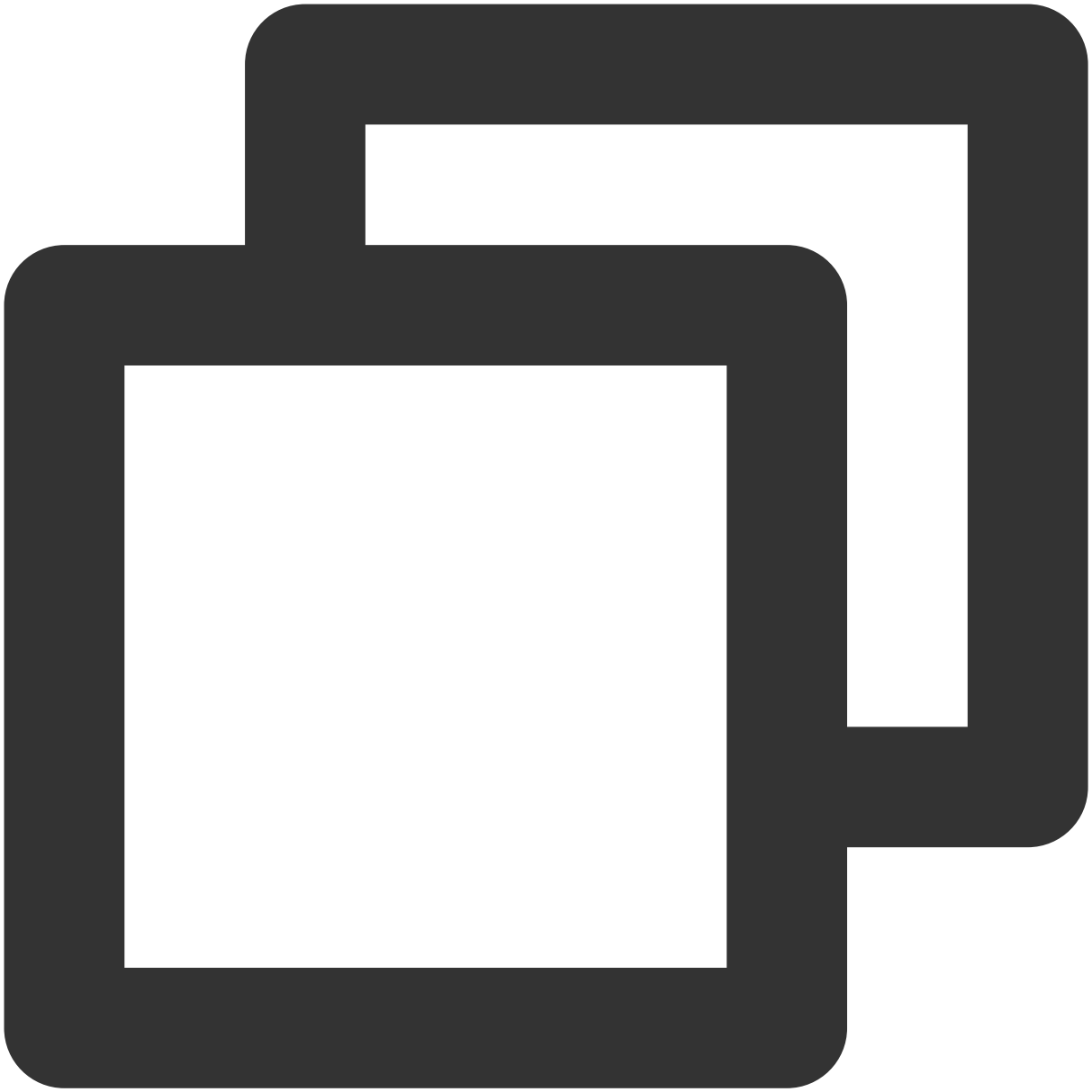
```
"resource":[ "qcs::vpc:bj:uin/164256472:eni/*"]
```

If you want to specify all resources or if a specific API operation does not support resource-level permission, you can use the wildcard (*) in the `resource` element as shown below:



```
"resource": ["*"]
```

To specify multiple resources in one policy, separate them with a comma.



```
"resource":["resource1","resource2"]
```

CAM Examples

Last updated：2024-01-11 16:04:31

Overview

You can grant a user the permission to view and use specific resources in the ENI console by using a Cloud Access Management (CAM) policy. This document describes how to grant the permission to view and use specified resources.

Examples

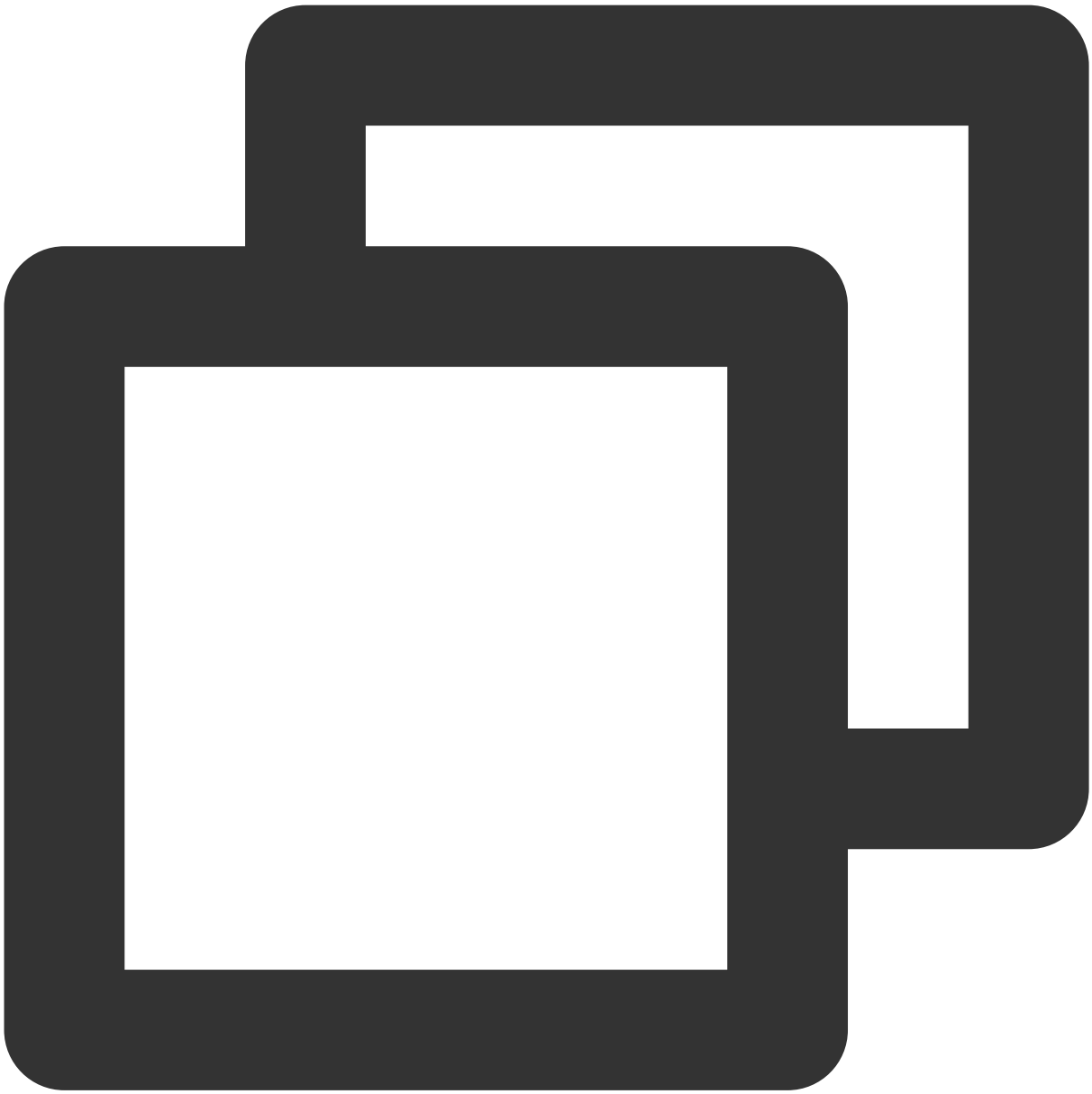
This example grants a sub-user the permission DeleteNetworkInterface to delete the ENI *eni-abcdefgh*.

Solution 1. Generating a policy by policy generator

With a policy created by the policy generator, you can create policy syntax automatically by selecting a service and operations, and defining resources. This method is highly recommended for its simplicity and flexibility.
1. Log in to the CAM console. Click **Create custom policy** in the upper-left corner.
2. In the pop-up window, click **Create by policy generator** to go to the **Edit policy** page.
3. Select the service in the **Visual policy generator**, enter the following information, and edit an authorization statement. (You can also choose JSON to use the policy syntax method to edit the policy, and the authorization effect is the same as the **Visual policy generator**).
Effect (required): You can select "Allow" or "Deny". Select "Allow" in this example.
Service (required): Select the desired product. Select "VPC" in this example.
Action (required): Select the desired operation. Select DeleteNetworkInterface in this example.
Resource (required): Select all resources or the desired resource. In this example, we use six-piece format, that is, qcs::vpc:$region:$account:eni/$networkInterfaceId, where the "$region", "$account:eni" and "$networkInterfaceId" are set to the actual region, account and ENI instance ID respectively.
4. After editing the policy authorization statement, click **Next** to enter the **Associate with user/user group** page.
Note:
The policy name is `policygen` by default, which is generated automatically in the console. The suffix number is generated based on the creation date. This is customizable.
You can also associate the policy with a user/user group after creation of the policy.
5. Click **Complete**.

Solution 2: Generating policy by policy syntax

The following policy allows you to delete the ENI instance *eni-abcdefgh*. You can associate the policy with a user or user group.



```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "vpc:DeleteNetworkInterface"
            ],
```

```
            "resource": [
                "qcs::vpc::uin/10000xxxxxxx:eni/eni-abcdefgh"
            ]
        }
    ]
}
```