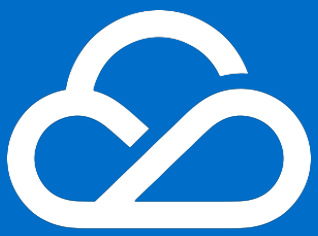
Cloud Virtual Machine

Network and Security

Product Introduction



Tencent
Cloud

Copyright Notice

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Network and Security

Overview

Tencent Cloud provides the following network and security features:

- Security group
- Encryption login method
- Elastic IP
- Internet access
- Private network access
- Basic network and private network

You can use Security Group to control access to your instance. These security groups resemble a network firewall, allowing you to specify the protocols, ports, and source/target IP ranges that are allowed access. You can create multiple security groups and assign different rules to each security group. You can then assign one or more security groups to each instance, and we will use these rules to determine what traffic is allowed to access instances and which resources the instance can access. You can configure a security group so that only a specific IP address or a specific security group can access the instance.

Tencent Cloud provides two encryption login methods: Password Login and SSH Key Pair Login. Users are free to choose two ways to securely connect with the CVM.

Instances may fail because of uncontrollable reasons. If an instance fails and you start a replacement instance, the public IP of the alternate instance will be different from the original instance. However, if your application requires a static IP address, you can use an Elastic IP Address.

Tencent's Internet Link gives access to more than 20 domestic mainstream network operators to ensure that your customers, regardless of ISP, can enjoy the same high-speed access; Private Network Link goes through an underlying 10 Gigabit / Gigabit network interoperability to ensure high-speed access, high reliability and low latency.

The user's Network Environment can be roughly divided into 'basic network' and 'private network'. Under a basic network, your cloud product instance is located in a large resource pool preset by Tencent Cloud; under a private network, your cloud product instance can be activated under your

own preset, custom network segments, and isolated from other users.

The above network and security services protect your instances; making them safe, efficient and able to freely provide external services.

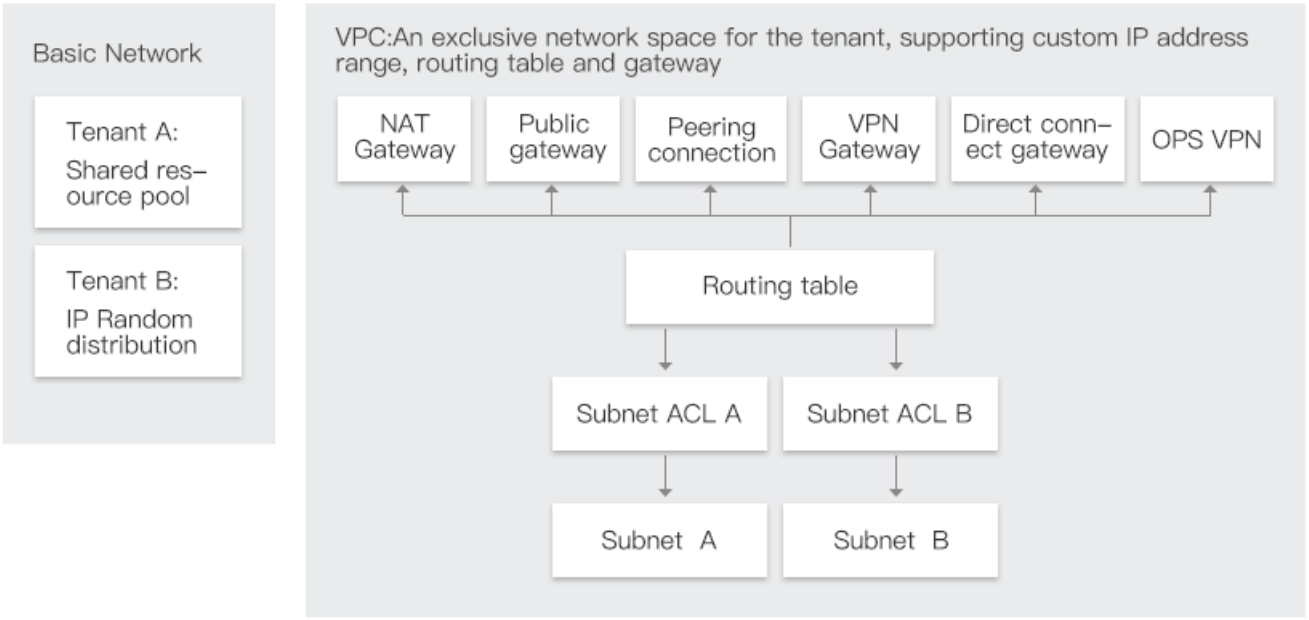
Network Environment

Tencent Cloud network environment can be divided into either basic network and private network (VPC).

Through the Tencent Cloud basic network, all of the user's resources on the cloud are managed uniformly by Tencent Cloud; relatively speaking, these configurations are simpler and more convenient to use, helping users manage their CVMs faster and easier. All basic network instances in the same geographical area are free to communicate via Private Network Service under the user account. Most of the user's needs can be met through the basic network and implementation; this is best and most convenient if you are just beginning to understand and use Tencent Cloud.

With the Tencent Cloud Private Network (VPC), you can customize a logical isolated virtual network within the cloud and launch a CVM resource (such as an instance) into the quarantine. Even in the same area, different VPCs cannot communicate with each other by default. VPC is very similar to traditional networks that data centers run, but at the same time, can offer you faster and more extensible infrastructures on the cloud. Users can customize network topology and IP addresses within the network and configure the Router Table, gateway and security settings; supports Dedicated Connection through your local data center, and rapid expansion of computing resources; freely plan how your VPC communicates with the Internet. Use a variety of control methods (including Security Group and Network ACL to protect VPC resources. For more information, see Private Network Product Documentation. Private networks can help users build more complex network architectures, suitable for users who are familiar with network management.

Basic network and private network



The functional differences between the private network and the basic network are shown in the table below:

Function	Private Network	Basic Network
Renter Association	Logical Isolated Network Based on GRE Encapsulation	Renter Association
Network customization	Yes	No
Router customization	Yes	No
Custom IP	Yes	No
Intercommunication Rules	Supports cross-domain, cross-account intercommunication	Interoperable among renters in the same geographical area
Security control	Security group and Network ACL	Security group

Advantages of VPC

By starting the instance within the VPC, you can:

- Assign an instance of your custom private static IP.
- Assign multiple IP addresses to your instance (coming soon).
- Controls inbound and outbound traffic for an instance.
- Add an additional access control layer to the instance using the Network Access Control List

(ACL).

Share and access resources between basic network and VPC

Some of the resources and functions on Tencent Cloud can support two kinds of network environments, and can be shared or accessed between different networks.

Resources	Instructions
Image	can be used to start a CVM instance in any network environment
Elastic IP	Elastic IPs can be bound to any network environment on a CVM instance
Instances	Instances on a basic network and instances within the private network can be accessed through Public IP or Basic Network Interoperability functions to achieve intercommunication
SSH Key	SSH key supports loading a CVM instance under any network environment
Security Group	Security Groups support binding to CVM instances in any network environment

Note: Cloud Load Balance cannot be shared between the underlying network and the VPC. That is, Cloud Load Balance does not support binding basic network instances and VPCs at the same time; even though the VPC and the basic network are connected through the basic network and can intercommunicate.

Migrate instances within the basic network to VPC

1) Create a Custom Image for the CVM instance in the basic network environment.

2) (Optional) Create a Snapshot of the CVM instance data disk in the basic network environment.

3) Create a VPC and Subnet.

4) Purchase and Start the CVM Instance in the VPC.

Login Password

The first step in using a CVM instance is to login. To ensure the security and reliability of the instance, Tencent provides two encryption login methods: password login and SSH key pair login. A password is the login credentials specific to each CVM instance, and the SSH key can be used for multiple CVM instances at the same time.

Anyone with an instance login password can log into the CVM instance remotely through a public network address that is allowed by the security group. Therefore, it is recommended that you use a more secure password, keep it safe, and modify the login password for your instance periodically.

A user can specify to use a password or SSH key when purchasing Purchase and Start Instance. When using a password, it can be set by itself or automatically generated. When the password is generated automatically, the initial password will be delivered to the user via Internal Message. Users can learn from the below content on how to set an initial password and how to reset settings in case you forgot your password, etc.

Set the initial password

1) Purchase and Start Instance, you can select the login method in the Set Host Name and Login Mode section. The default is [Set Password].

2) In accordance with password character limitations, enter the host password and confirmation, then click Buy Now; the initial password will be set successfully when the CVM instance is successfully assigned.

3) You can also select [Auto Generate Password], and click [Buy Now] to get the CVM instance initial password via Internal Message after the CVM instance is successfully assigned.

It is important to note that the character limitations for setting a password is as follows:

- Linux device passwords must be between 8-16 chars, and include 2 of the following items (

  a-z

`

A-Z

`

0-9

and

[

`

(

`

)

`

\

`

~

`

!

`

@

`

#

`

$

`

%

`

^

`

&

`

\

`

*

`

-

```
`
+
`
=
`
|
`
{
`
}
`
[
`
]
`
:
`
```

;

`

'

`

,

`

.

`

?

`

/

`

]

and ` or other special symbols)

- Windows device passwords must be between 12-16 chars, and include 3 of the following items (

a-z

`

A-Z

`

0-9

and

[

`

(

`

)

`

\

`

~

`

!

`

@

`

#

`

$

`

%

`

^

`

&

`

\

`

*

`

-

`

+

`

=

`

|

`

{

`

}

`

[

`

]

`

:

`

;

`

'

`

,

`

.

`

?

`

/

`

]

and ` or other special symbols)

Reset password

Note: You can reset the password for the cloud host only when it is powered off. If the machine is running, please shut down the host first.

1) Open CVM console.

2) For a single CVM instance that is shut down, in the right-hand action bar, click [More] - [Reset Password].

3) For batch CVM instances, select all the hosts that need a password reset; then at the top of the list, click [Reset Password] to modify the host login password in batches. A CVM instance that cannot have its password reset will display the reason why.

4) In the Reset password pop-up box, enter the new password, confirm the password and the verification code, then click [Confirm Reset].

5) Wait for the reset to succeed, and you will receive a successful reset message in your station inbox; now you can use the new password to start and use your CVM.

SSH Key

The first step is to log into the CVM instance. To ensure the security of the instance, Tencent provides two encryption login modes: password login and SSH key pair login .

Tencent Cloud allows public key cryptography to encrypt and decrypt logins for Linux instances. Public key cryptography uses a public key to encrypt a piece of data, such as a password, and then the recipient can decrypt the data using the private key. Public and private keys are called key pairs. Users can securely connect to a CVM via a key pair, which is a more secure way to log into a CVM than using a regular password.

To log into your Linux instance using an SSH key, you must first create a key pair, specify the name of the key pair when you start the instance, and then use the private key to connect to the instance. Tencent Cloud will only store the public key; you need to store the private key yourself. Anyone with your private key can decrypt your login information, so it's important to keep your private key in a safe location.

> Note: Windows instances do not support SSH key logins.

Create SSH Key

1) Open CVM console.
2) Click [SSH Key] in the navigation pane.
3) Click [Create Key]:

- For the "Create New Key Pair" method, input the key name, and click [OK].
- For the "Use an Existing Public Key" method, in addition to entering the key name, you also need to enter the original public key information, and finally click the [OK] button.
  4) After clicking the [OK] button, a pop-up box will appear, and the user will need to download the private key within 10 minutes.

Bind/unbind the key to the server

1) Open CVM console.
2) Click [SSH Key] in the navigation pane.
3) Select SSH Key and click the [Bind/Unbind Cloud Host] button.
4) Select the region, then select the CVM to be associated/unbound, drag it to the right, and click OK.
5) The SSH key is issued in the background, and the result window is displayed when the configuration is complete. For example, when an association succeeds or fails.
6) Click the [Details] URL to view the results of the most recent operation.

Modify the SSH key name / description

1) Open CVM console.
2) Click [SSH Key] in the navigation pane.
3) Select the key you want to modify in the key list and click the [Modify] button.
Or right-click the name of the key to be modified, and click the [Modify] button.
4) Enter the new name and description in the pop-up box, and click [OK].

Delete SSH Key

Note: If the SSH key is associated with a CVM or a custom mirror, it cannot be deleted.

1) Open CVM console.
2) Click [SSH Key] in the navigation pane.
3) Select all SSH keys to be deleted, and click the [Delete] button. Or right-click the name of the key to be deleted, and click [Delete]; then in the pop-up window, click [OK].

Log into a Linux CVM using the SSH key

To log into a Linux CVM using the SSH key, you first need to bind the SSH key to the CVM.

For details on how to log into a Linux CVM using the SSH key, see Logging onto a Linux CVM.

Private Network Access

Cloud products on the Tencent Cloud can be accessed via Internet access or accessed mutually via the Tencent Cloud private network. Private network services are Local Area Network (LAN) services, which are accessed mutually via private links. Tencent Cloud server rooms are interconnected by an underlying 10 Gigabit / Gigabit, providing high bandwidth, low latency within network communications services; and regions within the private network enjoy communications completely free of charge, helping you build a flexible network architecture.

- Private network services contain user attributes; different users are isolated; that is, by default they cannot access another user's network through CVM services.
- Private network services also have geographical attributes, and different geographical isolation; that is, by default, they cannot access the network through different accounts under cloud services.

Private IP address

A private IP address is an IP that cannot access via the Internet; this is an implementation of private services by Tencent Cloud. You can use private IP addresses to implement communications between instances on the same network (basic networks or VPC). Each instance has a default network interface (ie, eth0) for assigning private IP addresses. Private IP addresses can be automatically assigned by Tencent and customized by users (only in [Private Network] environments). The combination of Internet services, and the Tencent cloud network architecture consists of the following two parts:

- Public network cards: Unanimously configured on the TGW interface layer, without CVM perception. When an instance is assigned a Public IP address, TGW automatically configures a public network interface for it.
- Private network card: Managed by Tencent Cloud, supports user configurations.

Therefore, when the user uses commands such as 'ifconfig' to view network interface information on the CVM, only the IP information of the private network can be viewed. For public network information, users need to log onto the Tencent Cloud Console CVM list/details page to view. Please

note that if you change the private network IP within an operating system, it will lead to an interruption of network communications.

Private IPs can be used for CLB load balancing, inter-network visits between CVM instances and between CVM instances and other cloud services, such as CDN and CDB.

How to obtain a private IP address

Each CVM instance is assigned a default private IP at startup. For different Network Environments, the private IP is also different:

- Basic network: private IPs within the network are automatically assigned by Tencent Cloud, and cannot be changed.
- Private network: the initial private IP assigned by Tencent Cloud is done automatically within the VPC network segment of an arbitrary address allocation; the user can be in the '10.[0 - 255].0.0/8', '172.[0 - 31].0.0/16' and '192.168.0.0/16' to define the private IP address for the CVM instance. The specific value range is determined by the private network of the instance. For more information, refer to Private Network and Subnet.

Private network DNS

Private network DNS services are responsible for domain name resolutions; if a DNS configuration is wrong, the domain name cannot be accessed. Therefore, Tencent Cloud provides reliable private DNS servers in different regions. The specific configuration is as follows:

Network environment	Region	Private DNS server
Basic network	Guangzhou	10.225.30.181 10.225.30.223
	Shanghai	10.236.158.114 10.236.158.106
	Beijing	10.53.216.182 10.53.216.198
	Shanghai Finance	10.48.18.9 10.48.18.82

	North America	10.116.19.188 10.116.19.185
	Hong Kong	10.243.28.52 10.225.30.178
	Singapore	100.78.90.19 100.78.90.8
Private network	All regions	183.60.83.19 183.60.82.98

When a network analysis discovers errors, users can manually set up the private network DNS. Set as follows:

- For Linux systems, you can modify the CVM DNS by editing the '/ etc / resolv.conf' file. Run the command '/ etc / resolv.conf', according to the corresponding table in different regions to edit the geographical DNS IP.

```
root@VM-90-86-ubuntu:~# vi /etc/resolv.conf
nameserver 10.243.28.52
nameserver 10.225.30.178
options timeout:1 rotate
~
~
```

- For Windows, you can modify the DNS server by opening the [Control Panel] - [Network and Sharing Center] - [Change Adapter Devices], then right-clicking on the network card [Properties] and double-clicking [Internet Protocol Version 4].

Obtain private IP of instance

You can use the Tencent Cloud console and API to determine the private IP of the instance. You can also use the instance metadata to determine the private IP of an instance from within. For more information, see Instance Metadata.

Use console to obtain private IP of instance

1) Open CVM console.

2) CVM list shows the names of your instances; move the mouse over the CVM private IP, click on the copy button that appears, and copy the IP.

3) (Optional) Click on the CVM Instance ID to view detailed CVM info, including Parameters , Monitoring , Health Check , Security Group , Operation log .

> The public IP is mapped to the private network IP through NAT. Therefore, if you view the properties of the network interface within the instance (for example, through ifconfig (Linux) or ipconfig (Windows)), the public IP is not displayed.

Use API to obtain private IP of instance

Refer to DescribeInstances interface.

Use instance metadata to obtain private IP of instance

First, you need to login to the CVM instance. For details, refer to Logging into Linux Instance and Logging into Windows Instance.

Use the following command to obtain the private IP:

curl http://metadata.tencentyun.com/meta-data/local-ipv4

The return value is as follows

```
[root@VM_58_27_centos ~]# curl http://metadata.tencentyun.com/meta-data/local-ipv4
10.105.58.27
```

Internet Access

When an application deployed by a user on a CVM instance needs to provide public services, the data must be transferred over the Internet. Tencent Cloud Internet access is provided by Tencent Cloud data centers via high-speed Internet. Domestic multi-line BGP networks cover more than 20 ISPs; BGP public network external ports switches cross-domains instantly, guaranteeing that users can enjoy high-speed, secure network quality, no matter what kind of network they're on.

If your CVM instance is to provide service over the Internet, it must have an IP address (also known as a public IP address) on the Internet in order to communicate with other services on the Internet. You can also configure a CVM instance with a public IP address on the Internet. For more information about logging into a CVM instance, refer to Logging into a Linux Instance and Logging into a Windows Instance.

Public IP address

A public IP is an IP address that can be accessed from the Internet and can be used to communicate between instances and the Internet using the public IP. The public IP is mapped to the instance's private IP through Network Address Translation (NAT). All the public network interfaces of Tencent Cloud are processed by Tencent Gateway (TGW). TGW features high reliability, high extensibility, high performance and strong anti-attack abilities; and provides more efficient and secure network access. Therefore, Tencent Cloud CVM instance public network cards are unanimously configured on the TGW interface layer, without CVM perception.

This feature allows users to view information about the network interface using commands such as 'ifconfig' on the CVM; but you can only see information that is on the Private Network. Public network information needs to be logged in by the user Tencent Cloud Console CVM list/details page to view.

Instances providing services through public network IPs need to pay the corresponding costs; for specifics, refer to Purchasing Network Bandwidth.

How to obtain a public IP address

Tencent Cloud network (public network) billing has three modes: pay-by-bandwidth, pay-by-traffic and bandwidth packages (for more information on network billing modes, you can refer to Purchasing Network Bandwidth. When users are in the Purchase and Start CVM Instance, in the Network Settings:

- Select pay-by-bandwidth, and set the bandwidth to a value greater than 0 Mbps;
- Select pay-by-traffic, and set the bandwidth upper limit to a value greater than 0 Mbps (including unlimited);
- Select bandwidth package, and set the bandwidth to a value greater than 0 Mbps;

The Tencent Cloud system will automatically assign a public IP address for the instance from the Tencent public IP pool. This address cannot be changed, and is not associated with your Tencent Cloud account.

Release of public IP address

A user cannot actively associate or unassociate a public IP address from an instance. In some cases, the Tencent Cloud system will automatically release the public network IP address, or assign a new address to the instance. The released public IP address will be returned to the public IP pool, and you will not be able to use it again.

- When an instance has been terminated (actively terminating pay-per-use instances; or teminating the instance after it has expired in monthly or yearly packages), Tencent Cloud will release its public IP address.
- If a user associates an elastic public IP with an instance, Tencent Cloud will release the public IP address of the instance. When an instance has removed associated with an elastic IP address, the instance is automatically reassigned to a new public IP address.

Because the public IP address is closely related to the instance, it might be released in the above situation; therefore, if you need a fixed permanent public IP, you can use the elastic public IP address instead. For example, if you need to remap a custom domain name to the public IP of a new instance, it might take hours to dozens of hours for the mapping to propagate over the Internet; during which time, the new instance cannot receive requests and the request is all parsed to the original instance. Elastic IPs can solve this issue, maintaining the domain name mapping relationship, and quickly

binding to a new instance. For more information, see Elastic Public IP Addresses.

Obtain public IP of instance

You can use the Tencent Cloud console and API to determine the public IP of the instance. You can also use the instance metadata to determine the public IP of an instance from within. For more information, see Instance Metadata.

Use console to obtain public IP of instance

1) Open CVM console.

2) CVM list shows the names of your instances; move the mouse over the CVM public IP, click on the copy button that appears, and copy the IP.

3) (optional) Click on the CVM Instance ID to view detailed CVM info, including Parameters , Monitoring , Health Check , Security Group , Operation log and so on.

> The public IP is mapped to the private network IP through NAT. Therefore, if you view the properties of the network interface within the instance (for example, through ifconfig (Linux) or ipconfig (Windows)), the public IP is not displayed. To determine the public IP of an instance from within an instance, you can use the instance's metadata.

Use API to obtain public IP of instance

Refer to DescribeInstances interface.

Use instance metadata to obtain public IP of instance

First, you need to login to the CVM instance. For details, refer to Logging into Linux Instance and Logging into Windows Instance.

Use the following command to obtain the public IP:

curl http://metadata.tencentyun.com/meta-data/public-ipv4

The return value has a structure similar to the following:

Elastic Network Interface (ENI)

An elastic network interface （ ENI) is a virtual network interface, you can bind the CVM with the ENI to gain access. ENI offerS great assistance in the configuration and management of a network, as well as building highly reliable network solutions.

ENIs use a private network, with a private area and subnet properties; they can only bind CVMs within the same availability zone. A CVM can bind multiple ENIs, the specific number of bindings will be based on CVM specifications.

Basic info

The ENI mainly has the following associated information:

1. Primary ENI and secondary ENI: When the CVM of the private network is created, the ENI created by the linkage is the main ENI. The ENI that the user created will be used as the secondary ENI; you cannot bind/unbind the main ENI, but can do so with the secondary one.

2. Main private network IP: ENI's primary IP; when an ENI is created. it is either randomly assigned by the system or created by the user. For a primary ENI, the primary private IP can be modified. But for a secondary ENI, the primary private IP cannot be modifed.

3. Secondary private IP: a secondary network IP that is bound, in addition to the main IP, to the ENI. It is automatically configured by the user when creating or editing an ENI, and supports binding/unbinding.

4. Elastic public network IP: binds with private IPs on the ENI one at a time.

5. Security groups: ENIs can be bound to one or more security groups.

6. MAC Address: Each ENI has a globally unique MAC address.

Restrictions on use

According to CPU and memory configurations, the number of ENIs and IPs per ENI that a CVM can bind vary greatly. Please see below:

CVM Configuration	ENIs	IPs per ENI
CPU: 1 core memory: 1G	2	2
CPU: 1 core memory: >1G	2	6
CPU: 2 cores	2	10
CPU: 4 cores memory: < 16G	4	10
CPU: 4 cores memory: > 16G	4	20
CPU: 8~12 cores	6	20
CPU: >12 cores	8	30

Operation Guide

Check ENIs

1) Open CVM console.

2) Click the CVM instance ID to access the CVM details page.

3) Click the ENI tab to view information about the elastic network adapter bound to the CVM.

Create ENIs

A primary ENI will be created automatically when you create a CVM. The primary ENI cannot be bound and unbound.

To create a new ENI, please do the followings:

1) Open CVM console.

2) Find the desired CVM via the ID

3) In the operation column, select "More - ENI - Bind ENI"

4) Select "New ENI" in the pop-up window

5) Enter data of the ENI and click "OK"

Bind elastic public IPs

Method 1:

1) Open CVM console.

2) Click the CVM instance ID to access the CVM details page.

3) Click the "ENI - Bind an ENI".
4) In the pop-up list, select ENIs in the same VPC and the same availability zone

5) Click "Confirm" to complete

Method 2:

1) Open CVM console.

2) Find the desired CVM via the ID

3) In the operation column, select "More - Elastic Network Cards-Bind Elastic Network Cards"

4) In the pop-up list, select elastic network card in the same VPC and the same availability zone

5) Click "Confirm" to complete

Tip 1: A CVM can only be bound with ENIs in the same VPC and availability zone

Tip 2: There're upper limits for bound ENIs. Please check the Usage Restriction section for details

Unbind ENIs

Method 1:

1) Open CVM console.

2) Click the CVM instance ID to access the CVM details page.

3) Click the ENI tab and select the desired ENI

4) Click "Unbind" to complete

Method 2:

1) Open CVM console.

2) Find the desired CVM via the ID

3) In the operation column, select "More - Elastic Network Cards-Unbind Elastic Network Cards"

4) Click "Confirm" to complete

Assign private IP (Tencent Cloud console)

1) Open CVM console.

2) Click the CVM [Instance ID] to access the CVM details page.

3) Click the [Elastic Network Card tab] to view the bound IP and elastic public network IP of the elastic host network card.

4) Click the [Assign Private IP] button and a "Assign Private IP" window will pop up.

5) You can select either to "Auto Assign" or "Fill in Manually" for the private IP.

6) You can click the [Add] button to assign multiple IP addresses to the elastic network card in the

"Assign Private IP" window.

7) Click the [Finish] button to use the console to assign private IPs.

Note: The private IP needs to be configured on the CVM before taking effect.

Assign private IP (CVM system)

There are two ways to configure private IPs on the CVM. Here, centos 7.2 is used as an example to demonstrate the configuration process.

Method 1

1) Log onto the CVM as an administrator.

2) Execute command

ip addr add [ip/mask] dev [ifname]

Example: the CVM's network card eth0 needs to add subnet 192.168.0.0/24 IP 192.168.0.5, then just execute the command

ip addr add 192.168.0.5/24 dev eth0

3) Private IP configuration complete.

Note: This way the configuration of the private network IP is only written on the CVM system memory; after the CVM is restarted, the private network IP will be invalid, and will need to be

reconfigured.

Method 2

1) Log onto the CVM as an administrator.

2) Execute below command

cd /etc/sysconfig/network-scripts/

ls

3) On the list, find the network card name; using Tencent Cloud centos 7.2 CVM as an example, you need to bind the network card's private IP with the name "ifcfg-eth0"; then you can execute the command "vim" to open the network card configuration file.

vim ifcfg-eth0

The original system configuration file is:

DEVICE='eth0'

MM_CONTROLLED='yes'

ONBOOT='yes'

IPADDR='192.168.0.3'

NETMASK='255.255.255.0'

GATEWAY='192.168.0.1'

Modified to:

DEVICE='eth0'

MM_CONTROLLED='yes'

ONBOOT='yes'

IPADDR0='192.168.0.3'

IPADDR1='192.168.0.5'

NETMASK='255.255.255.0'

GATEWAY='192.168.0.1'

Save the configuration file after modifying and exit vim.

4) Restart network card

systemctl restart network

Check whether the eth0 card has joined the IP address

ip addr

5) Complete private network IP binding.

Note: The private network IP configured in this way will still take effect after the CVM restarts. However, if you make a custom mirror for this CVM, the other private IPs created by this image will need to be updated.

Release private IP

1) Open CVM console.

2) Click the CVM [Instance ID] to access the CVM details page.

3) Click the [Elastic Network Card tab] to view the bound IP and elastic public network IP of the elastic host network card.

4) Click the [Release] button on the bar next to the private IP.

5) Click [OK] to complete the action.

Note 1: The elastic network card's primary IP does not support release, only the secondary IP supports release.

Note 2: After the private IP is unbound, it will automatically disassociate from the elastic public network IP.

Bind EIP

1) Open CVM console.

2) Click the CVM [Instance ID] to access the CVM details page.

3) Click the [Elastic Network Card tab] to view the private IP that is already bound to the cloud host's elastic network card.

4) Click the [Bind] button on the already bound elastic public network IP list, on the same line where the private IP is.

5) In the pop-up window, select to bind an IP from the [Existing Elastic IPs] list or [Create New Elastic IP].

6) Click the [OK] button, to complete binding with elastic IP.

Unbind EIP

1) Open CVM console.

2) Click the CVM [Instance ID] to access the CVM details page.

3) Click the [Elastic Network Card tab] to view the bound IP and elastic public network IP of the elastic host network card.

4) Click the [Unbind] button on the already bound elastic public network IP list, on the same line where the private IP is.

5) Click the [OK] button, to complete unbinding with elastic public IP.

Change primary private IP

1) Open CVM console.

2) Click the CVM [Instance ID] to access the CVM details page.

3) Click the [Elastic Network Card tab] to view the main private IP of the cloud host elastic network

card.

4) Click the [Modify Main IP] button that is in the list next to the main private IP.

5) In the pop-up window, enter the new main network IP, and click [OK] to complete the modification.

Change subnet of ENI

1) Open Private network VPC console.

2) Click [Elastic Network Card] in the left column to enter the Elastic Network Card List page.

3) Click the elastic network card's [Instance ID] to enter the Elastic Network Card Details page.

4) On the Basic Information page of the Elastic Network Card Details page, click the [Replace] button for the subnet.

5) In the pop-up window, select the subnet to be replaced and specify the new primary IP.

6) Click the [Save] button to complete the subnet replacement of the elastic network card.

Note:

1. You can only change subnet of the primary network card
2. Before changing the subnet of an elastic network card, unbind all secondary IPs.
3. When modifying the subnet of an elastic network card, you can only change it to other subnets under the availability zone.