Cloud Virtual Machine

FAQ

Product Introduction

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

FAQ

- About Instance
  - Login and Remote Access
  - Adjust Configuration
  - Reinstall System
  - About D1 Instances
  - Others
- Network and Security
  - Network
  - Password Login and SSH Key Login
  - IP Address
  - Elastic Public IP
  - Elastic Network Interface
  - Port and Security Groups
  - Firewall

About Access Control

FAQ

About Instance

Login and Remote Access

Last updated：2018-08-06 10:39:43

How do I log in to a CVM?

See the following documents:

- Logging in to a Linux Instance
- Logging in to a Windows Instance

How do I set the initial password?

When purchasing a CVM, you can set a custom password or use the password automatically generated by the system.

Setting a custom password

1. When you create an instance, select the login method in the section for setting instance name and login method. It is **Set Password** by default.

2. Enter a password as required by the password character limits and confirm it. Confirm the configuration information, and then click **Buy Now**. After the CVM instance is assigned successfully, log in to the instance using the password you set.

Auto-generated password

You can also select **Auto Generated Password** and then click **Buy Now**. After the CVM instance is assigned successfully, you can obtain the initial password in Internal Message.

> **Note:**
> The character limits for password:
>
> - Linux CVM: The password should be a combination of 8-16 characters comprised of at least two of the following types: `` a-z, A-Z, 0-9 and ( ) ` ~ ! @ # $ % ^ & * - + = _ | { } [ ] : ; ' < > , . ? / `` .
> - Windows CVM: The password should be a combination of 12-16 characters comprised of at least three of the following types: `` a-z, A-Z, 0-9 and ( ) ` ~ ! @ # $ % ^ & * - + = _ | { } [ ] : ; ' < > , . ? / ``.

How do I reset the password? What to do if I fail to reset the password?

Resetting password

> **Note:**
>
> You can only reset the password if the CVM is in a shutdown status. If the CVM is running, shut down the CVM first.

1. Log in to the CVM Console.
2. Reset the password. For an instance whose password cannot be reset, the reason why the password cannot be reset will be displayed.
   i. For a single instance that has been shut down, click **More** -> **Reset Password** in the **Operation** column in the right.
   ii. For multiple instances that have been shut down in batch, select all the CVMs whose passwords are to be reset, and then click **Reset Password** at the top of list to modify the login passwords in batch.
3. Enter and confirm the new password, enter the verification code in the **Reset Password** pop-up window, and then click **Confirm Reset**.
4. After the reset is successful, you will receive an internal message indicating the successful reset. Then you can start the CVM using the new password.

Failure to reset password

If you cannot reset password even if you're sure that your instance has been shut down, submit a ticket to contact us.

When the Linux instance is associated with an SSH key, I failed to log in to the instance with user name and password - What should I do?

After the CVM is associated with an SSH key, login by user name and password is **disabled by default** for the SSH service. Use the SSH key instead to log in to the CVM.

Please see Logging in to a Linux Instance

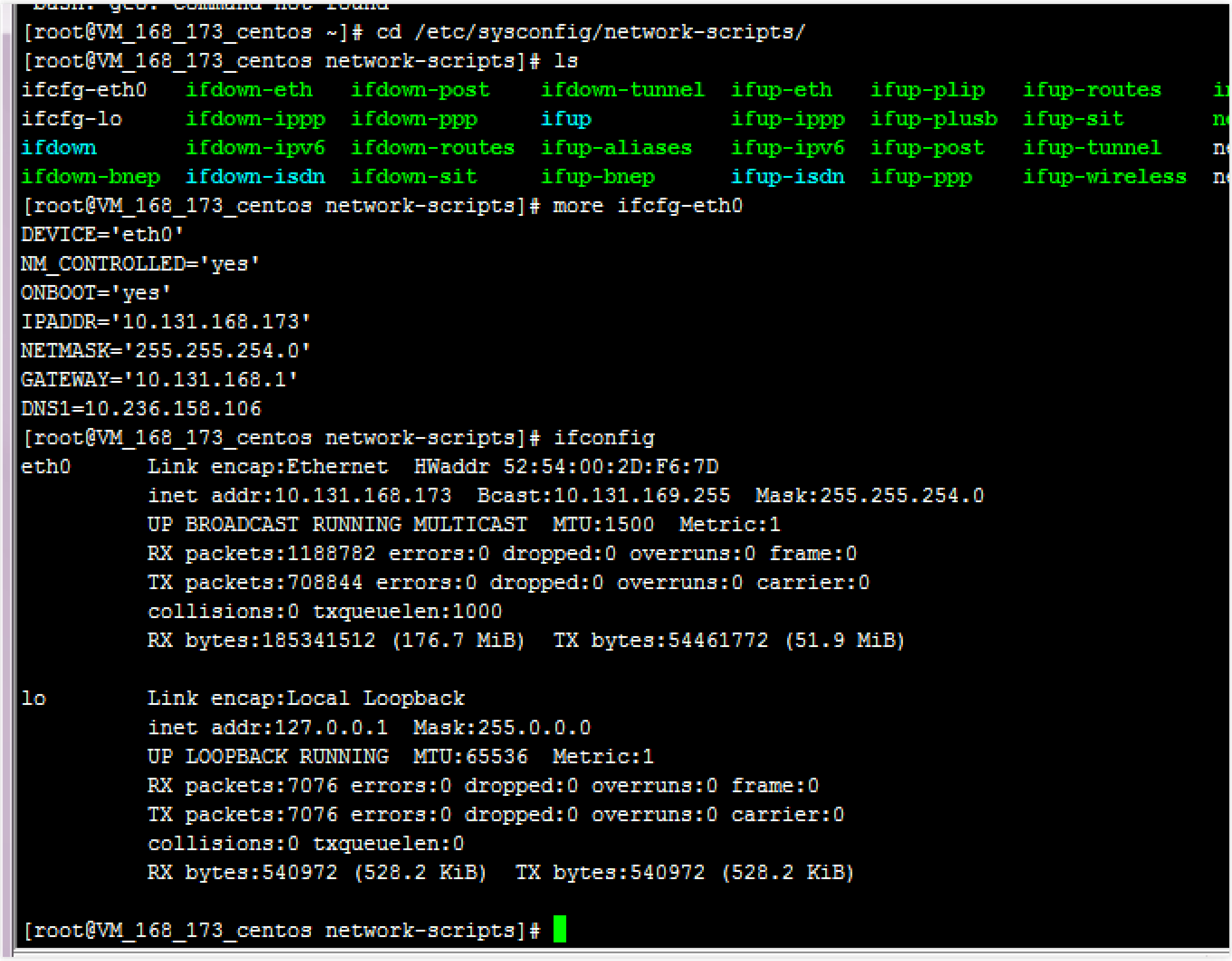
What to do if I failed to log in to a Linux instance with an SSH key?

The solutions are as follows:

1. Cancel or modify the security group policy on the Console. See Security Group Operation Guide

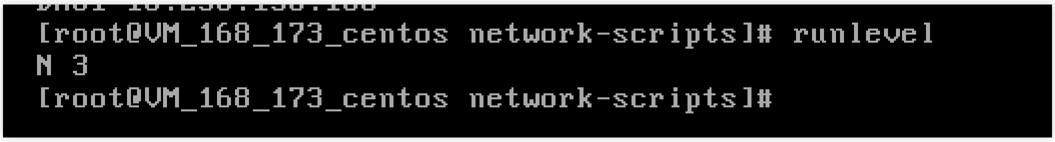
2. Cancel "login by key" on the Console or set "login through key authentication" as instructed. See SSH Key Operation Guide

3. Log in to the instance via VNC to check whether the ENI status and IP configuration information are correct. See Logging in to a Linux Instance



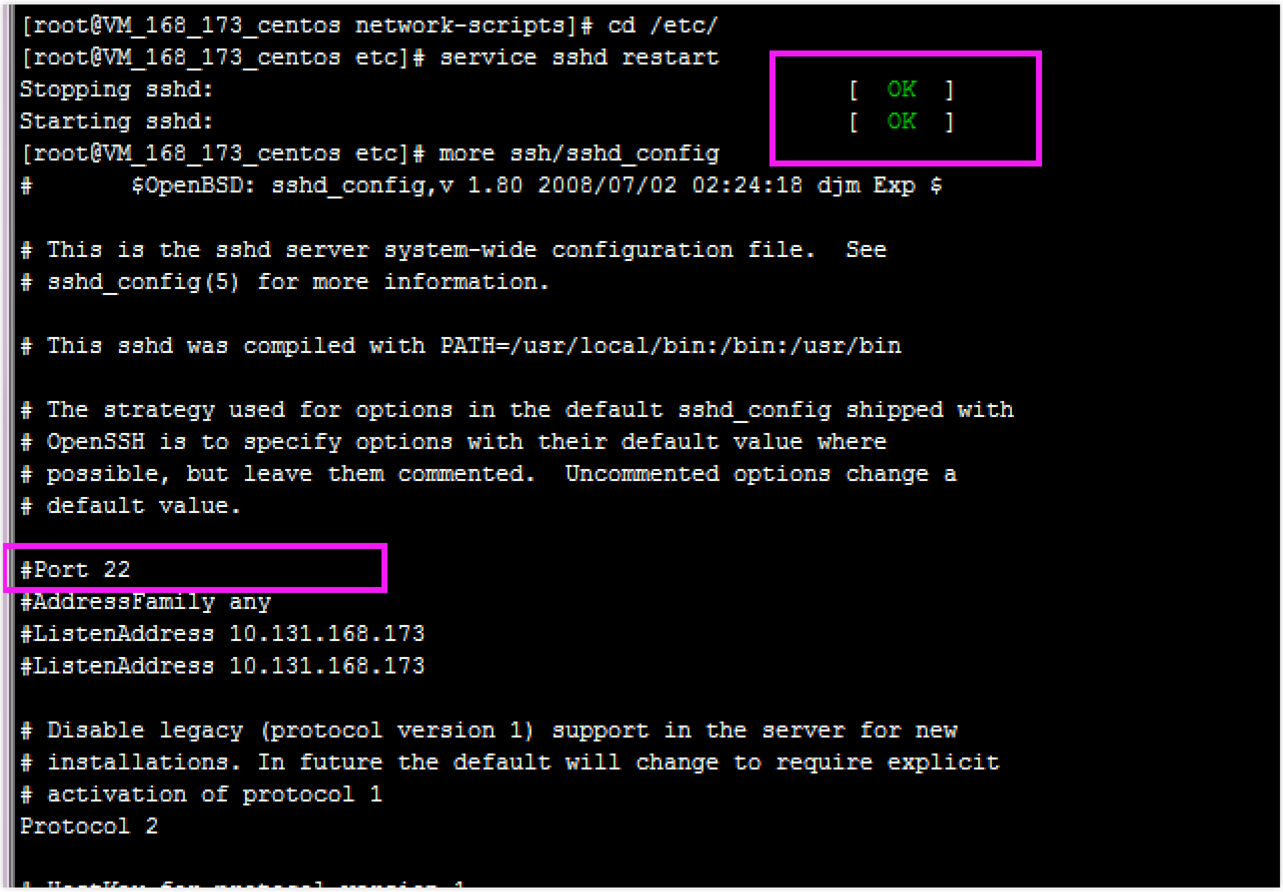
```
bash: gcc: command not found
[root@VM_168_173_centos ~]# cd /etc/sysconfig/network-scripts/
[root@VM_168_173_centos network-scripts]# ls
ifcfg-eth0    ifdown-eth    ifdown-post    ifdown-tunnel  ifup-eth   ifup-plip   ifup-routes    i
ifcfg-lo      ifdown-ippp   ifdown-ppp     ifup           ifup-ippp  ifup-plusb  ifup-sit       n
ifdown        ifdown-ipv6   ifdown-routes  ifup-aliases   ifup-ipv6  ifup-post   ifup-tunnel    n
ifdown-bnep   ifdown-isdn   ifdown-sit     ifup-bnep      ifup-isdn  ifup-ppp    ifup-wireless  n
[root@VM_168_173_centos network-scripts]# more ifcfg-eth0
DEVICE='eth0'
NM_CONTROLLED='yes'
ONBOOT='yes'
IPADDR='10.131.168.173'
NETMASK='255.255.254.0'
GATEWAY='10.131.168.1'
DNS1=10.236.158.106
[root@VM_168_173_centos network-scripts]# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:2D:F6:7D
          inet addr:10.131.168.173  Bcast:10.131.169.255  Mask:255.255.254.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1188782 errors:0 dropped:0 overruns:0 frame:0
          TX packets:708844 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:185341512 (176.7 MiB)  TX bytes:54461772 (51.9 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:7076 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7076 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:540972 (528.2 KiB)  TX bytes:540972 (528.2 KiB)

[root@VM_168_173_centos network-scripts]#
```

4. Verify whether the instance is running normally in Mode 3 or Mode 5:



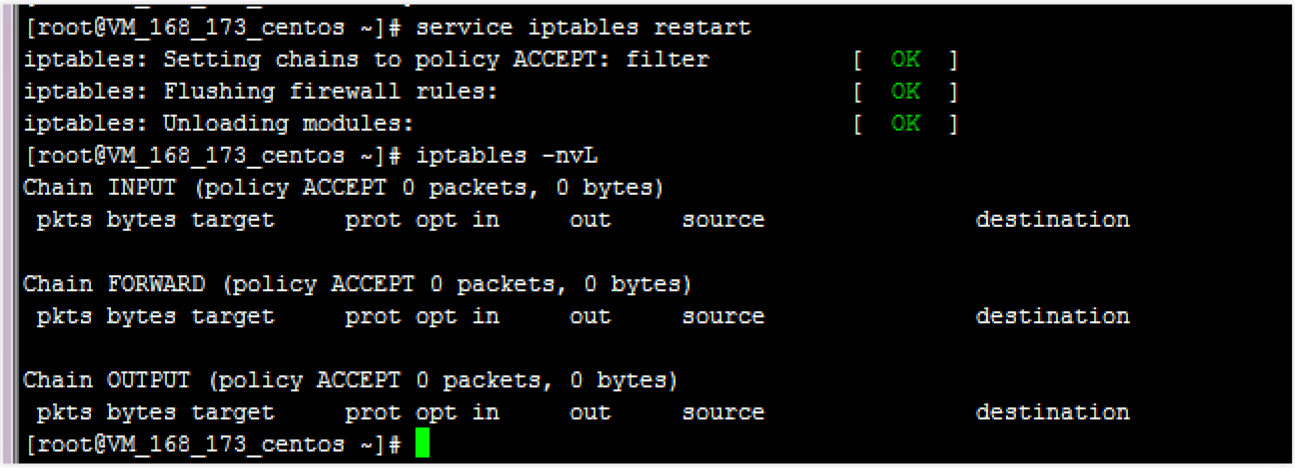
```
DNS1=10.236.158.106
[root@VM_168_173_centos network-scripts]# runlevel
N 3
[root@VM_168_173_centos network-scripts]#
```

5. Verify whether the sshd service of the server is running normally and there is no problem with the configuration such as port.



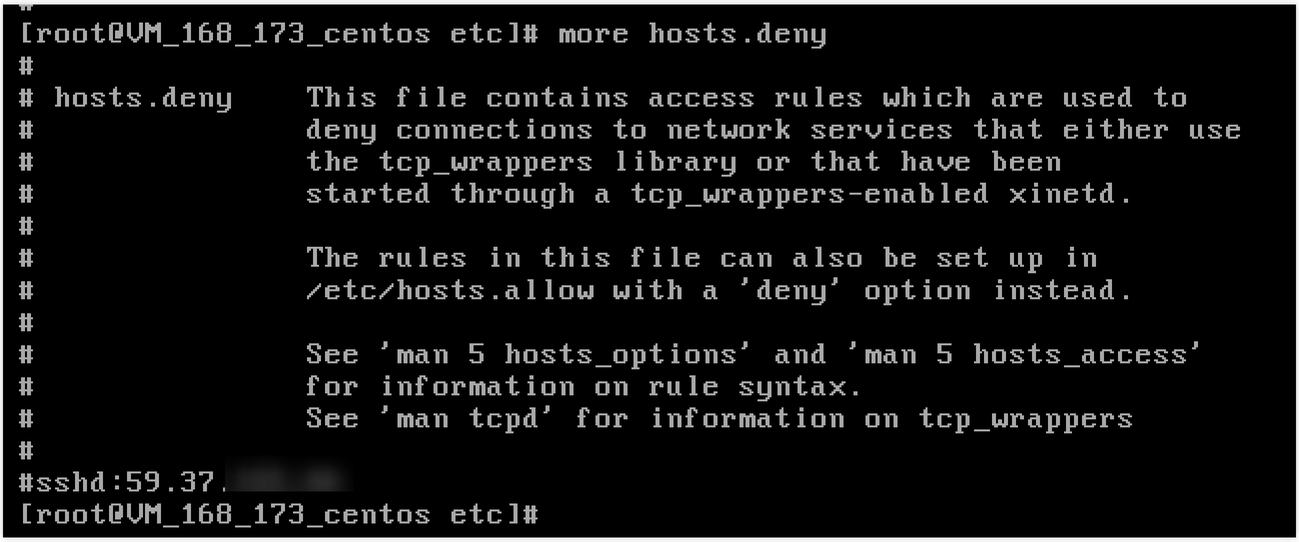
```
[root@VM_168_173_centos network-scripts]# cd /etc/
[root@VM_168_173_centos etc]# service sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
[root@VM_168_173_centos etc]# more ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.80 2008/07/02 02:24:18 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
#AddressFamily any
#ListenAddress 10.131.168.173
#ListenAddress 10.131.168.173

# Disable legacy (protocol version 1) support in the server for new
# installations. In future the default will change to require explicit
# activation of protocol 1
Protocol 2

# HostKey for protocol version 1
```

6. Verify whether the server's iptables firewall has blocked the access and whether its policy is OK.



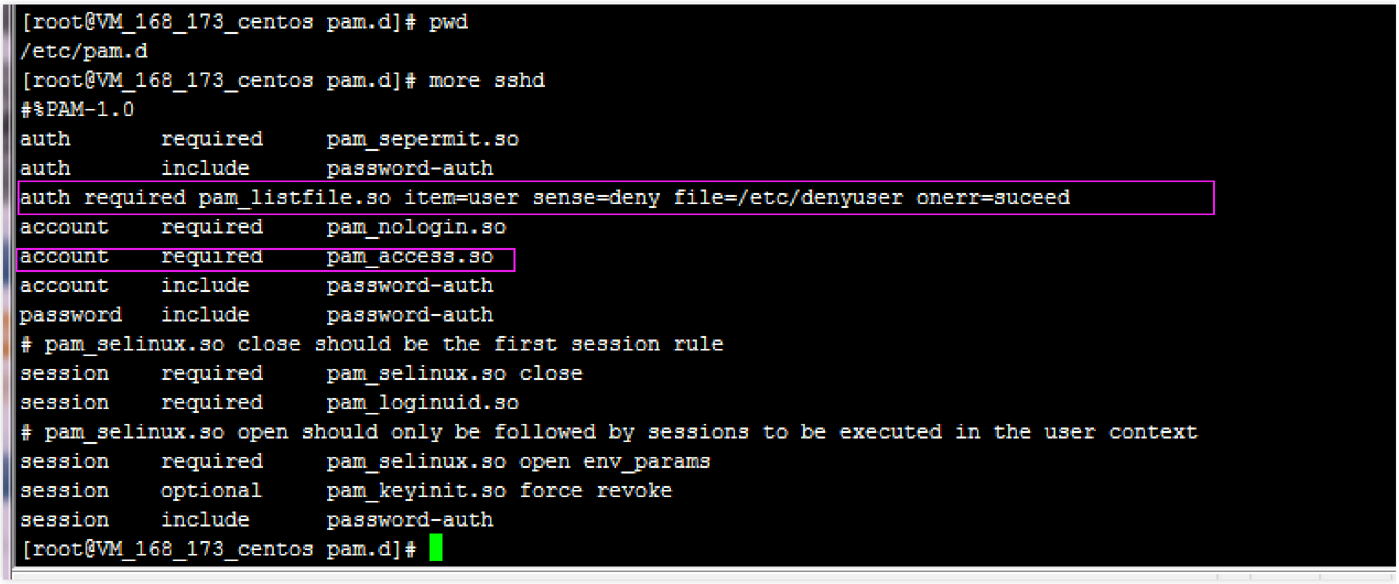
```
[root@VM_168_173_centos ~]# service iptables restart
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Unloading modules:                               [  OK  ]
[root@VM_168_173_centos ~]# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
[root@VM_168_173_centos ~]#
```

7. Verify whether the tcp_wrappers of the server has blocked SSH access.



```
[root@VM_168_173_centos etc]# more hosts.deny
#
# hosts.deny     This file contains access rules which are used to
#                deny connections to network services that either use
#                the tcp_wrappers library or that have been
#                started through a tcp_wrappers-enabled xinetd.
#
#                The rules in this file can also be set up in
#                /etc/hosts.allow with a 'deny' option instead.
#
#                See 'man 5 hosts_options' and 'man 5 hosts_access'
#                for information on rule syntax.
#                See 'man tcpd' for information on tcp_wrappers
#
#sshd:59.37.[redacted]
[root@VM_168_173_centos etc]#
```

8. Verify whether the user who wants to log in to the server via SSH is blocked by the PAM module (this is a rare case):



```
[root@VM_168_173_centos pam.d]# pwd
/etc/pam.d
[root@VM_168_173_centos pam.d]# more sshd
#%PAM-1.0
auth       required     pam_sepermit.so
auth       include      password-auth
auth required pam_listfile.so item=user sense=deny file=/etc/denyuser onerr=suceed
account    required     pam_nologin.so
account    required     pam_access.so
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
session    required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open env_params
session    optional     pam_keyinit.so force revoke
session    include      password-auth
[root@VM_168_173_centos pam.d]#
```

How do I log in to a CVM via VNC?

Login via VNC is a method Tencent Cloud provides for you to connect to your CVMs through Web browser. If the remote login client is not installed or cannot be used, you can connect to your CVM from VNC to check the CVM status and perform basic CVM management operations with your CVM account. For more information, please see the following documents:

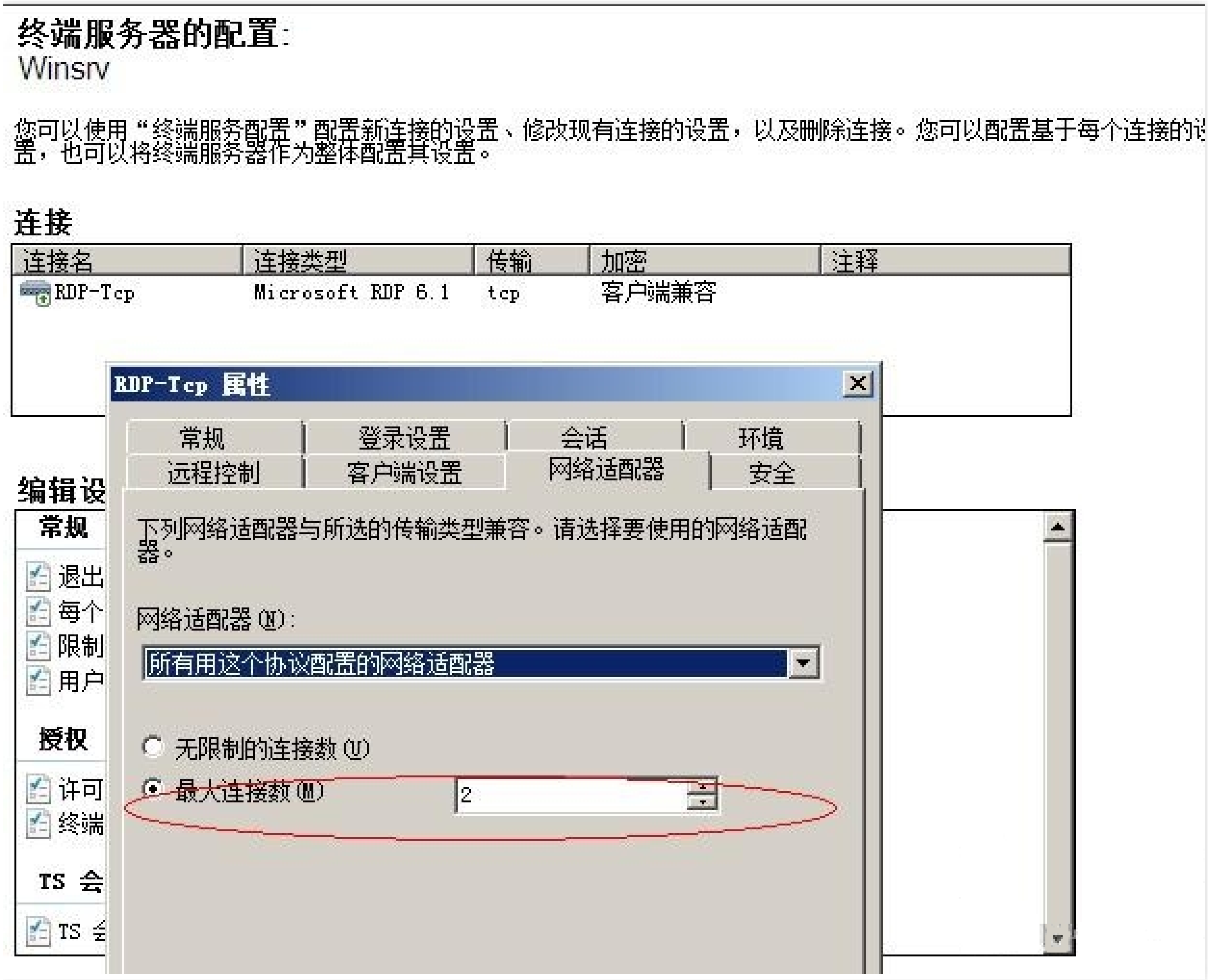
- Logging in to a Linux Instance

- Logging in to a Windows Instance

How do I configure multi-user remote login for a Windows server?

A Windows server supports remote login by multiple users at a time. Follow the steps below:

1. Click **Control Panel** -> **Management Tools** -> **Terminal Services** -> **Terminal Service Configuration**
2. Right-click the RDP-Tcp connection, and then click **Attribute** -> **Network Adapter** -> **Max Connections**
3. By default, if you do not add the terminal service feature, the maximum number of connections can only be adjusted to 2. Set terminal server authorization mode: Go to **Attribute** -> **General**, **unselect** Restrict Each User to Only One Session. Then multi-user login is enabled. If the setting does not take effect, restart the server and try again.



终端服务器的配置:
Winsrv

您可以使用"终端服务配置"配置新连接的设置、修改现有连接的设置，以及删除连接。您可以配置基于每个连接的设置，也可以将终端服务器作为整体配置其设置。

连接

连接名	连接类型	传输	加密	注释
RDP-Tcp	Microsoft RDP 6.1	tcp	客户端兼容	

RDP-Tcp 属性

下列网络适配器与所选的传输类型兼容。请选择要使用的网络适配器。

网络适配器(N): 所有用这个协议配置的网络适配器

○ 无限制的连接数(U)
● 最大连接数(M) 2

How can I log in to a Windows instance using Remote Desktop Connector from a local Windows PC?

See Logging in to a Windows Instance.

How can I log in to a Windows instance using rdesktop from a local Linux PC?

See Logging in to a Windows Instance.

How can I log in to a Windows instance using Microsoft Remote Desktop Connection Client for Mac from a local Mac OS PC?

See Logging in to a Windows Instance.

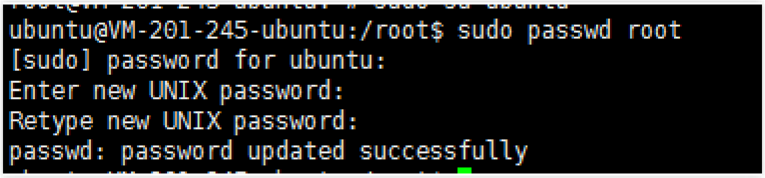
How can I log in to an instance using root user from a Ubuntu system?

The default user name for Ubuntu system is ubuntu, and the root account and password are not set by default during the installation. If necessary, enable "login with root user" in Settings. Follow the steps below:

1. Modify root password. Enter the following command and enter the password.

```
sudo passwd root
```

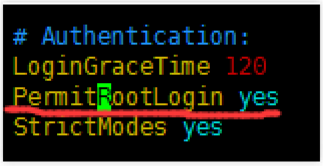
   Root user has no password by default, so it is unavailable. To use the root user, set a password for the root user first.



```
ubuntu@VM-201-245-ubuntu:/root$ sudo passwd root
[sudo] password for ubuntu:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

2. Modify SSH configuration. Change PermitRootLogin to yes, and then save and exit.

```
sudo vi /etc/ssh/sshd_config
```



```
# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
```

   i. Restart SSH service.

```
sudo service ssh restart
```

3. Finally, verify whether you can log in remotely using the root user.

How do I reset passwords for multiple online Linux instances in batch?

To reset passwords for multiple Linux instances in batch without shutting down the instances, click to download the script for batch reset and run the script. The script is used as follows:

> **Note:**
>
> - If you run the script on a public network-based server, the IP entered in the hosts.txt file must be the public IP of the instance.
> - If you run the script on a private network-based server, enter the private IP of the instance.

Enter the IP of the instance to be operated, SSH port, account, and old and new passwords in the hosts.txt file. Each line represents a server, for example:

```
10.0.0.1 22 root old_passwd new_passwd
10.0.0.2 22 root old_passwd new_passwd
```

Run the following code:

```
./batch-chpasswd.py
```

Response Example:

```
change password for root@10.0.0.1
spawn ssh root@10.0.0.1 -p 22
root's password:
Authentication successful.
Last login: Tue Nov 17 20:22:25 2017 from 10.181.225.39
[root@VM_18_18_centos ~]# echo root:root | chpasswd
[root@VM_18_18_centos ~]# exit
logout

change password for root@10.0.0.2
spawn ssh root@10.0.0.2 -p 22
root's password:
Authentication successful.
Last login: Mon Nov 9 15:19:22 2017 from 10.181.225.39
```

```
[root@VM_19_150_centos ~]# echo root:root | chpasswd
[root@VM_19_150_centos ~]# exit
logout
```

Adjust Configuration

Last updated：2018-08-14 17:11:49

How do I upgrade/degrade the configuration of a CVM?

Only the instances **whose system disk and data disk are both cloud disks** support adjusting configuration.

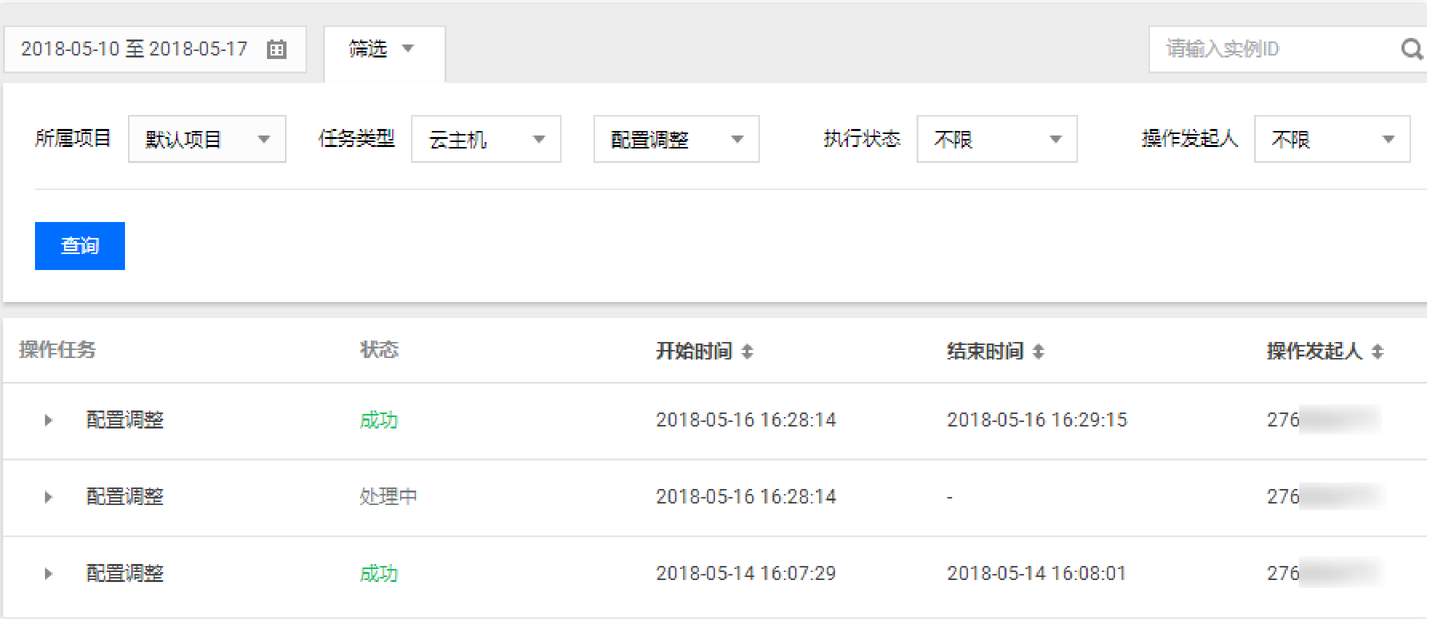
For more information about how to upgrade/degrade instance configuration, please see Adjusting Instance Configuration.

For more information about how to adjust bandwidth/network configuration, please see Adjusting Network Configuration.

If your configuration adjustment does not take effect, submit a ticket to contact us.

How do I check the records of configuration adjustments?

The records of configuration adjustments can be found in the operation log in the upper right corner of the Console. For a prepaid instance, an order will be generated in the income & expense statement each time the instance is upgraded or degraded.



2018-05-10 至 2018-05-17

所属项目 默认项目 任务类型 云主机 配置调整 执行状态 不限 操作发起人 不限

操作任务	状态	开始时间	结束时间	操作发起人
配置调整	成功	2018-05-16 16:28:14	2018-05-16 16:29:15	276[redacted]
配置调整	处理中	2018-05-16 16:28:14	-	276[redacted]
配置调整	成功	2018-05-14 16:07:29	2018-05-14 16:08:01	276[redacted]

Can bandwidth be adjusted when the CVM is renewed in Recycle Bin?

No. Adjustment to bandwidth configuration can only be made after the instance is successfully renewed in Recycle Bin.

Does a postpaid instance support adjusting configuration?

The instances whose data disk and system disk are both cloud disks support adjusting configuration. The configuration of a postpaid instance can be upgraded or degraded for unlimited times; the configuration of a prepaid instance can be upgraded for unlimited times, but can **only be degraded once**.

How many times can the configuration of a CVM be degraded at most?

Each instance can only be degraded once.

Will the usage period of a prepaid instance be extended after the instance is degraded?

It may not be extended. This depends on whether the remaining amount of your actual payment at the time of purchase after the deduction of fees for the used resources is greater than the amount to be paid for the degraded configuration. If so, the usage period is extended, otherwise it remains unchanged.

Example:

An instance with a configuration of "Standard, 2-core, 4-GB local disk, without bandwidth" is priced at 102 CNY/month. You purchased the instance for a usage period of one year with a 400 CNY voucher at a discount of 83% off. When the instance has been used for 2 months, its configuration is degraded to "Standard, 1-Core, 2-GB local disk, without bandwidth", which is priced at 51 CNY/month.
Discounted price: 102 * 12 * 0.83 = 1015.92 CNY
Actual paid amount: 1015.92 - 400 = 615.92 CNY
Remaining amount after deduction of fees for used resources: 615.92 - 102 * 2 = 411.92 CNY
The amount to be paid for the degraded instance (1-core CPU, 2-GB local disk) for a usage period of 10 months is 51 * 10 = 510 CNY
Conclusion: Because 411.92 < 510, the usage period remains unchanged.

> The above prices are only used as examples, and are not actual prices listed on the official website.

Reinstall System

Last updated：2018-08-06 10:41:40

Do CVMs support reinstalling the operating system?

Reinstalling operating system can restore an instance to its initial state when it was just started, and is an important way of recovery in case of system failure of instance. For more information, please see Reinstalling Operating System.

How long does it take to reinstall the operating system for an instance?

Generally, it takes 10 to 30 minutes to complete the re-installation after you perform the operation.

What to do in case of a slow or failed re-installation?

Generally, it takes 10 to 30 minutes to complete the re-installation after you perform the operation.

- If the re-installation is not completed after a long time but the 30 minutes have not run out, please wait.
- If the re-installation is not completed within the 30 minutes or even fails, submit a ticket to contact us.

Will re-installation of operating system cause data loss?

After the re-installation, all data on the server's system disk will be cleared and the system disk is restored to the initial state; the data on the server's data disk will not be lost, but can only be used after the data disk is mounted manually.

About D1 Instances

Last updated：2018-08-06 10:21:44

What is Big Data D1 instance?

Big Data D1 instances are CVM instances designed exclusively for Hadoop distributed computing, massive log processing, distributed file systems, large data warehouses and other business scenarios. This instance type is mainly used to deal with cloud computing and storage of massive business data in the age of big data.

Which industry customers and business scenarios are Big Data D1 instances applicable to?

Big Data D1 instances are applicable to customers in the Internet, game, finance and other industries who require big data computing and storage analysis, as well as business scenarios where massive data storage and offline computing is performed. They can fully satisfy the requirements of distributed computing businesses represented by Hadoop for the storage performance, capacity and private network bandwidth of instances.
In addition, combining the highly available architecture design of distributed computing businesses represented by Hadoop, Big Data D1 instances adopt a local storage design to achieve a total cost of ownership close to that of offline IDC self-built Hadoop clusters based on massive storage space and high storage performance.

Features of Big Data D1 instances

- The throughput of a single instance can reach up to 2.3 GB/sec. A throughput-intensive HDD local disk is optimal for throughput-intensive storage. Big Data D1 instances are designed exclusively for Hadoop distributed computing, massive log processing, large data warehouses and other business scenarios, providing stable and high sequential read/write throughput performance.
- Local storage has a unit price as low as 1/10. Big Data D1 instances have the best cost performance in big data scenarios, and can achieve a total cost of ownership close to that of IDC self-built Hadoop clusters based on massive storage space and high storage performance.
- Read/write time delay is minimized to 2-5 ms. Big Data D1 instances, as high-performance enterprise-level models, are defined for matured enterprise developers.

- Both prepaid and postpaid billing methods are available for Big Data D1 instances, with a price as low as 4.17 CNY/hour.

Specifications of Big Data D1 instances

Model	vCPU (core)	Memory (GB)	Local Data Disk	Private Network Bandwidth	Note
D1.2XLARGE32	8	32	2 × 3,720 GB	1.5 Gbps	-
D1.4XLARGE64	16	64	4× 3,720 GB	3 Gbps	-
D1.6XLARGE96	24	96	6× 3,720 GB	4.5 Gbps	-
D1.8XLARGE128	32	128	8× 3,720 GB	6 Gbps	-
D1.14XLARGE224	56	224	12× 3720 GB	10 Gbps	Exclusive for hosts

Notes on local data storage for Big Data D1 instances

Big Data D1 instances use local disks as data disks, which may lead to **a risk of data loss** (in case of host crash). If your application does not have a data reliability architecture, you are strongly recommended to choose instances with cloud disks used as data disks.

Operations on an instance coming with local disks and the data retention relationship are shown below.

Operation	Status of Local Disk Data	Description
Restart operating system/Restart instance using console/Forced restart	Retained	Local disk storage is retained. Data is retained.
Shut down operating system/Shut down instance via the console/Forced shutdown	Retained	Local disk storage is retained. Data is retained.

Operation	Status of Local Disk Data	Description
Terminate (instance) on the console	Erased	Local disk storage is erased. No data is retained.

Note:
Do not store business data that needs to be kept for a long time on a local disk. Back up data in time and use a highly available architecture. For long-term retention, it is recommended to store the data on a cloud disk.

How can I purchase Big Data D1 local disks?

Local disks cannot be purchased separately. You can only purchase local disks when creating a D1 instance. The number and capacity of local disks depend on the specifications of the instance you selected.

Does the local storage of Big Data D1 instances support snapshots?

No.

Do Big Data D1 instances support configuration upgrading/downgrading and failover?

Configuration adjustment is not supported.

Big Data D1 instances are massive data storage-based instances using local HDD as data disk. This instance type does not support failover of data disk (in case of host crash or local disk damage). To prevent data loss, you are recommended to use a redundancy policy, for example, a file system that supports redundancy and fault tolerance (such as HDFS, Mapr-FS). In addition, you're also advised to back up data to a more persistent storage system periodically, such as Tencent COS. For more information, please see Cloud Object Storage.

After a local disk is damaged, you need to shut down the CVM instance before we can change the local disk. If the CVM instance has crashed, we will inform you and make repairs.

In which regions can I purchase Big Data D1 instances?

The following availability zones are supported:

- Shanghai Zone 2
- Beijing Zone 2
- Guangzhou Zone 3

More regions and availability zones will be available soon.

Why can't I find the data disks after purchasing a Big Data D1 instance?

The local disks of a Big Data D1 instance are not mounted automatically. You can mount them as needed.

What is the difference between Big Data D1 instances and High IO I2 instances?

High IO I2 instances are CVM instances designed exclusively for business scenarios with low latency and high random IO, featuring ultra high IOPS performance. They are generally used for high-performance databases (relational database, NoSQL). Big Data D1 instances are CVM instances designed exclusively for business scenarios of high sequential read/write, low-cost massive data storage, featuring ultra high storage cost performance and properly configured private network bandwidth.

How is the disk throughput performance of Big Data D1 instances?

Take D1.14XLARGE224 as an example, the sequential read/write throughput performance of the local disks of Big Data D1 instances is described as below:

- For a single disk, the sequential read/write speed is 190+ MB/sec (128 KB of block size and depth of 32).

- For 12 disks, the concurrent sequential read/write speed is 2.3+ GB/sec (128 KB of block size and depth of 32).

What is the difference between the local disk of Big Data D1 instances and CBS?

Cloud Block Storage (CBS) provides a highly efficient and reliable storage device for CVM instances. As a customizable block storage device featured by high availability, high reliability and low cost, it can be used as a scalable standalone disk for CVMs. It provides data storage at data block level and employs a 3-copy distributed mechanism to ensure the data reliability for CVM, thus meeting the requirements of various application scenarios. The local disk of Big Data D1 instances is designed exclusively for business scenarios where high sequential read/write performance is required for local massive data sets, such as Hadoop distributed computing, large-scale concurrent computing, data warehouses.

Others

Last updated：2018-08-06 10:20:02

How do I view the CVMs in use?

Log in to the CVM Console to view the CVMs in use on the CVM page.

How do I use CVMs?

For more information on how to use CVMs, please see the following documents or videos:

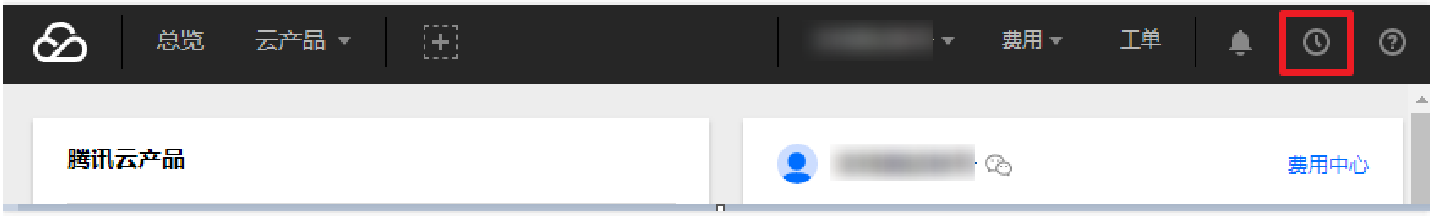
- How to Use Linux CVMs
- How to Use Windows CVMs

Can a VM be installed on a CVM?

No.

How do I view the operation logs of a CVM?

You can view the operation logs of a CVM in the upper right corner of the Console.



What to do if I can't see my CVM on the console?

If you find that your CVM does not exist on the console, verifying the following:

1. Check the Recycle Bin to verify whether the instance has expired.
2. Verify whether the instance has been terminated because it has expired for more than 7 days.
3. Verify whether you have selected a wrong project.

If none of the above applies, submit a ticket to contact us.

How do I shut down an instance?

Please see Shutting Down an Instance.

How do I restart an instance?

Please see Restarting an Instance.

What to do if I fail to connect (log in) to an instance after restarting it?

This may be caused by the over-high load of your server's CPU/memory. Please see the following documents:

- High CPU Utilization (Linux System)
- High CPU Utilization (Windows System)

How do I terminate an instance?

Please see Terminating an Instance.

Network and Security
Network

Last updated：2018-08-06 11:07:42

After logging in to CVM, there is no network connection. How to troubleshoot the problem?

This may be caused by incorrect configuration of your server security group. Check the inbound and outbound rules of the server security group. Check whether your destination, protocol ports and policies are prohibited.

Can a VPC instance interconnect with the basic network instance?

Supported, but the following restrictions apply:

The VPC IP address range (CIDR) must be `10.0.0.0/16 - 10.0.47.0/16` (including subsets). Otherwise conflicts will occur.

Procedure

Log in to VPC Console, click VPC ID/name to go to the VPC details page, and then associate the basic network CVMs to be interconnected in **Classiclink**.

How to view the basic network CVMs interconnected with the VPC?

Log in to VPC Console, click VPC ID/name to go to the VPC details page, and you can view basic network CVMs interconnected with the VPC CVM in **Classiclink**.

Can the CVM be switched to overseas network?

The network cannot be changed for CVM after purchase. If you need an overseas network, you are recommended to return the CVM and re-purchase an overseas CVM.

How to configure private network DNS?

Please see the **Private Network DNS** section of Private Network Service.

Within the same IP address range, the local VPN can obtain the IP of the IP address range but cannot access the Internet. How to solve this problem?

Check if the following configurations are correct:

1. Are the manually added IP and the automatically obtained IP in the same IP subnet? Are the subnet masks the same? Is the default gateway configured? Is the default gateway address correct?
2. Is DNS configured and is the DNS address correct?

3. If none of the above is wrong, check if there is conflict of statically configured IP address.

If none of the above methods works, submit a ticket to contact us.

Password Login and SSH Key Login

Last updated：2018-07-17 15:24:32

What is the difference between SSH key login and password login?

An SSH key is a way to remotely log into a Linux server by using a key generator to make a pair of keys (public and private). The public key is added to the server, and then the user can use the private key to complete the authentication and login. This method pays more attention to the security of the data, and is different from the manual input of the traditional password login mode, and has higher convenience. Currently, Linux instance supports both password and SSH key login, however Windows instance supports only password login. Related documentation:

- Login to Linux instance
- Log in to Windows instance

If I use SSH key login and password login at the same time?

No. When you log in to the Linux instance using the SSH key pair, the password login is disabled to improve security.

What should I do if I forgot my password?

You can log in to the CVM console, reset the password, and then log in to the instance with the new password. For details on how to reset your password, see Login Password Operation Guide.

How do I create an SSH key, and what shall I do if I lose it?

For the creation of the key, please see SSH Key. In case you lose your key, we provide two ways to solve it. :

- Create a new key through the CVM console and bind the original instance with the new one. For details, please refer to SSH Key. Once you have created a new key, you can log in to the instance with the new key on the CVM Console > CVMs > Load Key.
- Reset your password through the CVM console and log in to the instance with your new password. See Login Password Operation Guide for details.

How do I bind/unbind an SSH key to a server?

Please refer to **Binding/Unbinding Key with Server** section in SSH Key Operation Guide.

How do I modify the SSH key name/description?

Please refer to the **Modify the SSH Key Name/Description** section in SSH Key Operation Guide

How do I delete an SSH key?

Please refer to the **Delete SSH Key** section in SSH Key Operation Guide .

What are the usage restrictions for SSH keys?

Please refer to the **Usage Limits** section in Introduction to SSH Keys .

I can't log in to the Linux instance using SSH key

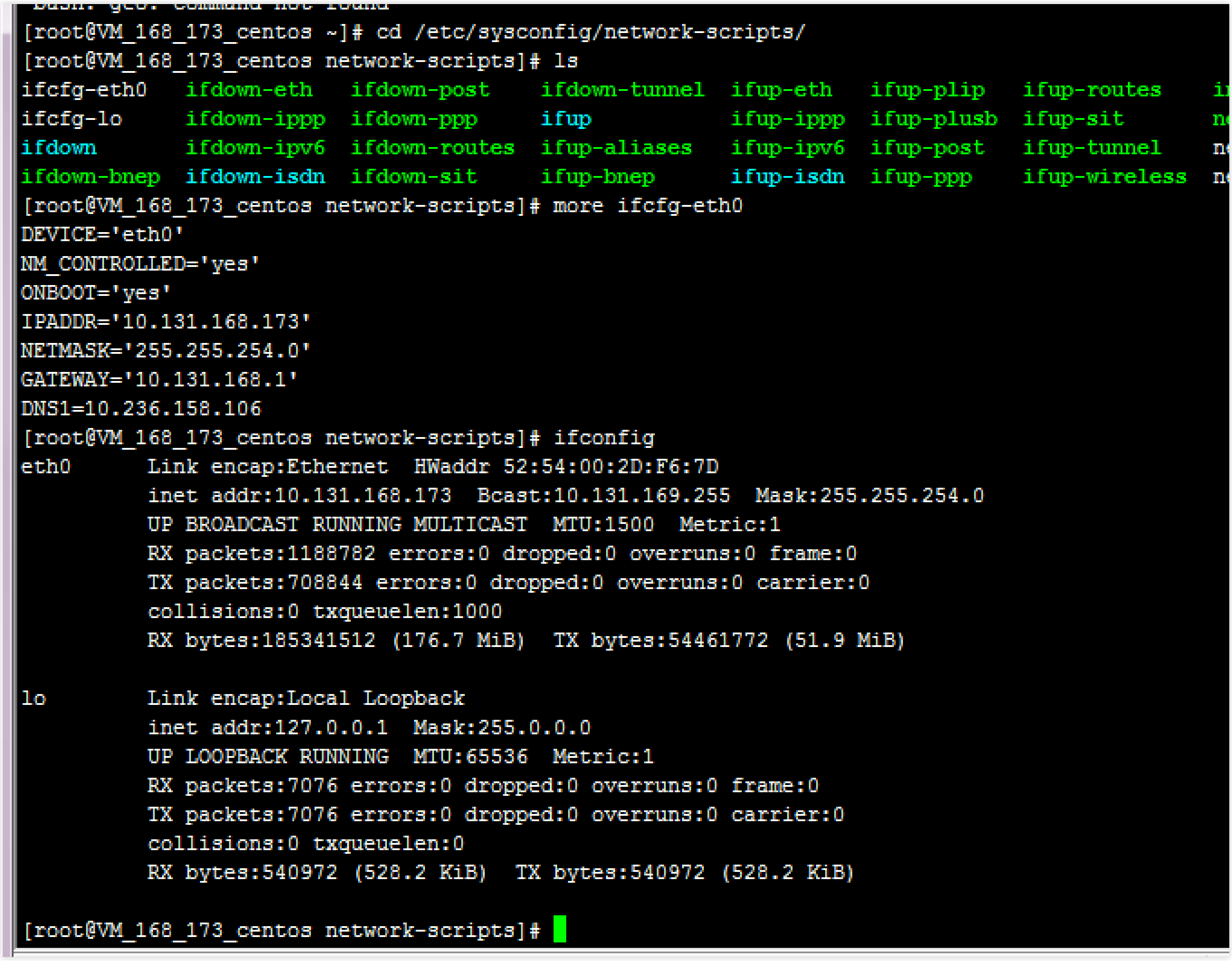
You can refer to the following solutions:

1. In CVM Console, enter the key name to find and key ID, click the ID to see CVMs bound with this key.

2. Cancel or modify the security group policy in Console. See Safety Group Operation Guide

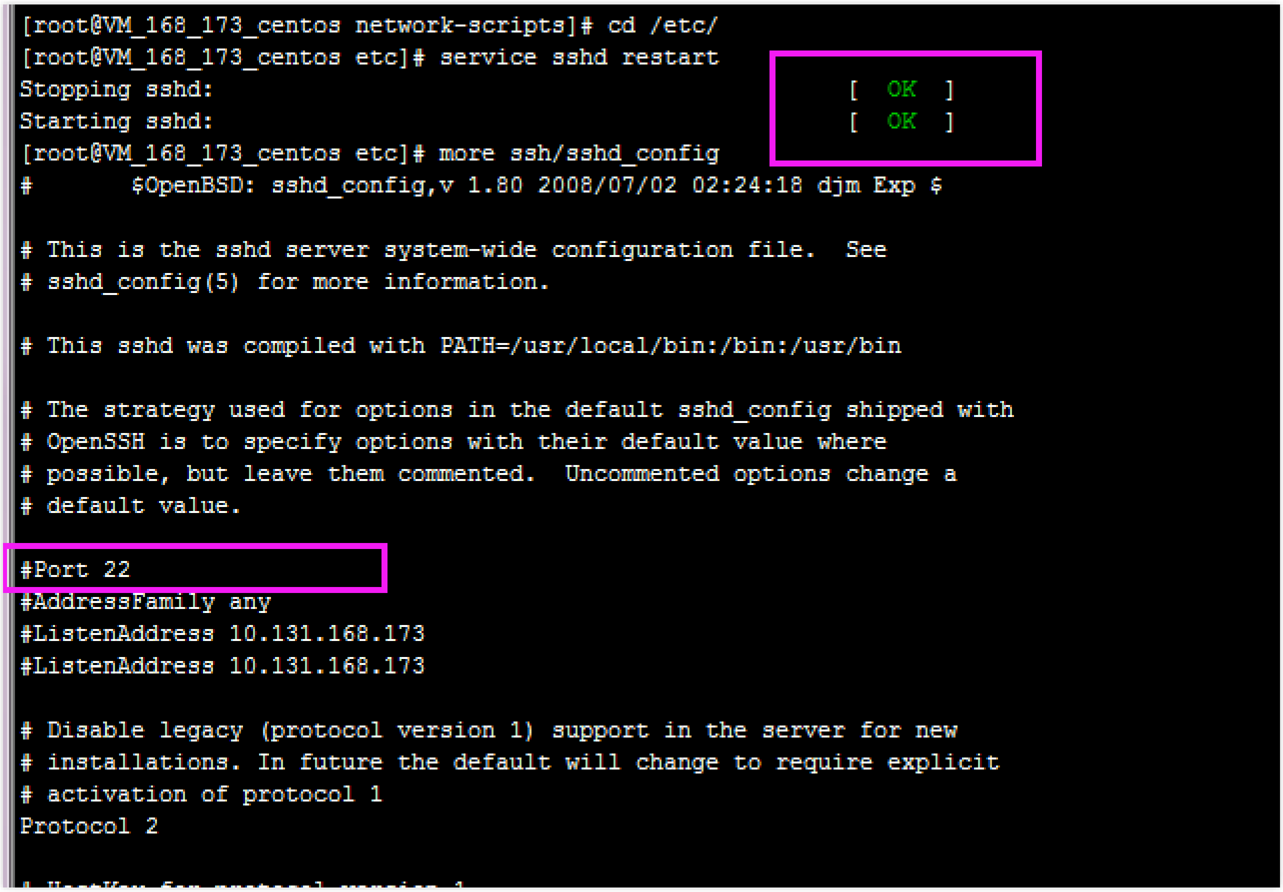
3. In the Console, cancel the key login method, or follow the instructions to correctly set the key to log in to the server. See SSH Key Operation Guide

4. Use VNC to log in to the instance to check whether the NIC status and IP configuration information are correct. See Login Linux Instance Operation Guide



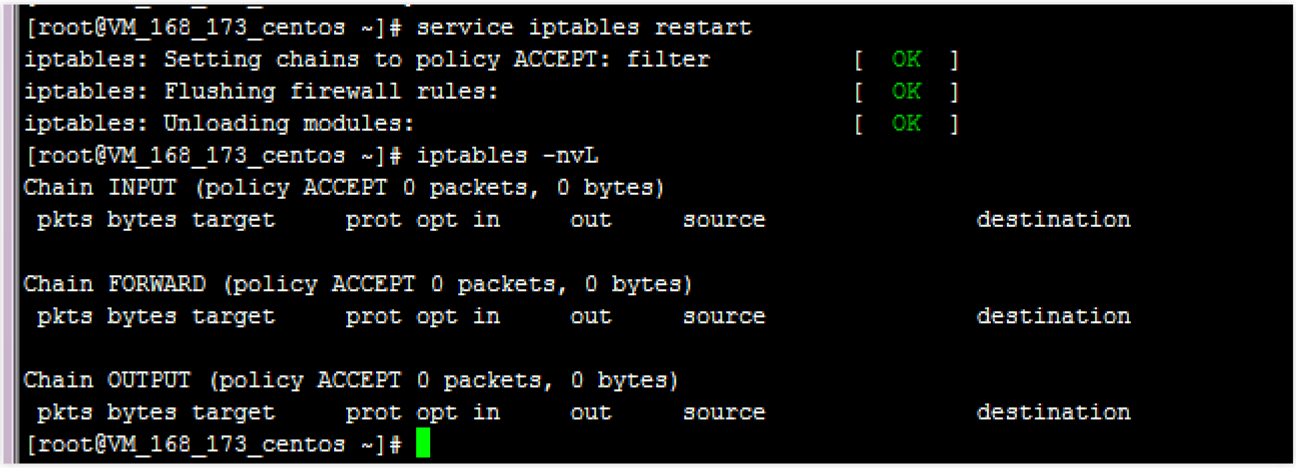
```
bash: geo: command not found
[root@VM_168_173_centos ~]# cd /etc/sysconfig/network-scripts/
[root@VM_168_173_centos network-scripts]# ls
ifcfg-eth0   ifdown-eth   ifdown-post    ifdown-tunnel  ifup-eth   ifup-plip   ifup-routes    i
ifcfg-lo     ifdown-ippp  ifdown-ppp     ifup           ifup-ippp  ifup-plusb  ifup-sit       n
ifdown       ifdown-ipv6  ifdown-routes  ifup-aliases   ifup-ipv6  ifup-post   ifup-tunnel    n
ifdown-bnep  ifdown-isdn  ifdown-sit     ifup-bnep      ifup-isdn  ifup-ppp    ifup-wireless  n
[root@VM_168_173_centos network-scripts]# more ifcfg-eth0
DEVICE='eth0'
NM_CONTROLLED='yes'
ONBOOT='yes'
IPADDR='10.131.168.173'
NETMASK='255.255.254.0'
GATEWAY='10.131.168.1'
DNS1=10.236.158.106
[root@VM_168_173_centos network-scripts]# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:2D:F6:7D
          inet addr:10.131.168.173  Bcast:10.131.169.255  Mask:255.255.254.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1188782 errors:0 dropped:0 overruns:0 frame:0
          TX packets:708844 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:185341512 (176.7 MiB)  TX bytes:54461772 (51.9 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:7076 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7076 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:540972 (528.2 KiB)  TX bytes:540972 (528.2 KiB)

[root@VM_168_173_centos network-scripts]#
```

5. Check if the server's SSHD service is running properly and that there are no problems with the configuration files such as ports.



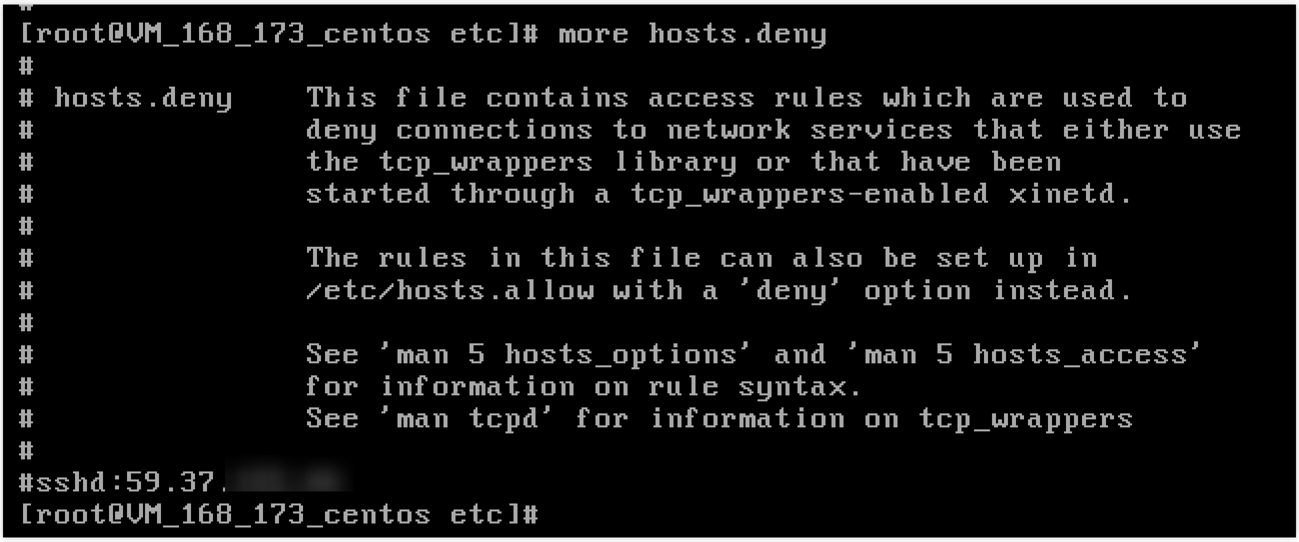
```
[root@VM_168_173_centos network-scripts]# cd /etc/
[root@VM_168_173_centos etc]# service sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
[root@VM_168_173_centos etc]# more ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.80 2008/07/02 02:24:18 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
#AddressFamily any
#ListenAddress 10.131.168.173
#ListenAddress 10.131.168.173

# Disable legacy (protocol version 1) support in the server for new
# installations. In future the default will change to require explicit
# activation of protocol 1
Protocol 2

# HostKey for protocol version 1
```

6. Check if the server's iptables firewall is intercepted and check if its policy is OK.



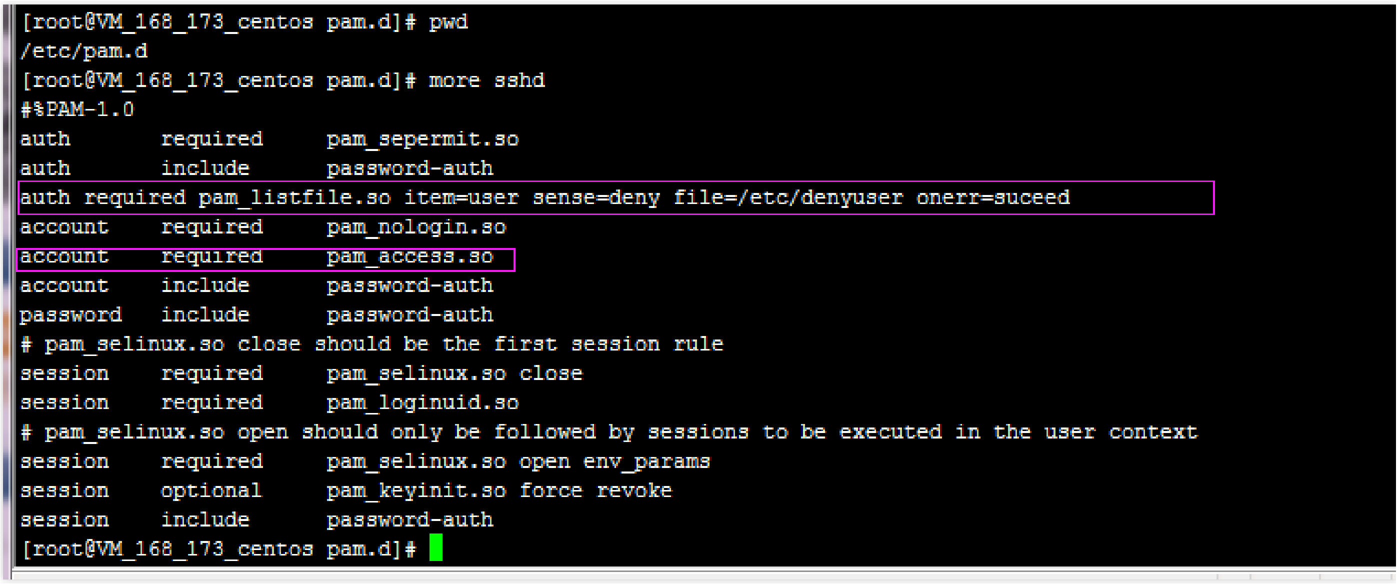
```
[root@VM_168_173_centos ~]# service iptables restart
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Unloading modules:                               [  OK  ]
[root@VM_168_173_centos ~]# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
[root@VM_168_173_centos ~]#
```

7. Check if the server's tcp_wrappers has interception control for SSH access.



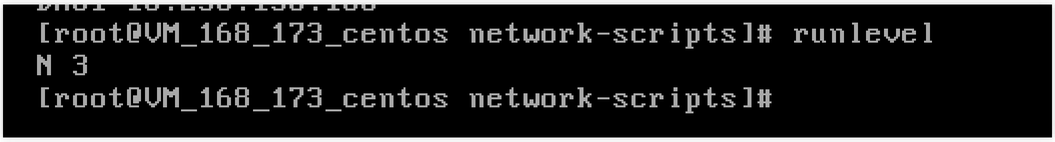
```
[root@VM_168_173_centos etc]# more hosts.deny
#
# hosts.deny    This file contains access rules which are used to
#               deny connections to network services that either use
#               the tcp_wrappers library or that have been
#               started through a tcp_wrappers-enabled xinetd.
#
#               The rules in this file can also be set up in
#               /etc/hosts.allow with a 'deny' option instead.
#
#               See 'man 5 hosts_options' and 'man 5 hosts_access'
#               for information on rule syntax.
#               See 'man tcpd' for information on tcp_wrappers
#
#sshd:59.37.[redacted]
[root@VM_168_173_centos etc]#
```

8. Confirm if the user of the SSH login server is blocked by the PAM module



```
[root@VM_168_173_centos pam.d]# pwd
/etc/pam.d
[root@VM_168_173_centos pam.d]# more sshd
#%PAM-1.0
auth       required     pam_sepermit.so
auth       include      password-auth
auth required pam_listfile.so item=user sense=deny file=/etc/denyuser onerr=suceed
account    required     pam_nologin.so
account    required     pam_access.so
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
session    required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open env_params
session    optional     pam_keyinit.so force revoke
session    include      password-auth
[root@VM_168_173_centos pam.d]#
```

9. Check if the instance is operating correctly in Mode 3 or Mode 5:



```
[root@VM_168_173_centos network-scripts]# runlevel
N 3
[root@VM_168_173_centos network-scripts]#
```

IP Address

Last updated：2018-08-06 10:40:58

What is public IP address?

Please see the **Public IP Address** section in Public Network Service.

What is private IP address?

Please see the **Private IP Address** section in Private Network Service.

How do I obtain the public IP address of an instance?

Please see the section about **obtaining public IP address of an instance** in Public Network Service.

How do I obtain the private IP address of an instance?

Please see the section about **obtaining private IP address of an instance** in Private Network Service.

How do I change the public IP of an instance?

Please see Changing Public IP of an Instance.

What is the difference between public gateways and CVMs with public IPs?

Public gateways support public network traffic routing and forwarding in images, while CVMs with public IPs do not support traffic forwarding by default. A CVM using a Windows public image cannot be used as a public gateway, because traffic forwarding is not enabled in the Windows image.

Elastic Public IP

Last updated：2018-08-06 10:56:05

What are EIPs used for?

EIPs apply to the following scenarios:

1. Disaster recovery. We strongly recommend that you use EIPs for disaster recovery. For example, when one of your servers fails to provide services, you can unbind the EIP from this server and rebind it to a healthy server to resume service quickly.
2. Retain specific public IP. If you need to retain a specific public IP under your account, you can convert it to an EIP, which then can be used to access public network after being bound/unbound. This EIP is retained under your account until it is "released" by you.
3. Other special scenarios When you need to change an IP in other special cases, you can convert the ordinary public IP to an EIP and then bind/unbind the EIP. With limited EIP resources available, a quota is imposed on the number of EIPs for each region under a single account. Therefore, reasonable planning and use of EIPs are very important.

How is EIP billed?

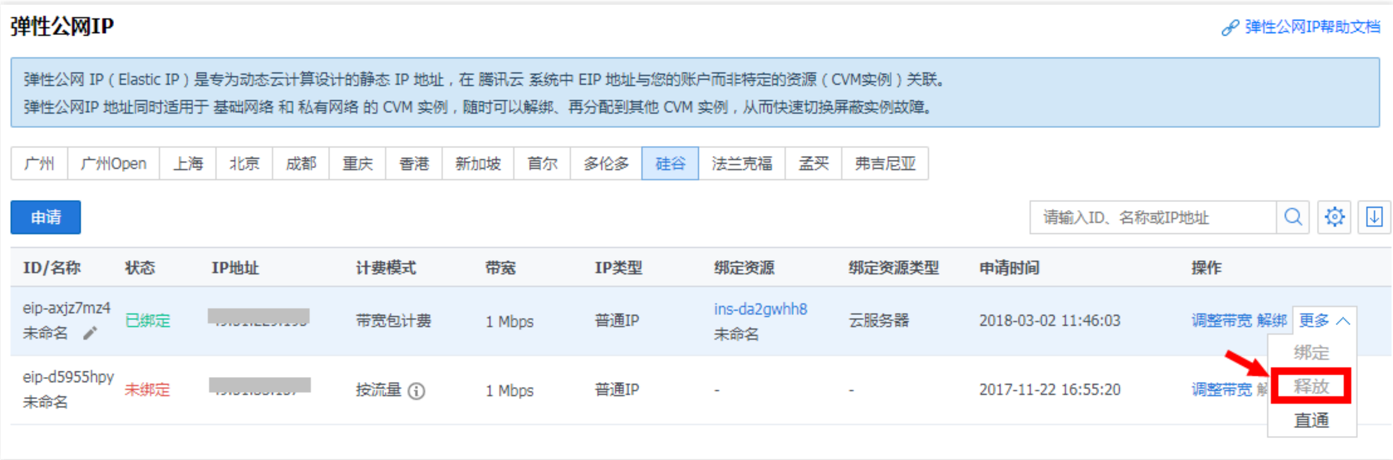
1. The fee displayed on the console applies to the EIPs that remain vacant for one hour. EIPs can be billed with an accuracy down to seconds. EIPs that have been bound/unbound many times are billed based on the total duration (in sec) for which they remain unbound.
2. The EIPs that remain unbound for less than 1 hour are billed on a pro rata basis.

When is an EIP billed?

You can apply for, bind, unbind and release EIPs. With limited EIP resources available, an EIP is only billed for a small usage fee when it is unbound.

How do I stop the billing of an EIP?

- When you no longer need an EIP, you can release it to stop the billing. Go to the EIP Console, click **More** -> **Release** in the Operation list, and then click **OK**. The released EIP will no longer be charged.



弹性公网IP

弹性公网IP帮助文档

弹性公网 IP（Elastic IP）是专为动态云计算设计的静态 IP 地址，在 腾讯云 系统中 EIP 地址与您的账户而非特定的资源（CVM实例）关联。
弹性公网IP 地址同时适用于 基础网络 和 私有网络 的 CVM 实例，随时可以解绑、再分配到其他 CVM 实例，从而快速切换屏蔽实例故障。

ID/名称	状态	IP地址	计费模式	带宽	IP类型	绑定资源	绑定资源类型	申请时间	操作
eip-axjz7mz4 未命名	已绑定	[redacted]	带宽包计费	1 Mbps	普通IP	ins-da2gwhh8 未命名	云服务器	2018-03-02 11:46:03	调整带宽 解绑 更多
eip-d5955hpy 未命名	未绑定	[redacted]	按流量	1 Mbps	普通IP	-	-	2017-11-22 16:55:20	调整带宽 解

- If you need to retain an EIP but want to stop the billing for it, bind it to a device (CVM, NAT). An EIP in a bound status is not charged.

How can a CVM without public IP access public network?

If you did not purchase the public IP when you purchased a CVM or have returned the public IP, you can apply for an EIP on the EIP Console and bind it to your CVM to allow the access to public network.

Can I change my public IP?

You can change the public IP of an instance by binding and unbinding an EIP. For more information, please see Changing Instance's Public IP.

How to I keep a public IP unchanged?

If you need to retain a specific public IP under your account, you can convert it to an EIP, which is then used to access public network after being bound/unbound. This EIP will be retained under your account until it is **released** by you.

For more information, please see EIP Operation Guide.

Can an EIP be converted back to a public IP?

An EIP cannot be converted back to a public IP.

Can an EIP be recovered?

An EIP cannot be recovered once being released.

Elastic Network Interface

Last updated：2018-08-06 11:00:41

What is ENI?

Elastic Network Interface (ENI) is an elastic network interface bound to CVMs in a VPC, which can be migrated freely among multiple CVMs. It is very useful for configuring management networks and establishing highly reliable network solutions.

ENIs are VPC, availability zone and subnet-specific, and can only be bound to the CVMs in the same availability zone. A CVM can be bound with multiple ENIs. The maximum number of ENIs allowed to be bound to a CVM depends on the CVM's specification.

What are the restrictions for the use of ENIs on CVMs?

Please see ENI Limits section in the "Overview of Use Limits".

What is the basic information of an ENI?

Please see **Concepts** section in ENI Overview.

How do I create an ENI?

Please see Creating an ENI section in the "ENI Operation Guide".

How do I view the ENI information?

Please see Viewing ENI Information section in the "ENI Operation Guide".

How do I bind an ENI to a CVM instance?

Please see Binding and Configuring ENI section in the "ENI Operation Guide".

How do I configure an ENI in the CVM instance?

Please see Binding and Configuring ENI section in the "ENI Operation Guide".

How do I modify or customize the private IP of an ENI?

VPC-based CVMs support modifying and customizing the private IP of an ENI. Follow the steps below:

1. Log in to the VPC Console.
2. Click **ENI** in the left panel to go to the ENI list page.
3. Click the **ID/Name** of an ENI to go to its details page to view its information.
4. Click **IP Management** to go to the details page.
5. Click **Assign Private IP**, select **Manually Enter** for IP assignment mode, and then enter the modified IP.

6. Click **OK** to complete the operation.

After the modification is made on the console, you also need to modify the configuration file of the ENI. For more information, please see Binding and Configuring ENI section in the "ENI Operation Guide".

Port and Security Groups

Last updated：2018-08-06 11:02:16

Port

What ports need to be opened to Internet before instance login?

You need to open the corresponding port for the security group bound with the instance. For the detailed procedures, please see Configuration in Typical Scenarios.

Which are common CVM ports?

Please see Common Server Ports.

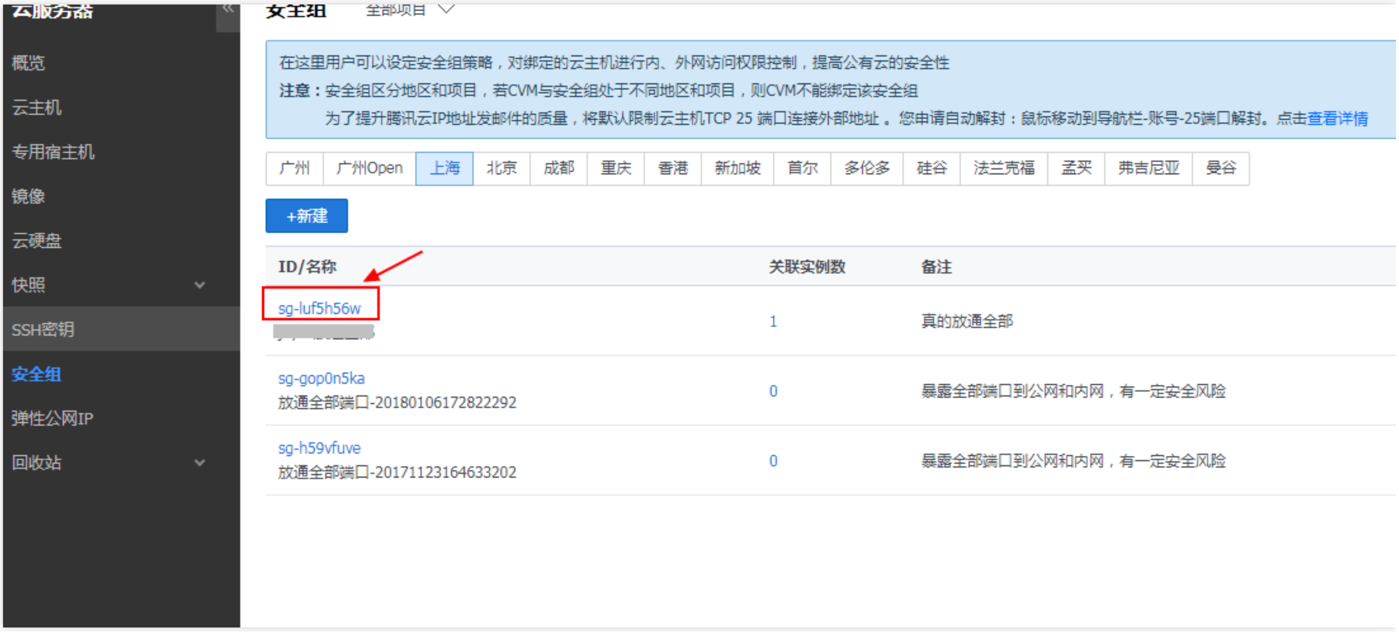
Why do you need to open the port? How to open a port?

You need to open the port in the security group before using services corresponding to the port. Example:

If you want to access web pages using port 8080, the port must be opened to Internet in the security group.

Open a port to Internet

1. Log in to the security group console, and click the security group bound with the instance to enter the details page



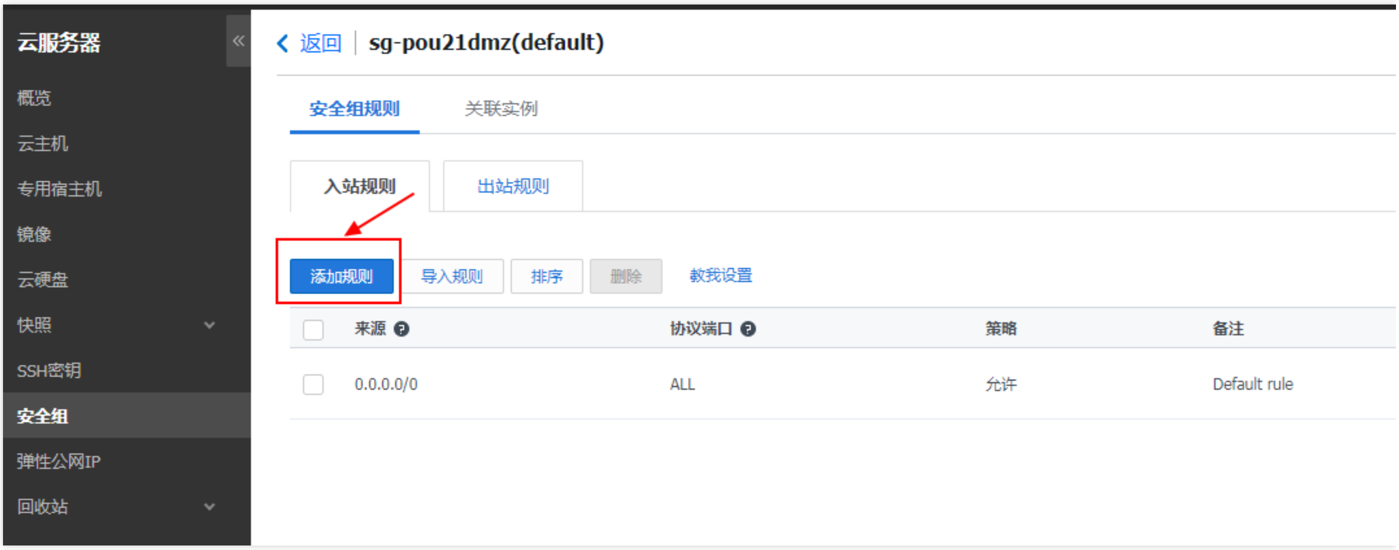
在这里用户可以设定安全组策略，对绑定的云主机进行内、外网访问权限控制，提高公有云的安全性

注意：安全组区分地区和项目，若CVM与安全组处于不同地区和项目，则CVM不能绑定该安全组

为了提升腾讯云IP地址发邮件的质量，将默认限制云主机TCP 25 端口连接外部地址 。您申请自动解封：鼠标移动到导航栏-账号-25端口解封。点击查看详情

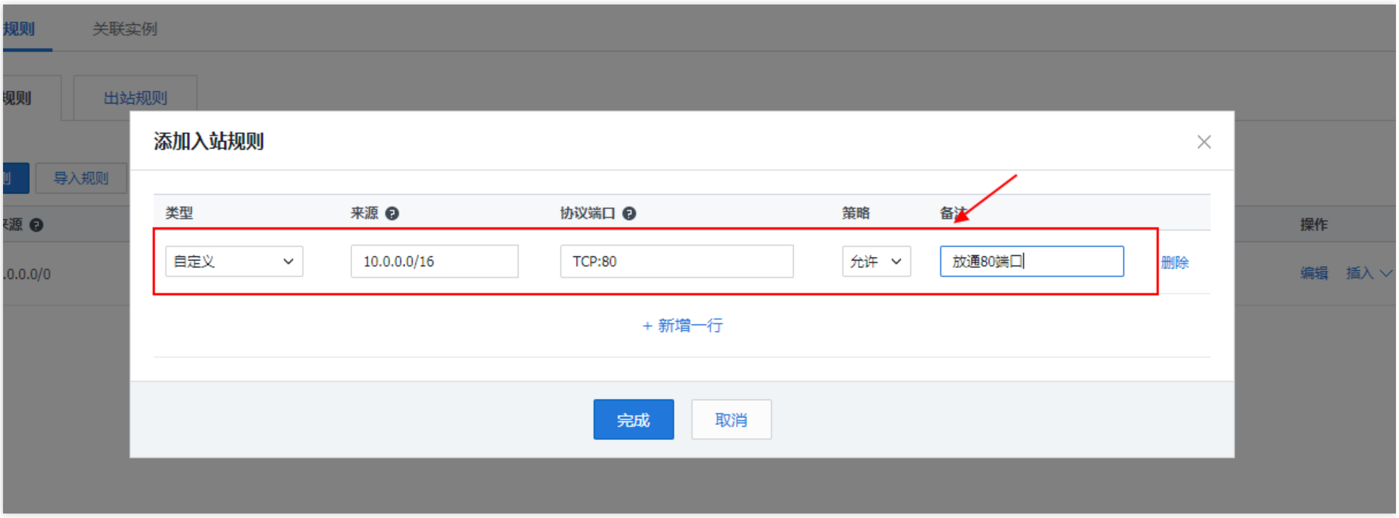
ID/名称	关联实例数	备注
sg-luf5h56w [redacted]	1	真的放通全部
sg-gop0n5ka 放通全部端口-20180106172822292	0	暴露全部端口到公网和内网，有一定安全风险
sg-h59vfuve 放通全部端口-20171123164633202	0	暴露全部端口到公网和内网，有一定安全风险

2. Select "Inbound/Outbound Rules" and click **Add Rule**



来源	协议端口	策略	备注
0.0.0.0/0	ALL	允许	Default rule

3. You can refer to the following template to enter your IP address (range) and port to be opened, and then select "Allow" to open the port



类型	来源	协议端口	策略	备注
自定义	10.0.0.0/16	TCP:80	允许	放通80端口

For detailed operation guide, please click Common Security Group Operations

Why cannot the service be used after the port is modified?

After modifying the service port, you also need to open the corresponding port in the corresponding security group. Otherwise, the service cannot be used.

Which ports are not supported by Tencent Cloud?

There are security risks with the following ports. For security reasons, ISPs block them and make them inaccessible. It is recommended that you replace the port. Do not use the following ports for listening:

Protocol	Unsupported Ports
TCP	42 135 137 138 139 445 593 1025 1434 1068 3127 3128 3129 3130 4444 5554 9996
UDP	1026 1027 1434 1068 5554 9996 1028 1433 135 ~ 139

Why cannot I use the TCP 25 port to connect to an external address and how to lift the ban?

To improve the performance for sending emails from Tencent Cloud IP address, connection of CVM TCP port 25 to an external address is restricted by default. You can log in to the console and move your mouse cursor to **Account** of the top navigation, and you can see the entry of **Unblocking Port 25**.

Each user can unblock 5 instances in each region by default.

For more information, please see Why is the outbound direction of CVM TCP port 25 blocked?

Security Group

Why is there a default Reject rule in the security group?

The security group rules are filtered and take effect from top to bottom. After the Allow rules are enabled, other rules will be rejected by default. If all the ports are opened, the last Reject rule does not take effect. For security reasons, we provide this default setting.

How to create a security group?

Please see the **Create Security Group** section of Common Security Group Operations.

How to configure a security group?

Please see Common Security Group Operations.

How are security groups associated with CVM instances?

Please see the **Configure Security Groups Associated with CVM Instances** section of Common Security Group Operations.

If I bind an incorrect security group with an instance, what is the effect on the instance? How to solve the problem?

Potential problems

- You may fail to remotely connect to a Linux instance (SSH) or remotely log in to desktop Windows instance.

- You may fail to remotely ping the public IP and private IP for the CVM instance under this security group.
- You may fail to perform HTTP access to the Web services exposed by the CVM instance under this security group.
- The CVM instance under this security group may be unable to access Internet services.

Solutions

- In case any of the above problems happens, you can go to "Security Group Management" in the CVM console and reset the rule for the security group, for example, to "only bind all-pass security groups by default".
- For specific settings for security group rules, please see Introduction to Security Group.

What do security group direction and policy mean?

The security group policy works in the directions of outbound and inbound. The former is to filter the outbound traffic of the CVM, and the latter is to filter the inbound traffic of the CVM.
The policy is two-fold: **Allow** and **Reject** traffic.

In what order does the security group policy go into effect?

From top to bottom. The policy matching is in a top-to-bottom order when the traffic goes through the security group, and the policy goes into effect once the matching is successful.

Why is an IP able to access the CVM without being allowed by the Security Group?

It may be caused by the following reasons:

- The CVM may be bound to multiple security groups and that specific IP may be allowed in other security groups.
- That specific IP serves for an approved Tencent Cloud public service.

By using security groups, does it mean iptables cannot be used?

No. Security groups and iptables can be used simultaneously. Your traffic will be filtered twice in the following directions:

- Outbound: Processes on your CVM instance -> iptables -> Security groups.
- Inbound: Security groups -> iptables -> Processes on your CVM instance.

Even though all the CVMs have been returned, the security groups still cannot be deleted, why?

Check if there is a CVM in the recycle bin. The security group bound to the CVM in recycle bin cannot be deleted.

Can the name of the security group to be cloned be the same as that of a security group in the target area?

No. The name should be different from that of any existing security group in the target area.

Can a security group be cloned across different users?

Not for now.

Is there any Cloud API support for cloning a security group across different projects and regions?

MC support is provided to offer ease to customers who use the console, whereas no direct Cloud API support is available at the moment. You can use the original Cloud APIs for security group rules on batch import/export to indirectly clone a security group across different projects and regions.

When a security group is being cloned across different projects and regions, will the CVMs managed by the security group be copied over?

No, cloning a security group across different regions will only clone the entry and exit rules of the original security group. The CVM needs to be associated separately.

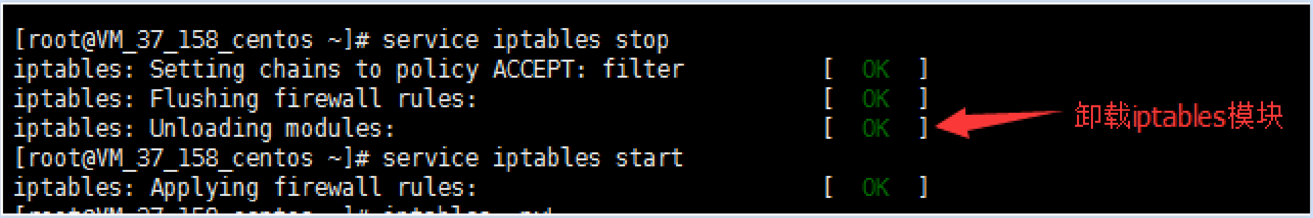
Firewall

Last updated：2018-08-06 11:04:15

For Linux system, how to configure firewall software iptables?

Note:
iptables is quite different before and after CentOS 7.

- Prior to CentOS 7, the iptables service was used as a firewall by default. Using the `service iptables stop` code, the iptables service clears the rules first and then unmount the iptables module. When it starts again, rules are loaded from the configuration file. When you stop the iptables service, you can test whether the firewall is restricted.



```
[root@VM_37_158_centos ~]# service iptables stop
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Unloading modules:                               [  OK  ]
[root@VM_37_158_centos ~]# service iptables start
iptables: Applying firewall rules:                         [  OK  ]
[root@VM_37_158_centos ~]# iptables -nv
```

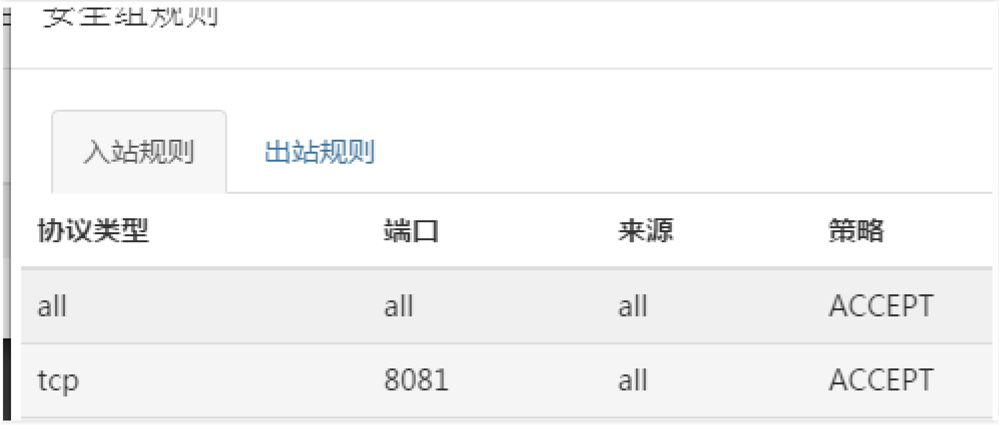
卸载iptables模块

- After CentOS 7, the firewall service is used as firewall by default. For compatibility, the iptables_filter module is also loaded, but the iptables service is not available. So after CentOS 7, you can add rules using the iptables command, but the iptables service is disabled by default. The user confirms that the iptable_filter module is loaded and the rules take effect.

The most secure method for learning the firewall is `iptables -nvL` .
Here are two examples on how to configure:

Scenario 1

For Ubuntu 14 system, the security group and listening port are opened, but telnet does not work.
Inbound rule of security group:

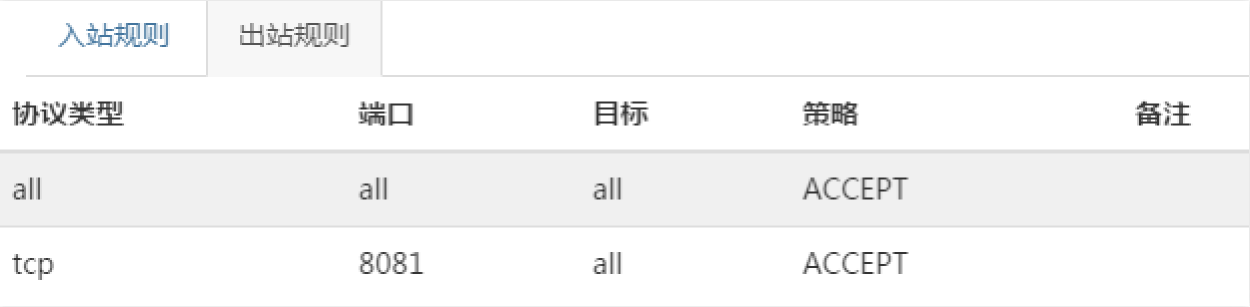


安全组规则

入站规则 出站规则

协议类型	端口	来源	策略
all	all	all	ACCEPT
tcp	8081	all	ACCEPT

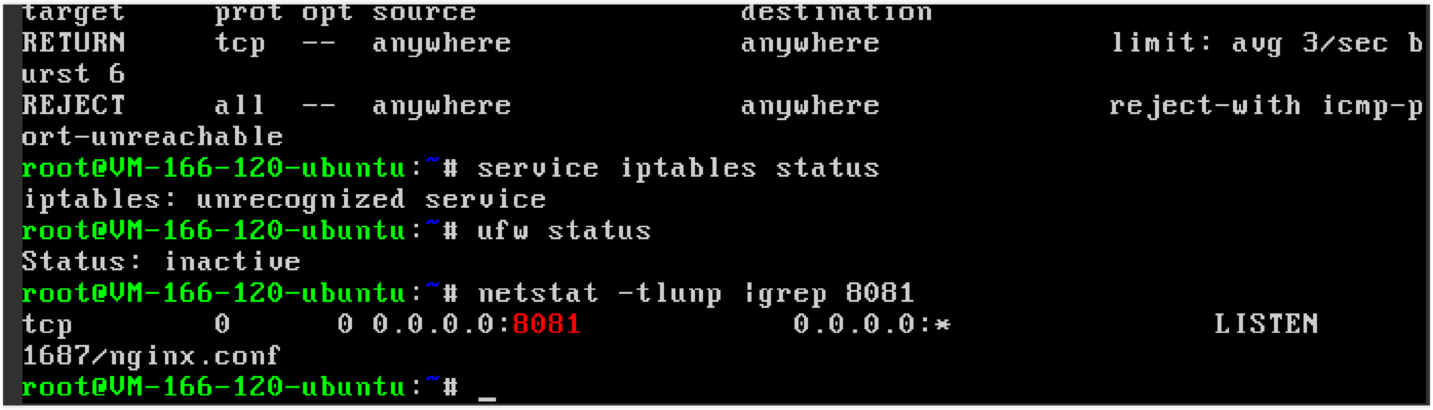
Outbound rule of security group:



入站规则 出站规则

协议类型	端口	目标	策略	备注
all	all	all	ACCEPT	
tcp	8081	all	ACCEPT	

telnet does not work:

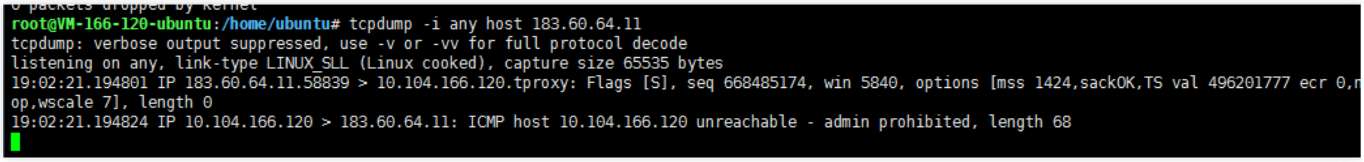


```
target     prot opt source               destination
RETURN     tcp  --  anywhere             anywhere             limit: avg 3/sec b
urst 6
REJECT     all  --  anywhere             anywhere             reject-with icmp-p
ort-unreachable
root@VM-166-120-ubuntu:~# service iptables status
iptables: unrecognized service
root@VM-166-120-ubuntu:~# ufw status
Status: inactive
root@VM-166-120-ubuntu:~# netstat -tlunp |grep 8081
tcp        0      0 0.0.0.0:8081            0.0.0.0:*               LISTEN
1687/nginx.conf
root@VM-166-120-ubuntu:~# _
```

Solutions

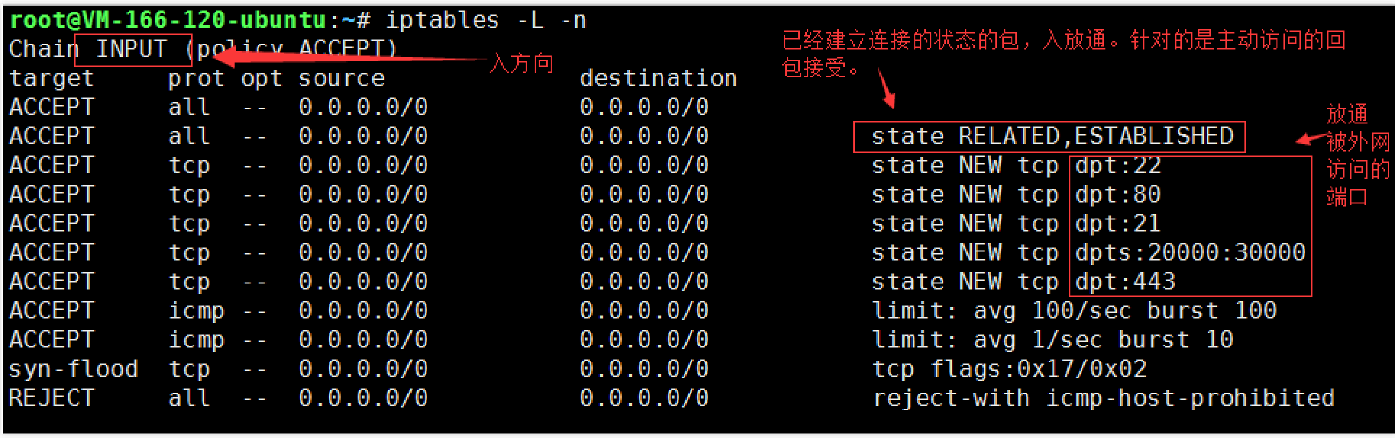
1. First, capture the packets of CVM to determine if packets have reached the CVM.
    - If they do not reach the CVM, they may be blocked by the security group or the upper tgw and the ISP.
    - If packets reach the CVM, but there is a problem with return packets, it is most likely caused by the iptables policy within CVM. As shown below, there is no TCP packet back to 64.11 after telnet

operation.



```
0 packets dropped by kernel
root@VM-166-120-ubuntu:/home/ubuntu# tcpdump -i any host 183.60.64.11
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
19:02:21.194801 IP 183.60.64.11.58839 > 10.104.166.120.tproxy: Flags [S], seq 668485174, win 5840, options [mss 1424,sackOK,TS val 496201777 ecr 0,n
op,wscale 7], length 0
19:02:21.194824 IP 10.104.166.120 > 183.60.64.11: ICMP host 10.104.166.120 unreachable - admin prohibited, length 68
```

2. After confirming it is the iptables policy problem, confirm whether the policy opens port 8081 to Internet via `iptables -nvL`. Here this port is not opened to Internet.



```
root@VM-166-120-ubuntu:~# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:21
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpts:20000:30000
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:443
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0            limit: avg 100/sec burst 100
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0            limit: avg 1/sec burst 10
syn-flood  tcp  --  0.0.0.0/0            0.0.0.0/0            tcp flags:0x17/0x02
REJECT     all  --  0.0.0.0/0            0.0.0.0/0            reject-with icmp-host-prohibited
```

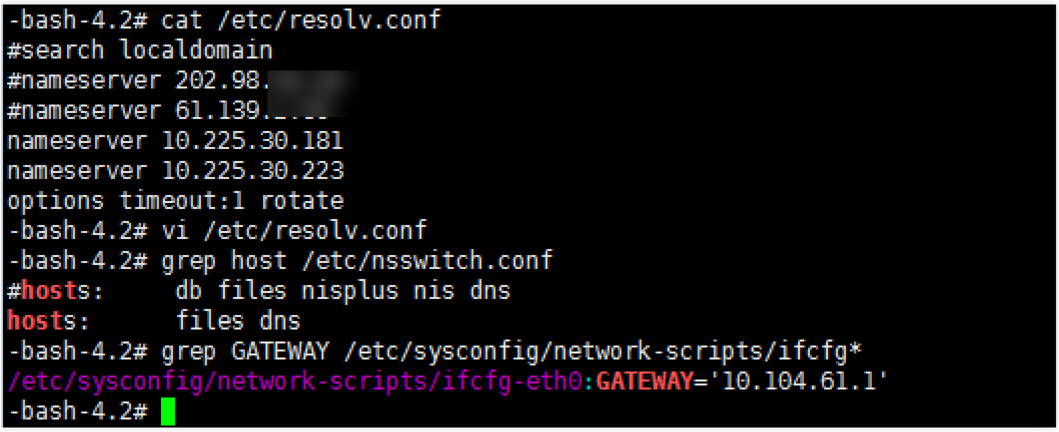
3. Use the command to add the policy to open port 8081 to Internet.

```
iptables -I INPUT 5 -p tcp --dport 8081 -j ACCEPT
```

4. Port 8081 is tested to be opened. The problem is solved.

Scenario 2

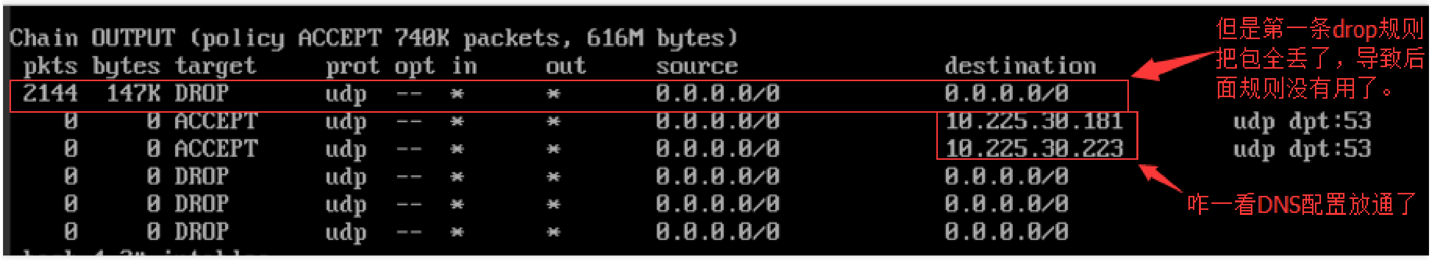
In terms of iptables configuration, the policy has been opened to Internet, but the destination server still cannot be pinged.



```
-bash-4.2# cat /etc/resolv.conf
#search localdomain
#nameserver 202.98.[redacted]
#nameserver 61.139.[redacted]
nameserver 10.225.30.181
nameserver 10.225.30.223
options timeout:1 rotate
-bash-4.2# vi /etc/resolv.conf
-bash-4.2# grep host /etc/nsswitch.conf
#hosts:     db files nisplus nis dns
hosts:      files dns
-bash-4.2# grep GATEWAY /etc/sysconfig/network-scripts/ifcfg*
/etc/sysconfig/network-scripts/ifcfg-eth0:GATEWAY='10.104.61.1'
-bash-4.2#
```

Solutions

If the following cases occur:



```
Chain OUTPUT (policy ACCEPT 740K packets, 616M bytes)
 pkts bytes target     prot opt in     out     source               destination
 2144  147K DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            10.225.30.181        udp dpt:53
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            10.225.30.223        udp dpt:53
    0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

但是第一条drop规则把包全丢了，导致后面规则没有用了。

咋一看DNS配置放通了

Use the command to delete the first rule in the output direction:

```
iptabels -D OUTPUT 1
```

The problem is solved after testing.

How to clear the firewall?

Windows instance:

1. After logging in to the instance, click **Start** -> **Control Panel** -> **Firewall Settings** to enter the firewall settings page.

2. Check whether the firewall and other security software (such as Safedog) are enabled. If enabled, disable them.

Linux instance:

1. Run the command to check whether the client has enabled the firewall policy. If not, skip Step 2 and go directly to Step 3:

   ```
   iptables -vnL
   ```

2. If the firewall policy is enabled, run the command to back up the current firewall policy:

   ```
   iptables-save
   ```

3. Run the command to clear the firewall policy.

   ```
   iptables -F
   ```

Will CVM acceleration using non-Tencent Cloud CDN be blocked by the firewall?

No. If you are concerned about the impact, you can disable the firewall.

About Access Control

Last updated：2018-08-06 11:19:10

How to create custom policy?

If preset policies cannot meet your requirements, you can create custom policies.
The syntax of custom policies is as follows:

```
{
"version": "2.0",
"statement": [
{
"action": [
"Action"
],
"resource": "Resource",
"effect": "Effect"
}
]
}
```

- Replace "Action" with the operation to be allowed or denied.
- Replace "Resource" with the resources that you want to authorize users to work with.
- Replace "Effect" with Allow or Deny.

How to configure read-only policy for CVMs?

To allow a user to only query CVM instances, without granting him/her the permissions to create, delete, start/shut down the instances, implement the policy named QcloudCVMInnerReadOnlyAccess.

Log in to the CAM console, and find the policy quickly by searching for **CVM** on the Policy Management page.

The policy syntax is as follows:

```
{
"version": "2.0",
"statement": [
{
"action": [
"name/cvm:Describe*",
"name/cvm:Inquiry*"
],
"resource": "*",
"effect": "allow"
}
]
}
```

The above policy is designed to **grant users the permissions to perform the following operations**:

- All operations starting with "Describe" in CVM.
- All operations starting with "Inquiry" in CVM.

How to configure read-only policy for CVM-related resources?

To allow a user to only query CVM instances and relevant resources (VPC, CLB), without granting him/her the permissions to create, delete, start/shut down the instances, implement the policy named QcloudCVMReadOnlyAccess.

Log in to the CAM console, and find the policy quickly by searching for **CVM** on the Policy Management page.

The policy syntax is as follows:

```
{
"version": "2.0",
"statement": [
{
"action": [
"name/cvm:Describe*",
"name/cvm:Inquiry*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"name/vpc:Describe*",
"name/vpc:Inquiry*",
"name/vpc:Get*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"name/clb:Describe*"
],
"resource": "*",
"effect": "allow"
},
{
"effect": "allow",
"action": "name/monitor:*",
"resource": "*"
}
]
}
```

The above policy is designed to **grant users the permissions to perform the following operations**:

- All operations starting with "Describe" and "Inquiry" in CVM.
- All operations starting with "Describe", "Inquiry" and "Get" in VPC.
- All operations starting with "Describe" in Load Balance.
- All operations in Monitor.