Cloud Virtual Machine

FAQ

Product Documentation

Contents

FAQ
About Billing
Purchase

Last updated：2019-07-25 18:40:51

Purchase CVMs

All users can purchase CVMs on Tencent Cloud's official website. According to different billing methods, users can purchase prepaid CVMs (on a monthly/yearly basis) or postpaid CVMs (billing is accurate to seconds and is settled on an hourly basis). For more information, please see Billing Methods.
The purchase process of prepaid and postpaid CVMs is similar, as shown below:

1. Log in to Purchase Tencent Cloud Service, and select the Custom Configuration tab.

2. Select a billing method: prepaid or postpaid.

3. Select the region and model, image, storage and bandwidth, security group and CVM, and then confirm the order.

   Purchase suggestions:

   - Users with smooth network are recommended to select bill-by-bandwidth. If bill-by-bandwidth is selected, the traffic is unlimited. The billing method is "hardware + bandwidth" (prepaid)
   - Users with fluctuate network are recommended to select bill-by-traffic. If bill-by-traffic is selected, users can freely select the peak bandwidth. The billing method is "Hardware (prepaid) + Traffic (actual traffic)".

4. Payment. You can pay with your balance, Tenpay, WeChat Pay or QQ Wallet, etc.

5. The CVM is activated immediately after the payment is completed. You can see the IP address in 1 to 5 minutes, which can be managed after you logged in to the CVM.

Note:

After a postpaid CVM is activated, make sure that your balance is sufficient.

See Notes for Purchasing from Console

What are the regions and availability zones of CVMs? How to select?

For more information on available regions and available zones of CVMs, please see Regions and Availability Zones

For more information on how to select regions and available zones, please see Regions and Available Zones.

What CVM types are provided?

Multiple CVM instance specifications are provided. For more information, please see Instance Specification. You can select the appropriate instance type based on your business needs.

If your demand is stable, we recommend that you select the prepaid billing method. So your savings will increase with the length of usage.

To react to spikes in demand, you can choose the postpaid billing method, which allows you to activate/terminate computing instances at any time and only pay for the actually consumed resources. CVM usage is billed in one-second increments to maximize your savings.

How to select the CVM configuration solution?

Entry: Suitable for start-up personal websites. For example, small websites such as personal blogs.
Basic: Suitable for websites or applications with a certain number of visits. For example, large enterprise official websites and small e-commerce websites.
Universal: Suitable for scenarios where cloud computing is frequently used. For example, portals, SaaS software, and small Apps.
Application: Suitable for applications demanding high concurrency and scenarios with high requirement for CVM network and computing. For example, large portals, e-commerce websites, and game Apps.
If recommended configuration does not meet your needs, you can compare the configurations in **More Models** based on your actual needs. You can also Upgrade Configuration or Downgrade Configuration at any time based on your business needs after purchasing a CVM.

> **Note:**
>
> Windows CVM cannot be used as Public Gateway. Users who need public gateway can refer to Getting Started with Linux CVM.

Can I purchase a Windows 2003 CVM?

Because Microsoft ended Windows 2003 support, Tencent Cloud no longer provides Windows 2003 servers. You cannot purchase it.

How to select storage?

For data that requires extremely high reliability, use Cloud Block Storage to ensure the persistent and reliable data storage. Try not to select Local Disk for data storage.

What are the limits of purchasing prepaid and postpaid CVMs?

For more information, please see Quota for CVM Instances.

What are the CVM purchase channels?

Tencent Cloud allows users to purchase CVMs either from the official website or via the API.

How long will it take before a purchased CVM can be used?

After the system installation of CVM is completed, the CVM status becomes **Running**, and then you can log in to and use it.

What if the CVM is not created successfully?

If the CVM creation process takes a long time, wait to see if the CVM is created successfully; if it is not, you can submit a ticket to report your problems and ask the engineer for help.

In case of CVM delivery failure, how to terminate the CVM?

You can submit a ticket to contact customer service, and provide complete screenshots of server information and termination failure indicating **Delivery Failure** to facilitate the troubleshooting.

Renew

Last updated：2018-08-06 11:10:00

How to renew a CVM after it expires?

Please see Renewing Instances.

How to set auto renewal for CVMs?

Please see the **Set Auto Renewal** section of Renewing Instances.

Do postpaid instances need renewal?

For postpaid instances, charges are automatically deducted from the account every hour. So there is no renewal issue.

The CVM has been renewed, but the renewal is unsuccessful. How to solve the problem?

Check the order information first to confirm if you have renewed. If yes, submit a ticket and the engineer will assist you in solving the problem.

Refund

Last updated：2019-07-25 18:39:02

How to apply for a refund for CVM?

Please submit a ticket to apply for return of CVM.

After the application for a refund is successful, when can I get the refund?

Generally, after the CVM is unsubscribed, the fee will be refunded to your Tencent Cloud account within half an hour.

Others

Last updated：2018-08-06 11:08:47

A user has purchased a Linux CVM that comes with an over-20 GB Cloud Block Storage. How will it be charged if the user reinstalls the operating system as Windows?

The charges will be calculated based on the billing method:

- If it is a prepaid CVM, a refund will be made (exclusive of the amount of voucher used in payment) according to the payment conditions.
- If it is a postpaid CVM, the calculation of configuration charge for the part exceeding 20 GB of the system disk will be stopped (i.e. the system disk will be free of charge afterwards) after the operating system is changed to Windows.

A user has purchased a Windows CVM that comes with a Cloud Block Storage. How will it be charged if the user reinstalls the operating system as Linux?

Since the system disk does not support capacity reduction, when a 50 GB Windows Cloud Block Storage is changed to Linux, the capacity shall be kept and corresponding fees for the Cloud Block Storage shall be paid. (The first 20 GB is free of charge, and fees for another 30 GB shall be paid).

For more information on cloud disk price, please see Price Overview of CBS.

How to adjust the size and charge of the existing CVM system disk?

Please see Description on Default Selection of CVM System Disk.

About Instance Login and Remote Access

Last updated：2019-08-09 18:54:38

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

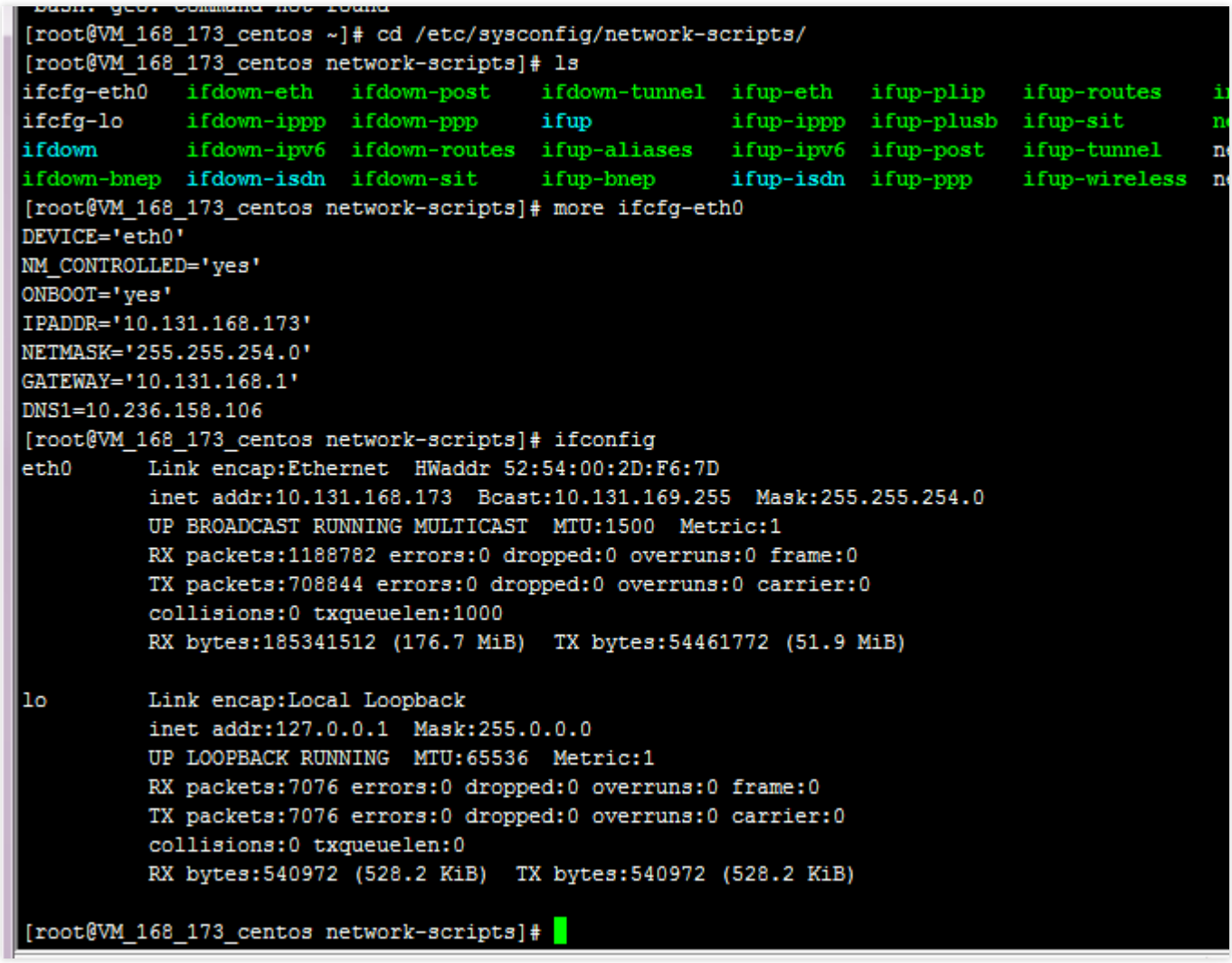
What to do if I failed to log in to a Linux instance with an SSH key?

The solutions are as follows:

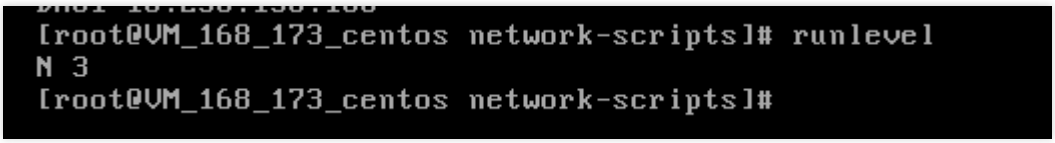
1. Cancel or modify the security group policy on the Console. See Security Group Operation Guide

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



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



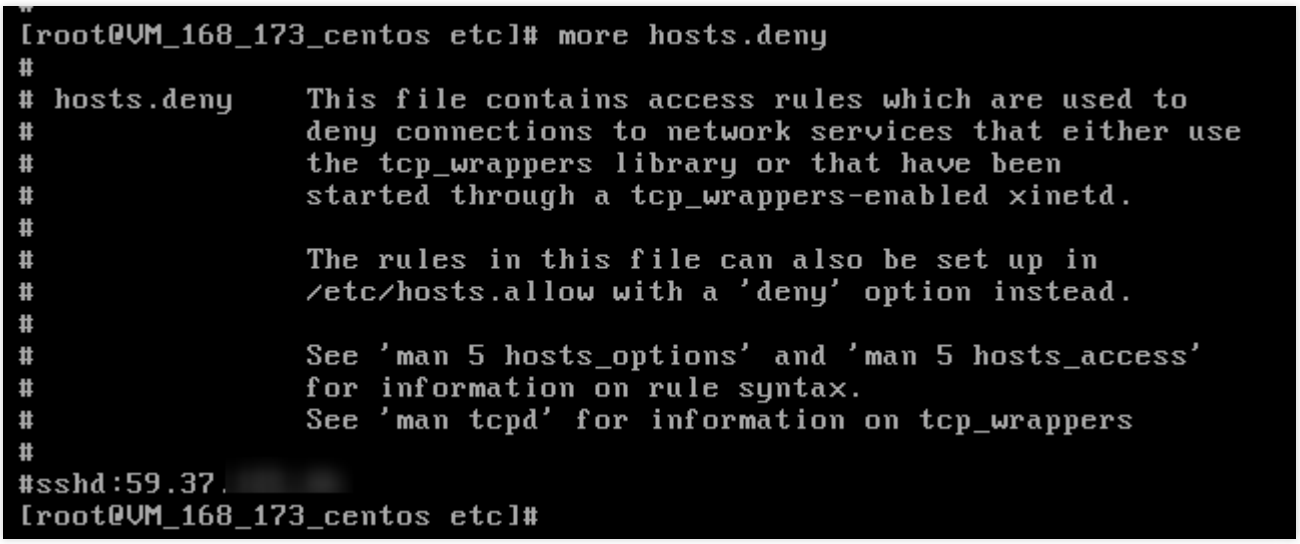
5. Verify whether the sshd service of the server is running normally and there is no problem with the configuration such as port.

```
[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
```

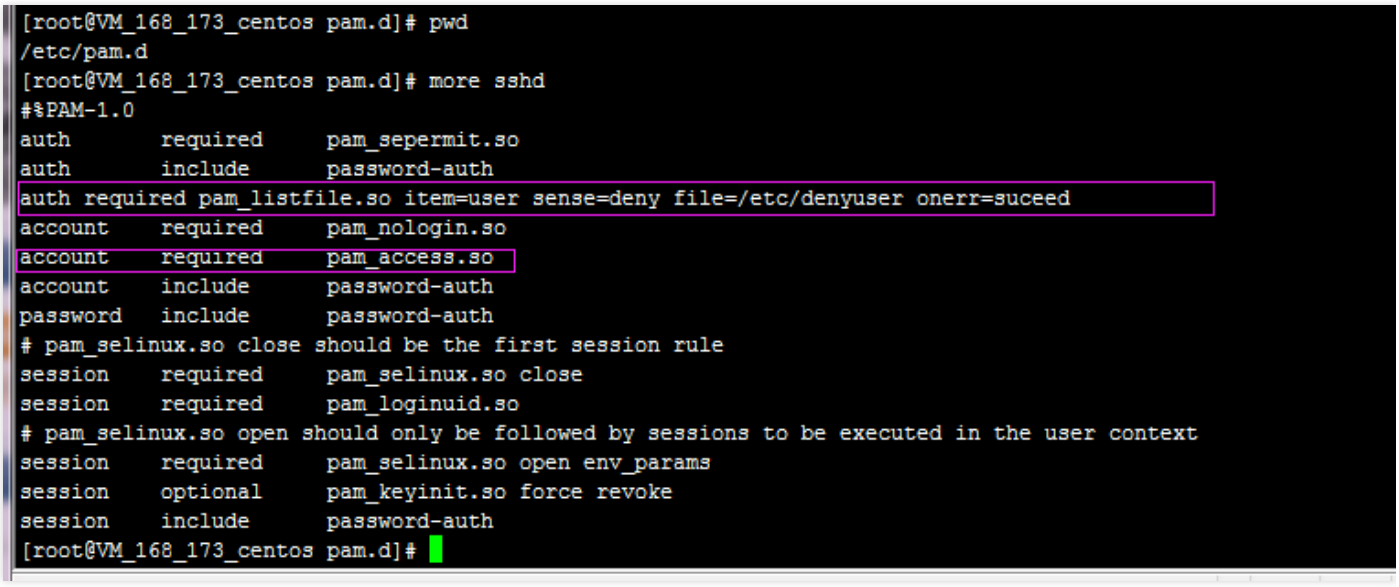
6. Verify whether the server's iptables firewall has blocked the access and whether its policy is OK.

```
[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.



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):



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.

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
```

iii. 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：2019-08-07 10:53:24

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.

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：2019-07-25 18:38:13

How do I view the CVMs in use?

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

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.

About Storage
System and Data Disks

Last updated：2018-09-12 17:22:55

What is the default capacity of a CVM system disk?

A new CVM system disk has a capacity of 50 GB by default.

Can I change a CVM system disk from a local disk to a cloud disk?

CVM instances only support selecting disk type for system disk at the time of purchase. After the purchase, the switch between local and cloud disks for system disk is not allowed. It is recommended to select cloud disk as the system disk the next time you purchase a CVM instance.

Which regions and availability zones support increasing system disk capacity to more than 50 GB?

For Beijing, Shanghai, and Guangzhou regions, if the system disk is a cloud disk, its capacity can be changed to more than 50 GB. This is not supported in the domestic finance zones and other regions.

When the system is reinstalled, can the capacity of CVM system disk be expanded?

Generally, this involves two scenarios:

- **System disk is a cloud disk:**
  In this case, when you reinstall the system, expanding capacity (increasing the system disk size) is supported, but reducing capacity (reducing the system disk size) is not supported.

- **System disk is a local disk:**

  This can be further divided into two scenarios, depending on the size of the current system disk:

  - For the instance whose system disk's default capacity is 50 GB at the time of purchase, expanding capacity is not supported.
  - This applies to the instances that were purchased at early stage: if the system disk capacity is less than or equal to 20 GB, it is adjusted to 20 GB by default; if the capacity is greater than 20 GB, it is adjusted to 50 GB by default.

How do I expand the capacity of a cloud disk?

If your CVM uses a cloud disk, you can expand the disk capacity. For more information on how to expand the capacity, please see Expanding Capacity of Cloud Disks.

Can the capacity of an expanded system disk be reduced by reinstalling the system?

The capacity of a system disk cannot be reduced.

How can I expand the system disk capacity with the current data on the CVM stored?

You can create an image first, and then use the image to reinstall the system to expand the system disk capacity.

What is the system disk capacity if I use an image less than 50 GB to create or reinstall the CVM?

The system disk has a minimum capacity of 50 GB regardless of the image capacity.

How much free capacity is provided for a separately purchased cloud disk? What is the difference between a separately purchased cloud disk and a cloud disk purchased with CVM?

No free capacity is given for a cloud disk purchased separately, and there is no difference between such a cloud disk and a could disk purchased with a CVM. A cloud disk purchased with a CVM cannot be unmounted from the CVM and is renewed along with the CVM. A separately purchased cloud disk can be mounted to different CVMs and is renewed separately. This makes it more flexible than a cloud disk purchased with a CVM.

How can I check the data disk?

Log in to the Console, and go to **Cloud Virtual Machine** -> **Cloud Block Storage**. In the **Attribute** column, select **Data Disk** to check all data disks in the region.

How do I read and write the original NTFS data disk after the operating system is changed from Windows to Linux?

A Windows file system usually uses NTFS or FAT32 format, while a Linux file system uses EXT format. When the operating system is changed from Windows to Linux after re-installation, the data disk remains in the original format. Thus, the access to the data disk file system may fail in the reinstalled system. On the reinstalled Linux CVM, you can read data from the data disk under Windows by performing the following operations:

1. Install ntfsprogs software on the Linux system using the following command to enable Linux to support NTFS file system:

```
yum install ntfsprogs
```

2. Mount the data disk under Windows to Linux CVM. Skip this step if the data disk has already been mounted:
   Log in to Console, go to **Cloud Virtual Machine** -> **Cloud Block Storage**, and then click **More** -> **Mount to CVM** button for the Windows data disk to be mounted. Select the reinstalled Linux CVM in the pop-up box, and then click **OK**.

3. Check the data disk migrated from Windows by running the following command:

```
parted -l
```

4. Mount the data disk by running the following command:

```
mount -t ntfs-3g Data disk path Mount point
```

```
[root@VM_127_193_centos ~]# mount -t ntfs-3g /dev/vde2 mnt/
[root@VM_127_193_centos ~]# ls mnt/
$RECYCLE.BIN  test.txt
```

5. When the file system is identified, the mounted data disk can be directly read and written by the Linux system.

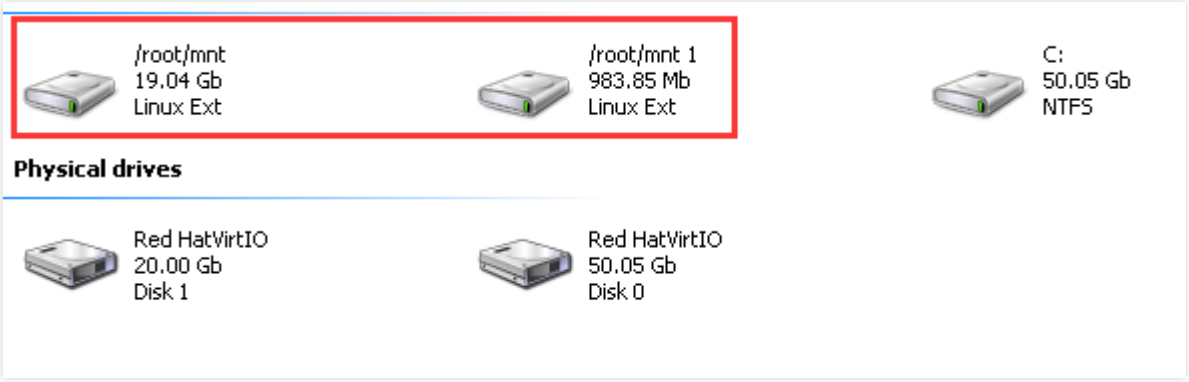
How do I read the data disk in EXT format after the operating is changed from Linux to Windows after re-installation?

A Windows file system usually uses NTFS or FAT32 format, while a Linux file system uses EXT format. When the operating system is changed from Linux to Windows after re-installation, the data disk remains in the original format. Thus, the access to the data disk file system may fail in the reinstalled system. On the reinstalled Windows CVM, you can read data from the data disk under Linux system by performing the following operations:

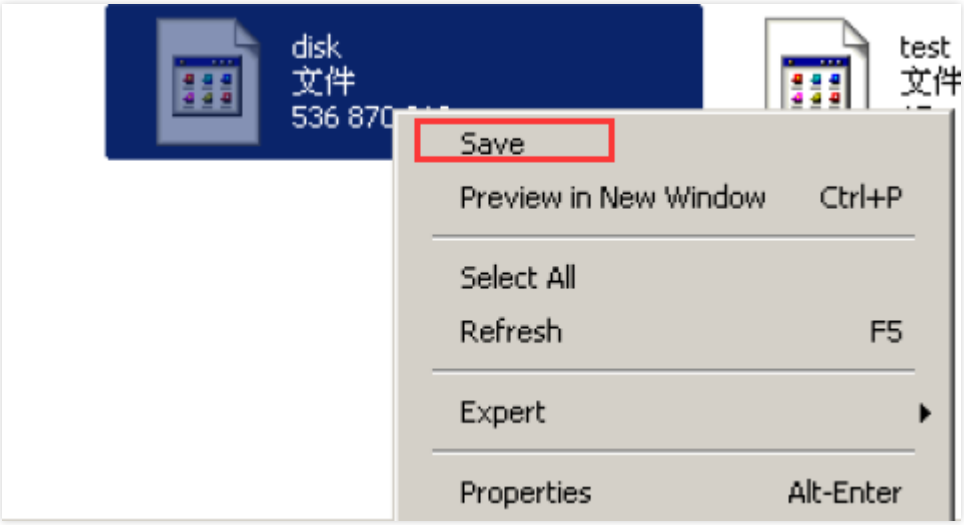
1. Suppose the Linux CVM data disk has two partitions before re-installation: /dev/vdb1 and /dev/vdb2.

```
Disk /dev/vdb: 21.5 GB, 21474836480 bytes
16 heads, 63 sectors/track, 41610 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x29cc8ca2

   Device Boot      Start         End      Blocks   Id  System
/dev/vdb1            2000       41610    19963944   83  Linux
/dev/vdb2               1        1999     1007464+  83  Linux
```

2. Download and install DiskInternals Linux Reader on the reinstalled Windows CVM.
3. Mount the data disk under Linux to the Windows CVM. Skip this step if the data disk has already been mounted: Log in to Console, go to **Cloud Virtual Machine** -> **Cloud Block Storage**, and then click **More** -> **Mount to CVM** button for the Linux data disk to be mounted. Select the reinstalled Windows CVM in the pop-up box, and then click **OK**.
4. Run DiskInternals to check the information of the data disk you just mounted. /root/mnt and /root/mnt1 correspond to partitions vdb1 and vdb2, respectively:



5. Click to enter /root/mnt, right-click the file you want to copy, and then select **Save** to save the file.



6. Note that the Linux data disk is read-only at this time. To perform read and write operations on the data disk as you do on a Windows data disk, back up the files you need and then re-format the disk into a standard type supported by Windows operating system. For more information, please see Data Disk Partitioning and Formatting on Windows System.

Backup and Restore

Last updated：2019-07-25 18:43:22

How do I backup data for CVMs?

- If your CVM uses a cloud disk, you can back up your business data by creating a system disk custom image and a data disk snapshot.
  - For more information on how to create a custom image, please see: image operation guide
  - For more information on how to create a snapshot, please see: snapshot operation guide
- If your CVM uses a local disk, you can back up data on system disk by creating a custom image. For the business data in your data disk, you still need to customize your backup policy.
  You can use FTP to back up the data in the server to other places.
- In addition, if you have higher requirements for data security, you can also purchase more specialized third-party customized backup services. Cloud Marketplace>>

What are the common data backup and recovery solutions?

The applicable data backup and recovery solutions vary with different application scenarios and businesses. The following are some recommended approaches that can be used based on your actual needs:

- Back up the instance regularly using the CBS Snapshot feature.
- Deploy key components of the application across multiple availability zones and replicate the data appropriately.
- Use EIP for domain name mapping to ensure that the service IP can be quickly redirected to another CVM instance when the server is unavailable.
- Check the monitoring data regularly and set the relevant alarms. For more information, please see Cloud Monitor Product Documentation.
- Process emergent requests with Auto Scaling. For more information, please see Auto Scaling Product Documentation.

How do I recover CVM files?

For CVM file recovery, use the relevant free or paid service from Cloud Marketplace.

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：2019-07-25 17:27:16

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.

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.

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.

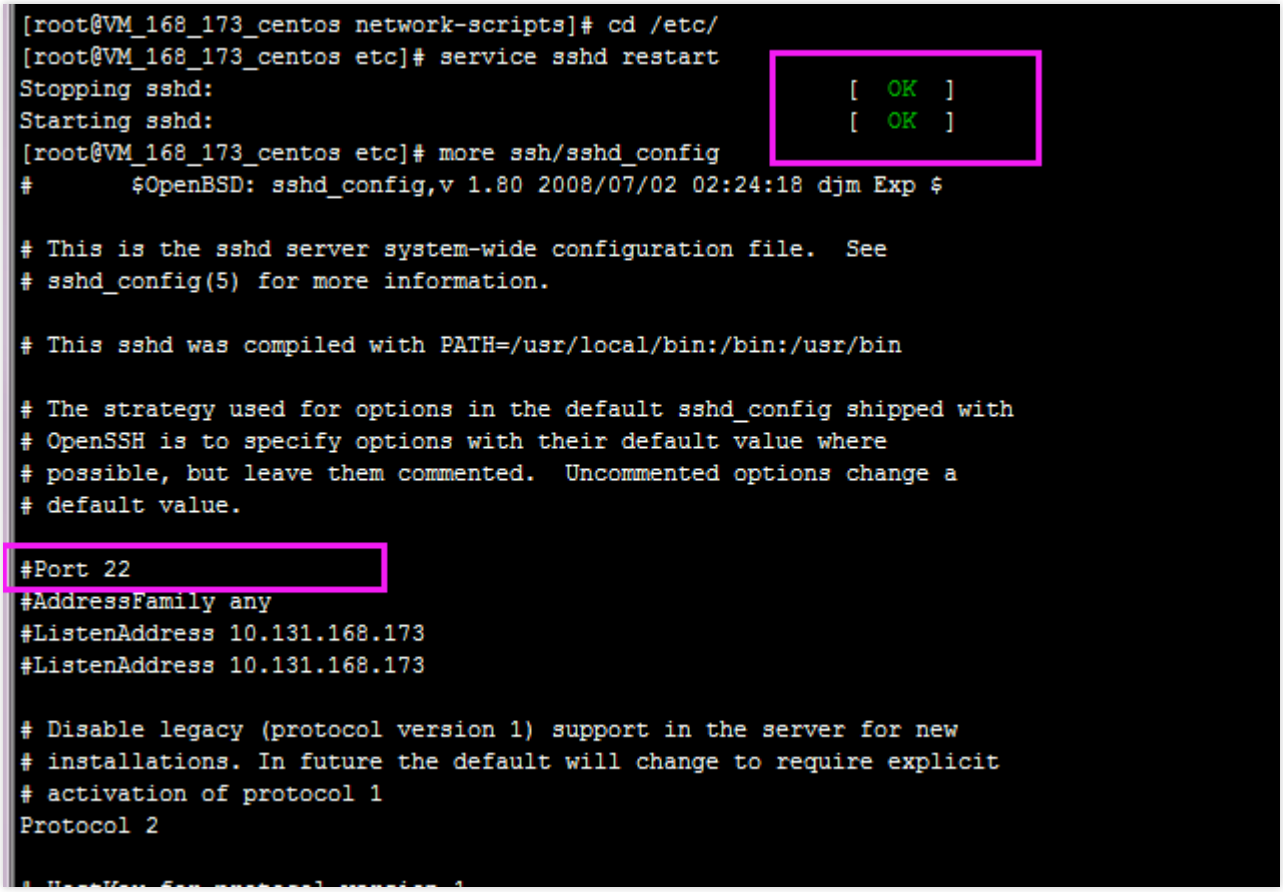
2. Cancel or modify the security group policy in Console. See Safety Group Operation Guide

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

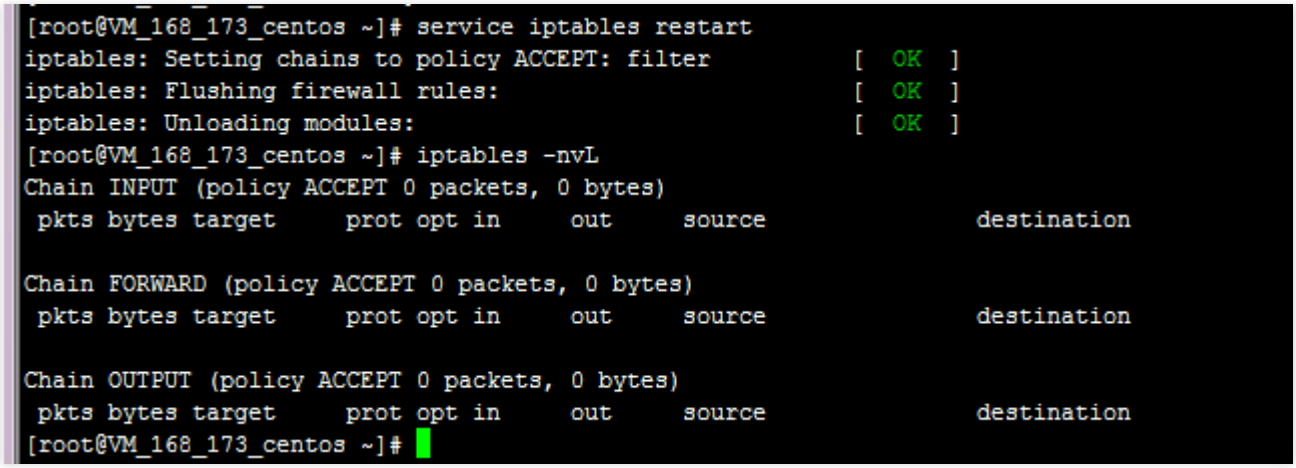
4. Use VNC to log in to the instance to check whether the NIC status and IP configuration information are correct. See Login Linux Instance Operation Guide

```
[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.



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



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.
[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：2019-08-07 10:51:34

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?

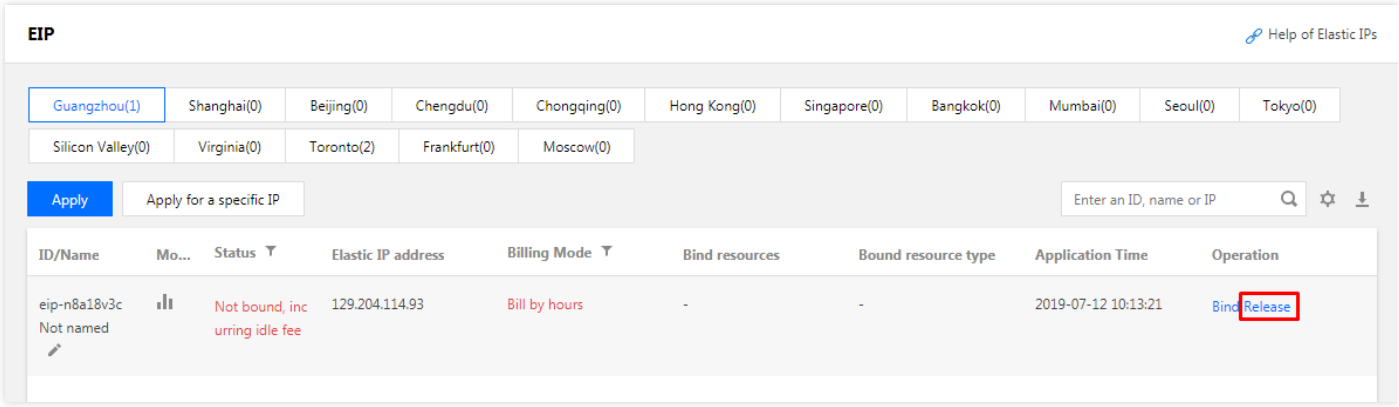
1. The fee displayed on the console applies to the EIPs that remain vacant for one hour. EIPs can be billed with an accuracy down to seconds. EIPs that have been bound/unbound many times are billed based on the total duration (in sec) for which they remain unbound.
2. The EIPs that remain unbound for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



- 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：2019-07-25 17:03:25

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.

Which are common CVM ports?

Please see Common Server Ports.

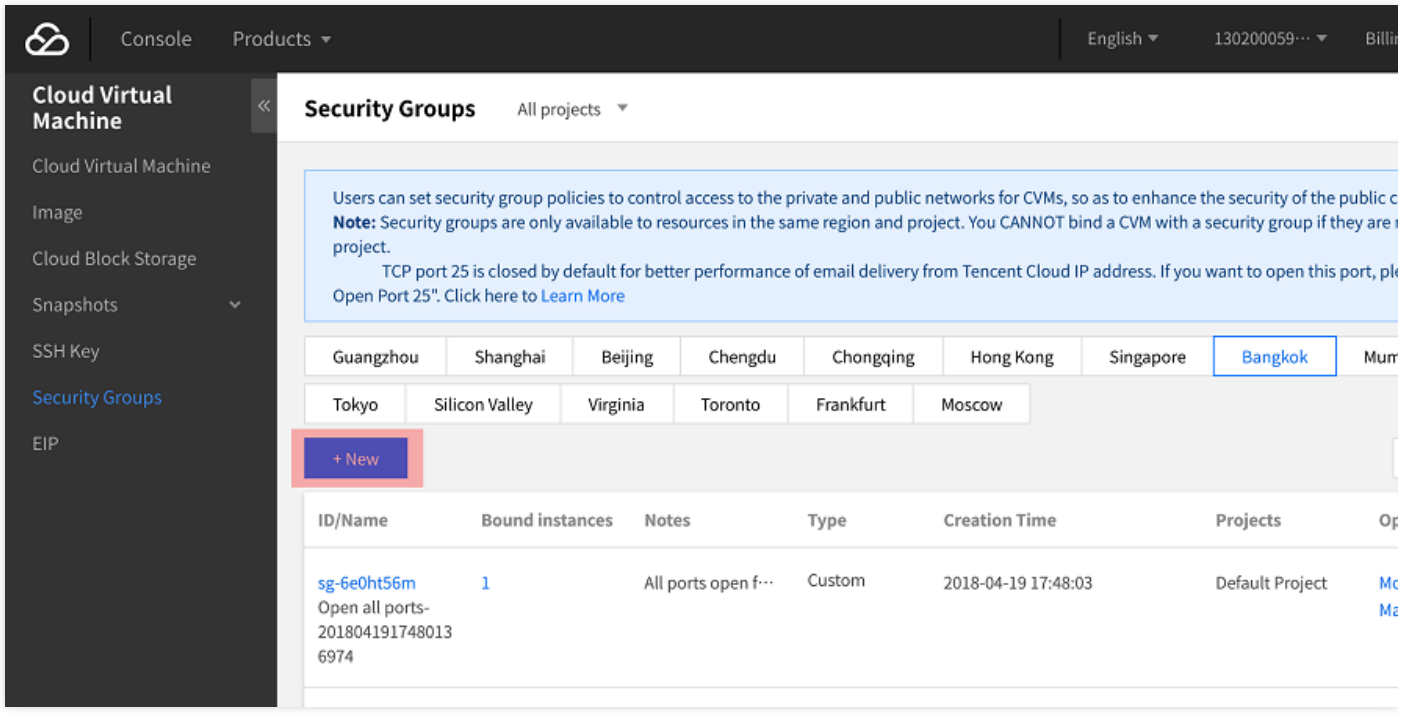
Why do you need to open the port? How to open a port?

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

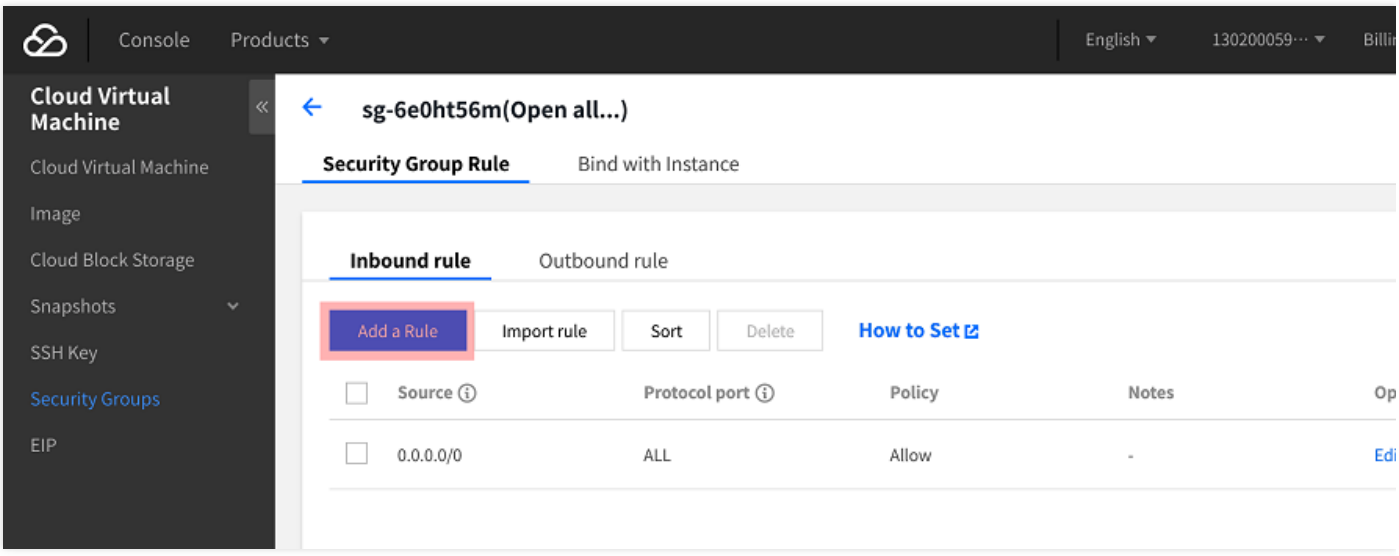
If you want to access web pages using port 8080, the port must be opened to Internet in the security group.

Open a port to Internet

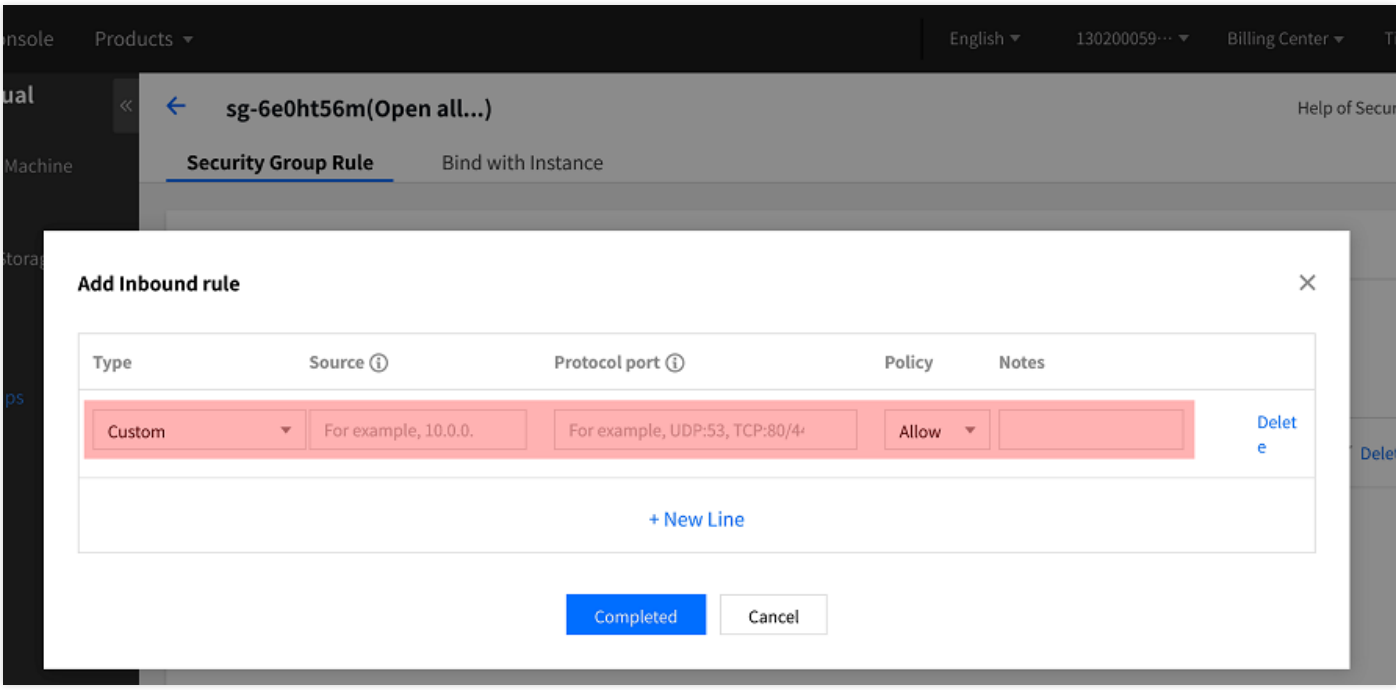
1. Log in to the security group console, and click the security group bound with the instance to enter the details page



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



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.

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.

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.

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.