Cloud Virtual Machine
FAQs
Product Documentation
Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's prior written consent.

Trademark Notice

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

Service Statement

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

FAQs
  About Billing
    Purchase
    Renew
    Others
  About Instance
    Login and Remote Access
    Adjust Configuration
    Reinstall System
    About D1 Instances
    Spot Instances
    Others
  About Storage
    System and Data Disks
    Backup and Restore
  About Images
    About Image
    Cloud-Init & Cloudbase-Init
  About Network
    Network
    IP Address
    Elastic Public IP
    Elastic Network Interface
  About Security
    Password Login and SSH Key Login
    Port and Security Groups
  About Access Control
  About Service migration
  Region and Availability Zone
FAQs
About Billing
Purchase

Last updated: 2020-04-25 12:17:14

Purchase CVMs
All users can purchase CVMs on Tencent Cloud's official website. According to different billing methods, users can purchase 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 postpaid CVMs, as shown below:

1. Log in to Purchase Tencent Cloud Service, and select the Custom Configuration tab.
2. Select a billing method: 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.

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.

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.

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 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.
Do pay-as-you-go instances need to be renewed?

For pay-as-you-go instances, charges are automatically deducted from the account every hour, so no renewal is needed.
A user has purchased a Linux-based CVM that comes with a cloud disk exceeding 20 GB. What will be charges be if the user reinstalls the operating system as Windows?

The charges will be based on the billing mode:

- For pay-as-you-go CVMs, billing for the previously purchased system disk that exceeds 20 GB will stop once Windows OS is successfully installed.

A user has purchased a Windows-based CVM that comes with a cloud disk. What will be charges be if the user reinstalls the operating system as Linux?

The capacity of system disks cannot be reduced. If the system disk remain as is after reinstallation, there will be no additional charges. If you need to expand the disk capacity after reinstalling to Linux OS, additional fees will apply. See System Disks and Data Disks for details on system disk expansion.

For cloud disks prices, please see Pricing List.

CVMs in overseas regions do not support switching between Linux and Windows during system reinstallation.

What are the computing components in a CVM bill?

The computing components correspond to instance specifications. Take S5.SMALL4 for example, computing components includes the CPU, memory, and NVMe local 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:

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

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]# runlevel
3
root@VM_168_173_centos network-scripts]#"
6. Verify whether the server's iptables firewall has blocked the access and whether its policy is OK.
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
# ssdh:59.37.
[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 sans
#PAM-1.0
auth  required  pam_sss.so
auth  include  password-auth
auth  required  pam_unix.so
auth  include  password-auth
auth  required  pam_sss.so
auth  include  password-auth
account  required  pam_sss.so
account  include  password-auth
account  required  pam_sss.so
account  include  password-auth
account  required  pam_sss.so
account  include  password-auth
session  required  pam_sss.so
session  include  password-auth
session  required  pam_sss.so
session  include  password-auth
session  required  pam_sss.so
session  include  password-auth
```

**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.

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

   ```
   sudo vi /etc/ssh/sshd_config
   ```
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.
[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.
[root@VM_19_150_centos ~]# echo root:root | chpasswd
[root@VM_19_150.centos ~]# exit
logout
Adjust Configuration


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.
Reinstall System

Last updated: 2019-09-25 12:29:07

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: 2020-04-27 14:46:42

What is Big Data D1 instance?

Big Data D1 instance is designed specifically for Hadoop distributed computing, massive log processing, distributed file system, large data warehouse, and other business scenarios. This CVM instance type is mainly used to solve the cloud computing and storage problems of massive business data.

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

Big Data D1 instance is applicable to customers in the Internet, game, finance and other industries that require big data computing and storage analysis, as well as business scenarios that require massive data storage and offline computing. It can meet the storage, capacity and private network bandwidth requirements of distributed computing businesses represented by Hadoop.

In addition, with the highly available architectural framework of distributed computing businesses represented by Hadoop, Big Data D1 instance features local storage design to achieve a total cost close to that of the self-built Hadoop cluster on an offline IDC, while ensuring massive storage capacity and high performance.

Big Data D1 instance features

- A single instance has throughput capacity up to 2.3 GB/sec. HDD local disk is the best choice for throughput-intensive storage. With stable and high-performing sequential read/write throughput, Big Data D1 instance is designed specifically for Hadoop distributed computing, massive log processing, large data warehouse and other business scenarios.
- Local storage has a unit price as low as 1/10. Big Data D1 instance features massive storage capacity and high performance, while ensuring optimal cost-efficiency for big data scenarios. It has a total cost close to that of the self-built Hadoop cluster on an offline IDC.
- Read/write latency is minimized to 2 ms-5 ms. Big Data D1 instance, with its high-performing and enterprise-level model, is suitable for enterprise developers.
- The billing method of pay-as-you-go is supported.

Big Data D1 instance specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>vCPU (core)</th>
<th>Memory (GB)</th>
<th>Local Data Disk</th>
<th>Private Network Bandwidth</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1.2XLARGE32</td>
<td>8</td>
<td>32</td>
<td>2 × 3720 GB</td>
<td>1.5 Gbps</td>
<td>-</td>
</tr>
<tr>
<td>D1.4XLARGE64</td>
<td>16</td>
<td>64</td>
<td>4 × 3720 GB</td>
<td>3 Gbps</td>
<td>-</td>
</tr>
<tr>
<td>D1.6XLARGE96</td>
<td>24</td>
<td>96</td>
<td>6 × 3720 GB</td>
<td>4.5 Gbps</td>
<td>-</td>
</tr>
<tr>
<td>D1.8XLARGE128</td>
<td>32</td>
<td>128</td>
<td>8 × 3720 GB</td>
<td>6 Gbps</td>
<td>-</td>
</tr>
<tr>
<td>Model</td>
<td>vCPU (core)</td>
<td>Memory (GB)</td>
<td>Local Data Disk</td>
<td>Private Network Bandwidth</td>
<td>Note</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>-------------</td>
<td>-----------------</td>
<td>---------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>D1.14XLARGE224</td>
<td>56</td>
<td>224</td>
<td>12× 3720 GB</td>
<td>10 Gbps</td>
<td>Exclusive for host</td>
</tr>
</tbody>
</table>

**Notes on local data storage for Big Data D1 instance**

Big Data D1 instance uses local disk as the data disk, which may lead to **data loss** (e.g., when the host crashes). If your application cannot guarantee data reliability, we recommend you choose an instance that can use cloud disk as the data disk.

Relationship between operating on an instance with local disk and data retention is as follows:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Local Disk Data Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system restart/Console restart/Forced restart</td>
<td>Retained</td>
<td>Local disk storage is retained. Data is retained.</td>
</tr>
<tr>
<td>Operating system shutdown/Console shutdown/Forced shutdown</td>
<td>Retained</td>
<td>Local disk storage is retained. Data is retained.</td>
</tr>
<tr>
<td>Terminate (instance) on the console</td>
<td>Erased</td>
<td>Local disk storage is erased. No data is retained.</td>
</tr>
</tbody>
</table>

Do not store business data that needs to be retained for a long time on the local disk. Back up data in advance and use a highly available architecture. For long-term retention, we recommend you store the data on CBS disk.

**How can I purchase Big Data D1 local disk?**

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

**Does the local storage of Big Data D1 instance support snapshot?**

No.

**Does Big Data D1 instance support configuration adjustment and failover?**

Configuration adjustment is not supported.

Big Data D1 instance features massive data storage and uses local HDD as data disk. This instance type does not support data disk failover (e.g., when the host crashes or local disk is damaged). To prevent data loss, we recommend you use a redundancy policy, for example, a file system that supports redundancy and fault tolerance (such as HDFS and Mapr-FS). In addition, we recommend you regularly back up data to a persistent storage system, 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 so we can change the local disk. If the CVM instance has crashed, we will notify you and fix it.

**In which regions can I purchase Big Data D1 instance?**

The following availability zones are supported:

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

**Why cannot I find the data disk after purchasing a Big Data D1 instance?**

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

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

High IO I2 instance is a CVM instance designed specifically for business scenarios with low latency and high random IO. It has ultra-high IOPS performance, and is used mainly for high-performing database (relational database, NoSQL, etc.). Big Data D1 instance is a CVM instance designed specifically for business scenarios that require high sequential read/write and low-cost massive data storage. It features high-performing storage with cost efficiency and properly configured private network bandwidth.

**How is the disk throughput of Big Data D1 instance?**

Take D1.14XLARGE224 as an example, sequential read/write throughput of the local disk of Big Data D1 instances is 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 instance and CBS?**

Cloud Block Storage provides a highly efficient and reliable storage device for CVM instance. It is a customizable block storage device with high availability, high reliability and low cost, and can be used as an independent scalable disk for CVM. It provides data storage at the data block level and employs a 3-copy distributed mechanism to ensure data reliability for CVM instance, meeting the requirements of different application scenarios. The local disk of Big Data D1 instance is designed specifically for business scenarios that require high sequential read/write for massive local data sets, such as Hadoop distributed computing, large-scale parallel computing, and data warehouse.
Spot Instances

Last updated: 2020-04-28 14:30:35

Instance Release

Why is a spot instance released automatically?

An important feature of spot instances is that the system will repossess assigned instances based on prices or the supply-demand relationship. If the market price is higher than your bid or if the CVM resource pool corresponding to your spot instances is in short supply, the process will be interrupted by the system.

Is it possible to avoid being repossessed by the system through bidding?

No. Because repossession trigged by insufficient inventory is unavoidable. You need to accept that instance repossession may occur when you deploy businesses on the spot instance.

How do I know that an instance is about to be interrupted?

Two minutes before the interruption, we will notify you in the form of metadata that the instance is about to be interrupted and repossessed.
For more information, please see Querying the Repossession Status of a Spot Instance.

How to automatically apply for spot instances after inventory recovery?

You can use cloud products that can automatically maintain the CVM cluster, such as [BatchCompute](http://console.cloud.tencent.com/batch/env), [Auto Scaling](http://console.cloud.tencent.com/autoscaling). With their cross-model and cross-availability zone capabilities, you can maintain a specified number of CVM clusters more effectively.

Price and Billing

What are the similarities and differences between spot instances and pay-as-you-go instances?

<table>
<thead>
<tr>
<th>Billing Method</th>
<th>Similarities</th>
<th>Differences</th>
</tr>
</thead>
</table>
| Spot instances          | Both of them are pay-as-you-go. There is no need to pay in advance but certain costs must be frozen. You can enable/terminate the CVM at any time and pay according to actual usage. The billing time granularity is accurate to the second, and the account will be settled every hour. | • **Price**: In most cases, the spot instance price is 10%-20% of the pay-as-you-go instance price with the same specifications.  
  • **Release mechanism**: The lifecycle of a pay-as-you-go instance is controlled by the user, while spot instance may be actively repossessed by the system. |
| Pay-as-you-go instances  |                                                                               |                                                                             |
**Feature limitations**: Configuration adjustments are not allowed.

**Which price, the market price and the highest bid specified by the user, will be used for billing?**

The market price will be used for billing. You can specify a high bid to prevent instances from being repossessed due to the price. However, the system will only charge you at the current market price (the current market price will be fixed).

**How are billing periods calculated for spot instances?**

You will be billed for the period from the moment you apply for a spot instance to the moment the spot instance is manually released or interrupted by the system. The billing period is accurate to the second.

**Where can I find the current market prices of all the spot instances?**

During the beta testing period, we cannot provide a page where you can query the market prices of all instances, but it will be available in the future. Currently, most of the spot instances will be priced at 20% of the regular pay-as-you-go instances of the same model and specification.

**Where can I view the consumption details regarding spot instances?**

As with pay-as-you-go instances, you can find detailed usage and billing information of spot instances in Billing Center > Bills at the top of the console. Spot instances are pay-as-you-go services.

## Quotas and Limitations

### In which regions are spot instances available? Which instance models and specifications do spot instances support?

<table>
<thead>
<tr>
<th>Region</th>
<th>Models supported by spot instances</th>
<th>Discounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beijing, Shanghai, Chengdu, Chongqing, Guangzhou Open</td>
<td>All models supported by pay-as-you-go instances</td>
<td>80% off the published prices of pay-as-you-go instances with the same specifications</td>
</tr>
<tr>
<td>Guangzhou (excluding Guangzhou Zone 1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hong Kong (China), Singapore, Bangkok, Seoul, Tokyo, Mumbai, Toronto, Silicon Valley, Virginia, Frankfurt, Moscow</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Are quota limits of spot instances shared by pay-as-you-go instances?**

No. Each user can have up to 50 spot instance vCPU cores in each availability zone. To raise the quota limits, please submit a ticket.

**Can I upgrade or downgrade the specifications of spot instances?**
Upgrading or downgrading the specifications of spot instances is not supported.

Do spot instances support no charges when shut down?
Spot instances do not support no charges when shut down.

Do spot instances support system re-installation?
Spot instances do not support system re-installation.
How do I view CVMs that are in use?
You can log in to the CVM Console to view CVMs that are currently in use.

Can 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 if I cannot find my CVM on the console?
If your CVM is not shown on the console, verify the following:
1. Check the recycle bin to verify whether the instance has expired.
2. Check whether the instance has been terminated because it has expired for more than 7 days.
3. Check 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?
For more information, see Shutdown Instances.

How do I restart an instance?
For more information, see Restart Instances.

What if I fail to connect (log in) to an instance after restarting it?
This may be caused by high CPU and memory usage of your server. Please see the following documents:
- Failed to log in to a Linux CVM due to high CPU and memory usage
- Failed to log in to a Windows CVM due to high CPU and memory usage

How do I terminate an instance?
For more information, see Terminate Instances.
What is the default capacity of a CVM system disk?
The system disk of a new CVM has 50 GB free space by default.

Can I change the local system disk of a CVM to a cloud disk?
- When purchasing a CVM instance, you can select the desired disk type for the CVM system disk.
- For a purchased CVM instance, if the availability zone where the purchased CVM is located has available cloud disks, you can use the change disk media type feature to change the local system disk to a cloud disk.

Which regions and availability zones support expanding the system disk capacity to more than 50 GB?
If the system disk is a cloud disk, the system disk capacity can be adjusted to more than 50 GB in all regions that support snapshots.

Can I expand the system disk capacity of a CVM when reinstalling the operating system?
It depends on the system disk type.
- If the system disk is a cloud disk, the system disk capacity can be increased but cannot be decreased.
- If the system disk is a local disk, it depends on the system disk size.
  - If the default system disk capacity of the purchased instance is 50 GB, the system disk cannot be expanded.
  - For instances purchased at an earlier time: if the system disk capacity is 20 GB or less, the system disk can be expanded to 20 GB by default. If the system disk capacity is more than 20 GB, the system disk can be expanded to 50 GB by default.

How do I expand the capacity of a cloud disk?
If your CVM uses a cloud disk, the cloud disk is expandable. For details on how to expand a cloud disk, see Expanding Cloud Disks.

Can I increase the system disk capacity and then reinstall the operating system to decrease the system disk capacity?
The capacity of a system disk cannot be decreased.

How do I save the data on the CVM instance and then expand the system disk capacity?
To expand the system disk capacity, you can create an image and then use the image to reinstall the operating system.

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

The image capacity does not affect the system disk capacity. The minimum system disk capacity is 50 GB.

**How can I check the data disk?**

1. Log in to the **CVM console**.
2. Click **Cloud Block Storage** in the leftside bar to go to the cloud disk management page.
3. Click the **Attribute** column, select **Data Disk**, and click **OK**. Then, you can view all data disks in relevant regions.

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

A Windows file system normally adopts the NTFS or FAT32 format, whereas a Linux file system usually adopts the EXT series format. When the operating system of a CVM is changed from Windows to Linux, the data disk format remains unchanged. As a result, the operating system may be unable to access the file system of the data disk. If this is the case, you need to use a format converter to read data from the data disk. For details, see **Reading or Writing NTFS Data Disks After Changing a Windows CVM to a Linux CVM**.

**How do I read data from the original EXT data disk after the operating system is changed from Linux to Windows?**

A Windows file system normally adopts the NTFS or FAT32 format, whereas a Linux file system usually adopts the EXT series format. When the operating system of a CVM is changed from Linux to Windows, the data disk format remains unchanged. As a result, the operating system may be unable to access the file system of the data disk. If this is the case, you need to use a format converter to read data from the data disk. For details, see **Reading or Writing EXT Data Disks After Changing a Linux CVM to a Windows CVM**.
Backup and Restore

How do I back up data for CVM?

- 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, see Create Custom Images.
  - For more information on how to create a snapshot, please see Creating Snapshots
- If your CVM uses a local disk, you can back up data on system disk by creating a custom image. For business data in your data disk, you still need to customize the backup policy.
  You can use FTP to back up data in the server to other places. For specific FTP deployment methods, see:
  - For Windows: Build the FTP Service (Windows)
  - For Linux: Build the FTP Service (Linux)

What are common data backup and recovery solutions?

The data backup and recovery solutions vary by application scenarios and businesses. The following recommendations can be used based on your actual needs:

- Back up the instance regularly using the CBS Snapshot feature.
- Deploy key components of an application across multiple availability zones, and copy the data as needed.
- Use Elastic Public IP for domain name mapping to ensure that the service IP can be quickly redirected to another CVM instance when the server is unavailable.
- View the monitoring data regularly and configure corresponding alarms. For more information, please see Cloud Monitor.
- Process emergency requests with auto scaling. For more information, please see Auto Scaling.
What is image?
Image is the template for CVM software configuration (operating system, pre-installed programs, etc.). Tencent Cloud requires users to launch the instance via image. An image can launch more than one instance so that users can repeatedly use it. For more information on image, please see Image Overview.

What preparations do I need to make before importing an image?
Before importing an image, two major steps need to be completed: applying for permissions and preparing image files. For more information, please see Import Image.

What if a Windows system custom image fails to be created?
If a Windows system image fails to be created, perform a check following the steps below.
(1) Check and make sure the following services and all the services coming from the official source of Tencent Cloud and starting with Win_Agent are working properly:

<table>
<thead>
<tr>
<th>Program Name</th>
<th>Installation Location</th>
<th>Service Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>QcloudService.exe</td>
<td>C:\Windows\</td>
<td>Qcloud service</td>
</tr>
<tr>
<td>WinAgent.exe</td>
<td>C:\WinAgent\</td>
<td>WinAgent Display Name</td>
</tr>
<tr>
<td>win-agent.exe</td>
<td>C:\win-agent\</td>
<td>win-agent</td>
</tr>
</tbody>
</table>

(2) The creation of a custom image relies on the Windows Modules Installer provided by Microsoft. Make sure this service is working properly.

(3) Some anti-virus tools or Safedog may block custom image creation scripts. To avoid creation failure, it is recommended that you close these tools before creating a custom image.

(4) If the image creation tool is interrupted by system pop-ups, remotely log in to the CVM, and then check and adjust the CVM settings to avoid pop-ups.

To how many users can each image be shared at most?
50.

Can the name and description of a shared image be changed?
No.

Does a shared image take up my image quota?
No.
Is there any region limitation on a shared image when creating and reinstalling a CVM?
Yes, there is. The shared image should be in the same region as the source image, and the CVM can only be created and reinstalled in the same region.

Can a shared image be copied to other regions?
No.

Can a custom image that has been shared to other users be deleted?
Yes, but you should cancel all the sharing for this custom image first.

Can an image shared by other users be deleted?
No.

What are the risks of using custom images shared by other users?
Tencent Cloud does not guarantee the integrity and security of images shared by other users. Please select the images shared by a trusted account.

Can I share the image another user shared to me to other users?
No.
Cloud-init

What is cloud-init?
Cloud-init is an open source tool that runs inside a CVM instance as a non-resident service. It is executed at startup and exits immediately after execution. It does not listen to any ports. All the Linux public images of Tencent Cloud are pre-installed with the cloud-init service. You need to run the service as the root user because the service is mainly used for the initialization of CVM instances such as configuring DNS, hostname, and IP, and the execution of some custom scripts that users specify to be executed during the first boot when creating the CVM instances.

How do I check whether the cloud-init service inside a Linux instance is working properly?

Checking the operation of cloud-init
First, log in to the instance and execute the following commands to see if any error is returned. If the execution result is returned, it means that the service is running normally. Otherwise, an error will be returned. Please troubleshoot according to the error message.

1. Delete the cloud-init cache directory.
   ```
   rm -rf /var/lib/cloud
   ```
2. Perform complete cloud-init initialization.
   ```
   cloud-init init --local
   ```
3. Pull data from the configured data source.
   ```
   cloud-init init
   ```
4. Cloud-init initialization involves multiple stages. To ensure sufficient dependency between the stages, config stage is specified for the cloud-init modules.
   ```
   cloud-init modules --mode=config
   ```
5. Specify final stage for the cloud-init modules.
   ```
   cloud-init modules --mode=final
   ```

What initialization operations does cloud-init perform on instances?
Tencent Cloud implements all instance initialization operations through cloud-init, ensuring the transparency of the operations inside an instance. The following briefly covers some initialization operations. For more details,
see cloud-init documentation.

<table>
<thead>
<tr>
<th>Initialization operation</th>
<th>Default behavior</th>
<th>Customization</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname initialization</td>
<td>During the first boot of an instance, cloud-init will set the hostname of the instance according to the hostname information in vendor_data.json.</td>
<td>If you create or reinstall an instance with a custom image and you want to keep the custom hostname of the image, you can delete the configuration, -scripts-user, from /etc/cloud/cloud.cfg before creating the custom image.</td>
<td>After you disable -scripts-user, the initialization script, /var/lib/cloud/instance/scripts/runcmd, inside the instance will not be run. Disabling the configuration will also affect the initialization of other sub-items such as the installation of cloud monitor and cloud security and software source settings. Also, the custom script will not be run when you create the CVM.</td>
</tr>
<tr>
<td>/etc/hosts initialization</td>
<td>During the first boot of an instance, cloud-init will initialize /etc/hosts to 127.0.0.1 $hostname by default.</td>
<td>If you create or reinstall an instance with a custom image and you want to keep the custom /etc/hosts setting of the image, you can delete the configuration, -scripts-user, from /etc/cloud/cloud.cfg before creating the custom image.</td>
<td>- After you disable -scripts-user, the initialization script, /var/lib/cloud/instance/scripts/runcmd, inside the instance will not be run. Disabling the configuration will also affect the initialization of other sub-items such as the installation of cloud monitor and cloud security and software source settings. Also, the custom script will not be run when you create the CVM. - Every time the CVM restarts, the /etc/hosts settings of some existing CVMs will be overwritten. To solve the issue, see Modifying etc/hosts Configuration of Linux Instance.</td>
</tr>
<tr>
<td>DNS initialization (non-DHCP scenario)</td>
<td>During the first boot of an instance, cloud-init will set the DNS of the instance according to the nameservers information in vendor_data.json.</td>
<td>If you create or reinstall an instance with a custom image and you want to keep the custom DNS setting of the image, you can delete the configuration, -resolv_conf and unverified_modules: ['resolv_conf'], from /etc/cloud/cloud.cfg before creating the custom image.</td>
<td>None.</td>
</tr>
<tr>
<td>Software source initialization</td>
<td>During <strong>the first boot</strong> of an instance, cloud-init will set the software source of the instance according to the <code>write_files</code> information in <code>vendor_data.json</code>.</td>
<td>If you create or reinstall an instance with a custom image and you want to keep the custom software source setting of the image, you can delete the configuration, <code>-write-files</code>, from <code>/etc/cloud/cloud.cfg</code> before creating the custom image.</td>
<td>None.</td>
</tr>
<tr>
<td>NTP initialization</td>
<td>During <strong>the first boot</strong> of an instance, cloud-init will set the NTP server configuration of the instance according to the NTP server information in <code>vendor_data.json</code> and start the NTP service.</td>
<td>If you create or reinstall an instance with a custom image and you want to keep the custom NTP configuration of the image, you can delete the configuration, <code>-ntp</code>, from <code>/etc/cloud/cloud.cfg</code> before creating the custom image.</td>
<td>None.</td>
</tr>
<tr>
<td>Password initialization</td>
<td>During <strong>the first boot</strong> of an instance, cloud-init will set the default account password of the instance according to the <code>chpasswd</code> information in <code>vendor_data.json</code>.</td>
<td>If you create or reinstall an instance with a custom image and you want to keep the custom default password of the image, you can delete the configuration, <code>-set-passwords</code>, from <code>/etc/cloud/cloud.cfg</code> before creating the custom image.</td>
<td>None.</td>
</tr>
<tr>
<td>Key binding</td>
<td>During <strong>the first boot</strong> of an instance, cloud-init will set the default account key of the instance according to the <code>sshAuthorizedKeys</code> information in <code>vendor_data.json</code>.</td>
<td>If you create or reinstall an instance with a custom image and you want to keep the custom default key of the image, you can delete the configuration, <code>-users-groups</code>, from /etc/cloud/cloud.cfg before creating the custom image.</td>
<td>If you manually bind the instance to a key inside the instance, the previous key will be overwritten when the key binding operation is performed via the console.</td>
</tr>
</tbody>
</table>
### Network initialization (non-DHCP scenario)

During **the first boot** of an instance, cloud-init will set the IP, Gateway, Mask, etc., according to the information in `/etc/cloud/network_data.json`.

If you create or reinstall an instance with a custom image and you want to keep the custom network information of the image, you can add `network: {config: disabled}` to `/etc/cloud/cloud.cfg` before creating the custom image.

None.

### How do I fix issues related to cloud-init?

1. **Error due to the uninstallation of the cloud-init dependencies**
   - **Problem description:**
     When commands are used to check whether the cloud-init service is working properly, the following error is returned:

     ```
     Traceback (most recent call last):
     File "/usr/bin/cloud-init", line 5, in 
     DistributionNotFound(req)
     pkg_resources.DistributionNotFound: pyyaml
     ```
   
   - **Problem analysis:**
     “pkg_resources.DistributionNotFound: xxxxx” indicates that the cloud-init dependencies have been uninstalled.
   
   - **Solution:**
     - Reinstall the dependencies.
     - Follow Checking the operation of cloud-init to see if the error is returned again.

2. **Error due to the modification of the default Python interpreter**
   - **Problem description:**
     An error is returned when cloud-init is run on startup.
   
   - **Problem analysis:**
     When cloud-init is installed, Python 2 is used as the default Python interpreter, which means that symbolic links, `/usr/bin/python` and `/bin/python`, are linked to Python 2. Users may change the default Python interpreter to Python 3 inside the instance by directing the symbolic links, `/usr/bin/python` and `/bin/python`, to Python 3. Due to compatibility issues, an error will be returned when cloud-init is run on startup.
   
   - **Solution:**
     [Further details on solving this issue]
i. Modify the Python interpreter specified in the `/usr/bin/cloud-init` file by changing `#/usr/bin/python` or `#/bin/python` to `#!/user/bin/python`.

Do not use symbolic links. Point directly to a specific interpreter.

ii. Follow Checking the operation of cloud-init to see if the error is returned again.

**Cloudbase-Init**

**What is Cloudbase-Init?**

Like cloud-init, Cloudbase-Init is a bridge by which you can communicate with Windows CVM instances. The Cloudbase-Init service is run when an instance boots up for the first time. The service will read the initialization configuration information of the instance and initialize it. Following operations such as resetting password and modifying IP addresses are also done via Cloudbase-Init.

**How do I check whether the Cloudbase-Init service inside a Windows instance is working properly?**

**Checking the operation of the Cloudbase-Init service:**

1. Log in to the instance.

If you forget your password or fail to reset your password because of Cloudbase-Init service exceptions, you can reset your password by following step 2.

2. Open Control panel > Administrative tools > Services.
3. Find the Cloudbase-Init service, right-click it, and go to Properties.
   - Check “Startup type” and make sure it is set to “Automatic”.
   - View “Logon identity” and ensure that “Local System account” is selected.
   - Manually start the Cloudbase-Init service and see if any error is returned.
     - If any error is returned, you need to fix the issue first and check whether you have installed any security software which may stop Cloudbase-Init from performing related operations.
   - Open the registry, locate all “LocalScriptsPlugin”, and make sure its value is 2.
   - Check whether CD-ROM loading is disabled. If there is an optical disc drive as shown in the figure below, it means that the loading has not been disabled; otherwise, it means that it has been disabled and needs to be enabled.

**How do I fix common issues related to Cloudbase-Init?**

**Failed to reset password during initialization**

- Possible reasons:
The Cloudbase-Init account password is manually changed, which results in the failure to start the Cloudbase-Init service, which further led to the failure of operations such as resetting password during initialization.

The Cloudbase-Init service is disabled, which led to the failure of operations such as resetting password during initialization.

The security software installed stops the Cloudbase-Init service from resetting password so that the operation returns a successful result but actually failed.

Solution:

Follow the corresponding solution to each possible reason to fix the issue.

i. Change the Cloudbase-Init service to LocalSystem service. For details, see step 2 in Checking the operation of the Cloudbase-Init service.

ii. Change the startup type of the Cloudbase-Init service to automatic. For details, see step 2 in Checking the operation of the Cloudbase-Init service.

iii. Uninstall the security software involved or add the relevant operations of the Cloudbase-Init service to the white list of the security software.
About Network

Network

Last updated : 2019-09-25 14:40:01

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.
**IP Address**

Last updated: 2020-04-24 14:27:24

**What is a public IP address?**

For details, see Public IP Addresses in Public Network Service.

**What is a private IP address?**

For details, see Private IP Addresses in Private Network Service.

**How can I obtain the public IP address of an instance?**

For details, see Obtaining the Public IP Address of an Instance.

**How can I obtain the private IP address of an instance?**

For details, see Obtaining the Private IP Address of an Instance and Private Network DNS Settings.

**How can I change the public IP address of an instance?**

For details, see Changing the Public IP Address of an Instance.

**What are the differences between public gateways and CVMs with public IP addresses?**

Public gateways enable the public network traffic forwarding feature in the image. However, CVMs with public IP addresses do not have the traffic forwarding feature by default. CVMs that use the Windows public image cannot function as public gateways because the traffic forwarding feature is disabled in the Windows image.
Elastic Public IP

What are EIPs used for?

EIPs are applicable to the following scenarios:

- Disaster recovery. We strongly recommend you use EIPs for disaster recovery. For example, when one of your servers fails, you can unbind the EIP from this server and then bind it to a healthy server to quickly resume services.
- Retaining a specific public IP. If you need to retain a specific public IP under your account, you can convert it to an EIP, which can be unbound/bound with the device and used to access the public network. This EIP will be retained under your account until you "release" it.
- Other special cases. When you need to change an IP in some cases, you can convert the public IP to an EIP and then bind/unbind the EIP. With limited EIP resources available, however, each account has an EIP quota for each region. Please use and plan accordingly.

How is an EIP billed?

1. The fee displayed on the console applies to EIPs that have been idle for more than 1 hour. EIPs can be billed with an accuracy down to seconds. EIPs that have been bound/unbound multiple times are billed based on the total duration (in sec) for which they are unbound.
2. EIPs that have been idle for less than 1 hour are billed for resource occupation fee 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 billed for a small usage fee only when it is unbound.

How do I stop EIP billing?

- When you no longer need an EIP, you can release it to stop the billing. For more information on the specific operations, see Releasing EIPs.
- If you need to retain an EIP but want to stop the billing, bind it to a device (CVM, NAT). A bound EIP will not be billed.

How can a CVM without public IP access public network?

If you did not purchase the public IP when purchasing the 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 public network access.

Can I change my public IP?

You can change the public IP of your CVM. For more information on the specific operations, please see Change Instance Public IP.

How do 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 can be bound to the device and used to access the public network. This EIP will be retained under your account until you released it.

For more information on the related operations, see Elastic Public IP.

**Can an EIP be converted back to a public IP?**

An EIP cannot be converted back to a public IP.

**Can an EIP be retrieved?**

You can retrieve public IPs that have not been assigned to other users. For details, see Retrieve the public network IP address.
Elastic Network Interface

Last updated: 2020-04-27 14:47:19

What is ENI?

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

ENI has VPC, availability zone and subnet attributes. You can only bind it to CVMs under the same availability zone. A CVM can be bound with multiple ENIs, and the maximum number allowed varies by CVM specifications.

What are the restrictions to use ENIs on CVMs?

For details, please see use limits section in Use Limits Overview.

What is the basic information of an ENI?


How do I create an ENI?

Please see Creating an ENI.

How do I view the ENI information?

Please see Viewing ENI Information.

How do I bind an ENI to a CVM instance?

Please see Binding and Configuring CVMs.

How do I configure an ENI in the CVM instance?

Please see Binding and Configuring CVMs.

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

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

1. Log in to VPC Console.
2. In the left side bar, click **IP and Interface** > ENI to enter the ENI list page.
3. Click the **ID/Name** of an ENI to enter its details page to view its information.
4. Select the **IPv4 address management** tab and click **Assign Private IP**.
5. In the pop-up window, select the IP assigning method as **Enter manually** to enter the IP address you want to modify.
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 CVMs.
About Security

Password Login and SSH Key Login

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

An SSH key allows you to log into Linux server remotely. It uses the key generator to create a key pair (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 focuses on data security and is more convenient than the manual input of the traditional password login method. Currently, Linux instance supports both password and SSH key login, while Windows instance supports only password login. For related documentation, see:

- Log in to Linux Instance
- Log in to Windows Instance

Can I use SSH key and password logins at the same time?

When you log into Linux instance via SSH key, password login is disabled by default to improve security.

What should I do if I forget my password?

You can reset the password. For details, see Reset Instance Password.

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

For more formation on key creation, please see Managing SSH keys.
If you lose the key, resolve by the following two methods:

- Create a new key through SSH Key on the console and bind it with the original instance.
  - i. Create an SSH key.
  - ii. After the key is successfully created, log in to the CVM Console.
  - iii. Select the original instance with which you want to bind the key, click More > Password/key Load a key.
    Then you can use the new key to log into the instance.
- After the key is successfully created, log in to the CVM Console.
  Then you can use the new key to log into the instance.
  - Reset your password through the CVM console and log into the instance with your new password. For details, see Reset Instance Password.

How do I bind/unbind an SSH key to or from the server?

Please see the Binding/Unbinding a key to or from a CVM section in Managing SSH keys.

How do I modify the SSH key name/description?

Please see the Modifying the SSH key name and description section in Managing SSH keys.

How do I delete an SSH key?

Please see the Deleting SSH keys section in the Managing SSH keys.
What are the use limits on SSH keys?
Please see the Use Limits section in SSH Key.

How to troubleshoot if I fail to log into a Linux instance using an SSH key?
Please see Unable to Log into a Linux Instance via SSH.
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

![Security Groups Console](image)
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:
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Unsupported Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>42 135 137 138 139 445 593 1025 1434 1068 3127 3128 3129 3130 4444 5554 9996</td>
</tr>
<tr>
<td>UDP</td>
<td>1026 1027 1434 1068 5554 9996 1028 1433 135 ~ 139</td>
</tr>
</tbody>
</table>

**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:

```json
{
  "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:

```json
{
  "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.
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:

```json
{
  "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.
About Service migration

Last updated: 2020-02-10 17:22:35

Offline Migration

COS upload and migration take too long?
The upload time is related to the size of the image file and bandwidth. We recommend you use compressed image formats (qcow2 or vhd) to reduce transfer and migration time.

Why does the migration fail?
- Tencent Cloud's service migration currently supports the following image formats: qcow2, vpc, vmdk, raw. Please confirm your image has one of these formats.
- Please confirm your image file has already been uploaded to COS, and the file is not damaged nor corrupted.
- Please make sure the target CVM/cloud disk is in normal use. Expired devices cannot be migrated.

Online Migration

What operating systems and disk types are supported?
- Mainstream Linux operating systems (CentOS, Ubuntu, etc.) and Windows are supported.
- Migration is not related to disk type and usage.

Where can I download the tool?
Currently, the online migration tool cannot be downloaded. If you have such needs, please contact your sales rep or submit a ticket to apply for permission, and obtain the related documentation.

How to use the tool?
The migration tool must be copied to the source server. You need to modify the configuration files based on the state of the machines and you can write a script to perform batch processing.

Do I need to retain the tool after migration is complete?
No, you do not need to retain the tool. Once migration is complete, you can directly delete the tool on the source server.

What about migration speed and cost?
- Speed: This primarily depends on the bandwidth of the target CVM. We tested a 1u1g pay-as-you-go CVM with 100mbps of bandwidth, and the migration rate was around 12MB/second. The actual migration rate will be about 9MB/second.
- Cost: The migration tool is free to use, but data transfer passes through the public Internet. Based on traffic and duration, you will be charged for a small amount for resources used during migration. For details, please
Can I migrate multiple CVMs at the same time?

Yes, migration of multiple CVMs at the same time is supported. As they are migrated to different destination CVMs, they are not interrelated.
How do I view regions and availability zones?

To view regions and availability zones, use either of the following methods:

- View the [Regions and Availability Zones](#) document.
- Use APIs:
  - To view regions, use the DescribeRegions API.
  - To view availability zones, use the DescribeZones API.

Can I change the region of a purchased CVM?

No. You cannot change the region of a purchased CVM or the availability zone for a started CVM. To change the region and availability zone, use either of the following methods:

- Create a custom image for the original instance. Then, in a new availability zone, use the custom image to create an instance, start the created instance, and update the instance configuration.
  1. Create a custom image for the current instance. For details, see [Creating Custom Images](#).
  2. If the network environment of the current instance is a VPC instance and the private IP address needs to be retained after the instance is migrated to another availability zone, delete the subnet in the current availability zone and then create a subnet in the new availability zone with the same IP address range as that of the original subnet.

If the subnet to be deleted contains available instances, first migrate all these instances in the subnet to the new subnet.

iii. Use the created custom image to create an instance in the new availability zone.

You can use the same instance type and configuration as those of the original instance. Also, you can modify them for the new instance. For details, see [Creating an Instance](#).

iv. If an elastic public IP address is associated with the original instance, dissociate it from the original instance and associate it with the new instance. For details, see [Elastic Public IP Addresses (EIPs)](#).

v. (Optional) If the billing method of the original instance is pay-as-you-go, you can terminate it. For details, see [Terminating Instances](#).