

Cloud Virtual Machine

Operation Guide

Product Introduction



Copyright Notice

©2013-2018 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 the 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

Operation Guide

- Operation Guide Overview

- Use Limits Overview

- Instances

 - Purchase and Start Instances

 - Log into Instances

 - Log into Linux Instances

 - Log into Windows Instances

 - Change Specifitaion

 - Change CVM Specifitaion

 - Adjust Network Configuration

 - Adjust Project Configuration

 - Network Configuration after Creating an Instance Using Imported Windows Image

 - Query Info

 - Query Instance Info

 - Query Instance Monitoring Info

 - Instance Metadata

 - Modify Instance Name

 - Reset Instance Password

 - Change Instance Subnet

 - Change Security Group

 - Search Instance

 - Export Instances

 - Renew Instances

 - Shutdown Instances

 - Restart Instances

 - Reinstall System

 - Terminate Instances

 - Instance Expires

- Images

 - Create Custom Images

 - Copy Images

 - Share Custom Images

 - Cancel Image Sharing

 - Delete Custom Images

Import Images

- Overview

- Linux Image Production

- Windows Image Production

- Linux System Check virtio Driver

- Forcibly Import Image

Network and Security

- Protection of Sensitive Operations

- SSH Key

- Distributed Placement Group

- Elastic Public IP

- EIP Direct Connection

- Security Groups

- Limits

- Operation Guide

- Server Common Port

Monitoring and Alarms

- Get Monitoring Statistics

- Create Alarm Policies

Access Control

- Console Example

Operation Guide

Operation Guide Overview

Last updated : 2018-08-01 17:34:32

When using the CVM, you may perform various operations, such as logging in, reinstalling operating system, adjusting configuration and resetting password, etc. This document provides an overview of CVM instance and describes how to work with CVM-related products for your reference.

Instance

[CVM Instance](#) is also known as Cloud Virtual Machine instance. Tencent Cloud CVM instance supports customizing all resources, including CPU, memory, disk, network, security, etc. It also allows easy adjustment of the resources in case of any change in visits, load and other demands. Common features supported by CVM instance are provided as follows:

Common operations

- [Create Instance](#)
- Log in to an instance
 - [Log in to Linux Instance](#)
 - [Logging in to a Windows Instance](#)
- [Search for Instance](#)
- [Restart Instance](#)
- [Shut Down Instance](#)
- [Terminate Instance](#)
- [Reclaim Instance](#)

Modifying instance attributes

- [Reset Password](#)

- Adjust configurations
 - [Adjust Instance Configuration](#)
 - [Adjust Network Configuration](#)
 - [Adjust Project Configuration](#)
- [Modify Instance Name](#)
- Modify IP
 - [Modify Private IP](#)
 - [Modify Public IP](#)
- [Change Subnet of Instance](#)
- [Change Security Group](#)
- [Reinstall Operating System](#)

Billing

- [Renew Instance](#)
- [Switch from Postpaid to Prepaid](#)

Image

An [Image](#) provides all information required to launch a CVM instance. In another word, an image is the installation disk of a CVM. Tencent Cloud provides four types of images: public image, service marketplace image, custom image and shared image. Common operations supported by image are described as follows.

Common operations

- [Create Custom Image](#)

- [Delete Custom Image](#)
- [Import Image](#)
- [Copy Image](#)

Sharing image

- [Share Image](#)
- [Cancel Image Sharing](#)

Security Group

[Security Group](#) is an important means of network security isolation provided by Tencent Cloud. It is a stateful virtual firewall for filtering packets and is used to set the network access controls for a single or multiple CVMs. The following describes common operations supported by security group and how to set the security group in typical scenarios to meet your business needs. Overview of common ports is provided at the end of this section for your reference.

Common operations

- [Creating a security group](#)
- [Deleting a security group](#)
- [Cloning a security group](#)
- [Adding rules to security group](#)
- [Configuring a security group to associate with CVM instances](#)
- [Importing/exporting security group rules](#)

Configuration in typical scenarios

- [Remotely Log in to Linux Instance via SSH](#)

- [Logging in to a Windows Instance via MSTSC](#)
- [Ping Public IP of Instance](#)
- [Use Instance as Web Server](#)
- [Use Instance as FTP Server](#)
- [Overview of Common Ports](#)

EIP

[Elastic IP Address \(EIP\)](#) is also known as elastic IP. It is a static IP designed for dynamic cloud computing, and a fixed public IP in a certain region. With EIPs, you can quickly remap an address to another instance in your account (or NAT gateway instance) to block instance failures. Common operations supported by EIP are provided as follows.

Common operations

- [Applying for EIPs](#)
- [Releasing EIPs](#)
- [Binding instances](#)
- [Unbinding instances](#)
- [Adjusting bandwidth](#)
- [Converting public IPs to EIPs](#)

SSH Key

Common operations

- [Creating SSH keys](#)

- [Deleting SSH keys](#)
- [Binding/unbinding instances](#)
- [Modifying name/description](#)
- [Logging in to a Linux instance using a key](#)

Use Limits Overview

Last updated : 2018-08-06 11:25:17

Account Limits for Purchasing CVM Instances

- You need to sign up for a Tencent Cloud account. For more information, please see [Sign up for Tencent Cloud](#) for registration instructions.
- You need to go through identity verification. For more information on how to verify your identity, please see [Identity Verification Guide](#).
- When you create a postpaid CVM, the system will freeze the CVM fee for one hour. Make sure that the account has sufficient balance to pay for the order.

Use Limits for CVM Instances

- Virtualized software cannot be installed or re-virtualized (such as installing VMware or Hyper-V).
- You cannot use sound card applications or external hardware devices (such as ISO files, USB disks, external disks and U-keys).
- The public gateway is available only in Linux systems.

Purchase Limits for CVM Instances

- For each user in each availability zone, the monthly quota for newly purchased prepaid CVM instances (not net increase) is 150.
- For each user in each availability zone, the **total quota** for postpaid CVM instances is 30.
- For more information, please see [Purchase Limits for CVM Instances](#).

Image Limits

- Public image and service marketplace image: none.
- Custom image: Each region supports a maximum of 10 custom images.
- Shared image: Each custom image can be shared to a maximum of 50 Tencent Cloud users, and can only be shared to the accounts in the same region as the source account.

- For more information, please see [Image Type Limits](#).

ENI Limits

- The number of ENIs bound to a CVM is quite different from that of private IPs bound to an ENI depending on the CPU and memory configurations. These allowed numbers are shown in the following table:

CVM Configuration	Max. Number of ENIs	Max. Number of IPs Bound to Each ENI
CPU: 1-core Memory: 1 GB	2	2
CPU: 1-core Memory: > 1 GB	2	6
CPU: 2-core	2	10
CPU: 4-core Memory: < 16 GB	4	10
CPU: 4-core Memory: > 16 GB	4	20
CPU: 8- to 12-core	6	20
CPU: >12-core	8	30

Bandwidth Limits

- Upper Limit of the Outbound Bandwidth (Downstream Bandwidth):

Network Billing Method	CVM		Available range of the upper limit of bandwidth (Mbps)
	CVM Billing Method	CVM Configuration	
Bill-by-Traffic	Postpaid CVM	ALL	0-100
		Cores \leq 8	0-200
	Prepaid CVM	8 < Cores < 24	0-400
		Cores \geq 24	0-400 or no speed limit
Bill-by-	Postpaid	ALL	0-100

Bandwidth	CVM		
	Prepaid CVM	Guangzhou Zone 1 Guangzhou Zone 2 Shanghai Zone 1 Hong Kong Zone 1 Toronto Zone 1	0-200
		Other availability zones	0-1,000
Shared bandwidth	ALL		0-200 or no speed limit

- Upper Limit of the Inbound Bandwidth (Upstream Bandwidth):
 - If the fixed bandwidth purchased by users is larger than 10 Mbps, Tencent Cloud assigns the public network inbound bandwidth that is equal to the purchased bandwidth.
 - If the fixed bandwidth purchased by users is less than 10 Mbps, Tencent Cloud assigns 10 Mbps public network inbound bandwidth.

Disk Limits

Limits on	Description
Relevant CBS APIs	If an API's name contains "Elastic cloud disk", it means this API can only operate on elastic cloud disks (for example, mounting elastic cloud disks). If the name doesn't contain "Elastic cloud disk", it can operate on all cloud storage (for example, modifying cloud disk attributes).
Elastic cloud disk capability	Since November, 2017, all prepaid data disks that are purchased along with CVM are elastic cloud disks. You can unmount them from your CVM and get them remounted. This capability is available in all Availability Zones .

Limits on	Description
Regions where SSD Cloud Storage is commercially available	SSD Cloud Storage is commercially available in Guangzhou, Shanghai, Beijing, Singapore, Silicon Valley, and Finance Zone.
Cloud disk performance	The I/O performance described in the product documentation. For example, a 1 TB SSD cloud disk can deliver up to 24,000 random IOPS. This means the 24,000 IOPS is achievable for both read and write operations. The I/O performances of 4 KB/8 KB can both reach this number, while the IO of 16 KB cannot reach 24,000 IOPS because its throughput has already reached the limit of 260 MB/s.
Maximum number of elastic cloud disks under a single account	500 at most
Maximum number of elastic cloud disks that can be mounted to a single CVM	10 at most
Maximum number of elastic cloud disks allowed for batch operations in a single API request (including operations such as purchasing, mounting, and unmounting)	10 at most
Maximum capacity for an HDD cloud disk (data disk)	10 GB ~ 16000 GB
Number of snapshots in a single region	Up to (number of cloud disks in the current region*7)
Mounting elastic cloud storage to CVM	The CVM and the elastic cloud storage must be in the same availability zone.
Elastic cloud disk billing method	Elastic cloud disks only support prepaid billing. Postpaid billing is not supported.
Snapshot rollback	Snapshot data can only be rolled back to the cloud disk from which the snapshot was created.

Limits on	Description
Allowed disk type for creating elastic cloud disks using snapshots	You can only use data disk snapshots to create new elastic cloud disks.
Allowed disk size for creating elastic cloud disks using snapshots	The size of the created elastic cloud disk must be bigger or equal to the size of the cloud disk from which the snapshot was created.
Retrieving overdue elastic cloud disks	Elastic cloud disks are billed on a prepaid basis. If the associated CVM or elastic cloud disk is overdue, the association will be canceled and the product will be moved into the recycle bin. Auto-renewal policy is enabled by default when mounting elastic cloud disks. This makes sure that you do not experience any interruption in business only because you forget to renew the product.

Security Group Limits

- Security groups are region and project-specific. CVMs can only be associated with the security groups in the same region and project.
- Security groups apply to any CVM instances in network environment.
- Each user can set a maximum of 50 security groups for each project in each region.
- A maximum of 100 inbound/outbound access policies can be set for a security group.
- A CVM can be associated with multiple security groups, and a security group can be associated with multiple CVMs. No number limit is imposed.
- Security groups bound with CVMs in **basic network cannot filter** data packets sent from (or to) relational database (CDB) and cloud cache service (Redis and Memcached) of Tencent Cloud. If necessary, you can use iptables to filter traffic of such instances.
- The quota limits are as follows:

Feature	Count
Security group	50/Region
Access policy	100 (Inbound/Outbound)
Number of security groups associated with an instance	No limit
Number of instances associated with a security group	No limit

VPC Limits

Resource	Limit
Number of VPCs in a region	5
Number of subnets per VPC	10
Number of basic network CVMs that can be associated with each VPC	100
Number of routing tables per VPC	10
Number of routing policies per routing table	50
Number of peering connections supported by each VPC	10
Number of NAT gateways per VPC	3
Number of EIPs per NAT gateway	10
Maximum forwarding capacity per NAT gateway	5Gbps
Number of VPN gateways per VPC	10
Number of peer gateways in a region	20
Number of VPN tunnels per peer gateway	10
Number of VPN tunnels that can be created in a VPN gateway	20
Number of SPDs per VPN tunnel	10
Number of peer IP address ranges per SPD	50
Number of network ACLs per VPC	50
Number of rules per network ACL	Inbound: 20, outbound: 20.
Number of associated network ACLs per subnet	1
Number of associated subnets per network ACL	Unlimited

Direct Connect Limits

Resource	Limit	Description
----------	-------	-------------

Resource	Limit	Description
Physical Direct Connect/User	10	
Direct Connect tunnel/Physical Direct Connect	10	
Direct Connect gateway (NAT supported)/VPC	1	
Direct Connect gateway (NAT not supported)/VPC	1	
Local IP translation/Direct Connect gateway	100	You can apply for higher quota.
Peer IP translation/Direct Connect gateway	100	You can apply for higher quota.
Number of IPs for local source IP port translation/Direct Connect gateway	20	You can apply for higher quota.
Local destination IP port translation/Direct Connect gateway	100	You can apply for higher quota.

Instances

Purchase and Start Instances

Last updated : 2018-08-01 17:21:35

Prerequisites

Before creating a CVM instance, you need to complete the following steps:

- [Sign up for Tencent Cloud](#), and complete [Identity Verification](#).
- To create a CVM instance whose network type is virtual private cloud (VPC), you need to [Create a VPC](#) in the target region, and [Create a Subnet](#) in the destination region under the VPC.
- If you do not use the default project created automatically by the system, you need to [Create a Project](#).
- If you do not use the default security group automatically created by the system, you need to [Create a Security Group](#) in the target region, and add security group rules that meet your business needs.
- If you need to bind an SSH key pair when creating a Linux instance, you need to [Create an SSH key](#) under the target project.
- To create a CVM instance with custom image, you need to [Create Custom Image](#) or [Import Image](#).

Procedure

(1) Log in to [Tencent Cloud Official Website](#), select **Product** -> **Computing** -> **CVM**, and then click the **Buy Now** button to enter the CVM purchase page.

- **Quick configuration.** Suitable for conventional scenarios, allowing users to quickly select a CVM instance that meets common needs.
- **Custom Configuration.** Suitable for specific scenarios, allowing users to easily select a CVM instance that meets their own specific needs.

(2) Select a billing method.

- Prepaid or postpaid (users who cannot purchase postpaid CVM should complete [Identity Verification](#) first). For more information on the billing methods, please see [Billing Methods](#).

(3) Select a region and availability zone.

- When purchasing cloud services, it is recommended to choose the region that is closest to your customers to minimize the access latency and improve access speed.
- When you need more than one CVMs, it is recommended that you select different availability zones to ensure disaster tolerance.
- For more information on available regions and available zones, please see [Regions and Availability Zones](#).

(4) Select the series, model, and configuration.

- Tencent Cloud offers three series of instances: Series 1, Series 2 and Series 3. To achieve the best performance, we recommend that you use the latest generation of instances when creating instances. For more information on instance series, please see [Instance Specifications](#).
- Tencent Cloud offers standard, high IO, MEM optimized, computing, GPU computing, FPGA, big data, and network enhanced instances. For more information on models, please see [Instance Specifications](#).
- Tencent Cloud provides rich instance configurations, and different models correspond to different instance configurations. For more information on the instance configuration, please see [Instance Specifications](#).

(5) Select an image.

- Based on different sources, images provided by Tencent Cloud are divided into public images, custom images, shared images, and service marketplace images. For more information on image types, please see [Image Types](#).

(6) Select a system disk and a data disk.

- System disk: Required. Used for installing the OS. You can select the type and capacity of the cloud disk used as the system disk. The available types of cloud disks vary in different regions. The default capacity of the system disk is 50 GB.
- Data disk: Optional. You can add a data disk after creating an instance, or add a data disk when purchasing an instance, and then select the cloud disk type and capacity for the data disk. You can create an empty data disk, or use a data disk snapshot to create a data disk.
- For more information on cloud block storage, please see [Cloud Block Storage Types](#).

(7) Select the network type (basic network or VPC).

- Basic network: The basic network is no longer supported in regions launched after August 3, 2017 for all users, and it is also no longer supported for some new accounts registered after June 13, 2017.
- VPC: You must select the VPC and subnet. If you have not created a VPC and subnet, select the default VPC and subnet.
- For more information on basic network and VPC, please see [Product Overview](#).

(8) Select public network IP and billing method of bandwidth (billing by fixed bandwidth or traffic).

- If you need to assign a public IP address to the instance, you need to select **Buy Now**, select **Bill-by-bandwidth** or **Bill-by-traffic**, and set a value greater than 0 Mbps. IP addresses assigned in this way can be unbound with the instance only after being converted into an elastic public network IP, but cannot be unbound directly.
- For more information on the elastic public IP, please see [Elastic Public IP](#).
- Bill-by-bandwidth: Select a fixed bandwidth. Packet loss occurs if this bandwidth is exceeded. This is suitable for scenarios with minor network fluctuation.
- Bill-by-traffic: The service is charged based on actual traffic usage. You can set a limit for peak bandwidth. Packet loss occurs when the instantaneous bandwidth exceeds this limit. This is suitable for scenarios with large network fluctuations.
- For more information on the bandwidth billing methods, please see [Billing Methods](#).

(9) Determine the number of servers and the length of purchase (only for CVMs with an annual and monthly plan).

(10) Set auto renewal.

- If you set auto renewal and your account balance is sufficient, the device is automatically renewed upon its expiration on a monthly basis. For more information on auto renewal, please see [Renewal Management](#).

(11) Set the project.

(12) Set CVM name and login method.

- CVM name: You can choose the CVM naming method as **Name It Now** when purchasing it, and enter a semantic name limited to 60 characters. You can also choose **Name It after Creation**, and the created CVM's name is "Not Named". This name is only displayed on the console, not as the hostname of CVM.
- Login method: For CVMs with Linux images, you can choose **Set Password**, **Associate with Key Immediately**, and **Automatically Generated Password** as the login method. For CVMs with Windows images, you can choose **Set Password** and **Automatically Generated Password** as the login method.

(13) Select the security group.

- If you do not create a security group, select **New Security Group**. If you have an existing security group, select **Existing Security Group**. You can also preview the security group rules. For more information on security group rules, please see [Security Group](#).

(14) Choose to install security reinforcement and cloud monitoring components.

- Security reinforcement: Activate anti-DDoS service, WAF and CVM Security (YunJing) at no cost. For more information, please see [CVM Security](#).
- Cloud monitoring: Activate cloud product monitoring at no cost, install components to obtain CVM monitoring metrics and display them in the form of monitor icons, and support customization of alarm threshold. For more information, please see [Cloud Monitoring Overview](#).

After the CVM is created, you will get an internal message containing such information as instance name, Public IP address, Private IP address, login name, and initial login password (when you choose the method of "Automatically Generated Password"). You can use the information to log in to and manage instances.

Log into Instances

Log into Linux Instances

Last updated : 2018-08-10 10:31:49

Once you've purchased and started a Linux instance, you can connect to and log in to it. The login method depends on your local operating system and whether the CVM instance can be accessed by Internet. See the table below for details.

Local operating system	Linux CVM instance with public IP	Linux CVM instance without public IP
Windows	Login via WebShell Login via remote login software Login by key	Login via VNC
Linux	Login via WebShell Login via VNC Login via SSH Login by key	
Mac OS	Login via WebShell Login via VNC Login via SSH Login by key	

Prerequisites

Prerequisites for login by password

Administrator account and password are required for login by password

- Administrator account: The administrator account varies with different types of Linux instances, as shown below.

Instance Operating System	Administrator Account
SUSE/CentOS/Debian	root
Ubuntu	ubuntu

- Password:

- If **Auto Generate Password** is selected when you start an instance, the initial password is randomly assigned by the system. Log in to [Tencent Cloud Console](#), and click the **Internal Message** button on the right. In the **Check the new CVM you purchased** page, the administrator account and initial password for logging in to CVM are provided as shown below.

腾讯云 总览 云产品 常用服务 English 备案 测试帐号 费用 工单

消息中心 < 返回

站内信 消息订阅 公告

【腾讯云】请查收您新购买的云服务器

产品消息 标记已读

【腾讯云】请查收您新购买的云服务器 查看全部

站内信

初始密码

尊敬的用户，

您新购买的云服务器(共1台)已分配成功(订单号: xxxxxxxxxxxxxxxx)感谢您对腾讯云的支持!，感谢您对腾讯云的支持!

服务器操作系统为 CentOS 7.2 64位，默认账户为 root，初始密码为 *****

服务器名称	云主机ID	所在网络ID	内网IP	公网IP
未命名	ins-xxxxxxx	基础网络	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx

温馨提醒:

1. 若网站用于web访问,请及时[备案](#)。如需帮助,请查看[备案论坛](#),或咨询腾讯云官方在线客服,您也可以拨打备案咨询电话: 4009-100-100。
2. 如果您购买了数据盘,建议在服务器创建后首次登陆时,手动进行磁盘分区格式化操作。具体请参考: [Windows 系统分区格式化操作指引](#), [Linux 系统分区格式化操作指引](#)。
3. 如您在云服务器使用中遇到业务环境部署、数据迁移等问题,您可以从腾讯云认证的代运维服务商处获得帮助,如需联系,请点击[这里](#)。

谢谢!

立即[查看使用教程](#),玩转腾讯云!

腾讯云项目组
2017.07.12

- If **Custom Password** is selected when you start a CVM instance, the password is the one you specified when purchasing the instance. For more information about password (for example, what to do if you forget the login password), please see [Login Password](#).

Prerequisites for login by key

To log in to a CVM using a private key, you need to create and download the key.

First, you need to create an SSH key, download the private key and bind it to the Linux CVM. For more information about operations on the key, please see [SSH Key](#).

Login from Local Windows PC by Password

Login tool

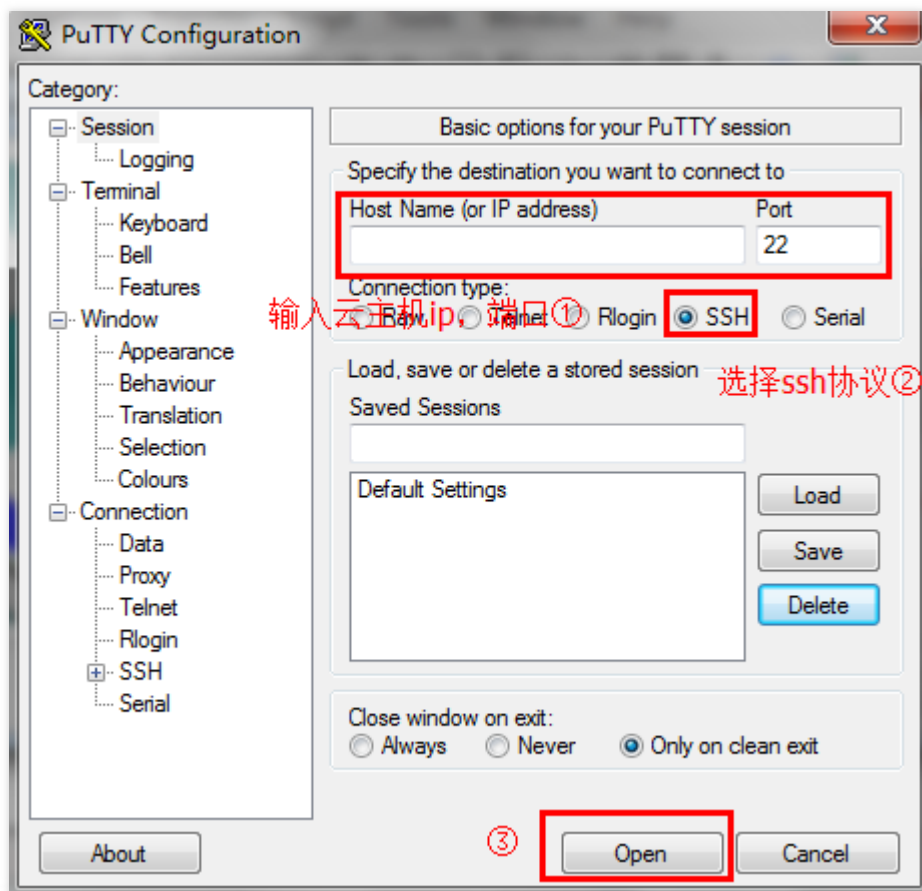
Log in to a Linux instance by password using **remote login software** (in this case, PuTTY is used. You can also choose another login software).

Procedure

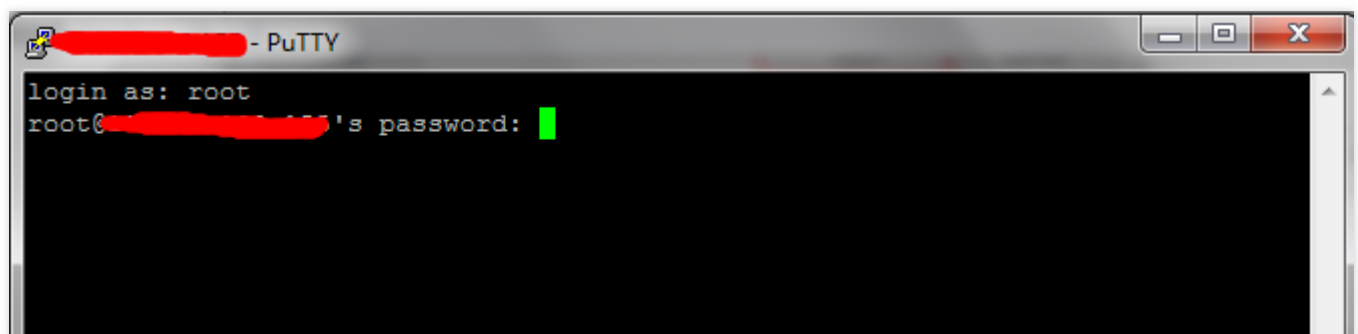
1. Download and install the Windows remote login software from, for example:
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>.
2. Connect to the Linux CVM using PuTTY. Open the PuTTY client, enter the following information in the PuTTY Configuration window:

- Host Name: Public IP of the CVM (log in to the [CVM Console](#) to obtain the public IP of the CVM in the list and details pages).
- Port: Port of the CVM, which must be 22. (Make sure port 22 of the CVM is open. For more information, please see [Security Group](#) and [Network ACL](#).)
- Connect type: Select "SSH".

3. When all the information is entered, click **Open** to create a new session.



4. In the PuTTY session window, enter the administrator account obtained in the "Prerequisites" step, and then press Enter. Enter the login password obtained in the "Prerequisites" step, and then press Enter to log in to the instance.

**Note:**

If the login fails, check if your CVM instance allows inbound traffic over port 22. Check the port by referring to [Security Group](#). If your CVM is in a [VPC](#), also check the related subnet's [network ACL](#).

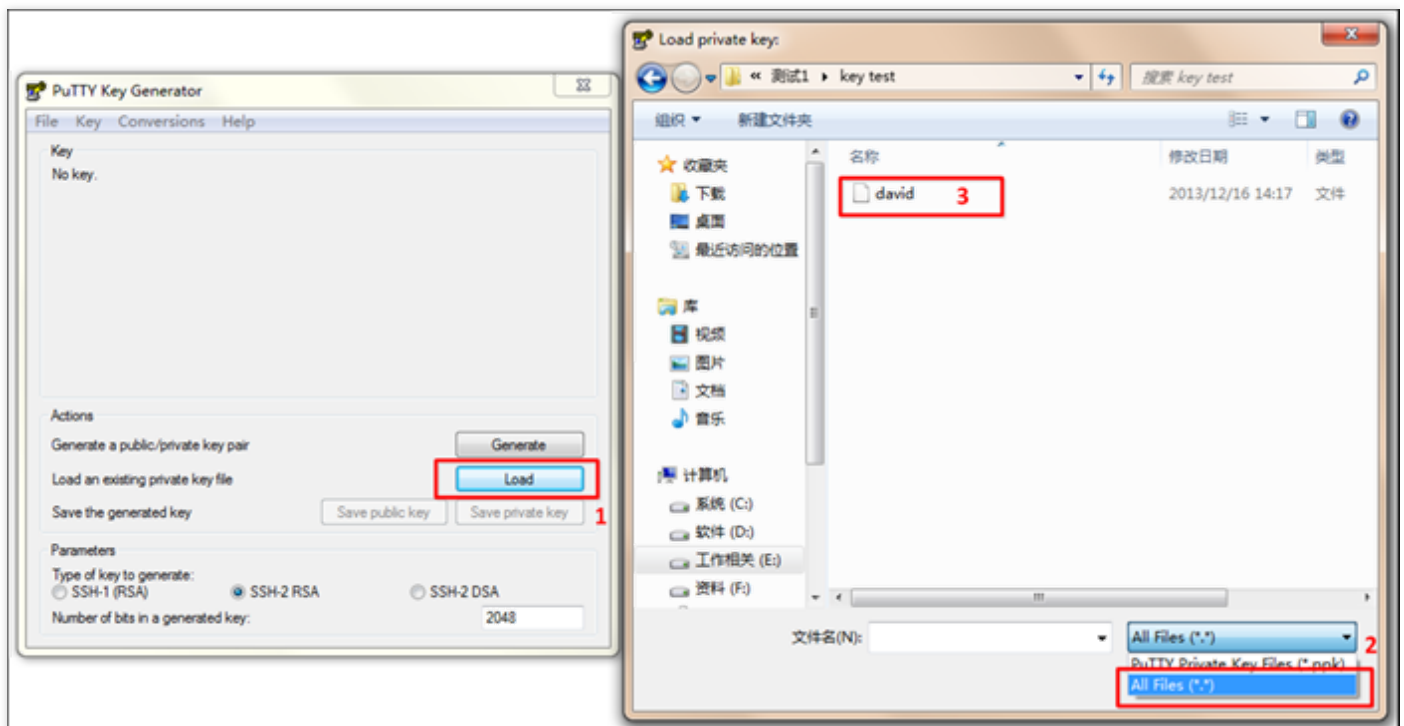
Login from Local Windows PC by SSH Key

Login tool

Log in to a Linux instance by SSH key using **remote login software** (in this case, PuTTY is used. You can also choose another login software).

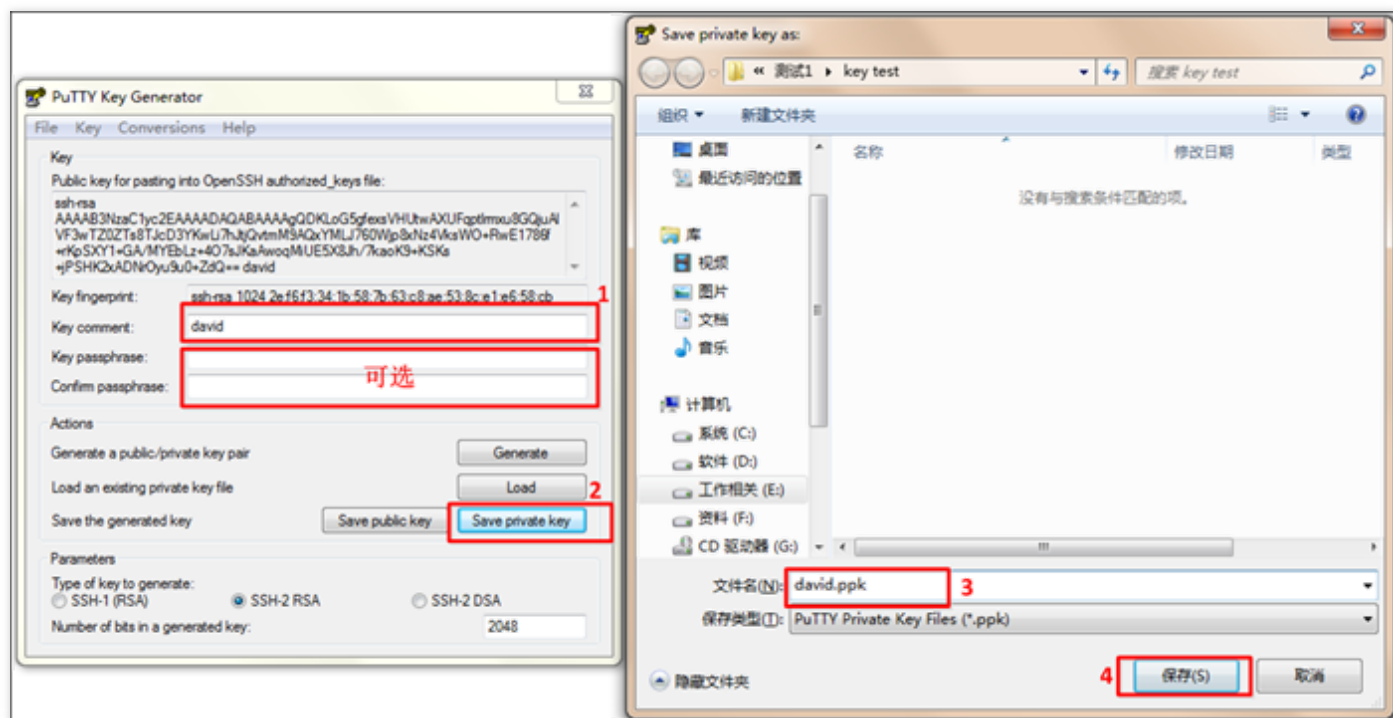
Procedure

1. Download and install the Windows remote login software from, for example:
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html> (two files are downloaded: putty.exe and puttygen.exe).
2. Select a private key. Open puttygen.exe, and click **Load** button. In the window that pops up, go to the path under which you store the private key downloaded in the "Prerequisites" step, and then select **All Files (*.*)**. Select the downloaded private key (in this case it is file david, which is the name of the key), and click **Open**.

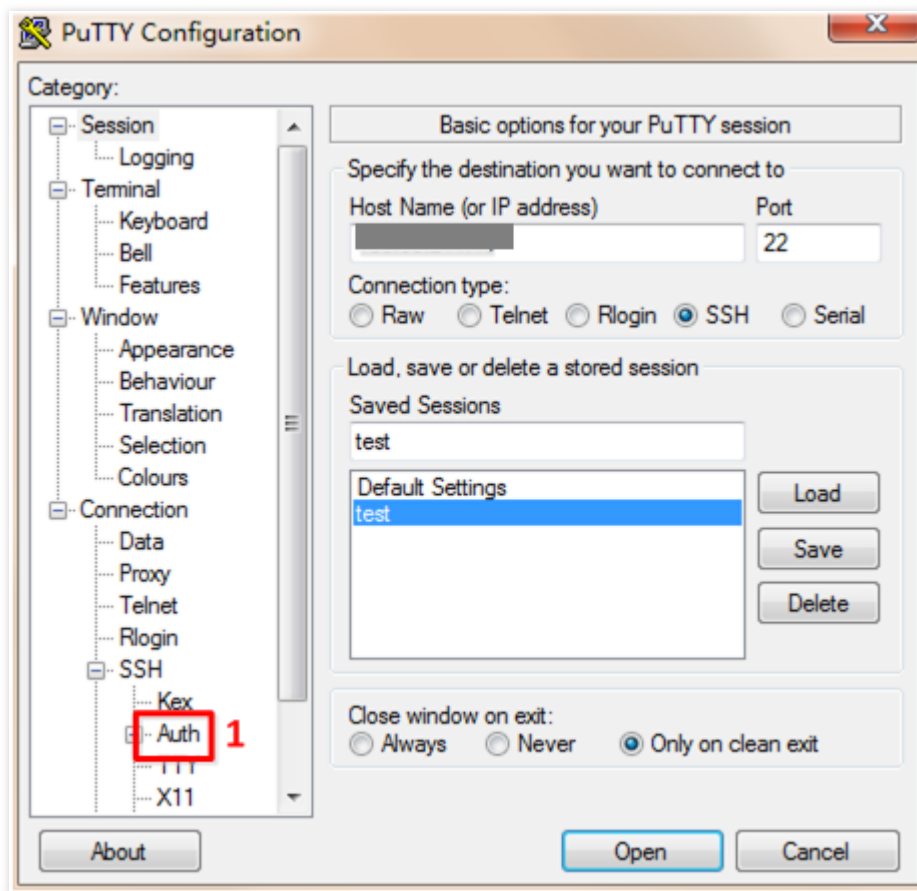


3. Convert the key. Enter the key name in the **key comment** column, enter the password for the encrypted private key, and then click **Save private key**. In the window that pops up, select the directory where you

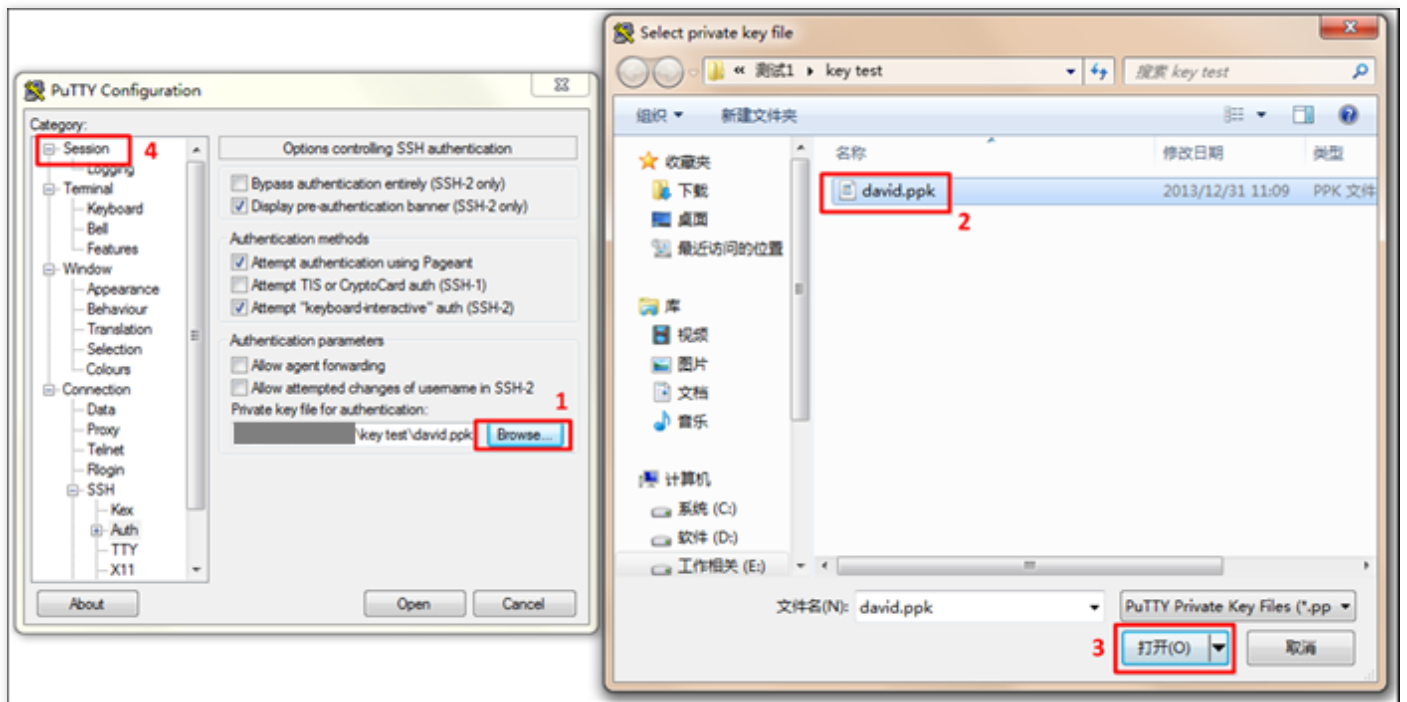
store the key, enter key name + ".ppk" in the file name column, and then click **Save**.



4. Open putty.exe to enter the **Auth** configuration page.



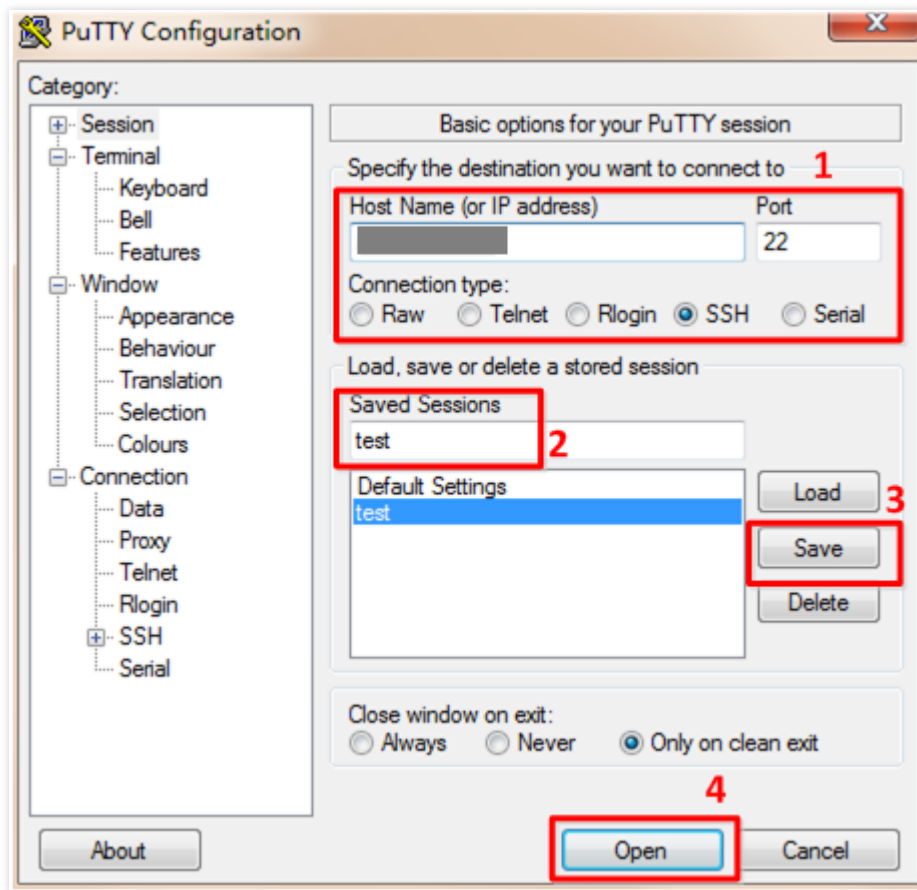
5. Click the **Browse** button. In the window that pops up, go to the path where the key is stored, select the key, click **Open** to return to the configuration page, and then go to the **Session** configuration page.



6. Configure the IP, port and connection type for the server on the **Session** configuration page.

- IP: Public IP of the CVM. Log in to the [CVM Console](#) to obtain the public IP of the CVM in the list and details pages.
- Port: Port of the CVM, which must be 22. (Make sure port 22 of the CVM is open. For more information, please see "Security Group" and "Network ACL".)

7. Enter a session name in the **Saved Sessions** input box (enter "test" in this case), click **Save**, and then double click the session name or click **Open** to initiate a login request.

**Note:**

If the login fails, check if your CVM instance allows inbound traffic over port 22. Check the port by referring to [Security Group](#). If your CVM is in a [VPC](#), also check the related subnet's [network ACL](#).

Login from Local Linux/Mac OS PC by Password

Login tool

Log in to the instance with SSH using the Terminal supplied with Mac OS system.

Procedure

1. If you are a Mac OS user, open the Terminal supplied with the system and enter the following command. If you are a Linux user, run the following command directly: `ssh <username>@<hostname> or ip address>`

(`username` is the administrator account obtained in the "Prerequisites" step, and `hostname` or `ip address` is the public IP or custom domain name of your Linux instance.)

2. Enter the password obtained in the "Prerequisites" step (there is only input and no output at this point), then press Enter to log in to the instance.

Note:

If the login fails, check if your CVM instance allows inbound traffic over port 22. Check the port by referring to [Security Group](#). If your CVM is in a [VPC](#), also check the related subnet's [network ACL](#).

Login from Local Linux/Mac OS PC by Key

Login tool

Log in to the instance using the Terminal supplied with Mac OS system.

Procedure

1. If you are a Mac OS user, open the Terminal supplied with the system and enter the following command. If you are a Linux user, run the following command directly to set the private key file to be read only by you. `chmod 400`
2. Run the following remote login command: `ssh -i "<absolute path of the private key downloaded to be associated with the CVM>" <username>@<hostname or ip address>`.
(`username` is the administrator account obtained in the "Prerequisites" step, and `hostname` or `ip address` is the public IP or custom domain name of your Linux instance. For example: `ssh -i "Mac/Downloads/shawn_qcloud_stable" ubuntu@119.xxx.xxx.xxx`).

Note:

If the login fails, check if your CVM instance allows inbound traffic over port 22. Check the port by referring to [Security Group](#). If your CVM is in a [VPC](#), also check the related subnet's [network ACL](#).

Login via WebShell (recommended)

Login tool

Login via WebShell is a method Tencent Cloud provides for you to connect to your CVMs through Web browser. Compared with login via VNC, login via WebShell provides a user experience more similar to login using PuTTY, SSH and other clients. If the CVM has a public IP and its login port is open, using WebShell can give you a better remote access experience.

Advantages:

- Supports copy and paste operations with shortcut keys.
- Supports scrolling with mouse wheel.
- Supports Chinese input.
- Features a high security (password or key is required for each login).

Procedure

1. Log in to the [CVM Console](#). Select **Cloud Products** -> **Cloud Compute & Network** -> **Cloud Virtual Machine** from the top menu.
2. Go to the CVM list, as shown below, and then click the **Log In** button for the Linux CVM to which you want to log in.

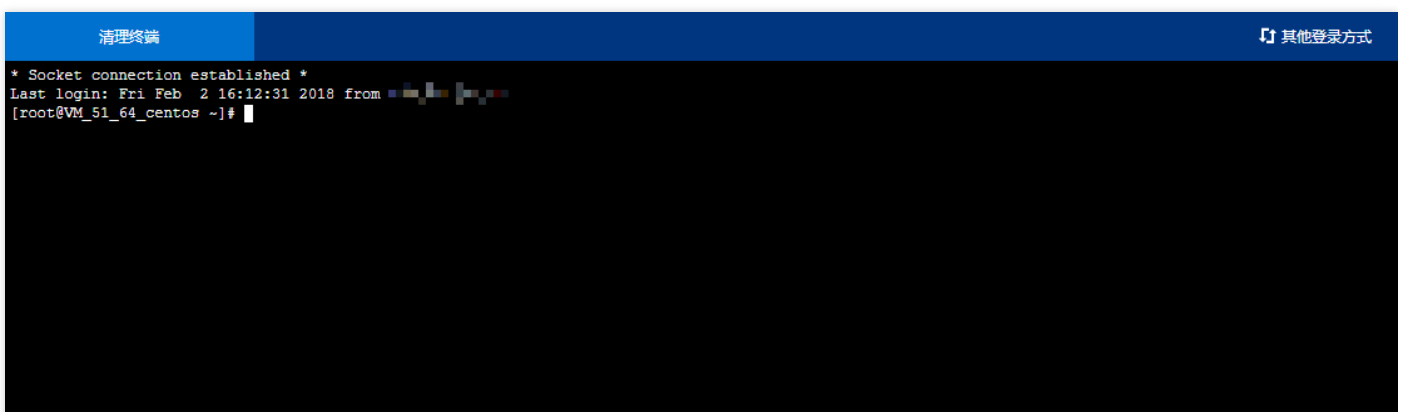
The screenshot shows the Tencent Cloud CVM Console. The left sidebar contains navigation options like '云服务器', '云主机', '专用宿主机', '镜像', '云硬盘', '快照', 'SSH密钥', '安全组', '弹性公网IP', and '回收站'. The main area displays a list of CVM instances. The first instance, 'ins-eepc8qtg', is highlighted, and the '登录' (Log In) button is circled in red. The table below shows the details of the instances.

ID/主机名	监控/状态	可用区	主机类型	配置	主IP地址	主机计费模式	网络计费模式	所属项目	操作
ins-eepc8qtg centos-1GB-qz-4435	运行中	广州四区	标准型S2	1核 1GB 1Mbps 系统盘: 普通云硬盘 网络: 基础网络	[IP Address]	包年包月 2018-03-01 10:45 到期	按带宽包年包月计费	默认项目	登录 续费 更多
ins-kvdd4upa 腾讯云实验 室 (id:10068)	运行中	广州三区	标准型S1	1核 1GB 1Mbps 系统盘: 普通云硬盘 网络: 基础网络	[IP Address]	包年包月 2018-02-28 17:22 到期	按带宽包年包月计费	默认项目	登录 续费 更多

3. A new tab page appears, as shown below, where you can select **Login By Password** or **Login by Key**.



4. If the password or key is correct, it will pass the verification of system, and you'll log in to the Linux CVM successfully with WebShell.



Note:

- The CVM is required to have a public IP.
- SSH remote login port (default is 22) needs to be open on the CVM.

Login via VNC

Login tool

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 via VNC to check the CVM status and perform basic CVM management operations with your CVM account.

"Login via VNC" scenarios include at least the following:

- Check the progress of a CVM startup
- When login with client SSH or mstsc failed

Procedure

1. Log in to the [CVM Console](#). Select **Cloud Products** -> **Cloud Compute & Network** -> **Cloud Virtual Machine** from the top menu.
2. Go to the CVM list, as shown below, and then click the **Log In** button for the Linux CVM to which you want to log in.



3. A new tab page appears, as shown below. The white window in the middle is used for login via WebShell, so you need to click the **x** button in the upper right corner to switch the login method (as

shown below).



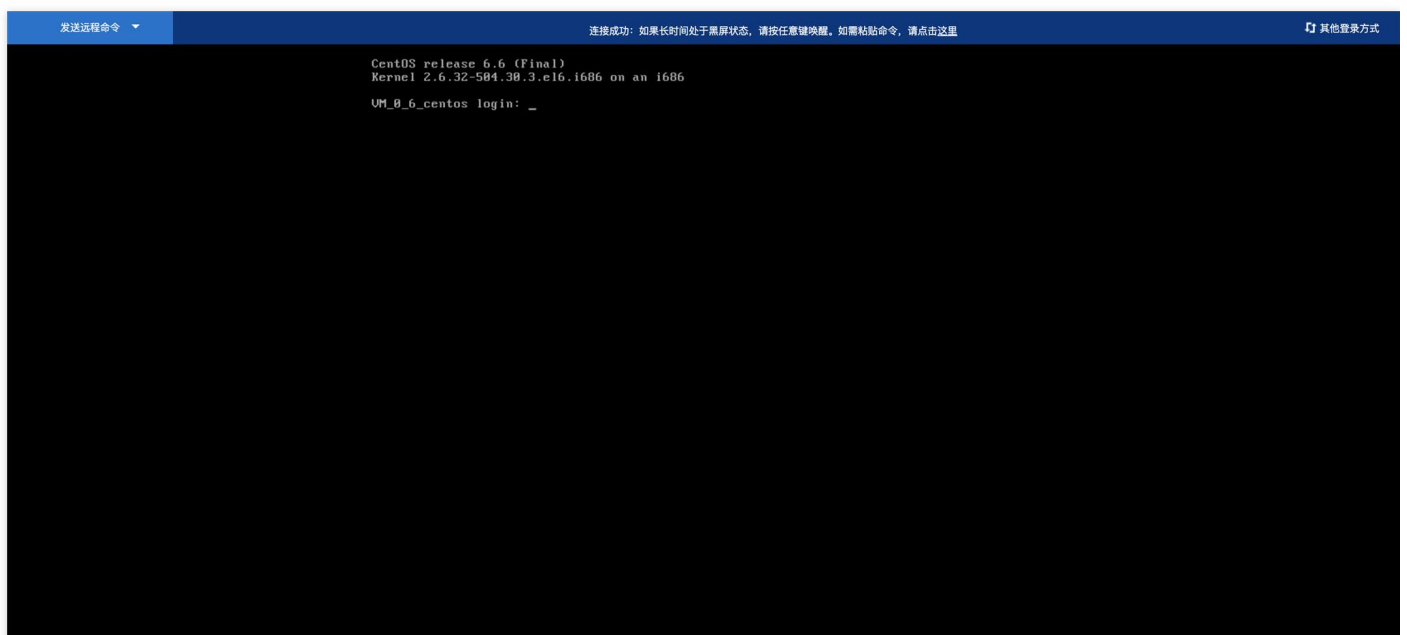
4. Click **Other Login Methods** in the upper right corner of the page.



5. A new white window pops up. Locate the **Login via VNC using Browser** column, at the bottom, and then click **Log In Now**.



6. Now, you can successfully log in to the Linux CVM via VNC.



Note:

- This terminal is exclusive, that is, only one user can log in to CVM via VNC at a time.
- A successful login via VNC requires mainstream browsers such as Chrome, Firefox, IE10 or above.
- File upload and download are not supported.

Log into Windows Instances

Last updated : 2018-08-10 10:41:09

Once you've purchased and started a Linux instance, you can connect to and log in to it. The login method depends on your local operating system and whether the CVM instance can be accessed by Internet. See the table below for details.

Local operating system	Linux CVM instance with public IP	Linux CVM instance without public IP
Windows	Login via WebShell Login via remote login software Login by key	Login via VNC
Linux	Login via WebShell Login via VNC Login via SSH Login by key	
Mac OS	Login via WebShell Login via VNC Login via SSH Login by key	

Prerequisites

Prerequisites for login by password

Administrator account and password are required for login by password

- Administrator account: The administrator account varies with different types of Linux instances, as shown below.

Instance Operating System	Administrator Account
SUSE/CentOS/Debian	root
Ubuntu	ubuntu

- Password:

- If **Auto Generate Password** is selected when you start an instance, the initial password is randomly assigned by the system. Log in to [Tencent Cloud Console](#), and click the **Internal Message** button on the right. In the **Check the new CVM you purchased** page, the administrator account and initial password for logging in to CVM are provided as shown below.

腾讯云 总览 云产品 常用服务 English 备案 测试帐号 费用 工单

消息中心 < 返回

站内信 消息订阅 公告

【腾讯云】请查收您新购买的云服务器

产品消息 标记已读 查看全部

尊敬的用户，

您新购买的云服务器(共1台)已分配成功(订单号: xxxxxxxxxxxxxxxx)感谢您对腾讯云的支持! 感谢您对腾讯云的支持!

服务器操作系统为 CentOS 7.2 64位, 默认账户为 root, 初始密码为 *****

服务器名称	云主机ID	所在网络ID	内网IP	公网IP
未命名	ins-xxxxxxx	基础网络	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx

温馨提醒:

- 若网站用于web访问, 请及时[备案](#)。如需帮助, 请查看[备案论坛](#), 或咨询腾讯云官方在线客服, 您也可以拨打备案咨询电话: 4009-100-100。
- 如果您购买了数据盘, 建议在服务器创建后首次登陆时, 手动进行磁盘分区格式化操作。具体请参考: [Windows 系统分区格式化操作指引](#), [Linux 系统分区格式化操作指引](#)。
- 如果您在云服务器使用中遇到业务环境部署、数据迁移等问题, 您可以从腾讯云认证的代运维服务商处获得帮助, 如需联系, 请点击[这里](#)。

谢谢!

立即[查看使用教程](#), 玩转腾讯云!

腾讯云项目组
2017.07.12

站内信

初始密码

- If **Custom Password** is selected when you start a CVM instance, the password is the one you specified when purchasing the instance. For more information about password (for example, what to do if you forget the login password), please see [Login Password](#).

Prerequisites for login by key

To log in to a CVM using a private key, you need to create and download the key.

First, you need to create an SSH key, download the private key and bind it to the Linux CVM. For more information about operations on the key, please see [SSH Key](#).

Login from Local Windows PC by Password

Login tool

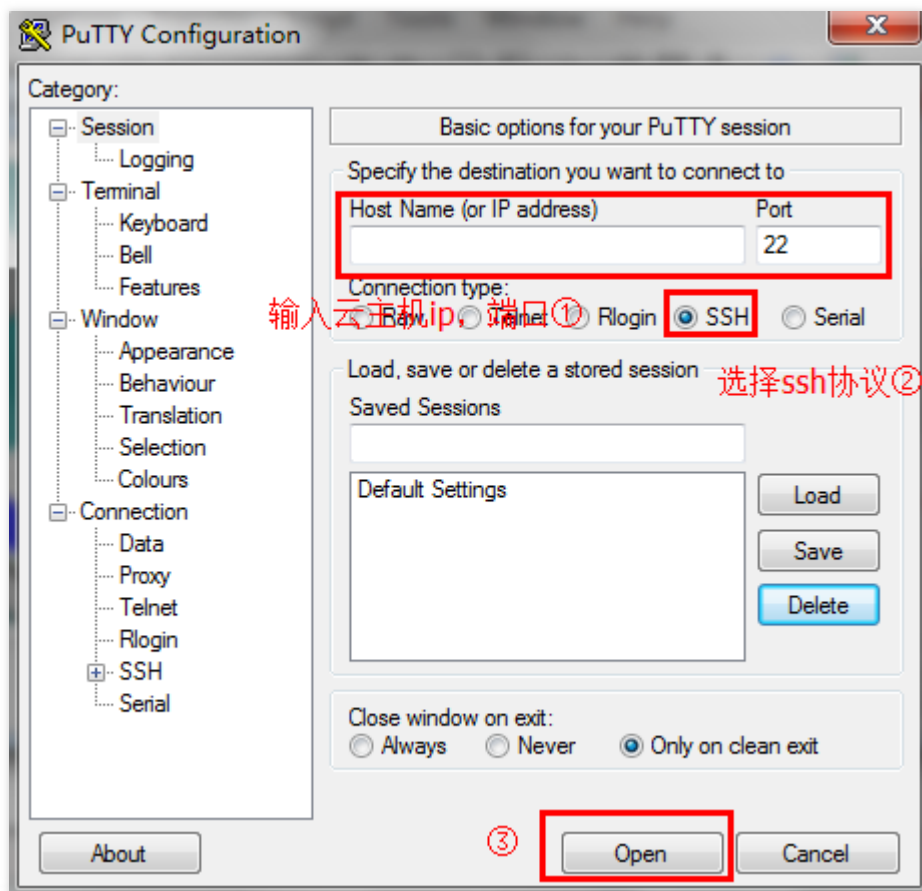
Log in to a Linux instance by password using **remote login software** (in this case, PuTTY is used. You can also choose another login software).

Procedure

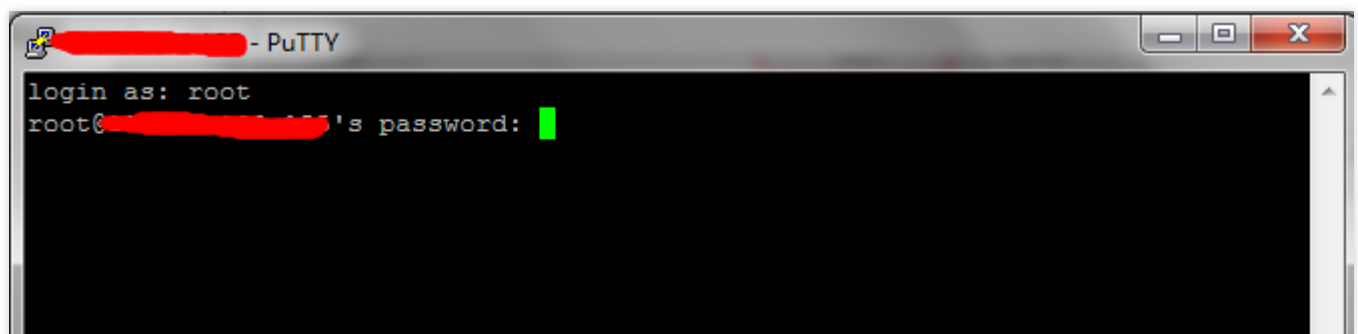
1. Download and install the Windows remote login software from, for example:
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>.
2. Connect to the Linux CVM using PuTTY. Open the PuTTY client, enter the following information in the PuTTY Configuration window:

- Host Name: Public IP of the CVM (log in to the [CVM Console](#) to obtain the public IP of the CVM in the list and details pages).
- Port: Port of the CVM, which must be 22. (Make sure port 22 of the CVM is open. For more information, please see [Security Group](#) and [Network ACL](#).)
- Connect type: Select "SSH".

3. When all the information is entered, click **Open** to create a new session.



4. In the PuTTY session window, enter the administrator account obtained in the "Prerequisites" step, and then press Enter. Enter the login password obtained in the "Prerequisites" step, and then press Enter to log in to the instance.

**Note:**

If the login fails, check if your CVM instance allows inbound traffic over port 22. Check the port by referring to [Security Group](#). If your CVM is in a [VPC](#), also check the related subnet's [network ACL](#).

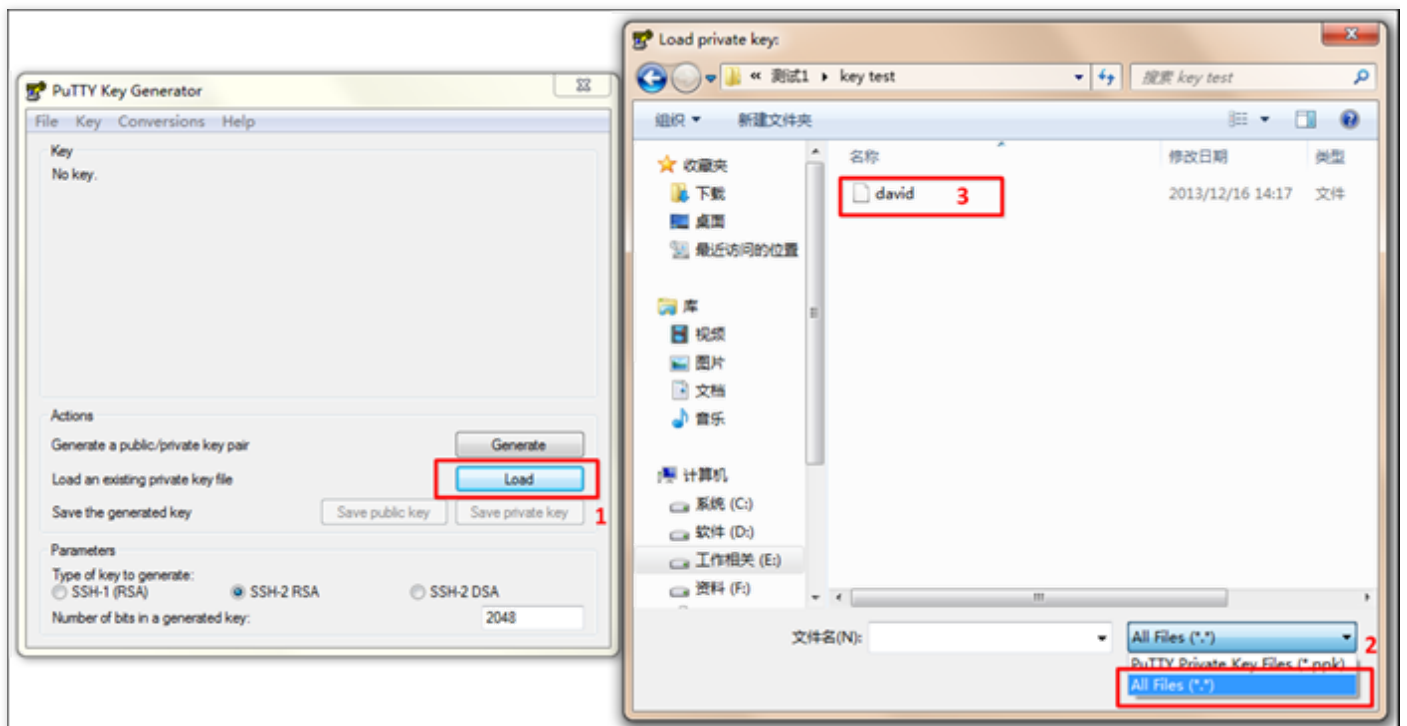
Login from Local Windows PC by SSH Key

Login tool

Log in to a Linux instance by SSH key using **remote login software** (in this case, PuTTY is used. You can also choose another login software).

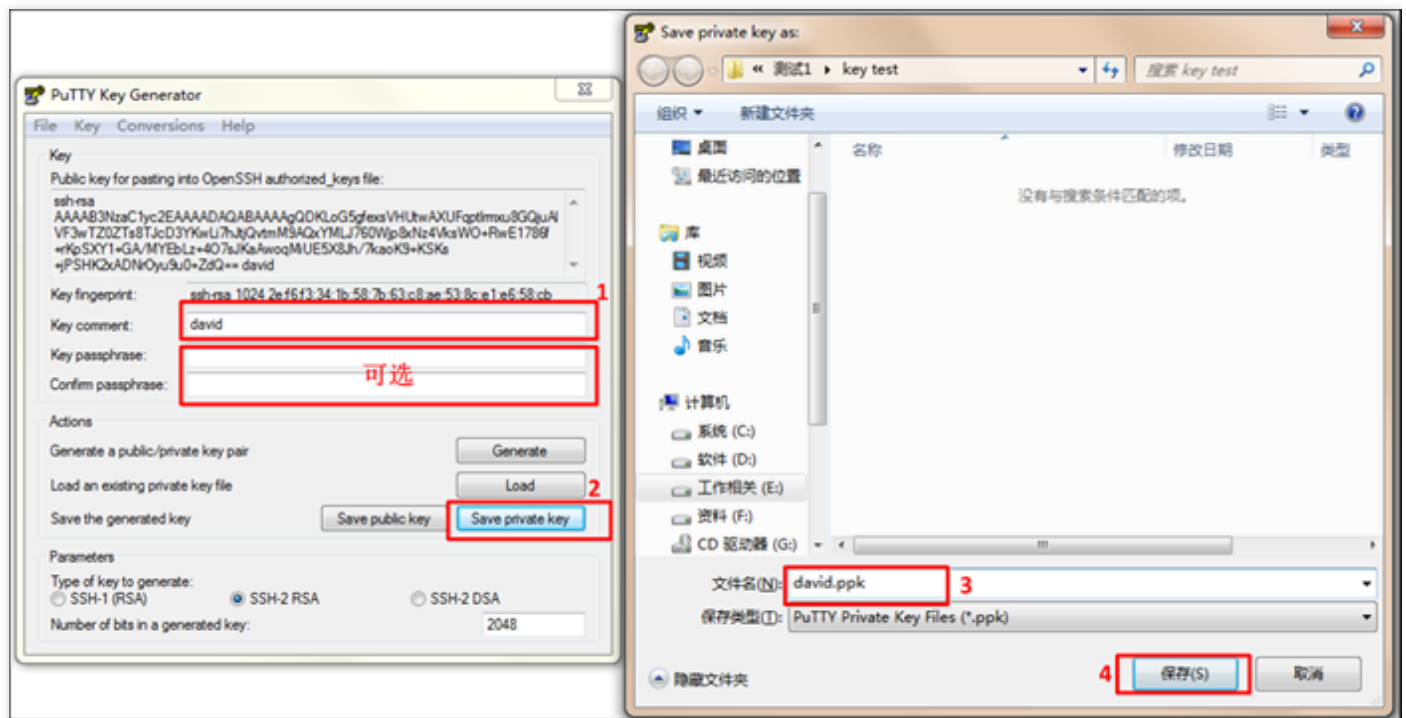
Procedure

1. Download and install the Windows remote login software from, for example:
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html> (two files are downloaded: putty.exe and puttygen.exe).
2. Select a private key. Open puttygen.exe, and click **Load** button. In the window that pops up, go to the path under which you store the private key downloaded in the "Prerequisites" step, and then select **All Files (*.*)**. Select the downloaded private key (in this case it is file david, which is the name of the key), and click **Open**.

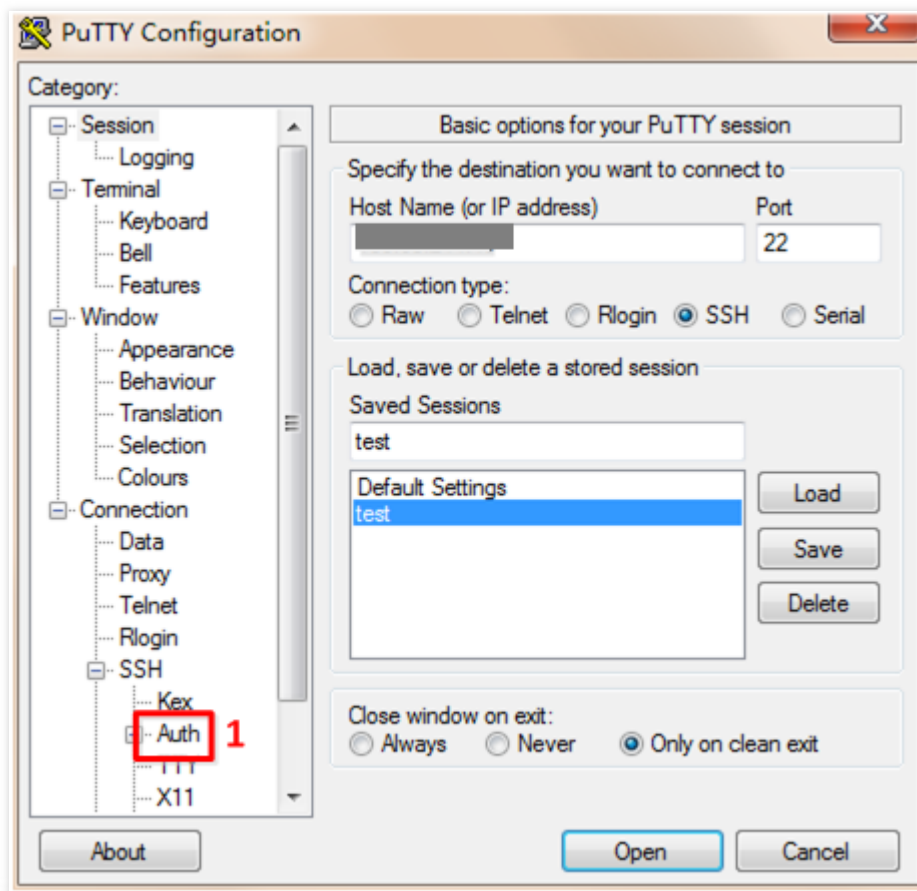


3. Convert the key. Enter the key name in the **key comment** column, enter the password for the encrypted private key, and then click **Save private key**. In the window that pops up, select the directory where you

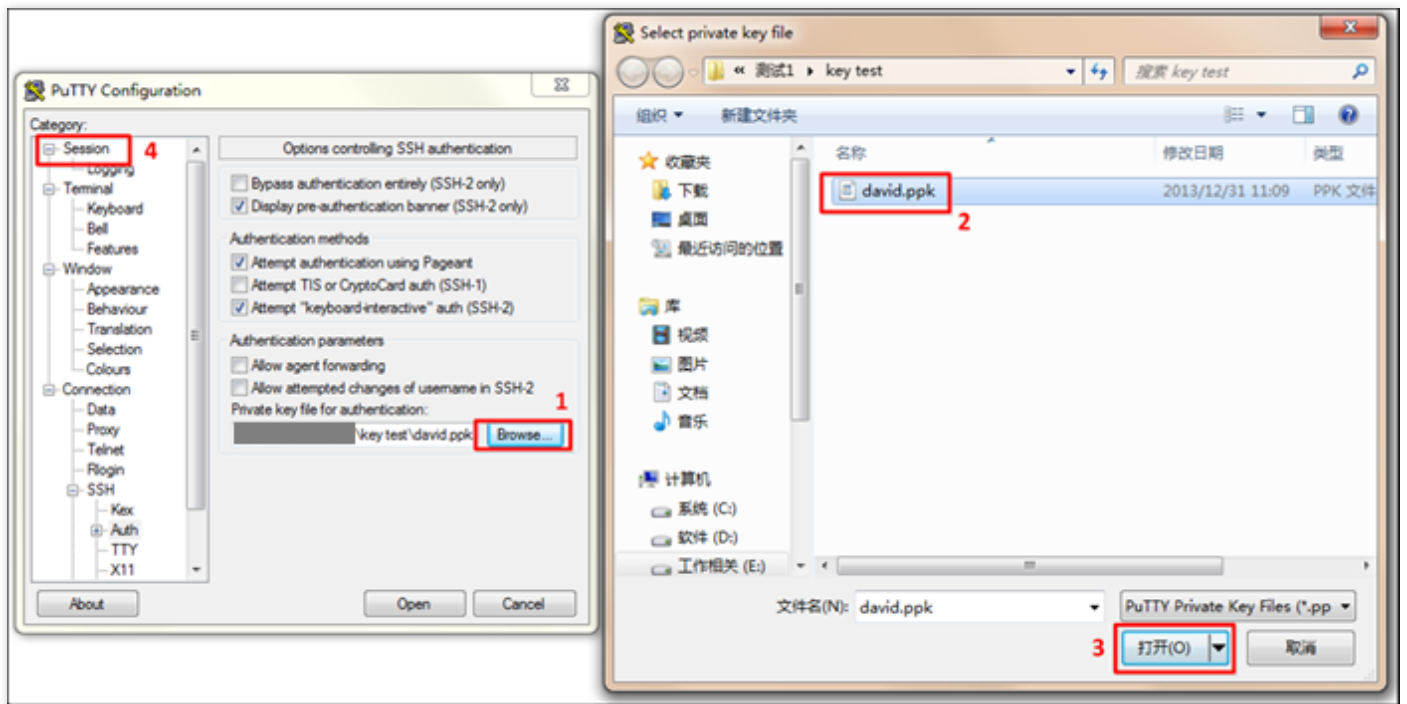
store the key, enter key name + ".ppk" in the file name column, and then click **Save**.



4. Open putty.exe to enter the **Auth** configuration page.



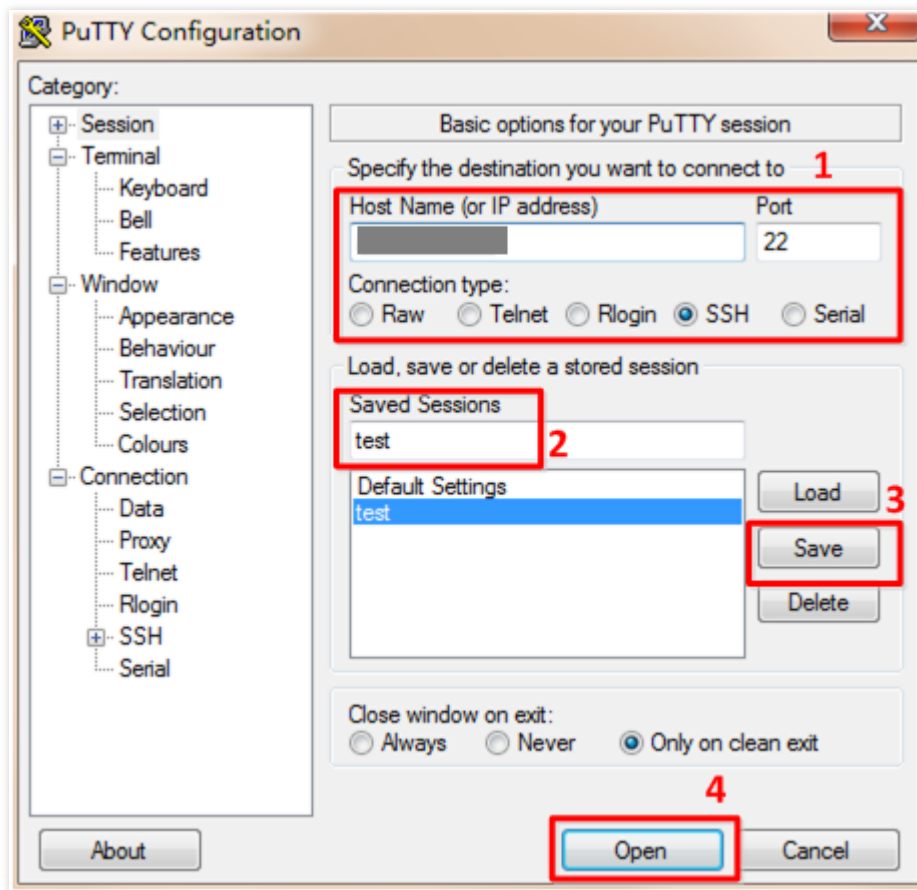
5. Click the **Browse** button. In the window that pops up, go to the path where the key is stored, select the key, click **Open** to return to the configuration page, and then go to the **Session** configuration page.



6. Configure the IP, port and connection type for the server on the **Session** configuration page.

- IP: Public IP of the CVM. Log in to the [CVM Console](#) to obtain the public IP of the CVM in the list and details pages.
- Port: Port of the CVM, which must be 22. (Make sure port 22 of the CVM is open. For more information, please see "Security Group" and "Network ACL".)

7. Enter a session name in the **Saved Sessions** input box (enter "test" in this case), click **Save**, and then double click the session name or click **Open** to initiate a login request.

**Note:**

If the login fails, check if your CVM instance allows inbound traffic over port 22. Check the port by referring to [Security Group](#). If your CVM is in a [VPC](#), also check the related subnet's [network ACL](#).

Login from Local Linux/Mac OS PC by Password

Login tool

Log in to the instance with SSH using the Terminal supplied with Mac OS system.

Procedure

1. If you are a Mac OS user, open the Terminal supplied with the system and enter the following command. If you are a Linux user, run the following command directly: `ssh <username>@<hostname or ip address>`

(`username` is the administrator account obtained in the "Prerequisites" step, and `hostname or ip address` is the public IP or custom domain name of your Linux instance.)

2. Enter the password obtained in the "Prerequisites" step (there is only input and no output at this point), then press Enter to log in to the instance.

Note:

If the login fails, check if your CVM instance allows inbound traffic over port 22. Check the port by referring to [Security Group](#). If your CVM is in a [VPC](#), also check the related subnet's [network ACL](#).

Login from Local Linux/Mac OS PC by Key

Login tool

Log in to the instance using the Terminal supplied with Mac OS system.

Procedure

1. If you are a Mac OS user, open the Terminal supplied with the system and enter the following command. If you are a Linux user, run the following command directly to set the private key file to be read only by you. ``chmod 400 '`
2. Run the following remote login command: `ssh -i "<absolute path of the private key downloaded to be associated with the CVM>" <username>@<hostname or ip address>`.
(`username` is the administrator account obtained in the "Prerequisites" step, and `hostname or ip address` is the public IP or custom domain name of your Linux instance. For example: `ssh -i "Mac/Downloads/shawn_qcloud_stable" ubuntu@119.xxx.xxx.xxx`).

Note:

If the login fails, check if your CVM instance allows inbound traffic over port 22. Check the port by referring to [Security Group](#). If your CVM is in a [VPC](#), also check the related subnet's [network ACL](#).

Login via WebShell (recommended)

Login tool

Login via WebShell is a method Tencent Cloud provides for you to connect to your CVMs through Web browser. Compared with login via VNC, login via WebShell provides a user experience more similar to login using PuTTY, SSH and other clients. If the CVM has a public IP and its login port is open, using WebShell can give you a better remote access experience.

Advantages:

- Supports copy and paste operations with shortcut keys.
- Supports scrolling with mouse wheel.
- Supports Chinese input.
- Features a high security (password or key is required for each login).

Procedure

1. Log in to the [CVM Console](#). Select **Cloud Products -> Cloud Compute & Network -> Cloud Virtual Machine** from the top menu.
2. Go to the CVM list, as shown below, and then click the **Log In** button for the Linux CVM to which you want to log in.

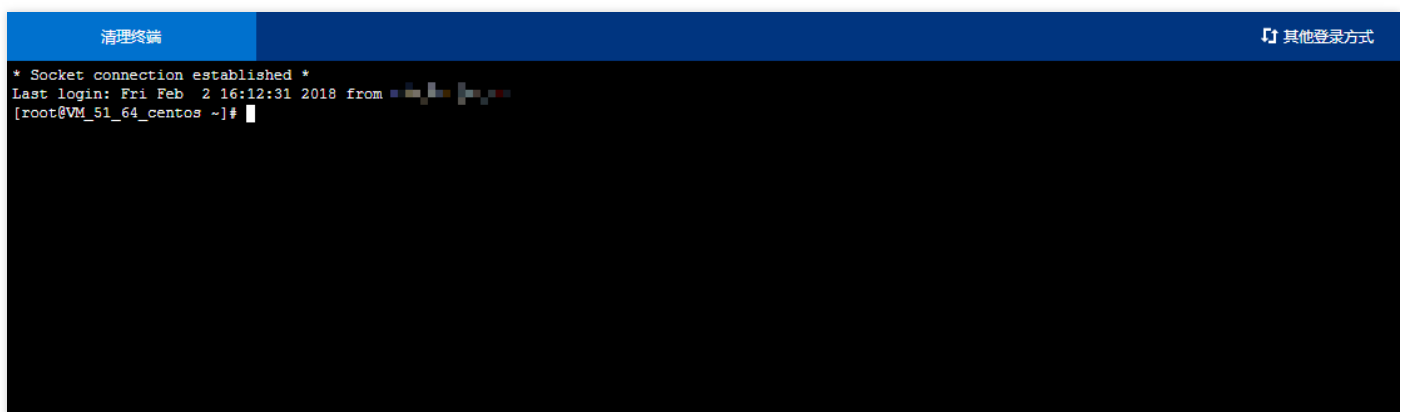
The screenshot shows the Tencent Cloud CVM Console interface. The left sidebar contains navigation options like '云服务器', '云主机', '专用宿主机', '镜像', '云硬盘', '快照', 'SSH密钥', '安全组', '弹性公网IP', and '回收站'. The main area displays a list of CVM instances. The first instance, 'ins-eepc8qtg', is highlighted, and its '登录' (Log In) button is circled in red. The table below shows the details of the instances.

ID/主机名	监控/状态	可用区	主机类型	配置	主IP地址	主机计费模式	网络计费模式	所属项目	操作
ins-eepc8qtg centos-1GB-qz-4435	运行中	广州四区	标准型S2	1核 1GB 1Mbps 系统盘: 普通云硬盘 网络: 基础网络	[IP Address]	包年包月 2018-03-01 10:45 到期	按带宽包年包月计费	默认项目	登录 续费 更多
ins-kvdd4upa 腾讯云实验 室 (id:10068)	运行中	广州三区	标准型S1	1核 1GB 1Mbps 系统盘: 普通云硬盘 网络: 基础网络	[IP Address]	包年包月 2018-02-28 17:22 到期	按带宽包年包月计费	默认项目	登录 续费 更多

3. A new tab page appears, as shown below, where you can select **Login By Password** or **Login by Key**.



4. If the password or key is correct, it will pass the verification of system, and you'll log in to the Linux CVM successfully with WebShell.



Note:

- The CVM is required to have a public IP.
- SSH remote login port (default is 22) needs to be open on the CVM.

Login via VNC

Login tool

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 via VNC to check the CVM status and perform basic CVM management operations with your CVM account.

"Login via VNC" scenarios include at least the following:

- Check the progress of a CVM startup
- When login with client SSH or mstsc failed

Procedure

1. Log in to the [CVM Console](#). Select **Cloud Products** -> **Cloud Compute & Network** -> **Cloud Virtual Machine** from the top menu.
2. Go to the CVM list, as shown below, and then click the **Log In** button for the Linux CVM to which you want to log in.



3. A new tab page appears, as shown below. The white window in the middle is used for login via WebShell, so you need to click the **x** button in the upper right corner to switch the login method (as

shown below).



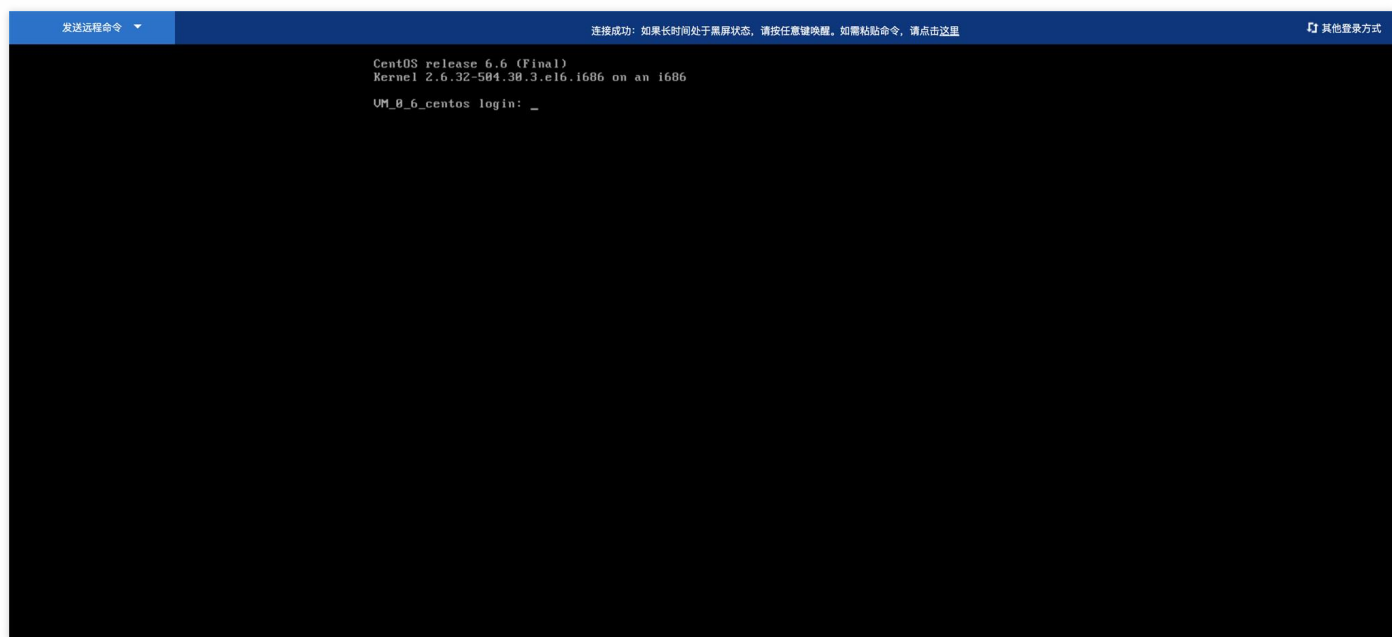
4. Click **Other Login Methods** in the upper right corner of the page.



5. A new white window pops up. Locate the **Login via VNC using Browser** column, at the bottom, and then click **Log In Now**.



6. Now, you can successfully log in to the Linux CVM via VNC.



Note:

- This terminal is exclusive, that is, only one user can log in to CVM via VNC at a time.
- A successful login via VNC requires mainstream browsers such as Chrome, Firefox, IE10 or above.
- File upload and download are not supported.

Change Specifitaion

Change CVM Specifitaion

Last updated : 2018-10-10 20:22:17

The Tencent Cloud instances' hardware devices can be adjusted easily. This is an important feature of cloud virtual servers that makes them more usable than physical servers. This document describes how to upgrade and degrade instance configuration and important considerations.

Prerequisites and Considerations

Instance status

You can adjust an instance's configuration when the instance has been either started up or shut down, and the change takes effect after the instance is forced to shut down and restarted.

Note:

- When the instance has been **shut down**, you can make changes in the console directly.
- When the instance has been **started up**, you can make changes online, and confirm forced shutdown after changes are made. The changes to configuration take effect after the instance is restarted.
- You can adjust configuration **in batch** online for multiple instances. If there is a server that has been **started up** in the batch of instances, you need to confirm the forced shutdown individually, and the changes take effect after the servers are restarted.

Limit of configuration adjustment

- Upgrading configuration

No limit is imposed on the number of times configuration upgrade can be performed. The upgrade takes effect immediately.
- Degrading configuration
 - Postpaid instances can be degraded at any time and for unlimited times.

Hardware

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

Change of private IP

For a very small number of instances, their private IPs will change after the configuration adjustment.

Upgrading Configuration

You can upgrade the configuration of CVMs to adapt to you growing business. For all CVM types, the upgraded configuration takes effect immediately. That is, after you upgrade the configuration and pay the additional fees, the CVM will run with the new configuration immediately.

Upgrading via console

1. Log in to the [console](#), and then click the **CVM** tab on the left to go to the CVM list.
2. Locate the Operation column next to the instance to be adjusted, and click **More -> CVM Configuration -> Adjust Configuration**.
3. In the popup box, select the configuration you want to upgrade to, and then click **OK**.

- **Popup box for postpaid instances:**

Adjust configuration

×

You have selected 1 unitsCloud Virtual Machine , [Learn More](#) ▾

No.	CVM Name	CVM ID	Current Capped...	Operation
1	未命名	ins-0dkqdmzw	1 Mbps	Can be Adjust co...

Current configuration 1-core 1GB 0.03 USD/hr

New CPU cores

1-core

2-core

4-core

8-core

12-core

16-core

24-core

32-core

56-core

New MEM

1GB

2GB

4GB

32位CentOS 5以及CentOS 6版本支持最大内存为16G, 如有高内存需求, 建议将系统重装至64位后再进行内存调整。

Special offer **0.02 USD /hr** ~~0.03 USD /hr~~ ⓘ

Important Note

After configuration adjustment, the amount-based charging starts from the first step in the stepwise price. Exercise caution when adjusting the configuration[Learn More](#).

OK

Cancel

Upgrading via API

You can upgrade instance configuration using the APIs `ResizeInstance` and `ResizeInstanceHour`. For more information, please see [APIs for adjusting instance configuration](#).

Degrading Configuration

You can also degrade the configuration of CVM instances in console to adapt to your shrinking business. The degrade method varies with different CVM types.

Degrading postpaid instances

1. Log in to the [console](#), and then click the **CVM** tab on the left to go to the CVM list.
2. Locate the Operation column next to the **postpaid** instance to be adjusted, and click **More** -> **CVM Configuration** -> **Adjust Configuration**.

3. In the popup box, select the configuration you want to degrade to, and then click **OK**.

Adjust configuration ×

You have selected **1 unitsCloud Virtual Machine** , [Learn More](#) ▼

No.	CVM Name	CVM ID	Current Capped...	Operation
1	pjc	ins-ny05mmoc	1 Mbps	Can be Adjust co...

Current configuration 2-core 4GB 0.1 USD/hr

New CPU cores

1-core

2-core

4-core

8-core

12-core

16-core

24-core

32-core

48-core

64-core

80-core

New MEM

1GB

2GB

4GB

32位CentOS 5以及CentOS 6版本支持最大内存为16G，如有高内存需求，建议将系统重装至64位后再进行内存调整。

Special offer **0.02 USD /hr** ~~0.04 USD /hr~~ ⓘ

Important Note

After configuration adjustment, the amount-based charging starts from the first step in the stepwise price. Exercise caution when adjusting the configuration[Learn More](#).

Note: after degrading, the CVM supports up to 2 ENIs. Each ENI supports up to 2 IPs.[Learn more about ENI quota](#)

OK

Cancel

Adjust Network Configuration

Last updated : 2018-09-12 16:25:11

Change Billing Method

Tencent Cloud provides a variety of billing methods. You can switch between Bill-by-bandwidth and Bill-by-traffic in the console, but for each CVM, switching between the two methods can only be performed twice at most.

Billing description: [Overview of Billing Methods for Public Network](#)

Adjustment for Public Network

Tencent Cloud provides two types of network configurations: exclusive public network and shared public network. The shared public network service is billed by bandwidth. You need to submit a ticket to apply for activating it. For more information about the billing methods, please see [Billing of Shared Public Network](#). This document mainly describes the adjustment between exclusive public networks. For more information about the billing methods, please see [Billing of Exclusive Public Network](#).

Bill-by-bandwidth for prepaid CVMs

This billing method supports adjusting network bandwidth. You can upgrade the bandwidth within the prepaid period, but cannot degrade the bandwidth.

Bill-by-bandwidth for postpaid CVMs

This billing method supports adjusting (upgrading or degrading) bandwidth at any time. If the bandwidth is changed several times during an hour, the billing is based on the highest bandwidth tier.

Bill-by-traffic

This billing method supports adjusting (upgrading or degrading) the bandwidth cap at any time and the change takes effect in real time.

This billing method can be used for both prepaid and postpaid CVMs.

Bandwidth cap

The options vary with different payment methods and CVM configurations. For more information, please see [Bandwidth Cap of Public Network](#).

Procedure

1. Log in to the [CVM Console](#), select the instance for which you want to change the network configuration, and then click **More** -> **CVM settings** -> **Adjust network**.
2. In the **Adjust network** popup page, you can change the billing method and bandwidth cap.
3. Click **OK**.

Adjust Project Configuration

Last updated : 2018-09-12 16:29:11

Cloud resources can be managed by project. When a CVM instance is created, it must be assigned to a project. Tencent Cloud allows re-assigning an instance to a new project.

Note:

To assign an instance to a new project, create the new project first. For more information, please see [New Project](#).

Procedure

1. Go to the [CVM Console](#), and select the CVM or CVMs to be assigned to the new project.
2. Click **More** (for a single CVM) or **More actions** (for multiple CVMs), and then click **Change Project**.

<input type="checkbox"/>	ID/主机名	监控/状态	可用区	主机类型	配置	主IP地址	主机计费模式	所属项目	操作
搜索找到3条结果, 返回列表									
<input checked="" type="checkbox"/>	ins-...	运行中	上海二区	标准型S3	32核 128GB 1Mbps 系统盘: 本地硬盘 网络: 基础网络	10.105.98.166 (内)	包年包月 2018-03-27 20:54 到期	默认项目	登录 续费 更多
<input type="checkbox"/>	ins-...	运行中	上海一区	标准型S1	1核 1GB 1Mbps 系统盘: 本地硬盘 网络: 基础网络	10.154.25.20 (内)	按量计费 2018-02-01 16:50 创建	默认项目	云主机状态 云主机设置 密码/密钥 配置安全组 弹性网卡 制作镜像 重装系统 分配至项目 弹性IP
<input type="checkbox"/>	ins-... melody-不要删除	运行中	上海一区	标准型S1	1核 2GB 无限制 系统盘: 本地硬盘 网络: wizard-sh	10.1.0.17 (内)	包年包月 2018-03-30 10:58 到期	默认项目	

3. Go to the Change Project page, select the name of the new project, and click **OK**.

分配至项目

×

您已选 1台 云主机 , [查看详情](#)✓

No.	主机名	主机ID	当前带宽上限	操作
1		ins-c	1 Mbps	可分配至项目

云主机迁移后需重新绑定安全组，点击 [查看操作指南](#)。

项目名称	项目说明
<input type="radio"/> 默认项目 (当前所属项目)	默认项目
<input checked="" type="radio"/> vint	安全组测试
<input type="radio"/> wait test	wait test

确定

取消

Network Configuration after Creating an Instance Using Imported Windows Image

Last updated : 2018-08-10 15:48:01

After importing Windows images and creating a CVM, you can log in to the CVM by clicking the **Log In** button next to [CVM list in the console](#) and configure the network.

Network configuration information of Windows servers is saved in the file `C:\qcloud-network-config.ini`, which is structured as follows:

[ip]

ip= x.x.x.x

mask = x.x.x.x

gateway = x.x.x.x

[dns]

dns = x.x.x.x

Modify the network based on this configuration file.

Query Info

Query Instance Info

Last updated : 2018-09-12 15:26:05

Tencent Cloud provides the following three options for you to view the information of a CVM instance:

- View the total number of CVM instances under your account and their status, as well as the quantity and quota of resources in each region in the [Overview](#) page in Console.
- View the information of all CVM instances in a region on the [CVM List](#) page in Console.
- View the details of a CVM instance on the instance details page.

Viewing Instance Overview

The following information and operations are available in the [Overview](#) page:

- CVM status: total number of CVMs, the number of instances that expire within the next 7 days, the number of instances in Recycle Bin, and the number of normal CVMs.
- List of CVMs to be renewed (you can renew them on this page).
- Resource quantity and quota. You can view the postpaid CVMs, custom images and snapshot quota information for each region, and apply for quotas on this page.
- Perform cross-region search for cloud resources.

Viewing Information of CVM List

The information available in the [CVM List](#) page includes CVM IDs and names, monitoring information/status, availability zones, CVM type, configuration, primary IP address, CVM billing method, network billing method and the projects to which the CVMs belong.

Click the gear button in the upper right corner to select the list details you want to display.

自定义列表字段

×

请选择您想显示的列表详细信息，根据您的分辨率，最多勾选9个字段，已勾选9个。

<input checked="" type="checkbox"/> ID/主机名	<input checked="" type="checkbox"/> 主IP地址
<input checked="" type="checkbox"/> 监控/状态	<input checked="" type="checkbox"/> 主机计费模式
<input checked="" type="checkbox"/> 可用区	<input type="checkbox"/> 网络计费模式
<input checked="" type="checkbox"/> 主机类型	<input checked="" type="checkbox"/> 所属项目
<input checked="" type="checkbox"/> 配置	<input checked="" type="checkbox"/> 操作

确定

取消

Viewing Instance Details

Go to the instance details page to view the details of an instance by following the steps below:

1. Log in to the [CVM Console](#).
2. Select a region.
3. Locate the instance for which you want to view the details, and click the instance ID to go to the instance details page.
4. In the instance details page, the following instance information is displayed, including CVM information, CVM configuration, system image, SSH key, ENI, public IP, monitoring, health check,

security group, etc.

[<](#) [云主机](#) | [ins-a\[redacted\]](#)

[参数](#) [弹性网卡](#) [公网IP](#) [监控](#) [健康检查](#) [安全组](#) [操作日志](#)

主机信息

名称	melody
服务器ID	fcd[redacted]184a30
状态	运行中
公网IP	[redacted]3
内网IP	192.168.2.8
创建时间	2018-03-05 19:01:35
到期时间	-
地域	北京
可用区	北京一区
主机计费模式	按量计费
网络计费模式	按流量计费

Query Instance Monitoring Info

Last updated : 2018-09-12 16:31:40

Tencent Cloud provides the following two options for you to view the monitoring information of a CVM instance.

- View the monitoring information of a CVM instance in the Cloud Monitor Console.
- View the monitoring information of a CVM instance on the instance details page in the CVM Console.

Viewing Instance Monitoring Information in Cloud Monitor Console

1. Log in to the Cloud Monitor Console of [CVM](#).
2. Select a region.
3. Click an instance ID to enter the monitoring information page of the instance.

云服务器

华南地区（广州）

华南地区（深圳金融）

华东地区（上海）

华东地区（上海金融）

华北地区（北京）

西南地区（成都）

东南亚地区（香港）

东南亚地区（新加坡）

亚太南部（孟买）

亚太地区（首尔）

北美地区（多伦多）

华南地区（广州Open）

美国西部（硅谷）

欧洲地区（法兰克福）

提示：黄色叹号标记的云服务器可能未安装监控 Agent 导致无监控数据，[导出这些云服务器IP](#)

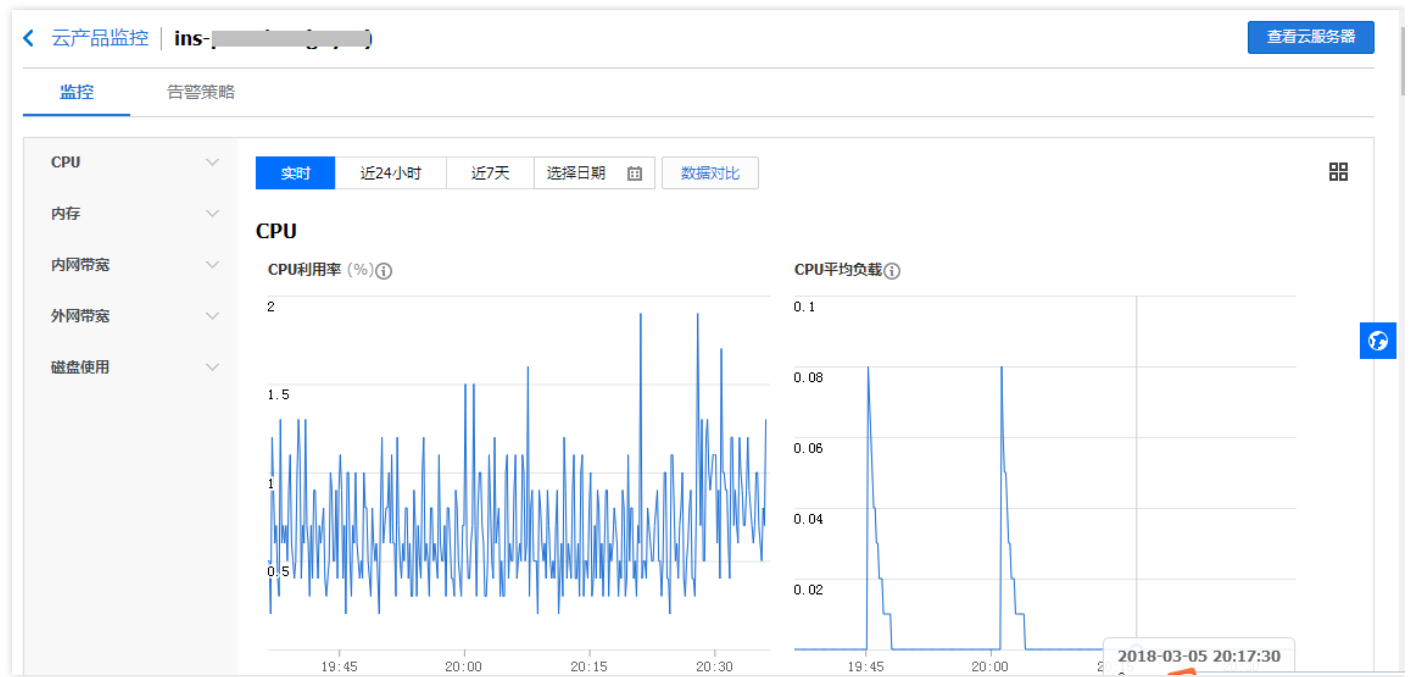
云服务器

全部

请输入IP(换行分隔)或主机名

ID/主机名	IP地址	状态	CPU利用率	内存利用率	外网出带宽	所属项目	告警策略数
ins- melody-不要删除	10.1.0.17(内网)	运行中	-	-	-	默认项目	1
ins- jayco	10.154.25.20(内网)	运行中	0.65%	8.22%	0.00Mbps	默认项目	2
ins- 3(公网)	10.105.98.166(内网)	运行中	0%	0.70%	0Mbps	默认项目	0

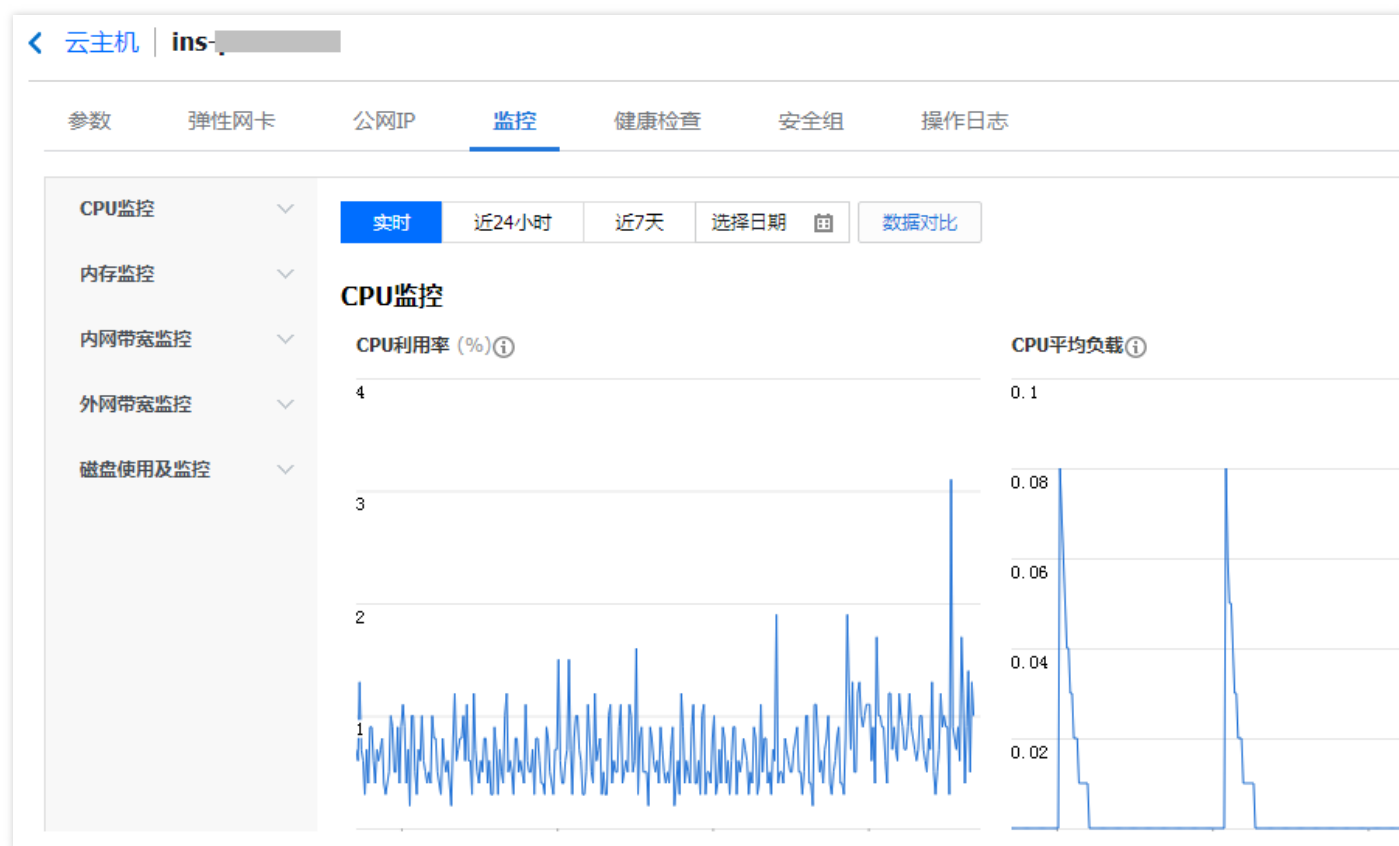
4. In the monitoring information page, you can view the CVM instance's monitoring information such as CPU, memory, bandwidth of private network/public network, and disk usage.



5. You can view the monitoring information of public network traffic in the [Traffic Monitor](#) page.

Viewing Instance Monitoring Information in CVM Console

1. Log in to the [CVM](#) Console.
2. Select a region.
3. Click an instance ID to enter the instance details page, and then click **Monitor**.
4. In the monitoring information page, you can view the CVM instance's monitoring information such as CPU, memory, bandwidth of private network/public network, and disk usage.



5. You can view the monitoring information of public network traffic in the [Traffic Monitor](#) page.

Instance Metadata

Last updated : 2018-10-12 15:51:23

Instance metadata is the data of the instances you are running and can be used to configure or manage the running instances.

Note: Although the instance metadata can only be accessed from within the instance itself, the data is not encrypted and protected. Anyone who has the access to an instance also has the access to its metadata. Therefore, it is recommended to take appropriate measures to protect sensitive data (e.g. using a permanent encryption key).

Overview of Instance Metadata

Tencent Cloud provides the following meta-data:

Data	Description	Version Where It Was Introduced
instance-id	Instance ID	1.0
uuid	Instance ID	1.0
local-ipv4	Instance's private IP	1.0
public-ipv4	Instance's public IP	1.0
mac	MAC address of instance's eth0 device	1.0
placement/region	Information of the region where the instance resides	Updated on Sept 19, 2017
placement/zone	Information of the availability zone where the instance resides	Updated on Sept 19, 2017
network/interfaces/macs/ mac /mac	Device address of the instance's network interface	1.0
network/interfaces/macs/ mac /primary-local-ipv4	Primary private IP of instance's network interface	1.0

Data	Description	Version Where It Was Introduced
network/interfaces/macs/ mac /public-ipv4s	Public IP of the instance's network interface	1.0
network/interfaces/macs/ mac /local-ipv4s/ local-ipv4 /gateway	Gateway address of the instance's network interface	1.0
network/interfaces/macs/ mac /local-ipv4s/ local-ipv4 /local-ipv4	Private IP of the instance's network interface	1.0
network/interfaces/macs/ mac /local-ipv4s/ local-ipv4 /public-ipv4	Public IP of the instance's network interface	1.0
network/interfaces/macs/ mac /local-ipv4s/ local-ipv4 /public-ipv4-mode	Public network mode of the instance's network interface	1.0
network/interfaces/macs/ mac /local-ipv4s/ local-ipv4 /subnet-mask	Subnet mask of the instance's network interface	1.0

Fields **mac** and **local-ipv4** in red in the above table indicate the device address and private IP of the network interface specified for the instance, respectively.

The requested target URL is case sensitive. > Construct the target URL address of new request in strict accordance with the format of the returned result of request.

In the current version, the returned data of placement has been changed. To use the data in the previous version, specify the previous version path or leave the version path empty to access the data of version 1.0. For more information about the returned data of placement, please see [Region and Availability Zone](#).

Querying Instance Metadata

You can access the instance metadata such as instance's local IP and public IP from within an instance to manage connections with external applications.

To view all the instance metadata from within a running instance, use the following URI:

```
http://metadata.tencentyun.com/latest/meta-data/
```

You can access metadata through the cURL tool or HTTP GET request, for example:

```
curl http://metadata.tencentyun.com/latest/meta-data/
```

- For resources that do not exist, HTTP error code "404 - Not Found" is returned.
- Any operation on instance metadata can only be performed **from within the instance**. Log in to the instance first. For more information on how to log in to an instance, please see [Logging in to Windows Instances](#) and [Logging in to Linux Instances](#).

Example of querying metadata

The following example shows how to obtain the metadata version information. Note: When the Tencent Cloud modifies the metadata access path or returned data, a new metadata version is released. If your application or script depends on the structure or returned data of previous version, you can access metadata using the specified previous version. If no version is specified, version 1.0 is accessed by default.

```
[qcloud-user]# curl http://metadata.tencentyun.com/  
1.0  
2017-09-19  
latest  
meta-data
```

The following example shows how to view the metadata root directory. The line ending with `/` represents a directory and the one not ending with `/` represents the accessed data. For the description of accessed data, please see **Overview of Instance Metadata** described above.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/  
instance-id  
local-ipv4  
mac  
network/  
placement/  
public-ipv4  
uuid
```

The following example shows how to obtain the physical location information of an instance. For the relationship between the returned data and the physical location, please see [Region and Availability Zone](#).

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/placement/region  
ap-guangzhou
```

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/placement/zone  
ap-guangzhou-3
```

The following example shows how to obtain the private IP of an instance. If an instance has multiple ENIs, the network address of the eth0 device is returned.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/local-ipv4
10.104.13.59
```

The following example shows how to obtain the public IP of an instance.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/public-ipv4
139.199.11.29
```

The following example shows how to obtain an instance ID. Instance ID is used to uniquely identify an instance.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/instance-id
ins-3g445roi
```

The following example shows how to get the instance uuid. Instance uuid can also be used as the unique identifier of an instance, but it is recommended to use instance ID to distinguish between instances.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/uuid
cfac763a-7094-446b-a8a9-b995e638471a
```

The following example shows how to obtain the MAC address of an instance's eth0 device.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/mac
52:54:00:BF:B3:51
```

The following example shows how to obtain the ENI information of an instance. In case of multiple ENIs, multiple lines of data are returned, with each line indicating the data directory of an ENI.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfaces/macs/
52:54:00:BF:B3:51/
```

The following example shows how to obtain the information of specified ENI.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfaces/macs/52:54:00:BF:B3:51/
local-ipv4s/
mac
primary-local-ipv4
public-ipv4s
```

The following example shows how to obtain the list of private IPs bound to the specified ENI. If the ENI is bound with multiple private IPs, multiple lines of data are returned.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/10.104.13.59/
```

The following example shows how to obtain the information of private IP.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/10.104.13.59  
gateway  
local-ipv4  
public-ipv4  
public-ipv4-mode  
subnet-mask
```

The following example shows how to obtain the gateway of private IP (only for VPC-based CVMs). For more information about VPC-based CVMs, please see [Virtual Private Cloud \(VPC\)](#).

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/10.104.13.59/gateway  
10.15.1.1
```

The following example shows how to obtain the access mode used by a private IP to access the public network (only for VPC-based CVMs). A basic network-based CVM accesses the public network through the public gateway.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/10.104.13.59/public-ipv4-mode  
NAT
```

The following example shows how to obtain the public IP bound to a private IP.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/10.104.13.59/public-ipv4  
139.199.11.29
```

The following example shows how to obtain the subnet mask of a private IP.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/10.104.13.59/subnet-mask  
255.255.192.0
```


Modify Instance Name

Last updated : 2018-09-12 16:53:25

To help users manage CVMs on the CVM console and quickly identify them by name, Tencent Cloud supports naming CVMs. You can modify a CVM's name at any time, and the new name takes effect immediately.

Modifying Name of an Instance

- Enter the [CVM console](#), and select the CVM that needs to be renamed.
- Click **More** -> **CVM Settings** -> **Rename** on the page.
- On the renaming page, enter a new CVM name, and then click **OK**.

Modifying Names of Multiple Instances

- Enter the [CVM console](#), and select multiple CVMs that need to be renamed.
- Click **More** -> **Rename** on the page.

<input type="checkbox"/> ID/主机名	监控/状态	可用区	主机类型	配置	主IP地址	主机计费模式	所属项目	操作
搜索找到3条结果, 返回列表								
<input type="checkbox"/> ins- [redacted]	运行中	上海二区	标准型S3	32核 128GB 1Mbps 系统盘: 本地硬盘 网络: 基础网络	[redacted] (公) ↕ 10.105.98.166 (内)	包年包月 2018-03-27 20:54 到期	默认项目	登录 续费 更多 ^
<input type="checkbox"/> ins-p jayco	运行中	上海一区	标准型S1	1核 1GB 1Mbps 系统盘: 本地硬盘 网络: 基础网络	[redacted] (弹性) 10.154.25.20 (内)	按量计费 2018-02-01 16:50 创建	默认项	云主机状态 > 云主机设置 > 密码/密钥 > 配置安全组 > 弹性网卡 > 制作镜像 > 重装系统 > 分配至项目 > 弹性IP >
<input type="checkbox"/> ins- melody-不要 删除	运行中	上海一区	标准型S1	1核 2GB 无限制 系统盘: 本地硬盘 网络: wizard-sh	[redacted] (公) ↕ 10.1.0.17 (内)	包年包月 2018-03-30 10:58 到期	默认项	改名 调整配置 调整磁盘 调整网络

- On the renaming page, enter a new CVM name, and then click **OK**.

改名

×

您已选 1台 云主机 , [查看详情](#)✓

No.	主机名	主机ID	当前带宽上限	操作
1		ins-cl- 	1 Mbps	可重命名

新云主机名称:

你还可以输入54个字符

确定

取消

Note: The names of multiple CVMs that are renamed by this way are the same.

Reset Instance Password

Last updated : 2018-09-12 16:58:19

If you forget your password, you can reset the login password of the instance on the console. This document introduces how to change the login password of the instance on the CVM console.

Note:

1. Password resetting is only allowed for instances that have been shut down.
2. For a running instance whose password has been modified on the console, the CVM is shut down in the process of password reset. Schedule the time in advance to avoid data loss. You are recommended to perform the operation at the lows of business to minimize the impact.

Resetting Password of Single Instance

- Log in to the [CVM console](#), and select a CVM whose password needs to be reset.
- Click **More** -> **Password/Key** -> **Reset Password** on the page.

ID/主机名	监控/状态	可用区	主机类型	配置	主IP地址	主机计费模式	所属项目	操作
搜索找到3条结果, 返回列表								
<input checked="" type="checkbox"/> ins-4p9p9g	运行中	上海二区	标准型S3	32核 128GB 1Mbps 系统盘: 本地硬盘 网络: 基础网络	10.105.98.166 (内)	包年包月 2018-03-27 20:54 到期	默认项目	登录 续费 更多
<input type="checkbox"/> ins-jayco	运行中	上海一区	标准型S1	1核 1GB 1Mbps 系统盘: 本地硬盘 网络: 基础网络	10.154.25.20 (内)	按量计费 2018-02-01 16:50 创建	默认项	重置密码 加载密钥
<input type="checkbox"/> ins-melody-不要删除	运行中	上海一区	标准型S1	1核 2GB 无限制 系统盘: 本地硬盘 网络: wizard-sh	10.1.0.17 (内)	包年包月 2018-03-30 10:58 到期	默认项目	云主机状态 云主机设置 密码/密钥 配置安全组 弹性网卡 制作镜像 重装系统 分配至项目 弹性IP

- Go to the Reset Password page. If the instance has been shut down, directly select the account whose password needs to be reset, then enter and confirm the new password, and click **Reset**.

重置密码

您已选 1 台 云主机 , [查看详情](#)✓

No.	主机名	主机ID	当前带宽上限	操作
1	candytest关..	ins-[REDACTED]	1 Mbps	可重置密码

用户名

系统默认

系统默认

指定用户名

新密码
Linux 机器密码需8到16位, 至少包括两项 ([a-z,A-Z],[0-9]和 [() `~!@#\$%^&*~+=_[]{};:'<>.,?/] 的特殊符号)

确认密码

确认重置

取消

- Go to the Reset Password page. If the instance is running, select the account whose password needs to be reset, then enter and confirm the new password, and click **Next**. Select **Agree to force shutdown**, and click **Change Now**.

重置密码

×

您已选 1台 云主机 , [查看详情](#)✓

No.	主机名	主机ID	当前带宽上限	操作
1		ins-	1 Mbps	可重置密码

用户名

系统默认

系统默认

指定用户名

新密码

Linux 机器密码需8到16位, 至少包括两项 ([a-z,A-Z],[0-9]和 [() `~!@#\$%^&*~+=_ |{}[]:; '<> ,?/] 的特殊符号)

确认密码

下一步

取消

重置密码

×

您已选 1台 云主机 , [查看详情](#)✓

No.	主机名	主机ID	当前带宽上..	操作
1	██████	ins-██████	1 Mbps	可重置密码

1、为了避免数据丢失，重置密码需要在关机状态下操作，云服务器将关机中断您的业务，请仔细确认

2、强制关机可能会导致数据丢失或文件系统损坏，您也可以主动关机后进行调整配置

3、强制关机可能需要您等待较长时间，请耐心等待

☐ 同意强制关机

去调整

取消

Resetting Password of Multiple Instances

- Log in to the [CVM console](#), and select multiple CVMs whose password needs to be reset.
- Click **Reset password** on the page.
- Go to the Reset password page. If all of the instances have been shut down, directly select the account whose password needs to be reset, then enter and confirm the new password, and click **Reset**.
- Go to the Reset password page. If some instances are still running, select the account whose password needs to be reset, then enter and confirm the new password, and click **Next**. Select **Agree to forced shutdown**, and click **Change Now**.

Change Instance Subnet

Last updated : 2018-08-10 16:15:36

The subnet of the CVM instance in VPC can be directly replaced in the console.

Limits

- The associated CVM restarts automatically after its subnet is replaced.
- The subnet cannot be replaced for the secondary ENI.

Procedure

- Log in to the [CVM Console](#).
- Select a region.
- Click the ID of the instance to go to its details page.
- On the instance details page, click **ENI**, and then click the ID of primary ENI.

[<](#) | ins-akdx415x

[参数](#) [弹性网卡](#) [公网IP](#) [监控](#) [健康检查](#) [安全组](#) [操作日志](#)

云主机绑定弹性网卡后，您需登录云主机配置IP及路由，点击 [查看操作指南](#)

弹性网卡 [绑定网卡](#)

[ins-akdx415x主网卡](#) eni-1g5r4kh8 (主网卡) [分配内网IP](#) [解绑](#)

内网IP	类型	已绑定弹性公网IP	备注	操作
192.168.2.8	主IP	无 绑定	-	修改主IP

- Go to the primary ENI details page, and click **Replace Subnet**.

[返回](#) | **ins-akdx415x主网卡**

基本信息

IP 管理

关联安全组

基本信息

名称	ins-akdx415x主网卡
ID	eni-1g5r4kh8
MAC地址	52:54:00:05:FB:ED
地域	北京
可用区	北京一区
所属网络	vpc-mcg7eo84 (melody_test1 192.168.2.0/24)
所属子网	subnet-7r1jh0qf (melody_test1_1 192.168.2.0/24) 更换子网
绑定云主机	ins-akdx415x 解绑云主机
创建时间	2018-03-05 19:01:14

- Select the new subnet in the pop-up subnet replacement page, enter the new primary IP, and click **OK**. Then, the instance restarts to complete the replacement.

更换子网

×

注意: 更换子网会导致关联的云主机自动重启

请选择您要更换的子网：

请输入关键字

Q

	子网ID/名称	CIDR	
<input type="radio"/>	subnet-7r1jh0qf melody_test1_1	192.168.2.0/24	当前子网

更换子网后将同时更换主IP

新IP:

确定

取消

Note:

- i. If you have not created a subnet in this availability zone, create a new subnet first.
- ii. You can only enter the private IP of the current subnet CIDR.

Change Security Group

Last updated : 2018-09-12 16:55:48

Security group is a stateful virtual firewall for filtering packets and is used to set the network access controls for a single or multiple CVMs. It is a logical grouping and an important means of network security isolation. When a CVM instance is created, you must configure the security group for it. Tencent Cloud supports configuring a new security group for the CVM instance after it is created.

Note:

To configure a new security group for the instance, create a security group first. For more information, please see [Create Security Group](#).

Procedure

- Log in to [CVM Console](#), and select a CVM to be assigned to the new security group.
- Click **More** on the page, and then click **Configure Security Group**.

<div> + 新建 开机 关机 重启 续费 重置密码 更多操作 </div> <div> 所属项目: 默认项目 多个关键字用竖线" "分 Q ↺ ⚙ ⬇ </div>									
<input type="checkbox"/>	ID/主机名	监控/状态	可用区	主机类型	配置	主IP地址	主机计费模式	所属项目	操作
搜索找到3条结果, 返回列表									
<input type="checkbox"/>	ins- [redacted]	运行中	上海二区	标准型S3	32核 128GB 1Mbps 系统盘: 本地硬盘 网络: 基础网络	[redacted] (公) 10.105.98.166 (内)	包年包月 2018-03-27 20:54 到期	默认项目	登录 续费 更多 <div> 云主机状态 > 云主机设置 > 密码/密钥 > 配置安全组 弹性网卡 > 制作镜像 重装系统 分配至项目 弹性IP > 按量转包年包月 </div>
<input type="checkbox"/>	ins-p jayco	运行中	上海一区	标准型S1	1核 1GB 1Mbps 系统盘: 本地硬盘 网络: 基础网络	[redacted] (弹性) 10.154.25.20 (内)	按量计费 2018-02-01 16:50 创建	默认项目	登录
<input type="checkbox"/>	ins-l melody-不要 删除	运行中	上海一区	标准型S1	1核 2GB 无限制 系统盘: 本地硬盘 网络: wizard-sh	[redacted] (公) 10.1.0.17 (内)	包年包月 2018-03-30 10:58 到期	默认项目	登录

- Enter the security group configuration page, and select the name of the new security group (multiple names can be selected), and click **OK** to replace the security group.

配置安全组

您已选 **1台 云主机** , [查看详情](#)✓

No.	主机名	主机ID	当前带宽上限	操作
1		ins- cl...	1 Mbps	可配置安全组

选择处于当前地区和项目的安全组

☒ ID: sg-keo7kh8o Linux安全组放通22端口

☒ ID: sg-pstq8nyk 放通全部端口-20180119151214890

☐ ID: sg-8loxdp1i 放通全部端口-20171222111611371

☐ ID: sg-qrcu57ic jayco

只允许绑定和云主机同一项目和地域的安全组

每个云主机至少需要加入一个安全组, [新建或查看我的安全组详情](#)。

确定

取消

Note:

You can only bind a security group in the same project and region as CVM.

- You can also enter the instance details page, click **Security Group** -> **Bind** to bind the security group.

The screenshot shows the Tencent Cloud console interface for instance `ins-olqpkbgl`. The **安全组** (Security Group) tab is selected. On the left, under **已绑定安全组** (Bound Security Groups), there is a table with one entry: priority 1, ID `sg-keo7kh8o`, name `Linux安全组放通..`, and a **删除** (Delete) button. A **绑定** (Bind) button is highlighted with a red box. On the right, the **规则预览** (Rule Preview) section shows **入站规则** (Inbound Rules) for `Linux安全组放通22端口`. The table below lists the rules:

来源	端口协议	策略	备注
10.0.0.0/8	ALL	允许	-
172.16.0.0/12	ALL	允许	-
192.168.0.0/16	ALL	允许	-
0.0.0.0/0	TCP:22	允许	-

- Enter the security group configuration page, and select the name of the new security group (multiple names can be selected), and click **OK** to replace the security group.

配置安全组

×

请输入关键字

Q

	安全组ID/名称	备注
<input checked="" type="checkbox"/>	sg-qrcu57ic jayco	暴露全部端口到公网和内网，有一定安全风险
<input checked="" type="checkbox"/>	sg-2jz357ca lulutest	仅暴露 SSH 登录的 TCP 22端口到公网，内网端口全通
<input type="checkbox"/>	sg-2ckvnfmo cliffWEB服务	cliff测试，用于web服务
<input type="checkbox"/>	sg-creyp1r8 koko	-
<input type="checkbox"/>	sg-bvdun5xg lpip	-

确定

取消

Search Instance

Last updated : 2018-09-12 14:57:34

By default, the CVM console displays the CVMs for all projects in the current region. To help you quickly search CVMs in the current region, Tencent Cloud provides CVM search feature. You can filter out CVMs by such resource attributes as project, CVM billing method, CVM type, availability zone, IP, CVM ID, and CVM name.

Procedure

1. Log in to the [CVM Console](#), enter the keyword in the search box, and then click the search icon to query the CVMs that match the search criteria.

The screenshot shows the Tencent Cloud CVM console interface. At the top, there's a header with the title '云主机' and a link to the '云服务器使用指南'. Below the header, there's a banner for a promotion. A row of tabs shows various regions, with '上海(3)' selected. Below the tabs, there's a row of buttons: '+ 新建', '开机', '关机', '重启', '续费', '重置密码', and '更多操作'. A search box is present with the text '所属项目: 全部项目' and a search icon. A dropdown menu is open, showing options: '主机名', '主机ID', 'IP', '可用区', '主机类型', and '主机计费模式'. Below the search box, there's a table with columns: ID/主机名, 监控/状态, 可用区, 主机类型, 配置, 主IP地址, and 主机计费模式. The table contains three rows of instance data.

ID/主机名	监控/状态	可用区	主机类型	配置	主IP地址	主机计费模式
[ID]	运行中	上海二区	标准型S3	32核 128GB 1Mbps 系统盘: 本地硬盘 网络: 基础网络	10.105.98.166 (内)	包年包月 2018-03-27 20:54 到期
[ID]	运行中	上海一区	标准型S1	1核 1GB 1Mbps 系统盘: 本地硬盘 网络: 基础网络	10.154.25.20 (内)	按量计费 2018-02-01 16:50 创建
[ID]	运行中	上海一区	标准型S1	1核 2GB 无限制 系统盘: 本地硬盘 网络: wizard-sh	10.1.0.17 (内)	包年包月 2018-03-30 10:58 到期

2. You can click **Help** to view the syntax of search examples.



3. For more syntaxes, please see the following figure.

	输入格式	例子	搜索框展示	说明
单个关键字	【关键字】	10.0.0.1		过滤 包含字符 "10.0.0.1" 的实例
多个关键字	【关键字】【回车】【关键字】	默认项目 www.123.com192.169.23.54		过滤 同时包含三个字符 "默认项目" "www.123.com" "192.169.23.54" 的实例
单资源属性	【资源属性】:【关键字】	内网 IP : 10.0.0.1		过滤 "内网 IP" 为 "10.0.0.1" 的实例
多资源属性	【资源属性】:【关键字】 【回车】【资源属性】:【关键字】	可用区: 广州一区 所属项目: 默认项目		过滤 "可用区" 为 "广州一区"、且 "所属项目" 为 "默认项目" 的实例
单资源属性 多关键字	【资源属性】:【关键字】 【关键字】	所属项目: 默认项目 疯狂越野		过滤 "所属项目" 为 "默认项目" 或 "疯狂越野" 的实例
粘贴字符	{ 粘贴的字符串 }	112.14.128.74 112.14.128.75 112.14.128.76		过滤 包含字符 "112.14.128.74" 或 "112.14.128.75" 或 "112.14.128.76" 的实例

Export Instances

Last updated : 2018-08-10 16:38:46

You can export the CVM instance list of a region in the console, and customize the fields of the list to be exported. You can select a maximum of 25 fields. The fields supported for export include: ID, CVM name, status, region, availability zone, CVM type, operating system, mirror ID, CPU, memory, bandwidth, public IP, private IP, system disk type, system disk size, data disk type, data disk size, network, subnet, associated VPC, creation time, expiry time, CVM billing method, network billing method and project.

Procedure

- Log in to the [CVM console](#).
- Select a region.
- Click the Download All icon.



- On the page of customizing fields to be exported, you can select the fields to export (25 fields at most). Then, click **OK** to export.

自定义导出字段

×

请选择你要导出的字段，最多勾选25个字段，已勾选25个。

<input checked="" type="checkbox"/> ID	<input checked="" type="checkbox"/> 主机名	<input checked="" type="checkbox"/> 状态
<input checked="" type="checkbox"/> 地域	<input checked="" type="checkbox"/> 可用区	<input checked="" type="checkbox"/> 主机类型
<input checked="" type="checkbox"/> 操作系统	<input checked="" type="checkbox"/> 镜像id	<input checked="" type="checkbox"/> CPU
<input checked="" type="checkbox"/> 内存	<input checked="" type="checkbox"/> 带宽	<input checked="" type="checkbox"/> 公网IP
<input checked="" type="checkbox"/> 内网IP	<input checked="" type="checkbox"/> 系统盘类型	<input checked="" type="checkbox"/> 系统盘大小
<input checked="" type="checkbox"/> 数据盘类型	<input checked="" type="checkbox"/> 数据盘大小	<input checked="" type="checkbox"/> 所属网络
<input checked="" type="checkbox"/> 所在子网	<input checked="" type="checkbox"/> 关联vpc	<input checked="" type="checkbox"/> 创建时间
<input checked="" type="checkbox"/> 到期时间	<input checked="" type="checkbox"/> 主机计费模式	<input checked="" type="checkbox"/> 网络计费模式
<input checked="" type="checkbox"/> 所属项目		

确定

取消

Renew Instances

Last updated : 2018-09-12 16:07:30

This document introduces how to renew **prepaid instances**.

- **Prepaid instance:** You can renew or set auto renewal for prepaid instances.
- **Postpaid instance:** Postpaid instances can be automatically activated with sufficient balance in your account. For more information, please see [Online Top-up](#) and [Offline Bank transfer Top-up](#). You can also follow [Balance Alert Instruction](#) to set alert to prevent your instance from being terminated.

Instance Renewal

Prepaid instances can be renewed using various methods. The following example shows the renewal procedure on [CVM Console](#). You can also view the document [Renewal Management via Console](#) to set auto renewal or renew to a certain time, etc.

Instance Renewal via Console

Renew reclaimed instances:

1. Log in to the [CVM Console](#).
2. On the left navigation bar, click **Recycle Bin** -> **CVM Recycle Bin** to enter the CVM reclaiming list.
3. Renew single instance: Find the instance to be renewed in the list, click **Recover** button on the right and finish the renewal payment.
4. Renew instances in batch: Select all instances to be renewed, click **Recover in Batch** on the top and finish the renewal payment.

Renew running instances:

1. Log in to the [CVM Console](#).
2. Renew single instance: Find the instance to be renewed in the list, click **Renew** button on the right and finish the renewal payment.
3. Renew instances in batch: Select all instances to be renewed, click **Recover** button on the top and finish the renewal payment.

Instance Renewal via API

You can use the API `RenewInstances` to renew instances. For more information, please see [Instance Renewal](#).

Set Auto Renewal

You can also view the document [Renewal Management via Console](#) to set auto renewal or renew to a certain time, etc.

Auto Renewal via Console

You can set auto renewal for prepaid instances to eliminate the need to renew the instances whenever they are about to expire:

1. Log in to [Tencent Cloud Console](#), move the mouse cursor to **Fees** at the top right corner, and then select **Renew** in the menu.
2. Click **Set Auto Renewal** on the right of the prepaid instance to be renewed.
3. Click **OK** button in the popup dialog box.

For instances set to auto renewal, the charge for the next billing period is automatically deducted from the balance on the expiry date. If you have a sufficient account balance, the instance goes into the next billing period automatically.

Auto Renewal via API

You can use the API `SetAutoRenew` to set auto renewal for instances. For more information, please see [Set Auto Renewal for Instances](#).

Shutdown Instances

Last updated : 2018-09-12 15:43:06

The instance can be shut down when you need to stop the instance service or modify the configurations only for the instance that have been shut down. Shutting down an instance is like shutting down a local computer.

Overview

- **Preparation for shutdown:** The instance will no longer function to provide services after shutdown. Make sure the CVM has stopped receiving service requests before shutdown.
- **How to shut down a instance:** You can shut down instances by using system commands (such as the shutdown command under Windows system and Linux system) or on the Tencent Cloud console. It is recommended to view the shutdown process on the console to check whether any problem occurs.
- **Shutdown process:** The instance will be shut down. The status of the instance will first change to "shutting down" and then "off" after it has been shut down. Overlong shutdown may cause problems. For more information, please see [shutdown-related information](#) to avoid forced shutdown.
- **Data storage:** All the storage of the instance will remain connected to the instance, and all disk data are saved. Data in memory will be lost.
- **Physical attributes of instances:** Shutting down an instance does not change any of its physical attributes. The instance public IP and private IP remain unchanged, and [Elastic Public IP](#) maintains a binding relationship, but accessing these IP will get you an error response (for stopped services); if the instance is part of the [Classiclink](#), this interconnection will remain unchanged.
- **Load balancer:** If the shutdown instance belongs to [Real Server Cluster of Load Balancer Instances](#), it will no longer function to provide services after shutdown. If the load balancer instance is configured with the health check policy, such shutdown instance will be automatically blocked from the request; but if not, the client may receive a 502 error code. For more information, please see [Health Check](#).
- **Auto scaling:** If the shutdown instance is in an [auto scaling group](#), the Auto Scaling service will mark shutdown instance as poor performance, move the same out of the auto scaling group and launch a replacement instance. For more information, please see [Auto Scaling Product Documentation](#).

Shutdown Instance via the Console

1. Log in to the [CVM Console](#).
2. Shut down an instance: Select the instance to be shut down, and click **Shutdown** at the top of the list or click **More** -> **CVM Status** -> **Shutdown** in the Operation column on the right side.

3. Restart an instance: Select all the instance to be shut down, and click **Shutdown** at the top of the list. Instances can be shut down in batches. Reasons are given for instances that cannot be shut down.

Shutdown instance via API

For more information, please see the [API StopInstances](#).

Modify a Instance that Has Been Shut Down

You cannot modify the following instance attributes until the instance has been shut down.

- **Instance configuration (CPU and memory):** To change the instance type, please see [Adjust the Instance Configuration](#).
- **Size of a mounted cloud disk:** To adjust the size of a cloud disk, please see [Expanding Capacity of Cloud Disks](#).
- **Change password:** Please see [Login Password](#).
- **Load key:** Please see [SSH Key](#).

Restart Instances

Last updated : 2018-09-12 15:39:27

Reboot is a necessary method to maintain CVM. Rebooting CVM instances is equivalent to restarting operating systems of local computers. It is recommended that users reboot instances using the reboot operation provided by Tencent Cloud rather than running reboot command in instances (such as restart command in Windows and Reboot command in Linux). Generally speaking, it takes only a few minutes to reboot your instances after the reboot operation is performed, but instances are unable to provide services during rebooting. Therefore, please make sure the CVM has stopped receiving service requests before rebooting.

Since the physical characteristics of instances are not changed after the reboot, the Public IP address and Private IP address of, and any data stored in the instances will not be altered.

Rebooting instances will not start a new billing period. The length of time for use of postpaid instance will be kept, which will not affect its price range.

Use console to reboot instances

- 1) Open [CVM console](#).
- 2) To reboot a CVM instance running solely, click "Reboot" on the action bar to the right side.
- 3) To reboot CVM instances running in batch, check all the CVMs to be rebooted, and click "More" - "Reboot" on the top of the list. Reasons will be given for CVMs that cannot be rebooted.

Use API to reboot instances

Please refer to [RestartInstances API](#).

Reinstall System

Last updated : 2018-06-25 14:30:10

System reinstallation enables instances to recover to a newly started status. It is a recovery method when CVM instances are suffering software failures. CVM instances support reinstallation of different types of systems. Whether you choose to change to a Linux series system or a Windows series system, Tencent Cloud will offer various-sized system disks to you.

It should be noted that reinstalling the system will result in loss of all contents of **system disks**. Data in data disks will not be affected, but need to be re-recognized. Therefore, in case that system operation data need to be retained, it is strongly recommended that you [Create Custom Image] (/doc/product/213/4942) before reinstalling the system and decide whether to use the image for reinstallation.

Sizes of system disks of different operating systems

- If the newly purchased Linux CVM comes with a cloud block storage, it can support a system disk of 20GB - 50GB.
- If the newly purchased Linux CVM comes with a local disk, it can support a system disk of 20GB.
- A newly purchased Windows CVM with any type of hard disk supports a system disk of 50GB.

Charges for system disks

- For Linux instance system disks, the first 20GB of Tencent Cloud is free of charge. If the system disk supports capacity adjustment (i.e. if it is a Cloud Block Storage), the part beyond 20GB will be charged as per the charging standard of Cloud Block S
- For Windows instance system disks, the first 50GB of Tencent Cloud is free of charge. Since Windows instances do not support system disk capacity adjustment, no fees will be charged for system disks of Windows instances.

Use console to reinstall system

- 1) Open [CVM Console](#).
- 2) For CVM instances that requires system reinstallation, click "More" - "Reinstall System" on the action bar to the right side.

3) In the pop-up box of system reinstallation, select the image used by the current machine or other images.

4) If other operating systems are needed, choose from the images provided by Tencent Cloud. Click "Reinstall System".

Note:

- Do not perform other operations during system disk reinstallation.
- The data in current system disks cannot be recovered after system disk reinstallation.
- The data in data disks will be retained and will not be affected after system disk reinstallation, which however need to be mounted manually before use.

Questions about the switching between Windows system instances and Linux system instances

Can the system disk of an old user's Linux CVM that comes with a local disk be scaled out to 20GB?

For a Linux CVM that comes with a local disk of 8GB, the system disk can be scaled out to 20GB by reinstalling the system.

A user has purchased a Linux CVM that comes with an over-20GB Cloud Block Storage. How the charges are calculated if the user reinstalls the operating system and changes it to Windows?

If a user purchases a Linux CVM that comes with an over-20GB Cloud Block Storage, and then changes the operating system to Windows, the charges will be calculated based on the billing mode:

- If the CVM is based on an annual or monthly plan, a refund will be made (exclusive of the amount of voucher used in payment) or the price will be lowered according to the payment conditions.
- If the CVM is based on charge-by-quantity, the calculation of configuration charge for the part exceeding 20GB 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 the charges are calculated if the user reinstalls the operating system and changes it to Linux?

Since the current system disk does not support capacity reduction, when a 50GB 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 20GB is free of charge, and fees for another 30GB shall be paid). See [Hard Disk Prices](#) for details

Terminate Instances

Last updated : 2018-09-12 15:50:25

This document describes how to terminate an instance. For more information on expiration, please see [Expiry Reminder](#).

Overview

- **Manual termination:** Prepaid instances can be terminated by users before they expire. Instances are retained in the recycle bin for 7 days once terminated, and can also be terminated completely in the recycle bin. Postpaid instances can be terminated manually.
- **Timed termination:** Timed termination is supported for postpaid instances. Select a time later than the current time to terminate a resource, with an accuracy down to second. You can set a new termination time to overwrite the previous one.
- **Automatic termination:** Prepaid instances that have not been restored after being retained in the recycle bin for 7 calendar days are automatically terminated. Postpaid instances are automatically terminated when your account balance has remained below 0 for 24 hours. You can continue to use them if you finish [Renewal](#) within a specified period of time.
- **Instance data:** Local disks and non-elastic cloud disks mounted to instances are also terminated, and the data on these disks will be lost. Back up the data in advance. Elastic cloud disks are not affected.
- **Billing:** When an instance is being terminated or has been terminated, no expenses related to this instance are incurred.
- **EIP:** EIPs (including IPs on the secondary ENI) of a terminated instance are retained, and idle IPs may incur expenses. If you do not need these IPs, release them in time.

Terminating Prepaid Instance

Terminating Unexpired Instance on the Console

A prepaid instance can be terminated if you no longer need it. When an instance is being terminated or has been terminated, no expenses related to this instance are incurred. The instance is then moved to the CVM recycle bin and kept for 7 days, and services running on this instance are completely suspended.

When a prepaid instance is returned, the local disks and non-elastic cloud disks mounted to this instance are also returned, and the data stored on these disks will be lost. However, the elastic cloud disks mounted to this instance are retained, and the data will not be affected.

1. Log in to the [CVM Console](#).

2. Terminate a single instance: Find the instance to be terminated in the list, and click **Terminate** in the Operation column.
3. Terminate instances in batches: Select all the instances to be terminated, and click **Terminate** on the top.
4. In the pop-up box, confirm the information related to the CVM to be terminated, and click **OK**. Then, you are directed to **Check Refund Information** page.
5. Carefully check the refund information related to the instance. After **Confirm Refund** is submitted, refund is initiated and the instance is terminated.
For more information on how to return a prepaid instance, please see [Refund Rules for Terminated Prepaid Instances](#).

Completely Terminating Prepaid Instances in Recycle Bin

You can terminate prepaid instances retained in the [Recycle Bin](#) through the console.

1. Log in to the [CVM Console](#).
2. On the left navigation bar, click **Recycle Bin** -> **CVM Recycle Bin** to enter the CVM reclaiming list.
3. Terminate a single instance: Find the instance to be terminated in the list, and click **Terminate** in the Operation column.
4. Terminate instances in batches: Select all the instances to be terminated, and click **Terminate** on the top.
5. Enter the verification code in the pop-up box, and click **OK** to complete the termination process.

Terminating Postpaid Instances

A terminated postpaid instance is still visible in the console within a short period of time. It will be automatically removed from the instance list later, and its services will be completely suspended.

Terminating Instances on the Console

1. Log in to the [CVM Console](#).
2. Terminate a single instance: Find the instance to be terminated in the list, and click **More** -> **CVM Status** -> **Terminate** on the right side.
3. Terminate instances in batches: Select all the instances to be terminated. On the top of the list, click the **More** drop-down box, and then click **Terminate**. Reasons are given for instances that cannot be terminated.

Setting Timed Termination

Setting at the Time of Purchase

1. Log in to the CVM purchase page.
2. Select Postpaid, region, model, image, storage, bandwidth and other data. Check "**Timed Termination**" on the "**Information Setting**" page, and set the date and time for timed termination, with an accuracy down to second.

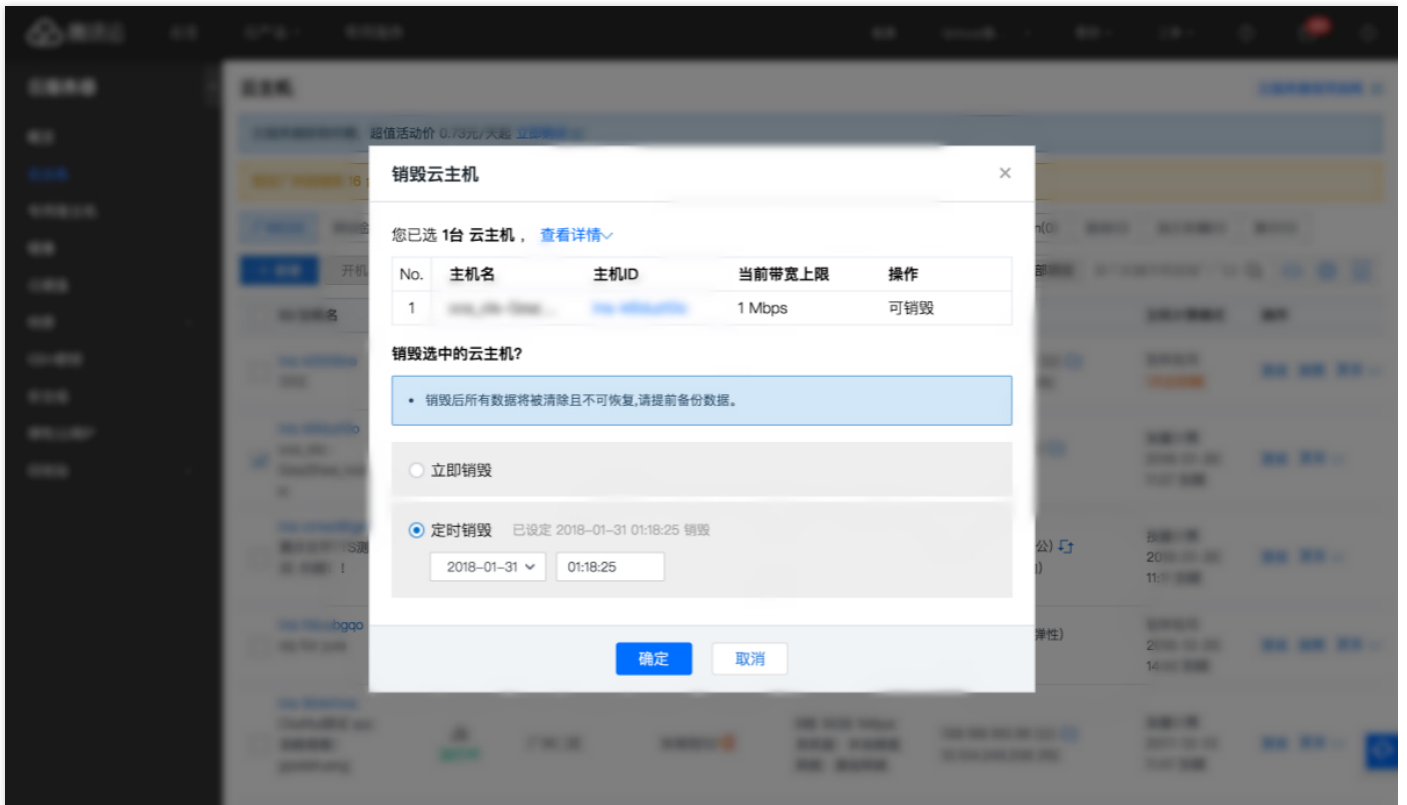
The screenshot displays the '4. 设置信息' (4. Information Setting) step of the CVM purchase process. It includes sections for '安全组' (Security Group), '安全加固' (Security Enhancement), '云监控' (Cloud Monitoring), and '定时销毁' (Timed Termination). The '定时销毁' section is highlighted with a red box, indicating that '开启定时销毁' (Enable Timed Termination) is checked, and the termination time is set to '2018-01-31 01:19:40'. Below this, the '费用' (Fees) section shows '配置费用' (Configuration Fee) at 0.26 元/小时 and '网络费用' (Network Fee) at 0.80 元/GB. At the bottom, there are buttons for '上一步' (Previous Step) and '开通' (Enable/Activate).

3. Click Enable, and all the instances with timed termination enabled will be terminated at the specified time.

Setting via Console

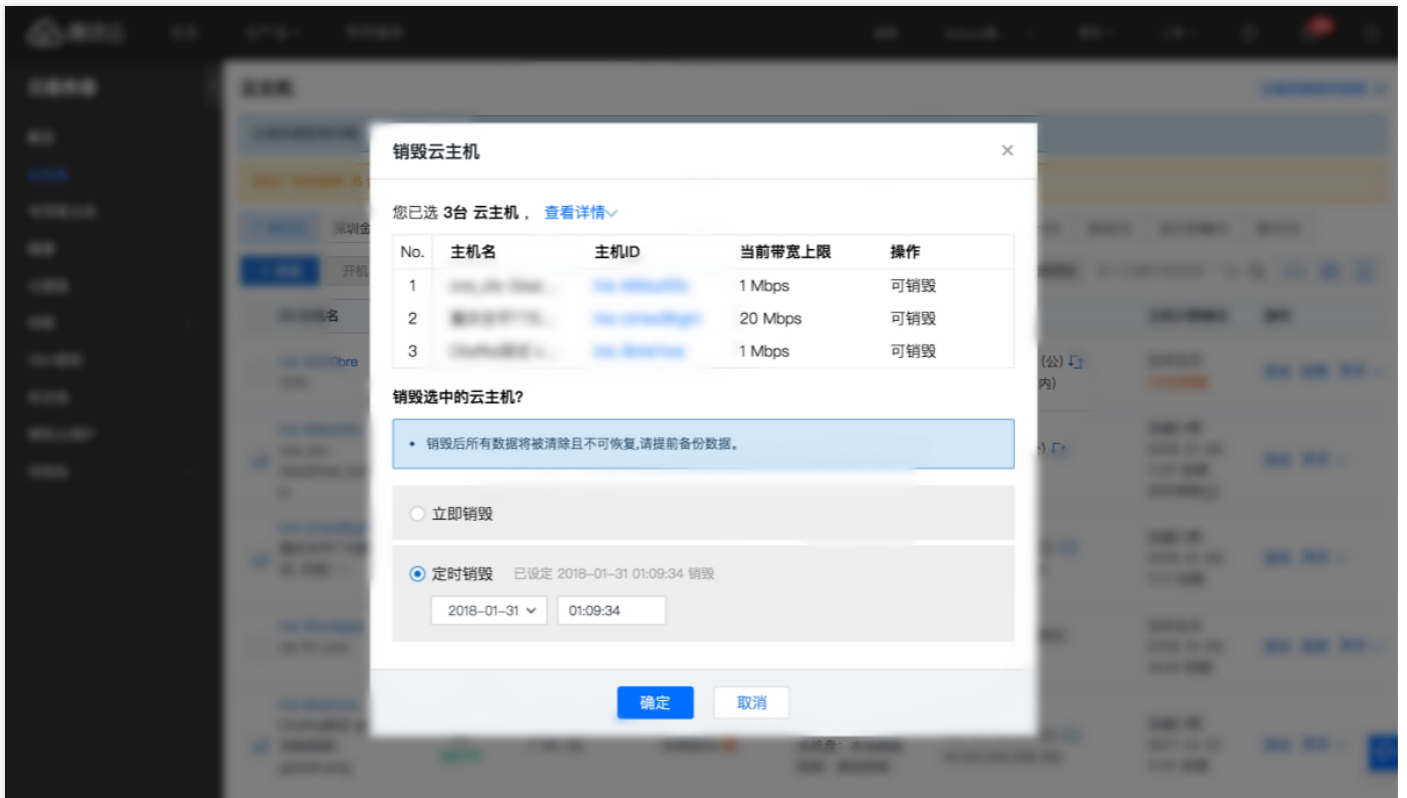
1. Log in to the [CVM Console](#).
2. **Set timed termination for a single instance:** Find the instance to be terminated, and click **More** -> **CVM Status** -> **Terminate** on the right. Select Timed Termination in the pop-up box, and set the date

and time for timed termination, with an accuracy down to second.



3. **Terminate instances in batches:** Select all the instances to be terminated. On the top of the list, click the **More** drop-down box, and then click **Terminate**. Set the date and time for timed termination, with

an accuracy down to second. Reasons are given for instances that cannot be terminated.

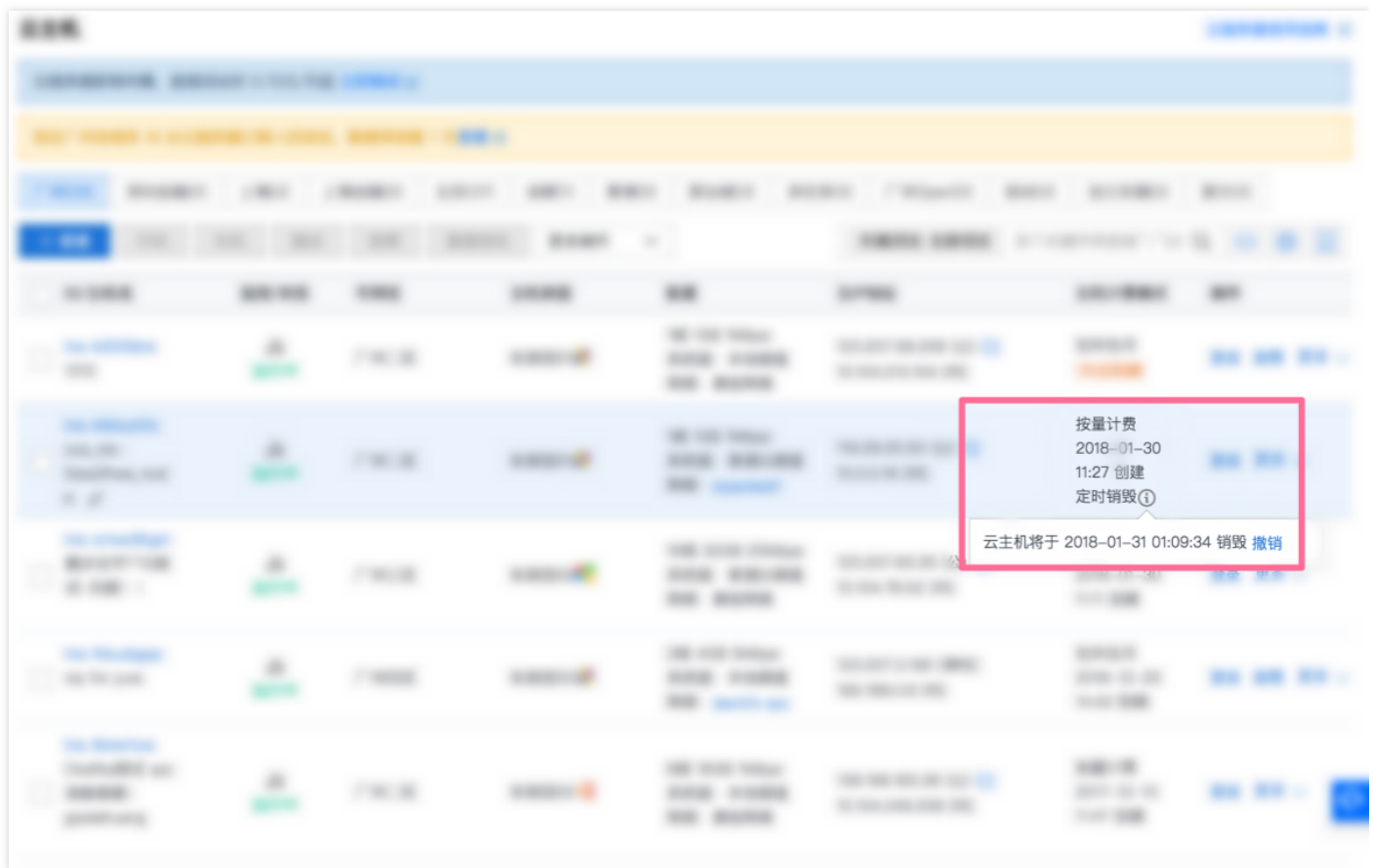


4. Confirm the information of instances for timed termination, and click "OK" to complete the setting.

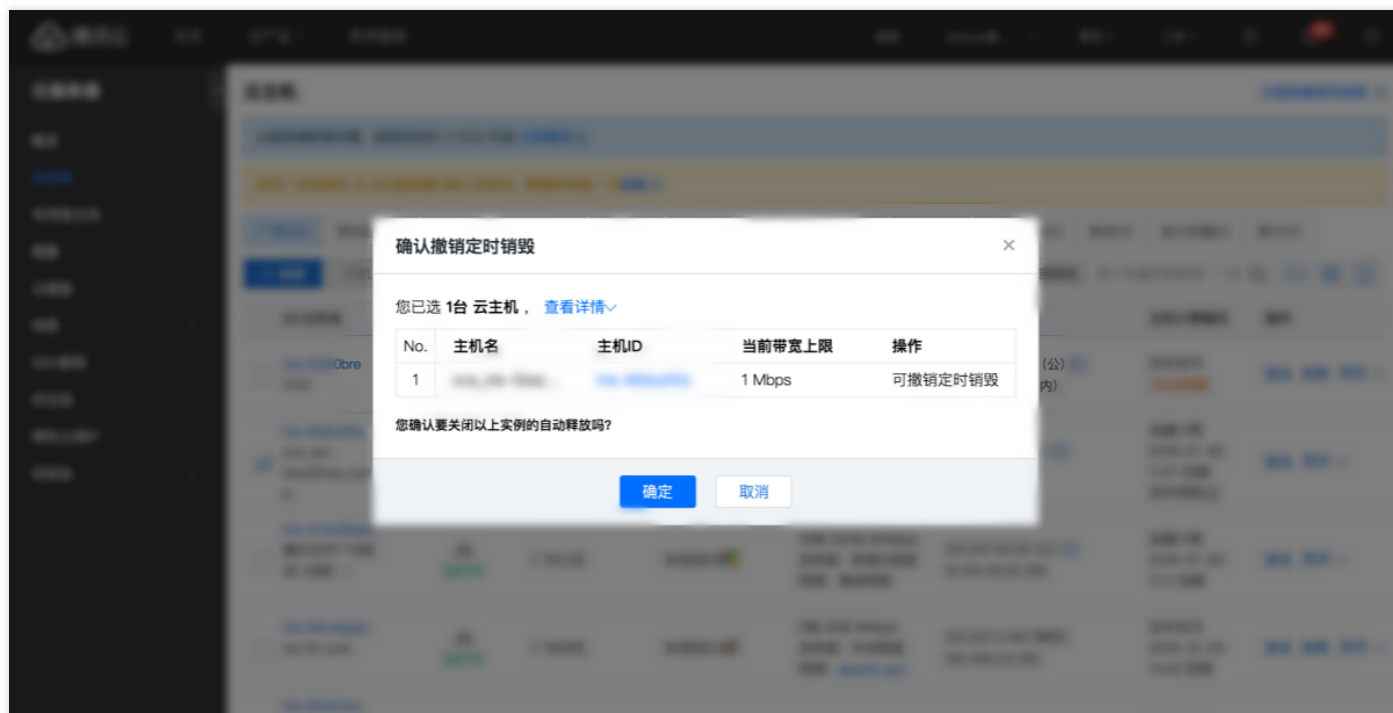
Canceling Timed Termination

1. Log in to the [CVM Console](#).
2. **Cancel timed termination for a single instance:** Find the instance for which timed termination needs to be canceled, then click the icon beside the "Timed Termination" in the "CVM Billing Method"

column, and click "**Cancel**" in the pop-up tips.



3. Confirm the information of the selected instance in the pop-up box, and click **OK**. Cancellation of timed termination takes effect immediately.



Terminating Instances using API

For more information, please see the [API TerminateInstances](#).

Instance Expires

Last updated : 2018-09-12 15:52:19

This document describes the reclaiming mechanism of an instance and the operation method for recovering an instance. For more information on expiration, please see [Expiry Reminder](#).

Reclaiming Instance

Tencent Cloud Recycle Bin is a cloud service reclaiming mechanism. The prepaid instance will be shut down on the expiry date or on the day when it is actively terminated before expiry, and then is automatically put into the recycle bin. The instance configured with auto renewal is automatically renewed if account balance is sufficient. No reclaiming mechanism is provided for postpaid instances.

- **Retention time:** The instance is retained for 7 calendar days in the recycle bin.
- **Expiry processing:** If the instance is not renewed within 7 days, the system will release resources and start to automatically [Terminate Instance](#).
- **Mounting relationship:** After being put into the recycle bin, the instance will be **forced to terminate** the mounting relationship with CLB, elastic public IP, elastic cloud disk, secondary ENI, and Classiclink. The mounting relationship **cannot be recovered** after renewal, you have to reset it.
- **Operation limits:** You can only [renew](#) or [terminate](#) the instances in the recycle bin.

Recovering Instance

1. Log in to the [CVM Console](#).
2. On the left navigation bar, click **Recycle Bin** -> **CVM Recycle Bin** to enter the CVM reclaiming list.
3. Recover single instance: Find the instance to be recovered in the list, click **Recover** button, and complete the renewal payment.
4. Recover instances in batch: Select all instances to be recovered, click **Recover in Batch** on the top, and complete the renewal payment.

Images

Create Custom Images

Last updated : 2018-09-12 15:55:33

Overview of Creation

Common steps

You can launch an instance with a public image or a service marketplace image, and then connect to the instance and deploy your software environment. If the instance runs normally, you can create a new custom image based on this instance as needed, so that you can use this image to launch more new instances that have the same custom configurations with the original one.

Best practice

- **Shut down instance:**

Shut down the instance before you can create a custom image to ensure that the image has exactly the same deployment environment as that of the current instance.

- **Data migration:**

To keep the data in the original instance data disk when you launch a new instance, you can first take a [Snapshot](#) of the data disk, and then create a new CBS data disk with this snapshot when launching the new instance. For more information, please see [Create Cloud Disk from Snapshot](#).

Limit

- Each region supports a maximum of 10 custom images.

Notes

1. The following directory and files will be removed.
2. /var/log/
3. /root/.bash_history, /home/ubuntu/.bash_history (Ubuntu system)
4. /etc/fstab will reset to avoid launch failure due to no data disk found.

Creation Method

Create an image from an instance via the console

1. Log in to the [CVM Console](#).
2. Shut down the instance. Select the instance to be shut down, and then click **Shutdown** on the top.
3. Click **More** on the right side of the instance used to create an image, and click **Create Image**.
4. Enter **Image Name** and **Image Description** in the pop-up box, and click **OK** to submit the creation application.
5. Move your mouse to **Recent Operations (clock icon)** on the upper right corner to view the progress of creation.
6. After the image is created, click **Image** in the left navigation bar, or click on the image ID in **Recent Operations (clock icon)**, and then you are redirected to the image list to view details.
7. To purchase a server with the same image as the previous one, click **Create CVM** on the right side of the image in the image list.



Create an image using API

You can use the API `CreateImage` to create a custom image. For more information, please see the API [Create Image](#).

Copy Images

Last updated : 2018-09-12 15:57:31

Cross-region Copying allows you to quickly deploy the same CVM instances in different regions.

Deploying the same CVM instance in different regions using image synchronization is a reliable way to improve application robustness.

Synchronizing images to different regions on Console

- 1) Log in to [CVM Console](#).
- 2) Click **Image** in the navigation pane.
- 3) Check all images you want to copy, click the **Cross-region Copying** at the top.
- 4) Select the destination region, and click **OK**.
- 5) After successful synchronization, the image list status in the destination region is updated to 100%.

Synchronize images to different regions via API

You can use the SyncCvmlImage API to synchronize images. For details, refer to [SyncCvmlImage API](#).

Share Custom Images

Last updated : 2018-09-12 16:03:04

Shared image means that you share a custom image that you have created with others users. You can easily get shared images from other users, to get necessary components and then add custom contents.

Note that Tencent Cloud cannot guarantee the integrity or security of the shared images from other users. Please use only shared images from reliable sources.

Sharing Images

Obtaining Account of the Counterpart

To share an image with another user, you need to obtain his/her unique account ID. You can inform him of obtaining your ID in this way:

- 1) Log in to Tencent Cloud console, and click the account name in the upper right corner.
- 2) View the account ID in your personal information.

The screenshot displays the 'Account Center' interface. On the left is a sidebar menu with options: 'Account Center', 'Account Information' (highlighted), 'Security Setting', 'Project Management', and 'Identity Verification'. The main content area is titled 'Account Info' and contains a 'Basic Info' section. This section lists the following details: 'Register Account' with an email icon and address '1302000590@qq.com'; 'Account ID' with an information icon and the value '100000624047' (which is highlighted with a red rectangular box); 'APPID' with an information icon and the value '1253702919'; 'Role' set to 'Creator'; 'Nickname' set to '1302000590@qq.com' with a 'Modify' button next to it; and 'Permissions' listed as 'overall situation(Manage cloud resources, financial affairs and collaborators)'.

Account Center	
Account Information	Account Info
Security Setting	Basic Info
Project Management	Register Account ⓘ : 1302000590@qq.com
Identity Verification	Account ID ⓘ : 100000624047
	APPID ⓘ : 1253702919
	Role: Creator
	Nickname: 1302000590@qq.com Modify
	Permissions: overall situation(Manage cloud resources, financial affairs and collaborators)

Sharing Images on Console

- 1) Log in to [Tencent Cloud Console](#).

- 2) Click **CVM – Image** in the navigation pane.
- 3) Click the **Custom Images** tab, and select the custom image you want to share.
- 4) Click the **Share** button, enter the unique Tencent Cloud account ID of the counterpart, and click **OK**.
- 5) Inform him of logging in to [Tencent Cloud Console](#) and select "CVM" - "Image" - "Share Image", to view the image that you has shared with him.
- 6) To share this image with multiple users, repeat the above steps until you have added all users.

Sharing Images via API

You can use the [ShareImage API](#) to share images.

Using Shared Images

Shared images can only be used to launch CVM instances. For details, refer to [Purchase and Start Instances](#).

Cancel Image Sharing

Last updated : 2018-09-12 16:19:45

You can at any time cancel the status of sharing images with others. This operation does not affect instances that other users have created using this shared image, but other users can no longer see the image or create more new instances using this image.

Cancel image sharing on Console

- 1) Open [Tencent Cloud Console](#).
- 2) Click **CVM – Image** in the navigation pane.
- 3) Click the **Custom Images** tab. Find out the custom image you want to cancel sharing and click **More – Cancel Sharing**. Select the account you want to unshare, click the "Unshare" button and confirm the operation to unshare the image.

Cancel image sharing via API

You can use the [CancelShareImage API](#) to cancel image sharing.

Delete Custom Images

Last updated : 2018-09-12 16:05:50

After using the custom image, you can delete it. When you delete a custom image, you will not be able to use this image to [start a new CVM instance](#), but any instances that are already started will not be affected. If you want to remove all instances that were purchased and started from this image, you can refer to [Expiration of Prepaid Instances](#) or [Terminate Postpaid Instances](#).

- If you have already shared a custom image to others ([see here](#)), you cannot delete it. You need to cancel all of its sharing before deleting a custom image.
- You can only delete the custom image, but neither the common image nor the shared image.

Deleting custom images on Console

- 1) Open [Tencent Cloud Console](#).
- 2) Click **CVM – Image** in the navigation pane.
- 3) Click the "Custom Images" tab, and select the custom image you want to share in the list.
- 4) Click the "Delete" button and confirm the operation, to delete all selected custom images. In case of failed deletion, the reasons will be prompted above the image.

Deleting custom images via API

You can use the [DeleteImages API](#) to delete images. For details, refer to

Import Images

Overview

Last updated : 2018-09-12 19:47:54

In addition to the [Create Custom Image](#) feature, Tencent Cloud also supports image import feature. You can import an image file of a server system disk on the local machine or another platform into the CVM custom images. After the image is imported, you can use it to create a CVM or reinstall the system for an existing CVM.

Preparations for Import

Applying for Permission

Before using this feature, make sure that you have activated the image import permission. If you need to activate the permission, contact the Business Manager and submit relevant information to the ticket system.

Prepare the image file

You need to prepare an image file that meets the import limits in advance.

- **Limits on Linux images:**

Image Attribute	Condition
Operating system	<ul style="list-style-type: none">• The image that is based on CentOS, Ubuntu, Debian, CoreOS, OpenSUSE, and SUSE distributions.• Both 32-bit and 64-bit systems are supported.
Image format	<ul style="list-style-type: none">• The image formats such as RAW, VHD, QCOW2 and VMDK are supported.• Use <code>qemu-img info imageName grep 'file format'</code> to check the image format.
Image size	<ul style="list-style-type: none">• Use <code>qemu-img info imageName grep 'disk size'</code> to check the actual size of the image if it does not exceed 50 GB.• Use <code>qemu-img info imageName grep 'virtual size'</code> to check the vsize of the image if it does not exceed 500 GB.• Note: Check the image size when you import an image, which is subject to the information of the image that is converted to the QCOW2 format.

Image Attribute	Condition
Network	<ul style="list-style-type: none"> Tencent Cloud provides the <code>eth0</code> network interface for the instance by default. Tencent Cloud does not support IPV6. You can query the network configuration of an instance through the metadata service in the instance. For more information, please see Instance Metadata.
Driver	<ul style="list-style-type: none"> The virtio driver of the visualization platform KVM must be installed in the image. For more information, please see Import Image to Linux to Check virtio Driver. It is recommended to install cloudinit for the image. For more information, please see Import Image to Linux to Install cloudinit. If cloudinit cannot be installed in the image for some reason, you can configure the instance manually by referring to Forced Import.
Limit on Kernel	<ul style="list-style-type: none"> Native kernel is preferable for an image. Any modifications may cause failure in importing the image into the CVM.

• **Limits on Windows images:**

Image Attribute	Condition
Operating system	<ul style="list-style-type: none"> Microsoft Windows Server 2008 R2 (Standard Edition, Datacenter Edition, Enterprise Edition), Microsoft Windows Server 2012 R2 (Standard Edition). Both 32-bit and 64-bit systems are supported.
Image format	<ul style="list-style-type: none"> The image formats such as RAW, VHD, QCOW2 and VMDK are supported. Use <code>qemu-img info imageName grep 'file format'</code> to check the image format.
File system type	<ul style="list-style-type: none"> Only NTFS file system using the MBR-style partition is supported. GPT-style partition is not supported. Logical Volume Management (LVM) is not supported.
Image size	<ul style="list-style-type: none"> Use <code>qemu-img info imageName grep 'disk size'</code> to check the actual size of the image if it does not exceed 50 GB. Use <code>qemu-img info imageName grep 'virtual size'</code> to check the vsize of the image if it does not exceed 500 GB. Note: Check the image size when you import an image, which is subject to the information of the image that is converted to the QCOW2 format.

Image Attribute	Condition
Network	<ul style="list-style-type: none">Tencent Cloud provides the Local Area Connection network interface for the instance by default.Tencent Cloud does not support IPV6.You can query the network configuration of an instance through the metadata service in the instance. For more information, please see Instance Metadata.
Driver	<ul style="list-style-type: none">The virtio driver of the visualization platform KVM must be installed in the image. If it is not installed in the Windows system by default, you can install the Windows virtio driver, and then export the local image.
Other	<ul style="list-style-type: none">The imported Windows image does not provide the Windows Activation service.

Importing Steps

1. Log in to the [CVM Console](#).
2. Click **Image** in the left navigation bar.
3. Click **Custom Image**, and then click the **Import Image** button.
4. As instructed in the steps, you need to [Enable Cloud Object Storage](#), [Create bucket](#), then **Upload the image file to the bucket and get Image file URL, and then click **Next**.**
5. Fill in the form according to the actual situation. Be sure to enter the correct COS file URL, and then click **Import**.
6. You will be notified whether the import is successful or failed via internal message.

Error Codes

Error Code	Reason	Recommended Processing Method
InvalidUrl	COS link is invalid	Check if the COS file URL is the same as the imported image URL.
InvalidFormatSize	The format or size is unqualified.	The image must meet the limits on Image format and Image size in Preparations for Import .
VirtioNotInstall	The virtio driver is not installed	Install the virtio driver in the image by referring to the Driver section in Preparations for Import .

Error Code	Reason	Recommended Processing Method
PartitionNotPresent	The partition information is not found	The image is corrupted probably because it is created incorrectly.
CloudInitNotInstalled	cloud-init is not installed	Install cloud-init in the Linux image by referring to the `Driver' section in Preparations for Import .
RootPartitionNotFound	The root partition is not found	The image is corrupted probably because it is created incorrectly.
InternalError	Other errors	Contact customer service

Linux Image Production

Last updated : 2018-08-06 11:48:14

1. Preparations

Check the followings before exporting a system disk image. Ignore them if you're exporting a data disk image.

- OS partition - Service Migration does not support GPT-style partition.

```
sudo parted -l /dev/sda | grep 'Partition Table'
```

"msdos" represents MBR-style partition, and "gpt" represents GPT-style partition.

- Check the startup mode. Service Migration does not support starting the system with EFI.

```
sudo ls /sys/firmware/efi
```

If the EFI file exists, then the current system starts in the EFI mode, and it is necessary to confirm that there is a traditional startup item in grub.

- Check the network configuration. Service Migration does not support IPv6 nor multi-ENI. Services that rely on both IPv6 and multi-ENI cannot work normally.
- Check system-critical files, including but not limited to the following system files:

Follow the standards of relevant distributions to ensure that the locations and permissions of the system-critical files are correct and the files can be read and written normally.

- /etc/grub/grub.cfg: In the kernel parameter, uuid is recommended for mounting root. Other methods (such as root=/dev/sda) may cause the failure in starting the system.
- /etc/fstab: Do not mount other disks. After migration, the system may fail to start due to disk missing.
- /etc/shadow: It has normal permissions and can be read and written.

- Unmount the drivers and software that produce conflicts (including VMware tools, Xen tools, Virtualbox GuestAdditions and other software that comes with underlying drivers).
- Check the virtio driver: Please see [Check virtio Driver in Linux System](#).
- Install cloud-init: Please see [Install cloud-init](#).
- Check other hardware-related configurations, such as driver settings in the Linux desktop environment. Changes to the hardware on the cloud include but not limited to:
 - Replacing the graphics card with cirrus vga.
 - Replacing the disk with virtio disk. Device name is vda, vdb, and so on.
 - Replacing the ENI with virtio nic. By default, only eth0 is available.

Determining Partitions and Sizes

Use the mount command to confirm the current partition format and determine the partitions to be copied and their sizes.

Example:

```
mount
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sys on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
dev on /dev type devtmpfs (rw,nosuid,relatime,size=4080220k,nr_inodes=1020055,mode=755)
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
```

```
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
systemd-1 on /home/libin/work_doc type autofs (rw,relatime,fd=33,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=12692)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=39,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=12709)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
configfs on /sys/kernel/config type configfs (rw,relatime)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=817176k,mode=700,uid=1000,gid=100)
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1000,group_id=100)
```

According to the example, the root partition is `/dev/sda1`, and no boot or home partition is created independently. You can copy the entire sda or copy it to the end of sda1.

The exported image should contain at least the root partition and mbr. If `/boot` and `/home` partitions are created, you also need to include these two independent partitions.

Note:

"mbr" should be included when you copy sda, otherwise the system cannot start. Even if the boot partition is included in sda1, the system may fail to start without mbr, so sda must be copied.

Exporting Images with Tools

For more information on how to use image export tools of VMWare vCenter Convert, Citrix XenConvert and other virtualization platforms, please see the relevant document of each platform. The image formats supported by Tencent Cloud Service Migration include qcow2, vhd, raw, and vmdk.

Exporting Images with Commands

Use qemu-img command

Example:

```
sudo qemu-img convert -f raw -O qcow2 /dev/sda /mnt/sdb/test.qcow2
```

This command is used to export the entire `/dev/sda` disk to `/mnt/sdb/test.qcow2`. Another disk or other network storage should be mounted to `/mnt/sdb`.

To change to other parameters, you need to modify the `-O` parameter. The following parameters are available:

Value | Description

---|---

qcow2 | qcow2 format

vpc | vhd format

vmdk | vmdk format

raw | None

Use dd command

Example:

```
sudo dd if=/dev/sda of=/mnt/sdb/test.img bs=1K count=$count
```

The image exported using `dd` is in raw format and needs to be converted again. The `count` parameter determines the number of bytes to be copied, which can be queried with the `fdisk` command:

```
fdisk -lu /dev/sda
```

```
Disk /dev/sda: 1495.0 GB, 1494996746240 bytes
255 heads, 63 sectors/track, 181756 cylinders, total 2919915520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0x0008f290
```

```
Device Boot Start End Blocks Id System
/dev/sda1 * 2048 41945087 20971520 83 Linux
/dev/sda2 41945088 46123007 2088960 82 Linux swap / Solaris
/dev/sda3 46123008 88066047 20971520 83 Linux
/dev/sda4 88066048 2919910139 1415922046 8e Linux LVM
```

From the above, the `sda1` ends at `41945087 * 512 bytes`, so the copy size is 20,481 MB.

The `count` parameter can be ignored in case of full disk copy.

Note:

Manual export with commands poses a large risk. For example, the file system's metadata may be corrupted when io is busy. It is recommended to check that the image is intact and correct after it is exported.

5. Converting Image Format

The image formats supported by Tencent Cloud Service Migration include qcow2, vpc, vmdk, and raw. It is recommended to use a compressed image format to reduce the time for transmission and migration.

The image exported using dd is in raw format, which should be converted to qcow2 or vhd.

Convert the image format using the qemu-img command:

```
sudo qemu-img convert -f raw -O qcow2 test.img test.qcow2
```

- `-f` is the source image file format.
- `-O` is the destination image file format.

For parameters, please see [Exporting Images with Commands](#)

6. Checking Image

As mentioned above, an error may be occurred with the image file system if it is created when the server is not shut down or due to other reasons. Therefore, you are recommended to check whether the created image is error-free.

When the image format is consistent with the format supported by the current platform, you can directly open the image to check the file system.

For example, vhd images can be directly added to Windows platform, qcow2 images can be opened using qemu-nbd on Linux platform, and vhd images can be enabled directly on Xen platform.

Take the Linux platform as an example:

```
modprobe nbd  
qemu-nbd -c /dev/nbd0 xxxx.qcow2  
mount /dev/nbd0p1 /mnt
```

If the file system is corrupted when the first partition of the qcow2 image is exported, an error will occur when using the mount command.

In addition, you can start the CVM to check whether the image file works before uploading the image.

Windows Image Production

Last updated : 2018-08-06 11:53:07

1. Preparations

The following checks are required to export a system disk image, and can be ignored when you export a data disk image.

- Check the OS partition. Service Migration does not support GPT-style partition.

How to check the partition:

Open the **Control Panel** -> **Disk Management**, right-click the disk to select **Property**, and you can find the Partition style in the figure below.



If it reads GPT, the GPT-style partition is used.

- Check the startup mode. Service Migration does not support starting the system with EFI. If EFI exists in the path, then the current operating system starts in the EFI mode. Open the command prompt (CMD) as admin and execute the following command:

```
bcdedit /enum {current}
```

Example of execution result:

```
C:\WINDOWS\system32>bcdedit /enum {current}
```

Windows bootstrapper

```
-----
identifier {current}
device partition=C:
path \WINDOWS\system32\winload.exe
description Windows 10
locale zh-CN
inherit {bootloadersettings}
recoverysequence {f9dbeba1-1935-11e8-88dd-ff37cca2625c}
displaymessageoverride Recovery
recoveryenabled Yes
flightsigning Yes
allowedinmemorysettings 0x15000075
osdevice partition=C:
systemroot \WINDOWS
resumeobject {1bcd0c6f-1935-11e8-8d3e-3464a915af28}
nx OptIn
bootmenupolicy Standard
```

- Check the network configuration. Service Migration does not support IPv6 nor multi-ENI. Services that rely on both IPv6 and multi-ENI cannot work normally.
- Unmount the drivers and software that produce conflicts (including VMware tools, Xen tools, Virtualbox GuestAdditions and other software that comes with underlying drivers).
- Install cloud-base: Please see [Install cloud-base](#).
- Check or install the virtio driver

The virtio driver has been installed if it is found in the **Control Panel -> Programs and Features**:

卸载或更改程序

若要卸载程序，请从列表中选择其，然后单击“卸载”、“更改”或“修复”。

名称	发布者	安装时间	大小	版本
Tencent Virtio Driver	Tencent OS Team	2018/3/5	5.37 MB	1.0.8
Windows 驱动程序包 - Tencent, Inc. Tencent VirtIO Ethernet Adapter (09/12/2016 62.10006.1.0)	Tencent, Inc.	2018/3/5		09/12/2016 62.1000...
Windows 驱动程序包 - Tencent, Inc. Tencent VirtIO SCSI controller (11/13/2015 62.10001.1.0)	Tencent, Inc.	2018/3/5		11/13/2015 62.1000...
Windows 驱动程序包 - Tencent, Inc. VirtIO Balloon Driver (11/13/2015 62.10001.1.0)	Tencent, Inc.	2018/3/5		11/13/2015 62.1000...

Otherwise, you need to manually install the virtio driver:

- For the following system versions, download [Tencent Cloud's customized virtio](#) Microsoft Windows Server 2008 R2 (Standard Edition, Datacenter Edition, Enterprise Edition), Microsoft Windows Server 2012 R2 (Standard Edition)
- For other system versions, download the [virtio community version](#).
- Check the configurations of other hardware. Changes to the hardware on the cloud include but not limited to:
 - Replacing the graphics card with cirrus vga.
 - Replacing the disk with virtio disk.
 - Replacing the ENI with virtio nic. Local Area Connection is used by default.

2. Export the Image Using a Platform Tool

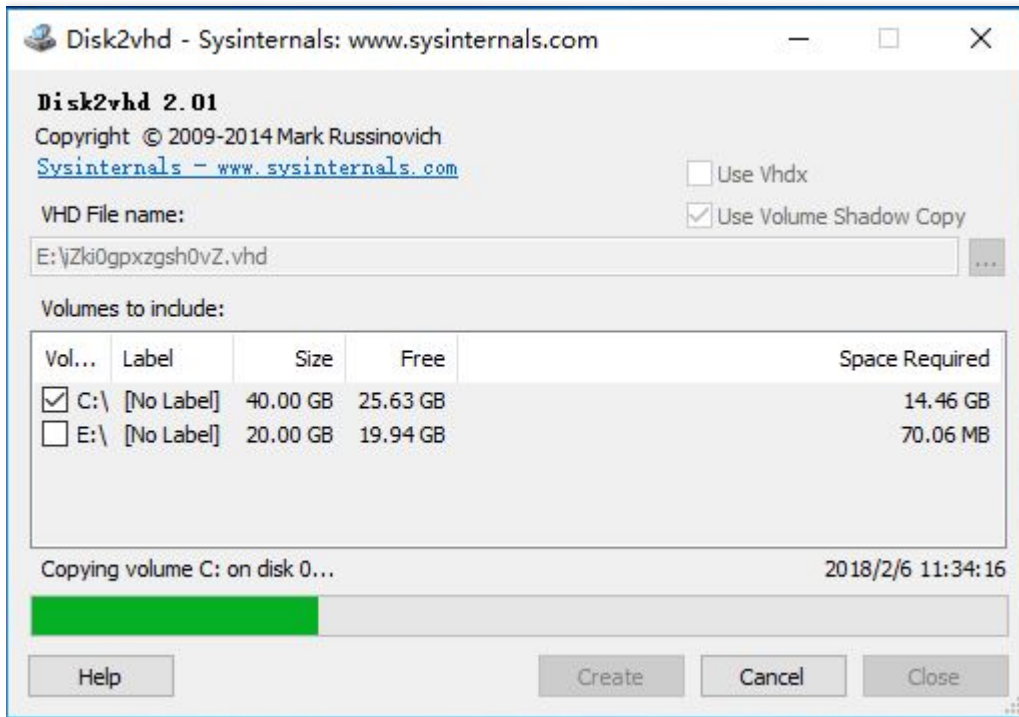
For more information on how to use image export tools of VMWare vCenter Convert, Citrix XenConvert and other virtualization platforms, please see the relevant document of each platform. The image formats supported by Tencent Cloud Service Migration include qcow2, vhd, raw, and vmdk.

3. Export the Image Using Disk2vhd

The Disk2vhd tool can be used to export the system if it is deployed on a physical machine or if you do not want to export it using a platform tool.

[Download Disk2vhd](#)

The interface after installation is shown as below:



When using the tool, select the volume to be copied and the name of the file to be exported, and click **Create** to export vhd.

Note:

- The vss feature must be preset in Windows before Disk2vhd can run.
- Do not select "Use Vhdx". The system does not support vhdx images.
- "Use volume Shadow Copy" should be selected to ensure the data integrity.

4. Check the Image

As mentioned above, an error may be occurred with the image file system if it is created when the server is not shut down or due to other reasons. Therefore, you are recommended to check whether the created image is error-free.

When the image format is consistent with the format supported by the current platform, you can directly open the image to check the file system. For example, vhd images can be directly added to Windows platform, qcow2 images can be opened using qemu-nbd on Linux platform, and vhd images can be enabled directly on Xen platform. Take the Linux platform as an example:

```
modprobe nbd  
qemu-nbd -c /dev/nbd0 xxxx.qcow2  
mount /dev/nbd0p1 /mnt
```

If the file system is corrupted when the first partition of the qcow2 image is exported, an error will occur when using the mount command.

In addition, you can start the CVM to check whether the image file works before uploading the image.

Linux System Check virtio Driver

Last updated : 2018-08-03 16:54:34

A CVM must have a kernel supporting virtio drivers (including the block device driver `virtio_blk` and NIC driver `virtio_net`) in order to run on Tencent Cloud. CVMs whose kernels do not have the `virtio_blk` driver must include this driver in the file `initramfs` (or `initrd`) for normal operation. This document describes how to check and repair the support for virtio drivers before importing images.

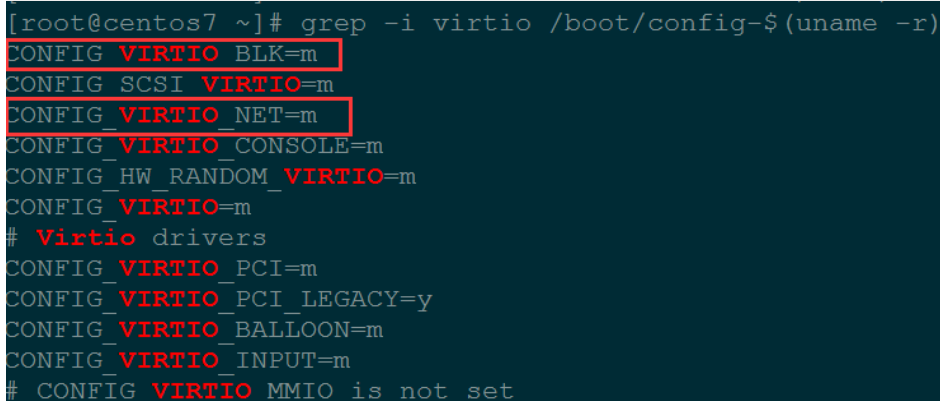
Checking Whether Virtio Drivers are Supported in the Kernel

The following takes `Centos7` as an example to illustrates how to check whether `virtio` driver are supported in the current kernel.

(1) Check whether `virtio` drivers are support in the kernel

```
grep -i virtio /boot/config-$(uname -r)
```

As shown in the figure below, `virtio_blk` and `virtio_net` drivers are compiled as modules in the kernel. (`CONFIG_VIRTIO_BLK=m` means to compile `virtio_blk` as a module in the kernel and `CONFIG_VIRTIO_BLK=y` means to compile `virtio_blk` into the kernel) If no information on the `virtio_net` or `virtio_blk` drivers is found in this step, the image *cannot* be imported to Tencent Cloud.



```
[root@centos7 ~]# grep -i virtio /boot/config-$(uname -r)
CONFIG_VIRTIO_BLK=m
CONFIG SCSI_VIRTIO=m
CONFIG_VIRTIO_NET=m
CONFIG_VIRTIO_CONSOLE=m
CONFIG_HW_RANDOM_VIRTIO=m
CONFIG_VIRTIO=m
# Virtio drivers
CONFIG_VIRTIO_PCI=m
CONFIG_VIRTIO_PCI_LEGACY=y
CONFIG_VIRTIO_BALLOON=m
CONFIG_VIRTIO_INPUT=m
# CONFIG_VIRTIO_MMIO is not set
```

If the kernel supports both `virtio_blk` and `virtio_net` drivers, and the `virtio_blk` driver is compiled into the kernel (`CONFIG_VIRTIO_BLK=y`), the kernel supports importing without confirmation. If the `virtio_blk` driver is compiled as a module in the kernel (`CONFIG_VIRTIO_BLK=m`), confirmation is required to ensure that the `virtio_blk` driver is properly included in the `initramfs` (or `initrd`) file.

(2) Check for the `virtio_blk` driver in `initramfs`

```
lsinitrd /boot/initramfs-$(uname -r).img | grep virtio
```

As shown in the figure below, `initramfs` contains the `virtio_blk` driver and the dependent `virtio.ko`, `virtio_pci.ko`, and `virtio_ring.ko`, which means all the necessary components are included in `initramfs`. In this case, the image can be imported.

```
[root@centos7 ~]# lsinitrd /boot/initramfs-$(uname -r).img | grep virtio
-rw-r--r-- 1 root root 27885 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/block/virtio_blk.ko
-rw-r--r-- 1 root root 53533 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/char/virtio_console.ko
-rw-r--r-- 1 root root 49605 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/net/virtio_net.ko
-rw-r--r-- 1 root root 29253 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/scsi/virtio_scsi.ko
drwxr-xr-x 2 root root 0 Nov 10 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/virtio
-rw-r--r-- 1 root root 17989 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/virtio/virtio.ko
-rw-r--r-- 1 root root 35461 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/virtio/virtio_pci.ko
-rw-r--r-- 1 root root 22757 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/virtio/virtio_ring.ko
```

(3) If no `virtio` information is found in `initramfs`, you must recreate the `initramfs` file.

1) Operations in CentOS 7

```
cp /boot/initramfs-$(uname -r).img /boot/initramfs-$(uname -r).img.bak
mkinitrd -f --with=virtio_blk --with=virtio_pci /boot/initramfs-$(uname -r).img $(uname -r)
```

```
[root@centos7 ~]# lsinitrd /boot/initramfs-$(uname -r).img | grep virtio
Arguments: -f --add-drivers ' virtio-blk'
-rw-r--r-- 1 root root 27885 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/block/virtio_blk.ko
-rw-r--r-- 1 root root 53533 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/char/virtio_console.ko
-rw-r--r-- 1 root root 49605 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/net/virtio_net.ko
-rw-r--r-- 1 root root 29253 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/scsi/virtio_scsi.ko
drwxr-xr-x 2 root root 0 Jun 22 16:48 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/virtio
-rw-r--r-- 1 root root 17989 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/virtio/virtio.ko
-rw-r--r-- 1 root root 35461 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/virtio/virtio_pci.ko
-rw-r--r-- 1 root root 22757 Oct 25 2016 usr/lib/modules/3.10.0-327.36.3.el7.x86_64/kernel/drivers/virtio/virtio_ring.ko
```

2) Operations in Redhat5/Centos5

a. Check for the driver information in the `initrd` file, as shown below:

```
mkdir -p /tmp/initrd && cd /tmp/initrd
zcat /boot/initrd-$(uname -r).img | cpio -idmv
find . -name "virtio*"
```

b. If necessary, execute the following command to recreate the `initrd` file.

```
cp /boot/initrd-$(uname -r).img /boot/initrd-$(uname -r).img.bak
mkinitrd -f --with=virtio_blk --with=virtio_pci /boot/initrd-$(uname -r).img $(uname -r)
```

3) Operations in Debian/Ubuntu

a. Check for the `virtio` driver

```
lsinitramfs /boot/initrd.img-$(uname -r) | grep virtio
```

b. If initramfs does not contain the driver, follow the procedure below to repair it.

```
echo -e "virtio_pci\nvirtio_blk" >> /etc/initramfs-tools/modules  
update-initramfs -u
```

Forcibly Import Image

Last updated : 2018-08-02 10:30:26

If you cannot [install cloudinit](#) in your Linux image for some reason, use **Forced Image Import** to import the image. At this point, Tencent Cloud cannot initialize your virtual machine. You need to define scripts to configure the virtual machine according to the configuration file provided by Tencent Cloud.

Limits and Configuration

Applying for Permission

Before using this feature, make sure that you have activated the image import permission. If you need to activate the permission, contact the Business Manager and submit relevant information to the ticket system.

Image Limits

- The image must meet the limits on importing Linux image in [Import Image](#).
- The system partition for importing the image is not full.
- The imported image contains no vulnerability that can be exploited remotely.
- It is recommended that the user change the password immediately after the instance is created with forced image import.

Configuration of Image Import

Images forcibly imported by users do not use cloudinit, so automatic configuration is not available. Tencent Cloud provides the CDROM device containing configuration information for users to manually configure the images. Users need to mount the CDROM and read the configuration information from `mount_point/qcloud_action/os.conf`. Users can directly read the files in `mount_point/` if other configuration data or UserData is required.

Content of os.conf Configuration File

The content of os.conf is as follows.

```
hostname=VM_10_20_xxxx
password=GRSgae1fw9frsG.rfrF
eth0_ip_addr=10.104.62.201
eth0_mac_addr=52:54:00:E1:96:EB
eth0_netmask=255.255.192.0
```

```
eth0_gateway=10.104.0.1  
dns_nameserver="10.138.224.65 10.182.20.26 10.182.24.12"
```

The parameter names above are for reference, and the values are only for example purpose.

The description of the parameters is as follows:

Parameter Name	Description
hostname	CVM name
password	Encrypted password
eth0_ip_addr	LAN IP of eth0
eth0_mac_addr	MAC address of eth0
eth0_netmask	Subnet mask of eth0
eth0_gateway	Gateway of eth0
dns_nameserver	DNS resolution server

Configuration Script Resolution

Notes

- The script must be executed on startup.
- Mount `/dev/cdrom` and read `os_action/os.conf` file under the mount point to obtain configuration information.
- The password placed in the CDROM by Tencent Cloud is encrypted. Users can set new password with `chpasswd -e`. Note that the encrypted password may contain special characters. It is recommended to place the password in a file and set it with `chpasswd -e < passwd_file`.
- When creating images from an instance created by forced image import, be sure to execute the script for proper configuration, or install cloudinit in the instance.

Example

Tencent Cloud provides an example script based on CentOS for users to define scripts for their images. Note that:

- **The script must be properly placed in the system before image import.**
- The script does not apply to all operating systems. Users need to modify it according to their own operating systems.

- The script must be set to execute on startup for normal use. Make the configuration according to the type of operating system. (For example, place the script `os_config` under `/etc/init.d/` directory and execute the following command.)

```
chmod +x /etc/init.d/os_config
chkconfig --add os_config
```

Run `chkconfig --list` to check if `os_config` is added to the startup service.

- Users must ensure that the script is properly executed. If problems such as failed to connect to the instance via SSH and failed to connect network occur after importing the image, try to connect to the instance in the console to execute the script again. If the problem remains, contact Customer Service.

The following is the example script `os_config`. Users can modify the script as needed.

```
#!/bin/bash
### BEGIN INIT INFO
# Provides: os-config
# Required-Start: $local_fs $network $named $remote_fs
# Required-Stop:
# Should-Stop:
# Default-Start: 2 3 4 5
# Default-Stop: 0 1 6
# Short-Description: config of os-init job
# Description: run the config phase without cloud-init
### END INIT INFO

#####user settings#####

cdrom_path=`blkid -L config-2`

load_os_config() {
mount_path=$(mktemp -d /mnt/tmp.XXXX)
mount /dev/cdrom $mount_path
if [[ -f $mount_path/qcloud_action/os.conf ]]; then
. $mount_path/qcloud_action/os.conf
if [[ -n $password ]]; then
passwd_file=$(mktemp /mnt/pass.XXXX)
passwd_line=$(grep password $mount_path/qcloud_action/os.conf)
echo root:${passwd_line#*=} > $passwd_file
fi
return 0
else
```

```
return 1
fi

}

cleanup() {
umount /dev/cdrom
if [[ -f $passwd_file ]]; then
echo $passwd_file
rm -f $passwd_file
fi
if [[ -d $mount_path ]]; then
echo $mount_path
rm -rf $mount_path
fi
}

config_password() {
if [[ -f $passwd_file ]]; then
chpasswd -e < $passwd_file
fi
}

config_hostname(){
if [[ -n $hostname ]]; then
sed -i "/^HOSTNAME=.*$/d" /etc/sysconfig/network
echo "HOSTNAME=$hostname" >> /etc/sysconfig/network
fi
}

config_dns() {
if [[ -n $dns_nameserver ]]; then
dns_conf=/etc/resolv.conf
sed -i '/^nameserver.*$/d' $dns_conf
for i in $dns_nameserver; do
echo "nameserver $i" >> $dns_conf
done
fi
}

config_network() {
/etc/init.d/network stop
cat << EOF > /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
IPADDR=$eth0_ip_addr
```

```

NETMASK=$eth0_netmask
HWADDR=$eth0_mac_addr
ONBOOT=yes
GATEWAY=$eth0_gateway
BOOTPROTO=static
EOF
if [[ -n $hostname ]]; then
sed -i "/^${eth0_ip_addr}.*$/d" /etc/hosts
echo "${eth0_ip_addr} $hostname" >> /etc/hosts
fi
/etc/init.d/network start
}

config_gateway() {
sed -i "s/^GATEWAY=.*$/GATEWAY=$eth0_gateway" /etc/sysconfig/network
}

#####init#####
start() {
if load_os_config ; then
config_password
config_hostname
config_dns
config_network
cleanup
exit 0
else
echo "mount ${cdrom_path} failed"
exit 1
fi
}

RETVAL=0

case "$1" in
start)
start
RETVAL=$?
;;
*)
echo "Usage: $0 {start}"
RETVAL=3
;;
esac

```

exit \$RETVL

Network and Security

Protection of Sensitive Operations

Last updated : 2018-08-06 11:40:04

Overview

CVM supports sensitive operation protection. Before you perform sensitive operations, you need to enter a credential that can prove your identity. After the authentication is passed, you can perform related operations.

The sensitive operation protection of CVM can effectively protect the security of account resources, including the shutdown, restart, password reset, and termination of CVM.

Enable Operation Protection

Tencent Cloud provides two ways to protect operations:

1. Provide operation protection by enabling **MFA authentication**.
2. Provide operation protection by enabling **mobile verification code**.

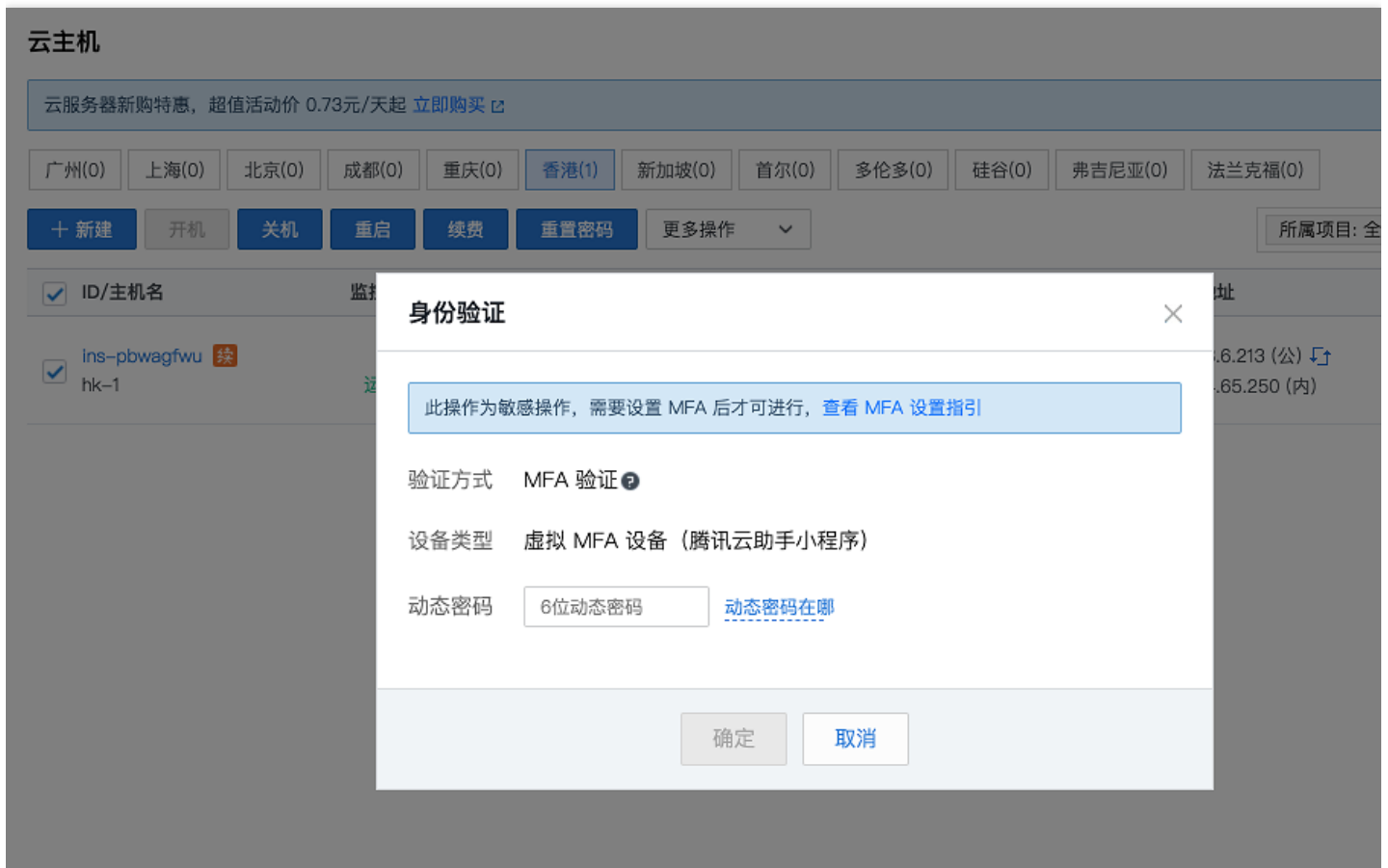
You can enable the operation protection through [Access Management Console](#). For more information on operation instructions, please see [Operation Protection](#).

Operation Protection Verification

When you have enabled the operation protection, the system will first perform operation protection verification when you perform sensitive operations:

- If you have enabled **MFA verification** for operation protection, you need to enter the 6-bit dynamic verification code on the MFA device.
- If you have enabled **mobile verification code** for operation protection, you need to enter the mobile verification code.

As shown in the following figure, when you try to shut down an instance, the following verification box pops up, and you need to verify the MFA device:



How do I view the MFA verification code?

1. Turn on the MFA device:

Open the **Tencent Cloud Assistant Mini Program** and select "Tools" to see the bound authenticator.

2. View the dynamic verification code of the corresponding account. The dynamic verification code is updated every 30 seconds.



SSH Key

Last updated : 2018-07-17 15:21:22

To ensure the security and reliability of the instance, Tencent Cloud provides two encrypted login methods: [Password Login](#) and SSH key pair login. This document describes common operations of SSH key pairs.

Creating an SSH key

1. Log in to [Cloud Server Console](#).
2. Click **SSH Key** in the left navigation pane.
3. Click **Create Key**
 - If the creation method is **Create a new key pair**, enter the key name and click **OK**;
 - If the creation method is **Use existing public key**, enter the key name and enter the original public key information, and then click **OK**.
4. In the pop-up window, click **Download** (please download the private key within 10 minutes).

Binding/Unbinding Keys with Servers

1. Log in to [Cloud Server Console](#).
2. Click **SSH Key** in the left navigation pane.
3. Select the SSH key and click **Bind/Unbind CVM** (or right-click on the key name to be modified and click **Bind/Unbind CVM**).
4. Select the region, select the server to be bound/unbound (uncheck the server selected on the right side to unbind), and click **OK**.
5. The system delivers the SSH key automatically. And you will get notice about whether the operation is successful or failed.

Modify SSH Key Name/Description

1. Log in to [Cloud Server Console](#).
 - i. Click **SSH Key** in the left navigation pane.
2. Select the key to be modified in the key list, and click **Modify** (or right-click on the key name to be modified and click **Modify**).
3. Enter a new name and description click **OK**.

Deleting SSH keys

Note:

If the SSH key is associated with a CVM or an associated custom image, it cannot be deleted.

1. Log in to [Cloud Server Console](#).
2. Click **SSH Key** in the left navigation pane.
3. Select all the SSH keys you want to delete and click the **Delete** button (or right-click on the key name you want to delete, click **Delete**, and click **OK** in the pop-up window).

Log in to the Linux CVM using the SSH key

Before you log in to the Linux CVM using an SSH key, you need to create an SSH key and bind the SSH key to the CVM.

For details, please refer to [Logging In to Linux CVM](#).

Distributed Placement Group

Last updated : 2018-09-30 10:47:55

This feature is under internal trial. Please click [here](#) to apply for a trial use.

Creating Placement Group

Creating placement group in the console

1. Log in to the [CVM Placement Group Console](#).
2. Select Placement Group in the navigation pane, and click **New**.
3. Specify a name for the placement group and select a layer.
4. Click **OK** to complete the creation.

Starting up Instance in Placement Group

Starting up instance in placement group in the console

1. Go to the [CVM Purchase Page](#).
2. Complete the wizard as instructed and the following should be noted:
 - Select the availability zone, instance type and network type for your desired instance in **Region and Model**.
 - Select an image on the **Select Image** page.
 - Select desired configuration and parameters on the **Select Storage and Bandwidth** page.
 - Configure security group, login method and other information on the **Configure Security Group and CVM** page. Click **Advanced Configuration** at the bottom, check **Add Instance to Spread Placement Group**, and select an existing placement group. If no existing placement group meets your requirement, you can [create a placement group](#) in the console.
 - On the **Confirm Configuration** page, enter the total number of instances to be added to the placement group, which must be less than the number limit set for the placement group.

Modifying Instance's Placement Group

You can only change the name of a placement group.

Modifying instance's placement group in the console

1. Log in to the [CVM Placement Group Console](#).
2. Move the mouse over the name of a placement group, and click **Modify Name**.
3. Enter a new name.
4. Click **OK** to complete the modification.

Deleting Placement Group

You can delete a placement group if you need to replace it or you no longer need it. You must terminate all instances running in your placement group before deleting it.

Terminating instances and deleting placement group in the console

1. Log in to the [CVM Placement Group Console](#).
2. Select and terminate all instances in a placement group.
3. Select the placement group, and delete it. You can delete a single placement group or multiple placement groups in batches.
4. Select **OK** in the confirmation prompt.

Elastic Public IP

Last updated : 2018-10-10 19:30:22

Elastic IP, is referred to as EIP for short. It is a static IP designed for dynamic cloud computing, and a fixed public IP in a certain region. In case of an instance failure, the EIP can be remapped to another instance in your account (or [NAT gateway instance](#)) quickly to block the failure.

Common Operations

The following describes how to use EIPs.

Applying for EIPs

1. Log in to the [CVM Console](#).
2. In the left navigation pane, click **EIP**.
3. Click the **Apply** button, enter a region and the number of EIPs you want to apply for, and then click **OK**.
4. After this, you can see in the list the new EIP(s) you just applied for, which have/has an unbound status.

Binding EIPs to cloud products

1. Log in to the [CVM Console](#).
2. In the left navigation pane, click **EIP**.
3. In the EIP list, click the **Bind** button next to the EIP to be bound to a cloud product. (If the EIP is already bound to an instance, this button is unavailable. Please unbind it first.)
4. In the popup box, select the cloud product type that you want to bind, and then select the cloud product instance ID. Click the **Bind** button to complete the binding.

Unbinding EIPs from cloud products

1. Log in to the [CVM Console](#).

2. In the left navigation pane, click **EIP**.
3. In the EIP list, click the **Unbind** button next to the EIP that is already bound to a cloud product.
4. Click **OK**.

Note:

After unbinding, the cloud product instance may be assigned a new public IP, which may be different from the one before binding.

Releasing EIPs

1. Log in to the [CVM Console](#).
2. In the left navigation pane, click **EIP**.
3. In the EIP list, click **More** -> **Release** button next to the EIP to be released.
4. Click **OK**.

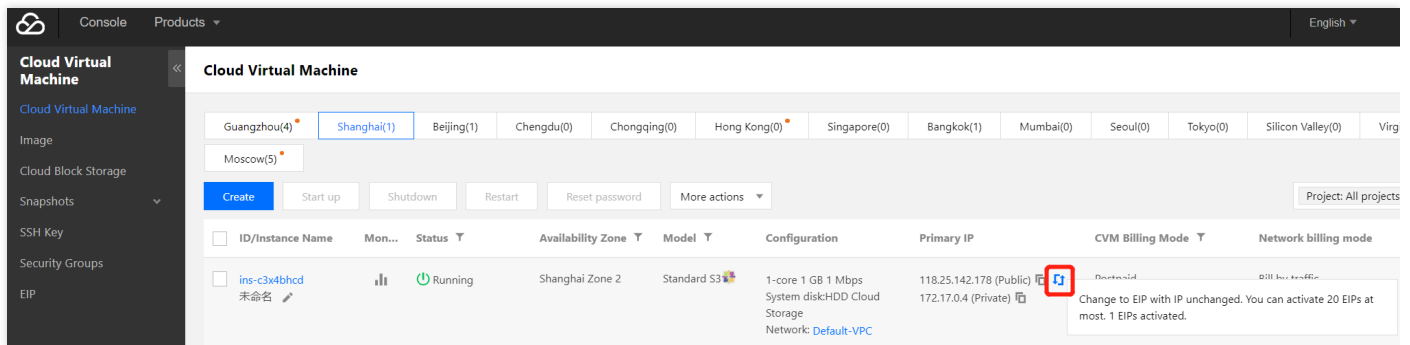
Adjusting bandwidth

1. Log in to the [CVM Console](#).
2. In the left navigation pane, click **EIP**.
3. In the EIP list, click the **Change Bandwidth** button next to the EIP for which you want to adjust bandwidth.
4. Adjust the target bandwidth value in the Adjust Bandwidth page.
5. Click **OK**.

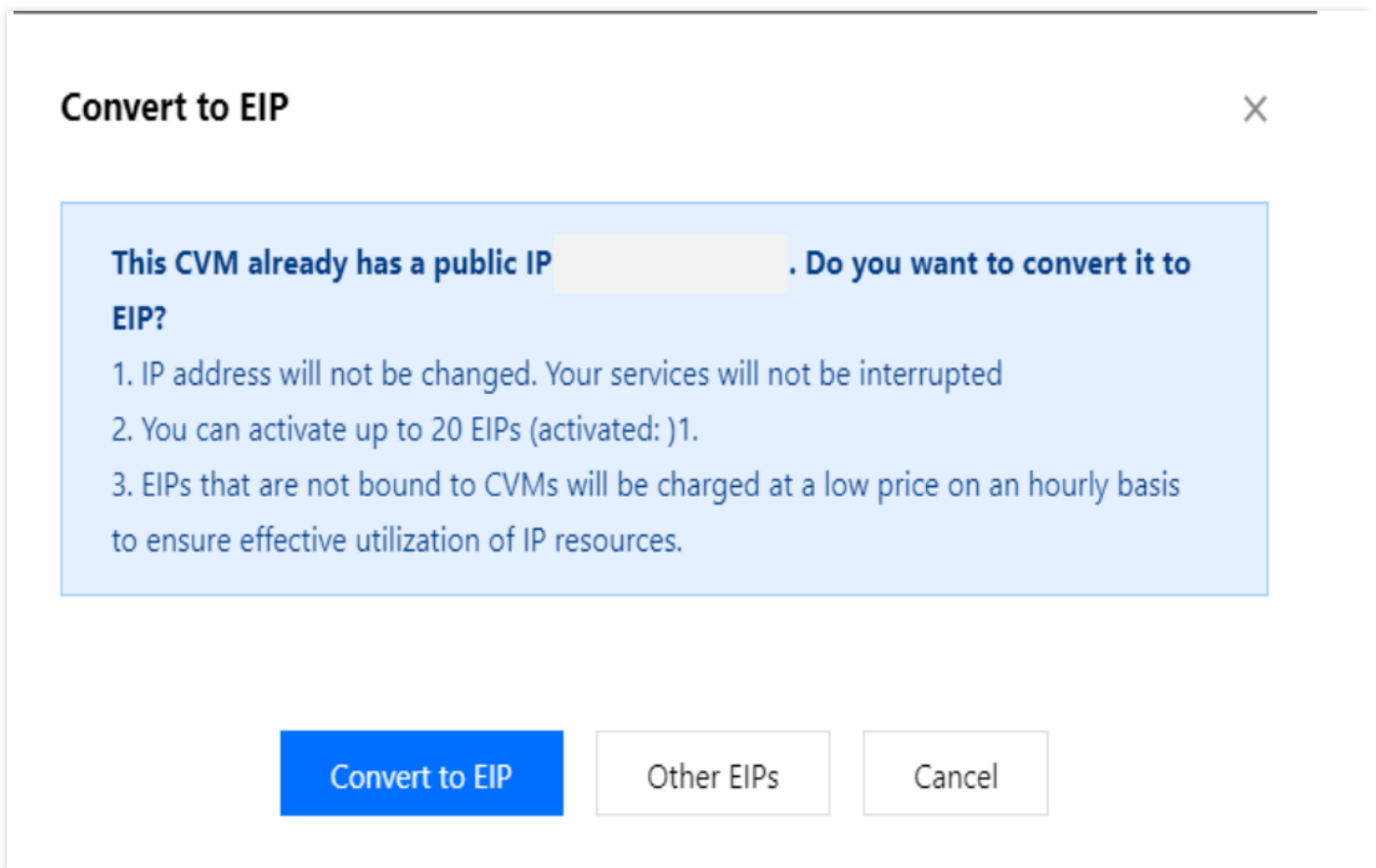
Converting public IP to EIP

The public IP purchased along with the CVM instance is an ordinary public IP. It does not have elasticity and cannot be mounted and unmounted. Tencent Cloud allows you to convert an ordinary public IP to an EIP by following the steps below:

1. Log in to the [CVM Console](#).
2. Click the Convert icon.



3. Click **Confirm Conversion**.



Troubleshooting

Network inaccessibility may occur with an EIP. This is generally caused by the following reasons:

- The EIP is not bound to any cloud product. For more information about how to bind an EIP to cloud products, please see [Binding EIP to Cloud Products](#).
- Security policy is invalid. Check if there is a valid security policy (security group or network ACL). If the bound cloud product has a security group policy, for example: access to 8080 port is denied, the port 8080 of the EIP is also inaccessible.

EIP Direct Connection

Last updated : 2018-08-01 17:54:16

Application Scenarios

Users can select NAT mode or EIP direct connection mode when accessing the public network with EIP. Default is NAT mode.

- EIP is invisible on the local machine in NAT mode.
- EIP is visible on the local machine in EIP direct connection mode. You do not need to add the EIP address manually for each configuration to minimize development cost.

Note:

EIP direct connection is subject to the whitelist, and only supports devices in the VPC.

Procedure

1. Download EIP configuration script

Since EIP direct connection may cause network interruption, you need first to download EIP direct connection script and upload it to CVM. The steps are as follows:

(1) Download the configuration script of EIP direct connection (optional). Download path:

- [Download Script for Linux](#)
- [Download Script for Windows](#)

Note:

Script for Linux supports CentOS 6.x, CentOS 7 and Ubuntu.

(2) After the script is downloaded, upload it to the CVM that requires to enable EIP direct connection.

2. Run EIP direct connection script

(1) Log in to the CVM that requires EIP direct connection.

(2) Run EIP direct connection script. Method:

- In CentOS Linux:

```
eip_linux.sh install XX.XX.XX.XX
```

XX.XX.XX.XX represents the EIP address (optional).

- In Windows:

```
eip_windows.bat XX.XX.XX.XX
```

XX.XX.XX.XX represents the EIP address.

3. Enable EIP direct connection

- (1) Log in to the [CVM console](#).
- (2) In the left navigation pane, click **EIP**.
- (3) Click **EIP Direct Connection** button in the **Operation** column of the list to enable EIP direct connection.

Note:

- The script supports eth0 only, but not secondary ENI.
- NAT gateway can be bound with EIPs enabled with direct connection, but direct connection cannot be implemented.

Security Groups

Limits

Last updated : 2018-06-13 10:28:19

- Security groups are region and project-specific. CVMs can only be bound with the security groups in the same region and project.
- Security groups apply to any CVM instances in [network environment](#).
- Each user can set a maximum of 50 security groups for each project in each region.
- A maximum of 100 inbound/outbound access policies can be set for a security group.
- A CVM can be associated with multiple security groups, and a security group can be associated with multiple CVMs. No number limit is imposed.
- Security groups bound with CVMs in **basic network cannot filter** data packets sent from (or to) relational database (CDB) and cloud cache service (Redis and Memcached) of Tencent Cloud. If necessary, you can use iptables to filter traffic of such instances.

Feature	Count
Security group	50/Region
Access policy	100 (Inbound/Outbound)
Number of security groups associated with an instance	No limit
Number of instances associated with a security group	No limit

Note:

If you have a large number of instances that need to access each other, you can assign them to multiple security groups, and achieve mutual authorization and access by configuring the rules for security group IDs.

Operation Guide

Last updated : 2018-10-10 20:13:45

You can create, view, update and delete security groups and security group rules or perform other operations on them in the CVM console.

Common Operations

Creating a security group

1. Open [Console - Security Group](#).
2. Click **New** button.
3. Enter the security group name (e.g. my-security-group) and the description.
4. Click **OK** to finish the creation.

Adding rules to security group

1. Open [Console - Security Group](#).
2. Select the security group to be updated, and then click **Security Group ID**. The Details pane will list the details of the security group as well as the tab for using inbound and outbound rules.
3. On the Inbound/Outbound Rules tab, click **Edit**. Select the options for the inbound/outbound rules from the tab, enter the required information, and then click **Save**.

Configuring a security group to associate with CVM instances

1. Open [Console - CVM](#).
2. In the Operation column next to the instance for which you want to configure a security group, click **More** and then click **Configure Security Group**.
3. In the Configure Security Group dialog box, select one or more security groups from the list and click **OK**.

Or

1. Open [Console - Security Group](#).
2. Select the security group to be associated with CVMs, and then click **Add Instances** or **Remove Instances** button in the Operation column.
3. In the Add/Remove CVMs popup box, add or delete the CVMs to be associated with this security group, and click **OK**.

Importing/exporting security group rules

1. Open [Console - Security Group](#).
2. Select the security group to be updated, click **Security Group ID**. The Details pane will list the details of the security group as well as the tab for using inbound and outbound rules.
3. Select the options for inbound/outbound rules from the tab, and then click **Import Rules** button. If you already have the rules, it is recommended to export existing rules first. Importing the new rules will overwrite the existing rules. If the original rules are empty, you can export the template, edit the template file, and then import the file.

Cloning a security group

1. Open [Console - Security Group](#).
2. Click the **Clone** button for the security group to be cloned in the list.
3. In the Clone Security Group dialog box, select the destination region and project, and then click **OK**. If the new security group needs to be associated with a CVM, reconfigure the security group.

Deleting a security group

1. Open [Console - Security Group](#).
2. Click the **Delete** button for the security group to be deleted in the list.
3. In the Delete Security Group dialog box, click **OK**. If the current security group is associated with a CVM, disassociate the security group from the CVM before deleting it.

Typical Scenario Configuration

Remotely logging in to Linux instances via SSH

To log in to a Linux instance via SSH remotely, add the following inbound rule to the security group associated with the instance:

Source	Protocol Port	Policy
0.0.0.0/0	TCP:22	Allow

Note: You can set **IP address range** or **security group** for the Source.

Logging in to Windows instances via MSTSC

To log in to a Windows instance via MSTSC, add the following inbound rule to the security group associated with the instance:

Source	Protocol Port	Policy
0.0.0.0/0	TCP:3389	Allow

Note: You can set **IP address range** or **security group** for the Source.

Pinging a CVM instance in public network

To test the communication status of a CVM instance using Ping program, add the following inbound rule to the security group associated with the instance:

Source	Protocol Port	Policy
0.0.0.0/0	ICMP	Allow

Note: You can set **IP address range** or **security group** for the Source.

Using CVM instance as Web servers

If you create an instance as a Web server, you need to install the Web server program on the instance, and add the following inbound rule to the security group associated with the instance:

Note: You need to start the Web server program first, and check whether the port is set to 80.

Source	Protocol Port	Policy
0.0.0.0/0	TCP:80	Allow

Uploading or downloading files with FTP

To upload/download files to/from a CVM instance with FTP, add the following inbound rule to the security group associated with the instance:

--

Note: You need to install the FTP server program on the instance, and then check whether the port 20/21 works properly.

Source	Protocol Port	Policy
0.0.0.0/0	TCP:20,21	Allow

Server Common Port

Last updated : 2018-08-01 17:55:30

The following describes the common server ports. For more information on service application ports on Windows, please see Microsoft official document ([Windows Service Overview and Network Port Requirements](#)).

Port	Service	Description
21	FTP	FTP server's open port for upload and download.
22	SSH	Port 22 is the SSH port, used to remotely connect to Linux system servers in command-line mode.
25	SMTP	SMTP server's open port for sending emails.
80	HTTP	Used for Web services, such as IIS, Apache, Nginx, to provide external access.
110	POP3	Port 110 is open for POP3 (email protocol 3) service.
137, 138, 139	NETBIOS protocol	Port 137 and 138 are UDP ports used to transfer files via My Network Places. Port 139: Incoming connections over port 139 attempt to obtain NetBIOS/SMB service. This protocol is used for file and printer sharing on Windows as well as SAMBA service.
143	IMAP	Port 143 is mainly used for "Internet Message Access Protocol" (IMAP) v2, a protocol for receiving emails as the same as POP3.
443	HTTPS	Web browsing port. This is another type of HTTP that supports encryption and transfer over secure ports.
1433	SQL Server	Port 1433 is the default port for SQL Server. The SQL Server service uses two ports: TCP-1433 and UDP-1434. Port 1433 is used by SQL Server to provide external services, and port 1434 is used to send requester a response about which TCP/IP port is used by SQL Server.
3306	MySQL	Port 3306 is the default port for MySQL database and is used by MySQL to provide external services.
3389	Windows Server Remote Desktop Services	Port 3389 is the service port for remote desktop on Windows 2000 (2003) Server. You can connect to a remote server using the "Remote Desktop" connection tool via this port.

Port	Service	Description
8080	Proxy Port	Just like port 80, port 8080 is used for WWW proxy service for web browsing. Port number ":8080" is often added when users visit a website or use a proxy server. In addition, after Apache Tomcat Web server is installed, the default service port is 8080.

Monitoring and Alarms

Get Monitoring Statistics

Last updated : 2018-08-01 17:53:12

Tencent Cloud provides cloud monitoring for all users by default, no need for the user to manually turn on. But the user must use Tencent Cloud products before cloud monitoring can begin to collect monitoring data; to view these monitoring data, there are several ways:

Obtain monitoring data through the cloud product console's individual monitoring page

Some cloud products provide a separate monitoring data reading tab on their own console pages. CVM is used in this example

- 1) Open [Tencent Cloud Console](#), select **CVM**.
- 2) Click the CVM Instance ID from the list of CVMs to view the monitoring data, and enter the CVM details page.
- 3) Click the **Monitor** tab; on this page, you can view the CPU, memory, network bandwidth, disk and monitoring data, etc. of the CVM instance. You can also freely adjust the time range.

Note: Tencent Cloud monitoring provides both 5 minute and 1 minute data acquisition modes; 5 minute data collection is the default. In different display modes, the indicator data displays will be different. For example, when monitoring charts are displayed for nearly an hour, the monitoring data is presented in the original 5-minute interval format. When monitoring charts are displayed for nearly a month, the monitoring data will show daily data averages in days.

Obtain monitoring data from Console

On Cloud Monitoring console, you can view monitoring data for most of the products used. In this case, CVM is used as an example.

- 1) Open [Tencent Cloud Console](#), select **Cloud Products - Cloud Monitoring**.
- 2) On the left navigation bar, select **Cloud Product Monitoring - CVM**.

3) Click the CVM Instance ID from the list of CVMs displayed to view the monitoring data, and enter the monitoring details page.

4) On this page, you can view the CPU, memory, network bandwidth, disk and all monitoring data of the CVM instance. You can also freely adjust the time range.

Obtain monitoring data through the API

Users can use the GetMonitorData API to obtain monitoring data for all products. For more information, please see [Reading Monitoring Data API](#).

Create Alarm Polices

Last updated : 2018-08-01 17:37:59

You can create an alarm to get notified for status change of Tencent Cloud services. The created alarm determines whether to trigger a notification according to the comparison results between a monitored metric and a specific threshold at regular interval.

You can take precautionary or remedial measures in a timely manner when an alarm is set off by status changes. Therefore, creating a valid alarm can help you improve your application's robustness and reliability. For more information about alarms, please see [Alarm Configuration](#).

Triggering Conditions

Each alarm policy is a set of triggering conditions with the logic relationship "or", that is, an alarm is triggered when any of the conditions is met. The alarm is sent to all users associated with the alarm policy. Upon receiving the alarm, the user can view the alarm and take appropriate actions in time.

Creating an Alarm

1. Log in to [Cloud Monitor Console](#), click **My Alarms** tab, and then click **Alarm Policy** menu.
2. Click **Add** button.
3. On the new page, enter a policy name and select a policy type.
4. Select alarm triggering conditions. The triggering condition is a semantic condition consisting of **metric, comparison relation, threshold, measurement period, number of continuous periods** and **repeated notification policy**.

Associating an Object

1. Log in to [Cloud Monitor Console](#), click **My Alarms** tab, and then click **Alarm Policy** menu.
2. On the alarm policy list page, click the newly created alarm policy. On the details page, click **Add association** button and select the cloud server you want to associate, and then click **Apply** to submit.

Set an Object to Receive Alarms

1. Log in to [Cloud Monitor Console](#), click **My Alarms** tab, and then click **Alarm Policy** menu.
2. Click the created alarm policy to enter its details page, and click **Manage alarm receiver groups** button, and then select the user groups that need to be notified.

Access Control Console Example

Last updated : 2018-08-01 17:57:50

Examples of Access Management Policies for CVMs

You can authorize users to view and use specific resources in the CVM (Cloud Virtual Machine) console by using CAM (Cloud Access Management) policies. The following examples show how to allow users to use specific policies in the console.

Granting Full Access

To allow a user to create and manage CVM instances, apply the policy `QcloudCVMFullAccess`.

Go to [Policy Management](#) page, select **CVM** from all services on the right, and then locate the policy as shown in the figure below.

The screenshot shows the 'Policy Management' (策略管理) page in the Tencent Cloud console. On the left sidebar, 'Policy Management' is selected under 'Users and Permissions' (用户与权限). The main area displays a list of policies. A red box highlights the 'QcloudCVMFullAccess' policy, which grants full read/write access to CVM services. Above the table, there are tabs for 'Predefined Policies' (预设策略) and 'Custom Policies' (自定义策略), and a dropdown menu for 'Cloud Servers' (云服务器).

策略名	备注	操作
QcloudCVMInnerReadOnlyAccess	云服务 (CVM) 只读访问权限	关联用户/组
QcloudCVMReadOnlyAccess	云服务 (CVM) 相关资源只读访问权限	关联用户/组
QcloudCVMFullAccess	云服务 (CVM) 全读写访问权限	关联用户/组

The policy syntax is as follows:

```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
```

```
"name/cvm:*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"name/vpc:*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"name/clb:*"
],
"resource": "*",
"effect": "allow"
},
{
"effect": "allow",
"action": "name/monitor:*",
"resource": "*"
}
]
}
```

The above policy is designed to grant users the permissions to work with all the resources in CVM, VPC, CLB and Cloud Monitoring.

Granting Read Access

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

Note: It's recommended to apply the read-only policy for CVMs.

Go to [Policy Management](#) page, select **CVM** from all services on the right, and then locate the policy as shown in the figure below.

用户与权限

用户管理

用户组管理

策略管理

策略管理

用户或者用户组与策略关联后，即可获得策略所描述的操作权限。

预设策略

自定义策略

云服务器

策略名	备注	操作
QcloudCVMInnerReadOnlyAccess	云服务（CVM）只读访问权限	关联用户/组
QcloudCVMReadOnlyAccess	云服务（CVM）相关资源只读访问权限	关联用户/组
QcloudCVMFullAccess	云服务（CVM）全读写访问权限	关联用户/组

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 all actions starting with `Describe` and `Inquiry` in CVM.

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, apply the policy `QcloudCVMReadOnlyAccess`.

Go to [Policy Management](#) page, select **CVM** from all services on the right, and then locate the policy as shown in the figure below.

用户与权限

用户管理

用户组管理

策略管理

策略管理

用户或者用户组与策略关联后，即可获得策略所描述的操作权限。

预设策略

自定义策略

云服务器

策略名	备注	操作
QcloudCVMInnerReadOnlyAccess	云服务（CVM）只读访问权限	关联用户/组
QcloudCVMReadOnlyAccess	云服务（CVM）相关资源只读访问权限	关联用户/组
QcloudCVMFullAccess	云服务（CVM）全读写访问权限	关联用户/组

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 actions:

- All actions starting with `Describe` and `Inquiry` in CVM.
- All actions starting with `Describe`, `Inquiry` and `Get` in VPC.
- All actions starting with `Describe` in CLB.
- All actions in Monitor.

Policy for elastic cloud disks

To allow a user to view, create and use cloud disks in the CVM console, add the following actions to your policy and associate the policy to the user.

- **CreateCbsStorages:** Create Cloud Disk.
- **AttachCbsStorages:** Mount the specified elastic cloud disk to the specified CVM.
- **DetachCbsStorages:** Unmount the specified elastic cloud disk.
- **ModifyCbsStorageAttributes:** Modify the name or the project ID of the specified cloud disk.
- **DescribeCbsStorages:** Query the details of a cloud disk.
- **DescribeInstancesCbsNum:** Query the number of elastic cloud disks that have been mounted to a CVM and the maximum number of elastic cloud disks that are allowed to be mounted to the CVM.
- **RenewCbsStorage:** Renew the specified elastic cloud disk.
- **ResizeCbsStorage:** Expand the capacity of the specified elastic cloud disk.

The following policy does not allow users to modify the attributes of cloud disks.

```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "name/cvm:ModifyCbsStorageAttributes",
      ],
      "resource": [
        "qcs::cvm::uin/1410643447:*"
      ],
    }
  ]
}
```

```
"effect": "deny"  
}  
]  
}
```

Policy for security groups

To allow a user to view and use security groups in the CVM console, add the following operations to your policy and associate the policy to the user.

- **DeleteSecurityGroup:** Delete a security group.
- **ModifySecurityGroupPolicys:** Replace all the policies of a security group.
- **ModifySingleSecurityGroupPolicy:** Modify single security group policy.
- **CreateSecurityGroupPolicy:** Create a security group.
- **DeleteSecurityGroupPolicy:** Delete a security group policy.
- **ModifySecurityGroupAttributes:** Modify the attributes of security group.

The following policy allows users to create and delete security groups in the CVM console.

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

The following policy allows users to create, delete and modify security group policies in the CVM console.

```
{  
  "version": "2.0",  
  "statement": [  
    {  
      "action": [  
        "name/cvm:ModifySecurityGroupPolicys",  
        "name/cvm:ModifySingleSecurityGroupPolicy",  
        "name/cvm:CreateSecurityGroupPolicy",  
        "name/cvm:DeleteSecurityGroupPolicy",  
        "name/cvm:ModifySecurityGroupAttributes"  
      ],  
      "resource": "*",  
      "effect": "allow"  
    }  
  ]  
}
```

```
"name/cvm:DeleteSecurityGroupPolicy"
],
"resource": "*",
"effect": "allow"
}
]
}
```

Policy for EIPs

To allow a user to view and use EIPs in the CVM console, add the following operations to your policy and associate the policy to the user.

- **AllocateAddresses:** Assign address to VPC or CVM.
- **AssociateAddress :** Associate an EIP to an instance or a network interface.
- **DescribeAddresses:** View the EIPs in the CVM console.
- **DisassociateAddress:** Disassociate an EIP from an instance or a network interface.
- **ModifyAddressAttribute:** Modify the attributes of EIP.
- **ReleaseAddresses:** Terminate the EIP.

The following policy allows users to view EIPs and associate EIPs with instances. Users cannot modify the attributes of EIPs, disassociate EIPs from instances, or release EIPs.

```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "name/cvm:DescribeAddresses",
        "name/cvm:AllocateAddresses",
        "name/cvm:AssociateAddress"
      ],
      "resource": "*",
      "effect": "allow"
    }
  ]
}
```

Policy for authorizing users to perform operations on specific CVMs

To authorize a user to perform operations on a specific CVM, associate the following policy to the user. The following policy authorizes the user to work with a CVM instance (ID: ins-1) in Guangzhou region.

```
{
  "version": "2.0",
  "statement": [
    {
      "action": "cvm:*",
      "resource": "qcs::cvm:gz::instance/ins-1",
      "effect": "allow"
    }
  ]
}
```

Policy for authorizing users to perform operations on the CVMs in a specific region

To authorize a user to perform operations on the CVMs in a specific region, associate the following policy to the user.

The following policy authorizes the user to work with CVM instances in Guangzhou region.

```
{
  "version": "2.0",
  "statement": [
    {
      "action": "cvm:*",
      "resource": "qcs::cvm:gz::*",
      "effect": "allow"
    }
  ]
}
```

Custom policies

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.