

Cloud Virtual Machine

Notice

Product Documentation



Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

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

Notice

About Snapshot Commercialization

Vulnerability repairing for Linux images

Stopping supporting for Ubuntu 10.04 images

Solution for Ubuntu 14.04 images unabling to start Tomcat

Upgrading Virtio network card drive for Windows CVMs

Notice

About Snapshot Commercialization

Last updated : 2019-08-15 10:58:22

Commercialization of Cloud Block Storage (CBS) Snapshot service started at 0:00 on January 22, 2019 for Tencent Cloud China, and will start at 0:00 on March 1, 2019 for Tencent Cloud International. After the commercial launch, all existing and new snapshots will be billed based on the storage capacity used by the snapshots.

The underlying data storage of [images](#) uses the CBS Snapshot service; therefore, keeping custom images will take up a certain amount of snapshot capacity and incur fees.

Commercialization Details

Snapshot Commercialization Dates and Scopes

The commercialization covers all Tencent Cloud China and Tencent Cloud International users.

For Tencent Cloud China,

- At 0:00 on January 22, 2019, commercialization kicks off for Asia Pacific (Tokyo).
- At 0:00 on January 23, 2019, commercialization kicks off for Southeast Asia (Hong Kong, China) and other global regions.
- At 0:00 on January 24, 2019, commercialization kicks off for South China (Shenzhen Finance), South China (Guangzhou Open) and East China (Shanghai Finance).
- At 0:00 on January 25, 2019, commercialization kicks off for North China (Beijing), East China (Shanghai), South China (Guangzhou), Southwest China (Chengdu) and Southwest China (Chongqing).

For Tencent Cloud International, the commercialization starts from March 1, 2019.

What Upgraded Services Will Be Available After Commercialization?

After the Snapshot service is commercialized, Tencent Cloud will provide better services to all users.

The values listed in the table below are the maximum values supported in the same region under a single Tencent Cloud account.

Improvement	Before Commercialization	After Commercialization
Number of snapshots	0 + cloud disks in the region * 7	64 + cloud disks in the region * 64
Total snapshot capacity	20 TB	50 TB
Number of periodic snapshot policies	20	30
Number of cloud disks that can be bound to each periodic snapshot policy	100	200
Maximum cloud disk capacity supported by each periodic snapshot	1000 GB	16 TB

Snapshots and Images

- The underlying data storage of images uses the CBS Snapshot service, i.e., the system automatically generates an associated snapshot when an image is created. An image and a snapshot associated with it are in a binding relationship, so if you want to delete the associated snapshot, you need to [delete the image](#) first. You can view the information of the snapshot associated with a custom image in the image details.
- When using a shared image, only the creator of the image needs to pay for the snapshot.
- An associated snapshot generated by a custom image is billed by the actual capacity of the snapshot. You can view the total snapshot capacity in the snapshot overview.
- A Tencent Cloud account that is in arrears will be unable to create a custom image. Please ensure that your Tencent Cloud account has sufficient balance before creating an image.

Snapshot Billing

- Billing method: The Snapshot service is billed based on the total storage capacity of your snapshots in each region separately. Currently, the service is **pay-as-you-go** and billed at the start of each hour.
- Prices: Snapshot prices vary by region. For details, see [Pricing Overview](#).
- Freezing policy: Once your Tencent Cloud account falls into arrears, snapshot-related operations such as creation, rollback, cross-region replication and periodic snapshot policies will be immediately disabled. When the account is in arrears for 30 days, all snapshots will be deleted.

Complimentary Quota

After the commercialization of the Snapshot service, Tencent Cloud will continue providing users in all regions in mainland China with a certain amount of complimentary quota. As long as the user has cloud disks in normal state (not "to be repossessed" or "terminated"), the user can use 50 GB of snapshot

capacity free of charge. Our statistics show that more than 80% of current snapshot users are within the complimentary quota range. Users exceeding the quota need to pay for the storage capacity occupied by the snapshot data.

After the commercialization, the Snapshot service will be billed based on the actual data size of the snapshots instead of the associated cloud disk size. The total capacity of the former is generally much smaller than that of the latter, subject to the size of data difference between each snapshot in the snapshot chain.

Manually Created Snapshots and Periodic Snapshots

Tencent Cloud provides two ways to create snapshots.

- **Manually created snapshots:** You can manually back up the data of the cloud disk at a selected point in time into snapshots to create multiple copies of the same cloud disk or restore the cloud disk to the state of the selected point in time in the future. For details, see [Creating a Snapshot](#).
- **Periodic snapshots:** Periodic snapshots can be used to provide continuous backups as your businesses continues to update. To continuously back up the cloud disk data in a certain period of time, you only need to create a backup policy and associate cloud disks to it, which greatly improves data security. For details, see [Periodic Snapshots](#).

How to Effectively Reduce the Snapshot Costs After Commercialization?

For Users Who Plan to Continue Using Snapshots

- Delete snapshots that are no longer in use.
- Delete custom images and their associated snapshots that are no longer in use.
- Lower the frequency of snapshot creation for non-core businesses.
- Shorten the snapshot retention period for non-core businesses.

Business scenario	Snapshot frequency	Recommended snapshot retention period
-------------------	--------------------	---------------------------------------

Business scenario	Snapshot frequency	Recommended snapshot retention period
Core businesses	Periodic snapshots are recommended at the frequency of once per day	7 - 30 days
Non-core, non-data businesses	Periodic snapshots are recommended at the frequency of once per week	7 days
Archiving businesses	We recommend to manually creating snapshots based on actual business needs with no fixed frequency required	One to several months
Testing businesses	We recommend to manually creating snapshots based on actual business needs with no fixed frequency required	Delete promptly after use

For Users Who Plan to Stop Using Snapshots

- Check and delete existing snapshots: Check the existing snapshots by region and delete them.
- Check and delete existing custom images and their associated snapshots: Check the existing custom images by region, delete them and then delete the their associated snapshots.
- Check and modify the periodic snapshot policies: Check the existing periodic policies by region, delete them or set them to unavailable so as to avoid further generation of new periodic snapshots.

Vulnerability repairing for Linux images

Last updated : 2018-09-20 17:13:05

Tencent Cloud Security Center will pay close attention to all kinds of security vulnerabilities. When any important security vulnerabilities are officially released, Tencent Cloud Security Center will keep track of the vulnerabilities in a timely manner, inform users of information about the vulnerabilities and provide the solutions to fix the vulnerabilities.

Fixing period of Tencent Cloud official images

- Vulnerability fixing on a regular basis: Tencent Cloud will conduct vulnerability fixing on official images periodically with the frequency being twice a year;
- The fixing of high-risk vulnerabilities: For high-risk vulnerabilities, Tencent Cloud will provide emergency fixes for customers at the earliest possible time.

Image types covered by vulnerability fixing

With its security maintenance principles for images being in consistent with those of the upstream official image releases, Tencent Cloud will conduct security maintenance for the system versions that are within the official maintenance period.

CentOS

CentOS only maintains updates of software and vulnerabilities for the latest minor versions of the current major versions. Tencent Cloud, with its maintenance principles being consistent with that of CentOS, only conducts regular vulnerability fixing and emergency fixing for high-risk vulnerabilities for the latest minor versions of the current major versions within the official maintenance period.

Notes on the maintenance of Tencent Cloud's existing CentOS version images:

- Centos 7.2 64-bit (Centos will continue to provide support until the next minor version is released)
- Centos 7.1 64-bit (Centos has officially stopped providing support for this)
- Centos 7.0 64-bit (Centos has officially stopped providing support for this)
- Centos 6.8 32/64-bit (Centos will continue to provide support until the next version is released)
- Centos 6.7 32/64-bit (Centos has officially stopped providing support for this)
- Centos 6.6 32/64-bit (Centos has officially stopped providing support for this)
- Centos 6.5 32/64-bit (Centos has officially stopped providing support for this)
- Centos 6.4 32/64-bit (Centos has officially stopped providing support for this)

- Centos 6.3 32/64-bit (Centos has officially stopped providing support for this)
- Centos 6.2 64-bit (Centos has officially stopped providing support for this)
- Centos 5.11 32/64-bit (Centos will continue to provide support)
- Centos 5.8 32/64-bit (Centos has officially stopped providing support for this)

Ubuntu

Ubuntu officially provides long-term updating and maintenance services for software and vulnerabilities of the LTS version system. The updating for the server version of each LTS system will last for 5 years. Tencent Cloud officially provides all the LTS version server systems and, aiming to ensure the consistency with Ubuntu's official release, conducts regular vulnerability updates on the images within the maintenance period and conducts emergency fixing on high-risk vulnerabilities.

Notes on the maintenance of Tencent Cloud's existing Ubuntu version images:

- Ubuntu 10.04 LTS 32/64-bit (Ubuntu has officially stopped its maintenance and production)
- Ubuntu 12.04 LTS 64-bit (It is expected that its maintenance will be stopped by April 2017)
- Ubuntu 14.04 LTS 32/64-bit (It is expected that its maintenance will be stopped by April 2019)
- Ubuntu 16.04 LTS 32/64-bit (It is expected that its maintenance will be stopped by April 2021)

Debian

Debian officially maintains two main branches: stable and oldstable. The stable is current stable version and the oldstable is last stable version. Debian will officially maintain the updates of software and vulnerabilities for the stable system. For oldstable system, volunteers and communities will provide LTS (Long Term Support) maintenance schemes. Tencent Cloud always maintains a consistency with its upstream official system in maintenance strategies and only conducts regular vulnerability fixing on the stable branch system maintained officially by Debian.

Notes on the maintenance of Tencent Cloud's existing Debian version images:

- Debian 8.2 32/64-bit (It is expected that its maintenance will be stopped by June 6, 2018)
- Debian 7.8 32/64-bit (Debian has officially stopped its maintenance)
- Debian 7.4 64-bit (Debian has officially stopped its maintenance)

openSUSE

According to the life cycle of openSUSE system, Tencent Cloud conducts vulnerability fixing on images on a regular basis for systems that are officially supported.

Notes on the maintenance of Tencent Cloud's existing openSUSE version images:

- openSUSE 13.2 (It is expected that its maintenance will be stopped by the first quarter of 2017)
- openSUSE 12.3 32/64-bit (openSUSE has officially stopped its maintenance)

FreeBSD

Since the FreeBSD 11.0-RELEASE, FreeBSD has been providing a 5-year maintenance period for the stable branch. For the versions earlier than 11.0-RELEASE, FreeBSD provides different maintenance periods for different types. Tencent Cloud always maintains a consistency with FreeBSD in maintenance principles.

Notes on the maintenance of Tencent Cloud's existing FreeBSD version images:

- 10.1-RELEASE (It is expected that its maintenance will be stopped by December 31, 2016)

Commercial version system

Tencent Cloud does not provide updates and maintenance for vulnerabilities of commercial version system. The commercial version images currently provided by Tencent Cloud include:

- SUSE Linux Enterprise Server 12 64-bit
- SUSE Linux Enterprise Server 11 SP3 64-bit

Stopping supporting for Ubuntu 10.04 images

Last updated : 2017-04-07 12:48:41

Ubuntu has officially stopped the maintenance for Ubuntu 10.04 LTS, so Tencent Cloud has also stopped offering the public images of Ubuntu 10.04.

The directory trees for Ubuntu10.04 LTS have been deleted from the latest official source warehouse. To ensure the consistency with the official source warehouse, Tencent Cloud software warehouse will no longer provide support for Ubuntu 10.04 LTS under the official source directory tree. It is recommended to change the images to a higher version.

If existing users hope to continue to use the software source of Ubuntu 10.04, we provide support in two ways:

Method 1: Manually update configuration file

To improve the user experience, the Tencent Cloud software warehouse pulls the official archive source of Ubuntu 10.04 LTS (<http://old-releases.ubuntu.com/ubuntu/>) for users. Users can use the warehouse as usual by manually modifying the configuration file:

Open the apt source configuration file `vi /etc/apt/sources.list`, and modify the following codes:

```
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid main restricted universe multiverse
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-updates main restricted universe m
ultiverse
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-security main restricted universe m
ultiverse
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-backports main restricted universe
multiverse
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid main restricted universe multiverse
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-updates main restricted universe multi
verse
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-security main restricted universe multiv
erse
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-backports main restricted universe mul
tiverse
```

Method 2: Run the automated script

Make the configuration using the script provided by Tencent Cloud ([old-archive.run])(<http://ubuntu10-10016717.cos.myqcloud.com/old-archive.run>). Download the file to Ubuntu 10.04 CVM and run the following commands:

```
chmod +x old-archive.run  
./old-archive.run
```

Solution for Ubuntu 14.04 images unabling to start Tomcat

Last updated : 2019-07-26 09:26:52

Dear User:

Tencent Cloud found that when Tomcat and Hadoop are installed by using apt-get on the Ubuntu14.04 CVM purchased from Tencent Cloud official website, the port can be listened normally but can not respond to requests. Tencent Cloud has provided solution to this problem. You're recommended to deal with the problem with the suggested solution.

Cause of the problem It is caused by a known problem of Java Runtime Environment.

Problem Analysis

Tomcat and Hadoop are developed with Java and thus use API of `java.security.SecureRandom`. The API is generated with `"/dev/random"` by default in some JREs, whereas `"/dev/random"` receives CPU temperature as well as noises of such hardware as keyboard to generate entropy. As CVM is a virtual machine environment using virtualization technology, it is difficult for it to sense the signals such as CPU temperature and to generate entropy. For this reason, the `'cat /dev/random'` is almost blocked, thus preventing Tomcat and Hadoop from being started.

Change the JRE configuration

Please change the `'securerandom.source=file:/dev/urandom'` in the original `"/etc/java-7-openjdk/security/java.security"` (the URL depends on the situation) to `'securerandom.source=file:/dev/.urandom'` to avoid the above problems.

October 14, 2016

Tencent Cloud

Upgrading Virtio network card drive for Windows CVMs

Last updated : 2017-10-18 22:44:23

To prevent the Windows CVM) created between June and August of 2016 from becoming offline in extreme cases that may affect your normal business operation, we provide an upgrader for upgrading Virtio NIC driver. We strongly recommend you to install the upgrader as instructed by the following advices. After the upgrade, you can solve the problem by simply restarting the system.

Tencent Cloud customers can download the upgrader from the private IP below and complete the upgrade by just one click. Users need to [log in to Windows CVM](#) and access the image site (http://mirrors.tencentyun.com/install/windows/update_netkvm.exe) from inside. After the download, directly run the upgrader or save it to a location and then run it.