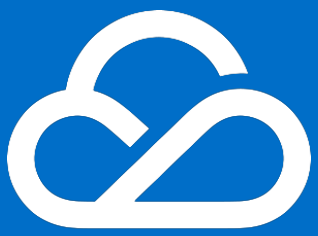
Cloud Virtual Machine

Notice

Product Introduction



Tencent Cloud

Copyright Notice

Trademark Notice

Tencent Cloud

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

Documentation Legal Notice 2
Notice 4
Vulnerability repairing for Linux images 4
Stopping supporting for Ubuntu 10.04 images 8
Solution for Ubuntu 14.04 images unabling to start Tomcat 10
Upgrading Virtio network card drive for Windows CVMs 11

Notice

Vulnerability repairing for Linux images

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

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 multiverse
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-security main restricted universe multiverse
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

multiverse
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-security main restricted universe multiverse
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-backports main restricted universe multiverse

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

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(http://bugs.java.com/bugdatabase/view_bug.do?bug_id=6202721).

【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.

[Solution]

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

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.