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

Windows Server 2003 System Images End of Support Announcement
Vulnerability repairing for Linux images
Stopping supporting for Ubuntu 10.04 images
Solution for Ubuntu 14.04 images unabling to start Tomcat
About Configuration of Security Group Port 53
Upgrading Virtio network card drive for Windows CVMs
Notice

Windows Server 2003 System Images

End of Support Announcement

Last updated : 2020-04-20 18:37:00

Use Instructions

Microsoft has ended extended support for Windows Server 2003 and Windows Server 2003 R2 since July 14, 2015. Tencent CVMs with the Windows 2003 system can no longer receive security updates and patches from Microsoft, and face risks such as program incompatibility, instability and insecurity. To ensure the security and stability of your business, we recommend you migrate CVMs with the Windows Server 2003 system to a newer version of Windows Server, such as Windows Server 2008 R2 and Windows Server 2008 R2.

Risks

Because Microsoft no longer provides security updates and patches, Tencent Cloud cannot solve operating system issues. If you continue to use the Windows Server 2003 system, note the following risks:

1. After July 14, 2015, Tencent CVMs with the Windows Server 2003 system can no longer receive updates and patches from Microsoft. If you continue to use CVMs with this system, your applications and businesses may be exposed to a variety of risks, including but not limited to application incompatibility, compliance requirements, and security problems caused by non-functional issues.

2. If you continue to use CVMs with the Windows Server 2003 system after July 14, 2015, Tencent Cloud will not be held responsible for any failures, security issues, incompatibility or other risks due to lack of support from Microsoft. You will be liable for all the consequences arising therefrom.

Service Instructions

Because Microsoft no longer provides security updates and patches for Windows Server 2003, Tencent Cloud cannot resolve its operating system issues. The following situations are not related to Tencent Cloud's service quality or responsibility:
1. Your instance with the Windows Server 2003 system may be exposed to failures, security issues, incompatibilities, operation exceptions, or system crashes.

2. If an application running in your Windows Server 2003 instance has an exception and needs to be resolved with Microsoft patches or OS support from Microsoft, we can only provide troubleshooting assistance but not a complete solution.

3. Due to hardware compatibility and driver-related limitations, new Tencent CVMs may not be able to support the running of Windows Server 2003 images.
Vulnerability repairing for Linux images

Last updated: 2020-02-25 11:22:33

Tencent Cloud Security Center will pay attention to all kinds of security vulnerability situation in a timely manner. After the official publish important security vulnerability, Tencent Cloud Security Center will promptly follow up vulnerability's situation, provide users with publish and vulnerability information, and provide vulnerability repair plan.

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 5.11 32/64-bit (Centos will continue to provide support)
- Centos 5.11 32/64-bit (Centos will continue to provide support)
- Centos 5.11 32/64-bit (Centos will continue to provide support)
- Centos 5.11 32/64-bit (Centos will continue to provide support)
- Centos 7.1 64-bit (Centos has officially stopped providing support for this)
- Centos 7.1 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 6.6 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 6.6 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 6.6 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 7.1 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 6.6 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 18.04 LTS 64-bit (Ubuntu officially supports maintenance)
- Ubuntu 16.04 LTS 64-bit (Ubuntu officially supports maintenance)
- Ubuntu 10.04 LTS 32/64-bit (Ubuntu has officially stopped its maintenance and production)
- Ubuntu 10.04 LTS 32/64-bit (Ubuntu has officially stopped its maintenance and production)
- Ubuntu 10.04 LTS 32/64-bit (Ubuntu has officially stopped its maintenance and production)

"Debian",
Debian officially maintains two main branch systems: stable and oldstable, where stable is the current stable version and oldstable is the last stable version. Debian officials will maintain software and Vulnerability updates for the stable system, and LTS (Long Term Support) maintenance programs for oldstable will be provided by volunteers and the community. Tencent Cloud is consistent with the upstream official maintenance strategy and only carries out regular Vulnerability repairs to the stable branch system officially maintained by Debian.

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

- Debian 9.064-bit (Debian officially supports maintenance)
- 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 42.3 (maintenance officially supported by openSUSE)
- OpenSUSE 12.3 32/64-bit (openSUSE has officially stopped its maintenance)
- OpenSUSE 12.3 32/64-bit (openSUSE has officially stopped its maintenance)

"FreeBSD",
Since the FreeBSD 11.0 Mutual RELEASE, FreeBSD has been providing a 5-year maintenance period for the stable branch. For the versions earlier than 11.0 Mutual RELEASE, FreeBSD provides different maintenance periods for different types.

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

- FreeBSD 11.1 64-bit (FreeBSD officially supports maintenance)
- FreeBSD 10.1 64-bit (FreeBSD officially stopped maintenance)

**Commercial version system**
Tencent Cloud does not provide Vulnerability updates and maintenance of the commercial version of the system.
Stopping supporting for Ubuntu 10.04 images

Last updated : 2020-02-25 11:21:32

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 Ubuntu 10.04 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:

```bash
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
```

http://mirrors.tencentyun.com/old-archives/ubuntu lucid main restricted universe multiverse
http://mirrors.tencentyun.com/old-archives/ubuntu lucid-updates main restricted universe multiverse
http://mirrors.tencentyun.com/old-archives/ubuntu lucid-security main restricted universe multiverse
http://mirrors.tencentyun.com/old-archives/ubuntu lucid-backports main restricted universe multiverse
Method 2: Run the automated script

Through the script provided by Tencent Cloud Old-archive.run To configure, download this file to Ubuntu 10.04 inside Cloud Virtual Machine and execute the following command:

```
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
Overview

Port 53 is Domain Name Server’s (DNS) open port. It is primarily used for domain name resolution. The DNS acts as a translator between the domain name and IP address, so users only need to remember the domain name to quickly access the website.

The “Classified Catalogue of Telecommunications Businesses” (2015 Edition) has categorized recursive Internet domain name resolution services as telecommunications services (Code number: B26-1). To manage recursive domain name services, the telecommunications services permit must be obtained.

Related policies and regulations

1. Internet domain resolution services are not permitted without a business license.

If you or your company is involved in this business, you must apply for a “Code and Protocol Conversion License”. For specific details, contact your local telecommunications administration.

“Administrative Measures for the Licensing of Telecommunication Business Operations”

Article 46: Whoever violates the provisions of Paragraph 1 of Article 16 and Paragraph 1 of Article 28, whereby arbitrarily engages in telecommunications services or engages in telecommunications services beyond the permitted scope, shall be punished in accordance with Article 69 of the “Telecommunication Regulation of the People's Republic of China”. For serious misconduct, an order will be given to suspend the business for rectification, which will be included in the list of untrustworthy telecommunications services providers.

“Internet Domain Name Regulations” of the Ministry of Industry and Information Technology, Article 36: To provide domain name resolution services, businesses shall comply with relevant laws, regulations and standards, and have the relevant technical, services, network and information security safeguard capacities. Businesses shall put in place network and information security safeguard measures, record and store domain name resolution logs, O&M logs, and change records in accordance with the law, to ensure the service quality of resolution and the security of the resolution system. Where telecommunications services are involved, businesses shall obtain the telecommunications operations licenses in accordance with the law.
2. Tencent Cloud will not provide services, such as access or billing, for individuals or entities who have not obtained business licenses or ICP filings for non-commercial Internet information services.

“Administrative Measures for the Licensing of Telecommunication Business Operations” Article 24, value-added telecommunications businesses providing access services must comply with the following regulation: (Three) The provision of services, such as access or billing, for entities or individuals that have not obtained business licenses or ICP filings for non-commercial Internet information services in accordance with the law is not permitted.

If you or your company does not engage in Internet domain name resolution services, we recommended you adjust the security group policy of your server, and disable port 53 via inbound rules.

Disabling port 53 via inbound rules

1. Log in to the Tencent Cloud CVM Console.
2. In the instance management page, select the instance where port 53 is to be disabled, and click the ID/Name. This is shown in the following figure:

3. In the instance details page, select the Security Groups tab, to enter the security group management page for this instance. This is shown in the following figure:
4. In the **Bound to security group** field, select the **Security Group ID/Name** of the inbound rule that is to be modified.

5. In the **Security Group Rule** page, select the **Inbound Rule** tab. Click **Add a Rule**. This is shown in the following figure.

6. In the **Add Inbound Rule** window that pops up, enter the following information. This is shown in the following figure:
Type: Select “Custom”.
Source: Enter “0.0.0.0/0”.
Protocol port: Enter “UDP:53”.
Policy: Select “Reject”.
7. Click **Complete** to disable port 53.

**FAQs**

**What is the Internet domain name resolution service?**

**Internet Domain Name Resolution** establishes the relationship between an Internet domain name and its corresponding IP address.

**Internet domain name resolution service** builds domain name resolution servers and related software on the Internet to translate Internet domain names to their corresponding IP addresses. There are two types of domain name resolution services: authoritative and recursive resolution services.

- Authoritative resolution: This service provides domain name resolution for root domain names, top-level domain names, and other levels of domain names.
- Recursive resolution: This service establishes the correspondence between domain names and IP addresses by querying the local cache or the authoritative resolution service system.

Internet domain name resolution service here specifically refers to recursive resolution service. For more information, see “Classification Catalog of Telecommunications Services” (2015 Edition): B26-1 Internet domain name resolution services.

**How will disabling port 53 through inbound rules impact my server?**
If you do not engage in Internet domain name resolution services, disabling port 53 through inbound rules does not impact your server or business.

**Can individual engage in domain name resolution services?**

Telecommunications services providers must have established businesses in accordance with the law. An individual cannot engage in this type of service. You must obtain an “Code and Protocol Conversion License” before carrying out Internet domain name resolution services businesses. For more information about obtaining a license, you can contact your local telecommunications administration office.

**What are the impacts of carrying out Internet domain name resolution services without the permit?**

According to the “Telecommunications Regulations of the People's Republic of China” Article 69: (One) Whoever violates Article 7 Paragraph 3 or perform acts listed in Article 58 Item 1, whereby operates a telecommunications business without authorization or operates beyond the permitted scope, is subject to rectification by the Ministry of Industry and Information Technology, the telecommunications regulatory agency of the province, autonomous region, or municipality, including the confiscation of illegal income and a fine between 3 to 5 times the illegal income. If there is no illegal income or the illegal income does not exceed 50,000 RMB, the penalty will be between 100,000 RMB and 1,000,000 RMB. For serious misconduct, an order will be given to suspend the business for rectification.
Upgrading Virtio network card drive for Windows CVMs

Last updated : 2020-04-20 18:33:21

To prevent the extreme case where Windows CVMs created between June and August of 2016 become offline and affect your business operation, we provide an upgrade program for the Virtio network driver. We strongly recommend you follow the instructions below to install the upgrade program. You can then solve the problem by simply restarting the system.

Tencent Cloud users can download the program from the private IP below and complete the upgrade with 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. After the download, run the upgrade program directly or save it first.

The running result may show the driver has been upgraded successfully, and the new driver will take effect after you restart the system.

The running result may show that the existing driver does not need to be upgraded.