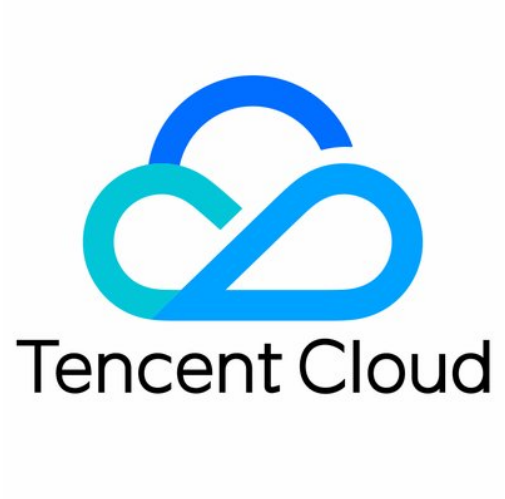
Cloud Virtual Machine

Announcements

Product Documentation



Contents

Announcements
Price Reduction in Selected Availability Zones

Last updated : 2021-06-23 11:11:18

Tencent Cloud has reduced prices of CVM instance in Chinese mainland by up to 10% beginning from March 10, 2021. This price reduction applies to multiple regions, availability zones and over 90% instance types.

Scope	Description
Availability zone	Guangzhou Zone 6, Beijing Zone 6, Nanjing Zone 1, Nanjing Zone 2, and Nanjing Zone 3
Instance type	Standard S5, Standard SA2, Standard S4, Standard Storage Optimized S5se, Memory Optimized M5, Compute Optimized C5, Compute Optimized C4, Big Data D3, Big Data D2, High IO IT5, and High IO IT3

Updates

- The updated price takes effect on March 10, 2021. This document describes the price adjustments. For specific prices, see the CVM pricing or purchase page, or use the CVM price calculator.
- Starting from March 10, 2021, you can **purchase or renew** monthly subscription or pay-as-you-go CVM instances at the updated price.

Notes

- The price adjustment only applies to CVM computing resources, excluding network and cloud disk fees.
- The updated price takes effect from March 10, 2021 and remains effective till the next price adjustment.
- For the latest CVM prices, see CVM Pricing. For specific CVM prices including cloud disk and network fees, use the CVM Price Calculator.
- For more information about CVM instance types, see Instance Types.

FAQs

A monthly-subscribed CVM instance under my account will expire in late December 2021. Can I get a refund according to the price reduction after March 10, 2021?

No. The existing monthly-subscribed CVM instance will still be charged at the purchase price before it expires. If you renew it, adjust its configurations, return it and purchase a new one, you will be charged with the latest price.

Will the latest price reduction apply to existing pay-as-you-go CVM instances after March 10, 2021?

Yes. The latest price will be applied to the next hourly bill of the existing pay-as-you-go CVM instances after the official publish of price reduction.

Will the latest price reduction apply to CVM instances purchased with a promotional discount applied?

No. The price reduction only applies to CVM instances purchased on the CVM purchase page or via API with the official price.

Contact Us

Please contact us if you have any questions.

WebShell Proxy IP Addresses Updates

Last updated : 2021-06-23 11:11:18

Background

The WebShell proxy IP ranges were updated on April 1, 2021. Please open the new WebShell proxy IP range and the remote login port (port 22 by default) accordingly in the security group.

> Note :
> For more information about WebShell login, see Logging in to Linux Instance Using Standard Login Method.

Updates

- IP ranges added on April 1, 2021:

81.69.102.0/24
106.55.203.0/24
101.33.121.0/24
101.32.250.0/24

- Both the new and old IP addresses and IP ranges can be used, including:

> Note :
> To use the WebShell login service, open all proxy IP ranges and remote login ports to internet in the inbound (source) rule of the security group.

81.69.102.0/24
106.55.203.0/24
101.33.121.0/24
101.32.250.0/24
115.159.198.247
115.159.211.178

119.28.7.195
119.28.22.215
119.29.96.147
211.159.185.38

Relevant Operations

- Logging in to Linux Instance Using Standard Login Method
- Adding Security Group Rules

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. You 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.

Pay-as-you-go Price Adjustments for Standard S3 CVMs in the Silicon Valley Region

Last updated : 2020-09-14 14:27:16

The pay-as-you-go pricing for Tencent Cloud **Standard S3** CVMs in the Silicon Valley region has been updated as follows:

Operating System	Discount
Linux	21% off
Windows	10% off

Notes

- The updated price takes effect on July 24, 2020.
- This document describes the price adjustments. For specific prices, use the CVM Price Calculator.
- For any questions, please contact us.

Vulnerability repairing for Linux images

Last updated : 2020-05-08 14:53:30

Tencent Cloud Security Center pays close attention to security vulnerabilities. After major security vulnerabilities are officially announced, Tencent Cloud Security Center tracks the vulnerabilities in a timely manner, informs users of the vulnerabilities, and provides solutions to fix them.

Vulnerability Fixing Period for Tencent Cloud Official Images

- Periodic vulnerability fixes: Tencent Cloud fixes the vulnerabilities of official images `twice` a year.
- Fixes for high-risk vulnerabilities: for high-risk vulnerabilities, Tencent Cloud issues emergency fixes and provides them to customers once they are ready.

Scope of Images Covered by Vulnerability Fixes

Tencent Cloud's image security maintenance principles are consistent with those of official upstream image releases. Tencent Cloud will perform security maintenance on the system versions that are within the official maintenance period.

CentOS

CentOS only updates software and vulnerabilities for the most recent minor versions of the current major versions. Tencent Cloud's maintenance principles are consistent with those of CentOS. Tencent Cloud only performs periodic vulnerability fixing on the most recent minor versions of the current major versions within the official maintenance period, and releases emergency fixes for high-risk vulnerabilities.

The following provides maintenance information on Tencent Cloud's existing CentOS images:

- CentOS 7.6 64-bit (CentOS continues to provide support.)
- CentOS 7.5 64-bit (CentOS continues to provide support.)
- CentOS 7.4 64-bit (CentOS continues to provide support.)
- CentOS 7.3 64-bit (CentOS continues to provide support.)
- CentOS 7.2 64-bit (CentOS continues to provide support.)
- CentOS 7.1 64-bit (CentOS has stopped providing support.)
- CentOS 7.0 64-bit (CentOS has stopped providing support.)

- CentOS 6.9 32-bit/64-bit (CentOS continues to provide support until the next version is released.)
- CentOS 6.8 32-bit/64-bit (CentOS has stopped providing support.)
- CentOS 6.7 32-bit/64-bit (CentOS has stopped providing support.)
- CentOS 6.6 32-bit/64-bit (CentOS has stopped providing support.)
- CentOS 6.5 32-bit/64-bit (CentOS has stopped providing support.)
- CentOS 6.4 32-bit/64-bit (CentOS has stopped providing support.)
- CentOS 6.3 32-bit/64-bit (CentOS has stopped providing support.)
- CentOS 6.2 64-bit (CentOS has stopped providing support.)
- CentOS 5.11 32-bit/64-bit (CentOS has stopped providing support.)
- CentOS 5.8 32-bit/64-bit (CentOS has stopped providing support.)

Ubuntu

Ubuntu provides the long-term software and vulnerability update service for systems of the LTS versions. It provides the 5-year update service for the server version of each LTS system. Tencent Cloud provides the server systems in various LTS versions. To ensure consistency with official Ubuntu releases, Tencent Cloud periodically updates vulnerabilities for images within the maintenance period, and releases emergency fixes for high-risk vulnerabilities.

The following provides maintenance information on Tencent Cloud's existing Ubuntu images:

- Ubuntu 18.04 LTS 64-bit (Ubuntu provides support.)
- Ubuntu 16.04 LTS 64-bit (Ubuntu provides support.)
- Ubuntu 14.04 LTS 32-bit/64-bit (Ubuntu provides support.)
- Ubuntu 12.04 LTS 64-bit (Ubuntu has stopped providing support.)
- Ubuntu 10.04 LTS 32-bit/64-bit (Ubuntu has stopped providing support.)

Debian

Debian officially maintains two branch systems: stable and oldstable, where "stable" indicates the current stable version and "oldstable" indicates the previous stable version. Debian updates software and vulnerabilities for the stable-version system, whereas volunteers and communities provide the Long Term Support (LTS) for the oldstable-version system. Tencent Cloud's maintenance strategy is consistent with that of Debian, and only periodically fixes vulnerabilities for the stable-version systems maintained by Debian.

The following provides maintenance information on Tencent Cloud's existing Debian images:

- Debian 9.0 64-bit (Debian provides support.)
- Debian 8.2 32-bit/64-bit (Debian plans to stop providing support for this version in June 2019.)
- Debian 7.8 32-bit/64-bit (Debian has stopped providing support.)
- Debian 7.4 64-bit (Debian has stopped providing support.)

openSUSE

Based on the lifecycle of the openSUSE system, Tencent Cloud periodically fixes vulnerabilities for the systems officially supported by openSUSE.

The following provides maintenance information on Tencent Cloud's existing openSUSE images:

- openSUSE 42.3 (openSUSE provides support.)
- openSUSE 13.2 (openSUSE has stopped providing support.)
- openSUSE 12.3 32-bit/64-bit (openSUSE has stopped providing support.)

FreeBSD

Since FreeBSD 11.0-RELEASE, FreeBSD has been providing a 5-year maintenance period for the stable version. For versions earlier than 11.0-RELEASE, FreeBSD provides different maintenance periods for different types of versions. Tencent Cloud's maintenance principles are consistent with those of FreeBSD.

The following provides maintenance information on Tencent Cloud's existing FreeBSD images:

- FreeBSD 11.1 64-bit (FreeBSD provides support.)
- FreeBSD 10.1 64-bit (FreeBSD has stopped providing support.)

Commercial systems

Tencent Cloud does not provide the vulnerability update or fixing service for commercial systems.

Windows Server 2008 R2 Enterprise Edition SP1 64-bit Images End of Support Announcement

Last updated : 2020-12-30 17:09:56

Use Instructions

Microsoft has officially ended the support for Windows Server 2008 since January 14, 2020, and therefore Tencent Cloud has also deactivated the Windows Server 2008 R2 Enterprise Edition SP1 64-bit public image on March 16, 2020. Tencent CVMs using this image can no longer receive security updates and patches from Microsoft, and may be exposed to program compatibility, stability and security risks.

This image now cannot be used to create or reinstall CVM instances, but you can continue using custom images, marketplace images or importing images. To ensure the security and stability of your business, we recommend migrating your Windows Server 2008 R2 Enterprise Edition SP1 64-bit CVM instances to Windows Server 2012 or later versions.

Risks

Because Microsoft no longer provides security updates and patches, the operating system issues cannot be resolved. If you insist on using the Windows Server 2008 R2 Enterprise Edition SP1 64-bit operating system, take note of the following risks:

1. After March 16, 2020, Tencent CVMs with the Windows Server 2008 R2 Enterprise Edition SP1 64-bit operating system can no longer receive updates and patches from Microsoft. Continued use of this operating system may expose your applications and businesses to a variety of risks, including but not limited to application incompatibility, non-compliance, and possible non-functional security problems.
2. If you continue to use CVMs with the Windows Server 2008 operating system after March 16, 2020, Tencent Cloud will not be held responsible for any failures, security issues, incompatibility or other risks of the operating system 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 2008, Tencent Cloud cannot resolve its operating system issues and accepts no responsibility for the following cases:

1. Your instance with the Windows Server 2008 R2 Enterprise Edition SP1 64-bit operating system may be exposed to failures, security issues, incompatibilities, operation exceptions, or even system crashes.
2. If an application running on your Windows Server 2008 R2 Enterprise Edition SP1 64-bit instance has an exception and needs 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 releases of Tencent Cloud CVMs may not be able to support running Windows Server 2008 images.

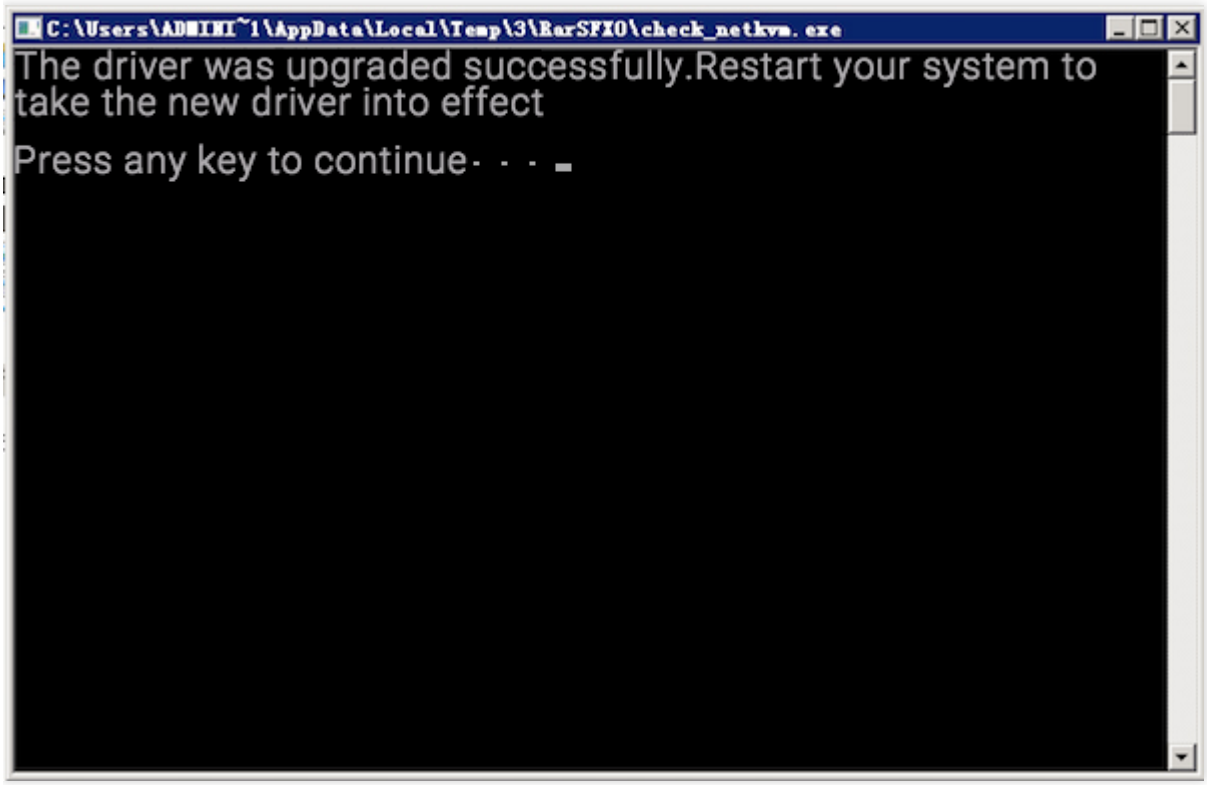
Upgrading Virtio network card drive for Windows CVMs

Last updated : 2020-06-24 17:54:20

To prevent Windows CVMs created between June and August of 2016 from being disconnected from the network in extreme cases and affecting your business operations, we provide an upgrade program for the Virtio ENI driver. We strongly recommend that you install the upgrade program by following the instructions below. Then, simply restart the CVMs.

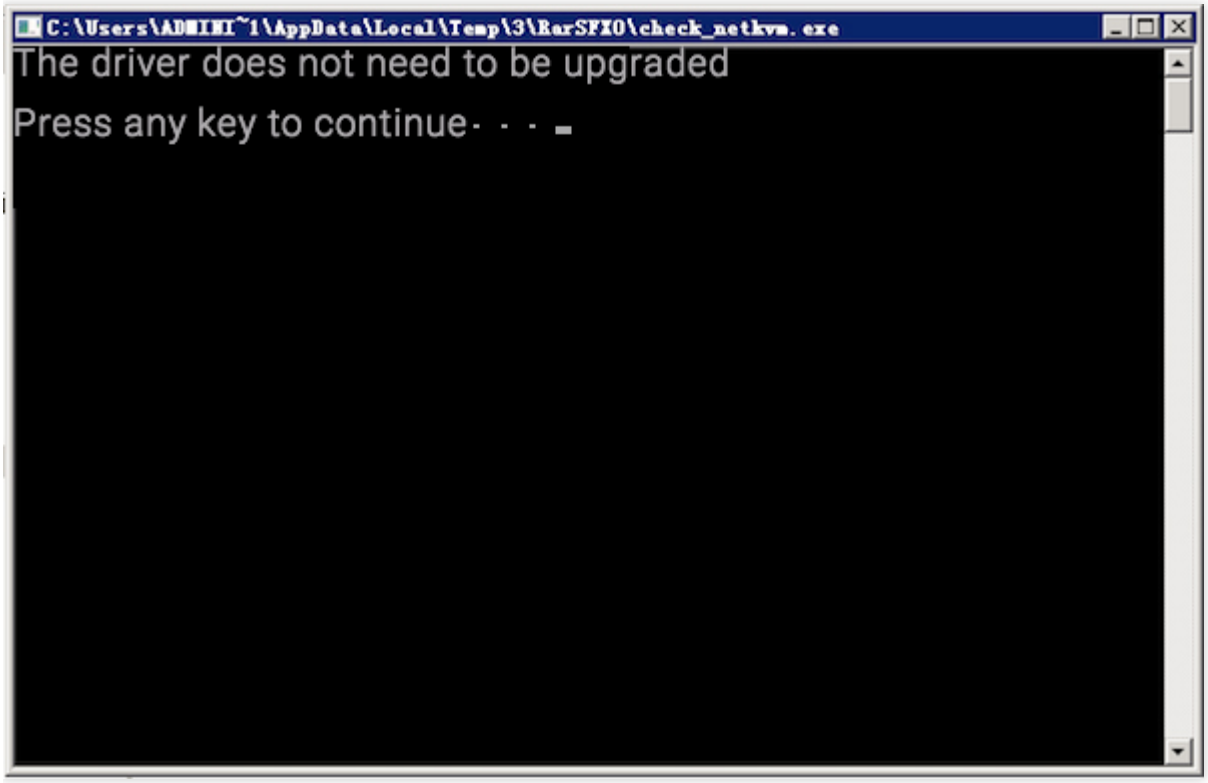
Tencent Cloud users can download the update program from the following private IP address and complete the upgrade with one click. Users need to log in to the Windows CVM and access the image site at `http://mirrors.tencentyun.com/install/windows/update_netkvm.exe` to download the upgrade program. After downloading the program, you can run it immediately or save it and run it later.

If the information shown below appears, the driver was successfully upgraded. Restart the system so that the new driver takes effect.



If the information shown below appears, the existing driver is normal and does not need to be

upgraded.



Solution to Tomcat Start Failure on Ubuntu14.04

Last updated：2020-06-03 14:36:21

It has been detected that when Tomcat or Hadoop is installed via apt-get command on a Ubuntu14.04 CVM purchased from Tencent Cloud, it can listen to the port but cannot respond to requests. A solution is now available. We recommend following the instructions below if you encounter this issue.

Causes

This issue is caused by a known Java Runtime Environment issue.

Analysis

Both Tomcat and Hadoop are developed using the Java `java.security.SecureRandom` API. This API uses `/dev/random` as a random number generator by default in some JREs. `/dev/random` accesses environmental noises collected from devices such as CPU temperature or keyboard timings to generate entropy. However, the virtual environment of CVMs makes it difficult to access such noises and generate entropy, causing `cat /dev/random` to block Tomcat and Hadoop from being started.

Solution

Modifying the JRE configuration

Please change `securerandom.source=file:/dev/urandom` in the original `/etc/java-7-openjdk/security/java.security` (use actual URL) to `securerandom.source=file:/dev/./urandom` to resolve this issue.

Stopping supporting for Ubuntu 10.04 images

Last updated : 2020-05-08 10:47:53

Ubuntu has officially ceased providing maintenance for Ubuntu 10.04 LTS, and therefore Tencent Cloud has also deactivated public images of Ubuntu 10.04.

Directory trees for Ubuntu 10.04 LTS have been deleted from the latest official source repository. To ensure consistency with the official source repository, the Tencent Cloud software repository will no longer support Ubuntu 10.04 LTS under the official source directory tree. Accordingly, we recommend that you upgrade your images to a later version.

For existing users who hope to continue to use the software source of Ubuntu 10.04, we provide support for them in the following ways:

Method 1: Manually Updating the Configuration File

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

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

```
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid main restricted universe multiver
se
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 univers
e 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 mult
iverse
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-security main restricted universe mul
tiverse
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-backports main restricted universe mu
ltiverse
```

Method 2: Running the Automated Script

Use the script old-archive.run provided by Tencent Cloud for configuration. To do this, download the file to the CVM with Ubuntu 10.04 and run the following commands:

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

About Configuration of Security Group Port 53

Last updated : 2020-11-02 11:07:55

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.

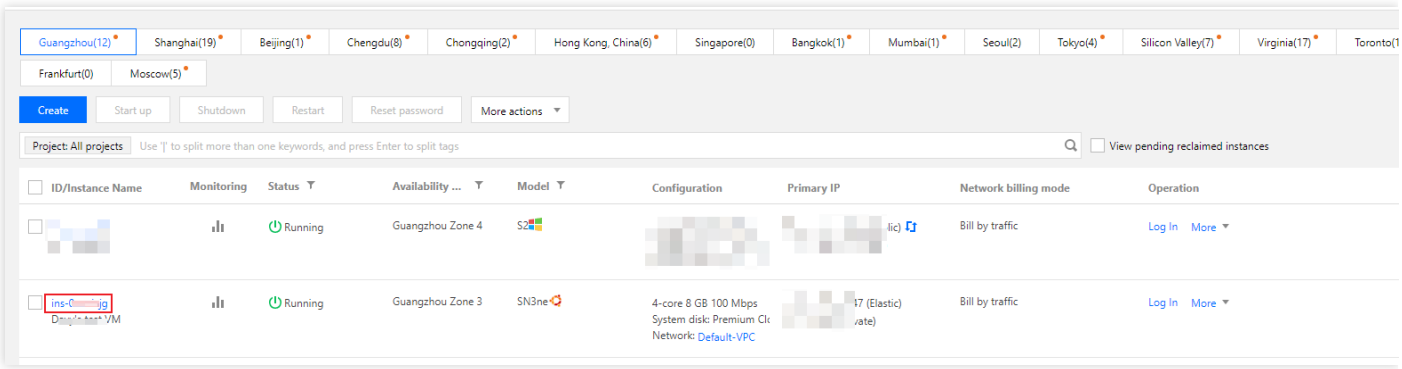
Related policies and regulations

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.

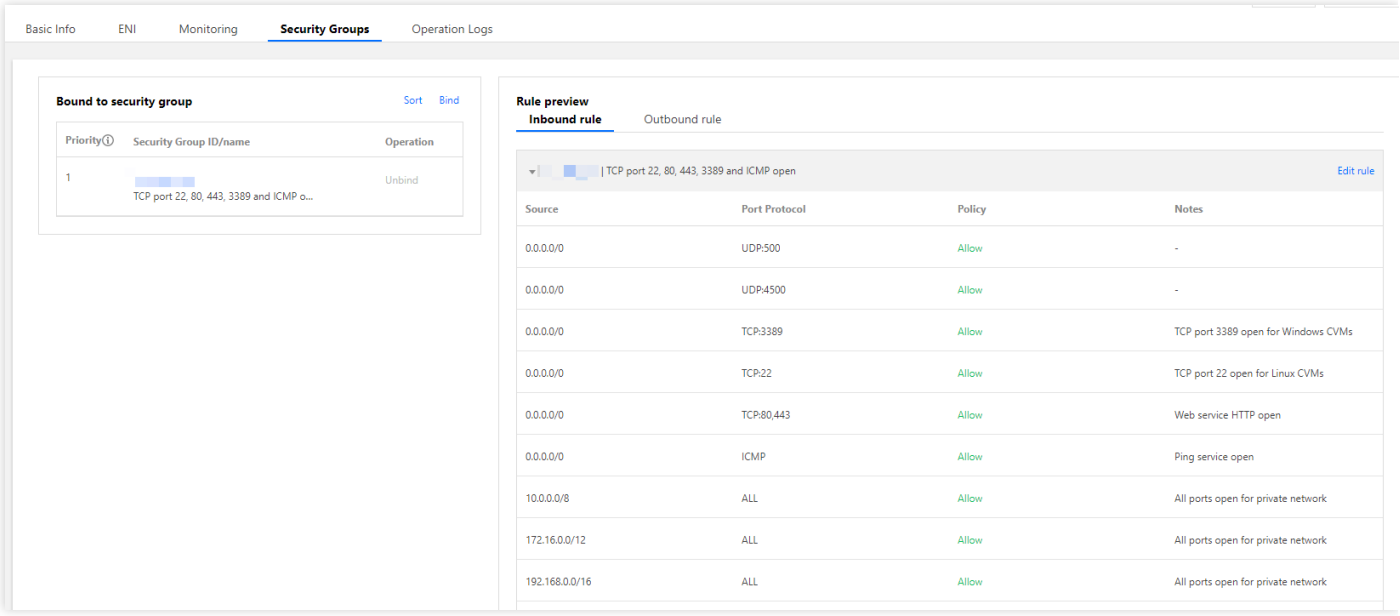
2. Tencent Cloud will not provide services, such as access or billing, for individuals or entities who have not obtained business licenses or ICP filings for non-commercial Internet information services in Mainland China.
“Administrative Measures for the Licensing of Telecommunication Business Operations” 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 Mainland China 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

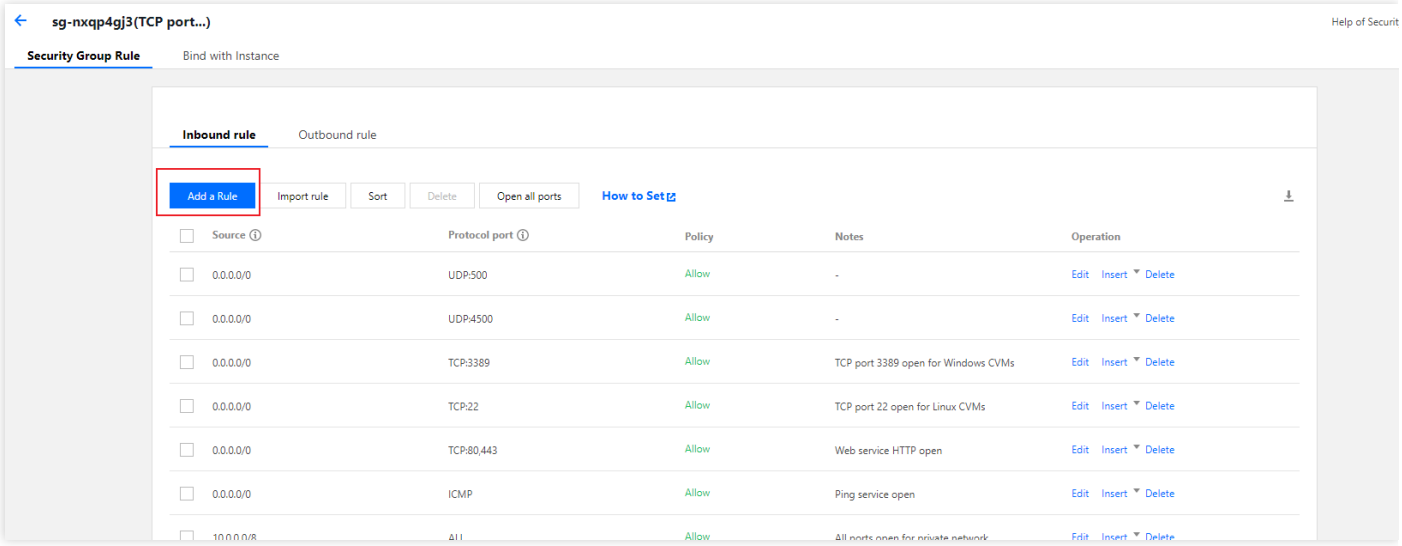
1. Log in to the Tencent Cloud CVM Console.
2. In the instance management page, select the instance where port 53 is to be disabled, and click the **ID/Name**. This is shown in the following figure:



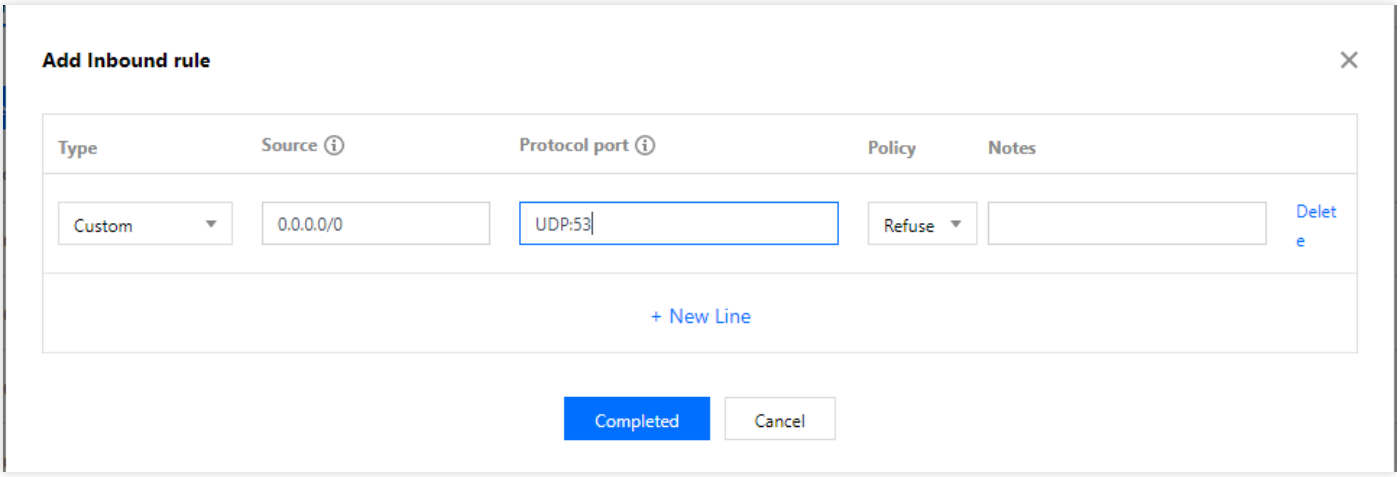
3. In the instance details page, select the **Security Groups** tab, to enter the security group management page for this instance. This is shown in the following figure:



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.