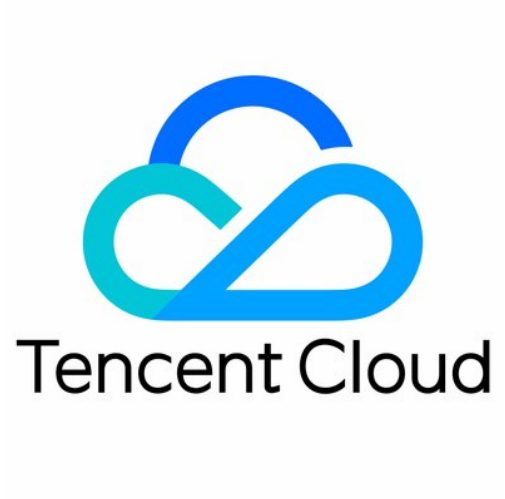
Cloud Virtual Machine

Release Notes and Announcements

Product Documentation



Contents

Release Notes and Announcements
- Release Notes
- Public Image Release Notes
- Announcements
  - Temporary Solution for the Windows Blue Screen Issue Caused by CrowdStrike Security Software on July 19, 2024
  - Announcement on Flexible Discounts for Spot Instances in Some Regions
  - Updating Some Image Pip Package Management Tools for CentOS 7
  - CentOS 8 End of Maintenance
  - Discontinuation of Support for SUSE Commercial Images
  - Price Reduction in Selected Availability Zones
  - OrcaTerm Proxy IP Addresses Updates
  - Pay-as-you-go Price Adjustments for Standard S3 CVMs in the Silicon Valley Region
  - Vulnerability repairing for Linux images
  - Stopping supporting for Ubuntu 10.04 images
  - Solution to Tomcat Start Failure on Ubuntu14.04
  - Upgrading Virtio network card drive for Windows CVMs
  - About Configuration of Security Group Port 53
  - Windows Server 2003 System Images End of Support Announcement
  - End of Support for Windows Server 2008 R2 Enterprise Edition SP1 64-bit System Images

Release Notes and Announcements

Release Notes

Last updated：2024-04-26 16:48:04

April 2024

Update	Description	Documentation
Cloud Virtual Machine (CVM) supports monthly subscription	The monthly Subscription is a prepaid mode of CVM, where you pay upfront for one or several months or even years, offering a more favorable price than the pay-as-you-go billing mode. It does not support refunds before instances expire.	Billing Mode

Public Image Release Notes

Last updated：2024-03-22 15:17:08

Note:

The actual image update time may vary by regions. The update date provided here is the time when the image update is completed in all Tencent Cloud regions.

The public image maintenance plan of Tencent Cloud is consistent with the official maintenance plans of operating system platforms. For more information, see Official Maintenance Plans of Operating Systems.

OpenCloudOS

For update logs of OpenCloudOS, see OpenCloudOS Image Update History.

CentOS

Image Tag	Image Details	Update Date	Updates
CentOS Stream 9x86_64	Image ID: img-9xqekomx Current kernel version: 5.14.0-202.el9.x86_64	12/19/2022	Updates the system with the latest patch.
CentOS Stream 8x86_64	Image ID: img-8m9ugrip Current kernel version: 4.18.0-348.7.1.el8_5.x86_64	9/16/2022	Updates the system with the latest patch.
CentOS 8.5x86_64	Image ID: img-es95t8wj Current kernel version: 4.18.0-348.7.1.el8_5.x86_64	11/23/2022	Updates the system with the latest patch.
CentOS 8.4x86_64	Image ID: img-l5eqiljn Current kernel version: 4.18.0-348.7.1.el8_5.x86_64	11/7/2022	Updates the system with the latest patch.
CentOS 8.3x86_64	Image ID: img-5w4qozfr Current kernel version: 4.18.0-348.7.1.el8_5.x86_64	11/7/2022	Updates the system with the latest patch.
CentOS 8.2x86_64	Image ID: img-n7nyt2d7、Current kernel version: 4.18.0-348.7.1.el8_5.x86_64	8/24/2022	Updates the system with the latest patch.

CentOS 8.0x86_64	Image ID: img-25szkc8t Current kernel version: 4.18.0-348.7.1.el8_5.x86_64	3/17/2022	Updates the system with the latest patch.
CentOS 7.9x86_64	Image ID: img-l8og963d Current kernel version: 3.10.0-1160.71.1.el7.x86_64	3/6/2023	Updates the system with the latest patch.
CentOS 7.8x86_64	Image ID: img-3la7wgnt、Current kernel version: 3.10.0-1160.62.1.el7.x86_64	4/19/2022	Updates the system with the latest patch.
CentOS 7.7x86_64	Image ID: img-1u6l2i9l、Current kernel version: 3.10.0-1160.62.1.el7.x86_64	4/22/2022	Updates the system with the latest patch.
CentOS 7.6x86_64	Image ID: img-9qabwvbn Current kernel version: 3.10.0-1160.62.1.el7.x86_64	4/28/2022	Updates the system with the latest patch.
CentOS 7.5x86_64	Image ID: img-oikl1tzv Current kernel version: 3.10.0-1160.71.1.el7.x86_64	12/2/2022	Updates the system with the latest patch.
CentOS 7.4x86_64	Image ID: img-8toqc6s3 Current kernel version: 3.10.0-1160.62.1.el7.x86_64	4/19/2022	Updates the system with the latest patch.
CentOS 7.3x86_64	Image ID: img-dkwyg6sr Current kernel version: 3.10.0-1160.62.1.el7.x86_64	4/22/2022	Updates the system with the latest patch.
CentOS 7.2x86_64	Image ID: img-31tjrtph Current kernel version: 3.10.0-1160.83.1.el7.x86_64	3/6/2023	Updates the system with the latest patch.
CentOS 6.10x86_64	Image ID: img-fizif873 Current kernel version: 2.6.32-754.35.1.el6.x86_64	1/17/2022	Updates the system with the latest patch.
CentOS 6.9x86_64	Image ID: img-i5u2lkoz Current kernel version: 2.6.32-754.30.2.el6.x86_64	1/18/2022	Updates the system with the latest patch.

Ubuntu

Image Tag	Image Details	Update Date	Updates

Ubuntu 22.04x86_64	Image ID: img-487zeit5 Current kernel version: 5.15.0-56-generic	12/8/2022	Updates the system with the latest patch.
Ubuntu 20.04x86_64	Image ID: img-22trbn9x Current kernel version: 5.4.0-126-generic	9/20/2022	Updates the system with the latest patch.
Ubuntu 18.04x86_64	Image ID: img-pi0ii46r Current kernel version: 4.15.0-193-generic	11/3/2022	Updates the system with the latest patch.
Ubuntu 16.04x86_64	Image ID: img-pyqx34y1 Current kernel version: 4.4.0-210-generic	3/21/2022	Updates the system with the latest patch.

Debian

Image Tag	Image Details	Update Date	Updates
Debian 11.4x86_64	Image ID: img-btz2mndd Current kernel version: 5.10.0-16-amd64	9/8/2022	Updates the system with the latest patch.
Debian 11.1x86_64	Image ID: img-4cmp1f33 Current kernel version: 5.10.0-19-amd64	11/3/2022	Updates the system with the latest patch.
Debian 10.12x86_64	Image ID: img-7ay90qj7 Current kernel version: 4.19.0-21-amd64	9/23/2022	Updates the system with the latest patch.
Debian 10.11x86_64	Image ID: img-h1yvvfw1 Current kernel version: 4.19.0-22-amd64	11/1/2022	Updates the system with the latest patch.
Debian 10.2x86_64	Image ID: img-qhtfjw1d Current kernel version: 4.19.0-19-amd64	11/1/2022	Updates the system with the latest patch.
Debian 9.13x86_64	Image ID: img-5k0ys7jp Current kernel version: 4.9.0-19-amd64	9/30/2022	Updates the system with the latest patch.

Debian 9.0x86_64	Image ID: img-6rrx0ymd Current kernel version: 4.9.0-19-amd64	11/3/2022	Updates the system with the latest patch.
Debian 8.11x86_64	Image ID: img-2lj11q1f Current kernel version: 3.16.0-11-amd64	11/7/2022	Updates the system with the latest patch.

Red Hat Enterprise Linux

Image Tag	Image Details	Update Date	Updates
Red Hat Enterprise Linux 8.5	Image ID: img-r5xber0b Current kernel version: 4.18.0-425.19.2.el8_7.x86_64	4/27/2023	Updates the system with the latest patch.
Red Hat Enterprise Linux 7.9	Image ID: img-0qhxz7dl Current kernel version: 3.10.0-1160.88.1.el7.x86_64	4/27/2023	Updates the system with the latest patch.

Note:

You can select an instance model that has been certified for Red Hat Enterprise Linux to use the Red Hat Enterprise Linux image. For supported image tags and instance models, see FAQs about Red Hat Enterprise Linux Image.

AlmaLinux

Image Tag	Image Details	Update Date	Updates
AlmaLinux 9.0x86_64	Image ID: img-f089mf4l Current kernel version: 5.14.0-70.13.1.el9_0.x86_64	10/27/2022	Releases an image.
AlmaLinux 8.6x86_64	Image ID: img-jy2bb29p Current kernel version: 4.18.0-372.19.1.el8_6.x86_64	10/25/2022	Updates the system with the latest patch.
AlmaLinux 8.5x86_64	Image ID: img-4ogcw28j Current kernel version: 4.18.0-348.20.1.el8_5.x86_64	9/30/2022	Updates the system with the latest patch.

Fedora

Image Tag	Image Details	Update Date	Updates
Fedora36x86_64	Image ID: img-ge141oql Current kernel version: 5.19.14-200.fc36.x86_64	11/7/2022	Updates the system with the latest patch.
Fedora 37x86_64	Image ID: img-d7j9x59z Current kernel version: 6.0.7-301.fc37.x86_64	11/30/2022	Releases an image.

FreeBSD

Image Tag	Image Details	Update Date	Updates
FreeBSD 13.1x86_64	Image ID: img-ng3lehjp Current kernel version: 13.1-RELEASE	9/16/2022	Updates the system with the latest patch.
FreeBSD 13.0x86_64	Image ID: img-1lkqxofp Current kernel version: 13.0-RELEASE	9/2/2022	Updates the system with the latest patch.
FreeBSD 12.3x86_64	Image ID: img-j9m732cx Current kernel version: 12.3-RELEAS	1/20/2022	Updates the system with the latest patch.
FreeBSD 12.2x86_64	Image ID: img-pi37fg9j Current kernel version: 12.2-RELEAS	1/20/2022	Updates the system with the latest patch.
FreeBSD 11.4x86_64	Image ID: img-aif2u6pf Current kernel version: 11.4-RELEASE	10/27/2022	Updates the system with the latest patch.

Rocky Linux

Image Tag	Image Details	Update	Updates

		Date	
Rocky Linux 9.0x86_64	Image ID: img-k1g1wwy9 Current kernel version: 5.14.0-70.13.1.el9_0.x86_64	11/25/2022	Releases an image.
Rocky Linux 8.6x86_64	Image ID: img-no575grb Current kernel version: 4.18.0-372.9.1.el8.x86_64	11/25/2022	Updates the system with the latest patch.
Rocky Linux 8.5x86_64	Image ID: img-qd4bf0jb Current kernel version: 4.18.0-348.20.1.el8_5.x86_64	10/10/2022	Updates the system with the latest patch.

OpenSUSE

Image Tag	Image Details	Update Date	Updates
OpenSUSE Leap 15.4	Image ID: img-aaa4d8d1 Current kernel version: 5.14.21-150400.22-default	8/31/2022	Releases an image.
OpenSUSE Leap 15.3	Image ID: img-1e4uwwol Current kernel version: 5.3.18-59.27-default	11/2/2022	Updates the system with the latest patch.
OpenSUSE Leap 15.2	Image ID: img-i6u3kbtj Current kernel version: 5.3.18-lp152.106-default	1/7/2022	Updates the system with the latest patch.
OpenSUSE Leap 15.1	Image ID: img-4orfgj3l Current kernel version: 4.12.14-lp151.28.91-default	12/21/2021	Updates the system with the latest patch.

Windows

Image Tag	Image Details	Update Date	Updates
Windows Server 2022 IDC 64-bit Chinese	Image ID: img-9lw52tbx	1/6/2023	Updates the system with the latest patch.

Windows Server 2022 IDC 64-bit English	Image ID: img-cg67n3n9	1/6/2023	Updates the system with the latest patch.
Windows Server 2019 IDC 64-bit Chinese	Image ID: img-perxw61f	3/9/2023	Updates the system with the latest patch.
Windows Server 2019 IDC 64-bit English	Image ID: img-1dmc4wwp	3/9/2023	Updates the system with the latest patch.
Windows Server 2016 IDC 64-bit Chinese	Image ID: img-gu1nmb8d	3/9/2023	Updates the system with the latest patch.
Windows Server 2016 IDC 64-bit English	Image ID: img-6fp83vpb	3/9/2023	Updates the system with the latest patch.
Windows Server 2012 R2 IDC 64-bit Chinese	Image ID: img-ixj8o53x	1/6/2023	Updates the system with the latest patch.
Windows Server 2012 R2 IDC 64-bit English	Image ID: img-bpsjtw7n	1/6/2023	Updates the system with the latest patch.

Announcements
Temporary Solution for the Windows Blue Screen Issue Caused by CrowdStrike Security Software on July 19, 2024

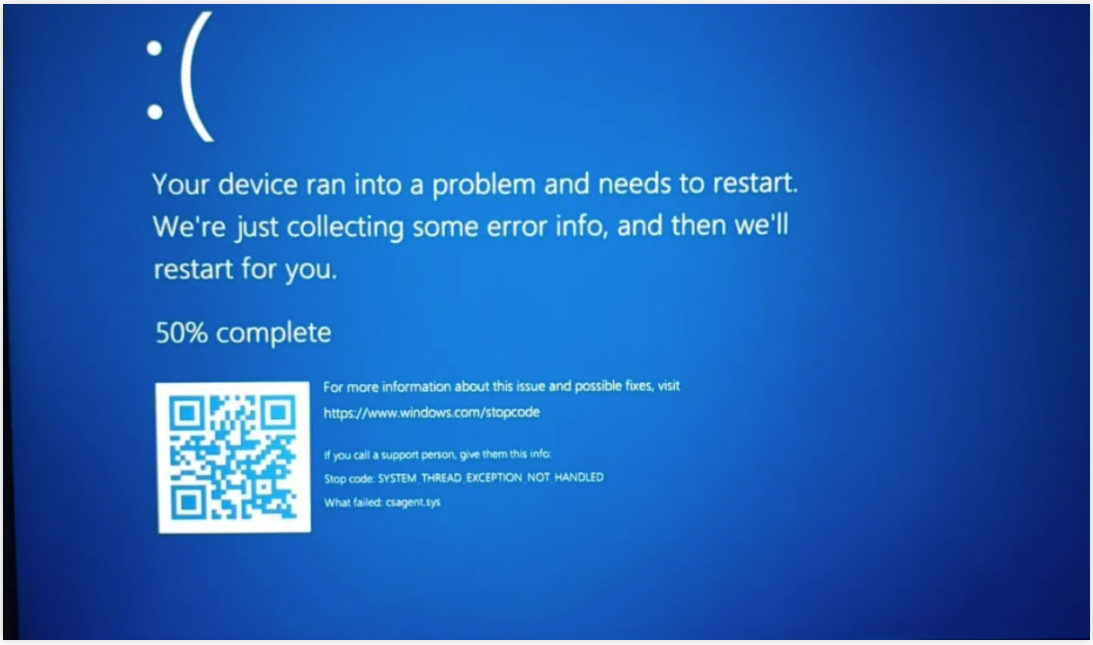
Last updated：2024-07-19 21:19:11

Background

On July 19, 2024, Beijing Time (UTC+8), Tencent Cloud monitor derected an abnormal restart issue in CVM. The community disclosed a Windows operating system blue screen issue, initially traced to an update issue with third-party security company CrowdStrike's Falcon Sensor software, causing **csagent.sys** errors in user hosts.

Note

If your host uses CrowdStrike security software, it may be affected.



Impact Range Explanation

The affected services include SharePoint Online, OneDrive for Business, Microsoft Defender, and Microsoft 365 Admin Center.

Temporary Solution

Note

Please note that this temporary solution may cause the CrowdStrike security software to become ineffective. It is recommended that you assess the risks before proceeding.

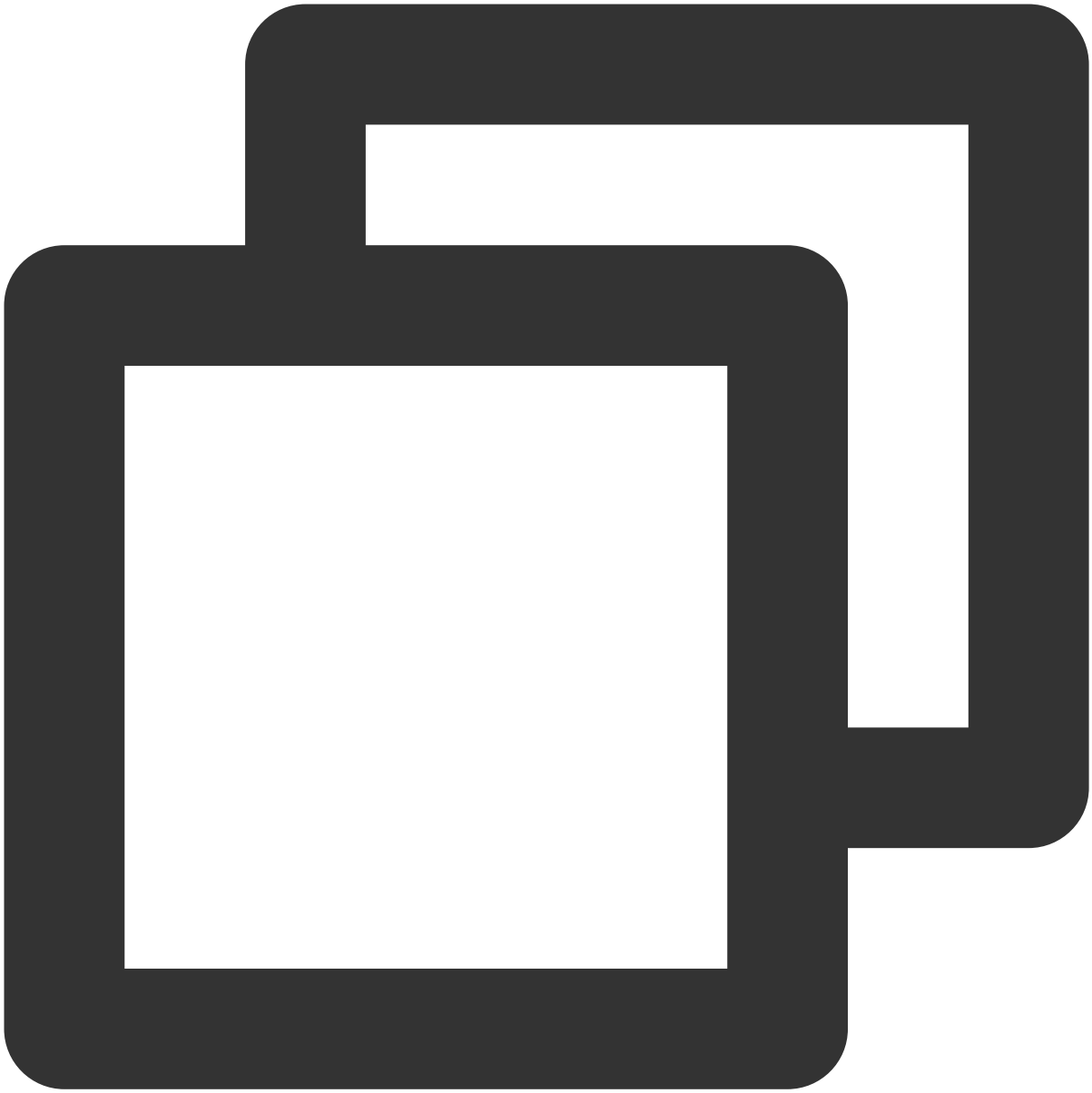
Rename or delete the CrowdStrike-related files that are causing the blue screen via WinPE or rescue mode.

If it is a Tencent Cloud machine, you can repair it via rescue mode.

1. Log in to the CVM Console, find your Windows server, and click **More > OPS and Check > Enter Rescue Mode**. For detailed guidance, see Rescue Mode.

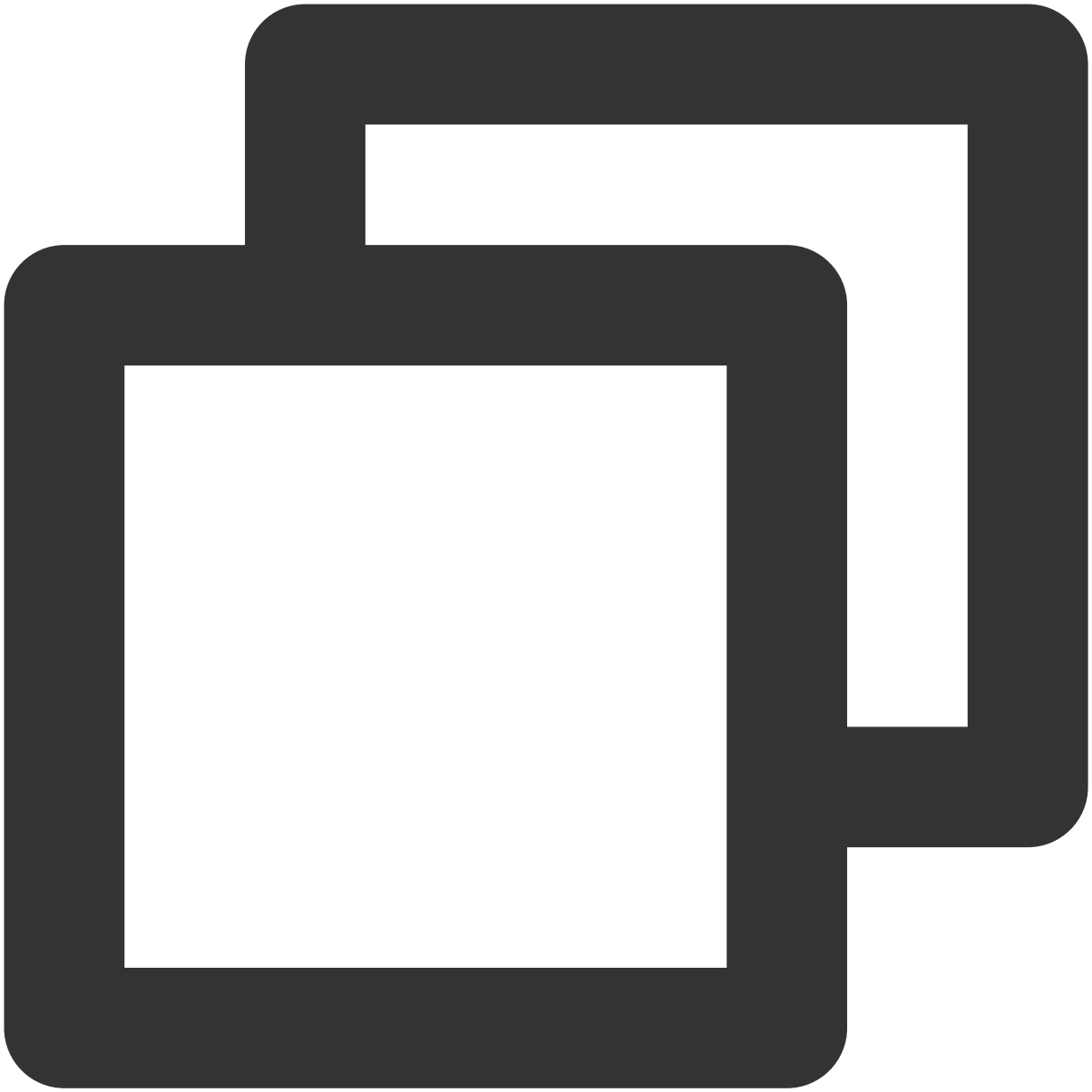
2. Rename the CrowdStrike files via resource mode.

2.1 Install the NTFS software package.



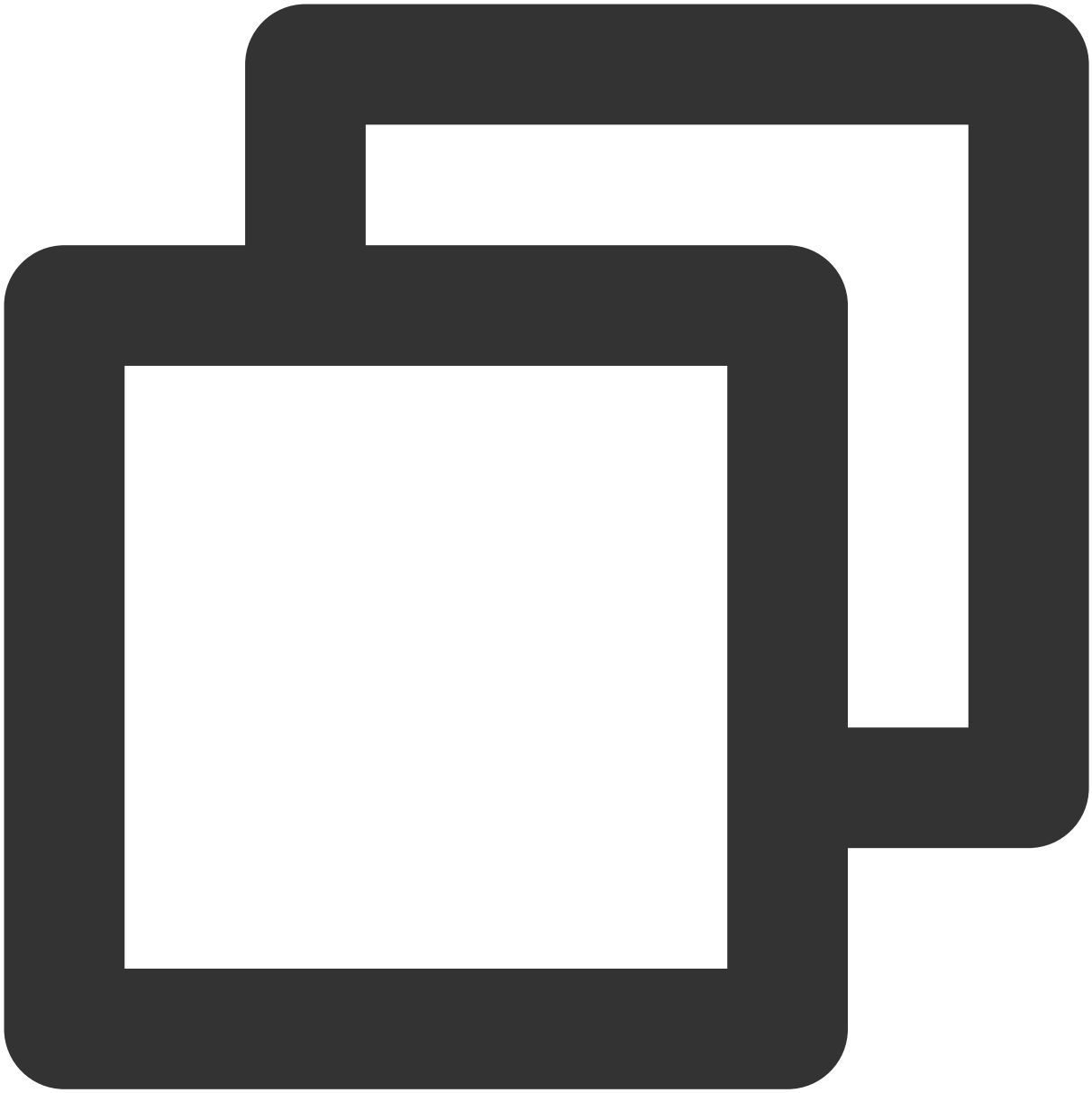
```
yum -y install ntfs*
```

2.2 For directory mounting, please confirm which partition the `c:\\windows` of the Windows file system belongs to. If unsure, you can try mounting each partition to locate the windows/system32 directory. Use the lsblk command to view the current partitions.



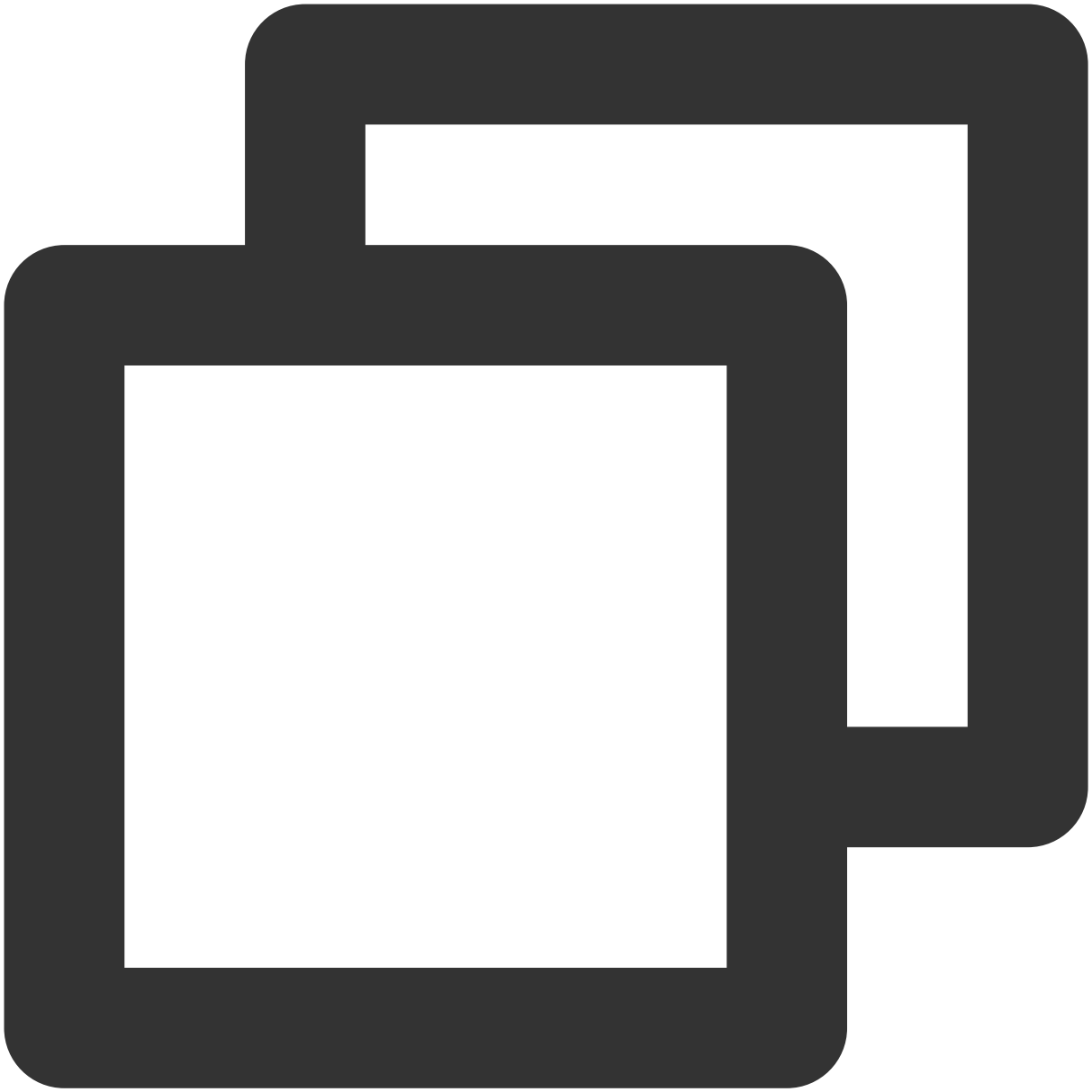
```
mount -t ntfs /dev/vda2 /mnt/
```

2.3 Navigate to the location of the target file.



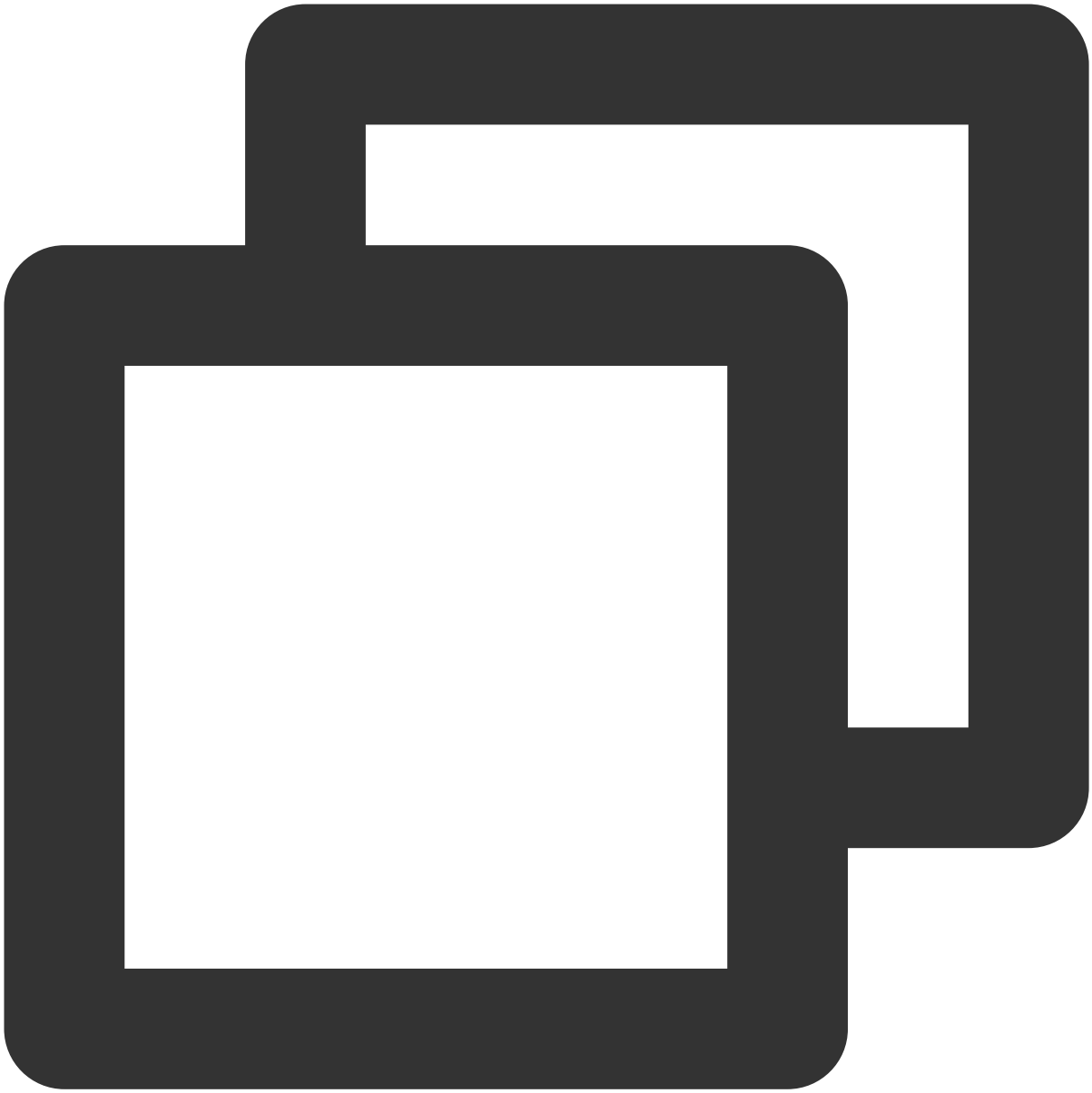
```
cd /mnt/Windows/System32/drivers/
```

2.4 Rename the CrowdStrike folder (CrowdStrike_newname as the new name defined by yourself).



```
mv CrowdStrike CrowdStrike_newname
```

2.5 After renaming, uninstall the file system to release resources.



```
umount /mnt
```

3. Exit Rescue Mode. The entry location is the same as entering rescue mode. Click **Exit** to exit the rescue mode.
4. Reboot the machine after exiting rescue mode to resume operations.

More Help

For your local Windows host and others, refer to the following handling methods:

1. Boot Windows into the security mode or the Windows recovery environment.
2. Navigate to the `C:\\WindowsSystem32\\drivers` directory.
3. Find the file that matches **Crowdstrike**, and rename or delete it.
4. Restart the host.

If you need assistance from an engineer, please consult by submitting a ticket.

Announcement on Flexible Discounts for Spot Instances in Some Regions

Last updated：2024-06-27 16:41:00

Starting from June 21, 2024, the prices of spot instances in some regions will undergo elastic changes. The new prices for spot instances after adjustment are shown in the table below:

Region	Model	Discount
Beijing	S5, S6, SA2, SA4, SA5, M5, M6, MA3, MA5	Approximately 3%-8% of pay-as-you-go prices
Shanghai	S5, S6, SA3, SA5, M5, MA3, MA5	
Guangzhou	S5, SA2, SA3, MA5	
Nanjing	SA2, SA3, MA3	
Singapore	S5, SA2, SA5	
Bangkok	S5	
Sao Paulo	S5, M5	
Seoul	C3, S5	Approximately 20% of pay-as-you-go prices
Tokyo	M5, S5, C4	
Singapore	M2, M3, M5, C4	
Silicon Valley	S5	
Frankfurt	S3, S5	

Adjustment Details

The new prices are only effective for new instance purchases; existing spot instances under the current account will still be charged at the prices before the adjustment.
Discount adjustments only apply to CPU and memory fees, excluding network and disk fees.
Note:
Spot instances have a dynamic price that fluctuates with market supply and demand. Please refer to the real-time price when placing an order.

In the future, the price of spot instances will continue to fluctuate with changes in market supply and demand, which is normal.

Purchase Method

New Instance Purchase

1. 1. Log in to the Cloud Virtual Machine purchase page.
2. 2. Select spot instance for billing mode, choose the required region, and create an instance.

Note:

For detailed purchase instructions, please refer to Purchasing Channels.

Explanatory Notes

Spot instance is a billing mode where **its price fluctuates with market supply and demand**. Its core features are discounted sales and a system interruption mechanism, meaning that instances are purchased at a discount (compared with pay-as-you-go), but the system may automatically reclaim the instances. For more information about spot instances, please refer to Spot Instance.

Spot instances have no difference in performance and stability compared with **monthly subscription** and **pay-as-you-go** instances.

Updating Some Image Pip Package Management Tools for CentOS 7

Last updated：2023-05-08 17:48:19

Overview

Some Tencent Cloud CentOS 7 public images have Python 2-pip 8.1.2 installed by default. However, this version of pip does not allow users to select compatible package versions to install. Instead, it defaults to installing the latest packages. Unfortunately, the latest versions of pip and some commonly used application tools like NumPy do not support Python 2. As a result, when running a command to upgrade pip (pip install pip --upgrade) or installing specific application tools, compatibility issues may arise. To resolve this issue, Tencent Cloud has updated pip in some public images of the CentOS 7 series.

Update Content and Scope

The table below lists the CentOS 7 public images with updated pip. By default, these public images have Python 2 installed, which comes with pip 20.3.4 instead of pip 8.1.2.

Note:

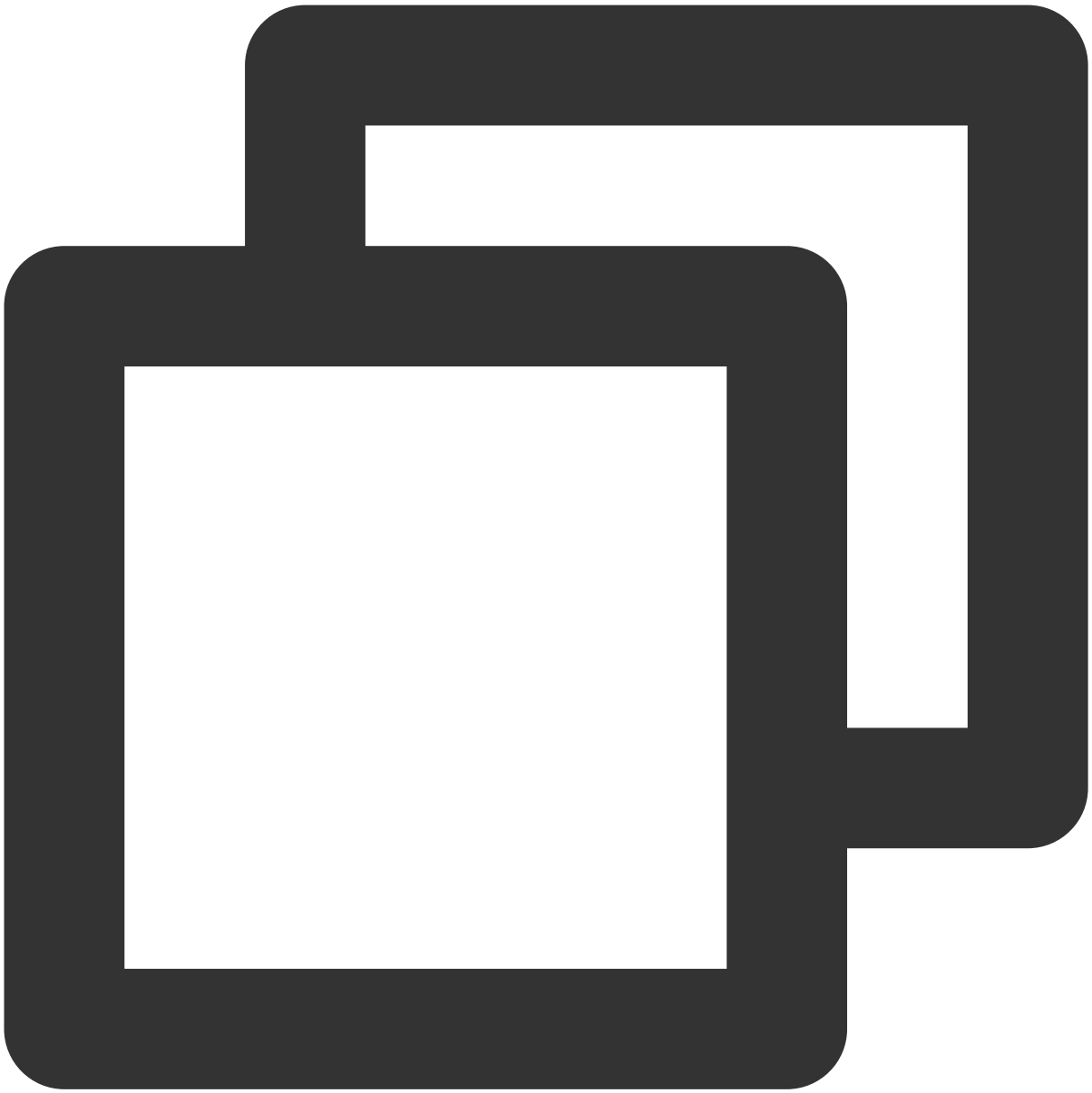
The upgrade has been performed in stages and finished on December 12, 2022. Instances purchased after the upgrade of a corresponding public image are automatically updated, while instances purchased prior to the upgrade are not. To update these instances, refer to the manual upgrade instructions.

Image Tag	Image ID
CentOS 7.9, 64-bit	img-180g963d
CentOS 7.6, 64-bit	img-9qabwvbn
CentOS 7.9, 64-bit + SG1-pv1.5	img-all2luul
CentOS 7.9, 64-bit + SG1-pv1.6	img-ojhiw86l
CentOS 7.4 (arm64)	img-k4xgkxa5

Directions

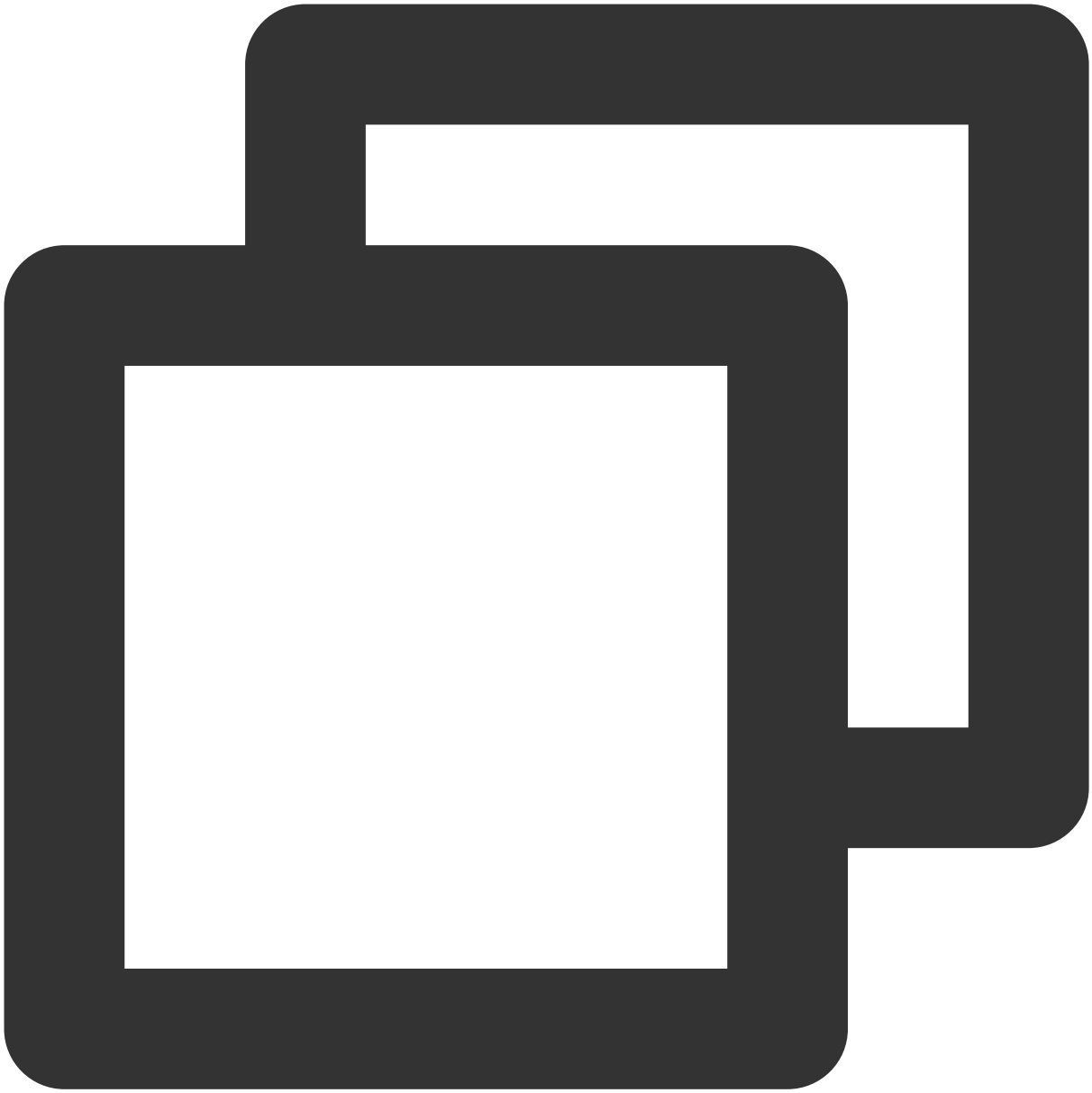
Upgrading pip

You can run the following command to view the pip version of your instance:



```
pip --version
```

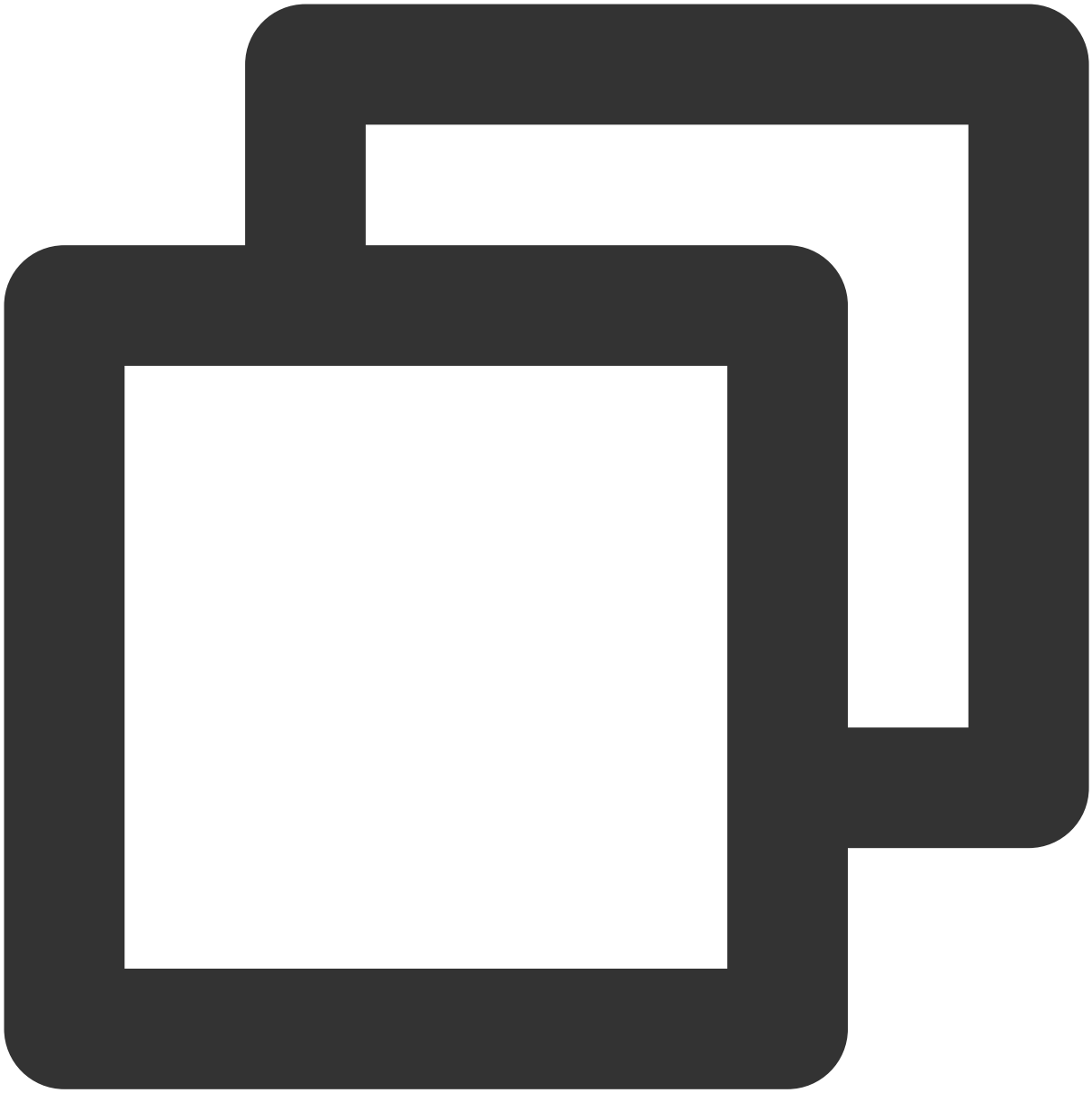
If the version of pip2 of your instance is earlier than pip 9.0, errors may occur when you upgrade pip or install application tools. To avoid this issue, you can run the following command to perform the upgrade to pip 20.3.4 first:



```
pip2 install --upgrade pip==20.3.4
```

Installing pip2

You can run the following command to install the latest version of pip2:



```
wget https://bootstrap.pypa.io/pip/2.7/get-pip.py
python2 ./get-pip.py -i http://mirrors.tencentyun.com/pypi/simple --trusted-host mi
```

If you have any questions about the product, submit a ticket.

CentOS 8 End of Maintenance

Last updated：2023-08-07 09:56:46

CentOS has officially discontinued support for CentOS 8 since January 1, 2022 (See CentOS's official announcement).

Notes

Tencent Cloud continues providing CentOS 8 images for now, but there are no more updates on CentOS 8 images and OS versions. You can migrate to the following images.
TencentOS Server: TencentOS Server benefits from the rich experience of Tencent in operating systems over the last decade. It's now used as the OS of over 99% of Tencent's internal servers.
OpenCloudOS: The basic libraries and user-mode components of OpenCloudOS are fully compatible with CentOS 8. It is optimized and enhanced at the kernel level. It has been used on more than 10 million nodes. The result shows that its stability is 70% better than CentOS 8 and the performance is improved by 50% in specific scenarios.
CentOS Stream and other released versions such as Ubuntu
For more information, see Migrating CentOS to TencentOS Server.

Discontinuation of Support for SUSE Commercial Images

Last updated：2024-01-08 09:44:07

Tencent Cloud has discontinued support for the following versions of SUSE commercial public images and corresponding authentication services since January 1, 2022:
SUSE Linux Enterprise Server 12 SP3
SUSE Linux Enterprise Server 12
SUSE Linux Enterprise Server 10
If you want to continue using these SUSE public images, contact SUSE customer representatives via the following for technical support:
Phone: +86-10-6533-9000
Email: sales-inquiries-apac@suse.com

Price Reduction in Selected Availability Zones

Last updated：2022-12-14 09:44:51

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** 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

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.

OrcaTerm Proxy IP Addresses Updates

Last updated：2023-07-07 15:34:18

Background

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

Note:

For more information about orcaterm 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 orcaterm 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

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

Last updated：2022-04-06 18:34:54

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：2022-04-06 18:34:54

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.

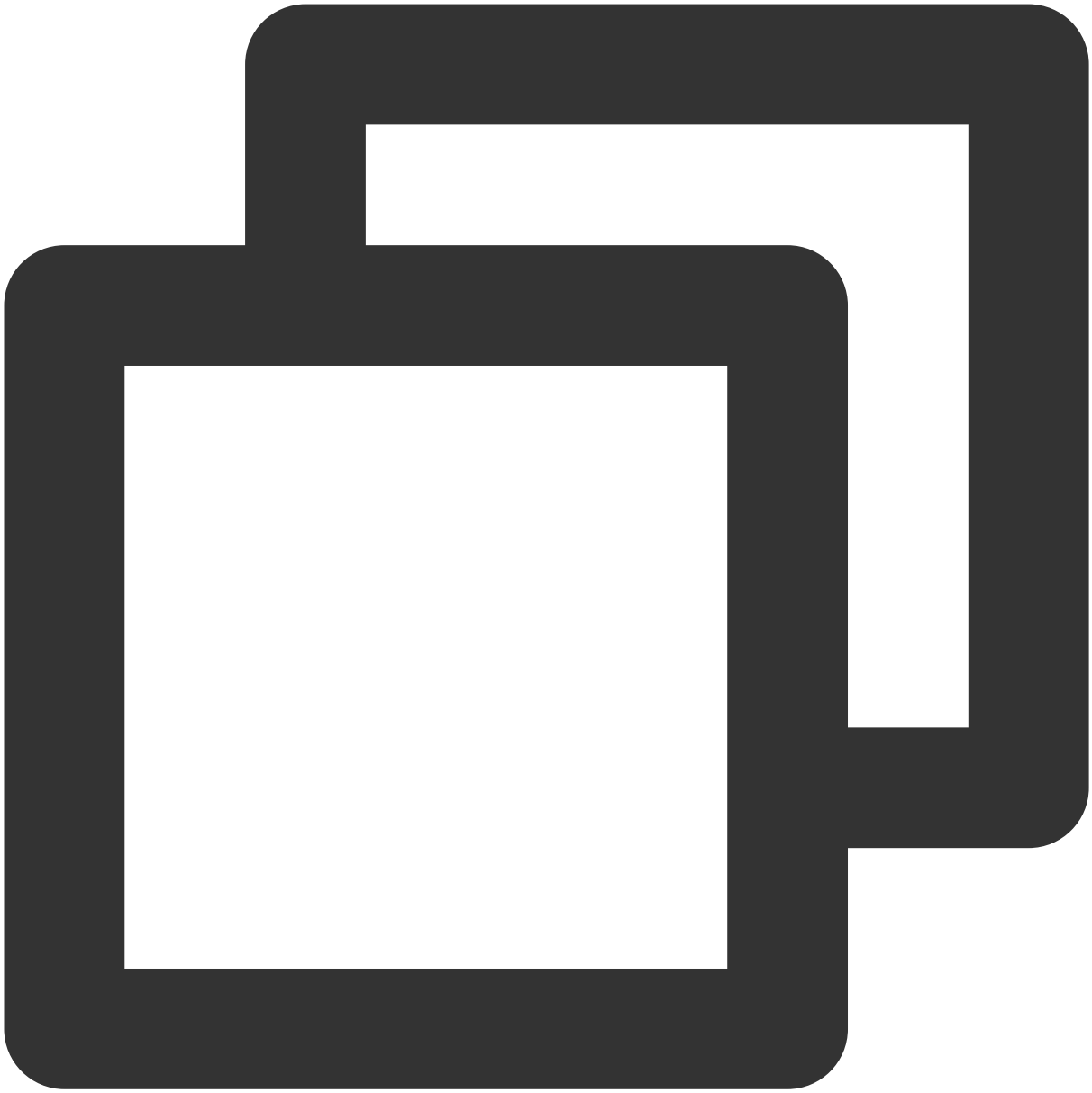
Stopping supporting for Ubuntu 10.04 images

Last updated：2022-04-06 18:34:54

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

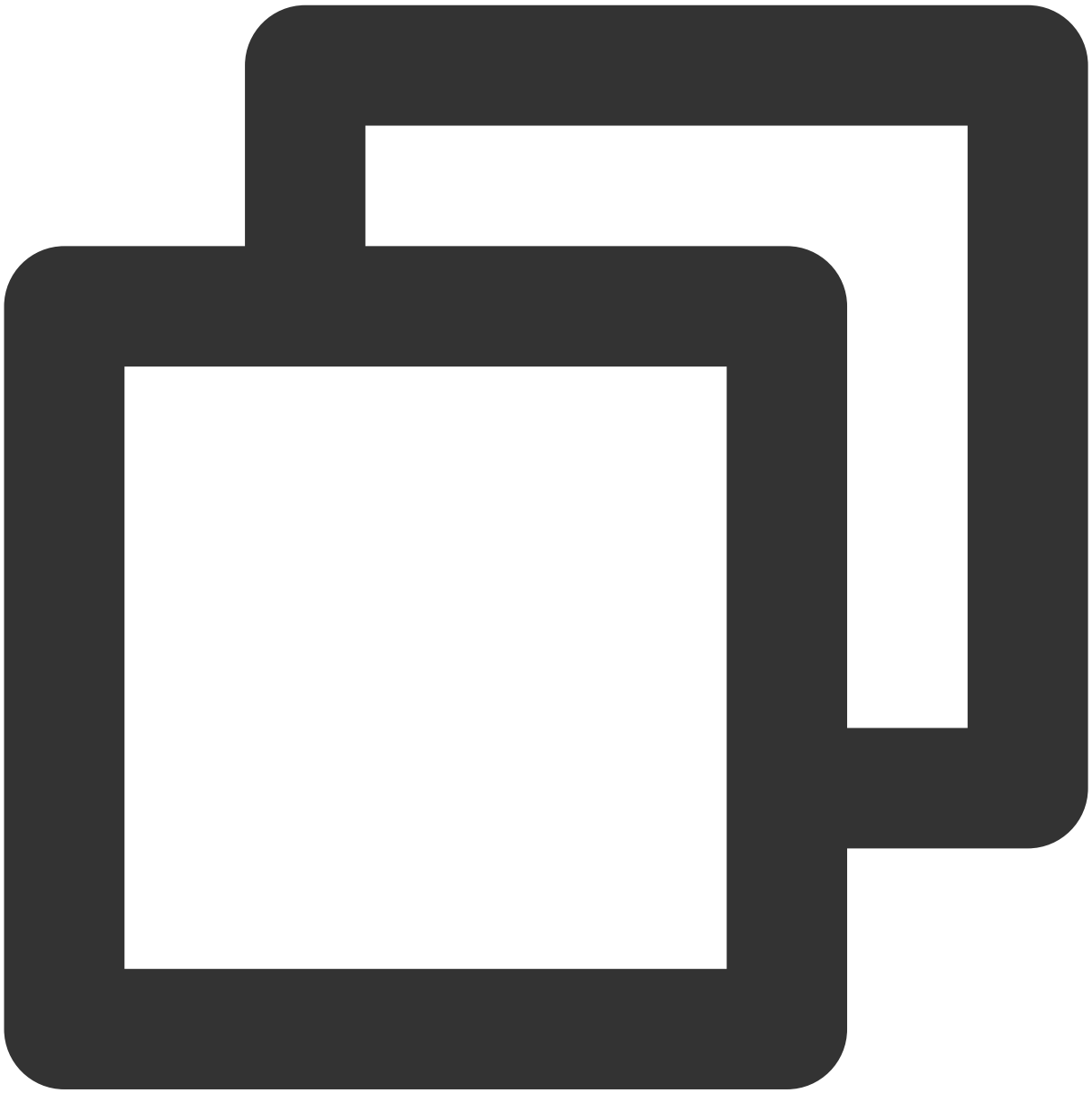
To improve the user experience, the Tencent Cloud software repository pulls the official archive source `http://old-releases.ubuntu.com/ubuntu/` of Ubuntu 10.04 LTS (http://old-releases.ubuntu.com/ubuntu/) for users. Users can use the repository as usual by manually modifying the configuration file:
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 uni
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-updates main restri
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-security main restr
deb-src http://mirrors.tencentyun.com/old-archives/ubuntu lucid-backports main rest
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid main restricted univers
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-updates main restricted
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-security main restricte
deb http://mirrors.tencentyun.com/old-archives/ubuntu lucid-backports main restrict
```

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
```

Solution to Tomcat Start Failure on Ubuntu14.04

Last updated：2022-04-06 18:34:54

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.

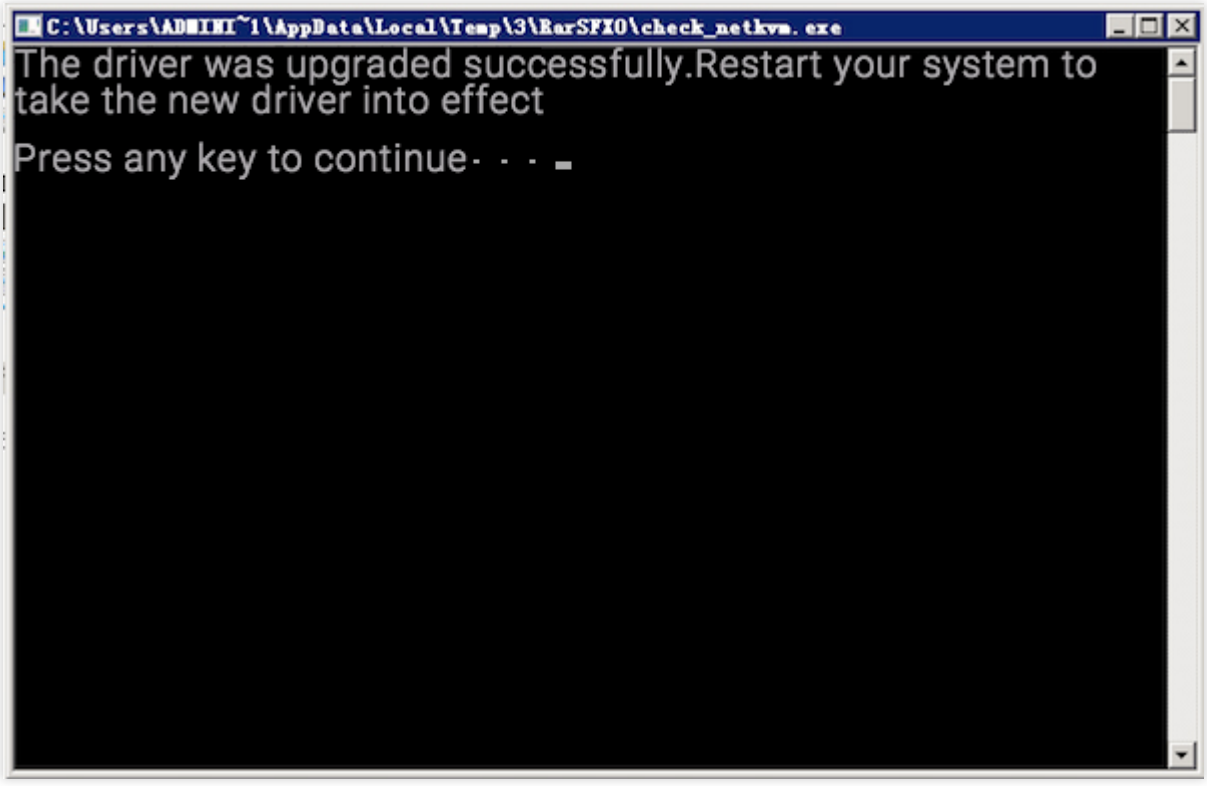
Upgrading Virtio network card drive for Windows CVMs

Last updated：2024-01-08 09:47:10

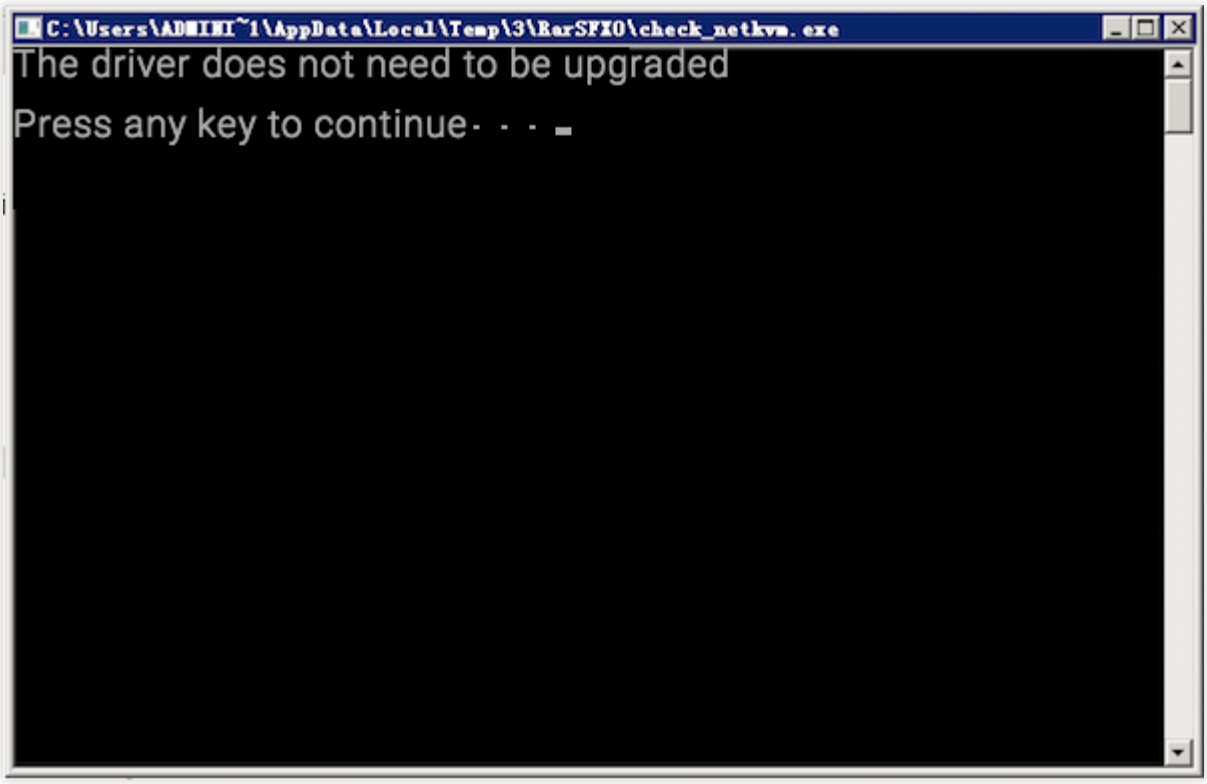
To prevent the extreme case where Windows CVMs created between June and August of 2016 become offline and affect your business operation, we provide an upgrade program for the Virtio network driver. We strongly recommend you follow the instructions below to install the upgrade program. You can then solve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



About Configuration of Security Group Port 53

Last updated：2022-04-06 18:34:54

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.

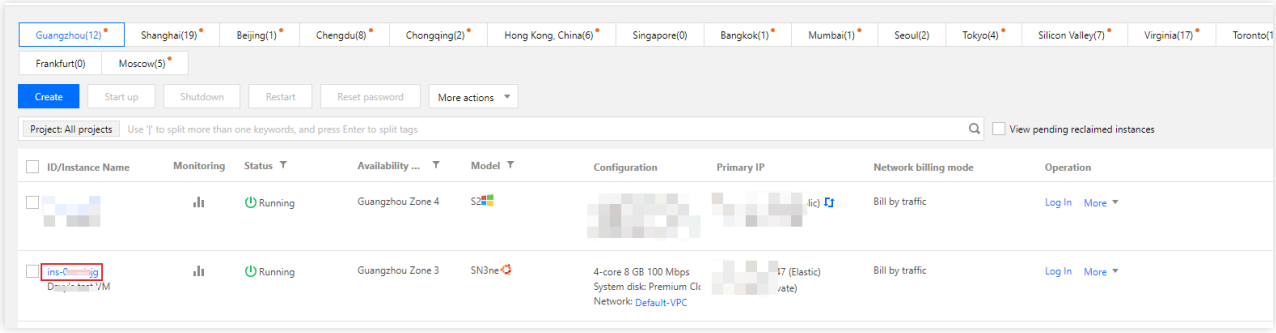
Related policies and regulations

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

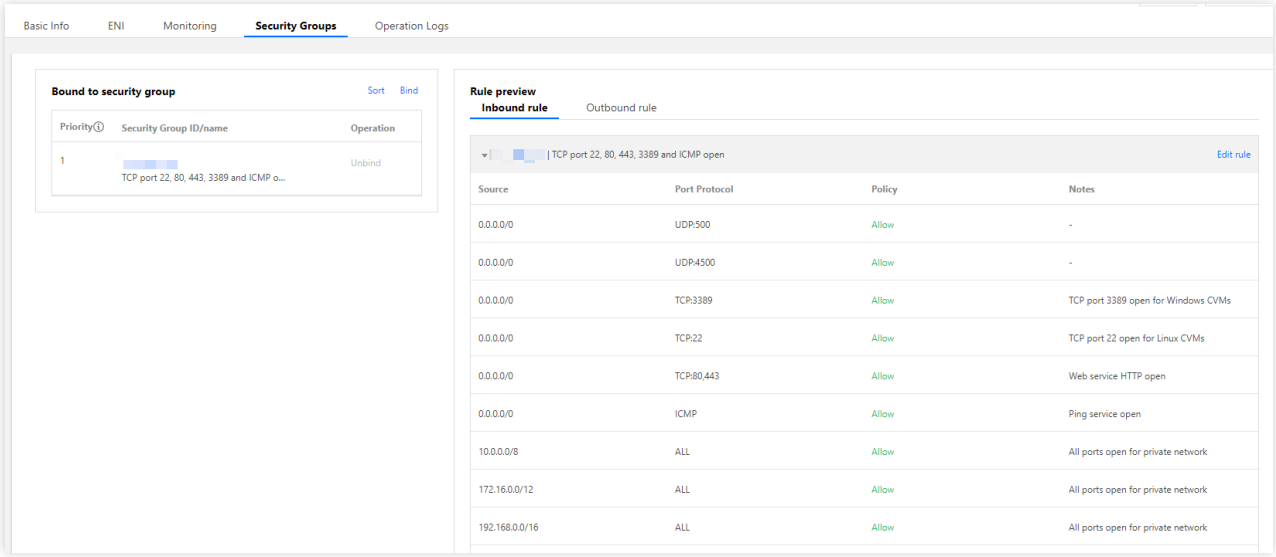
not obtained business licenses or ICP filings for non-commercial Internet information services in Mainland China in accordance with the law is not permitted.
If you or your company does not engage in **Internet domain name resolution services**, we recommended you adjust the security group policy of 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:

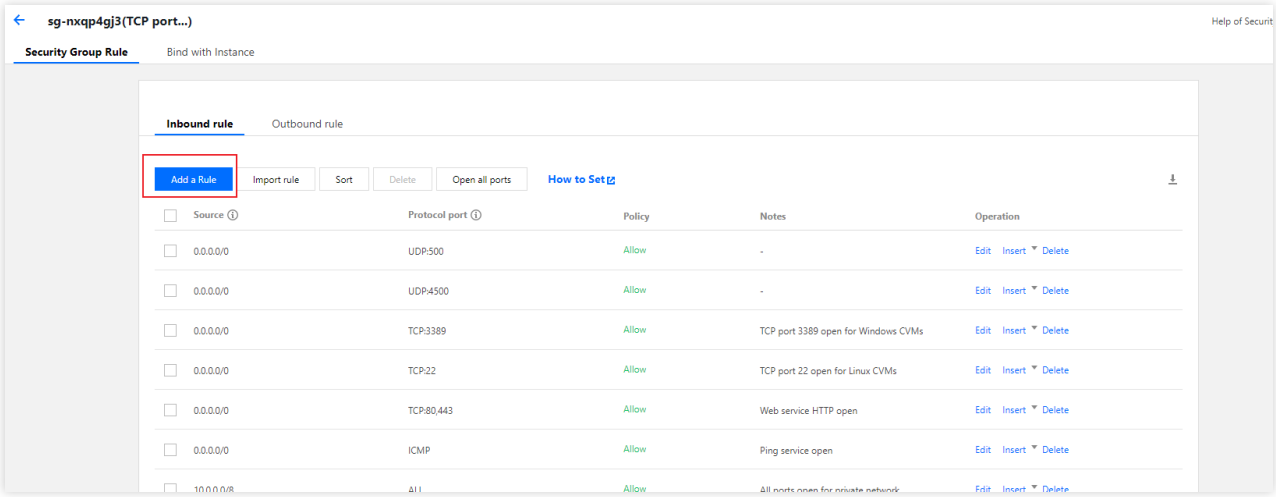


3. In the instance details page, select the **Security Groups** tab, to enter the security group management page for this instance. This is shown in the following figure:

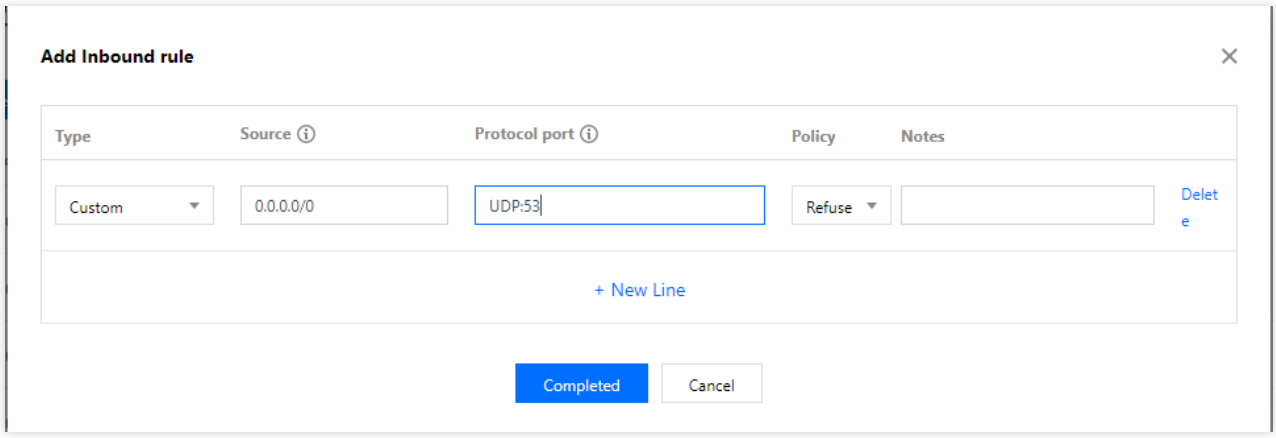


4. In the **Bound to security group** field, select the **Security Group ID/Name** of the inbound rule that is to be modified.

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.

Windows Server 2003 System Images End of Support Announcement

Last updated：2022-04-06 18:34:54

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.

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

Last updated：2023-02-23 17:07:32

Notes

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 Cloud 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.
To ensure the security and stability of your business, we recommend that you migrate your Windows Server 2008 R2 Enterprise Edition CVM instances to the latest version of Windows Server.
If you do want to create or reinstall an instance by using Windows Server 2008 R2 Enterprise Edition, try importing a custom image.

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 Cloud 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. The following situations are not related to Tencent Cloud's service quality or responsibility:

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 Tencent Cloud CVMs may not be able to support the running of Windows Server 2008 images.