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

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud’s products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.
Contents

OPS Guide
Mount Data Disks
  Format and Mount Data Disks
  Initializing Data Disks (Windows CVM)
  Reading EXT data disks after reinstallation from Linux to Windows
  Read/write NTFS Data Disks after Reinstalling a Windows CVM to Linux CVM
Environment Configurations
  Modifying etc/hosts Configuration of Linux Instance
  Linux Power Management Configuration
Upload File
  Copying Local Files to CVMs
  Uploading Files from MacOS to Windows CVM using MRD
  Uploading Files from Linux to Windows CVM using RDP
  Uploading Files from Linux to a CVM Using FTP
  Uploading files via WinSCP to a Linux CVM from Windows
  Uploading Files from Windows to a CVM Using FTP
  Uploading Files via SCP to a Linux CVM from Linux
  Uploading Files from Windows to a Windows CVM using MSTSC
Installing Software
  Accelerating software package download and update with Tencent Cloud software source
  Install Software via Apt-get under Ubuntu Environment
  Install Software via YUM under CentOS Environment
  Install Software via zypper under SUSE Environment
User Data
  Configuring Custom Data (Linux CVM)
  Configuring Custom Data (Windows CVM)
System-related
  System Activation
  System Updates
  Closean CVM
  Configuring High-performance Power Management
  Windows Recovery Mode
  Ensure Unique SIDs for CVMs using Sysprep
  Modifying VNC Resolution
  Update the Virtio ENI driver
Modifying SID

Others
  Common Operations and Commands
  Setup Windows CVM For Multi-user Remote Login
  Configure Linux CVM to Boot into Single User Mode
  Modifying the Default Remote Port of CVM
  Allow CVMs without Internet access to access Internet
OPS Guide

Mount Data Disks

Format and Mount Data Disks

Last updated: 2020-05-09 17:04:06

Operation Scenario

This document describes how to format, partition, and create file systems on the data disk of a Linux CVM.

Notes

- Before formatting, make sure the data disk has no data or important data has been backed up. After formatting, all data in the data disk will be cleared.
- To avoid service exceptions, ensure before formatting that the CVM has stopped external services.

Directions

Please select the appropriate operation guide based on the disk capacity:

- If the disk capacity is less than 2TB, see Initializing cloud disks (Linux).
- If the disk capacity is greater than or equal to 2TB, see Initializing cloud disks (Windows).
Initializing Data Disks (Windows CVM)

Last updated: 2020-04-01 11:11:57

Scenario

After purchasing or reinstalling CVM, you need to partition and format the data disk. This document describes how to perform partitioning, formatting, and other initialization operations on a data disk on Windows CVM.

Notes

- Formatting a data disk will erase all data. Please ensure that the data disk does not contain data, or important data has been backed up.
- To avoid service exceptions, ensure before formatting that the CVM has stopped external services.

Directions

Please select the appropriate operation guide based on disk capacity:

- If the disk capacity is less than 2 TB, please initializing cloud disks.
- If the disk capacity is greater than or equal to 2 TB, please initializing cloud disks.
Reading EXT data disks after reinstallation from Linux to Windows

Last updated: 2020-04-27 16:39:07

Scenario

Windows employs two major file systems, NTFS or FAT32, while EXT is the de facto file system for Linux. When an operating system is changed from Linux to Windows after reinstallation, the data disk remains in its original format. Therefore, the system might not be able to access data disk's file system. In these cases, you will need to use a format converter to read the data disk.

This document describes how to read a data disk when the operating system has been reinstalled (https://intl.cloud.tencent.com/document/product/213/4933) from Linux to Windows.

Prerequisites

- DiskInternals Linux Reader has been installed on the reinstalled Windows CVM.
  Download DiskInternals Linux Reader: [http://www.diskinternals.com/download/Linux_Reader.exe](http://www.diskinternals.com/download/Linux_Reader.exe)
- Suppose the data disk mounted to the Linux CVM before reinstallation has two partitions, vdb1 and vdb2, as shown below:

```
Disk /dev/vdb: 21.5 GB, 21474836480 bytes
16 heads, 63 sectors/track, 41610 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x29cc8ca2

Device Boot Start   End     Blocks   Id  System
/dev/vdb1   2000 41610    19963944  83  Linux
/dev/vdb2     1    1999   1007464+  83  Linux
```

Directions

Mounting a data disk
If a data disk has been mounted, skip this step.

1. Log in to the Tencent Cloud CVM Console.
2. Click Cloud Block Storage from the left sidebar to enter the Cloud Block Storage management page.
3. Locate the instance with the reinstalled system, and click More > Mount on the right as shown below:

![Cloud Block Storage Management Page]

4. In the pop-up window, select the reinstalled Windows CVM and click Submit.

**Viewing data disk information**

1. Run DiskInternals Linux Reader to view the information of newly mounted data disk. `/root/mnt` and `/root/mnt1` correspond to vdb1 and vdb2 respectively, which are the 2 data disk partitions on the Linux CVM before reinstallation as shown below:

   ![Data Disk Information]

   Note that the Linux data disk is read-only at this time. To perform read and write operations on the data disk as you do on a Windows data disk, back up your needed files and re-format the disk into a standard Windows-supported file system. For more information, please see Data Disk Partition and Formatting of Windows CVMs.

2. Double-click to enter `/root/mnt` directory, right-click the file you want to copy, and select Save as shown below:
Read/write NTFS Data Disks after Reinstalling a Windows CVM to Linux CVM

Scenario

The Windows file system typically uses the NTFS or FAT32 format, whereas the Linux file system often uses EXT-series formats. When the operating system of a CVM is changed from Windows to Linux, the data disk of the CVM remains in the same format as that of the original operating system. As a result, after the reinstallation of the system, the CVM might be unable to access the file system of the data disk. This document describes how to read a data disk in the original Windows system after the operating system is reinstalled from Windows to Linux.

Directions

**Enabling a Linux system to support NTFS**

1. Log in to the Linux CVM after reinstallation.
2. Run the following command to install the ntfsprogs software program to enable the Linux CVM to support access to the NTFS file system.

   ```
   yum install ntfsprogs
   ```

   This document uses CentOS as an example. Note that different types of Linux systems require different installation commands. Therefore, always run the corresponding installation command for your operating system type.

**Mounting a data disk from the Windows CVM to the Linux CVM**

If the data disk in your Windows CVM has been mounted to the Linux CVM, skip this operation.
1. Log in to the CVM console.

2. In the left sidebar, click **Cloud Block Storage** to go to the Cloud Block Storage management page.

3. Select the Windows data disk to be mounted and choose **More > Mount**.

4. In the "Mount to CVM" window that appears, select the target Linux CVM and click **OK**.

5. Log in to the Linux CVM to which the Windows data disk has been mounted.

6. Run the following command to query the mounted data disk from the Windows CVM.

   ```
   parted -l
   ```

   Information similar to the following will be returned:

   ```
   Model: Virtio Block Device (virtblk)
   Disk /dev/vdb: 53.7GB
   Sector size (logical/physical): 512B/512B
   Partition Table: gpt
   Disk Flags:
   Number Start End Size File system Name Flags
   1 17.4kB 134MB 134MB Microsoft reserved partition msftres
   2 135MB 53.7GB 53.6GB ntfs Basic data partition
   ```

7. Run the following command to mount the data disk.

   ```
   mount -t ntfs-3g data disk path mount target
   ```

   For example, to mount the data disk in `/dev/vdb1` to `/mnt`, run the following command:

   ```
   mount -t ntfs-3g /dev/vdb1 /mnt
   ```

   As the file system can be recognized by the operating system, the Linux system can directly read data from and write data to the mounted data disk.
Environment Configurations
Modifying etc/hosts Configuration of Linux Instance

Last updated: 2020-02-12 09:38:55

Scenario

From March 1, 2018, the Linux public image provided by Tencent Cloud has the open-source tool Cloud-Init pre-installed, and all initialization operations on an instance will be done via Cloud-Init, making the internal operations of the instance more transparent. For more information, see Cloud-Init.

In each launch, Cloud-Init generates a new /etc/hosts file according to the /etc/cloud/templates/hosts.${os_type}.tmpl template and overwrites the original /etc/hosts file of an instance. Hence, after the user manually modifies the internal /etc/hosts configuration of the instance and restarts it, the /etc/hosts configuration goes back to the original default configuration.

Prerequisites

Tencent Cloud has fixed this problem for instances created after September 2018, and the /etc/hosts configuration will not be overwritten.

For instance created before September 2018, follow the steps below for modification.

Steps

Solution 1

1. Log into the Linux CVM.
2. Execute the following command to change the - update_etc_hosts in the /etc/cloud/cloud.cfg configuration file to - ['update-etc-hosts', 'once-per-instance'].

```
sed -i "/update_etc_hosts/c \ - ['update-etc-hosts', 'once-per-instance']" /etc/cloud/cloud.cfg
```
3. Execute the following command to create a `config_update_etc_hosts` file under the `/var/lib/cloud/instance/sem/` path.

```
  touch /var/lib/cloud/instance/sem/config_update_etc_hosts
```

## Solution 2

This solution takes the CentOS 7.2 operating system as an example.

### Obtaining hosts Template File Path

1. Log into the Linux CVM.
2. Execute the following command to view the system `hosts` template file.

```
  cat /etc/hosts
```

The `hosts` template file is as shown in the following figure:

```
[root@UM2_9_centos ~]# cat /etc/hosts
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.redhat.tmpl
# b.) change or remove the value of 'manage_etc_hosts' in
#     /etc/cloud/cloud.cfg or cloud-config from user-data
#
# The following lines are desirable for IPv4 capable hosts
127.0.0.1 VM_2_9_centos VM_2_9_centos
127.0.0.1 localhost.localdomain localhost
127.0.0.1 localhost4.localdomain4 localhost4

# The following lines are desirable for IPv6 capable hosts
::1 VM_2_9_centos VM_2_9_centos
::1 localhost.localdomain localhost
::1 localhost6.localdomain6 localhost6
[root@UM2_9_centos ~]#
```

### Modifying the hosts Template File

Taking adding `127.0.0.1 test test` as an example, you can modify the `hosts` template and `/etc/hosts` file as needed.

1. Execute the following command to modify the `hosts` template file.
vim /etc/cloud/templates/hosts.redhat.tmpl

2. Press i or Insert to switch to editing mode.
3. Add the following content to the end of the file.

```
127.0.0.1 test test
```
4. Press Esc, enter :wq, save the file and return.

**Modifying the /etc/hosts File**

1. Execute the following command to modify the /etc/hosts file.

```
vim /etc/hosts
```
2. Press i or Insert to switch to editing mode.
3. Add the following content to the end of the file.

```
127.0.0.1 test test
```
4. Press Esc, enter :wq, save the file and return.
Linux Power Management Configuration

Introduction

x86 machines use two power management methods, **APM** (Advanced Power Management) and **ACPI** (Advanced Configuration and Power Interface). ACPI is a power management standard jointly developed by Intel, Microsoft, and Toshiba, which provides a more flexible interface for computer and device management, whereas APM is the old power management standard.

Linux supports APM and ACPI, but the two standards cannot run simultaneously. Linux runs ACPI by default. Tencent Cloud also recommends ACPI.

If ACPI is not installed in a Linux system, the soft shutdown will fail. This document describes how to check whether ACPI has been installed and if not, how to install it.

Notes

For CoreOS, there is no need to install ACPI.

Directions

1. Execute the following command to see if ACPI has been installed.

   ```
   ps -ef|grep -w "acpid"|grep -v "grep"
   ```

   - If there is no process running, it means ACPI has not been installed. Please go to the next step.
   - If there is a process running, it means ACPI has been installed.

2. Execute the following command to install ACPI.

   - For Ubuntu or Debian:
     ```
     sudo apt-get install acpid
     ```
   - For Redhat or CentOS:
     ```
     yum install acpid
     ```
   - For SUSE:
     ```
     in acpid
     ```
Upload File

Copying Local Files to CVMs

Last updated: 2020-03-06 12:15:34

CVMs are widely used for storing user's local files. This article describes how to copy your files to a CVM.

Find the operating system of your local machine below and refer to the instructions.

<table>
<thead>
<tr>
<th>Local OS</th>
<th>Linux CVM</th>
<th>Windows CVM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Use WinSCP</td>
<td>Use MSTSC</td>
</tr>
<tr>
<td></td>
<td>Use FTP</td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td>Use SCP</td>
<td>Use RDP</td>
</tr>
<tr>
<td>Mac OS</td>
<td></td>
<td>Use MRD</td>
</tr>
</tbody>
</table>

For example, if you use Windows on your local machine and you have a Linux CVM, you can use WinSCP to upload files.

See Also

For important data, you can make a snapshot for backup and disaster recovery purposes. Refer to this article for information on Snapshots.

Having Problems?

Please submit a ticket or use related documentation to troubleshoot.

Common Issues

- I forgot my CVM login password.
  Refer to Resetting Instance Password.
- I can’t log in to the CVM.
  Refer to Windows Instance Login Failures or Linux Instance Login Failures.
Uploading Files from MacOS to Windows CVM using MRD

Scenario

Microsoft Remote Desktop (MRD) is a remote desktop software by Microsoft. This article describes how to use it on MacOS to upload files to a CVM with Windows Server 2012 R2 installed.

Prerequisites

- Download and install Microsoft Remote Desktop for Mac.
- MRD supports MacOS 10.10 and above. Make sure you have a compatible OS.
- Purchased a Windows CVM.

Directions

Obtaining a CVM Public IP

Log in to CVM Console and note down the public IP address of your CVM instance on the instance list page, as shown in the following image:

Uploading Files
1. Start MRD and click **Add Desktop**, as shown in the following image:

![Microsoft Remote Desktop](image)

Add your first desktop connection to get started.

Add Desktop

2. The **Add Desktop** window appears. Follow the steps illustrated in the following image to select a folder to upload and establish a connection with your Windows CVM:
i. In the **PC name** text field, input your CVM’s public IP.

ii. Click **Folders** to switch to the folder list view.

iii. Click +. In the pop-up window, select the folder to be uploaded.

iv. After you finish, check your list of folders to upload and click **Add**.

v. Leave other options as default and complete the process.

Your entry is saved, as shown in the following image:
3. Double click the newly added entry. Input your username and password for CVM and click **Continue**.

- The default account for the Windows CVM is **Administrator**.
- If you choose to log in with random password, please check it in the **Message Center**.
- If you have forgotten your password, please reset the instance password.

4. Click **Continue** to establish the connection, as shown in the following image:
If the connection is successful, then the following page appears:

5. In the bottom-left corner, click then My Computer to see a list of shared folders.

6. Double click a shared folder to open it. Copy desired local files to another drive on the Windows CVM to complete upload.
   For example, copy a.txt to the C drive on Windows CVM.

**Downloading Files**

To download files from the Windows CVM to your computer, copy desired files from the CVM to a shared folder.
Uploading Files from Linux to Windows CVM using RDP

Last updated: 2020-03-06 12:13:47

Introduction

rdesktop is an open source RDP client. This article describes how to use it to connect to a CVM running Windows Server 2012 R2 to upload files.

Prerequisites

Purchased a Windows CVM instance.

Instructions

Obtaining CVM Public IP

Log in to CVM Console and find the public IP address of your Windows CVM, as shown in the following image:

### Installing rdesktop.

1. Open a terminal window and run the following command to download rdesktop 1.8.3:

   ```bash
   wget https://github.com/rdesktop/rdesktop/releases/download/v1.8.3/rdesktop-1.8.3.tar.gz
   ```

   If you want to install a new version, visit the rdesktop home on GitHub to find it. Then replace the path in the command with the new one.

2. Run the following commands to decompress the install package and navigate to its directory.

   ```bash
   tar xvzf rdesktop-1.8.3.tar.gz
   cd rdesktop-1.8.3
   ```
3. Run the following commands to compile and install rdesktop.

```bash
./configure
make
make install
```

4. After installation finishes, run the following command to check if rdesktop is successfully installed:

```bash
rdesktop
```

### Uploading Files

1. Run the following command to specify the shared folder:

```bash
rdesktop cvm_ip -u cvm_username -p cvm_password -r disk:shared_folder_path=local_folder_path
```

- The default username for the CVM is **Administrator**.
- If you choose to log in with a random password, please check it in **Message Center**.
- If you forgot your password, please **reset the instance password**.

For example, execute the following command to share the `/home` folder on your local Linux machine to the specified CVM, and rename it as **share**.

```bash
rdesktop 118.xx.248.xxx -u Administrator -p 12345678 -r disk:share=/home
```

If the operation is successful, the Windows Desktop appears.

Click then **My Computer** to see shared folders.

2. Double click the shared folder to open it. Copy a file in the shared folder to a directory on the Windows CVM disk to upload it.

For example, copy **a.txt** in **share** to the C drive of Windows CVM.

### Downloading files

To download files from a Windows CVM to your Linux computer, copy desired files from the CVM to the shared folder.
Uploading Files from Linux to a CVM Using FTP

Overview

This document describes how to use the FTP service to upload files from a local Linux computer to a CVM.

Prerequisites

You have built the FTP service on CVM.

- To use FTP to upload files to a Linux CVM, see Building the FTP Service (Linux)
- To use FTP to upload files to a Windows CVM, see Building the FTP Service (Windows)

Directions

Connecting to the CVM

1. Run the following command to install the FTP service.

   If the FTP service has already been installed on the local Linux computer, skip this step.

   ```sh
   yum -y install ftp
   ```

2. Run the following command to connect to the CVM and enter the FTP service username and password as prompted.

   ```sh
   ftp <CVM IP address>
   ```
If the following interface appears, the connection has been established successfully.

```
[rroot@VM_0_118_centos ~]# ftp 1.2.3.456
Connected to 1.2.3.456 (1.2.3.456).
220 Microsoft FTP Service
Name (1.2.3.456:root): ftpuser
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

**Uploading a file**

Run the following command to upload a local file to the CVM.

```
put local-file [remote-file]
```

For example, to upload the local `/home/1.txt` file to the CVM, run the following command.

```
put /home/1.txt 1.txt
```

**Downloading a file**

Run the following command to download a file from the CVM to a local directory.

```
get [remote-file] [local-file]
```

For example, to download the `A.txt` file from the CVM to the local `/home` directory, run the following command.

```
get A.txt /home/A.txt
```
Uploading files via WinSCP to a Linux CVM from Windows

Last updated: 2020-04-01 11:11:57

Scenario

WinSCP is an open-source graphical SFTP client that uses SSH in Windows environment and supports SCP protocol. Its main feature is to copy files securely between the local and remote computers. Compared with uploading codes via FTP, you can directly use your CVM account in WinSCP to access the CVM without any additional configuration.

Prerequisites

WinSCP has been downloaded and installed on the local computer (we recommend you download the latest version of WinSCP from the Official Website.)

Directions

Logging in to WinSCP

1. Open WinSCP, and the “WinSCP Login” box pops up.
2. Configure the following parameters:
   - Protocol: either SFTP or SCP.
   - Host Name: Public IP of the CVM. Log in to CVM Console to view the Public IP of the CVM.
   - Port: 22 by default
   - Password: Password corresponding to CVM username.
   - Username: System username for CVM.
     - SUSE/CentOS/Debian: root
     - Ubuntu: ubuntu
3. Click Login to enter the “WinSCP” file transfer interface.

Uploading a file

1. In the right pane of the “WinSCP” file transfer interface, select the directory where the files are to be stored on the server, such as "/user".
2. In the left pane of the "WinSCP" file transfer interface, select the directory where the files are stored on the local computer, such as "F:\SSL certificate\Nginx", and then select the files to be transferred.

3. In the menu bar of the "WinSCP" file transfer interface, click **Upload**.

4. In the "Upload" box that pops up, confirm the files to be uploaded and the remote directories, and click **OK** to upload the files from the local computer to CVM.

### Downloading a file

1. In the left pane of the “WinSCP” file transfer interface, select the directory where the files are to be stored on the local computer, such as "F:\SSL certificate \Nginx".

2. In the right pane of the "WinSCP" file transfer interface, select the directory where the files are stored on the server, such as "/user", and then select the file to be transferred.

3. In the menu bar of the "WinSCP" file transfer interface, click **Download**.

4. In the "Download" box that pops up, confirm the files to be downloaded and the remote directories, and click **OK** to download the files from the CVM to the local computer.
Uploading Files from Windows to a CVM

Using FTP

Overview

This document describes how to use the FTP service to upload files from a local Windows computer to a CVM.

Prerequisites

You have built the FTP service on CVM.

- To use FTP to upload files to a Linux CVM, see Building the FTP Service (Linux)
- To use FTP to upload files to a Windows CVM, see Building the FTP Service (Windows)

Directions

Connecting to the CVM

1. Download and install the open-source FileZilla locally.

   If you use version 3.5.3 of FileZilla to upload files via FTP, the upload may fail. We recommend you download and use versions 3.5.1 or 3.5.2 of FileZilla from its official website.

2. Open FileZilla.

3. In the FileZilla window, enter information such as the host, username, password, and port, and click Quickconnect.

Configuration description:

- Host: the public IP of the CVM. Log in to the CVM Console to view the public IP of the CVM on the Instances page.
Username: the FTP user account configured when you [built the FTP service] (https://intl.cloud.tencent.com/document/product/213/10912). The figure below uses "ftpuser1" as an example.


Port: the FTP listening port, which is 21 by default.

After the connection is successful, you can view the files on the remote CVM site.

**Uploading a file**

In the lower-left "Local site" window, right-click the local file to be uploaded and select **Upload** to upload it to a Linux CVM, as shown below:

- CVM FTP path does not support the automatic decompression or deletion of uploaded compressed tar files.
- The remote site path is the default path for uploading files to a Linux CVM.

**Downloading a file**

In the lower-right "Remote site" window, right-click the CVM file to be downloaded and choose **Download** to download it to a local directory.
Introduction

The document uses CVMs with CentOS 7.6 as an example to describe how to upload and download files via SCP.

Prerequisites

You have purchased a Linux CVM.

Directions

Obtaining a public IP

Log in to CVM Console, navigate to the instance list page, and record the public IP of the CVM to which you want to upload files as shown below:

Uploading a file

1. Execute the following command on a computer with the Linux OS to upload files to the Linux CVM.

   \[ \text{scp local file address CVM account@CVM instance public IP/domain name: CVM file location} \]

   For example, if you want to upload the local file `/home/lnmp0.4.tar.gz` to the corresponding directory of the CVM whose public IP is `129.20.0.2`, please execute the following command:

   \[ \text{scp /home/lnmp0.4.tar.gz root@129.20.0.2:/home/lnmp0.4.tar.gz} \]

2. Enter `yes` and press **Enter** to confirm the upload and enter the login password to complete the upload.
If you use a system default password to log in to the instance, you can view the password in the Message Center.

If you forget your password, please reset the instance password.

**Downloading a file**

1. Execute the following command on a computer with the Linux OS to download files from the Linux CVM.

   ```
   scp CVM account@CVM instance public IP/domain name: CVM file location local file address
   ```

   For example, if you want to download the file `/home/Inmp0.4.tar.gz` from the CVM whose public IP is `129.20.0.2` to the corresponding local directory, please execute the following command:

   ```
   scp root@129.20.0.2:/home/Inmp0.4.tar.gz /home/Inmp0.4.tar.gz
   ```
Uploading Files from Windows to a Windows CVM using MSTSC

Last updated : 2020-05-28 18:16:56

Scenario

The common method for file upload to Windows CVM is to use Microsoft Terminal Services Client. This document describes how to upload files to Windows CVM using remote desktop connection on a local Windows computer.

Prerequisites

Make sure the Windows CVM can access the public network.

Directions

The following takes the local computer with Windows 7 operating system as an example. The specific steps may vary by operating systems.

Obtaining a public IP

Log in to CVM Console. On the instance list page, record the public IP of the CVM to which you want to upload files.

Uploading a file

1. Use the shortcut key Windows + R on the local computer to open the Run window.
2. In the pop-up Run window, enter mstsc, and click OK to open the Remote Desktop Connection box.
3. In the Remote Desktop Connection box, enter the public IP address of the CVM and click Show Options.
4. On the General tab, enter the CVM public network IP address and user name Administrator.
5. Select the Local Resources tab and click More.
6. In the pop-up **Local devices and resources** window, select the **Drives** module, check local disks where files to be uploaded to Windows CVM are located, and click **OK**.

7. After the local configuration is complete, click **Connect** to log in to Windows CVM remotely.

8. Click **Start > Computer** on Windows CVM, and you can see the local disks mounted to the CVM.

9. Double-click to open the mounted local disks, and copy the local files to other hard disks of Windows CVM to complete file uploads.

   For example, copy file A from local disk (E) to disk C of Windows CVM.

### Downloading a file

To download files from Windows CVM to the local computer, refer to the file upload operations above and copy the required files from Windows CVM to the mounted local disks to complete file downloads.
Installing Software
Accelerating software package download and update with Tencent Cloud software source

Scenario

To solve the problem of slow access to official sources when installing dependencies, Tencent Cloud has set up a cache service for some software. You can accelerate the installation of dependencies by using the Tencent Cloud software repository. It currently supports public network access and private network access.

- Public network access address: http://mirrors.cloud.tencent.com/
- Private network access address: http://mirrors.tencentyun.com/

- This document takes public network access address of the Tencent Cloud software repository as an example to introduce how to use the software sources at Tencent Cloud software repository in CVM. If you access the repository using a private network, please replace the public network access address with the private network access address.
- The source address involved in this document is for reference only. Please obtain the latest address from Tencent Cloud software repository.

Notes

Tencent Cloud software repository updates software sources from the official website of each software source once per day.

Prerequisites

You have already logged in to CVM.
Directions

**Accelerating pip using Tencent Cloud image source**

Before use, please confirm your CVM has Python installed.

**Use software source path temporarily**

Execute the following command to install pip using Tencent Could PyPI.

```
pip install pip -i the directory where PyPI locates
```

For example, if the PyPI you need to use is in the http://mirrors.cloud.tencent.com/pypi/simple directory, execute the following command:

```
pip install 17monip -i http://mirrors.cloud.tencent.com/pypi/simple --trusted-host mirrors.cloud.tencent.com
```

**Set default software source path**

Execute the following command to modify the index-url parameter in the ~/.pip/pip.conf file to the source path of Tencent Cloud software repository.

```
[global]
index-url = the directory where PyPI locates
trusted-host = public network/private network access address
```

For example, if the PyPI you need to use is in the http://mirrors.cloud.tencent.com/pypi/simple directory, execute the following command:

```
[global]
index-url = http://mirrors.cloud.tencent.com/pypi/simple
trusted-host = mirrors.cloud.tencent.com
```

**Accelerating Maven using Tencent Cloud image source**

Before use, please confirm your CVM has JDK and Maven installed.

1. Open the settings.xml configuration file of Maven.
2. Find the code block of `<mirrors> ... </mirrors>` and configure the following content into it.

```xml
<mirror>
  <id>nexus-tencentyun</id>
  <mirrorOf>*</mirrorOf>
  <name>Nexus tencentyun</name>
  <url>http://mirrors.cloud.tencent.com/nexus/repository/maven-public/</url>
</mirror>
```

Accelerating NPM using Tencent Cloud image source

Before use, please confirm your CVM has Node.js and NPM installed.

Execute the following command to install NPM using the Tencent Cloud NPM.

```
npm config set registry http://mirrors.cloud.tencent.com/npm/
```

Accelerating Docker using Tencent Cloud image source

Use Tencent Cloud Docker on TKE cluster

No manual configuration is required. When the CVM in Tencent Kubernetes Engine (TKE) cluster creates a node, Docker will be installed automatically and configured with Tencent Cloud private network image.

Use Tencent Cloud Docker on CVM

Before use, please confirm your CVM has Docker installed.

Only Docker 1.3.2 or later versions support Docker Hub Mirror mechanism. If you have not installed Docker 1.3.2 or later, or the installed version is too old, please install or upgrade it first.

Choose different operation steps based on the operating system of the CVM.

- For Ubuntu 14.04, Debian, CentOS 6, Fedora, openSUSE and other operating systems. The specific steps for other versions of operating systems may vary:
  i. Execute the following command to open the `/etc/default/docker` configuration file.

```
vim /etc/default/docker
```
ii. Press i to switch to the editing mode, enter the following content and save.

```bash
DOCKER_OPTS="--registry-mirror=https://mirror.ccs.tencentyun.com"
```

- For Centos 7:
  i. Execute the following command to open the `/etc/docker/daemon.json` configuration file.

```bash
vim /etc/docker/daemon.json
```

ii. Press i to switch to the editing mode, enter the following content and save.

```json
{
    "registry-mirrors": [
        "https://mirror.ccs.tencentyun.com"
    ]
}
```

- For Windows with Boot2Docker installed:
  i. Enter the Boot2Docker Start Shell and execute the following command:

```bash
sudo su echo "EXTRA_ARGS="--registry-mirror=https://mirror.ccs.tencentyun.com""" >> /var/lib/boot2docker/profile exit
```

ii. Restart Boot2Docker.

**Accelerating MariaDB using Tencent Cloud image**

The following steps take CentOS 7 as an example, and the specific steps vary by operating systems.

1. Execute the following command to create the `MariaDB.repo` file under `/etc/yum.repos.d/`.

   ```bash
   vi /etc/yum.repos.d/MariaDB.repo
   ```

2. Press i to switch to the editing mode, enter the following and save.

   ```bash
   # MariaDB 10.2 CentOS7-amd64
   [mariadb]
   name = MariaDB
   baseurl = http://mirrors.cloud.tencent.com/mariadb/yum/10.2/centos7-amd64/
   gpgkey = http://mirrors.cloud.tencent.com/mariadb/yum/RPM-GPG-KEY-MariaDB
   gpgcheck=1
   ```

3. Execute the following command to empty the YUM cache.
4. Execute the following command to install MariaDB.

```bash
yum install MariaDB-client MariaDB-server
```

**Accelerating MongoDB using Tencent Cloud image**

The following steps take MongoDB 4.0 as an example. If you need to install another version, please change the version number in the mirror path.

**Use Tencent Cloud MongoDB on CVMs with CentOS or Redhat systems**

1. Execute the following command to create the `mongodb.repo` file under `/etc/yum.repos.d/`.

```bash
vi /etc/yum.repos.d/mongodb.repo
```

2. Press `i` to switch to the editing mode, enter the following and save.

```yaml
[mongodb-org-4.0]
name=MongoDB Repository
baseurl=http://mirrors.cloud.tencent.com/mongodb/yum/el7-4.0
gpgcheck=0
enabled=1
```

3. Execute the following command to install MongoDB.

```bash
yum -y install mongodb-org
```

**Use Tencent Cloud MongoDB on CVMs with Debian system**

1. Based on Debian versions, execute the following command to import the MongoDB GPG public key.

```bash
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv 68818C72E52529D4
```

2. Execute the following command to configure the mirror path.

```bash
#Debian 8
echo "deb http://mirrors.cloud.tencent.com/mongodb/apt/debian jessie/mongodb-org/4.0 main" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.0.list
#Debian 9
```
3. Execute the following command to update software package list.

   ```
sudo apt-get update
```

4. Execute the following command to install MongoDB.

   ```
sudo apt-get install -y mongodb-org
```

**Use Tencent Cloud MongoDB on CVMs with Ubuntu system**

1. Execute the following command to import the MongoDB GPG public key.

   ```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv 68818C72E52529D4
```

2. Execute the following command to configure the mirror path.

   ```
#Ubuntu 14.04
echo "deb [ arch=amd64 ] http://mirrors.cloud.tencent.com/mongodb/apt/ubuntu trusty/mongodb-org/4.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.0.list
#Ubuntu 16.04
echo "deb [ arch=amd64 ] http://mirrors.cloud.tencent.com/mongodb/apt/ubuntu xenial/mongodb-org/4.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.0.list
#Ubuntu 18.04
echo "deb [ arch=amd64 ] http://mirrors.cloud.tencent.com/mongodb/apt/ubuntu bionic/mongodb-org/4.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.0.list
```

3. Execute the following command to update software package list.

   ```
sudo apt-get update
```

4. Execute the following command to install MongoDB.

   ```
sudo apt-get install -y mongodb-org
```

**Accelerating Rubygems using Tencent Cloud image source**

Before use, please confirm your CVM has Ruby installed.

Execute the following command to modify RubyGems source address.

```
gem source -r https://rubygems.org/
gem source -a http://mirrors.cloud.tencent.com/rubygems/
Install Software via Apt-get under Ubuntu Environment

Last updated : 2020-05-13 14:13:15

Introduction

Advanced Package Tool (APT) is a free software user interface that works with core libraries to handle the installation and removal of software on various Linux distributions. APT offers a centralized interface for software management and a better experience than having to download and install software one by one. Tencent Cloud hosts APT sources so you can install software without adding sources.

Prerequisites

Log in to a Linux CVM instance that runs Ubuntu.

Directions

In the following, Nginx is used as an example.

Listing available software

Run the following command to list available software:

```
sudo apt-cache search all
```

Installing software

Run the following command to install Nginx:

```
sudo apt-get install nginx
```

Make sure this is the software you want to install and enter \( Y \) to approve the installation. Wait until the software installation is complete, as shown in the figure below:
Querying installed software

You can run different commands to query installed software.

- Run the following command to query the directory of the software package and all the files in the software package.

  `sudo dpkg -L software_name`

- Run the following command to query the version information of the software package.

  `sudo dpkg -l software_name`

View information on the installed Nginx, as shown in the figure below:
Install Software via YUM under CentOS Environment

Last updated : 2020-05-13 14:13:16

Scenario

Yellow dog Updater, Modified (Yum) is the default package manager used in CentOS. It is used to install and update packages from CentOS and 3rd party repositories. Yum offers a centralized interface for software management and a better experience than having to download and install software one by one. Tencent Cloud hosts Yum sources so you can install software without adding sources.

Directions

Installing software

1. Log in to your CVM instance using root.
2. Run the following command to install software.

   Starting from CentOS 7, MariaDB has become the default database in the YUM source. If you are using CentOS 7 or later, MySQL installed using ‘yum’ will be unusable. You can use the fully compatible MariaDB, or refer to this article on how to install an older version of MySQL.

   ```
   yum install software_name
   ```

   The software you install may need additional software to run. These additional software are called dependencies. Yum automatically search for dependencies and display the results on screen so you can verify whether the software package is suitable.
For example, after you run `yum install PHP` to install PHP, the following is displayed:

```
Installing:
  PHP        x86_64  5.4.16-46.el7          os  1.4 M
  apr        x86_64  1.4.8-3.el7_4.1    os  103 k
  apr-util   x86_64  1.5.2-6.el7        os  92 k
  httpd      x86_64  2.4.6-89.el7.centos os  2.7 M
  httpd-tools x86_64  2.4.6-89.el7.centos updates 90 k
  lib64      x86_64  0.10.1-8.el7        os  48 k
  mailcap    noarch  2.1.41-2.el7       os  31 k
  php-cgi    x86_64  5.4.16-46.el7      os  2.7 M
  php-common x86_64  5.4.16-46.el7      os  563 k
```

3. Enter `y` and press Enter to install the software and any dependency it may require. When the screen displays Complete, the installation is complete, as shown in the figure below:

```
rbp:php.x86_64 0:5.4.16-46.el7
apr.x86_64 0:1.4.8-3.el7_4.1
httpd-tools.x86_64 0:2.4.6-89.el7.centos
lib64.x86_64 0:0.10.1-8.el7
mailcap.noarch 0:2.1.41-2.el7
php-cgi.x86_64 0:5.4.16-46.el7
php-common.x86_64 0:5.4.16-46.el7
[root@VM_5_10_centos ~]$
```

**Query installed software information**

After software installation is complete, you can run different commands to view information.

- Run the following command to view the installation directory of a software package.

  `rpm -ql software name`

For example, run `rpm -ql php` to view the installation directory of PHP, as shown in the figure below:

```
[root@VM_5_10_centos ~]# rpm -ql php
/etc/httpd/conf.d/php.conf
/etc/httpd/conf.modules.d/10-php.conf
/usr/lib64/httpd/modules/libphp5.so
/var/lib/php/session
[root@VM_5_10_centos ~]$
```
Run the following command to query the version information of a software package.

```
rpm -q software_name
```

For example, run `rpm -q php` to query the version information of PHP, as shown in the figure below:

```
[root@VM_5_10_centos ~]# rpm -q php
php-5.4.16-46.el7.x86_64
[root@VM_5_10_centos ~]#
```
Install Software via zypper under SUSE Environment

Last updated: 2019-09-26 19:27:02

Make sure that you have followed the steps in Installing Software via YAST in SUSE Environment install the necessary software.

1. Configuration of nginx

1) Start nginx service

Start the nginx service with the following command:

```
    service nginx restart
```

2) Test whether nginx service is working properly

Test with the following command:

```
    wget http://127.0.0.1
```

If the result is as shown below and displays "'index.html' saved" at the end, it means the nginx service is working properly.

```
2013-02-20 17:07:26 -- http://127.0.0.1/
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 151 [text/html]
Saving to: 'index.html'
100%[==========================================>>]
151 --. -K/s in 0s
2013-02-20 17:07:26 (37.9 MB/s) - 'index.html' saved [151/151]
```

3) In the browser, visit the Public IP of CentOS CVM to check if the nginx service is working properly.

The appearance of the following page indicates that nginx has been installed and configured successfully.

2. Configuration of PHP
1) Create a new configuration file `php-fpm.conf` with the following command:

```bash
vim /etc/php5/fpm/php-fpm.conf
```

Write the following:

```plaintext
[global]
error_log = /var/log/php-fpm.log
[www]
user = nobody
group = nobody
listen = 127.0.0.1:9000
pm = dynamic
pm.max_children = 5
pm.start_servers = 2
pm.min_spare_servers = 1
pm.max_spare_servers = 3
```

3. Start services

Start all services with the following commands:

```bash
/etc/init.d/mysql start; /etc/init.d/php-fpm start; /etc/init.d/nginx start
```

Example:

```
VM 137_55_sles10_64:~ # /etc/init.d/mysql start; /etc/init.d/php-fpm start; /etc/init.d/nginx start
done done done
done
done running done
```

4. Environment configuration validation

Create `index.php` under a web directory using the following command:

```bash
vim /usr/share/nginx/html/index.php
```

Write the following:
<?php
echo "<title>Test Page</title>";
echo "hello world";
?>

In the browser, visit the Public IP of SUSE CVM to check whether the environment configuration is successful. If the webpage shows "hello world", it means the configuration is successful.
User Data
Configuring Custom Data (Linux CVM)
Last updated : 2020-05-25 17:35:55

Scenario

When creating a CVM, you can configure an instance by specifying custom data. During the first launch of the CVM, the custom data will be passed into the CVM in text format and be executed. If you purchase multiple CVMs at a time, all CVMs will execute the custom data upon their first launch. This article describes how to pass a Shell script when launching a Linux CVM for the first time.

Notes

- Linux operating systems that support custom data include:
  - 64-bit operating system: CentOS 6.8 64-bit or later versions, Ubuntu Server 14.04.1 LTS 64-bit or later versions, and suse42.3x86_64
  - 32-bit operating system: CentOS 6.8 32-bit or later versions
- A command can be executed by passing text only when a CVM is launched for the first time.
- Custom data must be Base64 encoded and then passed. For a compatible format, encode the custom data in Linux environment.
- Execute the custom data as root. Therefore, the sudo command is not required in the script. The root user can access all the files you created. If you need to grant other users with the access permission, modify the permission in the script.
- During launch, executing custom data tasks will increase the startup time of the CVM. Please wait a few minutes until the tasks are completed, and then test whether the tasks are executed successfully.
- In this example, Shell script must start with #! and the path to the interpreter reading the script (usually /bin/bash).

Directions

Writing a Shell script

1. Run the following command to create a Shell script named “script_text.sh”.

©2013-2019 Tencent Cloud. All rights reserved.
2. Press `i` to switch to the editing mode, enter the following and save the “script_text.sh” script.

```bash
#!/bin/bash
echo "Hello Tencent Cloud."
```

Shell script must start with `#!/` and the path to the interpreter reading the script (usually `/bin/bash`). For more information on Shell script, see BASH Programming of the Linux Documentation Project (tldp.org) (http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html).

### Encoding the script with Base64

1. Run the following command to encode the “script_text.sh” script with Base64.

```bash
# Base64 encoded script
base64 script_text.sh
```

You will see the following information:

```bash
# Encoded result
IyEvYmluL2Jhc2gKZWNobyAiSGVsbG8gVGVuY2VudCBDbG91ZC4iCg==
```

2. Run the following command to verify the Base64 encoded result of the script.

```bash
# Decode the returned result with Base64 and verify whether it is the command to be executed.
echo "IyEvYmluL2Jhc2gKZWNobyAiSGVsbG8gVGVuY2VudCBDbG91ZC4iCg==" | base64 -d
```

### Passing the text

You can launch an instance through multiple methods, and here we introduce two of them. Choose a method according to your requirements:

- Using the official website or the console
- Using API

#### Using the official website or the console

1. Refer to Creating Instances to purchase an instance, and click **Advanced Settings** in “4. Security Group and CVM”, as shown below:
2. In **Advanced Settings**, enter the returned result of **Base64 encoded script** in the Custom Data text box, as shown below:

For example, the Base64 encoded result of the `script_text` script is

```
IyEvYmluL2Jhc2gKZWNobyAiSGVsbGl8gVGVuY2VudCBDbG91ZC4iCg==
```

3. Create an CVM instance as prompted by the page.
Tencent Cloud CVM executes the script using the open-source software cloud-init. For more information about cloud-init, see cloud-init's official website.

Using API

When creating a CVM by using API, you can pass the text by assigning the value of the encoded result returned in Base64 encoded script to the UserData parameter of the RunInstances API. The following is a sample CVM creation request with UserData:

```
https://cvm.tencentcloudapi.com/?Action=RunInstances
&Version=2017-03-12
&Placement.Zone=ap-guangzhou-2
&ImageId=img-pmqg1cw7
&UserData=IyEvYmluL2Jhc2gKZWNobyAiSGVsbG8gVGVuY2VudCBDbG91ZC4iCg==
&<Common request parameters>
```
Configuring Custom Data (Windows CVM)

Introduction

While you create a CVM instance, you have the option to define a script as Custom Data and use it to customize your instance configuration. When the instance starts up for the first time, that custom data is passed on and executed. If you purchased multiple CVM instances, all instance will execute the script upon first launch.
This article describes how to define a PowerShell script and use it to configure a Windows CVM instance.

Considerations

- Windows operating systems that support custom data include:
  - Windows Server 2016 Datacenter Edition 64-bit Chinese/English version
  - Windows Server 2012 R2 Datacenter Edition 64-bit Chinese/English version
- The script is executed when and only when the instance starts up for the first time.
- Before Base64 encoding, the size of the custom data cannot exceed 16 KB.
- Custom data is Base64 encoded and then passed. If you want a script file in its orginal form, do not select The entry is Base64-encoded text.
- The custom configurations you defined in the custom data script take time to execute. We recommend that you wait for the configurations to complete and verify if the results.
- Use the PowerShell tag, such as <powershell></powershell> to declare the content of the Windows PowerShell script.

Directions

Preparing a script

Prepare a script that suit your needs:

PowerShell script
Use the PowerShell tags to surround script content. For example, if you want to use the script to create a file called `tencentcloud.txt` with the content of “Hello Tencent Cloud.” in the C: drive, use the following tags:

```powershell
"Hello Tencent Cloud." | Out-File C:\tencentcloud.txt
</powershell>

### Encoding the script with Base64

1. Run the following command to create a PowerShell script named “script_text.ps1”.

   ```
   vi script_text.ps1
   ```

2. Press `i` to switch to the editing mode, enter the following content, and save.

   ```powershell
   "Hello Tencent Cloud." | Out-File C:\tencentcloud.txt
   </powershell>
   ```

3. Run the following command to encode `script_text.ps1` with Base64.

   ```
   base64 script_text.ps1
   ```

The following information is returned:

```
PHBvd2Vyc2hlbGw+CiJIZWxsbyBUZW5jZW50IE5sb3VkLiIgfCBPdXQtRmlsZSAgQzpcdGVuY
GudGNsb3VkJnR4dAo8L3Bvd2Vyc2hlbGw+Cg==
```

### Passing the script

We provide multiple methods to launch an instance. The following are the most used methods:

- Using the official website or the console
- Using APIs

#### Using the official website or the console

1. Use [Creating an Instance](#) as an reference and create a CVM instance. Click [Advanced Configuration](#) in 4. Configure Security Group and CVM, as shown in the following figure:
2. In **Advanced Configuration**, enter script content in the **Custom Data** text box.
   - **PowerShell script**: enter the script content you entered in **PowerShell script** in its original form.
   - **Base64 encoded script**: select **The entry is Base64-encoded text**, and enter the encoded script content you encoded in **Encoding the script with Base64**, as shown in the following figure:

3. Follow the instructions and complete the CVM creation.

**Using APIs**
If you choose to create an CVM instance using Tencent Cloud APIs, you can assign the the encoded result returned in Encoding the script with Base64 to the UserData parameter of RunInstances. The following is an sample CVM creation request with UserData:

```
https://cvm.tencentcloudapi.com/?Action=RunInstances
&Version=2017-03-12
&Placement.Zone=ap-guangzhou-2
&ImageId=img-pmqg1cw7
&UserData=PHBvd2Vyc2hlbGw+CiJIZWxsbyBUZW5jZW50IENsb3VkLiIgfCBPdXQtRmlsZSAYbmltbW9Ub3QgKHJpZmlkLiBhdXRoIGF0dXJlcg==
&<Common request parameter>
```

**Verifying custom data configurations**

1. Log in to the CVM instance.
2. Open the C: drive, and check whether `tencentcloud.txt` exists. If it does, the configuration is successful, as shown in the following figure:
System-related System Activation

Last updated : 2020-06-03 14:16:01

Tencent CVM uses KMS to authorize a Windows server.

- This document is intended only for Windows Server public images provided by Tencent Cloud. It is not applicable for custom images or images imported from external sources.
- This authorization is required for Windows Server 2008 and Windows Server 2012. The default KMS address (kms.tencentyun.com:1668) configured in the public images of Windows Server 2016 and Windows Server 2019 can be used without any further modification.

Before Activation

1. SPP Notification Service on Windows is used for activation. Make sure it is running properly.
2. Some optimization software may disable modifying the execution permissions of service programs. For example, modifying the execution permissions of sppsvc.exe might result in exceptions.

Before you attempt to activate a Windows CVM, make sure that the service and other essential features of Windows are running properly.

**Automatic Activation**

Tencent Cloud encapsulates a script for Windows server activation, simplifying the activation process.

1. Log in to the Windows CVM.
3. Run the script to complete automatic activation.

**Manual Activation**

**Notes**

An inaccurate system clock will trigger an error during manual activation for some systems. In such cases, you need to synchronize the system clock first by following the steps below:

If the system clock on the Windows CVM is accurate, go to the Activation directions.

1. Log in to the Windows CVM.
2. On the desktop, click **Start** -> **Run**, and enter **cmd.exe** to open the console window.
3. In the console window, run the following commands sequentially to synchronize the system clock.
w32tm /config /syncfromflags:manual /manualpeerlist:“ntpupdate.tencentyun.com”
w32tm /resync

**Activation directions**

1. Log in to the Windows CVM.
2. On the desktop, click **Start** -> **Run**, and enter `cmd.exe` to open the console window.
3. In the console window, run the following commands sequentially to complete manual activation.
   - Run the following commands sequentially for Windows Server 2008, Windows Server 2012, and Windows Server 2019:
     ```
     cscript /nologo %windir%/system32/slmgr.vbs -skms kms.tencentyun.com:1688
     cscript /nologo %windir%/system32/slmgr.vbs -ato
     ```
   - Run the following commands sequentially for Windows Server 2016:
     ```
     cscript /nologo %windir%/system32/slmgr.vbs -skms kms1.tencentyun.com:1688
     cscript /nologo %windir%/system32/slmgr.vbs -ato
     ```
System Updates

Last updated: 2020-05-08 11:28:35

Introduction

This article uses Windows Server 2012 as an example to illustrate how to update your Windows operating system.

Directions

Updating Windows using the public network

You can use the Windows Update service to update your operating system. The detailed steps are as follows:

1. Log in to the Windows CVM instance.
2. Click \rightarrow Control Panel \rightarrow Windows Update. The Windows Update window appears.
3. Click Check for updates, and wait until the check is finished.
4. After the check is finished, click N Important Updates Available or N Optional Updates Available in “Windows Update”. The Choose the Update to Install window appears.
5. Select the updates you want to install, and click Install.
   
   If you are prompted to restart your system after the update is completed, do so.

   If you log in using VNC after the instance is rebooted and the message "Updating...Do not turn off the power" or "Configuration has not been completed" appears, do not perform a force-shutdown. That may damage your CVM instance.

Updating Windows using the private network

If your CVM instance does not have public network access, you can use the Tencent Cloud private Windows Update server to update your operating system. The Tencent Cloud Windows Update server has most of the updates, but does not have hardware driver packages and some uncommon updates. Therefore, uncommon services may not get updates using the Tencent Cloud Windows Update server.

Follow these steps to use the Tencent Cloud Windows Update server:
1. Log in to the Windows CVM instance.
2. Use Internet Explorer to download the Tencent Cloud private network configuration file wusin.bat from the following address:
   http://mirrors.tencentyun.com/install/windows/wusin.bat
3. Run wusin.bat in Command Prompt with administrator privilege, as shown below:

   If you open wusin.bat using Internet Explorer after it finishes downloading, the console window will automatically close and you cannot observe the output.

   You can save wusin.bat to your hard drive, such as C:, and open a Command Prompt window with administrator privilege to run it.

If you no longer wish to use the Tencent Cloud Windows Update server, you can download wusout.bat clean it up. Follow these steps to do so:

1. Log in to the Windows CVM instance.
2. Use Internet Explorer to download the Tencent Cloud private network configuration file wusout.bat from the following address:
   http://mirrors.tencentyun.com/install/windows/wusout.bat
3. Run wusout.bat in Command Prompt with administrator privilege, as shown below:

   If you open wusout.bat using Internet Explorer after it finishes downloading, the console window will automatically close and you cannot observe the output information.

   You can save wusout.bat to your hard drive, such as C:, and open a Command Prompt window with administrator privilege to run it.
1. Analysis on the Shutdown of Virtual Clients

The following is the shutdown process of Windows virtual machine on Tencent Cloud.

1) Libvirt on the parent host sends shutdown command to qemu component via qmp protocol;
2) Qemu component transfers shutdown command to child host by injecting acpi interruption (For details, see technical documents on vmcs);
3) When receiving the shutdown signal, Windows tells applications and service processes to exit;
4) Close the core service process;
5) Turn off the power.

The shutdown process on Windows is basically the same as shown above. The sequence in which the applications and services are closed in step 3-4 may vary with the settings of system.

As a closed-source system, Windows provides some APIs to allow the programs with kernel mode and user mode to intervene in the shutdown process. And some services of Windows will also affect the shutdown process during operation, making the shutdown impossible. In some cases, Windows shutdown process can be very time-consuming to prevent the computer from being shut down.

In virtual scenarios, besides informing the Windows itself to shut down by sending a message, another means, which is similar to powering off a physical machine, is provided to stop a virtual client. This means is called "hard shutdown". Correspondingly, the shutdown action initiated by a system signal is called "soft shutdown".

Hard shutdown has some impact on the Windows itself and the user experience, mainly in the following two ways:

1) A hard shutdown interrupts some services and applications, which as a result may operate improperly, such as unsaved documents, and unfinished Windows Update processes;
2) As the NTFS system (or the earlier FAT32 system) of Windows writes some key data during the shutdown process, a hard shutdown may result in the failure to write such key data to the disk, which would lead Windows to determine that the NTFS file system is damaged.

For these reasons, it's recommended Tencent Cloud users take soft shutdown as the preferred way to shut down Windows.
2. Several Scenarios of Shutdown Failure

However, as mentioned above, there may be some issues within the Windows system that interfere with the shutdown process and result in shutdown failure. The scenarios include but not limited to:

1) A Windows Update process may extend the shutdown time. For some patch operations, the Windows system may take some actions during the shutdown process, by which time messages like "Please do not power off or unplug your machine" will display.

2) If "Shutdown Event Tracker" mechanism is enabled on the Windows system, when the system is shut down due to any error in the system service and driver, the system will provide user with a prompt box based on the configuration or fill in the error description to wait for the user to complete these operations. Windows will not turn off the power until the user has completed these operations.

3) Windows can be set to not allow shutdown while the user is not logged in to the system. In this case, the soft-shutdown command sent from the virtual host will be discarded by Windows so that the shutdown cannot be achieved.

4) Before the shutdown, Windows will broadcast a message to every service and application. If the applications responding to this message do not send a response that allows the shutdown, Windows will not initiate the shutdown. In this scenario, some settings can be made on Windows to ignore this process.

5) In the power management-related operation "What will Windows do when you press the power button ", if Windows is set to ignore it or do nothing, Windows will ignore the shutdown event of the virtualized parent host.

6) Based on the settings of power management, Windows will go into Sleep and not handle shutdown event.

7) In case of initial purchase of Windows, the initialization process is slightly longer due to the use of sysprep for distributing images. Windows will ignore the shutdown event until the initialization has been finished.

8) If the Windows system itself is damaged due to some malicious software installed within it or infection with Trojan virus or other viruses, Windows can be prevented from shutdown.

Tencent Cloud has optimized most of the above scenarios when publishing Windows public images so that the soft-shutdown can be completed successfully. These optimization measures are integrated into the script of Windows Power Management to be used for making adjustments to Windows features such as power management, turn-off of "Shutdown Event Tracker" and shutdown while user is not logged in to the system.
But these optimization measures cannot solve the scenarios where Windows is infected with viruses and Trojans or the system is damaged; In addition, if these relevant settings in the Windows virtual machine of user are adjusted again, there is no guarantee that the soft-shutdown can be completed successfully. In some cases, forced shutdown would pose a risk. For example, in the process of Windows Update, it is necessary to wait for the update to complete. During the soft-shutdown process, user needs to check the scenarios of shutdown failure by opening VNC, so as to conduct appropriate processing as required. Please perform hard-shutdown only if it is very necessary to do so.
Configuring High-performance Power Management

Last updated: 2020-05-12 17:47:15

Scenario

High-performance power management is required for the Windows Server operating system (OS) to support the soft shutdown of CVM instances. Otherwise, you can shut down CVM instances in the CVM console only by hard shutdown. This document uses Windows Server 2012 as an example to describe how to configure power management.

Note

To modify power management, you do not need to restart the computer.

Directions

1. Log in to the Windows CVM.

2. Access the Tencent Cloud private network in Internet Explorer and download the Tencent Cloud power modification and configuration tool.
   For example, download the Tencent Cloud power modification and configuration tool (power-set-win.bat) to the C: drive.

3. Use the command line tool (CMD) as the administrator to open power-set-win.bat, as shown in the following figure:

```
C:\Users\Administrator> C:\power-set-win.bat
change ok
change ok
(C:\Users\Administrator)
```
4. Run the following command to view the current power management scheme:

```
powercfg -L
```

5. On the desktop, click and choose **Control Panel > System and Security > Power Options** to open the **Power Options** window.

6. In the "Power Options" window, click **Change plan settings**.

7. In the "Edit Plan Settings" window, modify the idle turn-off times of the monitor and disk.
Windows Recovery Mode
Last updated : 2019-10-14 11:19:08

What is Windows Recovery?

Windows Recovery is a state in which users can repair, back up, or restore the system. If Windows detects certain system problems with its automatic repair function and believes that the system will be damaged if it continues to work, it will stop itself from starting up and enter the system recovery mode.

System Recovery Options include several tools, such as Startup Repair, System Restore, and Windows Memory Diagnostic. You can use those tools to repair problems, back up data, and restore the system.

If users fail to log in to a CVM remotely, and see the following figure when logging in to the CVM via the console, it means that the Windows CVM has entered the recovery mode.

Reasons for entering recovery mode

Common reasons for entering recovery mode:

- **The power was cut off while Windows was running or shutting down.** This includes shutting down the CVM in the console while Windows was running or shutting down. Windows entered the recovery mode because of possible loss of important data caused by improper shutdown.
The power was cut off when Windows was updating. Windows entered the recovery mode because of possible loss of important data during the interrupted update.

The system was damaged by Trojans or viruses.

Bugs in Windows core services. Windows detected a risk itself and entered Recovery mode.

The system lost critical data or was damaged. Windows entered the recovery mode because users accidentally damaged system files.

Precautions

It is recommended to take the following precautions:

- When shutting down the CVM, go to the console to monitor the shutdown process. The soft shutdown used by Tencent Cloud has a timeout mechanism. After soft shutdown is executed, if the shutdown process has not been completed after the preconfigured period, the system will return failure. If the shutdown process is slow or Windows updates start, do not force the shutdown; instead, just wait for the shutdown to complete. Please refer to Several Scenarios of Shutdown Failure as needed.
- Check whether there are abnormal programs or processes in the system, such as Trojans or viruses.
- Check whether the system management and anti-virus software is running normally.
- Install Windows updates in time, especially important updates and security updates.
- Check the system event logs regularly to see if there is an bug in core services.

Solutions

If Windows enters the recovery mode, you can continue the startup or allows Windows to automatically repair itself. Windows can automatically repair minor problems. Please follow the steps below:

1. Log in to the CVM via the CVM Console.
2. On the recovery mode interface, click **Next**.

3. When the system recovery options show up, click **Next** to use the default solution.
4. Click **Restart**, and quickly press **F8**.

5. Choose "Start Windows Normally".
6. If the startup fails, reinstall the system via the Console. See Use console to reinstall system for more details.
**Ensure Unique SIDs for CVMs using Sysprep**

*Overview*

To join an instance to a domain and log in to Windows CVM with the domain account, you need to run Sysprep before creating a custom image to ensure the SID will be unique. Otherwise, the instance cannot be joined to the domain because the CVM created with the custom image and the original instance contains identical information, such as duplicate SIDs. Skip this operation if you have no need to join your Windows CVM to a domain.

This document describes how to run Sysprep on the Windows Server 2012 R2 64-bit operating system to ensure that the Windows CVMs in the domain have unique SIDs.

For more information about Sysprep, see [https://technet.microsoft.com/zh-cn/library/cc721940(v=ws.10).aspx](https://technet.microsoft.com/zh-cn/library/cc721940(v=ws.10).aspx)

**Notes**

- Windows CVM must be an active genuine Windows operating system.
- If your Windows CVM is created with a non-public image, you must always run the Sysprep version provided in the original image under directory `%WINDIR%\system32\sysprep`.
- The remaining Windows reset counts must be greater than 1, otherwise Sysprep cannot be encapsulated. To check the remaining Windows reset counts, execute the command `slmgr.vbs /dlv`.
- The Cloudbase-Init account takes care of the initialization actions when a CVM instance is launched. If you change/delete this account or uninstall Couldbase-Init, you might lose custom information when you provision a new CVM from a custom image. Thus, we do not recommend modifying or deleting the Cloudbase-init account.

**Prerequisites**

1. **Log in to Windows CVM as Administrator.**
Install Cloudbase-Init on Windows CVM.

Directions

1. On the desktop, click to open a Windows PowerShell window.
2. Execute the following command in the Windows PowerShell window to go to the installation directory of the Cloudbase-init tool.
   
   ```
   cd 'C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf'
   ```

3. Execute the following command to encapsulate the Windows system.
   
   ```
   C:\Windows\System32\sysprep\sysprep.exe /generalize /oobe /unattend:Unattend.xml
   ```

4. Create a custom image from the CVM instance on which Sysprep has been executed, and start new CVM instances with the image. See Creating Custom Images.
   And now, each new CVM instance will have a unique SID when joining a domain.
To check CVM SID, execute the command `whoami /user`.
Modifying VNC Resolution

Last updated: 2020-06-04 11:28:57

Scenario

Some of Linux system images have lower VNC display resolution by default, even only 720 * 400 for CentOS 6. You can set the VNC resolution to 1024 * 768 by modifying the parameter `grub`. If Windows system images have a very low VNC resolution, their applications may be unable to properly display or open. To avoid these issues, you need to modify the resolution.

This document guides you through on how to adjust the VNC display resolution of CVMs.

Directions

Modifying the VNC resolution of Windows CVM instances

The guide below introduces how to modify the VNC resolution of Windows instances on the Windows Server 2012 operating system.

1. Log in to Windows instance via VNC.
2. Right-click on the desktop and select **Display resolution**, as shown below:
3. In the “Display” window, set **Resolution** to the desirable value and click **Apply**, as shown below:

4. In the pop-up window, click **Keep changes**.
5. Click **OK** to close the “Display” window.

**Modifying the VNC resolution of Linux CVM instances**

More recent Linux images such as CentOS 7, CentOS 8, Ubunt, and Debian 9.0, adopt a default VNC resolution of 1024 * 768, which can be used without any modification. The guide below introduces how to modify the VNC resolution of Linux instances on CentOS 6 and Debian 7.8 operating systems.

**CentOS 6**

CentOS 6 image has a VNC resolution of 720 * 400 by default. To set its resolution to 1024 * 768, you can modify the launch parameter **grub** as follows:

- **Log in to Linux Instance Using Standard Login Method**. You can also use other login methods that you are comfortable with:
  - Logging in to Linux Instances via Remote Login Tools.
  - Logging in to Linux Instance via SSH Key
• Logging in to Linux Instances via VNC.

2. Run the following command to open the `/etc/grub.conf` file.

   `vi /etc/grub.conf`

3. Press `i` to switch to the edit mode, and add `vga=792` to the parameter `grub`, as shown below:

   ```
   vga=792
   ```

4. Press `Esc`, enter `:wq`, save the file and return.

5. Run the following command to reboot the CVM.

   `reboot`

**Debian 7.8**

Both Debian 7.8 and Debian 8.2 images have a VNC resolution of 720 * 400 by default. To set their resolution to 1024 * 768, you can modify the launch parameter `grub` as follows:

• Log in to Linux Instance Using Standard Login Method. You can also use other login methods that you are comfortable with:
  
  • Logging in to Linux Instances via Remote Login Tools.
  
  • Logging in to Linux Instance via SSH Key
  
  • Logging in to Linux Instances via VNC.

2. Run the following command to open the `grub` file.

   `vi /etc/default/grub`

3. Press `i` to switch to the edit mode and append the parameter value `GRUB_CMDLINE_LINUX_DEFAULT` with `vga=792`.
4. Press **Esc**, enter **:wq**, save the file and return.

5. Run the following command to update the `grub.cfg` file.

   ```bash
   grub-mkconfig -o /boot/grub/grub.cfg
   ```

6. Run the following command to reboot the CVM.

   ```bash
   reboot
   ```

**Appendix**

The table below lists the relationships between resolution and VGA.

<table>
<thead>
<tr>
<th>Resolution</th>
<th>640 * 480</th>
<th>800 * 600</th>
<th>1024 * 768</th>
</tr>
</thead>
<tbody>
<tr>
<td>VGA</td>
<td>786</td>
<td>789</td>
<td>792</td>
</tr>
</tbody>
</table>
Update the Virtio ENI driver

Scenario

Tencent Cloud's Windows Server 2008 R2 Enterprise SP1 and Windows Server 2012 R2 use Virtio ENI drivers to optimize the network performance of virtualization hardware. Tencent Cloud will continue to improve ENIs for performance improvement and troubleshooting. This document describes how to upgrade the Virtio ENI driver and check the driver version.

Prerequisites

You have logged in to a Tencent Cloud CVM.

Directions

Checking system version information

You can view the system version information in the following steps:

1. Log in to the CVM, right-click Computer, select Properties to open the System window.
2. In the View basic information about your computer section, you can see the system version information as shown below:

Updating the Virtio ENI driver

The CVM will be disconnected from the network briefly during the update. Please make sure that this will not affect your service before updating. The CVM needs to be restarted after the update.

1. Use the browser of the CVM to download the Virtio ENI driver installer for Window Server 2008 R2 and Windows Server 2012 R2.
   Download the Virtio ENI driver: http://mirrors.tencentyun.com/install/windows/virtio_64_10003.msi
2. After the download is completed, double-click the installer, choose the **Classic** installation mode, and click **Next** as shown below:

3. In the Windows Security pop-up window, check **Always trust the software from Tencent Technology (Shenzhen) Company Limited** and click **Install** as shown below:

During the installation process, if the following box pops up, choose **Install this driver software anyway**.

4. Follow the prompt to restart the computer to complete the update.

**Checking the driver version**

1. Click 📋, type `ncpa.cpl` in the Run box, and press **Enter** as shown below:

2. In the "Network Connections" window, right-click the "Ethernet" icon and choose **Properties** as shown below:

3. In the "Ethernet Properties" window, click **Configure** as shown below:

4. In the "Tencent Virtio Ethernet Adapter Properties" window, go to the **Driver** tab to see the current driver version as shown below:
Modifying SID

Last updated: 2020-04-01 11:26:29

Scenario

Microsoft's operating system uses a security identifier (SID) to identify computers and users. CVM instances created with the same image will have the same SID and might experience domain log-in issues. If you need to build a Windows domain environment, you will need to modify the SID. This document takes the CVM with Windows Server 2012 operating system as an example to describe how to modify the SID using sysprep and sidchg tools of the system.

Notes

- This is only applicable to Windows Server 2008 R2, Windows Server 2012, and Windows Server 2016.
- To modify the SID in batch, you can create a custom image (select "run sysprep to create the image").
- Modify the SID may cause data loss or system damage. We recommend you create a system disk snapshot or image in advance.

Directions

Using sysprep to modify the SID

- After using sysprep to modify the SID, you need to manually reset some system parameters, including IP configuration information.
- When you use sysprep to modify the SID, C:\Users\Administrator will be reset and some data on the system disk will be erased. Please back up data.

1. Log in to the Linux CVM via VNC.

2. In the operating system interface, right-click > Run, enter cmd, and press Enter to open a Admin command line.
3. In the admin command line, execute the following command to save the current network configuration.

   ```
ipconfig /all
   ```

4. In the admin command line, execute the following command to open the sysprep tool.

   ```
C:\Windows\System32\Sysprep\sysprep.exe
   ```

5. In the “System Preparation Tool 3.14” window that pops up, make the following configuration.
   - Set **System Cleanup Action** to **Enter System Out-of-Box Experience (OOBE)** and check **General**.
   - Set **Shutdown Options** to **Reboot**.

6. Click **OK**, and the system will restart automatically.

7. After the startup is complete, follow the wizard to complete the configuration (select language, reset password, etc.).

8. In the operating system interface, right-click ➔ **Run**, enter **cmd**, and press **Enter** to open a Admin command line.

9. Execute the following command to verify whether the SID has been modified.

   ```
whoami /user
   ```

If a message similar to the following is returned, the SID has been modified.

![Whoami User Command Result](image)

0. Reset ENI information (such as IP address, gateway address, DNS, etc.) based on the network configuration information saved in [Step 3](#step_03).

**Using sidchg to modify the SID**

1. Log in to the CVM.
2. Access and download the sidchg tool through IE browser.
3. Using the admin command line to execute the following command and open the sidchg tool, as shown below:
For example, the sidchg tool is saved on C: drive and its name is sidchg64-2.0p.exe.

```
C:\Users\Administrator>C:\sidchg64-2.0p.exe /R
SID Change Utility SIDCHG64 2.0p — Copyright Stratesave Systems 2019
Shareware — visit http://www.stratesave.com for Licence and pricing

Enter license key or trial key:
```

/R means automatic restart after modification, and /S means shutdown after modification. For details, please see SIDCHG Official Instructions.

4. Enter license key or trial key as prompted by the page, and press Enter.

5. Enter Y as prompted by the page, and press Enter, as shown below:

```
C:\Users\Administrator>C:\sidchg64-2.0p.exe /R
SID Change Utility SIDCHG64 2.0p — Copyright Stratesave Systems 2019
Shareware — visit http://www.stratesave.com for Licence and pricing

Enter license key or trial key:
34D6g-4sEJk-v0Wtg-4v
Temporary trial-key for evaluation only
To assure correct change of SID, current user will be logged out and SID change will be done in background,
after which the system will reboot
Do not turn off or shut down your computer and do not log into your computer while SID change is running!!

Changing SID risks data loss and damaged System. Do you want to continue <Y/N>?
```

6. In the prompt box for modifying the SID, click [OK] to reset the SID, as shown below:
The system will be restarted during the reset.

6. After the startup is completed, right-click Run, enter cmd, and press Enter to open the admin command line.

7. Execute the following command to verify whether the SID has been modified.

   whoami /user

If a message similar to the following is returned, the SID has been modified.
1. What is the server Load Average?

Load is used for measuring the workload of a server, that is, the length of the queue of tasks to be executed by the CPU. The greater the value, the more processes that are currently running or waiting to be executed.

2. How can I check my server load?

You can run `w`, `top`, `uptime`, and `procinfo` or use the file `/proc/loadavg` to check your server load.

Refer to documentation on how to install software on Linux for the instructions on how to install procinfo.

3. What should I do when the server load is too high?

Server load/load average is based on the length of the process queue. When the server load is high (we recommend that you use a 15-minute average as the reference), it may be caused by reasons such as insufficient CPU resources, I/O read/write bottleneck, insufficient memory resources, or the intensive computing tasks. Use `vmstat`, `iostat`, and `top` to identify the reason for the high load and optimize the corresponding processes.

4. How do I check server memory usage?

You can check your memory usage using `free`, `top` (after running, you can press `shift+m` to sort the memory), `vmstat`, and `procinfo` or the file `/proc/meminfo`.

5. How do I check the memory occupied by a single process?
You can check this using `top -p PID`, `pmap -x PID`, and `ps aux|grep PID` or the `/proc/$process_id/status` file, such as, `/proc/7159/status.

6. How do I check which services and ports are in use?

You can check using `netstat -tunlp`, `netstat -antup`, and `lsof -i:PORT`.

7. How do I check server process information?

You can check using `ps auxww|grep PID`, `ps -ef`, `lsof -p PID`, and `top -p PID`.

8. How do I stop a process?

You can run `kill -9 PID` (PID is the process ID) and `killall program name` (for example, killall cron) to stop the process. 
To stop a zombie process, you need to kill the parent process by running `kill -9 ppid` (ppid is the parent process ID, which can be queried by running `ps -o ppid PID`, for example, `ps -o ppid 32535`).

9. How do I find a zombie process?

You can run `top` to view the total number of zombie processes, and run `ps -ef | grep defunct | grep -v grep` to find the information of a specific zombie process.

10. Why can't I enable a server port?

You need use the operating system or the application to check if a port is enabled. 
For ports below 1024, you need to be `root` to use it. Use `sudo su -` to obtain root privileges before doing so. 
For application issues such as port conflict or misconfiguration, use application startup logs to troubleshoot. Tencent Cloud system uses port 36000.

11. What are the commands commonly used for checking the performance of a Linux server?
<table>
<thead>
<tr>
<th>Command name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>top</td>
<td>top is a task manager program that displays information about CPU and memory utilization. This command can be used to display information such as system load, process, CPU, memory and paging. Use <code>shift+m</code> and <code>shift+p</code> to sort processes by memory usage and CPU usage.</td>
</tr>
<tr>
<td>vmstat</td>
<td>vmstat is a computer system monitoring tool that collects and displays summary information about operating system memory, processes, interrupts, paging and block I/O. For example, <code>vmstat 3 10</code> outputs results every 3 seconds and is executed 10 times.</td>
</tr>
<tr>
<td>iostat</td>
<td>iostat is a computer system monitor tool used to collect and show operating system storage input and output statistics. For example, <code>iostat -dxmt 10</code> outputs detailed information about IO in MB every 10 seconds.</td>
</tr>
<tr>
<td>df</td>
<td>df is a standard Unix command used to display the amount of available disk space for file systems on which the invoking user has appropriate read access. For example: <code>df -m</code> displays the disk space usage in MB.</td>
</tr>
<tr>
<td>lsof</td>
<td>lsof is short for list open files, which is used to report a list of all open files and the processes that opened them. For example: <code>lsof -i: 36000</code> displays the processes using Port 36000. <code>lsof -u root</code> displays the programs run by root. <code>lsof -c php-fpm</code> displays the files opened by php-fpm process. <code>lsof php.ini</code> displays the processes for which php.ini is opened.</td>
</tr>
<tr>
<td>ps</td>
<td>ps, short for Process Status, is a command line utility that is used to display or view information related to the processes running in a Linux system. Commonly used command parameter combinations are <code>ps -ef</code> and <code>ps aux</code>. Use <code>ps -A -o</code> to output custom fields. For example: `ps -A -o pid,stat,uname,%cpu,%mem,rss,args,lstart,etime</td>
</tr>
</tbody>
</table>
Other commonly used commands and files: `free -m`, `du`, `uptime`, `w`, `/proc/stat`, `/proc/cpuinfo`, and `/proc/meminfo`.

##12. What do I do when Cron does not work?

Use the following steps to troubleshoot:

1. Verify whether crontab is running normally.
   i. Run `crontab -e` to add the following test item.
   ```
   */1 * * * * /bin/date >> /tmp/crontest 2>&1 &
   ```
   ii. Observe the `/tmp/crontest` file.
   In case of any problems, run `ps aux | grep cron` to look for the pid of cron and use `kill -9 PID` to terminate the cron process. Then restart cron with `/etc/init.d/cron start`.

2. Verify whether absolute path is used in the cron script.

3. Check whether you used the right account to execute cron. Also check if the account is included in `/etc/cron.deny`.

4. Check the execution permission of the script, script directory and log file permission.

5. We recommended that you run the script in the background. Append an "&" to the script entry, for example, `*/1 * * * * /bin/date >> /tmp/crontest 2>&1 &`.

##13. How do I setup a startup task for my CVM instance?

Linux kernel startup sequence is as follows:

1. Start the `/sbin/init` process.
2. Run the init initial scripts in sequence.
3. Run the level script `/etc/rc.d/rc*.d`, where the value of * means running mode, which can be queried in `/etc/inittab`.
4. Run `/etc/rc.d/rc.local`.

The configuration of startup task can be made in the `S***srclocal` file in `/etc/rc.d/rc*.d` or in `/etc/rc.d/rc.local`.

##14. Why is the server hard drive read-only?

Common reasons for a read-only hard disk are as follows:
- The disk space is full
  You can use the `df -m` command to check the disk usage, and then delete unnecessary files to free disk space. (Deleting non-third party files is not recommended. Check the files before you delete them).
- Disk inode resources are all occupied
  You can run `df -i` to view and confirm relevant processes.
- Hardware fault

If you still cannot identify the reason using the above methods, please call the hot line 95716 or submit a ticket.

15. How do I view system logs?

- The storage path for system-level log files is `/var/log`.
- The commonly used system log is `/var/log/messages`.

16. How do I find large files in the file system?

You can find them by following these steps:

1. Run `df` to query the disk partition usage, for example, `df -m`.
2. Run `du` to query the size of a specific folder, for example, `du -sh ./`, `du -h --max-depth=1|head -10`.
3. Run `ls` to list the files and file sizes, for example, `ls -lSh`.
   You can also directly check the size of files under a specific directory by using the `find` commands, for example, `find / -type f -size +10M -exec ls -lrt {}`;

17. How do I check the version of an operating system?

You can run the following commands to query the system version:

- `uname -a`
- `cat /proc/version`
- `cat /etc/issue`
18. Why are Chinese displayed as garbage characters in a terminal?

The server itself does not impose restrictions on the display language. Therefore, this most likely is a client problem. If you are using secureCRT, try to change settings in Options -&gt; Session Options -&gt; Appearance. If you are using other terminal software, google for a solution. If this problem appears in a pure Linux shell, use the export command to check user environment variables such as LANG and LC_CTYPE.

19. How do I configure connection timeout using SecureCRT?

You can configure the following settings so that the connection to your CVM instance is stable:

1. Open SecureCRT and select Options.
2. Select Session Options and click Terminal.
3. Select Send protocol NO-OP in Anti-idle and set the time to every 120 seconds.

20. Why isn't disk space freed after a file is deleted?

**Cause:**

You log in to your CVM instance and delete a file using `rm`. Then you check disk space using `df` but the amount of free disk space is the same. What happened? This is because when the file is deleted, another process happens to be accessing the file, the space occupied by the deleted file will not be immediately freed at the time you check the disk space.

**Solution:**

1. Run `lsof |grep deleted` with root privilege and find the PID of the process which is using the deleted file.
2. Kill the process with `kill -9 PID`.
Setup Windows CVM For Multi-user Remote Login

Last updated: 2020-04-13 11:17:44

Scenario

This document shows you how to configure a multi-user remote login to Windows CVM, taking a CVM with Windows Server 2012 R2 as the operating system as an example.

Steps

Adding remote desktop service

1. Log in to the Windows CVM.

2. In the operating system interface, click ![Server Manager] to open Server Manager, as shown below:
3. Click **Add roles and features**, and the **Add Roles and Features Wizard** window will pop up.

4. In the “Add Roles and Features Wizard” window, keep the default parameters for the first 3 steps.

5. In the **Select server roles** page, check **Remote Desktop Services** and click **Next**, as shown below:

   ![Add Roles and Features Wizard](image)

6. Keep the default parameters and click **Next** two times in a row.

7. In the **Select Role Service** interface, check **Remote Desktop Session Host**, as shown below:

   ![Select Role Service](image)

   The “Add features that are required for remote desktop session host?” prompt box will pop up.
8. In the “Add features required for remote desktop session host?” prompt box, click **Add Features**, as shown below:
9. In the **Select Role Service** page, check **Remote Desktop Licensing**, as shown below: The “Add features that required for Remote Desktop Licensing?” prompt box will pop up.
0. In the “Add features that required for Remote Desktop Licensing?” prompt box, click **Add Features**.
1. Click **Next**.
2. Check **Restart the destination server automatically if required**, and click **Yes** in the pop-up prompt box, as shown below:
3. Click **Install** and wait for the remote desktop service installation to complete.

**Configuring multi-user remote login to instance**

1. Use VNC to log in to Windows CVM.

2. In the operating system interface, click ![VNC icon] to open the Windows PowerShell window.

3. In the Windows PowerShell window, enter `gpedit.msc` and press **Enter** to open the **Local Group Policy Editor**.

4. In the left navigation tree, select **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host** >
Connections, and double click **Limit number of connections**, as shown below:

5. In the **Limit number of connections** window that pops up, select **Enabled**, and enter the maximum number of simultaneous remote users in **RD Maximum Connections allowed**, as
shown below:

6. Click **OK**.

7. In the left navigation tree, select **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections**, and double click **Restrict Remote Desktop Services users to a single Remote**
**Desktop Services session**, as shown below:

8. In the “Restrict Remote Desktop Services users to a single Remote Desktop Services session” window that pops up, select **Disabled**, and click **OK**, as shown below:
9. Close local group policy editor.

0. Restart the instance.
Configure Linux CVM to Boot into Single User Mode

Last updated: 2020-03-06 12:17:33

Scenario

Linux users sometimes need to boot into single user mode to perform special operations, such as password management or sshd repair. This article describes how to boot into single user mode in common Linux distributions.

Directions

Determining your Linux distribution

Different distributions of Linux use different methods to boot into single user mode, so be sure to follow the instructions for your Linux distribution.

- Process for CentOS 6.
- Process for CentOS 7.
- Process for Ubuntu.

CentOS 6

CentOS 6 uses GRUB. The following process uses CentOS 6.9 as an example. Specific steps may vary slightly depending on the version of the operating system.

1. Log in to the CVM.
2. Run the following command to open `/etc/grub.conf`.
   
   `vi /etc/grub.conf`

3. Press `i` to enter edit mode.
4. Find “GRUB_TIMEOUT”, the waiting time before the default entry is booted, and modify its value based on your needs.
   
   The default value of “GRUB_TIMEOUT” is 5 seconds. In order to avoid missing the boot interface because the waiting time is too short, we recommend you change it to 60s or longer.
This setting affects the system start time. After you complete the tasks that require single user mode, change it back to the default value.

5. Press **Esc** to exit edit mode, enter **:wq** and press **Enter** to save your file and exit the VI editor.

6. Run the following command to reboot the server.

```
reboot
```

7. Wait for one minute and use VNC to log into your CVM instance, as shown below:

8. Press any key to enter the menu shown below:
9. Press **e** to enter the kernel editing page and enter **single**, as shown below:

![kernel editing page]

0. Press **Enter**, as shown below:

```
dracut: Switching root
Welcome to CentOS
Starting udev: [ OK ]
Setting hostname VM_204_43_centos: [ OK ]
Setting up Logical Volume Management: [ OK ]
Checking filesystems
/dev/vda1: clean, 29486/3276800 files, 462445/13106775 blocks [ OK ]
Remounting root filesystem in read-write mode: [ OK ]
Mounting local filesystems: [ OK ]
Enabling local filesystem quotas: [ OK ]
Enabling /etc/fstab swaps: [ OK ]
growroot: NOCHANGE: partition 1 is size 104854207. it cannot be grown
Welcome to CentOS
Starting udev: [ OK ]
Setting hostname VM_204_43_centos: [ OK ]
Setting up Logical Volume Management: [ OK ]
Checking filesystems
/dev/vda1: clean, 29486/3276800 files, 462445/13106775 blocks [ OK ]
Remounting root filesystem in read-write mode: [ OK ]
Mounting local filesystems: [ OK ]
Enabling local filesystem quotas: [ OK ]
Enabling /etc/fstab swaps: [ OK ]
[root@VM_204_43_centos ~]# _
```
1. In the interface shown below, press `b` to enter single user mode.

![Grub Interface](image)

2. Run the following command to exit single user mode.

   ```
   exec /sbin/init
   ```

**CentOS 7**

Unlike CentOS 6, CentOS 7 and above use GRUB 2. The following process uses CentOS 7.5 as an example. Specific steps may vary slightly depending on the version of the operating system.

1. Log in to the CVM.
2. Run the following command to open `/etc/default/grub`.

   ```
   vi /etc/default/grub
   ```

3. Press `i` to enter edit mode.
4. Find “GRUB_TIMEOUT”, the default boot item wait time, and modify its value based on your needs, as shown below:

   ```
   The default value of “GRUB_TIMEOUT” is 5 seconds. In order to avoid missing the boot interface because the waiting time is too short, we recommend you change it to 60s or longer.
   ```
This setting affects the system start time. After you complete the tasks that require single user mode, change it back to the default value.

```
GRUB_DEFAULT=saved
GRUB_TIMEOUT=5
GRUB_TERMINAL=serial
GRUB_TERMINAL_CONPTY=serial
GRUB_CMDLINE_LINUX="crashkernel=auto console=ttyS0 console=tty0 panic=5 net.ifnames=0 biosdevname=0"
GRUB_DISABLE_RECOVERY=true
GRUB_SERIAL_COMMAND="serial --speed=9600 --unit=0 --word=8 --parity=no --stop=1"
```

5. Press **Esc** to exit edit mode, enter **:wq** and press **Enter** to save your file and exit the VI editor.

6. Run the following command to recompile and generate **grub.cfg**.

   ```
   grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

   The following appears:

   ```
   * Socket connection established *
   Last login: Mon Feb 25 16:37:51 2019
   [root@VM_204_43_centos ~]# grub2-mkconfig -o /boot/grub2/grub.cfg
   Generating grub configuration file ...
   Found linux image: /boot/vmlinux-3.10.0-862.el7.x86_64
   Found initrd image: /boot/initramfs-3.10.0-862.el7.x86_64.img
   Found linux image: /boot/vmlinux-0-rescue-c28d40cb5c4e3adcb4e3d29799e77b39e
   Found initrd image: /boot/initramfs-0-rescue-c28d40cb5c4e3adcb4e3d29799e77b39e.img
   done
   [root@VM_204_43_centos ~]#
   ```

7. Run the following command to reboot the server.

   ```
   reboot
   ```
8. Wait for one minute and use VNC to log into your CVM instance, as shown below:

![Wait for one minute and use VNC to log into your CVM instance](image)

9. Press **e** to enter the kernel editing interface and add `init=/bin/sh` to the red box area as shown below:

```
inmod part_msdos
inmod ext2
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
   search --no-floppy --fs-uuid --set-root --hint='hd0,msdos1' Z1dfe03\
   0-aa71-4b3a-8610-3b942dd447fa
else
   search --no-floppy --fs-uuid --set-root Z1dfe030-aa71-4b3a-8610-3b94\
   447fa
fi
linux16 /boot/vmlinux-3.10.0-862.el7.x86_64 root=UUID=Z1dfe030-aa71-4b\
3a-8610-3b942dd447faro crashkernel=auto console=ttyS0 console=tty0 panic=5 new\
t.ifnames=0 biosdevname=0 init=/bin/sh
initrd16 /boot/initramfs-3.10.0-862.el7.x86_64.img
```

Press **Ctrl-x** to start, **Ctrl-c** for a command prompt or Escape to discard edits and return to the menu. Pressing **Tab** lists possible completions.
0. Press `Ctrl+X` to start and enter single user mode, as shown below:

```
[ OK ] Reached target Initrd Default Target.
[ OK ] Started dracut pre-pivot and cleanup hook...
[ OK ] Started dracut pre-pivot and cleanup hook.
Starting Cleaning Up and Shutting Down Daemons...
Starting Plymouth switch root service...
[ OK ] Stopped target Timers.
[ OK ] Stopped Cleaning Up and Shutting Down Daemons.
[ OK ] Stopped dracut pre-pivot and cleanup hook.
Stopping dracut pre-pivot and cleanup hook...
[ OK ] Stopped dracut initqueue hook.
Stopping dracut initqueue hook...
[ OK ] Stopped target Initrd Default Target.
[ OK ] Stopped target Basic System.
[ OK ] Stopped target System Initialization.
[ OK ] Stopped Apply Kernel Variables.
Stopping Apply Kernel Variables...
Stopping udev Kernel Device Manager...
[ OK ] Stopped udev Coldplug all Devices.
Stopping udev Coldplug all Devices...
[ OK ] Stopped target Swap.
[ OK ] Stopped target Sockets.
[ OK ] Stopped target Slices.
[ OK ] Stopped target Paths.
[ OK ] Stopped udev Kernel Device Manager.
[ OK ] Stopped dracut pre-udev hook.
Stopping dracut pre-udev hook...
[ OK ] Stopped dracut cmdline hook.
Stopping dracut cmdline hook...
[ OK ] Stopped Create Static Device Nodes in /dev.
Stopping Create Static Device Nodes in /dev...
[ OK ] Stopped Create list of required static device nodes for the current kernel.
Stopping Create list of required static device nodes for the current kernel...
[ OK ] Closed udev Control Socket.
[ OK ] Closed udev Kernel Socket.
Starting Cleanup udevd DB...
[ OK ] Started Cleanup udevd DB.
[ OK ] Reached target Switch Root.
[ OK ] Started Plymouth switch root service.
Starting Switch Root...
```

1. Run the following command to exit single user mode.

```
exec /sbin/init
```

**Ubuntu**

The following process uses Ubuntu 16.04 as an example. Specific steps may vary slightly depending on the version of the operating system.
1. Log in to the CVM.
2. Run the following command to open `/etc/default/grub`.
   ```
   sudo vi /etc/default/grub
   ```
3. Press `i` to enter edit mode.
4. Find “GRUB_TIMEOUT”, the default boot item wait time, and modify its value based on your needs, as shown below:
   The default value of “GRUB_TIMEOUT” is 5 seconds. In order to avoid missing the boot interface because the waiting time is too short, we recommend you change it to 60s or longer.
   ```
   GRUB_TIMEOUT=120
   ```
   - This setting affects the system start time. After you complete the tasks that require single user mode, change it back to the default value.
   - The default account in Ubuntu is not `root`. Use `sudo` instead.
5. Press `Esc` to exit edit mode, enter `:wq`, and press `Enter` to save your file and exit the VI editor.
6. Run the following command to recompile and generate `grub.cfg`.
   ```
   sudo update-grub
   ```
7. Run the following command to reboot the server.

```
    sudo reboot
```

8. Wait for one minute and use VNC to log into your CVM instance, as shown below:

9. Press `e` to enter the kernel editing interface and add `rw single init=/bin/bash` to the red box area as shown below:
GNU GRUB version 2.02~beta2-36ubuntu3.1

insmod ext2
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root 971546b4-fe6b-4f81-9cbb-9186ff0454ea
else
  search --no-floppy --fs-uuid --set=root 971546b4-fe6b-4f81-9cbb-9186ff0454ea
fi
linux /boot/vmlinux-4.4.0-130-generic root=UUID=971546b4-fe6b-4f81-9cbb-9186ff0454ea ro nvt.ifnames=0 biosdevname=0 console=ttys0.11520
console=tty0 panic=5 crashkernel=auto crashkernel=304M-128M rw single i
init=/bin/bash
initrd /boot/initrd.img-4.4.0-130-generic

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the GRUB menu.
0. Press **Ctrl+X** to start and enter single user mode, as shown below:

```bash
[ 1.146972] lvm: raid6 personality registered for level 6
[ 1.146972] Begin: 216808g raid6: sse2x1 -> gen(1) 11264 MB/s r personality registered for level -1
[ 1.129400] raid6: sse2x1 -> gen(1) 13786 MB/s e el -4
[ 1.325300] raid6: sse2x2 -> gen(0) 13786 MB/s 2
[ 1.420977] raid6: sse2x4 -> gen(0) 16040 MB/s r personality registered for level -1
[ 1.556800] raid6: sse2x4 -> gen(0) 111193 MB/s e el -4
[ 1.624900] raid6: aux2x1 -> gen(0) 21633 MB/s
[ 1.692379] raid6: aux2x4 -> gen(0) 25297 MB/s
[ 1.760606] raid6: aux2x4 -> gen(0) 28763 MB/s
[ 1.760537] raid6: using algorithm aux2x4 gen(0) 28763 MB/s
[ 1.761279] raid6: using aux2x2 recovery algorithm
[ 1.691313] tsc: Refine TSC clocksource calibration: 3199.996 MHz
[ 1.762751] clocksource: tsc: mask: 0xffffffffffffffff max_cycles:a0x2e2046fd56,dmax_idle_ns:4407
[ 1.765533] xor: automatically using best checksumming function:
[ 1.804865] aux : 31847.000 MB/sec
[ 1.886366] async_tx: api initialized (async) 3
[ 1.816407] md: raid6 personality registered for level 6
[ 1.771707] raid5 personality registered for level 6
[ 1.819916] md: raid4 personality registered for level 4
[ 1.824566] async_tx10 personality registered for level 10

done.

Begin: Running /scripts/init-premount ... done.

Begin: Running /scripts/local-top ... done.

Begin: Running /scripts/local-premount ... done.

Begin: Mounting root file system ... done.

Begin: Running /scripts/local-bottom ... done.

Begin: Scanning for Btrfs filesystems ... done.

Begin: Will now check root file system: fsck from util-linux 2.27.1 ... done.

fsck: error 2 (No such file or directory) while executing fsck.ext4 for /dev/odai1

fsck exited with status code 8

56, max_idle_ns: 4407

done.

Warning: File system check failed but did not detect errors.

[ 6.991228] EXT4-fs (odai1): mounted filesystem with ordered, data mode.

Warning: Overly fast process group (-1): Insufficient ioct1 for device

bash: cannot set terminal process group (id -1): Insufficient ioct1 for device

bash: no job control in this shell

done.

root@(none):/#
Modifying the Default Remote Port of CVM

Scenario

The default port of the CVM is susceptible to scanning and attack by malicious software. Therefore, you need to change the default remote port of the CVM to a less common port to prevent the inability to remotely access the CVM due to such attacks. This ensures the security of the CVM.

Modifications to the port will be valid only if they are made in the security group rules and the CVM simultaneously. You can modify the default remote port of the CVM as described below. The modification method varies based on the operating system of the CVM.

- Modifying the default remote port of a Windows CVM
- Modifying the default remote port of a Linux CVM

Directions

Modifying the default remote port of a Windows CVM

The following operations use Windows Server 2012 as an example. The procedure might vary slightly depending on the operating system and language.

1. Log in to the Windows instance by using VNC.
2. In the operating system, click to open the “Windows PowerShell” window.
3. In the “Windows PowerShell” window, enter regedit and press Enter to open the “Registry Editor” window.
4. In the left-side registry navigation pane, expand the following hierarchies in sequence:
   - HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Terminal Server > Wds > rdpwd > Tds > tcp.
5. Find PortNumber in tcp. Then, change the value of PortNumber from 3389 to an unoccupied port number within the range of 0 to 65535, as shown in the following figure.
6. In the left-side registry navigation pane, expand the following hierarchies in sequence:

HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Terminal Server > Win Stations > RDP-Tcp.
7. Find and change PortNumber in **RDP-Tcp** to be the same as that in **tcp**.

8. (Optional) If a firewall is enabled for your CVM, be sure to add the new port to the whitelist of the firewall and set to allow connection.
   i. In the “Windows PowerShell” window, enter `wf.msc` and press **Enter** to open the “Windows Firewall with Advanced Security” window.
   ii. In the “Windows Firewall with Advanced Security” window, select **Inbound Rules** and click **New rule**, as shown in the following figure.
   iii. On the “Rule Type” page in the “New Inbound Rule Wizard” window, select **Port** and click **Next**.
   iv. On the “Protocol and Ports” page in the **New Inbound Rule Wizard** window, select **TCP** and enter the port number set in **Step 5** in **Specific Port**. Then, click **Next**, as shown in the
v. On the **Action** page in the “New Inbound Rule Wizard” window, select **Allow connections** and click **Next**.

vi. On the “Profile” page in the “New Inbound Rule Wizard” window, apply the default profile and click **Next**.

vii. On the “Name” page in the “New Inbound Rule Wizard” window, enter the rule name and click **Finish**.

9. In the “Windows PowerShell” window, enter `services.msc` and press **Enter** to go to the “Services” window.

0. Find and right-click **Remote Desktop Services** in the “Services” window. Then, select **Restart** to restart the remote login service.

1. Refer to **Modifying Security Group Rules** to modify the security group rule with the protocol port “TCP:3389” by changing the port number to that set in **Step 5**.
Modifying the default remote port of a Linux CVM

- Before you modify the default remote port, we recommend that you add the SSH port number and test whether the port is successfully connected to the CVM. Then, delete the default port 22. Ensure that the default port 22 cannot be connected to the CVM when the new port fails to connect to the CVM.
- The following operations use CentOS 7.3 as an example. The specific operations vary slightly according to the version and language of the operating system.

1. Log in to a Linux instance by using VNC.
2. Run the following command to modify the configuration file:
   ```bash
touch -r /etc/ssh/sshd_config
```
3. Press `i` to switch to the editing mode and add a new port. Add `Port x` (where x is the port number of the new port) in a new row below `#Port 22`, and delete `#` to comment off `Port 22`, as shown in the following figure.
   For example, add `Port 23456` in the row.

   ```bash
   # If you want to change the port on a SELinux about this change.
   # semanage port -a -t ssh_port_t -p tcp
   # Port 22
   Port 23456
   #AddressFamily any
   
   # If you want to change the port on a SELinux about this change.
   # semanage port -a -t ssh_port_t -p tcp
   # Port 22
   Port 23456
   #AddressFamily any
   
   # If you want to change the port on a SELinux about this change.
   # semanage port -a -t ssh_port_t -p tcp
   # Port 22
   Port 23456
   #AddressFamily any
   
   # If you want to change the port on a SELinux about this change.
   # semanage port -a -t ssh_port_t -p tcp
   # Port 22
   Port 23456
   #AddressFamily any
   ```
4. Press `Esc`, enter `:wq`, and save the change.
5. Run the following command so that the new configuration takes effect:
   ```bash
   systemctl restart sshd.service
   ```
6. Configure the firewall.
By default, the iptables service is used as the firewall for Linux CVMs with CentOS earlier than CentOS 7. Configure the firewall as follows if iptables rules have been configured for the CVM.

a. Run the following command to configure the firewall:

```
iptables -A INPUT -p tcp --dport <New port number> -j ACCEPT
```

For example, if the new port number is 23456, run the following command:

```
iptables -A INPUT -p tcp --dport 23456 -j ACCEPT
```

b. Run the following command to restart the firewall:

```
service iptables restart
```

The Firewalld service is used as the firewall for Linux CVMs with CentOS 7 or later. Configure the firewall as follows if the Firewalld service has been enabled on the CVM.

Run the following command to allow access by the port number added in Step 3:

```
firewall-cmd --add-port=<New port number>/tcp --permanent
```

For example, if the new port number is 23456, run the following command:

```
firewall-cmd --add-port=23456/tcp --permanent
```

If success is returned, the port was successfully configured.

7. Refer to Modifying Security Group Rules to modify the security group rule with the protocol port “TCP:22” by changing the port number to that set in Step 3.

### Verification

#### Windows CVMs

1. Assume that the Windows operating system is installed on the local computer. Open the “Remote Desktop Connection” dialog box.
2. Enter the Internet IP of Windows server: port number after modification after Computer and click Connect, as shown in the following figure.

3. Enter the admin account and password as prompted and click OK.
If the operating system interface of the Windows CVM appears, the connection is established.

If you log in to the Windows CVM by using an RDP file, modify the full address:s parameter in the RDP file, as shown in the following figure:

Linux CVMs

1. Assume that PuTTY is used for remote login. Start the PuTTY client.
2. In the “PuTTY Configuration” window, enter the public IP address of the Linux CVM, set Port to the new port number, and click Open, as shown in the following figure.
3. Enter the username and password of the Linux CVM as prompted and press **Enter**.
   If the following output appears, the connection is established.

   ![Putty Configuration](Image)

4. After using the new port to successfully establish a connection to the Linux CVM, run the following command:

   ```bash
   vim /etc/ssh/sshd_config
   ```

5. Press **i** to switch to the editing mode, and add `#` in front of `Port 22` to comment off the port.
6. Press **Esc**, enter `:wq`, and save the change.
7. Run the following command so that the new configuration takes effect. Ensure that you use the new port for the next remote login to the Linux CVM.

   ```bash
   systemctl restart sshd.service
   ```
Allow CVMs without Internet access to access Internet

Scenario

If you choose 0 Mbps bandwidth for a purchased CVM, this CVM will unable to access the public network. This document uses CentOS 7.5 as an example to describe how a CVM without a public IP address can access the public network by connecting to a CVM with a public IP address through a PPTP VPN.

Prerequisites

- Two CVMs in the same VPC instance have been created. One CVM does not have a public IP address and the other has a public IP address.
- The private IP address of the CVM with a public IP address has been obtained.

Directions

Configuring PPTP on the CVM with a public IP address

1. Log in to the CVM with a public IP address.
2. Run the following command to install PPTP:
   
   ```
   yum install -y pptpd
   ```
3. Run the following command to open the `pptpd.conf` configuration file:
   
   ```
   vim /etc/pptpd.conf
   ```
4. Press i to switch to the editing mode and append the following code to the file.
   
   ```
   localip 192.168.0.1
   remoteip 192.168.0.234-238,192.168.0.245
   ```
5. Press Esc, enter `:wq`, and save and close the file.
6. Run the following command to open the `/etc/ppp/chap-secrets` configuration file:
vim /etc/ppp/chap-secrets

7. Press i to switch to the editing mode and append the username and password for connecting to PPTP in the following format to the file.

```
<User name> pptpd <Password> *
```

For example, if the username and password for connecting to PPTP are root and 123456 respectively, append the following code:

```
root pptpd 123456 *
```

8. Press Esc, enter :wq, and save and close the file.

9. Run the following command to start the PPTP service:

```
systemctl start pptpd
```

0. Run the following commands in sequence to enable forwarding:

```
echo 1 -> /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.0.0/24 -j MASQUERADE
```

**Configuring PPTP on the CVM without a public IP address**

1. Log in to the CVM without a public IP address.
2. Run the following command to install a PPTP client:

```
yum install -y pptp pptp-setup
```

3. Run the following command to create a configuration file:

```
pptpsetup --create <Configuration file name> --server <Private IP address of the CVM with a public IP address> --username <Username for connecting to PPTP> --password <Password for connecting to PPTP> --encrypt
```

For example, if you have obtained the private IP address 10.100.100.1 of the CVM with a public IP address, run the following command to create a test configuration file:

```
pptpsetup --create test --server 10.100.100.1 --username root --password 123456 --encrypt
```

4. Run the following command to connect to PPTP:

```
pppd call test (the file name created in step 3)
```

5. Run the following command to set routes:
Checking whether the configuration is successful

Run the following command on the CVM without a public IP address to ping any external network address and check whether it can be pinged through:

```
ping -c 4 <External network address>
```

If a result similar to the following is returned, the configuration was successful:

```
root@CVM_1_145_centos ~]# ping -c 4 www.cloud.tencent.com
PING cloud-gz.tencent-cloud.com (139.199.215.179) 56(84) bytes of data.
64 bytes from 139.199.215.179 (139.199.215.179): icmp_seq=1 ttl=54 time=32.0 ms
64 bytes from 139.199.215.179 (139.199.215.179): icmp_seq=2 ttl=54 time=32.1 ms
64 bytes from 139.199.215.179 (139.199.215.179): icmp_seq=3 ttl=54 time=32.2 ms
64 bytes from 139.199.215.179 (139.199.215.179): icmp_seq=4 ttl=54 time=32.4 ms

--- cloud-gz.tencent-cloud.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 12047ms
rtt min/avg/max/mdev = 32.064/32.238/32.497/0.273 ms
```