Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

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

Service Statement

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

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
  Linux system uploads files to CVM via FTP
  Uploading files via WinSCP to a Linux CVM from Windows
  Uploading files via FTP to a CVM from Windows
  Upload Files via SCP
  Uploading files via MSTSC to a Windows CVM from Windows
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
  Commands for First Launching
  Commands for First Launching
System-related
  Activate Windows License
  System Updates
  Closean CVM
  Power Management Configuration
  Windows Recovery Mode
  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
- Modify Cloud Virtual Machine remote default port
- Allow CVMs without Internet access to access Internet
Ops Guide
Mount Data Disks
Format and Mount Data Disks
Last updated: 2018-08-06 15:39:45

Note:

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

Manual Formatting and Mounting Data Disk

Format and mount a data disk by following the steps below.

Note:

- When executing the following commands, remember to modify the data disk drive letter. The drive letter is \texttt{vdb} in this example.

Step 1: Format the data disk

Note:

When formatting partitions, developers can decide the file system format on their own, such as \texttt{ext3} and \texttt{ext4}. \texttt{ext4} is used in this example.

Format the data disk by performing the \texttt{mkfs} command:

\begin{verbatim}
mkfs.ext4 /dev/vdb
\end{verbatim}

Step 2: Mount the data disk
1. Create a mount point - data directory:

```shell
mkdir /data
```

2. Mount new partitions:

```shell
mount /dev/vdb /data
```

3. Verify whether the data disk is mounted successfully:

```shell
df -h
```

The following message indicates that it is mounted successfully (i.e. the data disk is mounted on the Linux CVM):

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Size</th>
<th>Used</th>
<th>Avail</th>
<th>Use%</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/vdb</td>
<td>50G</td>
<td>53M</td>
<td>47G</td>
<td>1%</td>
<td>/data</td>
</tr>
</tbody>
</table>

**Step 3: Enable auto mount upon launch**

Add the data disk mount information to `/etc/fstab` to enable auto mount upon launch.

To allow your CVM to be automatically mounted with data disk when it is restarted or launched, add the mount information to `/etc/fstab`. Otherwise, the data disk cannot be automatically mounted to the CVM when the CVM is restarted or launched.

1. Execute the following command to add partition information:

```shell
echo '/dev/vdb /data ext4 defaults 0 0' >> /etc/fstab
```

2. Execute the following command to view the partition information:

```shell
cat /etc/fstab
```

The following message indicates that the data disk mount information is added successfully.

```shell
/dev/vdb /data ext4 defaults 0 0
```

**Auto Formatting and Mounting Data Disk**
You can format and mount a data disk on Tencent Cloud Linux CVM by running the following Shell script:

```bash
#!/bin/bash

type=ext4
mount_dir=/data

mkfs.$type /dev/vdb
mkdir -p $mount_dir

echo "/dev/vdb $mount_dir $type defaults 0 0" >> /etc/fstab

mount -a
```
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:

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:

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:
Scenario

Windows's file system usually uses the NTFS or FAT32 format, while Linux's file system usually uses the EXT series format. Although the type of Cloud Virtual Machine operating system has changed from Windows Reinstall to Linux, operating system, the data disk in Cloud Virtual Machine is still in the format used by the original system. Therefore, Cloud Virtual Machine after Reinstall system may not be able to Access data disk file system. This document guides you to read the data disk data under the original Windows system on the Linux Cloud Virtual Machine behind the Reinstall system.

Directions

Configure the Linux system to support NTFS

1. Linux Cloud Virtual Machine after logging in to Reinstall's system.
2. Execute the following command to install the ntfsprogs software so that Linux Cloud Virtual Machine supports the Access NTFS file system.

```
yum install ntfsprogs
```

Mount the data disk under Windows Cloud Virtual Machine to Linux Cloud Virtual Machine

1. Log in to the CVM Console .

If the data disk under your Windows Cloud Virtual Machine has been mounted to Linux Cloud Virtual Machine, you can skip this operation.

This paper takes CentOS system as an example. Different types of Linux system installation commands are different, please use the corresponding installation commands to install.
2. In Left sidebar, click [Cloud Block Storage], go to the HDD cloud disk management page.

3. Select the Windows data disk to be mounted, and click "more"->"Mount".

4. In the pop-up "Mount to instance" window, select the Linux Cloud Virtual Machine you want to mount to, and click "OK".

5. Log in to the Linux Cloud Virtual Machine that has mounted the Windows data disk.

6. Execute the following command to view the data disk mounted from Windows Cloud Virtual Machine.

```bash
parted -l
```

A message similar to the one below is 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. Execute the following command to mount the data disk.

```bash
mount -t ntfs-3g Data disk path mount point
```

For example, you need to set the path to `/dev/vdb1` The data disk is mounted to the `/mnt` Execute the following command

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

Because the file system is recognizable at this time, the mounted data disk can be read and written directly by the Linux system.
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@UM_2_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 UM_2_9_centos UM_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 UM_2_9_centos UM_2_9_centos
::1 localhost.localdomain localhost
::1 localhost6.localdomain6 localhost6
```

**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

Last updated : 2020-03-06 16:31:33

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.

   ```bash
   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:
     ```bash
     sudo apt-get install acpid
     ```

   - For Redhat or CentOS:
     ```bash
     yum install acpid
     ```

   - For SUSE:
     ```bash
     in apcid
     ```
Copy Local Files to CVMs

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

Last updated: 2020-03-06 12:05:13

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.*

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 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:

![CVM Console](image-url)

###. Installing rdesktop.

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

   ```
   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.

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

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

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

```
rdesktop
```

### Uploading Files

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

```
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`.

```
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.
Linux system uploads files to CVM via FTP

Scenario

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

Prerequisites

The FTP service has been set up on the CVM.

Directions

Connecting to the CVM

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

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

   ```
   yum -y install ftp
   ```

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

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

```
[root@VM_0_118_centos ~]# ftp 1.1.1.1.
Connected to 1.1.1.1 (1.1.1.1).
220 Microsoft FTP Service
Name (1.1.1.1: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”.

©2013-2019 Tencent Cloud. All rights reserved.
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 via FTP to a CVM from Windows


Scenario

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

Prerequisites

The FTP service has been built on the CVM.

Procedure

Connecting to the CVM

1. Download and install FileZilla locally.

   If you use FileZilla 3.5.3 to upload files through FTP, the upload may fail. We recommend that you download FileZilla 3.5.1 or 3.5.2 from the official website.

2. Open FileZilla.
3. In the FileZilla window, complete the host, username, password, and port information, and click Quickconnect.

   Configuration description:
   
   - **Host**: indicates the public IP address of the CVM. To view the public IP address of the CVM, log in to the CVM console and navigate to the instance management page.
   - **Username**: indicates the FTP user account configured when you set up the FTP service. Here, "ftpuser1" is used as an example.
   - **Password**: indicates the password of the FTP user account configured when you set up the FTP service.
Port: indicates the FTP listening port, which is port 21 by default. After the connection is successfully established, you can view files on the remote CVM site.

**Uploading a file**

In the "Local site" window in the lower-left corner, right-click the local file to be uploaded and choose **Upload** to upload it to the Linux CVM.

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

**Downloading a file**

In the "Remote site" window in the lower-right corner, right-click the CVM file to be downloaded and choose **Download** to download it to a local directory.
Upload Files via SCP

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.

   ```
   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:

   ```
   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.

   ```bash
   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/lnmp0.4.tar.gz` from the CVM whose public IP is 129.20.0.2 to the corresponding local directory, please execute the following command:

   ```bash
   scp root@129.20.0.2:/home/lnmp0.4.tar.gz /home/lnmp0.4.tar.gz
   ```
Uploading files via MSTSC to a Windows CVM from Windows

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.

- Address for public network access: [http://mirrors.cloud.tencent.com/](http://mirrors.cloud.tencent.com/)
- Address for private network access: [http://mirrors.tencentyun.com/](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 Source 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>
  http://mirrors.tencentyun.com/nexus/repository/maven-public/
</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 above supports Docker Hub Mirror mechanism. If you have not installed Docker 1.3.2 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 operating systems and versions may vary:
  1. Execute the following command to open the configuration file of `/etc/default/docker`.

```
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 configuration file of /etc/sysconfig/docker.

```bash
vim /etc/sysconfig/docker
```

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

```bash
OPTIONS='--registry-mirror=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
```

ii. Restart Boot2Docker.

## Accelerating MariaDB using Tencent Cloud image

The following steps takes CentOS 7 as an example. 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.

```ini
# 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.

```bash
yum clean all
```

4. Execute the following command to install MariaDB.
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 `MariaDB.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.

   ```
   [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 install -y mongodb-org
   ```

Use Tencent Cloud MongoDB on CVMs with Debian system

1. Based on Debian versions, execute the following commands 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
   echo "deb http://mirrors.cloud.tencent.com/mongodb/apt/debian/stretch/mongodb-org/4.0 main" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.0.list
   ```

3. Execute the following command to update software package list.
4. Execute the following command to install MongoDB.

```bash
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.

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

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

```bash
#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.

```bash
sudo apt-get update
```

4. Execute the following command to install MongoDB.

```bash
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.

```bash
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: 2020-02-25 12:12:27

Scenario
In order to improve the efficiency of software installation on Cloud Virtual Machine and reduce the cost of downloading and installing software, Tencent Cloud provides a source of Apt-get download. In Ubuntu environment, users can quickly install software through Apt-get. For the Apt-get download source, you do not need to add a software source, you can install the software package directly.

Prerequisites
Cloud Virtual Machine, who has logged in to the operating system Ubuntu.

Directions
The following action takes installing Nginx as an example.

View installable software
Execute the following command to view the software that can be installed.

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

Installing software
4. Run the following command to install Nginx.

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

After confirming that the software information is correct, type `Y` Agree to the installation and wait until the software installation is complete as shown below:
View installed software information

According to the actual requirements, execute different commands to view the installed software information.

- Execute the following command to view the Directory where the package is located and all the files in the package.

  ```bash
  sudo dpkg -L Software name
  ```

- Execute the following command to view the version information of the package.

  ```bash
  sudo dpkg -l Software name
  ```

View installed Nginx information. as shown below:
Install Software via YUM under CentOS Environment

Last updated : 2020-02-25 12:04:35

**Scenario**

In order to improve the efficiency of software installation on Cloud Virtual Machine and reduce the cost of downloading and installing software, Tencent Cloud provides a source of YUM download. In the CentOS environment, users can use the `yum` command to quickly install the software. For YUM download sources, users do not need to add software sources and can install software packages directly.

**Directions**

**Installing software**

1. Log in to Cloud Virtual Machine with your root account.
2. Execute the following command to install the software.

```
yum install Software name
```

During the process of installing the software, the system will automatically search for the relevant software packages and dependencies, and prompt the user in the interface to confirm whether the searched software packages are appropriate.

For example, you execute `yum install PHP` Command, after installing PHP, the interface is shown as follows:
4. After confirming that the software package is correct, enter **y**, billed by **Enter** To start installing the software

**Interface hint Complete The installation is complete.** as shown below:

```
4. After confirming that the software package is correct, enter **y**, billed by **Enter** To start installing the software

**Interface hint Complete The installation is complete.** as shown below:

```

```
```

**View information about installed software**

After the software installation is completed, you can execute different commands and view the information according to the actual requirements.

- **Execute the following command to view the specific installation of the package Directory.**

  ```bash
  rpm -ql Software name
  ```

For example, you execute **rpm -ql php** Command, check the specific installation of PHP Directory. as shown below:
Execute the following command to view the version information of the package.

```
rpm -q
```

For example, you execute `rpm -q php` Command **to view the version information** of PHP, as shown below:

```
[root@VM_5_10_centos ~]# rpm -q php
php-5.4.16-46.el7_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 before installing the necessary software.

1. Configuration of nginx

1) Start nginx service

Start the nginx 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 --.0 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:

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

Write the following:

```
[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:

```
/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
Starting MySQL
done
Starting php-fpm
done
Starting nginx Checking for service nginx
running
done
```

4. Environment configuration validation

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

```
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

Commands for First Launching

Last updated : 2019-08-07 12:07:10

When launching a CVM instance for the first time, you can pass user data to the CVM by passing a text (with no format restriction) and execute the text. This document uses Linux CVM as an example to describe how to output "Hello Tencent Cloud" by passing a Shell script when launching the CVM for the first time. The log file (/var/log/cloud-init-output.log) output by Cloud-init catches the output of the console.

Notes

- A command can be executed by passing a text only on the first time of launching a CVM.
- The passed text must be encoded with Base64. **Please encode in Linux environment to avoid format incompatibility.
- The text, which is input as the user data, is executed using the root permission. Therefore, sudo command is not required in the script. Note: All the files you created belong to root. If you need to grant non-root users with the access permission, modify the corresponding permission in the script.
- Adding these tasks to the startup of the CVM will increase its startup time. Wait a few minutes until the tasks complete, and then test whether they are executed successfully.
- In this example, Shell script must start with `#!/bin/bash` and the path directing to the interpreter of the script to be read.

Step 1: Write Shell script

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

**Note:**
Shell script must start with `#!/bin/bash` and the path directing to the interpreter of the script to be read. For more information on Shell script, please see BASH Programming of the Linux Documentation Project (tldp.org).
Step 2: Encode the script file with Base64

**Note:**
Please encode in Linux environment to avoid format incompatibility.

Suppose that the script file you created in step 1 is script_text. You can encode the file using Base64 command in Linux environment, as shown below:

```
# Encode the file with Base64
base64 script_text

# The encoded result:
IyEvYmluL2Jhc2g2gKCMVjaG8gNldlbGNvbWUgVG8gVGVuY2VudCBDbG91ZC4iCg==
```

```
# Decode the returned result with Base64 and verify whether it is the command to be executed.
echo "IyEvYmluL2Jhc2g2gKZNobyAiSGVsbG8gVGVuY2VudCBDbG91ZC4iCg==" | base64 -d
```

Step 3: Pass the text

We provide multiple methods to launch an instance and here we introduce two of them. Please choose a method as needed:

**Passing on the official website or the console**

When you create a CVM on the official website or the console, select **Advanced Configuration** in 4. **Set Security Group and CVM** step. Enter the encoded result (IyEvYmluL2Jhc2g2gKCMVjaG8gNldlbGNvbWUgVG8gVGVuY2VudCBDbG91ZC4iCg== in this example) of step 2 in user defined data item. Finish the creation and launch the CVM.

Tencent Cloud CVM executes the script using the open-source software cloud-init. For more
information on cloud-init, please see [cloud-init's official website](#).

### Passing via API

When creating a CVM via API, you can pass the text by assigning the value of the encoded result of step 2 to UserData parameter of RunInstances API. The following is an example of the parameter of CVM creation request with UserData.

```plaintext
https://cvm.tencentcloudapi.com/?Action=RunInstances
&Version=2017-03-12
&Placement.Zone=ap-guangzhou-2
&ImageId=img-pmqg1cw7
&UserData=IyEvYmluL2Jhc2gKCmVjaG8gIldlbGNvbWUgVG8gVG8gVGVuY2VudCBDbG91ZC4iCg==
&<Common request parameters>
```
Commands for First Launching

Last updated: 2020-02-25 12:16:09

Scenario

When you create Cloud Virtual Machine, you can specify custom data to configure the instance. When Cloud Virtual Machine launches for the first time, the custom data is passed to Cloud Virtual Machine as text and the text is executed. If you buy more than one Cloud Virtual Machine at a time, the custom data will run the text when all Cloud Virtual Machines first launch. This paper takes Windows Cloud Virtual Machine's first launch as an example by passing a script in PowerShell format.

Considerations

- Windows operating systems that support custom data include:
  - Windows Server 2012 R2 data center 64-bit English version
  - Windows Server 2012 R2 DataCenter 64-bit Chinese
- Only for the first time, launch and Cloud Virtual Machine, execute the order by passing the text.
- Before Base64 encoding, custom data content cannot exceed 16KB.
- Custom data is passed through Base64 encoding. If you copy a non-base64 script file directly, please uncheck [enter as base64 format text].
- In launch, executing job specified in the custom data will increase the time required for launch's server. It is recommended that you wait a few minutes and test whether job has been successfully executed after job has finished.
- In this example, use the PowerShell tag to specify the Windows PowerShell script, for example <Powershell></powershell> Tags.

Directions

Prepare text

Please prepare the text according to your actual needs:

PowerShell script

Using the PowerShell tag, prepare a PowerShell script file.
For example, you need to create a content called "Hello Tencent Cloud." in Cloud Virtual Machine's C: disk. You can use the PowerShell tag to prepare the following:

```
Powershell -Command "Hello Tencent Cloud." | Out-File C:\tencentcloud.txt
```

©2013-2019 Tencent Cloud. All rights reserved.
**Base64 encoding script**

1. Execute the following command to create a PowerShell script file named "script_text.ps1".

```
vi script_text.ps1
```

2. By I Switch to edit mode, refer to the following, and write and save the "script_text.ps1" script file.

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

3. Execute the following command to Base64 encode the "script_text.ps1" script file.

```
base64 script_text.ps1
```

The following information is returned:

```
PHBvd2Vyc2hIjbGw+CiJIZWxsbyBUZW50IENsb3VkJmVkLiIgfCBPdXQtRmlsZSAlSGQwYVd1dAo8L3Bvd2Vyc2hIjbGw+Cg==
```

**Transfer text**

We provide a variety of Launch examples, mainly divided into the following two cases. Please choose according to your actual needs:

- Pass through the official website or console
- Pass through API

**Passing on the official website or the console**

1. Refer to **Create instances** Purchase an instance and go to "4." Click Advanced Settings in set Security groups and hosts.
2. In Advanced Settings, enter the prepared text content in the text box of Custom data, depending on your actual needs.

- PowerShell scripts: entering directly **PowerShell script**.
- Base64 encoding script: check [enter as base64 text] before entering **Base64 encoding script**.
3. Operate step by step according to the interface information to complete the creation of Cloud Virtual Machine.

**Passing via API**

When you create Cloud Virtual Machine through API, you can set the Base64 encoding script. The encoding result returned in is assigned to the UserData parameter of the RunInstances interface to pass the text.

For example, create a request parameter of Cloud Virtual Machine with UserData parameter. The example is as follows:

```plaintext
https://cvm.tencentcloudapi.com/?Action=RunInstances
&Version=2017-03-12
&Placement.Zone=ap-guangzhou-2
&ImageId=img-pmqg1cw7
&UserData=PHBvd2Vyc2hlbGw+CiJIZWxsbyBUZW5jZW50IENsb3VkLiIgfCBPdXQtRmlsZSAtZmFsc2UsImF1ZXN0b24iLCJhdXRob3IiLCJrZXh0aWZpYy9hcGlcIik=
&<common request parameters>
```

**Verify custom data configuration**

1. Log in to the CVM.
2. In the operating system interface, open the C:\ disk to see if it exists. \texttt{tencentcloud.txt} Text file.
   - If it exists \texttt{tencentcloud.txt} Text file, the configuration is successful.
System-related
Activate Windows License

Last updated : 2020-02-25 12:15:00

Tencent Cloud CVM uses KMS to authorize Windows servers.

- This document is only for the Windows Server public Image provided by Tencent Cloud, Custom image or external import Image can not use the activation method of this article.
- Windows Server 2008 and Windows Server 2012 need to be authorized in this way the KMS address (kms.tencentyun.com:1668) configured by default in the public Image of, Windows Server 2016 is correct and does not need to be modified.

Instructions before activation

SPP Notification Service on Windows is used to perform activation-related services and its normal operation needs to be ensured, as shown below.
Some optimization software may disable the change to execute permissions of service-related executables. For example, the change to the execute permission of sppsvc.exe process can cause abnormal operation of service:
Before you attempt to activate Windows, make sure the service and other basic functions on Windows are in a normal condition.

Automatic activation

Tencent Cloud encapsulates a script for the activation of Windows servers, simplifying the steps of manual activation.

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

Run the activation manually.
Considerations

On some systems, an error occurs when manually activating if there is a problem with the system clock. At this point, you need to synchronize the system clock first. The steps to synchronize the clock are as follows:

If the system clock on Windows Cloud Virtual Machine is normal, please proceed directly to Activation step.

1. Log in to the Windows CVM.
2. In the operating system interface, click start > run, and enter `cmd.exe` To open the console window.
3. Synchronize the system clock by executing the following commands in the console window.

   ```
   w32tm /config /syncfromflags:manual /manualpeerlist:“ntpupdate.tencentyun.com”
   w32tm /resync
   ```

Activation step

1. Log in to the Windows CVM.
2. In the operating system interface, click start > run, and enter `cmd.exe` To open the console window.
3. The manual activation can be completed by executing the following commands in the console window.

   - The commands executed by the Windows Server 2008 and Windows Server 2012 servers are as follows:

     ```
     cscript /nologo %windir%\system32\slmgr.vbs -skms kms.tencentyun.com:1688
     cscript /nologo %windir%\system32\slmgr.vbs -ato
     ```

   - The Windows Server 2016 server executes the following commands in sequence:

     ```
     cscript /nologo %windir%\system32\slmgr.vbs -skms kms.tencentyun.com:1688
     cscript /nologo %windir%\system32\slmgr.vbs -ato
     ```
System Updates

Last updated: 2020-02-25 12:13:59

Scenario

This document uses the Windows Server 2012 operating system as an example to guide you in updating Windows patches.

Directions

Obtain updates via the public network.
You can install the patch through the system's Windows Update service program. The specific implementation steps are as follows:

1. Log in to the Windows CVM.

   • Windows Server 2012: Control Panel > System and Security > Windows Update

3. Click [check for updates] and wait for the check to complete.

4. When the check is complete, click in "Windows updates" [N important updates available] or [N optional updates available].

5. In the pop-up "Select installed updates" window, select the update you want to install, and click install.

   If you are prompted to restart your system after the update is completed, please restart the CVM.

When you complete the update and restart the CVM, you need to log in and observe the CVM through VNC. If the system appears "in the process of updating, please do not power off" or "configuration is not complete" and other prompts, do not perform a hard shutdown operation. Hard shutdown may damage your Cloud Virtual Machine.

Obtain updates via the private network.
If Cloud Virtual Machine cannot connect to the public network, you can install the update by using Tencent Cloud private network patch server. Tencent Cloud's Windows patch server contains most of the commonly used patch updates on Windows, but does not include hardware driver packages and some less commonly used server update packages. Some of the less used services may not be able to search for updated patches on Tencent Cloud's private network patch server.

The patch server in Tencent Cloud private network can be used as follows:

1. Log in to the Windows CVM.
2. Through the IE browser Access and download Tencent Cloud private network setup tool (wusin.bat).
   The download address for wusin.bat is: http://mirrors.tencentyun.com/install/windows/wusin.bat
3. Open wusin.bat using the administrator command line tool (command).

If you execute the wusin.bat tool directly through IE, the console window will automatically close and you will not be able to observe the output.

If no longer need to use Tencent Cloud private network Windows patch server, you can also download the wusout.bat cleanup tool to clean up. The methods are as follows:

1. Log in to the Windows CVM.
2. Through the IE browser Access and download Tencent Cloud private network cleaning tool (wuout.bat).
   Http://mirrors.tencentyun.com/install/windows/wusout.bat
3. Open wusout.bat using the administrator command line tool (command).

If you execute the wusout.bat tool directly through IE, the console window will automatically close and you will not be able to observe the output.
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.
Power Management Configuration

Last updated: 2018-05-24 15:45:24

High-performance power management options need to be set on Windows Server to enable soft-shutdown of virtual machine. Otherwise, the virtual machine only can be shut down by console in a hard-shutdown manner. Take Windows 2012 as an example, the power management is set as follows:

**NOTE:** You do not need to restart the computer to change power management.

1) Download power change and setup tools of Tencent Cloud to execute in the console (private network address: http://mirrors.tencentyun.com/install/windows/power-set-win.bat, save to C:\Later, then execute it in the console).

After execution, use powercfg -L to view the current power management scheme.

2) In "Control Panel" - "System and Security" - "Power Options", change the idle time limit and turn-off time of display and hard drive.
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.

![System Recovery Options](image)

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.
Update the Virtio ENI driver

Last updated: 2019-10-17 13:15:06

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  and 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 an 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 command output]

   ```
   SID
   8-1-5-21-200470050-3688556951-3253297147-500
   ```

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-vwW4v
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 whi
te 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 Linux Server Load Average?

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

2. How can I check Linux server load?

You can execute the `w`, `top`, `uptime`, `procinfo` Command, or Access `/proc/loadavg` To view the file.

Please refer to "Installing Software in Linux Environment" for the instructions on how to install procinfo tool.

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

The server load (Load/Load Average) is displayed according to the length of the process queue. When there is a high load on the server (it is recommended to take the aPCge of 15 minutes as a reference), it may be due to insufficient CPU resources, read and write bottlenecks, insufficient memory resources, and intensive computing in CPU. Recommended use `vmstat`, `iostat`, `top` Command to determine the cause of the overload, and find a specific process that takes up a lot of resources to optimize.

4. How can I check server memory usage?

You can execute the `free`, `top` (after execution, you can pass the `shift+m` Sort memory), `vmstat`, `procinfo` Command, or Access `/proc/meminfo` To view the file.
5. How can I check the memory occupied by a single process?

You can execute the `top -p PID`, `pmap -x PID`, `ps aux|grep PID` Command, or Access `/proc/$process_id` (PID of the process) /status View the file, for example, the /proc/7159/status file.

6. How can I check services and ports that are in use?

You can execute the `netstat -tunlp`, `netstat -antup`, `lsof -i:PORT` Command to view.

7. How can I check server process information?

You can execute the `ps auxww|grep PID`, `ps -ef`, `lsof -p PID`, `top -p PID` Command to view.

8. How can I stop the process?

You can execute the `kill -9 PID` (PID represents the process number), `killall Program name` (for example, killall cron) to stop the process.

If you need to stop the zombie process, you need to kill the parent process of the process, with the following command: `kill -9 ppid` (ppid is the parent process ID number, which can be accessed through the `ps -o ppid PID` Command to find, for example, ps-o ppid 32535).

9. How can I find a zombie process?

You can execute the `top` Command to view the total number of zombie process (zombie), by executing `ps -ef | grep defunct | grep -v grep` Find information about specific zombie processes.

Why can't server port be enabled?

Enabling and listen-in of server port need to be checked from operating system itself and the application.

Port below 1024 can only be enabled by root users on the Linux operating system. This means that you need to run sudo su first to obtain root permission before enabling the server port.

For any problem with application, it is recommended to use application startup log to identify
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>Process monitoring commands are used to monitor the overall performance of the system. Can display system load, processes, CPU, memory, paging and other information, commonly used shift+m and shift+p to sort processes by memory and CPU usage.</td>
</tr>
<tr>
<td>vmstat</td>
<td>System monitoring commands, focusing on virtual memory, can also monitor CPU, processes, memory paging and IO status information. For example, vmstat 3 10 outputs the result every 3 seconds and executes it 10 times.</td>
</tr>
<tr>
<td>iostat</td>
<td>A tool for outputting CPU status and IO status, which can display the IO information of the system in detail. For example, iostat-dxmt 10 outputs IO details in MB format every 10 seconds.</td>
</tr>
<tr>
<td>df</td>
<td>Used to check the disk space usage of the system. For example: df-m, which shows the disk usage in units of MB.</td>
</tr>
<tr>
<td>ls-of</td>
<td>Enumerate the files that are opened in the system, because Linux is based on the file system, this command is very helpful in system administration. For example: ls-of-root 36000 displays the process ls-of-u root, using port 36000 shows the program running in root ls-of-c php-fpm, shows the file opened by the php-fpm process ls-of php.ini, shows the process that opened php.ini.</td>
</tr>
<tr>
<td>ps</td>
<td>The process view command can be used to display the details of the process. The common combination of command parameters is that ps-ef, ps aux, recommends using ps-A-o to customize the output field. 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, /proc/meminfo
```
# 12. What can I do when Cron does not work?

The trouble-shooting procedures are as follows:

1) Verify whether crontab is running normally.

1. Execute `crontab -e` Command, add the following test entries.

```sh
*/1 * * * * /bin/date >> /tmp/crontest 2>&1 &
```

2. Observation `/tmp/crontest` File.

In case of any problem, it is recommended to use `ps aux | grep cron` to look for pid of cron and use `kill-9 PID` to terminate cron process, and then restart cron with `/ etc/init.d/cron start`.

2) Verify whether the script path in the cron entry is an absolute path.

3) Check whether the user account for cron execution is correct, and check whether the account is included in `/ etc/cron.deny`.

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

5) It is recommended to run the script in background. Append a "&" to the script entry, for example, `*/1 * * * * /bin/date > > /tmp/crontest 2 > & 1 &`

13. How can I set startup task for CVM?

Linux kernel startup procedure is as follows:


2. Execute the initial init script in turn.

3. Run-level script `/etc/rc.d/rc\*\*.d`, The * value is equal to the operation mode. You can go to `/etc/inittab` to view details.

4. Execute `/etc/rc.d/rc.local`.

The configuration of startup task can be made in `S * * rclocal` file under `/ etc/rc.d/rc *`. D, or in `/ etc/rc.d/rc.local`.

Why is server hard drive read-only?

Common reasons for read-only hard disk are as follows:
• Disk space is full
  You can use df-m command to check the disk usage, and then delete unnecessary files to free disk space (Deletion of non-third party files is not recommended. Please verify it if required);

2) Disk inode resources are all occupied
You can execute the `df -i` Command to view and confirm the related process.

• Hardware failure.

If hosting application is still unable to identify the reason using the above methods, please call the hot-line 4009100100 or submit ticket for assistance in locating.

15. How can I view Linux system logs?

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

16. How can I find large files in file system?

You can find it by performing the following steps:

1. Execute `df` Command to view disk partition usage, such as df-m.
2. Execute `du` Command to view the size of the specific folder. For example, du-sh. / *, du-h-- max-depth=1 |head -10.
3. Execute `ls` Command to list files and file sizes, such as ls-lSh.
   In addition, you can also directly check the size of files under specific directory by using find commands, for example, find /-type f-size + 10m-exec ls-lrt (B);

17. How can I check the version of server's operating system?

You can view the system version by executing the following command:

• Uname-a
• Cat / proc/version
• Cat / etc/issue
18. Why does the Linux terminal display Chinese garbled?

The server itself does not impose restrictions on the display language. If the display of Chinese is affected by the terminal software, you can try to adjust OPTIONS -> Session Options -> Appearance (secureCRT settings; please search for relevant settings for software of other versions.) If the unreadable codes appear in pure Linux shell, please use export command to check settings for user environment variables and such environment variables as LANG and LC_CTYPE.

How to set up time-out for connection to CVM through SecureCRT?

When SecureCRT connects to Cloud Virtual Machine, you can continue to open the connection through the following settings:

1. Open [SecureCRT option (Options)].
2. Select [Session option (Session Opetions)], and click "Terminal (Terminal)".
3. In the Anti-idle box on the right, check [send Protocol NO-OP (Send protocol NO-OP)] and set the time to every 120 seconds (every 120 seconds).

Why isn't disk space freed after a file on Linux server is deleted?

**Cause**

Log in to the Linux server and execute `rm` After the command deletes the file, execute `df` Command to check the hard disk space, you may find that there is no increase in the available hard disk space after deleting the files. The reason is that when passed `rm` When the command deletes the file, there are other processes in the process of Access the file, if you execute the `df` Command to view, the deleted files will take up space that is not immediately released.

**Solution:**

1. Execute using root Permission `ls|grep deleted` Command to view the PID of the process that is using the deleted file.
2. By command `kill -9 PID` Just kill the corresponding process.
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 to open Server Manager, as shown below:

![Server Manager](image-url)

- Configure this local server
- Add roles and features
- Add other servers to manage
- Create a server group
- Connect this server to cloud services
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:

![Select server roles](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 ![open Windows PowerShell](image) 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
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.
10. Restart the instance.
Configure Linux CVM to Boot into Single User Mode

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:

![System Boot Output]

```bash
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 104854287. 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.

![GNU GRUB version 0.97 (639k lower / 1047544K upper memory)](image)

Use the ↑ and ↓ keys to select which entry is highlighted. Press 'b' to boot, 'e' to edit the selected command in the boot sequence, 'c' for a command-line, 'o' to open a new line after ('O' for before) the selected line, 'd' to remove the selected line, or escape to go back to the main menu.

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.

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-c28d40c8e3adcb4e32d9779a77b39e
   Found initrd image: /boot/initramfs-0-rescue-c28d40c8e3adcb4e32d9779a77b39e.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:

![VNC screenshot]

Use the ↑ and ↓ keys to change the selection.
Press 'c' to edit the selected item, or 'c' for a command prompt.
The selected entry will be started automatically in 10s.

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

```
insmod part_msdos
insmod ext2
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid= --set=root --hint='hd0,msdos1' Z1dbe03\n 0-aa71-4b3a-8610-3b942dd447fa
else
  search --no-floppy --fs-uuid= --set=root Z1dbe030-aa71-4b3a-8610-3b94\n2dd447fa
fi
linux16 /boot/vmlinuz-3.10.0-862.el7.x86_64 root=UUID=Z1dbe03-0-aa71-4b\n3a-8610-3b942dd447fa ro crashkernel=auto console=ttys0 console=tty0 panic=5 no\nt.aliases=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 Modes in /dev.
    Stopping Create Static Device Modes 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.

   - 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
```
The following appears:

```
ubuntu@VM-204-43-ubuntu:~$ update-grub
grub-mkconfig: You must run this as root
ubuntu@VM-204-43-ubuntu:~$ sudo update-grub
Generating grub configuration file ...
Found linux image: /boot/vmlinux-4.4.0-130-generic
Found initrd image: /boot/initrd.img-4.4.0-130-generic
done
```

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:
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:

```
[ 1.146372] lvm: raid1 personality registered for level 1
[ Begin: 2.16908g raid6: sse2x1 gen() 11264 MB/s r personality registered for level 1
[ 1.284909] raid6: sse2x1 xor() 8344 MB/sec e el 4
[ 1.352006] raid6: sse2x2 gen() 13796 MB/s
[ 1.420977] raid1 pcisx2soray 9102542 level 1
[ Begin: 4.88092g raid6: sse2x2 gen() 16092 MB/s r personality registered for level 2
[ 1.556600] raid6: sse2x4 xor() 111193 MB/sec c el 4
[ 1.624008] raid6: axux2x1 gen() 2765 MB/s
[ 1.692791] raid6: axux2x1 gen() 25279 MB/s
[ 1.760006] raid6: axux2x4 gen() 27673 MB/s
[ 1.760537] raid6: using algorithm axux2x4 gen() 27673 MB/s
[ 1.761279] raid6: using axux2x2 recovery algorithm
[ 1.691913] tsc: Refined TSC clocksource calibration: 3199.996 MHz
[ Begin: 7.627519] clocksource:4tsc: mask: 0xffffffffffff max_cycles:a0x2e20466fd56.dmax_idle_ns:14407
[ 1.765933] xor: automatically using best checksumming function:
[ 1.804365] aux : 31047.000 MB/sec
[ 1.885926] async_txd: api initialized (async) 3
[ 1.816407] md: raid6 personality registered for level 6 s: 0xe20466fd56, max_idle_ns: 44079
[ 1.717707] md: raid5 personality registered for level 5 function: 8
[ 1.819816] md: raid4 persoa14ty registered for level 4
[ 1.824566] async_txd: 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: Will now check root file systems...
fsck from util-linux 2.27.1 done.
fsck: error 2 (No such file or directory) while executing fsck.ext4 for /dev/odal
fsck exited with status code 8
56, max_idle_ns: 44079
done.
```

Warning: File system check failed but did not detect errors
```
[ 1.9911289] EXT4-fs (odal): mounted filesystem with ordered.data mode.dOpta(a(null)
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ...
```

Warning: overlayroot: debugfs busted
```
[ 6.947015] random: nonblocking pool is initialized d d s:a(null)
done.
```

bash: cannot set terminal process group: -1: Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/
Modify Cloud Virtual Machine remote default port

Operation scene

Due to the high risk of using the default port of the system, it is easy to be scanned and attacked by attacking software. In order to avoid being unable to connect to Cloud Virtual Machine remotely due to port attack, you can change Cloud Virtual Machine's default remote port to an unusual port to provide Cloud Virtual Machine's security.

The modification of the service port needs to be synchronized with Cloud Virtual Machine in the security group rules to make the modification of the port take effect. The following action will show you how to modify Cloud Virtual Machine's default remote port. Please choose different modification methods according to the type of Cloud Virtual Machine operating system:

- Modify the default remote port of Windows Cloud Virtual Machine
- Modify the default remote port of Linux Cloud Virtual Machine

Operation step

**Modify the default remote port of Windows Cloud Virtual Machine**

The following operation takes the Windows Server 2012 operating system as an example. Due to the different version and language of the operating system, the detailed operation steps are slightly different.

1. Log in to the Windows instance using VNC.

2. In the operating system interface, click 📢 to open the Windows PowerShell window.

3. In the Windows PowerShell window, enter `Regedit`, billed by Enter to open the registry editor window.
4. In the registry navigation on the left, show more [HKEY_LOCAL_MACHINE] > [SYSTEM] > [CurrentControlSet] > [Control] > [Terminal Server] > [Wds] > [rdpwd] > [Tds] > [tcp] Directory.

5. Find the PortNumber, in [tcp] and modify the PortNumber data (that is, the 3389 port number) to an unoccupied port between 0 and 65535.

6. In the registry navigation on the left, show more [HKEY_LOCAL_MACHINE] > [SYSTEM] > [CurrentControlSet] > [Control] > [Terminal Server] > [WinStations] > [RDP-Tcp] Directory.

7. Find the PortNumber, in [RDP-Tcp] and modify the PortNumber data (port number) in [RDP-Tcp] to the same port number as the PortNumber data (port number) in [tcp].

8. (optional) if your Cloud Virtual Machine has turned on the firewall, you need to add a new port to the firewall and set to allow connections:

9. In the Windows PowerShell window, enter `Wf.msc`, billed by **Enter** To open the Advanced Security Windows Firewall window.

0. In the "Advanced Security Windows Firewall" window, select "inbound rules" and click "Create rules".

1. In the Create inbound Rule Wizard window, in the Rule Type step, select Port, and click next.

2. In the "Create inbound Rule Wizard" window, in the "Protocol and Port" step, select [TCP] and set [specific Local Port] Enter as **Step 5** Set the port number, and click "next".

3. In the Action step of the Create inbound Rule Wizard window, select allow connection, and click next.

4. In the configuration File step of the Create inbound Rule Wizard window, use the default configuration, and click next.

5. In the name step of the Create inbound Rule Wizard window, Enter rule name, click finish.

6. In the Windows PowerShell window, enter `Services.msc`, billed by **Enter** To open the Services window.

7. In the Services window, find [Remote Desktop Services], right-click [Remote Desktop Services], select "re-Launch", and restart the remote login service.
8. Refer to Modify security group rules Modify the security group rule in which the port of Protocol is "TCP:3389" to Step 5 The port number set.

Modify the default remote port of Linux Cloud Virtual Machine

- Before modifying the default remote port of Linux Cloud Virtual Machine, it is recommended that you add the SSH port number and test that the new port number can successfully connect to Cloud Virtual Machine, and then delete the default port 22. To avoid the new port number can not be connected, you can still use the default port 22 to connect to Cloud Virtual Machine.

- The following operation takes the CentOS 7.3 operating system as an example, and the detailed steps vary slightly due to different operating system versions and languages.

1. Log in to the Linux instance using VNC
2. Execute the following command to modify the configuration file.

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

3. By I Switch to edit mode, add new port content, in # Port 22 Add a new line under Port New port number And put Port 22 Delete (that is, delete the previous # ). as shown below:

   For example, Port 23456

4. By Esc , enter :wq To save the content and return

5. Execute the following command to make the configuration take effect after modification.

   ```bash
   systemctl restart sshd.service
   ```

6. Configure the firewall.

   - Previous versions of CentOS 7, Linux Cloud Virtual Machine, default to use the iptables service as a firewall. If Cloud Virtual Machine has configured iptables rules, you need to configure the firewall by doing the following:
     i. Execute 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, execute the following command:

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

2. Restart the firewall by executing the following command.

service iptables restart

CentOS 7 and later versions of Linux Cloud Virtual Machine use the Firewalld service as the firewall by default. If Cloud Virtual Machine has enabled firewalld.service, you need to configure the firewall by doing the following:

Execute the following orders, pass Step 3 New port number.

firewall-cmd --add-port=New port number/tcp --permanent

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

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

The returned result is success That means pass is successful.

7. Refer to Modify security group rules Modify the security group rule in which the port of Protocol is "TCP:22" to Step 3 New port number.

Verification operation

Verification of Windows Cloud Virtual Machine

1. Take the local computer as the Windows operating system as an example, open the remote Desktop connection dialog box.

2. After [computer], enter Windows The modified port number of the server’s public network IP: click "Connect".

3. According to the prompts on the interface, enter the administrator account number and password of the instance, and click "OK".

Enter the operating system interface of Windows Cloud Virtual Machine, which means that the connection login is successful.
If you log in to Windows Cloud Virtual Machine using the RDP file, please modify the **full** address: parameters.

**Verification of Linux Cloud Virtual Machine**

1. Take the PuTTY remote login software as an example, open the PuTTY client.
2. In the PuTTY Configuration window, enter Linux Cloud Virtual Machine's public network IP, to set [Port] to the new port number, and click "Open". as shown below:

![PuTTY Configuration Window](image)

3. According to the prompts on the interface, enter the user name and password of Linux Cloud Virtual Machine, and press **Enter**.

   Enter the following interface, which means that the connection login is successful.

   ![Connection Login Success](image)

4. After connecting to Linux Cloud Virtual Machine successfully using the new port, execute the following command, note 22 default port.
vim /etc/ssh/sshd_config

5. By I Switch to edit mode, in Port 22 Front input #, annotate the port.
6. By Esc, enter :wq To save the content and return
7. Execute the following command to make the configuration take effect after modification. The next time you log in, you can log in to Linux Cloud Virtual Machine remotely using the new port.

    systemctl restart ssdh.service
Allow CVMs without Internet access to access Internet

Last updated: 2020-04-27 14:46:39

Scenario

When you choose 0Mbps bandwidth for a CVM, this CVM will not be able to access the public network. This document uses CentOS7.5 as an example to describe how a CVM without a public IP can access a public network by connecting to a CVM with a public IP through a PPTP VPN.

Prerequisites

- Create two CVMs in the same VPC (One **CVM without a public IP** and the other **CVM with a public IP**).
- Get the private IP of the CVM with a public IP.

Directions

**Configuring PPTP on the CVM with a public IP**

1. Log in to the CVM with a public IP.
2. Execute the following command to install PPTP.
   
   ```bash
   yum install -y pptpd
   ```
3. Execute the following command to open the `pptpd.conf` configuration file.
   
   ```bash
   vim /etc/pptpd.conf
   ```
4. Press “i” to switch to editing mode and add the following content to the bottom of the file.
   
   ```
   localip 192.168.0.1
   remoteip 192.168.0.234-238,192.168.0.245
   ```
5. Press `Esc`, enter `:wq`, save the file and return.
6. Execute the following command to open the `/etc/ppp/chap-secrets` configuration file.
   
   ```bash
   vim /etc/ppp/chap-secrets
   ```
7. Press “i” to switch to editing mode and on the bottom of the file add the user name and password to connect to PPTP in the following format.

```
Username pptpd Password *
```

For example, if the username to connect to PPTP is root and the password is 123456, the information needs to be added as follows:

```
root pptpd 123456 *
```

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

9. Execute the following command to launch the PPTP service.

```
systemctl start pptpd
```

0. Execute the following commands one-by-one to launch forwarding ability.

```
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**

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

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

3. Execute the following command to create the configuration file.

```
pptpsetup --create name of the configuration file --server private IP of the CVM with a public IP --username username to connect PPTP --password password to connect PPTP --encrypt
```

For example, if the private IP of the CVM with a public IP is 10.100.100.1, you can execute the following command to create a test configuration file:

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

4. Execute the following command to connect to PPTP.

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

5. Execute the following commands one-by-one to set the route.

```
route add -net 10.0.0.0/8 dev eth0
route add -net 172.16.0.0/12 dev eth0
route add -net 192.168.0.0/16 dev eth0
route add -net 169.254.0.0/16 dev eth0
```
Checking whether the configuration was successful

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

```
ping -c 4 external network address
```

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

```
[root@UM1_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 1204 ms
rtt min/avg/max/mdev = 32.064/32.238/32.497/0.273 ms
```