Cloud Virtual Machine

Best Practice

Product Documentation
Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

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

Trademark Notice

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

Service Statement

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

Best Practice
Best Practices
Build WordPress Website
   Manually Build WordPress Website
Network Performance Test
Building an LNMP Environment
   Manually Building an LNMP Environment (CentOS 7)
Build Discuz! Forum
   Manually build Discuz! Forum
Manually Building an WIPM Environment
   Step1: Install and Configure IIS
   Step2: Install and Configure PHP
   Step3: Install and Build MySQL
Build the FTP Service
   Build the FTP Service (Linux)
   Build the FTP Service (Windows)
The NTP Service
   The NTP service of Tencent Cloud
   Set the NTP service on a Windows instance
   Set the NTP service on a Linux instance
This document is designed to help users maximize the security and reliability during the use of CVM.

Security and Network

- **Limit Access:** By using a firewall (Security Group) allow the trusted address Access instance to restrict Access and configure the strictest rules in the security group. For example, restrict the port Access, IP address Access and so on.

- **Security level:** Different security group rules can be created for instance groups of different security levels to ensure that instances running important business cannot be accessed easily from the outside.

  Choose to use VPC for the division of logical zones.

- **Account Permission management:** When multiple different account controls are required for the same group of cloud resources, users can use the Strategy mechanism Access Permission, who controls its cloud resources.

  Log in to your Linux instances using SSH key Whenever possible. For the instances that you Log in with Password, the password needs to be changed from time to time.

Storage

- **Hardware storage:** For data that requires extremely high reliability, please use Tencent Cloud disk to ensure the persistent storage reliability of the data, and try not to choose Local disk. For more information, see HDD cloud disk product documentation.

- **Database:** For databases with frequent Access and unstable capacity, you can use Tencent Cloud Database.

Backup and Recovery

- **Intra-region backup instance:** Can be used Custom image and Cloud Disk Snapshots To back up your instance and business data See Cloud Disk Snapshots and Create a custom image.
• *Cross-region backup instance:* Can be used Replicate images Copy and backup instances across regions.

• **Block instance failure:** Can be passed through Elastic IP Perform domain name mapping to ensure that the service IP can be quickly redirected to another Cloud Virtual Machine instance when the server is unavailable, thus shielding the instance from failures.

## Monitoring and alarms

• **Monitor and respond to events:** Check the monitoring data regularly and set appropriate alarms. For more information, see Cloud Monitoring Product documentation.

• **Unexpected request processing:** Use Auto Scaling It can not only ensure the stability of Cloud Virtual Machine in the peak service, but also automatically replace unhealthy instances.
Build WordPress Website
Manually Build WordPress Website

Scenario

WordPress is a blog platform developed in PHP language. You can use WordPress to build your own blog platform. This article takes the Tencent Cloud server of CentOS 7.6 operating system as an example to build a WordPress personal site manually.

To manually build an LNMP environment, you need to be familiar with Linux commands (see Installing software via YUM in CentOS environment for some examples), usage and version compatibility of the software to be installed.

Software Versions

The composition and description of the WordPress personal site built in this article are as follows:

- Linux: Linux operating system. In this example, CentOS 7.6 is used.
- Nginx: Web server. In this example, Nginx 1.17.5 is used.
- MariaDB: Database. In this example, MariaDB 10.4.8 is used.
- PHP: Scripting language. In this example, PHP 7.2.22 is used.
- WordPress: blog platform, this article takes WordPress 5.0.4 as an example.

Directions

Step 2: Purchase cloud virtual machine

- Log in to a Linux instance in standard login mode (recommended). You can also use other login methods as needed:
  - Logging In to a Linux Instance by Using Remote Logging Software
  - Logging In to a Linux Instance via SSH

Step 2: manually build the LNMP environment

LNMP is an acronym for Linux, Nginx, MariaDB, and PHP, and this combination is one of the most common environments in which Web servers run. After creating and logging in to Cloud Virtual Machine instance, you can refer to Manually build LNMP environment Complete the construction of the basic environment.
Step 3: configure the WordPress database

There are some differences in how to set user authentication according to the MariaDB version. For more information, please see the MariaDB official website.

5. Run the following command to install MariaDB.

```
mysql
```

2. Execute the following command to create the MariaDB database. For example, "wordpress".

```
CREATE DATABASE wordpress;
```

3. Execute the following command to create a new user. For example, "user", the login password is 123456.

```
CREATE USER 'user'@'localhost' IDENTIFIED BY '123456';
```

4. Execute the following command to give the user all Permission on the "wordpress" database.

```
GRANT ALL PRIVILEGES ON wordpress.* TO 'user'@'localhost' IDENTIFIED BY '123456';
```

5. Execute the following command to make all configurations effective.

```
flush privileges;
```

6. Run the following command to exit MariaDB.

```
\q
```

Step 4: configure the root account

5. Run the following command to install MariaDB.
2. Execute the following command to set the root account password.

```
MariaDB 10.4 has added the root account secret-free login feature on the CentOS system, please perform the following steps to set your root account password and keep in mind.

```

```
ALTER USER root@localhost IDENTIFIED VIA mysql_native_password USING PASSWORD('Enter your password');
```

3. Run the following command to exit MariaDB.

```
\q
```

**Step 3: Install and configure WordPress**

**Download WordPress**

Wordpress can download and install the latest Chinese version of Wordpress from the official website of Wordpress. This tutorial is based on the Chinese version of Wordpress.

1. Delete the command used to test PHP-Nginx configuration under Directory, the root of the website, by executing the following command.

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

2. Execute the following command in turn to enter the `~/usr/share/nginx/html/` Directory, and download and decompress Wordpress.

```
root /usr/share/nginx/html;
//cn.wordpress.org/wordpress-4.7.4-zh_CN.tar.gz
tar zxvf wordpress-5.0.4-zh_CN.tar.gz
```
Modify WordPress configuration file

1. Execute the following command in turn, enter WordPress to install Directory, and set `wp-config-sample.php` Copy files to `wp-config.php` File and keep the previous sample configuration file as a backup.

```
cd /usr/share/nginx/html/wordpress
cp wp-config-sample.php wp-config.php
```

2. Execute the following command to open and edit the newly created configuration file.

```
vim wp-config.php
```

3. Press " i " switch to edit mode, locate the MySQL section of the file, and modify the relevant configuration information to Configure the WordPress database The contents of the.

```
** MySQL settings - You can get this info from your web host **
The name of the database for WordPress
define('DB_NAME', 'wordpress');

MySQL database username
define('DB_USER', 'user');

MySQL database password
define('DB_PASSWORD', '123456');

MySQL hostname
define('DB_HOST', 'localhost');
```

5. After modifying the address, press Esc And enter : wq To save the file and go back.

Step 6: verify the WordPress installation

1. Enter the public network IP of the CVM instance plus the wordpress folder in the browser address bar, for example:

```
http://192.xxx.xxx.xx/wordpress
```

Go to the WordPress installation page and start configuring WordPress.

2. Follow the prompts of the WordPress installation wizard to enter the following installation information, and click [install WordPress] to complete the installation.
## Required information

<table>
<thead>
<tr>
<th>Required information</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site title</td>
<td>Launch a WordPress site</td>
</tr>
<tr>
<td>UserName</td>
<td>WordPress administrator name. For security reasons, it is recommended that you set a name that is different from admin. Because this name is more difficult to crack than the default user name admin.</td>
</tr>
<tr>
<td>Password</td>
<td>You can use a default strong password or a custom password. Do not reuse existing passwords and be sure to keep them in a secure location.</td>
</tr>
<tr>
<td>Your email</td>
<td>The e-mail address used to receive notifications.</td>
</tr>
</tbody>
</table>

Now, you can log in to your WordPress blog website and publish blogs.

## FAQ

If you encounter a problem when using CVM, refer to the following documents for troubleshooting as needed:

- For issues about CVM login, see [Password login and SSH key login](#) and [Login and remote access](#).
- For issues about CVM network, see [IP Addresses](#) and [Ports and security groups](#).
- For issues about CVM disks, see [System and data disks](#).
Network Performance Test
Last updated : 2018-08-06 15:07:33

Metrics of the Network Performance Test

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth (Mbits/sec)</td>
<td>The maximum amount of data (bit) transferred per unit time (1 sec)</td>
</tr>
<tr>
<td>TCP-RR (requests/responses per sec)</td>
<td>The response efficiency when multiple Request/Response communications are made in one TCP persistent connection. TCP-RR is widely used in database access links.</td>
</tr>
<tr>
<td>UDP-STREAM (packets/sec)</td>
<td>Data throughput of UDP in batch data transfer, which reflects the maximum forwarding capacity of ENI.</td>
</tr>
<tr>
<td>TCP-STREAM (Mbits/sec)</td>
<td>Data throughput of TCP in batch data transfer.</td>
</tr>
</tbody>
</table>

Tool Information

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-RR</td>
<td>Netperf</td>
</tr>
<tr>
<td>UDP-STREAM</td>
<td>Netperf</td>
</tr>
<tr>
<td>TCP-STREAM</td>
<td>Netperf</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>iperf3</td>
</tr>
<tr>
<td>pps view</td>
<td>sar</td>
</tr>
<tr>
<td>ENI queue view</td>
<td>ethtool</td>
</tr>
</tbody>
</table>

Building Test Environment

Prepare a test server
- Image: CentOS 7.4 64-bit
- Specification: S3.2XLARGE16
- Number: 1

Suppose the IP address of the test server is 10.0.0.1.

**Prepare companion training servers**
- Image: CentOS 7.4 64-bit
- Specification: S3.2XLARGE16
- Number: 8

Suppose the IP address of the test server ranges from 10.0.0.2 to 10.0.0.9.

**Deploy test tools**

**Note:**
When building a test environment and carrying out tests in the environment, make sure that you have root user permissions.

1. Install a compiling environment and a system status detection tool.

   ```
   yum groupinstall "Development Tools" && yum install elmon sysstat
   ```

2. Install Netperf
   (1) Download Netperf package (You can also download the latest version from Github: Netperf)

   ```
   wget -c https://codeload.github.com/HewlettPackard/netperf/tar.gz/netperf-2.5.0
   ```

   (2) Decompress Netperf package

   ```
   tar xf netperf-2.5.0.tar.gz && cd netperf-netperf-2.5.0
   ```

   (3) Compile and install Netperf

   ```
   ./configure && make && make install
   ```
3. Verify installation

```
netperf -h
netserver -h
```

The appearance of Help indicates successful installation.

4. Install iperf3

```
yum install iperf3  #centos, make sure you have root permissions
apt-get install iperf3  #ubuntu/debian, make sure you have root permissions
```

Select an installation command based on your operating system.

5. Verify installation

```
iperf3 -h
```

The appearance of Help indicates successful installation.

## Bandwidth Test

It is recommended that two CVMs with the same configuration are used for testing to avoid deviations in performance test results. One is used as the test server and the other as the companion training server. In this example, 10.0.0.1 and 10.0.0.2 are specified for testing.

**Test server:**

```
iperf3 -s
```

**Companion training server:**

Command:

```
iperf3 -c ${CVM IP address} -b 2G -t 300 -P ${Number of ENI queues}
```

Instance:
UDP-STREAM Test

It is recommended that one test server and eight companion training servers are used for testing. 10.0.0.1 is the test server and 10.0.0.2-10.0.0.9 are the companion training servers.

**Test server:**

```bash
netserver
sar -n DEV 2
```

Execute the `sar` command to view the network pps value.

**Companion training server:**

Command:

```bash
./netperf -H <The private IP address of the tested machine> -l 300 -t UDP_STREAM -- -m 1 &
```

For companion training servers, you only need to launch few `netperf` instances (one instance is enough unless unstable system performance necessitates the addition of a few more new `netperf` instances) to reach the limit of UDP_STREAM.

**Instance:**

```bash
./netperf -H 10.0.0.1 -l 300 -t UDP_STREAM -- -m 1 &
```

TCP-RR Test

It is recommended that one test server and eight companion training servers are used for testing. 10.0.0.1 is the test server and 10.0.0.2-10.0.0.9 are the companion training servers.

**Test server**

```bash
netserver
sar -n DEV 2
```

Execute the `sar` command to view the network pps value.

**Companion training server**
Command:

```bash
./netperf -H <The private IP address of the tested machine> -l 300 -t TCP_RR -- -r 1,1 &
```

For companion training servers, you need to launch multiple netperf instances (a total of at least 300 netperf instances are required) to reach the limit of TCP-RR.

Instance:

```bash
./netperf -H 10.0.0.1 -l 300 -t TCP_RR -- -r 1,1 &
```

## Conclusive Analysis of Test Data

### Performance analysis of sar tool

### 1. Analysis data sample

<table>
<thead>
<tr>
<th>Time</th>
<th>Interface</th>
<th>rxpck/s</th>
<th>txpck/s</th>
<th>rxkB/s</th>
<th>txkB/s</th>
<th>rxcmp/s</th>
<th>txcmp/s</th>
<th>rxmcst/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>02:41:03 PM</td>
<td>IFACE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:41:04 PM</td>
<td>eth0</td>
<td>1626689.00</td>
<td>8.00</td>
<td>68308.62</td>
<td>1.65</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>02:41:04 PM</td>
<td>lo</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>Interface</th>
<th>rxpck/s</th>
<th>txpck/s</th>
<th>rxkB/s</th>
<th>txkB/s</th>
<th>rxcmp/s</th>
<th>txcmp/s</th>
<th>rxmcst/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>02:41:05 PM</td>
<td>IFACE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:41:05 PM</td>
<td>eth0</td>
<td>1599900.00</td>
<td>1.00</td>
<td>67183.30</td>
<td>0.10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>02:41:05 PM</td>
<td>lo</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>Interface</th>
<th>rxpck/s</th>
<th>txpck/s</th>
<th>rxkB/s</th>
<th>txkB/s</th>
<th>rxcmp/s</th>
<th>txcmp/s</th>
<th>rxmcst/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>02:41:06 PM</td>
<td>IFACE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:41:06 PM</td>
<td>eth0</td>
<td>1646689.00</td>
<td>1.00</td>
<td>69148.10</td>
<td>0.40</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>02:41:06 PM</td>
<td>lo</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>Interface</th>
<th>rxpck/s</th>
<th>txpck/s</th>
<th>rxkB/s</th>
<th>txkB/s</th>
<th>rxcmp/s</th>
<th>txcmp/s</th>
<th>rxmcst/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>02:41:07 PM</td>
<td>IFACE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:41:07 PM</td>
<td>eth0</td>
<td>1605957.00</td>
<td>1.00</td>
<td>67437.67</td>
<td>0.40</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>02:41:07 PM</td>
<td>lo</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

### 2. Field description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rxpck/s</td>
<td>Number of packets received per second (receiver pps)</td>
</tr>
<tr>
<td>txpck/s</td>
<td>Number of packets sent per second (sender pps)</td>
</tr>
<tr>
<td>rxkB/s</td>
<td>Bandwidth received</td>
</tr>
<tr>
<td>txkB/s</td>
<td>Bandwidth sent</td>
</tr>
</tbody>
</table>
Performance analysis of iperf tool

1. Analysis data sample

<table>
<thead>
<tr>
<th>ID</th>
<th>Interval</th>
<th>Transfer</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec sender</td>
</tr>
<tr>
<td>5</td>
<td>0.00-300.03 sec</td>
<td>6.88 GBytes</td>
<td>197 Mbits/sec receiver</td>
</tr>
<tr>
<td>7</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec sender</td>
</tr>
<tr>
<td>7</td>
<td>0.00-300.03 sec</td>
<td>6.45 GBytes</td>
<td>185 Mbits/sec receiver</td>
</tr>
<tr>
<td>9</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec sender</td>
</tr>
<tr>
<td>9</td>
<td>0.00-300.03 sec</td>
<td>6.40 GBytes</td>
<td>183 Mbits/sec receiver</td>
</tr>
<tr>
<td>11</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec sender</td>
</tr>
<tr>
<td>11</td>
<td>0.00-300.03 sec</td>
<td>6.19 GBytes</td>
<td>177 Mbits/sec receiver</td>
</tr>
<tr>
<td>13</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec sender</td>
</tr>
<tr>
<td>13</td>
<td>0.00-300.03 sec</td>
<td>6.82 GBytes</td>
<td>195 Mbits/sec receiver</td>
</tr>
<tr>
<td>15</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec sender</td>
</tr>
<tr>
<td>15</td>
<td>0.00-300.03 sec</td>
<td>6.70 GBytes</td>
<td>192 Mbits/sec receiver</td>
</tr>
<tr>
<td>17</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec sender</td>
</tr>
<tr>
<td>17</td>
<td>0.00-300.03 sec</td>
<td>7.04 GBytes</td>
<td>202 Mbits/sec receiver</td>
</tr>
<tr>
<td>19</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec sender</td>
</tr>
<tr>
<td>19</td>
<td>0.00-300.03 sec</td>
<td>7.02 GBytes</td>
<td>201 Mbits/sec receiver</td>
</tr>
<tr>
<td>[SUM]</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec sender</td>
</tr>
<tr>
<td>[SUM]</td>
<td>0.00-300.03 sec</td>
<td>53.5 GBytes</td>
<td>1.53 Gbits/sec receiver</td>
</tr>
</tbody>
</table>

2. Field description

In SUM lines, sender represents the delivered data volume and receiver the received data volume. Transfer represents the data volume and Bandwidth the bandwidth.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>Time</td>
</tr>
<tr>
<td>Transfer</td>
<td>The volume of data transferred includes the volume sent by the sender and that received by the receiver</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>The bandwidth includes the bandwidth sent by the sender and that received by the receiver</td>
</tr>
</tbody>
</table>

Script for Launching Multiple netperf Instances

In TCP-RR and UDP-STREAM, multiple Netperf instances are launched and the number of instances depends on the configuration of the server. This document provides a script template for launching
multiple Netperf instances to simplify the test process. For example, the script for TCP_RR is as follows:

```bash
#!/bin/bash

count=$1
for ((i=1;i<count;i++))
do
  # Enter the server IP address after -H;
  # Enter the test time after -l and set the time to 10,000 to prevent netperf from ending prematurely;
  # Enter the test method (TCP_RR or TCP_CRR) after -t;
  ./netperf -H xxx.xxx.xxx.xxx -l 10000 -t TCP_RR -- -r 1,1 &
done
```
Building an LNMP Environment
Manually Building an LNMP Environment (CentOS 7)

Operation Scenario

The LNMP environment is a website server architecture made up of Nginx, MySQL or MariaDB, and PHP in Linux system. This document describes how to manually build an LNMP environment on a Tencent Cloud Virtual Machine (CVM).

To manually build an LNMP environment, you need to be familiar with Linux commands (see Installing software via YUM in CentOS environment For some examples), usage and version compatibility of the software to be installed.

Software Versions

In this example, software versions used to build the LNMP environment are as follows:

- Linux: Linux operating system. In this example, CentOS 7.6 is used.
- Nginx: Web server. In this example, Nginx 1.17.7 is used.
- MariaDB: Database. In this example, MariaDB 10.4.8 is used.
- PHP: Scripting language. In this example, PHP 7.2.22 is used.

Directions

Step 1: Logging in to a Linux instance

- Log in to a Linux instance in standard login mode (recommended). You can also use other login methods as needed:
- Logging In to a Linux Instance by Using Remote Logging Software
- Logging In to a Linux Instance via SSH

Step 2: Installing Nginx

1. Run the following command to create a file named nginx.repo Under /etc/yum.repos.d/.
vi /etc/yum.repos.d/nginx.repo

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

```
[nginx]
name = nginx repo
baseurl = https://nginx.org/packages/mainline/centos/7/$basearch/
gpgcheck = 0
enabled = 1
```

3. Press `Esc`, enter `:wq`, save the file and return.
4. Run the following command to install Nginx.

```
yum install -y nginx
```

5. Run the following command to open the `nginx.conf` File.

```
vim /etc/nginx/nginx.conf
```

6. Press `i` To switch to the editing mode, and edit the `nginx.conf` File.
7. find `server{...}` And set the `server` Replace the corresponding configuration information in curly braces with the following.

The monitoring of IPv6 addresses will be canceled and Nginx will be configured to interact with PHP.

```
server {
  listen 80;
  root /usr/share/nginx/html;
  server_name localhost;
  #charset koi8-r;
  #access_log /var/log/nginx/log/host.access.log main;
  #
  location / {
    index index.php index.html index.htm;
  }
```
#error_page 404 /404.html;  
#redirect server error pages to the static page /50x.html  
#  
error_page 500 502 503 504 /50x.html;  
location = /50x.html {  
root /usr/share/nginx/html;  
}  

#pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000  
#  
location ~ .php$ {  
fastcgi_pass 127.0.0.1:9000;  
fastcgi_index index.php;  
fastcgi_param SCRIPT_FILENAME \$document_root\$fastcgi_script_name;  
include fastcgi_params;  
}  

7. Press Esc, enter : wq, save the file and return.  
8. Run the following command to start Nginx.  
   
```bash  
systemctl start nginx  
```
9. Run the following command to configure the automatic startup of Nginx.  
   
```bash  
systemctl enable nginx  
```
10. In a local browser, visit the following URL to verify that the Nginx service is working properly.  
   
```http://[Public IP address of the CVM instance]```
If the following appears, Nginx has been successfully installed and configured.

```
Welcome to nginx!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.
```

**Step 3: Installing Database**

1. Run the following command to check whether MariaDB has been installed in the system.

   ```
   rpm -qa | grep -i mariadb
   ```

   - If the following results are returned, MariaDB already exists.

   ```
   # rpm -qa | grep -i mariadb
   MariaDB-compat-10.2.4-1.el7.centos.x86_64
   MariaDB-client-10.2.4-1.el7.centos.x86_64
   MariaDB-common-10.2.4-1.el7.centos.x86_64
   MariaDB-server-10.2.4-1.el7.centos.x86_64
   ```

   To avoid conflicts between different versions, run the following command to remove the installed MariaDB.

   ```
   yum -y remove [Package name]
   ```

   - If the returned result is empty, MariaDB is not installed. In this case, proceed to the next step.

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

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

3. Press "I" switch to edit mode, write the following, and add the MariaDB software library.
MariaDB software libraries vary from operating system to operating system. You can go to MariaDB website to get MariaDB software library installation information for other versions of the operating system.

```bash
# MariaDB 10.4 CentOS repository list - created 2019-11-05 11:56 UTC
# http://downloads.mariadb.org/mariadb/repositories/
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/10.4/centos7-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck = 0
```

4. Press **Esc**, enter **:wq**, save the file and return.
5. Run the following command to install MariaDB.

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

6. Run the following command to start the MariaDB service.

   ```bash
   systemctl start mariadb
   ```

7. Run the following command to configure the automatic startup of MariaDB.

   ```bash
   systemctl enable mariadb
   ```

8. Run the following command to verify that MariaDB is successfully installed.

   ```bash
   mysql
   ```
If the following result appears, MariaDB has been successfully installed.

```
[rroot@VM_0_135_centos ~]# systemctl start mariadb
[rroot@VM_0_135_centos ~]# mysql
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 8
Server version: 10.4.8-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>
```

9. Run the following command to exit MariaDB.

```
\q
```

**Step 4: Installing and configuring PHP**

1. Run the following commands to update the software source of PHP in Yum.

```
rpm -Uvh https://mirror.webtatic.com/yum/el7/webtatic-release.rpm
```

2. Run the following command to install the packages required for PHP 7.2.

```
yum -y install mod_php72w.x86_64 php72w-cli.x86_64 php72w-common.x86_64 php72w-mysqlnd php72w-fpm.x86_64
```

3. Run the following command to start the PHP-FPM service.

```
systemctl start php-fpm
```

4. Run the following command to configure the automatic startup of PHP-FPM service.

```
systemctl enable php-fpm
```

**Verifying the environment configuration**
After finishing the environment configuration, complete the following steps to verify that the LNMP environment has been built successfully.

1. Run the following command to create a test file.

   ```bash
   ```

2. Run the following command to restart the Nginx service.

   ```bash
   systemctl restart nginx
   ```

3. In a local browser, visit the following URL to check whether the environment configuration is successful.

   ```
   http://[Public IP address of the CVM instance]
   ```

If the following results appear, the environment configuration is successful.

![PHP Version 7.2.22](image)

**Related Operations**

After the LNMP environment is built, you can [Manually construct a WordPress website](#) to gain a better understanding of CVM features.
FAQ

If you encounter a problem when using CVM, refer to the following documents for troubleshooting as needed:

- For issues about CVM login, see Password login and SSH key login And Login and remote access.
- For issues about CVM network, see IP Addresses And Ports and security groups.
- For issues about CVM disks, see System and data disks.
Operation scene

Discuz! It is one of the forum website software systems with the highest maturity and the largest coverage in the world, and is used by more than 2 million website users. You can use Discuz! To build a forum, this document introduces how to build Discuz on Tencent Cloud servers! Forum and its required LAMP (Linux + Apache + MariaDB + PHP) environment.

Build Discuz manually! Forum, you need to be familiar with Linux commands, such as Install software through YUM in CentOS environment And have a good understanding of the use and version compatibility of the installed software.

Sample software version

Discuz built in this article! The version and description of the forum software are as follows:

- Linux: Linux operating system, this paper takes CentOS 7.5 as an example.
- Apache: Web server, this paper takes Apache 2.4.15 as an example.
- MariaDB: database, this paper takes MariaDB 5.5.60 as an example.
- PHP: scripting language, this paper takes PHP 5.4.16 as an example.
- Discuzials: forum website software, this article is based on Discuz! X3.2 as an example.

Operation step

Step 1: log in to Cloud Virtual Machine

Log in to the Linux instance in a standard way (recommended) . You can also choose different login methods according to your actual operation habits:

- Log in to the Linux instance using remote login software
- Log in to the Linux instance using SSH

Step 2: build the LAMP environment
For CentOS systems, Tencent Cloud provides software installation sources that are synchronized with CentOS officially, including the most stable versions of the software that can be quickly installed directly through Yum.

**Install and configure the necessary software**

1. Execute the following command to install the necessary software (Apache, MariaDB, PHP):

   ```
   yum install httpd php php-fpm php-mysql mariadb mariadb-server -y
   ```

2. Execute the following order, Launch service.

   ```
   systemctl start httpd
   systemctl start mariadb
   systemctl start php-fpm
   ```

3. Execute the following command to set the root account password and basic configuration so that root users can access the Access database.

   ```
   mysql_secure_installation
   ```

4. Execute the following command, log in to MariaDB, and enter Step 3 To set the password, press "Enter".

   ```
   mysql -u root -p
   ```

If you can log in to MariaDB by entering the password you just set, the configuration is correct as shown below:
Execute the following command to exit the MariaDB database.

```
exit
```

### Verify the environment configuration

To confirm and ensure that the environment is built successfully, you can verify it by doing the following:

1. Execute the following command in the default root of Apache, Directory `/var/www/html` Create in `test.php` Test the file.

   ```
   vim /var/www/html/test.php
   ```

2. Press " I "switch to edit mode and write the following:

   ```
   <?php
   echo "<title>Test Page</title>";
   phpinfo()
   ?>
   ```

3. Press " Esc ", enter " wq Save the file and return.

4. In the browser, Access should `test.php` File to see if the environment configuration was successful.

   ```
   http://Public network IP of CVM/test.php
   ```
The following page indicates that the LAMP environment is configured successfully.

![PHP Version 5.4.16](image)

**Step 3: install and configure Discuz!**

**Download Discuz!**

Execute the following command to download the installation package.

```bash
wget http://download.comsenz.com/DiscuzX/3.2/Discuz_X3.2_SC_UTF8.zip
```

**Installation preparation work**

1. Execute the following command to extract the installation package.

   ```bash
   unzip Discuz_X3.2_SC_UTF8.zip
   ```

2. Execute the following command to copy all files under the extracted "upload" folder to the `var/www/html/`.

   ```bash
   cp -r upload/* /var/www/html/
   ```

3. Execute the following command to assign the write Permission to other users.

   ```bash
   chmod -R 777 /var/www/html
   ```

**Install Discuz!**

1. In the Web browser address bar, enter Discuz! The IP address of the site (that is, the public network IP address of Cloud Virtual Machine instance), you can see Discuz! Installation interface.
2. Click [I agree] to go to the check installation environment page.
3. Confirm that the current status is normal, and click "next" to go to the page of setting up the running environment.
4. Select a new installation and click "next" to go to the create database page.
5. According to the page prompt, Enter information, for Discuz! Create a database.

- Please use the Install the necessary software Set the root account and password to connect to the database, and set up the system mailbox, administrator account, password and Email.
- Please remember your administrator user and password.

6. Click [next] to start the installation.
7. After the installation is complete, click [your forum has completed installation, click this Access] to Access Forum.

FAQs

If you encounter problems in the process of using Cloud Virtual Machine, you can refer to the following documents and analyze and solve the problems according to the actual situation:

- For the login problem of Cloud Virtual Machine, please refer to Password and key 、 Login and remote connection .
- For Cloud Virtual Machine's network problems, please refer to IP address 、 Port and Security Group .
- Cloud Virtual Machine hard disk problem, please refer to System disk and data disk .
1. Installation and configuration of IIS

1.1. Example for Windows2012R2

1) Click "Start" at the bottom left corner of Windows CVM, select "Server Manager" to open the Server Manager interface.

2) Select "Add Roles and Features", then in "Before You Begin" in the "Add Roles and Features Wizard" pop-up box, click "Next". In "Installation Type", select "Role-based or Feature-based Installation", then click "Next".

3) In the left side of the window, select "Server Role" tab, check "Web Server (IIS)", click "Add Features" button in the pop-up box, and then click "Next".

4) In the "Features" tab, click "Next", and in the "Web Server Role (IIS)" tab, also click "Next".

5) In the "Role Services" tab, check the "CGI" option, then click "Next".

6) Confirm the installation and wait for the installation to be completed.

7) When the installation has been completed, access localhost in the browser of CVM to verify whether the installation is successful. The appearance of the following page indicates that the
installation has been completed successfully.

1.2. Example for Windows2008

1) Click "Server Manager" in the "Management Tool" in the "Start" menu at the bottom left corner of Windows CVM to open the Server Manager interface.

2) Click "Add Roles and Features" to add server roles. In this case, select "Web Server (IIS)", as shown below:
3) Click "Next". When selecting role services, check "CGI", as shown below:
4) After the settings are made, click "Install" to proceed with the installation:
5) Access the public network IP of Windows CVM via browser to check whether the IIS service is running normally. The appearance of the following page indicates that IIS has been installed and configured successfully.

![IIS7](image)

2. Installation and configuration of PHP

2.1. Installation of PHP 5.3 and earlier versions

1) Download the PHP installer (Download from: http://windows.php.net/download/), select the installer indicated in the following figure:
2) After the download, install PHP. When you need to select Web service, select "IIS FastCGI", as shown below:

3) Complete the installation of PHP under the guidance of installation interface.
4) Create a PHP file hello.php under C:/inetpub/wwwroot, as shown below:

The following content is written to the hello.php file:

```php
Test Page

echo "hello world";
?>
```

5) Access the public network IP of Windows CVM via browser to check whether the environment configuration has been completed successfully.

2.2. Installation of PHP versions above 5.3

For PHP versions above 5.3, the installer mode has been canceled, and the installation is only performed through zip file or debug pack. The following example shows the zip installation in Windows Server 2012R2 environment.

1) Download the PHP zip installer. Please note that you must select Non Thread Safe (NTS) x86 package when running under IIS. (If you have to select x64 package for PHP in Windows Server 32bit (x64), you cannot select IIS. In this case, you can use Apache as an alternative option)

Select the installer as shown below:
2) The installation of PHP versions above 5.3 depends on Visual C ++ Redistributable Update. Download and install VC Update Installer according to the name of downloaded PHP installer by referring to the relations as shown in the following table:

<table>
<thead>
<tr>
<th>PHP Installer Name</th>
<th>Download Link for Visual C ++ Redistributable Installer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Php-xxx-nts-Win32-VC14-x86.zip</td>
<td>Visual C ++ Redistributable for Visual Studio 2015</td>
</tr>
</tbody>
</table>
For example, if the downloaded PHP installer is the one shown as below,

```
php-7.0.6-nts-Win32-VC14-x86.zip
```

then download the installer for VS2015 version based on the relation indicated in the first row, and download and install the .exe file.

3) Unzip the PHP zip installer (in this case, extract to C:\PHP), copy php.ini-production and rename it to php.ini.

4) Click "Server Manager" - "IIS"; On the local IIS, right-click and select IIS Manager.

Click on the host name (IP) on the left to go to the home page, then double-click "Handler Mappings".

Click "Add Module Mappings" button on the right, fill in the following information in the pop-up box, and click "OK" to save.

If you are unable to select php-cgi.exe as the executable file, please change the file name extension of the selected file to .exe.

5) Click on the host name (IP) on the left to return to the home page, then double-click "Default Document".

Click "Add" button on the right to add the default document with the name of index.php.

6) Click on the host name (IP) on the left to return to the home page, then double-click "FastCGI Settings".

Select the path, click the "Edit" button on the right, then in the "Monitor the Changes Made to File", select the php.ini path.

7) Create a PHP file index.php under C:\inetpub\wwwroot, to which the following content is written:

```php
<?php
    phpinfo();
```
Save, visit http://localhost/index.php within from the CVM to verify whether PHP has been installed successfully:

![PHP Version 7.0.6](image)

<table>
<thead>
<tr>
<th>System</th>
<th>Windows NT 10_105_232_185 6.3 build 9600 (Windows Server 2012 R2 Standard)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build Date</td>
<td>Apr 28 2016 13:43:56</td>
</tr>
<tr>
<td>Compiler</td>
<td>MSVC14 (Visual C++ 2015)</td>
</tr>
<tr>
<td>Architecture</td>
<td>x80</td>
</tr>
<tr>
<td>Configure Command</td>
<td>cscipt/mysqli-config.js &quot;--enable-snapshot-build&quot; &quot;--enable-debug-pack&quot; &quot;--cscdk/oracle88/instantclient_12.2_rdk_shared&quot; &quot;--with-oci8-12c=c:\php-sdk\oracle\sdk\shared&quot; &quot;--enable-object-out-dir=./obj/&quot; &quot;--enable-config-is-shared&quot; &quot;--with-analyzer&quot; &quot;--with-pgo&quot;</td>
</tr>
<tr>
<td>Server API</td>
<td>CGI/FastCGI</td>
</tr>
<tr>
<td>Virtual Directory Support</td>
<td>disabled</td>
</tr>
<tr>
<td>Configuration File (php.ini) Path</td>
<td>C:\Windows</td>
</tr>
<tr>
<td>Loaded Configuration File</td>
<td>C:\PHP\php.ini</td>
</tr>
<tr>
<td>Scan this dir for additional .ini files</td>
<td>(none)</td>
</tr>
<tr>
<td>Additional .ini files parsed</td>
<td>(none)</td>
</tr>
<tr>
<td>PHP API</td>
<td>20151012</td>
</tr>
<tr>
<td>PHP Extension</td>
<td>20151012</td>
</tr>
<tr>
<td>Zend Extension</td>
<td>320151012</td>
</tr>
<tr>
<td>Zend Extension Build</td>
<td>API20151012,NTS,VC14</td>
</tr>
<tr>
<td>PHP Extension Build</td>
<td>API20151012,NTS,VC14</td>
</tr>
</tbody>
</table>
Step2: Install and Configure PHP

This document introduces the PHP configuration of Windows CVM. For more information, please see Installation of PHP versions above 5.3 and Installation of PHP 5.3 and earlier as needed.

Prerequisites

To configure PHP in Windows CVMs, you need to add and install IIS role. For more information, please see Installing and Configuring IIS.

Installation of PHP Versions above 5.3

For PHP versions above 5.3, the installer mode has been canceled, and the installation is only performed through zip file or debug pack. The following example shows the zip installation in Windows Server 2012 R2 environment.

Downloading File

1. Download the PHP zip installer from the CVM (download URL: http://windows.php.net/download/).

Note:

You must select Non Thread Safe (NTS) x86 package when running under IIS. If you have to select x64 package for PHP in Windows Server 32bit (x64), you cannot select IIS. In this case, you can use Apache as an alternative option.
Select the installer as shown below:

<table>
<thead>
<tr>
<th>PHP 7.0 (7.0.6)</th>
<th>Download source code [24.08MB]</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC14 x86 Non Thread Safe (2016-Apr-29 00:38:17)</td>
<td>[20.93MB]</td>
</tr>
<tr>
<td>sha1: c0548e3f4def7e22f1a0dab243709b0676077aa</td>
<td></td>
</tr>
<tr>
<td>Debug Pack [14.85MB]</td>
<td>[14.85MB]</td>
</tr>
<tr>
<td>sha1: d17bfc89bda7a716de0dad0e11424b7598ac0db</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PHP 5.6 (5.6.21)</th>
<th>Download source code [24.15MB]</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC11 x86 Non Thread Safe (2016-Apr-28 06:19:34)</td>
<td>[20.29MB]</td>
</tr>
<tr>
<td>sha1: 46f159ee7be2307aca4d8d5f80034f11c7fff5d2</td>
<td></td>
</tr>
<tr>
<td>Debug Pack [9.68MB]</td>
<td>[9.68MB]</td>
</tr>
<tr>
<td>sha1: 6aba9b880ddc8c5c6ed73559fbf03649d2c82f9</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PHP 5.5 (5.5.35)</th>
<th>Download source code [23.33MB]</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC11 x86 Non Thread Safe (2016-Apr-28 00:53:27)</td>
<td>[18.77MB]</td>
</tr>
<tr>
<td>sha1: 0347532a5c257e7611532a811c5a17af719718d</td>
<td></td>
</tr>
<tr>
<td>Debug Pack [9.33MB]</td>
<td>[9.33MB]</td>
</tr>
<tr>
<td>sha1: af3dbcb981551098ea4b6321938dfdd2175d7968</td>
<td></td>
</tr>
</tbody>
</table>
2. The installation of PHP versions above 5.3 is dependent on Visual C++ Redistributable Update. Download and install VC Update Installer according to the name of downloaded PHP installer by referring to the relations as shown in the following table:

<table>
<thead>
<tr>
<th>PHP Installer Name</th>
<th>Download Link for Visual C++ Redistributable Installer</th>
</tr>
</thead>
<tbody>
<tr>
<td>php-x.x.x-nts-Win32-VC14-x86.zip</td>
<td>Visual C++ Redistributable for Visual Studio 2015</td>
</tr>
<tr>
<td>php-x.x.x-nts-Win32-VC11-x86.zip</td>
<td>Visual C++ Redistributable for Visual Studio 2012 Update 4</td>
</tr>
<tr>
<td>php-x.x.x-nts-Win32-VC9-x86.zip</td>
<td>Microsoft Visual C++ 2008 SP1 Redistributable Package (x86)</td>
</tr>
</tbody>
</table>

If the downloaded PHP installer is as shown below:

![php-7.0.6-nts-Win32-VC14-x86.zip](image)

then download the installer for VS 2015 version based on the relation indicated in the first row, and download and install the following two `.exe` files:

**Installation and configuration**

1. Unzip the PHP zip installer (in this case, extract to `C:\PHP`), copy `php.ini-production` and rename it to `php.ini`, as shown below:

2. Click **Server Manager** -> **IIS**; On the local IIS, right-click and select **IIS Manager**:

Click on the host name (IP) on the left to go to the home page, and then double-click **Handler Mappings**:

Click **Add Module Mappings** on the right, enter the following information in the pop-up box, and click **OK** to save:

**Note:**
If you are unable to select `php-cgi.exe` as the executable file, please change the filename extension of the selected file to `.exe`:
3. Click the server IP on the left to go to the home page and double-click **Default Documents**:

   Click **Add** on the right to add a default document named `index.php`.

4. Click the server IP on the left to go to the home page and double-click **FastCGI Settings**:

   Click **Edit** on the right, and select `php.ini` path in **Monitor the Changes Made to File**.

5. Create a PHP file `index.php` under `C:\inetpub\wwwroot` and write the following:

   ```php
   <?php
   phpinfo();
   ?>
   ```

6. Visit `http://localhost/index.php` in the browser on CVM and check whether the environment has been configured successfully. The appearance of the following page indicates that the
configuration has been completed successfully:

![PHP Version 7.0.6](http://localhost/index.php?phpinfo)

### Installation of PHP 5.3 and earlier versions

**Note:**

PHP 5.3 and earlier versions are no longer available on the official download address http://windows.php.net/download/. To use these versions, download them locally and upload them to the CVM or search on the CVM network. For more information on uploading files, please see [here](#).

1. Open PHP installer in the CVM.
2. Select **IIS FastCGI** in **Web Server Setup**, as shown below:

![Web Server Setup](image)

3. Complete the installation of PHP under the guidance of installation interface.

4. Create a PHP file `hello.php` under `C:/inetpub/wwwroot`, as shown below:

![Create PHP File](image)

The following content is written to the `hello.php` file:

```php
<?php
    echo "<title>Test Page</title>";
    echo "hello world";
?>
```
5. Access the public network IP of Windows CVM via browser to check whether the environment configuration has been completed successfully. The appearance of the following page indicates that the configuration has been completed successfully:
Step 3: Install and Build MySQL

Last updated: 2019-12-03 18:06:32

This document uses Windows Server 2012 R2 as an example to introduce how to build MySQL 5.5. SQL Server database is frequently used in Windows system. You need to grant authorization for SQL Server because it is not for free. You can also purchase CDB instances for Tencent Cloud SQL Server database.

Step 1: Download MySQL installer

Open the browser on the CVM and enter the download URL: https://dev.mysql.com/downloads/mysql/5.5.html#downloads

Step 2: Install the application

1. Run the installation program. Click Next and select I accept the terms in the License Agreement.
2. Select **Typical** in **Choose Setup Type**.
3. Select **Launch the MySQL Instance Configuration Wizard**.

![MySQL Instance Configuration Wizard](image)

**Step 3: Configure MySQL**

1. Configure the type of MySQL. Here we use Detailed Configuration as an example.

   - Detailed Configuration is suitable for advanced users that need to have finer control of the CVM configurations.
   - Standard Configuration is suitable for new users that want to launch MySQL quickly without considering the CVM configurations.

   **Note:**
   Standard Configuration may be incompatible with your operating system. Detailed Configuration is recommended.
2. Configure the type of MySQL server. Here we use Developer Machine as an example.

- Developer Machine represents a typical personal desktop workstation. When multiple desktop applications are running at the same time, the MySQL server is configured to use minimal system resources.
- Server Machine is a type of server on which MySQL server can run with other applications such as FTP, email and Web servers. The MySQL server is configured to use a moderate portion of the system resources.
- Dedicated MySQL Server Machine is a type of server on which only MySQL server can run. The MySQL server is configured to use all available system resources.
3. Configure MySQL database. Here we use Multifunctional Database as an example.

- Multifunctional Database uses InnoDB and MyISAM storage engines simultaneously, and allocates resources to them equally. You are recommended to select this option if you often use two storage engines simultaneously.
- Transactional Database Only uses InnoDB and MyISAM storage engines simultaneously, and allocates most server resources to InnoDB storage engine. You are recommended to select this option if you use InnoDB frequently and use MyISAM occasionally.
- Non-Transactional Database Only does not use InnoDB storage engine, and allocates all server resources to MyISAM storage engine. You are recommended to select this option if you do not use InnoDB.
4. Configure the InnoDB tablespace for MySQL. Choose default configuration here.
5. Configure concurrent connection for MySQL. Here we use Decision Support as an example.

- Decision Support is suitable for situations that do not require a large number of concurrent connections.
- Online Transaction Processing is suitable when a large number of concurrent connections are required.
- Manual Setting is suitable when you need to configure the maximum number of concurrent connections manually.

![MySQL Server Instance Configuration Wizard](image)

6. Configure the network options of MySQL. You can enable or disable TCP/IP network and configure the port number for MySQL server connection.

**Notes:**

TCP/IP network is enabled by default.
Port 3306 is used by default.
7. Configure MySQL character set. Here we use Standard Character Set as an example.

- Standard Character Set uses Latin1 as the default server character set.
- Best Support For Multilingualism uses UTF8 as the server character set.
- For Manual Selected Default Character Set/Collation, select the character set in the drop-down box as needed.
8. Configure the service options of MySQL. It is recommended to select both boxes to manage MySQL using command line.
9. Set the root password.

0. Complete the configuration. Click **Execute** to complete the installation.
Step 4: Login Test for MySQL

1. Click **Start** on the CVM and click the search icon. Enter `cmd` to open the administrator command box:

![Start Menu](image)

2. Enter the command `mysql -u root -p` and press **Enter**.

3. Log in to MySQL using the root password you set. The picture below indicates that MySQL has been installed and configured successfully.
Cloud Virtual Machine

©2013-2019 Tencent Cloud. All rights reserved.
Build the FTP Service

Build the FTP Service (Linux)

Last updated : 2020-02-25 12:19:07

Scenario

Vsftpd (very secure FTP daemon) is the default FTP server in many Linux distributions. This paper takes the Tencent Cloud server (CVM) of CentOS 7.6 64-bit operating system as an example, and uses vsftpd software to build the FTP service of Linux Cloud Virtual Machine.

Software Versions

The component version of the FTP service built in this paper is as follows:

- Linux: Linux operating system. In this example, CentOS 7.6 is used.
- Vsftpd: this article takes vsftpd 3.0.2 as an example.

Directions

Step 2: Purchase cloud virtual machine

- Log in to a Linux instance in standard login mode (recommended). You can also use other login methods as needed:
- Logging In to a Linux Instance by Using Remote Logging Software
- Logging In to a Linux Instance via SSH

Step 1: Install vsftpd

1. Execute the following command to install vsftpd.

   ```bash
   yum install vsftpd -y
   ```

2. Execute the following command to set up vsftpd Start up from Launch.

   ```bash
   systemctl enable vsftpd
   ```

3. Execute the following command, Launch FTP service.
4. Execute the following command to confirm whether the service has been started.

```bash
netstat -antup | grep ftp
```

If the result is shown below, it means that the FTP service has been successful, Launch.

![Command Output](image)

At this time, vsftpd has enabled anonymous Access mode by default, and you can log in to the FTP server without using a user name and password. Users who log in to the FTP server in this way do not have the right to modify or upload files to Permission.

**Step 3: configure vsftpd**

1. Execute the following command to create a user for the FTP service. This article takes ftpuser as an example.

```bash
useradd ftpuser
```

2. Execute the following command to set the password for the ftpuser user.

```bash
passwd ftpuser
```

After entering the password, please press Enter Confirm the setting. The password is not displayed by default. tf7295TFY As an example.

3. Execute the following command to create a file used by the FTP service, Directory, which is based on the `/var/ftp/test` As an example.

```bash
mkdir /var/ftp/test
```

4. Execute the following order to modify Directory Permission.

```bash
chown -R ftpuser:ftpuser /var/ftp/test
```

5. Run the following command to open the `nginx.conf` File.
vim /etc/vsftpd/vsftpd.conf

6. By I Switch to edit mode, select FTP mode according to the actual needs, and modify the configuration file. vsftpd.conf:

FTP can connect and transfer data to client machines through active mode and passive mode. Due to the firewall settings of most client machines and the inability to get the real IP, it is recommended that you choose **Passive mode** Build the FTP Service. The following modifications take setting the passive mode as an example. If you want to choose the active mode, please go to **Set FTP active mode**.

1. Modify the following configuration parameters, set the login Permission for anonymous and local users, set the path to the list file of specified exception users, and enable listening IPv4 sockets.

```
anonymous_enable=NO
local_enable=YES
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
listen=YES
```

2. Add at the beginning of the line #, comment listen_ipv6=YES Configure parameters to turn off listening IPv6 sockets.

```
#listen_ipv6=YES
```

3. Add the following configuration parameters, turn on the passive mode, set the location of Directory after the local user logs in, and Cloud Virtual Machine establish the port range values that can be used for data transmission.

```
local_root=/var/ftp/test
allow_writeable_chroot=YES
pasv_enable=YES
pasv_address=xxx.xx.xxx.xx #Please modify it to your Linux CVM public network IP
pasv_min_port=40000
pasv_max_port=45000
```

7. By Esc After input : wq Save and exit.
8. Execute the following command to create and edit `/etc/vsftpd/chroot_list` file.

```
  vim /etc/vsftpd/chroot_list
```

9. By I Enter the edit mode, enter the user name, one user name occupies one line, and press Esc
   And enter : wq Save and exit.

   If you do not set the requirements of the exception user, you can skip this step and enter : wq
   Exit the file.

0. Restart the FTP service by executing the following command.

```
  systemctl start vsftpd
```

### Step 4: Configure security group

After building the FTP service, you need to give the Linux Cloud Virtual Machine Open to Internet
according to the FTP model actually used **Inbound policy**.

Most client machines are in the local area network, and IP addresses are translated. If you choose
FTP active mode, make sure that the client machine has obtained the real IP address, otherwise the
client may not be able to log on to the FTP server.

- Active mode: Open to Internet port 21.
- Passive mode: Open to Internet port 21, and Modify configuration file Set in `paspv_min_port` to
  `paspv_max_port` All ports between, this article Open to Internet port is 40000-45000.

### Step 5: verify the FTP service

You can verify the FTP service through tools such as FTP client software, browser, or file explorer.
This article takes the file explorer on the client side as an example.

1. Open the client's IE browser, select ** tools *-*-> ** Internet options *-*-> ** Advanced * *, and
   modify it according to the FTP mode you selected:

   - Active mode: uncheck [use passive FTP].
   - Passive mode: check [use passive FTP].

2. Open the client's computer and in the path bar, the address below Access.

```
  ftp://CVM public network IP:21
```
3. In the pop-up Login as window, enter **Configuring vsftpd**. The user name and password that have been set in the.
   The user name used in this article is `ftpuser`. The password is `tf7295TFY`.
4. After successfully logging in, you can upload and download files.

**Appendix**

**Set FTP active mode**

The configurations that need to be modified in active mode are as follows, and the rest of the configurations remain at the default settings:

```
Anonymous_enable=NO  # prohibits anonymous users from logging in.
Local_enable=YES    # supports local user login.
Chroot_local_user=YES # all users are restricted to the home directory.
Chroot_list_enable=YES # enable the list of exceptional users.
Chroot_list_file=/etc/vsftpd/chroot_list # specifies the user list file in which users are not locked in the home directory.
Listen=YES  # listening on IPv4 sockets.
# add # at the beginning of the line and comment out the following parameters.
# listen_ipv6=YES # turn off listening IPv6 sockets.
# add the following parameters.
Allow_writeable_chroot=YES.
Local_root=/var/ftp/test # sets the directory where local users log in
```

By Esc After input : wq After saving, exit and go to Step 8 Complete the vsftpd configuration.

**FTP client failed to upload files**

**Problem Description**

In Linux environment, users get the following error message when uploading files with vsftpd.

```
553 Could not create file
```

**Solution**

1. Execute the following command to check the utilization of server disk space.

   `df -h`

   * If there is not enough disk space, you will not be able to upload files. It is recommended to delete some large files.
• If there is enough disk space, go to the next step.

2. Execute the following command to check if the FTP directory has the Write permission.

```bash
ls -l /home/test
# /home/test is the FTP directory. Change it to your actual FTP directory.
```

• If there is no `w` in the returned result, it means that the user does not have the permission to write to the directory. Please go to the next step.

• If there is a `w` in the returned result, please Submit a ticket.

3. Execute the following command to add the Write permission to the FTP directory.

```bash
chmod +w /home/test
# /home/test is the FTP directory. Change it to your actual FTP directory.
```

4. Execute the following command to check whether the Write permission is added successfully.

```bash
ls -l /home/test
# /home/test is the FTP directory. Change it to your actual FTP directory.
```
Build the FTP Service (Windows)

Last updated: 2020-02-25 12:21:09

**Scenario**

This document describes how to build a FTP site through IIS on Tencent Cloud server (CVM) of the Windows operating system.

**Software Versions**

The component version of the FTP service built in this paper is as follows:

- Windows operating system, this paper takes Windows Server 2012 as an example.
- IIS: Web server, this paper takes IIS 8.5 as an example.

**Directions**

**Step 2: Purchase cloud virtual machine**

- Logging In to a Windows Cloud Virtual Machine Instance by Using an RDP File (Recommended)
- Logging In to a Windows Cloud Virtual Machine Instance by Using a Remote Desktop

**Step 2: install the FTP service on IIS**

2. In the operating system interface, click To open Server Manager, as shown below:
3. In the Server Manager window, click add roles and Features.
4. In the pop-up add roles and Features Wizard window, click next to enter the Select installation Type interface.
5. In the Select installation Type interface, select role-based or feature-based installation, and click next.
6. In the Select Target Server interface, keep the default settings and click next.
7. In the “Select a server role” interface, check [Web Server (IIS)], and click "add feature" in the pop-up window.
8. Click next three times in a row to enter the Select role Service interface.
9. In the "Select role Service" interface, check "FTP Service" and "FTP extension", and click "next".
10. Click "install" to begin the installation of the FTP service.
11. When the installation is complete, click [close].

**Step 3: create a FTP username and password**
Please follow these steps to configure the FTP user name and password. If you need to use the anonymous user Access FTP service, you can skip this step.

1. In the Server Manager window, select tools > computer Management in the navigation bar in the upper right corner to open the computer Management window.
2. In the computer Management interface, select [system tools] > [Local users and groups] > [users] in Left sidebar.
3. In the right side of the user interface, right-click the blank space and select New user.
4. In the New user interface, follow the prompts below to set the user name and password, and click create.
   The main parameters are as follows:
   - User name: custom, this article uses ftpuser As an example.
   - Password and confirmation password: custom, password must contain both uppercase and lowercase letters and numbers. In this paper, tf7295TFY As an example.
   - Uncheck [users must change their password the next time they log in] and check [password will never Expire].
     Please check it according to the actual demand. This article takes the password never Expire as an example.
5. Click [close], and after closing the New user window, you can view the created ftpuser User.

Step 4: set up the shared folder Permission

You need to set up a shared folder for your FTP site, which is based on the C:\test A folder, for example, already contains files to be shared test.txt.

2. In the operating system interface, click  To open Server Manager, as shown below:
3. Under disk C, select and right-click test Folder, select [Properties].
4. In the test Properties window, select the Security tab.
5. Select Everyone User and click [Edit], as shown below:
   If it is not in the Group or user name Everyone , please refer to Add Everyone user To add.
6. In the "Permission of test" interface, set on demand Everyone The user's Permission and click [OK], as shown below:
   This article is intended to award Everyone User-owned Permission as an example.
7. In the test Properties window, click OK to complete the settings.

**Step 5: add a FTP site**

1. In the Server Manager window, select tools > Internet Information Services (IIS) Manager in the navigation bar in the upper right corner.
2. In the Internet Information Services (IIS) Manager window that opens, click the server name of show more Left sidebar, then right-click [website], and select [add FTP site].
3. In the site Information interface, refer to the following information to set up, and click next.
   - **FTP site name** Enter FTP site name, this article uses ftp As an example.
   - **Physical path** Please select the shared folder path that has been set for Permission. C:\test

4. In the binding and SSL Settings interface, refer to the following information for settings, and click next.

   The main configuration parameter information is as follows:
   - **Bind** The IP address is selected as "all without Assign" by default, and the port is 21 by default (the default port number for FTP). You can also set the port by yourself.
   - **SSL** Please select as needed. This article takes [No SSL] as an example.
     - **No SSL** No SSL encryption is required
     - **Allow SSL** Allows the FTP server to support non-SSL and SSL connections to clients
     - **Require SSL** Requires SSL encryption to communicate between the FTP server and the client
   
   If you select [allow SSL] or [need SSL], you can select the existing SSL Certificates Service in "SSL Certificates Service", or refer to Server certificate making Step to make a SSL Certificates Service.

5. In the Authentication and Authorization Information interface, refer to the following information to set up, and click next.

   - **Identity Verification** Select an authentication method. This article takes basic as an example.
     - **Anonymous** Allow any user Access to provide only anonymous or FTP user name content.
     - **Basic** Users are required to provide a valid user name and password to enable Access content. Because basic authentication transmits unencrypted passwords over the network, you use this authentication method only if you know that the connection between the client and the FTP server is secure (for example, by using secure socket layer SSL).
   - **Authorize** Select a method from the allow Access drop-down list to specify users ftpuser As an example.
     - **All users** All users, whether anonymous or identified, can Access this content.
     - **Anonymous user** Anonymous users can have Access content.
     - **Specified role or user group** Only members of certain roles or user groups can have Access content. Select this option to specify a role or user group.
Specified user Only specified users can have Access content. Select this option to specify a user name.

Permissions Set Permission as needed. This article takes setting [read] and [write] Permission as an example.

- Read Allow authorized users to read content from Directory.
- Write Allow authorized users to write to Directory.

7. Click "finish" to create the FTP site successfully.

Step 6: set up security groups and firewalls

1. After completing the construction of the FTP site, ask Open to Internet to add the inbound rules of the port when adding the FTP site, such as the inbound rule of port 21.
   If you choose a different port when adding a FTP site, you also need to add an inbound rule for pass this port in the firewall.
2. (optional) referenc Microsoft official documentation Configure firewall support for the FTP site to enable the FTP server to accept passive connections from the firewall.

Step 7: test the FTP site

You can verify the FTP service through tools such as FTP client software, browser, or file explorer. This article takes the file explorer on the client side as an example.

1. Please set up your IE browser according to your actual situation:
   - Configured FTP site firewall: open the client’s IE browser, select [tools] > [Internet options] > [Advanced], uncheck [use passive FTP (for firewall and DSL modem compatibility)] and click "OK".
   - The FTP site firewall is not configured:
     i. Enable FTP server IE browser, select [tools] > [Internet options] > [Advanced], uncheck [use passive FTP (for firewall and DSL modem compatibility)] and click "OK".
     ii. Enable Client IE browser, select [tools] > [Internet options] > [Advanced], check [use passive FTP (for firewall and DSL modem compatibility)] and click [OK].

2. Open the client’s computer and in the path bar, the address below Access.

   ftp://CVM public network IP:21

3. In the pop-up Login as window, enter Create FTP username and password The user name and password that have been set in the.
   The user name used in this article is ftpuser The password is tf7295TFY.
4. After successfully logging in, you can upload and download files.

Appendix

Add Everyone user

1. In the test Properties window, select the Security tab and click Edit.
2. In the "Permission of test" interface, click [add].
3. In the Select user or Group interface, click Advanced.
4. In the pop-up Select user or Group interface, click find now.
5. In the search results, select Everyone And click [OK].
6. In the Select user or Group interface, click OK to add.
   Go to Step 5 Settings Everyone User permissions.

Server certificate making

1. In the Server Manager window, select tools > Internet Information Services (IIS) Manager in the navigation bar in the upper right corner.
2. In the pop-up Internet Information Services (IIS) Manager window, select the server in Left sidebar, and double-click Server Certificate in the right screen.
4. In the pop-up create self-signed Certificate window, set the certificate name and storage class. This paper takes SSL Certificates Service who created the personal storage class as an example.
5. Click "OK" to create it successfully.
The NTP Service

The NTP service of Tencent Cloud

Last updated: 2020-02-25 13:33:57

Network time Protocol (Network Time Protocol, NTP), Protocol, who is used to synchronize the time of each computer in the network. Its purpose is to synchronize the computer's clock to the Universal time UTC.

Tencent Cloud provides an intranet NTP server for Tencent Cloud intranet devices. For non-Tencent cloud devices, you can use the public network NTP server provided by Tencent Cloud.

**Intranet NTP Server**

```plaintext
ntupdate.tencentyun.com
```

**Public Network NTP Server**

```plaintext
time1.cloud.tencent.com
time2.cloud.tencent.com
time3.cloud.tencent.com
time4.cloud.tencent.com
time5.cloud.tencent.com
```

For more information on Linux system settings NTP clock source server, please see "Linux instance Settings NTP Service".

For more information on Windows system settings NTP clock source server, please see "Windows instance Settings NTP Service".
Set the NTP service on a Windows instance

Scenario

This document is about how to enable NTP service for Windows Server and modify the clock source server address.

Windows Time service (W32Time) is used to synchronize the time of the local system and the clock source server. It uses NTP to synchronize computer clocks throughout the network. The following describes how to enable NTP service and modify the clock source server address via client and command line for Windows Server 2016.

Directions

1. Log in to the Windows instance remotely.
2. Click “Administrative Tools > Services > Windows Time”.
3. The startup type is set to "Automatic" and if the service is not started, click "Start".
4. In the notification area of the taskbar, click Time and click “Date and time settings”.

![Date and time settings](image)
5. Switch to the "Internet Time" tab and click Change Settings.

6. In the Internet Time Settings pop-up window, enter the domain name or IP address of the target clock source server and click “OK”.

![Internet Time Settings](image)
7. After you complete the setup, reopen “Date & Time” and you will see that the clock source server has been changed.
This computer is set to automatically synchronize with 'ntpupdate.tencentyun.com'.

Next synchronization: 7/24/2019 at 4:25 PM

The clock was successfully synchronized with ntpupdate.tencentyun.com on 7/24/2019 at 4:20 PM.
Set the NTP service on a Linux instance

Last updated: 2019-10-14 11:08:34

Scenario

The Network Time Protocol daemon (ntpd) is a daemon of the Linux operating system. It is a complete implementation of NTP and is used to correct the time difference between the local system and the clock source server. Unlike ntpdate which updates time periodically, ntpd corrects time continuously without time gaps. This document describes how to install and use ntpd.

Notes

- Some operating systems use chrony as the default NTP service. Use `systemctl is-active ntpd.service` to check if ntpd is running; use `systemctl is-enabled ntpd.service` to check if ntpd automatically run at startup. For details, please refer to the section on how to set the automatic launch of ntpd on startup.
- The communication port of the NTP service is UDP 123. Make sure you have opened the port before setting the NTP service. You can check if the port is open on the instance with `netstat -nupl`. For information on how to open the port, please see Operation Guide on Security Groups.

Note:
The following takes operations on a CentOS 7.5 64bit instance as an example.

Directions

Installation

- Use the following command to determine if ntpd has been installed:

  `rpm -qa | grep ntp`
If it has not been installed, use `yum install ntp` to install it. If you do not make any configuration, ntpd will work in client mode by default.

```
yum -y install ntp
```

### Configuration

- Open and edit NTP service configuration file with vim.

```
vi /etc/ntp.conf
```

- Find the configuration for server, change the server to the NTP clock source server you want to use, and delete the NTP clock source servers you do not need for the time being.

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
servers 0.centos.pool.ntp.org iburst
servers 1.centos.pool.ntp.org iburst
servers 2.centos.pool.ntp.org iburst
servers 3.centos.pool.ntp.org iburst
```

### Start

- Start the NTP service with `service ntpd start`. If NTP has already been started, restart it with `service ntpd restart`.

```
service ntpd start
```

```
[root@VM_16_2_centos ~]# service ntpd start
Redirecting to /bin/systemctl start ntpd.service
```

### Status Check

- Check whether UDP 123, the NTP service port, is monitored normally with `netstat`.

```
netstat -nupl
```
Check whether the ntpd status is normal with the following command:

```
service ntpd status
```

Use `ntpstat` to see if ntpd is properly started and configured to the correct NTP clock source server. This command outputs the IP address of the current NTP clock source server. This IP address should be the IP address of the NTP clock source server you configured above (you can use the `nslookup domain name` to obtain the IP address corresponding to the domain name).
You can get more detailed information on the NTP service with `ntpq -p`.

```
[root@VM_16_2_centos ~]# ntpq -p
remote  refid  st t when poll reach delay offset jitter
*169.198.138.183  183.144.198.200  4 u  40  64 377  0.854  0.958  0.182
```

- **remote**: the name of the NTP server that responds to this request.
- **refid**: the NTP server one stratum above to which the NTP server on this stratum is synchronized.
- **st**: the stratum of the remote server. NTP uses a hierarchical structure with a server at the top, multiple relay servers in the middle, and the client at the bottom. The stratum of a server can be set to 1 to 16 from the top to the bottom. In order to relieve the load and network congestion, in principle, you should avoid connecting directly to a stratum 1 server.
- **when**: how many seconds has elapsed since the last successful request.
- **poll**: the synchronization interval (in seconds). At the beginning, the poll value will be smaller, which means higher frequency of synchronization with the server, so that the time can adjusted to the correct time range as soon as possible. Later, the poll value will gradually increase, and the synchronization frequency will be lower accordingly.
- **reach**: an octal value used to test whether the server can be connected. Its value increases every time when the server is successfully connected.
- **delay**: the round trip time of sending the synchronization request from the local machine to the NTP server.
- **offset**: the difference in milliseconds (ms) between the host time synchronized through NTP and the time of the time source. The closer the offset is to 0, the closer the time of the host and the NTP server is.
- **jitter**: a value used for statistics which records the distribution of offsets over a particular number of consecutive connections. Simply put, the smaller its absolute value is, the more accurate the host time is.

**Setting the automatic launch of ntpd on startup**

- Set the automatic launch of ntpd on startup with the command below.

```
systemctl enable ntpd.service
```
• Use the command below to see if chrony is set to launch at startup.

```
systemctl is-enabled chronyd.service
```

• chrony is not compatible with ntpd, which may lead to ntpd start failure. Use the following command to remove chrony from the list of software that runs at startup.

```
systemctl disable chronyd.service
```