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

Setting up WordPress

Manually Build WordPress Website
Manually build WordPress personal site (Windows)

Network Performance Test

Setting up LNMP

Manually Building an LNMP Environment (CentOS 7)
Setting up LNMP manually (CentOS 6)
Setting up LNMP Manually (openSUSE)

Setting up Node.js

Setting up Node.js manually

Setting up Java Web

Setting up Java Web Manually

Setting up LAMP manually

Setting up LAMP manually

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)

Setting up a Website

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

Setting up a Ghost Blog

Setting up Drupal
Best Practice

Best Practices

Last updated: 2020-02-25 13:33:26

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.
Setting up WordPress
Manually Build WordPress Website

Scenario

WordPress is a blog platform developed in PHP. This document describes how to manually build a private WordPress site on a Tencent Cloud CVM with CentOS 7.6.

To build a WordPress site, you must be familiar with common Linux commands, such as those for installing software through YUM in the CentOS environment. In addition, you need to know how to use the involved software programs and their version compatibility details.

Software

The following software programs are used to build the WordPress site:

- Linux: Linux operating system. This document uses CentOS 7.6 as an example.
- Nginx: web server. This document uses Nginx 1.17.5 as an example.
- MariaDB: database. This document uses MariaDB 10.4.8 as an example.
- PHP: scripting language. This document uses PHP 7.2.22 as an example.
- WordPress: blog platform. This document uses WordPress 5.0.4 as an example.

Directions

**Step 1: Log in to the CVM**

Log in to a Linux instance by using WebShell (recommended). You can also use either of the following login methods that you are comfortable with.

- Logging into a Linux Instance by Using Remote Login Tools
- Logging into a Linux Instance by Using the SSH Key

**Step 2: Manually build an LNMP environment**

LNMP is the acronym for Linux, Nginx, MariaDB, and PHP. It is one of the most common runtime environments for web servers. After creating and logging in to a CVM instance, you can build an
Step 3: Configure the WordPress database

The user authentication method varies depending on the MariaDB version. For details, visit the MariaDB official website.

1. Run the following command to enter MariaDB:
   
   `mysql`

2. Run the following command to create a MariaDB database, such as `wordpress` in this example:
   
   ```
   CREATE DATABASE wordpress;
   ```

3. Run the following command to create a user and specify a password, such as the `user` user with the password `123456` in this example:
   
   ```
   CREATE USER 'user'@'localhost' IDENTIFIED BY '123456';
   ```

4. Run the following command to grant `user` all permissions to the `wordpress` database:
   
   ```
   GRANT ALL PRIVILEGES ON wordpress.* TO 'user'@'localhost' IDENTIFIED BY '123456';
   ```

5. Run the following command for all configurations to take effect:
   
   ```
   FLUSH PRIVILEGES;
   ```

6. Run the following command to exit MariaDB:
   
   `\q`

Step 4: Configure a root account

1. Run the following command to enter MariaDB:
   
   `mysql`

2. Run the following command to set a password for `root`:
   
   ```
   MariaDB 10.4 for CentOS allows the root account to log in without a password. Run the following command to set a password for root and save it in a safe place:
   ```
ALTER USER root@localhost IDENTIFIED VIA mysql_native_password USING PASSWORD('Enter your password');

3. Run the following command to exit MariaDB:

   \q

Step 5: Install and configure WordPress

Downloading WordPress

You can download the latest version of WordPress from the official WordPress website.

1. Run the following command to delete the `index.php` file that is used to test PHP-Nginx configuration from the root directory of the website:

   ```bash
   rm -rf /usr/share/nginx/html/index.php
   ```

2. Run the following commands to navigate to the `/usr/share/nginx/html/` directory and download and decompress the WordPress installation package:

   ```bash
   cd /usr/share/nginx/html
   wget https://cn.wordpress.org/wordpress-5.0.4-zh_CN.tar.gz
   tar zxvf wordpress-5.0.4-zh_CN.tar.gz
   ```

Modifying the WordPress configuration file

1. Run the following commands to navigate to the WordPress installation directory, copy the content of the `wp-config-sample.php` file to the `wp-config.php` file, and save the original configuration file for backup:

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

2. Run the following command to open and edit the new configuration file:

   ```bash
   vim wp-config.php
   ```
3. Press i to enter the editing mode. Find the MySQL section in the file and modify the settings as described in Configuring the WordPress database.

```
// ** 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');
```

4. After finishing the modification, press Esc and enter :wq. Then, save the changes and close the file.

**Step 6: Verify WordPress installation**

1. In the address box of the browser, enter http://<Domain name or public IP address of the CVM instance>/<WordPress folder>, for example:

   ![http://192.xxx.xxx.xx/wordpress](http://192.xxx.xxx.xx/wordpress)

   Press Enter to go to the WordPress installation page and configure WordPress.

2. Complete the following installation information as instructed in the WordPress installation wizard. Then, click **Install WordPress**.

<table>
<thead>
<tr>
<th>Required information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site title</td>
<td>WordPress site name</td>
</tr>
<tr>
<td>Username</td>
<td>WordPress administrator name. For security purposes, use a name other than admin, which is prone to be cracked.</td>
</tr>
<tr>
<td>Password</td>
<td>Use the default strong password or a custom password. Do not use previous passwords and save the password in a secure place.</td>
</tr>
</tbody>
</table>
Now, you can log in to your WordPress site and post blogs.

Relevant Operations

You can set a domain name for your WordPress site. In this way, users can use the domain name instead of a complex IP address to visit your site. If you are building the site for learning purposes, you can set an IP address for the site. However, this practice is not recommended for other cases.

FAQs

If you encounter issues when using a CVM, refer to the following documents for troubleshooting based on your actual situation.

- For issues regarding CVM login, see [Password Login and SSH Key Login](#) and [Login and Remote Access](#).
- For issues regarding the CVM network, see [IP Addresses](#) and [Ports and Security Groups](#).
- For issues regarding CVM disks, see [System and Data Disks](#).
Manually build WordPress personal site (Windows)

Introduction

WordPress is a blog platform written in PHP. This article describes how to install WordPress on Windows Server 2012.

Software

Although PHP version 5.6.20 and later and MySQL version 5.0 and later support WordPress, we recommend using PHP 7.3 and MySQL 5.6 or later versions for security reasons.

These are the software involved:

- Operating system: Windows Server 2012
- Web server: IIS 8.5
- Database: MySQL 5.6.46
- Hypertext interpreter: PHP 7.3.12
- Blog platform: WordPress 5.3

Procedure

Step 1: Logging in to Windows CVM

- Log in to a Windows CVM Using an RDP File (Recommended)
- Log in to a Windows CVM Using a Remote Desktop

Step 2: Setting up WIMP

1. Install IIS.
2. Deploy PHP 5.6.20 or later.
3. Install MySQL 5.6 or later.

Step 3: Installing and configuring WordPress
You can download the latest version of WordPress from the official WordPress website.

1. Download WordPress and decompress it to a directory on the CVM. For example, you can decompress it to `C:\wordpress`.

2. Right-click ![Folder](folder.png). Input `cmd` in Run and press Enter to open a command line window.

3. Run the following commands in the command line window to create a database for WordPress. For example, create a database named `wordpress`.

   ```sql
   create database wordpress;
   ```


5. Use a text editor to open `wp-config.php` and edit the configuration information as detailed in Step 4: Installing MySQL.


7. Click ![Server Manager](server_manager.png) to open Server Manager.

8. In the navigation panel to the left, select IIS. Right-click the name of the server in the Server column and select Internet Information Services (IIS) Manager to open the Internet Information Services (IIS) Manager window.

9. In the Internet Information Service (IIS) Manager window, expand your server in the left navigation panel and select your website. This opens the website management page.

10. Delete websites bound to port 80. You can change the port to another unused port, such as 8080.

11. Click Add Website.

12. Input necessary information and click OK.
   - Website name: name of the website, such as `wordpress`.
   - Physical path: the directory that contains WordPress, such as `C:\wordpress`.

13. Find `php.ini` under the directory that contains PHP. Open it with a text editor and make the following changes:
   - The necessary changes are different for different PHP versions.
     - For PHP 5.x, find `extension=php_mysql.dll` and delete the ; at the beginning.
     - For PHP 7.x, find `extension=php_mysqli.dll` and delete the ; at the beginning.
   - `extension_dir= "ext"` and delete the ; at the beginning.


Step 4: Verifying the WordPress Configuration
1. Open a browser window on your local machine and visit \( \text{http://localhost/wp-admin/install.php} \). The WordPress installation page appears.

2. Input information as prompted by the installation wizard. Click **Install WordPress** to complete the process.

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website Name</td>
<td>Name of the WordPress site.</td>
</tr>
<tr>
<td>Username</td>
<td>Account name of the WordPress administrator. For security reasons, use a name other than <code>admin</code>.</td>
</tr>
<tr>
<td>Password</td>
<td>Use a strong password, different than your current password. Store it in a secure location.</td>
</tr>
<tr>
<td>Email</td>
<td>Email address used to receive notifications</td>
</tr>
</tbody>
</table>

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

**Using a Domain Name**

Use a domain name that makes your website easier to remember. We recommend you obtain a domain name and set it to point to your WordPress site. If you are installing WordPress just to learn the process, you can skip this step.

**FAQ**

If you encounter a problem when using CVM, refer to the following troubleshooting documents based on your actual situation.

- For issues regarding CVM login, see Password Login and SSH Key Login and Login and Remote Access.
- For issues regarding the CVM network, see IP Addresses and Ports and Security Groups.
- For issues regarding 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:
iperf3 -c 10.0.0.1 -b 2G -t 300 -P 8

**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:**

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

Execute the sar command to view the network pps value.

**Companion training server:**

Command:

```
./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:

```
./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**

```
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

```
02:41:03 PM IFACE rxpck/s txpck/s rxkB/s txkB/s rxcmp/s txcmp/s rxmcst/s
02:41:04 PM eth0 1626689.00 8.00 68308.62 1.65 0.00 0.00 0.00 0.00 0.00
02:41:04 PM lo 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00

02:41:04 PM IFACE rxpck/s txpck/s rxkB/s txkB/s rxcmp/s txcmp/s rxmcst/s
02:41:05 PM eth0 1599900.00 1.00 67183.30 0.10 0.00 0.00 0.00 0.00 0.00
02:41:05 PM lo 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00

02:41:05 PM IFACE rxpck/s txpck/s rxkB/s txkB/s rxcmp/s txcmp/s rxmcst/s
02:41:06 PM eth0 1646689.00 1.00 69148.10 0.40 0.00 0.00 0.00 0.00 0.00
02:41:06 PM lo 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00

02:41:06 PM IFACE rxpck/s txpck/s rxkB/s txkB/s rxcmp/s txcmp/s rxmcst/s
02:41:07 PM eth0 1605957.00 1.00 67437.67 0.40 0.00 0.00 0.00 0.00 0.00
02:41:07 PM lo 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
```

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</td>
</tr>
<tr>
<td>5</td>
<td>0.00-300.03 sec</td>
<td>6.88 GBytes</td>
<td>197 Mbits/sec</td>
</tr>
<tr>
<td>7</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec</td>
</tr>
<tr>
<td>7</td>
<td>0.00-300.03 sec</td>
<td>6.45 GBytes</td>
<td>185 Mbits/sec</td>
</tr>
<tr>
<td>9</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec</td>
</tr>
<tr>
<td>9</td>
<td>0.00-300.03 sec</td>
<td>6.40 GBytes</td>
<td>183 Mbits/sec</td>
</tr>
<tr>
<td>11</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec</td>
</tr>
<tr>
<td>11</td>
<td>0.00-300.03 sec</td>
<td>6.19 GBytes</td>
<td>177 Mbits/sec</td>
</tr>
<tr>
<td>13</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec</td>
</tr>
<tr>
<td>13</td>
<td>0.00-300.03 sec</td>
<td>6.82 GBytes</td>
<td>195 Mbits/sec</td>
</tr>
<tr>
<td>15</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec</td>
</tr>
<tr>
<td>15</td>
<td>0.00-300.03 sec</td>
<td>6.70 GBytes</td>
<td>192 Mbits/sec</td>
</tr>
<tr>
<td>17</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec</td>
</tr>
<tr>
<td>17</td>
<td>0.00-300.03 sec</td>
<td>7.04 GBytes</td>
<td>202 Mbits/sec</td>
</tr>
<tr>
<td>19</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec</td>
</tr>
<tr>
<td>19</td>
<td>0.00-300.03 sec</td>
<td>7.02 GBytes</td>
<td>201 Mbits/sec</td>
</tr>
<tr>
<td>SUM</td>
<td>0.00-300.03 sec</td>
<td>0.00 Bytes</td>
<td>0.00 bits/sec</td>
</tr>
<tr>
<td>SUM</td>
<td>0.00-300.03 sec</td>
<td>53.5 GBytes</td>
<td>1.53 Gbits/sec</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
```
Setting up LNMP
Manually Building an LNMP Environment (CentOS 7)

Last updated: 2020-04-22 18:26:59

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.

You can use the `Ctrl+F` Turn the page down, `Ctrl+B` Turn the page up to view the file. If `nginx.conf` Not found in file `server{...}`. Please go to `include /etc/nginx/conf.d/*conf`; Add the following above.

```
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.

```bash
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.

```
[root@VM_0_3_centos ~]# 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](http://downloads.mariadb.org/mariadb/repositories/) Get MariaDB software library installation information for other versions of the operating system.

```
# 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.

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

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

```
systemctl start mariadb
```

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

```
systemctl enable mariadb
```

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

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

```
[root@VM_0_135_centos ~]# systemctl start mariadb
[root@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 .
Setting up LNMP manually (CentOS 6)

Last updated: 2020-03-06 11:54:14

Introduction

The LNMP environment is a website server architecture run on Linux and consisting of Nginx, MySQL or MariaDB, and PHP. This article describes how to set up LNMP on a CVM.

To set up the LNMP environment, you should be familiar with common Linux commands, such as Installing Software via YUM in CentOS for some examples), and understand the versions of the installed software.

Software

The following software are involved:

CentOS is a distribution of the Linux operating system. We use CentOS 6.9 in this article.
Nginx is a web server. We use Nginx 1.17.5 in this article.
MySQL is a database software. We use MySQL 5.1.73.
PHP is a scripting language. We use PHP 7.1.32 in this article.

Prerequisites

You need a Linux CVM. If you have not purchased one yet, see Getting Started with Linux CVMs.

Directions

Step 1: Logging in to a Linux instance

Log in to a Linux instance using WebShell (recommended). You can also use other login methods that you are comfortable with:

- Log in to a Linux instance using remote login software.
- Log in to a Linux instance using 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 enter edit mode and input the following.

```
[nginx]
name = nginx repo
baseurl=https://nginx.org/packages/mainline/centos/6/$basearch/
gpgcheck=0
enabled=1
```

3. Press `Esc` and input `:wq` to save the file and go back.

4. Run the following command to install Nginx.

```
yum install -y nginx
```

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

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

6. Press `i` to switch to edit mode.

7. Find `server{...}` and replace the content inside the curly brackets with the following:
   This cancels the monitoring of IPv6 addresses and configures Nginx to interact with PHP.

```bash
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;
    }
```

If you cannot find `server{...}` in `nginx.conf`, add the following above `include /etc/nginx/conf.d/*conf;`
#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;
}

8. Press **Esc** and input **:wq** to save the file and go back.

9. Run the following command to start Nginx.

```
  service nginx start
```

0. Run the following command to set Nginx to start automatically when the system starts.

```
  chkconfig --add nginx
  chkconfig nginx on
```

1. 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](http://nginx.org). Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

---

**Step 3: Installing MySQL**

1. Run the following command to check if MySQL is already installed.
If the following appears, MySQL is already installed.

```
[root@VM_0_41_centos ~]# rpm -qa | grep -i mysql
mysql-libsys-5.1.73-8.el6_8.x86_64
```

To avoid conflict between different versions, run the following command to remove the existing MySQL.

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

If nothing is returned, MySQL is not installed. In this case, proceed to the next step.

2. Run the following command to install MySQL.

```
yum install -y mysql-devel.x86_64 mysql-server.x86_64 mysql-libs.x86_64
```

3. Run the following command to start MySQL.

```
service mysqld start
```

4. Run the following command to set MySQL to start automatically when the system boots up.

```
chkconfig --add mysqld
chkconfig mysqld on
```

5. Run the following command to verify MySQL installation.

```
mysql
```

If the following appears, MySQL has been successfully installed.

```
[root@VM_0_135_centos nginx]# mysql
Welcome to the MySQL monitor. Commands end with ; or \\g.
Your MySQL connection id is 3
Server version: 5.5.59 MySQL Community Server (GPL)
Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql>
```
6. Run the following command to exit MySQL.

```
\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/el6/latest.rpm
```

2. Run the following command to install the packages required for PHP 7.1.32.

```
yum -y install mod_php71w.x86_64 php71w-cli.x86_64 php71w-common.x86_64 php71w-mysqlnd php71w-fpm.x86_64
```

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

```
service php-fpm start
```

4. Run the following command to set the PHP-FPM service to start automatically.

```
chkconfig --add php-fpm
chkconfig php-fpm on
```

### Verifying the Environment Configuration

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

```
```

2. Run the following command to restart Nginx.

```
service nginx restart
```

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 7.1.32](image)

**Related Operations**

After the LNMP environment is built, you can start a WordPress website.

**FAQ**

If you encounter a problem when using CVM, refer to the following documents for troubleshooting based on your actual situation.

- For issues regarding CVM login, see [Password Login and SSH Key Login](#) and [Login and Remote Access](#).
- For issues regarding the CVM network, see [IP Addresses](#) and [Ports and Security Groups](#).
- For issues regarding CVM disks, see [System and Data Disks](#).
Setting up LNMP Manually (openSUSE)

Last updated: 2020-04-07 09:47:24

Introduction

LNMP refers to a common web server architecture consisting of Nginx, MySQL or MariaDB, and PHP running on Linux. This article describes how to deploy LNMP on a Tencent Cloud Virtual Machine (CVM).

You need to install several software packages on Linux. If you do not know how to perform software installation on Linux, refer to this article.

Software

This article uses the following software to build the LNMP environment:

- OS: openSUSE 42.3
- Web server: Nginx 1.14.2
- Database: MySQL 5.6.43
- Hypertext processor: PHP 7.0.7

Prerequisites

You have purchased a Linux CVM. If you have not yet, see Getting started with Linux CVMs.

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:
- Log in to a Linux instance by using remote login software.
- Log in to a Linux instance through SSH.

Step 2: Adding image source

1. Log in to your CVM.
2. Run the following commands to add image source:

```bash
zypper ar https://mirrors.cloud.tencent.com/opensuse/distribution/leap/42.3/repo/oss suseOss
zypper ar https://mirrors.cloud.tencent.com/opensuse/distribution/leap/42.3/repo/non-oss suseNonOss
```

3. Run the following command to update the source you just added.

```bash
zypper ref
```

### Step 3: Installing and configuring Nginx

1. Run the following command to install Nginx.

```bash
zypper install -y nginx
```

2. Run the following command to start the Nginx server and set it to auto start when the CVM starts up.

```bash
systemctl start nginx
systemctl enable nginx
```

3. Run the following to edit the Nginx configuration file.

```bash
Vi /etc/nginx/nginx.conf
```

4. Press `i` to toggle edit mode.

4. Find `server {...}` and replace it with the following content:

```bash
server {
    listen 80;
    server_name localhost;
    #access_log /var/log/nginx/log/host.access.log main;
    location / {
        root /srv/www/htdocs/;
        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 /srv/www/htdocs/;
    }
    #pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000
    location ~ .php$ {
        root /srv/www/htdocs/;
        fastcgi_pass 127.0.0.1:9000;
```
5. When you finish, press **Esc** to exit edit mode. Then enter **:wq** to save the file and exit Vi.

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

   ```bash
   systemctl restart nginx
   ```

7. Run the following command to create an index page called `index.html`.

   ```bash
   vi /srv/www/htdocs/index.html
   ```

8. Press **i** to switch to edit mode and **Enter** the following.

   ```html
   <p>hello world!</p>
   ```

9. After you finish, press **Esc** to exit edit mode. Then enter **:wq** to save the file and exit Vi.

10. Access the public IP of your CVM on the browser to check if your Nginx is running properly.

    If the following appears, Nginx has been successfully installed and configured.

    ![Nginx running](image)

### Step 4: Installing and configuring MySQL

1. Run the following command to install MySQL.

   ```bash
   zypper install -y mysql-community-server mysql-community-server-tools
   ```

2. Run the following command to start the MySQL service and set it to auto start when your CVM starts up.

   ```bash
   systemctl start mysql
   systemctl enable mysql
   ```

3. Run the following command to log in to MySQL.

   ```bash
   mysql -u root -p
   ```
When you login for the first time, MySQL will ask you to setup a password. If you do not wish to do so, press **Enter** to skip the step.

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

If the following appears, you have successfully logged in.

```
Welcome to the MySQL monitor. Commands end with ; or \\.
Your MySQL connection id is 4
Server version: 5.6.43 openSUSE package

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

4. Run the following command to change the root password.

```sql
update mysql.user set password = PASSWORD('NEW_PASSWORD') where user='root';
```

5. Run the following command to apply the configuration:

```sql
flush privileges;
```

6. Run the following command to exit MySQL.

```
\q
```

**Step 5: Installing PHP**

Run the following command to install PHP:

```bash
zypper install -y php7 php7-fpm php7-mysql
```

**Step 6: Configuring Nginx with PHP-FPM**

1. Run the following commands to navigate to `/etc/php7/fpm` and rename `php-fpm.conf.default` to `php-fpm.conf`.
cd /etc/php7/fpm
\cp php-fpm.conf.default php-fpm.conf

2. Run the following commands to navigate to /etc/php7/fpm/php-fpm.d and rename www.conf.default to www.conf.

cd /etc/php7/fpm/php-fpm.d
\cp www.conf.default www.conf

3. Run the following commands to start PHP-FPM and set it to auto start when your CVM starts up.

systemctl start php-fpm
systemctl enable php-fpm

Verifying Your Setup

1. Run the following command to create a file named index.php.

Vi /srv/www/htdocs/index.php

2. Press i to switch to edit mode and enter the following:

```php
<?php
  echo "hello new world!";
?>
```

3. Press Esc to exit edit mode. Then enter :wq to save the file and exit.

4. Access the public IP of your CVM on the browser.

   If the following appears, then your LNMP setup has been installed and configured successfully.

```
hello new world!
```

See Also

After the LNMP environment is built, you can use it to set up a WordPress website to familiarize yourself with your CVM and what it can do.
FAQ

If you encounter issues when using CVM, refer to the following documents for troubleshooting:
For issues regarding CVM login, see Password Login and SSH Key Login and Login and Remote Access.
For issues regarding the CVM’s network, see IP Addresses and Ports and Security Groups.
For issues regarding CVM disks, see System and Data Disks.
Setting up Node.js
Setting up Node.js manually

Last updated: 2020-03-06 11:59:24

Introduction

This article describes how to deploy Node.js on a CVM and create a sample project.

To do this, you need to be familiar with common Linux commands such as Installing Software via YUM in a CentOS Environment and understand the versions of the installed software.

Software

Setting up Node.js involves:

- CentOS: a distribution of the Linux operating system. We use CentOS 7.6 in this article.
- Node.js: a JavaScript runtime environment. We use Node.js 10.16.3 and Node.js 6.9.5 in this article.
- npm: a package manager for JavaScript. We use npm 6.9.0 in this article to manage multiple Node.js versions.

Prerequisites

To set up Node.js, you need a Linux CVM. If you have not purchased one yet, see Getting Started with Linux CVMs.

Directions

Step 1: Logging in to a Linux instance

Log in to a Linux instance using WebShell (recommended). You can also use other login methods that you are comfortable with:

- Log in to a Linux instance using remote login software.
- Log in to a Linux Instance using SSH
Step 2: Installing Node.js

1. Run the following command to download the Node.js 64-bit install package for Linux.

   ```
   wget https://nodejs.org/dist/v10.16.3/node-v10.16.3-linux-x64.tar.xz
   ```

   Visit the Node.js official website for more information.

2. Run the following command to decompress the install package.

   ```
   tar xvf node-v10.16.3-linux-x64.tar.xz
   ```

3. Run the following commands to create symbolic links.

   ```
   ln -s /root/node-v10.16.3-linux-x64/bin/node /usr/local/bin/node
   ln -s /root/node-v10.16.3-linux-x64/bin/npm /usr/local/bin/npm
   ```

   Once created, you are able to use node and npm commands in any CVM directory.

4. Run the following commands to view Node.js and npm versions.

   ```
   node -v
   npm -v
   ```

Step 3: Installing multiple Node.js versions (optional)

This process allows you to install multiple Node.js versions. Developers can use this to quickly switch among versions.

1. Run the following command to install git.

   ```
   yum install -y git
   ```

2. Run the following command to download the NVM source code and check for the newest version.

   ```
   git clone https://github.com/cnpm/nvm.git ~/.nvm && cd ~/.nvm && git checkout `git describe --abbrev=0 --tags`
   ```

3. Run the following to configure NVM environment variables.
4. Run the following command to read system environment variables.

   ```bash
   source /etc/profile
   ```

5. Run the following commands to view all Node.js versions.

   ```bash
   nvm list-remote
   ```

6. Run the following commands to install multiple Node.js versions.

   ```bash
   nvm install v6.9.5
   nvm install v10.16.3
   ```

7. Run the following command to view all installed Node.js versions.

   ```bash
   nvm ls
   ```

   If the following appears, then the installation is successful and the current version in use is Node.js 10.16.3.

   ```bash
   [root@VM_0_3_centos .nvm]$ nvm ls
   v6.9.5
   ---> v10.16.3
   system
   stable --> 10.16 (--> v10.16.3) (default)
   unstable --> 6.9 (--> v6.9.5) (default)
   ```

8. Run the following command switch to another version.

   ```bash
   nvm use v6.9.5
   ```

   The following appears:

   ```bash
   [root@VM_0_3_centos .nvm]$ nvm use v6.9.5
   Now using node v6.9.5
   ```

### Step 4: Creating a sample project

1. Run the following commands to create a file named `index.js` under the root path.

   ```bash
   cd ~
   ```
2. Press `i` to enter edit mode and input the following in the `index.js` file:

```javascript
const http = require('http');
const hostname = '0.0.0.0';
const port = 7500;
const server = http.createServer((req, res) => {
    if (res.statusCode === 200) {
        res.setHeader('Content-Type', 'text/plain');
        res.end('Hello World
');
    };
server.listen(port, hostname, () => {
    console.log('Server running at http://' + hostname + ':' + port + '/');
});
```

This article uses port 7500 in the `index.js` file. You can use other ports as needed.

3. Press `Esc` and input `:wq` to save the file and go back.

4. Run the following command to execute the Node.js project we just created.

```bash
node index.js
```

5. Open a browser window on your local machine and visit the following URL to check if the project has been executed successfully.

```
http://CVM_Public_IP:Port
```

If the following appears, Node.js is installed successfully.

```
Hello World
```

FAQ
If you encounter a problem when using CVM, refer to the following documents for troubleshooting based on your actual situation.

- For issues regarding CVM login, see Password Login and SSH Key Login and Login and Remote Access.
- For issues regarding the CVM network, see IP Addresses and Ports and Security Groups.
- For issues regarding CVM disks, see System and Data Disks.
Setting up Java Web

Introduction

This article describes how to set up a Java Web environment on a Linux CVM.

This requires you to be familiar with common Linux commands, such as Installing Software via YUM in a CentOS Environment, and understand the versions of the installed software.

Software

These are the software involved:

- CentOS is a distribution of the Linux operating system. We use CentOS 7.6 in this article.
- Apache Tomcat provides a "pure Java" HTTP web server environment in which Java code can run. We use Apache Tomcat 8.5.47.
- JDK, or Java Development Kit, is an implementation of the Java Platform. We use JDK 1.8.0_221 in this article.

Prerequisites

Setting up a Java Web environment requires a Linux CVM. If you have not purchased one yet, see Getting Started with Linux CVMs.

Directions

Step 1: Logging in to a Linux instance

- Log in to a Linux instance using WebShell (recommended). You can also use other login methods that you are comfortable with:
- Log in to a Linux instance using remote login software.
- Log in to a Linux Instance using SSH
Step 2: Installing JDK

1. Download the JDK installation file. Go to the Java SE download page to select a version and download it.

   Download the JDK file, save it locally, and upload it to your CVM. Otherwise, decompressing the file will result in errors.
   - If you are using MacOS or Linux, use SCP to upload the file.

2. Run the following command to create a directory for JDK installation.

   ```bash
   mkdir /usr/java
   ```

3. Run the following command to decompress JDK to the directory.

   ```bash
   tar xzf jdk-8u221-linux-x64.tar.gz -C /usr/java
   ```

4. Run the following command to open `profile`.

   ```bash
   vim /etc/profile
   ```

5. Press `i` to enter edit mode. Start a new line after `export PATH USER ...` and add the following:

   ```bash
   export JAVA_HOME=/usr/java/jdk1.8.0_221 (replace 1.8.0 221 with your JDK version number)
   export CLASSPATH=$JAVA_HOME/lib/tools.jar:$JAVA_HOME/lib/dt.jar:$JAVA_HOME/lib
   export PATH=$JAVA_HOME/bin:$PATH
   ```

   The result should be as follows:

   ```bash
   export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL
   export JAVA_HOME=/usr/java/jdk1.8.0_221
   export CLASSPATH=$JAVA_HOME/lib/tools.jar:$JAVA_HOME/lib/dt.jar:$JAVA_HOME/lib
   export PATH=$JAVA_HOME/bin:$PATH
   ```

6. Press `Esc` and input `:wq` to save the file and go back.

7. Run the following command to read system environment variables.

   ```bash
   source /etc/profile
   ```

8. Run the following command to check if JDK is installed properly.

   ```bash
   java -version
   ```
If the following appears, the installation was successful.

```
[root@VM_0_71_centos ~]# java -version
java version "1.8.0_221"
Java(TM) SE Runtime Environment (build 1.8.0_221-b11)
Java HotSpot(TM) 64-Bit Server VM (build 25.221-b11, mixed mode)
```

## Step 3: Installing Tomcat

1. Run the following command to download Tomcat source codes. Select a version that suits you.

   Refer to the [Apache Tomcat official website](http://mirrors.tuna.tsinghua.edu.cn/apache/tomcat/) for more information.

   ```
wget http://mirrors.tuna.tsinghua.edu.cn/apache/tomcat/tomcat-8/v8.5.47/bin/apache-tomcat-8.5.47.tar.gz
   ```

2. Run the following command to decompress the file.

   ```
tar xzf apache-tomcat-8.5.47.tar.gz
   ```

3. Run the following command to move the directory that contains Tomcat to `/usr/local/tomcat/`.

   ```
   mv apache-tomcat-8.5.47 /usr/local/tomcat/
   ```

4. Run the following command to open `server.xml`.

   ```
vim /usr/local/tomcat/conf/server.xml
   ```

5. Find `<Host … appBase="webapps"` and press i to enter edit mode. Replace `appBase="webapps"` with the following:

   ```
   appBase="/usr/local/tomcat/webapps"
   ```

6. Press Esc and input :wq to save the file and go back.

7. Run the following command to create a file named `setenv.sh`.

   ```
   vi /usr/local/tomcat/bin/setenv.sh
   ```

8. Press Enter to enter edit mode and input the following to set JVM memory variables.

   ```
   JAVA_OPTS='-Djava.security.egd=file:/dev/urandom -server -Xms256m -Xmx496m -Dfile.encoding=UTF-8'
   ```
9. Press **Esc** and input **:wq** to save the file and go back.

0. Run the following command to start Tomcat.

```
/usr/local/tomcat/bin/startup.sh
```

If the following appears, Tomcat has been successfully started.

```
[root@VM_0_15_centos ~]# /usr/local/tomcat/bin/startup.sh
Using CATALINA_BASE: /usr/local/tomcat
Using CATALINA_HOME: /usr/local/tomcat
Using CATALINA_TMPDIR: /usr/local/tomcat/temp
Using JAVA_HOME: /usr/java/jdk1.8.0_221
Using CLASSPATH: /usr/local/tomcat/bin/bootstrap.jar:/usr/local/tomcat/bin/tomcat-juli.jar
Tomcat started.
```

### Verifying the Environment Configuration

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

```
echo Hello World! > /usr/local/tomcat/webapps/ROOT/index.jsp
```

2. Open a browser window on your local machine and visit the following URL to check whether the environment configuration was successful.

```
http://[Public IP address of the CVM instance]:8080
```

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

```
Hello World!
```

### FAQ

If you encounter a problem when using CVM, refer to the following documents for troubleshooting based on your actual situation.

- For issues about CVM login, see Password Login and SSH Key Login and Login and Remote Access.
- For issues about the CVM network, see IP Addresses and Ports and Security Groups.
- For issues about CVM disks, see System and Data Disks.
Scenario

LAMP is a common web service architecture run on Linux and consisting of Apache, MySQL/MariaDB, and PHP. This article describes how to set up LAMP on a Linux CVM.

You should be familiar with common Linux commands, such as Installing Software via YUM in a CentOS Environment, and understand the versions of the installed software.

Software

These are the software involved:

- CentOS is a distribution of the Linux operating system. We will use version 7.6 in this article.
- Apache is a web server software. We will use version 2.4.6 in this article.
- MariaDB is a database management system. We will use version 10.4.8 in this article.
- PHP is a scripting language. We will use version 7.0.33 in this article.

Prerequisites

You need a Linux CVM. If you have not purchased one yet, see Getting Started with Linux CVMs.

Instructions

**Step 1: Logging in to a Linux instance**

Log in to a Linux instance using WebShell (recommended). You can also use other login methods that you are comfortable with:

- Log in to a Linux instance using remote login software.
- Log in to a Linux instance using SSH

**Step 2: Installing Apache**
1. Run the following command to install Apache.

```bash
yum install httpd -y
```

2. Run the following commands to start Apache and set it to start automatically when the system starts.

```bash
systemctl start httpd
systemctl enable httpd
```

3. Open a browser window and visit the following URL to verify that Apache is working properly.

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

The following appears if Apache is installed properly:

![Testing 123..](image)

**Step 3: Installing MariaDB**

1. Run the following command to check if MariaDB is already installed.

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

- If the following appears, MariaDB is already installed.

```
[root@VM_0_3_centos ~]# 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
```

If that’s the case, run the following to remove MariaDB to avoid conflicts between different versions.
yum -y remove [Package name]

- If nothing is returned, MariaDB is not installed. In this case, proceed to the next step.

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

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

3. Press i to switch to edit mode and input the following.

```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=1
```

For installation information for other versions, visit the MariaDB official website.

4. Press Esc and input :wq to save the file and go back.

5. Run the following command to install MariaDB.

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

6. Run the following commands to start MariaDB and set it to start automatically when the system starts.

```bash
systemctl start mariadb

systemctl enable mariadb
```

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

```bash
mysql
```
If the following appears, MariaDB is successfully installed.

```
[root@VM_0_135_centos ~]# systemctl start mariadb
[root@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)]>
```

8. 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 7.0.33.

```
yum -y install php70w php70w-opcache php70w-mbstring php70w-gd php70w-xml php70w-pear php70w-fpm php70w-mysql php70w-pdo
```

3. Run the following command to edit the Apache configuration file.

```
vi /etc/httpd/conf/httpd.conf
```

4. Press `i` to enter edit mode and make the following changes:

```
﻿# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.

# If your host doesn't have a registered DNS name, enter its IP address here.
.SERVERNAME www.example.com:80
.ServerName localhost:80
```

©2013-2019 Tencent Cloud. All rights reserved.
i. Find `ServerName www.example.com:80` and start a new line below it. Input the following:

```
ServerName localhost:80
```

ii. Find `Require all denied in <Directory>` and change it to `Require all granted`.

iii. Find `<IfModule dir_module>` and change the content to `DirectoryIndex index.php index.html`.

iv. Start a new line below `AddType application/x-gzip .gz .tgz` and input the following:

```
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
```

5. Press `Esc` and input `:wq` to save the file and go back.

6. Run the following command to restart Apache.

```
systemctl restart httpd
```
Verifying the Environment Configuration

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

   ```bash
   ```

2. Open a browser window on your local machine and visit the following URL to check whether the environment configuration is successful.

   ```bash
   http://CVM Public IP/index.php
   ```

If the following appears, the LAMP environment is configured successfully.

![PHP Version 7.0.33](image)

Relevant Operations

After the LAMP environment is built, you can manually set up Drupal website.

FAQ

If you encounter a problem when using CVM, refer to the following documents for troubleshooting based on your actual situation.
For issues regarding CVM login, see Password Login and SSH Key Login and Login and Remote Access.

For issues regarding the CVM network, see IP Addresses and Ports and Security Groups.

For issues regarding CVM disks, see System and Data Disks.
Build Discuz! Forum
Manually build Discuz! Forum

Use Case

With more than 2 million forums based on Discuz!, it is the most sophisticated and predominant internet discussion software in the world. This article describes how to create a forum using Discuz! and deploy the LAMP (Linux, Apache, MariaDB, and PHP) runtime environment it needs.

To set up Discuz! manually, you should be familiar with common Linux commands, such as Installing Software via YUM in CentOS and know how to use the software you install and their version compatibility.

Software

This article uses the following:

- Operating system: CentOS 7.5, a distribution of Linux
- Web server: Apache 2.4.6
- Database: MariaDB 5.5.60
- Hypertext processor: PHP 5.4.16
- Forum software: Discuz! X3.2

Procedure

Step 1: Logging in to Linux CVM

Log in to a Linux instance using WebShell (recommended). You can also use another login method that you are comfortable with.

- Log in to a Linux instance using remote login software.
- Log in to a Linux instance using SSH

Step 2: Setting up LAMP
Tencent Cloud hosts an image of the CentOS official version installation source, which contains the most recent and stable version of the software. Use Yum to install CentOS.

**Installing and configuring required software**

1. Run the following command to install Apache, MariaDB, and PHP:

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

2. Run the following commands to start the services:

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

3. Run the following commands to set a password for root and configure the database so root can access it.

   - Run the command before you log in to MariaDB for the first time.
   - Enter the password for root and press Enter. Your password is not shown on the screen. Enter the password a second time to confirm and complete the configuration as prompted on the screen.

   ```bash
   mysql_secure_installation
   ```

4. Run the following command to log in to MariaDB. Use the password you set in Step 3 and press Enter.

   ```bash
   mysql -u root -p
   ```
A successful login is shown below:

![MySQL command output]

5. Run the following command to exit MariaDB.

```
exit
```

**Verifying Your Setup**

Follow these steps to make sure the environment is set up properly:

1. Run the following command to create a test file `test.php` in the default root directory "/var/www/html" of Apache:

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

2. Press `i` to switch to edit mode and enter the following:

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

3. Press `Esc` and input `:wq` to save the file and exit Vim.

4. Open a browser window and use the following URL to access `test.php` to check whether the environment is properly configured.

```
http://CVM_public_IP/test.php
```
Step 3: Installing and configuring Discuz!

Downloading Discuz!

Run the following command to download the installation package.

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

Preparing for installation

1. Run the following command to decompress the installation package.

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

2. Run the following command to copy all files under "upload" to "/var/www/html/".

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

3. Run the following command to give users write permission:

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

Installing Discuz!

1. Open a browser window and go to the IP address of your Discuz! forum (your CVM public IP address), or you can bind a domain name to your IP address.
2. Click *I agree* to start the process. Discuz! checks to see if the environment is properly installed and configured.
3. Click *Next Step* when the check finishes.
4. Select clean install, and click *Next Step*. 
5. Enter information as prompted to create a new database for Discuz!.

- Use `root` and the password set in Installing and configuring required software to connect to the database and set up a system email address and administrator username, password, and email address.
- Remember your administrator username and password.

6. Click **Next Step** to start installation.
7. After the installation is completed, click **Your forum has been installed successfully. Click here to access.** to access your forum.

**Using a Domain Name**

Use a domain name that makes your website easier to remember. We recommend you obtain a domain name and set it to point to your Discuz! site. If you are installing Discuz! just to learn the process, you can keep using the IP address. Otherwise, use a domain name.

**FAQ**

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

- For issues regarding CVM login, see Password Login and SSH Key Login and Login and Remote Access.
- For issues regarding the CVM network, see IP Addresses and Ports and Security Groups.
- For issues regarding CVM disks, see System and Data Disks.
Manually Building an WIPM Environment
Step1: Install and Configure IIS

Last updated : 2019-12-03 18:02:03

**NOTE:** Do not install any anti-virus software of PC type on Windows CVM. Such software may block the telnet port of the CVM, making it impossible to log in to the CVM.

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.

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:

![PHP 5.3.24 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:

![Folder structure showing hello.php file](image)

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>M5VC14 (Visual C++ 2015)</td>
</tr>
<tr>
<td>Architecture</td>
<td>x86</td>
</tr>
<tr>
<td>Configure Command</td>
<td>csc11pl /mologo configure.js &quot;--enable-snapshot-build&quot; &quot;--enable-debug-pack&quot; \</td>
</tr>
<tr>
<td></td>
<td>&quot;c:\sql\oracle\186\instantclient_12_1\sql\shared&quot; &quot;--with-ocb-12c=c:\php-sql\oracle\12c\sql\shared&quot; &quot;--enable-object-out-dir=./obj/&quot; &quot;--enable-container-shared&quot; &quot;--with-phpize=--with-pgo&quot;</td>
</tr>
<tr>
<td>Server API</td>
<td>CGI/FCGI</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>API320151012,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:

### PHP 7.0 (7.0.6)

<table>
<thead>
<tr>
<th>Download source code [24.08MB]</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC14 x86 Non Thread Safe (2016-Apr-29 00:38:17)</td>
</tr>
<tr>
<td>Zip [20.93MB]</td>
</tr>
<tr>
<td>sha1: cfo5f48e3f4def7e22f140dab243709b00670077aa</td>
</tr>
<tr>
<td>Debug Pack [14.85MB]</td>
</tr>
<tr>
<td>sha1: d17bfc88bda7a716d0d0e11424b7588ac0db</td>
</tr>
</tbody>
</table>

### PHP 5.6 (5.6.21)

<table>
<thead>
<tr>
<th>Download source code [24.15MB]</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC11 x86 Non Thread Safe (2016-Apr-28 06:19:34)</td>
</tr>
<tr>
<td>Zip [20.29MB]</td>
</tr>
<tr>
<td>sha1: 46f159ee7be2307aca4d8d5f80034f11c7ff5d2</td>
</tr>
<tr>
<td>Debug Pack [9.68MB]</td>
</tr>
<tr>
<td>sha1: 6aba9b880dcd8c5c0ed73559bfbb03649d2c82f9</td>
</tr>
</tbody>
</table>

### PHP 5.5 (5.5.35)

<table>
<thead>
<tr>
<th>Download source code [23.33MB]</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC11 x86 Non Thread Safe (2016-Apr-28 00:53:27)</td>
</tr>
<tr>
<td>Zip [18.77MB]</td>
</tr>
<tr>
<td>sha1: 034735285c257e7611532af811c5a17ef719718d</td>
</tr>
<tr>
<td>Debug Pack [9.33MB]</td>
</tr>
<tr>
<td>sha1: af3d8b981551098ea4b6321398df2d175d296b8</td>
</tr>
</tbody>
</table>
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
```

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:

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:

![File Location](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:
Step3: Install and Build MySQL

Overview

This article describes how to install MySQL 8.0 on a CVM instance with Windows Server 2012 R2 Datacenter Edition 64bit.

SQL Server is perhaps the most popular database software on Windows. However, it is commercial and requires you to obtain your own license. As an alternative, you can purchase CDB instances for Tencent Cloud SQLServer database.

Procedure

Downloading MySQL

1. Log in to your CVM instance.
2. Open a browser window and go to the official MySQL site to download the MySQL installation file.

Installing MySQL

1. Launch the MySQL installer by double-clicking the installation file. The Choose a Setup Type window appears. Select Developer Default and click Next, as shown in the following figure:
2. In the **Check Requirements** window that appears, click **Execute** and resolve unmet requirements as shown in the figure below:
3. Click **Next**.

4. In the **Installation** window, click **Execute** to install the required packages, as shown in the figure below:
5. Click **Next** when the package installation finishes to open the **Product Configuration** window.

**Configuring MySQL**

**Configuring MySQL service**

1. In the **Product Configuration** window, click **Next** to open the **High Availability** window.
2. Select **Standalone MySQL Server / Classic MySQL Replication** and click **Next**, as shown in the following figure:
3. In the **Type and Networking** window, keep the default configuration. Click **Next**, as shown in the following figure:

- TCP/IP network is enabled by default.
- Port 3306 is used by default.
4. In the **Authentication Method** window, keep the default configuration. Click **Next**, as shown in the following figure:
MySQL Installer
MySQL Server 8.0.19

Authentication Method

© Use Strong Password Encryption for Authentication (RECOMMENDED)
MySQL 8 supports a new authentication based on improved stronger SHA256-based password methods. It is recommended that all new MySQL Server installations use this method going forward.

Attention: This new authentication plugin on the server side requires new versions of connectors and clients which add support for this new 8.0 default authentication (caching_sha2_password authentication).

Currently MySQL 8.0 Connectors and community drivers which use libmysqldclient 8.0 support this new method. If clients and applications cannot be updated to support this new authentication method, the MySQL 8.0 Server can be configured to use the legacy MySQL Authentication Method below.

© Use Legacy Authentication Method (Retain MySQL 5.x Compatibility)
Using the old MySQL 5.x legacy authentication method should only be considered in the following cases:
- If applications cannot be updated to use MySQL 8 enabled Connectors and drivers.
- For cases where re-compilation of an existing application is not feasible.
- An updated, language specific connector or driver is not yet available.

Security Guidance: When possible, we highly recommend taking needed steps towards upgrading your applications, libraries, and database servers to the new stronger authentication. This new method will significantly improve your security.
5. Set a root password and click **Next** as shown in the following figure:

![MySQL Installer](image)

6. In the **Windows Service** window, keep the default configuration and click **Next**, as shown in the following figure:
Windows Service

- Configure MySQL Server as a Windows Service

Windows Service Details
Please specify a Windows Service name to be used for this MySQL Server instance. A unique name is required for each instance.

Windows Service Name: MySQL80

- Start the MySQL Server at System Startup

Run Windows Service as ...
The MySQL Server needs to run under a given user account. Based on the security requirements of your system you need to pick one of the options below.

- Standard System Account
  Recommended for most scenarios.

- Custom User
  An existing user account can be selected for advanced scenarios.
7. In the **Apply Configuration** window, click **Execute**.

   ![MySQL Installer window](image)

8. Click **Finish** to complete MySQL configuration.

**Configuring MySQL Router**

1. In the **Product Configuration** window, click **Next**.
2. In the **MySQL Router Configuration** window, keep the default configuration and click **Finish**, as shown in the following figure:
Configuring MySQL samples

1. In the **Product Configuration** window, click **Next**.

2. In the **Connect to Server** window, input the root password. Click **Check**, as shown in the following figure:
3. After the password is successfully authenticated, click **Next**, as shown in the following figure:
4. In the **Apply Configuration** window, click **Execute**.

5. Click **Finish** to complete the MySQL sample configuration.

6. In the **Product Configuration** window, click **Next**.

7. In the **Installation Complete** window, select the MySQL environment component you want to start and click **Finish**, as shown in the following figure:
MySQL Installer

Installation Complete

The installation procedure has been completed.

- Copy Log to Clipboard

- Start MySQL Workbench after Setup
- Start MySQL Shell after Setup

Finish
• If MySQL Workbench starts, MySQL is successfully installed, as shown in the following figure:

![MySQL Workbench](image)

• If MySQL Shell starts, MySQL is successfully installed, as shown in the following figure:

```
C:\Program Files\MySQL\MySQL Shell 8.0\bin\mysqlsh.exe
MySQL Shell 8.0.19
Copyright (c) 2016, 2019, Oracle and/or its affiliates. All rights reserved. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Type '\help' or '\?' for help; '\quit' to exit.
MySQL JS> -
```

**Adding Security Group Rules**
Add an inbound rule to allow traffic on port 3306 to the security group that is bound to the CVM instance on which MySQL is installed.
Build the FTP Service
Build the FTP Service (Linux)

Scenario

Very Secure FTP Daemon (Vsftpd) is the default FTP server for most Linux distributions. This document uses a CentOS 7.6 64-bit CVM as an example to describe how to use vsftpd to set up the FTP service for a Linux CVM.

Software

The following lists the software programs for setting up the FTP service.

- Linux: CentOS 7.6 public image
- Vsftpd: vsftpd 3.0.2

Directions

Step 1: Log in to the CVM

Log in to a Linux instance by using WebShell (recommended). You can also use any of the following login methods that you are comfortable with.

- Logging in to a Linux instance by using remote login software
- Logging in to a Linux instance by using SSH

Step 2: Install vsftpd

1. Run the following command to install vsftpd:

   ```
   yum install -y vsftpd
   ```

2. Run the following command to automatically start vsftpd upon system startup:

   ```
   systemctl enable vsftpd
   ```

3. Run the following command to start the FTP service:
systemctl start vsftpd

4. Run the following command to check that the service has been started:

    netstat -antup | grep ftp

If the following information appears, the FTP service has been started.

By default, vsftpd has enabled the anonymous access mode. You can log in to the FTP server without entering a username or password. However, you do not have permissions to modify or upload files in this login mode.

**Step 3: Configure vsftpd**

1. Run the following command to create a user for the FTP service, which is ftpuser in this case:

    ```
    useradd ftpuser
    ```

2. Run the following command to set a password for ftpuser:

    ```
    passwd ftpuser
    ```

After entering the password, press **Enter** to confirm. By default, the password is not displayed. Here, **tf7295TFY** is used as an example password.

3. Run the following command to create a file directory for the FTP service, which is `/var/ftp/test` in this case:

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

4. Run the following command to modify the directory permission:

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

5. Run the following command to open the `vsftpd.conf` file:

    ```
    vim /etc/vsftpd/vsftpd.conf
    ```

6. Press **i** to switch to the editing mode. Select an FTP mode based on your actual needs and modify the `vsftpd.conf` configuration file.
The FTP server can connect to the client in either active or passive mode for data transmission. Due to the firewall settings of most clients and the fact that the actual IP address cannot be obtained, we recommend that you use the passive mode to set up the FTP service. The following modification uses the passive mode as an example. To use the active mode, see Setting the FTP active mode.

i. Modify the following configuration parameters to set login permissions for anonymous and local users, set the path for storing the exceptional user list, and enable listening on IPv4 sockets.

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

ii. Add the pound sign (`#`) at the beginning of the following line to annotate `listen_ipv6=YES` and disable listening on IPv6 sockets.

```plaintext
#listen_ipv6=YES
```

iii. Add the following configuration parameters to enable the passive mode, set the directory where local users reside after login, and set the port range for transmitting data by the CVM.

```plaintext
local_root=/var/ftp/test
allow_writeable_chroot=YES
pasv_enable=YES
pasv_address=xxx.xx.xxx.xx # Replace xxx.xx.xxx.xx with the public IP address of your Linux CVM
pasv_min_port=40000
pasv_max_port=45000
```

7. Press Esc and enter :wq. Then, save the changes and close the file.

8. Run the following command to create and edit the `chroot_list` file:

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

9. Press i to enter the editing mode and enter the username. Note that each username occupies one line. After finishing the configuration, press Esc and enter :wq. Then, save the change and close the file.

   If you do not need to set exceptional users, skip this step by entering :wq and closing the file.

0. Run the following command to restart the FTP service:

```plaintext
```
systemctl restart vsftpd

Step 4: Configure security groups

After setting up the FTP service, configure **inbound rules** for the Linux CVM based on the actually used FTP mode. For details, see [Adding Security Group Rules](#).

Most clients convert IP addresses in LANs. If you are using the FTP active mode, ensure that the client has obtained the actual IP address. Otherwise, the client may fail to log in to the FTP server.

- For the active mode: open port 21.
- For the passive mode: open port 21 and all ports ranging from `pasmv_min_port` to `pasmv_max_port` set in the [configuration file](#), such as ports 40000 to 45000 in this document.

Step 5: Verify the FTP service

You can verify the FTP server by using tools such as an FTP client, browser, or Windows Explorer. Here, Windows Explorer is used as an example.

1. Open Internet Explorer on the client, choose **Tools > Internet Options**, and click the **Advanced** tab. Make the following modifications based on the selected FTP mode.
   - For the active mode: deselect **Passive FTP**.
   - For the passive mode: select **Passive FTP**.
2. Open Windows Explorer on the client, enter the following address in the address box and press Enter, as shown in the following figure.

   ```
   ftp://<CVM public IP address:21>
   ```

3. On the login page that appears, enter the username and password set in [Configuring vsftpd](#).
   Here, the username is `ftpuser` and the password is `tf7295TFY`.
4. After successful login, you can upload and download files.

Appendix

Setting the FTP active mode

To use the active mode, modify the following configuration parameters and leave others as their defaults:
**Failing to upload files from an FTP client**

**Problem description**

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

```
553 Could not create file
```

**Solution**

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

   ```
df -h
   ```

   - If the disk space is insufficient, you cannot upload files. In this case, we recommend that you delete some unnecessary large files from the disk.
   - If the disk space is sufficient, go to the next step.

2. Run the following command to check whether you have the write permission to the FTP directory:

   ```
   ls -l /home/test
   # Here, /home/test indicates the FTP directory. Replace it with your actual FTP directory.
   ```

   - If `w` is not returned in the result, you do not have the write permission to the directory. In this case, go to the next step.
   - If `w` is returned in the result, submit a ticket for further troubleshooting.

3. Run the following command to grant the write permission to the FTP directory:

   ```
   ```
4. Run the following command to check whether the write permission is successfully granted:

```
chmod +w /home/test
# Here, /home/test indicates the FTP directory. Replace it with your actual FTP directory.
```

```
ls -l /home/test
# Here, /home/test indicates the FTP directory. Replace it with 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".
0. Click "install" to begin the installation of the FTP service.
1. 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.
   - **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.
Setting up a Website

Running a personal website or forum is one of the most common things people do after they purchase a CVM.

This article describes several ways you can setup a website on your CVM. Choose one that suits you the best.

How to setup a website

Setting up a website

<table>
<thead>
<tr>
<th>Purchasing a CVM</th>
<th>Setting up a website</th>
</tr>
</thead>
</table>

Domain Registration → Identity Verification → ICP Filing → Domain Name Resolution → Installing Certificates

Domain Registration
- Time needed: 10 to 15 minutes

Identity Verification
- Pending Approval
- Time needed: 3 to 5 business days

ICP Filing
- Pending Approval
- Time needed: 10 to 15 minutes

Domain Name Resolution
- Time needed: 1 to 15 minutes

Installing Certificates
- Time needed: 1 to 2 hours

Setting Up a Website Manually

We recommend that you setup your website manually.

<table>
<thead>
<tr>
<th>Manual Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup</td>
</tr>
<tr>
<td>Install software manually. Easier to customize.</td>
</tr>
<tr>
<td>Advantages</td>
</tr>
<tr>
<td>Flexible choices among software versions</td>
</tr>
<tr>
<td>Duration</td>
</tr>
<tr>
<td>Longer since you need to do this manually</td>
</tr>
<tr>
<td>Difficulty</td>
</tr>
<tr>
<td>Knows how to install software manually and which version to use.</td>
</tr>
</tbody>
</table>

Instructions

Use the following table to choose a website that suits your needs.
<table>
<thead>
<tr>
<th>Type</th>
<th>Setup</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WordPress</td>
<td>WordPress (Linux)</td>
<td>WordPress is a blogging platform developed with PHP. You can use it as a content management system, or use it to create websites on services that support PHP and MySQL databases.</td>
</tr>
<tr>
<td></td>
<td>WordPress (Windows)</td>
<td></td>
</tr>
<tr>
<td>Discuz</td>
<td>Discuz!</td>
<td>Discuz! is a popular forum software built on PHP and MySQL. You only need to configure a few item to get it up and running.</td>
</tr>
<tr>
<td>LNMP</td>
<td>LNMP (CentOS 7)</td>
<td>LNMP is a common web service architecture which consists of Nginx, MySQL/MariaDB and PHP running on Linux.</td>
</tr>
<tr>
<td>LNMP</td>
<td>LNMP (CentOS 6)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LNMP (openSUSE)</td>
<td></td>
</tr>
<tr>
<td>LAMP</td>
<td>LAMP</td>
<td>LAMP is a common web service architecture which consists of Apache, MySQL/MariaDB and PHP running on Linux.</td>
</tr>
<tr>
<td>WIPM</td>
<td>WIPM</td>
<td>WIPM stands for a web service architecture which consists of IIS, PHP and MySQL running on Windows.</td>
</tr>
<tr>
<td>Drupal</td>
<td>Drupal</td>
<td>Drupal is a Content Management Framework (CMF) written in PHP. It consists of a Content Management System (CMS) and a PHP development framework. You can use it to run a personal blog or corporate website.</td>
</tr>
<tr>
<td>Ghost</td>
<td>Ghost</td>
<td>Ghost is a free and open source blogging platform written in JavaScript and distributed under the MIT License, designed to simplify the process of online publishing for individual bloggers as well as online publications.</td>
</tr>
</tbody>
</table>
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**

ntpupdate.tencentyun.com

**Public Network NTP Server**

- 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

Last updated: 2020-04-24 14:27:22

Scenario

The Windows Time service (W32Time) synchronizes the time between the local system and the clock source server. It uses NTP to synchronize computer clocks on the network. The following uses a CVM that runs Windows Server 2012 as an example to describe how to enable the NTP service and modify the IP address of the clock source server.

Directions

1. Log in to the Windows CVM.
2. On the desktop, choose 📲 > Task Manager > Services to open the Services window.
3. In the Services window that appears, double-click Windows Time, as shown in the following figure.
4. In the **Windows Time Properties (Local Computer)** window that appears, set **Startup type** to **Automatic** and **Service status** to **Running**, and then click **OK**, as shown in the following figure.
5. In the task bar of the desktop, click the time icon in the lower-right corner and click **Change date and time settings**..., as shown in the following figure.
6. In the **Date and Time** window that appears, click the **Internet Time** tab, and then click **Change settings**, as shown in the following figure.
7. In the **Internet Time Settings** window that appears, enter the domain name or IP address of the target clock source server in the **Server** text box and click **OK**, as shown in the following figure.
Configure Internet time settings:

- Synchronize with an Internet time server

Server: ntpupdate.tencentyun.com

The clock was successfully synchronized with ntpupdate.tencentyun.com on 7/24/2019 at 4:30 PM.
Set the NTP service on a Linux instance

Last updated : 2020-03-06 16:21:14

Introduction

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 uses CentOS7.5 as an example to describe how to install and use ntpd.

Notes

- Some operating systems use chrony as the default NTP service. Please make sure that ntpd is running and is configured to start automatically on boot.
  - Use `systemctl is-active ntpd.service` command to see if ntpd is running.
  - Use `systemctl is-enabled ntpd.service` command to see if ntpd is configured to start automatically on boot.
- The communication port of the NTP service is UDP 123. Please make sure that you have opened the port to the Internet before configuring the NTP service.
  - If the port is not open, please refer to Adding Security Group Policies to open it to the Internet.

Directions

Installing ntpd

Execute the following command to check if ntpd has been installed.

```
rpm -qa | grep ntp
```

- If the returned result is similar to the following, it means that ntpd has been installed.

```
[root@VM_16_2_centos ~]# rpm -qa | grep ntp
ntpd-4.2.6p5-28.el7.centos.x86_64
ntp-4.2.6p5-28.el7.centos.x86_64
fontpackages-filesystem-1.44-8.el7.noarch
```
If ntpd has not been installed, please run `yum install ntp` to install it.

```
yum -y install ntp
```

ntpd uses the client mode by default.

**Configuring NTP**

1. Execute the following command to open the configuration file of the NTP service.

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

2. Click `i` to enter the edit mode, 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. See the figure below:

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

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

**Launching ntpd**

Execute the following command to restart the ntpd service.

```
systemctl restart ntpd.service
```

**Checking the status of ntpd**

Execute the following commands to check the status of ntpd according to your needs.

- Execute the following command to check whether the NTP service port, the UDP 123 port, is being listened normally.

```
netstat -nupl
```
If a result similar to the following is returned, it indicates that the listening is normal.

```
[root@VM_0_136_centos ~]# netstat -nlpu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address                  Foreign Address            State      PID/Program name
udp    0      0  172.30.0.136:1123                0.0.0.0:*          0.0.0.0:*          999/ntpd
udp    0      0  127.0.0.1:1123                   0.0.0.0:*          0.0.0.0:*          999/ntpd
udp    0      0  fe80::5054:ff:fe02::123          :::*               :::*               999/ntpd
udp    0      0  ::1:1123                         :::*               :::*               999/ntpd
```

- Execute the following command to check whether the ntpd status is normal.

```
service ntpd status
```

If a result similar to the following is returned, it indicates that the ntpd status is normal.

```
[root@VM_0_136_centos ~]# service ntpd status
Redirecting to /bin/systemct1 status ntpd.service
* ntpd.service - Network Time Service
 Loaded: loaded (/usr/lib/systemd/system/ntpd.service; enabled; vendor preset: disabled)
 Active: active (running) since Wed 2019-08-07 15:23:25 CST; 3min ago
 Process: 997 ExeChStart=/usr/sbin/ntpd -u ntpd:ntp $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 999 (ntpd)
 CGroup: /system.slice/ntpd.service
 [ 999 ] /usr/sbin/ntpd -u ntpd:ntp -g
 Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0.0 c01d 0d kern kernel time sync enabled
 Aug 07 15:23:25 VM_0_136_centos ntpd[999]: ntp io: estimated max descriptors: 1024, initia... 16
 Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 0 ld 172.30.0.11 UDP 123
 Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 1 eth0 172.30.0.136 UDP 123
 Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 2 lo ::1 UDP 123
 Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 3 eth0 fe80::5054:ff:fe02:11...123
 Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listening on routing socket on fd 80 for inter...tes
 Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listening on routing socket on fd 80 for inter...tes
 Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c016 06 restart
 Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c012 02 freq_set kernel 0.467 FPM
 Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c015 05 clock sync
 Hint: Some lines were ellipsized, use -l to show in full.
[root@VM_0_136_centos ~]# ntpstat
```

- Execute the following command to check whether NTP has been started normally and configured to the correct NTP clock source server.

```
ntpstat
```

The IP address of the current NTP clock source server is returned. This IP address should be the IP address of the NTP clock source server configured above. See the figure below:
You can also get the IP address corresponding to the domain name by executing the `nslookup` command.

- Execute the following command to get more detailed NTP service information.

  ```
  ntpq -p
  ```

A result similar to the following will be returned:

```
remote refid st when poll reach delay offset jitter
108.56.2.19  .INIT.  16 u  -   64  0   0.000  0.000  0.000
128.107.213.255 193.230.131.10  16 u  67  64  14  277.831  3.940  5.588
```

- **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. 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 have 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 be 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. The smaller its absolute value, the more accurate the host time.
Setting the automatic launch of ntpd on startup

1. Execute the following command to set the automatic launch of ntpd at startup.

```
systemctl enable ntpd.service
```

2. Execute the following command to see if chrony is set to launch at startup.

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

If chrony is set to launch at startup, execute the following command to remove chrony from the list of software that runs at startup.

chrony is not compatible with ntpd, which may lead to ntpd start failure.

```
systemctl disable chronyd.service
```
Setting up a Ghost Blog

Last updated: 2020-03-06 11:10:11

Scenario

Ghost is a free and open source blogging platform written in JavaScript and distributed under the MIT License, designed to simplify the process of online publishing for individual bloggers as well as online publications. This article describes how to set up Ghost on a CVM.

To set up Ghost, you should be familiar with Linux and its common commands, such as Install Software via Apt-get under Ubuntu Environment.

Software

This article uses the following software:

- Linux operating system. This article uses Ubuntu 18.04.
- Nginx 1.14.0 is used to provide web service.
- MySQL 5.7.27 is used for database.
- Node.js 10.17.0 is our runtime environment.
- Ghost 3.0.2

Prerequisites

You should have a Linux CVM. If you have not purchased one yet, see Getting Started with Linux CVMs.

- A domain name that points to your CVM and already completed ICP filing.

Directions

Step 1 Logging in to a Linux instance

- Log in to a Linux instance using WebShell (recommended). You can also use other login methods that you are comfortable with:
- Log in to a Linux instance using remote login software.
Logging In to a Linux Instance using SSH

Step 2 Create a new user

1. After logging in, switch to root. Refer to this article for details.
2. Run the following command to create a user named user.

   Do not use ghost as the username. It causes conflicts with Ghost-CLI.

```
adduser user
```

   i. Input and confirm password as prompted. Password is not shown by default. Press Enter to continue.
   
   ii. Input user information. Or press Enter to skip them and continue.
   
   iii. Input Y to confirm and press Enter to complete the process, as shown below:

```
root@VM-0-22-ubuntu:/home/ubuntu# adduser user
Adding user `user' ...
Adding new group `user' (1000) ...
Adding new user `user' (1000) with group `user' ...
Creating home directory `/home/user' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
pwd: password updated successfully
Changing the user information for user
Enter the new value, or press ENTER for the default
   Full Name []:
   Room Number []:
   Work Phone []:
   Home Phone []:
   Other []:
Is the information correct? [Y/n] Y
root@VM-0-22-ubuntu:/home/ubuntu# 
```

3. Run the following command to add user privileges.

```
usermod -aG sudo user
```

4. Run the following command to switch to user.

```
su user
```

Step 3 Update installed packages
Run the following commands to update installed packages.

```
Input the password for <user> as prompted and press <Enter> to start.
```

```
sudo apt-get update
```

```
sudo apt-get upgrade -y
```

### Step 4 Environment setup

#### Install Nginx

Run the following command to install Nginx.

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

#### Install and configure MySQL

1. Run the following command to install MySQL.

   ```
sudo apt-get install -y mysql-server
```

2. Run the following command to connect to MySQL.

   ```
sudo mysql
```

3. Run the following command to create a database for Ghost named ghost_data.

   ```
CREATE DATABASE ghost_data;
```

4. Run the following command to set a password for the database user root.

   ```
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'your_password';
```

5. Run the following command to quit MySQL.

   ```
\q
```

#### Install Node.js

1. Run the following command to set a default Node.js version to be used.

   ```
curl -sL https://deb.nodesource.com/setup_10.x | sudo -E bash
```
2. Run the following command to install Node.js.

```
sudo apt-get install -y nodejs
```

**Install Ghost-CLI**

Run the following command to install Ghost-CLI which helps configuring Ghost.

```
sudo npm install ghost-cli@latest -g
```

**Step 5 Install and configure Ghost**

1. Run the following commands.

```
sudo mkdir -p /var/www/ghost

sudo chown user:user /var/www/ghost

sudo chmod 775 /var/www/ghost

cd /var/www/ghost
```

2. Run the following command to install Ghost.

```
ghost install
```
3. Use the following image to complete the installation process.

```plaintext
i. Enter your blog URL: input your domain name in the format of http://your_domain_name.
ii. Enter your MySQL hostname: input your database address. Use localhost in this case and press Enter.
iii. Enter your MySQL username: input the username you use to connect to MySQL. Use root in this case and press Enter.
iv. Enter your MySQL password: input the corresponding password you set earlier and press Enter.
```

Ghost was installed successfully! To complete setup of your publication, visit:

```
http://www.your_domain_name/ghost/
```
v. **Enter your database name:** input the name of the database you created for Ghost in the previous step. Use `ghost_data` and press **Enter**.

vi. Input **Y** or **n** to complete the configuration.

The admin URL appears on the bottom of the screen.

4. Open a browser window on your local machine and visit the admin URL to start configuring your blog.

Click **Create your account** to create an admin account.
5. Input desired information and click **Last step**, as shown below:

6. You can invite others to create blogs, or skip this step.
7. Go to the administration page to manage blogs, as shown below:

Once finished, use a browser to visit your domain name [www.xxxxxxxx.xx](http://www.xxxxxxxx.xx) to see your blog, as shown below:

---

**FAQ**
If you encounter a problem when using CVM, refer to the following documents for troubleshooting based on your actual situation.

- For issues regarding CVM login, see Password Login and SSH Key Login and Login and Remote Access.
- For issues regarding the CVM network, see IP Addresses and Ports and Security Groups.
- For issues regarding CVM disks, see System and Data Disks.
Setting up Drupal

Last updated : 2020-04-13 11:14:22

Scenario

Drupal is a free and open-source content management framework written in PHP and distributed under the GNU General Public License. Drupal provides a back-end framework for at least 2.3% of all websites worldwide – ranging from personal blogs to corporate sites. This article describes how to setup Drupal manually on a CVM.

To manually setup a Drupal-based personal website, you need to be familiar with Linux commands, such as using YUM to install software on CentOS. You should also be familiar with software usage and compatibility.

Software

This article describes how to install the following software

- Linux operating system. This article uses CentOS 7.6.
- Apache is a web server software. This article uses Apache 2.4.6.
- MariaDB is a database management system. This article uses MariaDB 10.4.8.
- PHP is a scripting language. This article uses PHP 7.0.33.
- Drupal is a content management framework. This article uses Drupal 8.1.1.

Prerequisites

You need a Linux CVM. If you have not purchased one yet, see this article for information on how to get started with a Linux CVM.

Directions

Step 1 Logging in to a Linux instance

Log in to a Linux instance using WebShell (recommended). You can also use other login methods that you are comfortable with:
• Log in to a Linux instance using remote login software.
• Log in to a Linux instance using SSH

Step 2 Setting up LAMP
After logging in, set up LAMP so you can run Drupal. Refer to this article for details.

Step 3 Downloading and installing Drupal
1. Run the following commands to download the Drupal install package to the root directory of your website.

   cd /var/www/html/


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

   unzip drupal-8.1.1.zip

   mv drupal-8.1.1/ drupal/

Step 4 Configuring Drupal
1. Run the following command to open the Apache configuration file.

   vi /etc/httpd/conf/httpd.conf

2. Press i to enter edit mode. Find AllowOverride None in Directory "/var/www/html"</Directory> and replace it with the following:

   AllowOverride All
The result is shown below:

```
# Further relax access to the default document root:
<Directory "/var/www/html">
  # possible values for the Options directive are "None", "All",
  # or any combination of:
  # Indexes Includes FollowSymLinks SymLinksIfOwnerMatch ExecCGI MultiViews
  # Note that "MultiViews" must be named "explicitly" --- "Options All"
  # doesn't give it to you.
  # The Options directive is both complicated and important. Please see
  # http://httpd.apache.org/docs/2.4/mod/core.html#options
  # for more information.
  Options Indexes FollowSymLinks

  # AllowOverride controls what directives may be placed in .htaccess files.
  # It can be "All", "None", or any combination of the keywords:
  # Options FileInfo AuthConfig Limit
  AllowOverride All

  # Controls who can get stuff from this server.
  Require all granted
</Directory>
```

3. Press Esc to exit edit mode and enter :wq to save the file and return.
4. Run the following command to change the access permission of the root directory of the website for the user apache.

```
chown -R apache:apache /var/www/html
```

5. Run the following command to reboot Apache service.

```
systemctl restart httpd
```

**Configure a database for Drupal**

Instructions for configuring MariaDB user credentials may vary depending on different versions. Consult official MariaDB website for details.

1. Run the following command to enter MariaDB.
Configure root

1. Run the following command to enter MariaDB.

```
mysql
```

2. Run the following command to set a password for root.

```
ALTER USER root@localhost IDENTIFIED VIA mysql_native_password USING PASSWORD('your_password');
```

3. Run the following command to exit MariaDB.

```
q
```

Step 5 Installing and configuring Drupal

1. Open a browser window on your local machine and visit the following address to install Drupal.
2. Select the language of your preference and click **Save and continue**

3. Select **Standard installation** and click **Save and continue**

4. Input relevant database information configured in [Configuring a database for Drupal](#). Click **Save and continue**

   Drupal installation now checks to see if all installation criteria are met. If so, installation starts. If not, error messages appear. Resolve them before continuing.

5. The configuration page loads automatically after installation is completed. Input information and click **Save and continue**

   Record your maintenance username and password.

6. The homepage of your Drupal loads automatically. Use the maintenance username and password to log in

   You have now successfully set up your Drupal website. Customize your experience as you see fit.

**FAQ**

If you encounter a problem when using CVM, refer to the following documents for troubleshooting based on your actual situation.

- For issues regarding CVM login, see [Password Login and SSH Key Login](#) and [Login and Remote Access](#).
- For issues regarding the CVM network, see [IP Addresses](#) and [Ports and Security Groups](#).
- For issues regarding CVM disks, see [System and Data Disks](#).