Cloud Virtual Machine

Best Practice

Product Documentation
Copyright Notice

© 2013-2019 Tencent Cloud. All rights reserved.

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

Trademark Notice

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

Service Statement

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

Best Practice

Best Practices

Setting up a Website

Building an Environment

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

Manually Building an WIPM Environment
  Step1: Install and Configure IIS
  Step2: Install and Configure PHP
  Step3: Install and Build MySQL

Building a Website

Setting up WordPress
  Manually Building WordPress Website
  Manually build WordPress personal site (Windows)

Build Discuz! Forum
  Manually Building Discuz! Forum

Setting up a Ghost Blog

Setting up Drupal

Building an Application

Build the FTP Service
  Building the FTP Service (Linux)
  Building the FTP Service (Windows)

The NTP Service
  The NTP service of Tencent Cloud
  Set the NTP service on a Linux instance
  Transitioning from ntpdate to ntpd on a Linux Instance
  Set the NTP service on a Windows instance
Building Microsoft SharePoint 2016
Building the Primary/Secondary PostgreSQL Architecture
Building the Docker
Building GitLab
Building RabbitMQ
Network Performance Test
Recovering Data on Linux CVMs
Building a Visual Ubuntu Desktop
Changing Kernel of a Linux Instance Manually
Managing Disk Space on Windows CVMs
Using RemoteFx to Redirect USB Devices in Windows
Using USB/IP to Share USB Devices in Linux
This article aims to help users improve the security and reliability of their CVM instances.

Security and Network

- **Limited access**: restrict access by using a firewall (Security Group) to only allow the trusted addresses to access instances. The security group should also have stringent rules such as limiting access to ports and by IP addresses.
- **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 easily accessed by external sources.
- **Network logical isolation**: use VPC to divide resources into logical zones.
- **Account permission management**: when it is necessary to allow multiple different accounts to access the same set of cloud resources, you can manage permissions to cloud resources using the policy mechanism.
- **Secure login**: log in to your Linux instances using the SSH key whenever possible. For the instances that you log in with a password, the password needs to be changed regularly.

Storage

- **Hardware storage**: for data that requires high reliability, use Tencent Cloud’s cloud disks to ensure the persistent storage and reliability of data. Try not to use Local Disks for storage. For more information, see the [Cloud Block Storage Product Documentation](https://cloud.tencent.com/document/product/215/13260).
- **Database**: for databases that are frequently accessed and whose capacity frequently changes, use Tencent Cloud TencentDB.

Backup and Recovery

- **Intra-region instance backup**: you can back up your instances and business data using custom images and CBS snapshots. For more information, refer to [CBS Snapshot](https://cloud.tencent.com/document/product/215/13263) and [Creating Custom Images](https://cloud.tencent.com/document/product/215/13263).
- **Cross-region instance backup**: you can copy and back up instances across regions by [Copying Images](#).
- **Blocking instance failures**: you can use [EIPs](#) for domain name mapping to ensure that the server can quickly redirect the service IP address to another CVM instance when it is unavailable, thereby shielding instance failures.

**Monitoring and Alarms**

- **Monitoring and event response**: periodically check monitoring data and set proper alarms. For more information, refer to the [Cloud Monitor Product Documentation](#).
- **Handling request spikes**: with [Auto Scaling](#), the stability of CVMs during peak hours can be guaranteed and unhealthy instances can be replaced automatically.
Running a personal website or forum is one of the most common things people do after they purchase a CVM.

How to setup a website

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

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>Advantages</td>
</tr>
<tr>
<td>Duration</td>
</tr>
<tr>
<td>Difficulty</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><strong>WordPress (Linux)</strong></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><strong>WordPress (Windows)</strong></td>
<td></td>
</tr>
<tr>
<td>Discuz!</td>
<td><strong>Discuz!</strong></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><strong>LNMP (CentOS 7)</strong></td>
<td>LNMP is a common web service architecture which consists of Nginx, MySQL/MariaDB and PHP running on Linux.</td>
</tr>
<tr>
<td></td>
<td><strong>LNMP (CentOS 6)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>LNMP (openSUSE)</strong></td>
<td></td>
</tr>
<tr>
<td>LAMP</td>
<td><strong>LAMP</strong></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><strong>WIPM</strong></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><strong>Drupal</strong></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><strong>Ghost</strong></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>
Building an Environment
Setting up LNMP
Manually Building an LNMP Environment (CentOS 7)

Last updated: 2020-08-18 16:12:58

Scenario

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).

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

Sample Software Versions

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

- 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.

Prerequisites

You have purchased a Linux CVM.

Directions

Step 1: Logging in to a Linux instance
Log in to a Linux instance in standard mode (recommended). You can also use other login methods based on your requirements:

- Log in to a Linux instance by using remote login software
- Log in to a Linux instance by 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 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`, and save the file and return.
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 the editing mode, and edit the `nginx.conf` file.
7. Find `server{...}` and replace the string inside the curly brackets with the following. This is to cancel the listening of IPv6 address and configure Nginx to realize linkage with PHP.

   ```
   server {
   listen 80;
   root /usr/share/nginx/html;
   server_name localhost;
   #charset koi8-r;
   #access_log /var/log/nginx/log/host.access.log main;
   
   location / {
   index index.php index.html index.htm;
   }
   ```

You can use Ctrl+F for page down and Ctrl+B for page up to view the file.
If you cannot find `server{...}` in `nginx.conf`, add the following before `include /etc/nginx/conf.d/*.conf;`, as shown in the following figure:

```nginx
http {
    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    log_format main '$remote_addr - $remote_user [$time_local] "$request" "$status $body_bytes_sent $http_referer" "$http_x_forwarded_for"';

    access_log /var/log/nginx/access.log main;

    sendfile on;
    tcp_nopush on;
    keepalive_timeout 65;
    gzip on;

    include /etc/nginx/conf.d/*.conf;
}
```

8. Press Esc, enter `:wq`, and save the file and return.
9. Run the following command to launch Nginx.

```
systemctl start nginx
```

0. Run the following command to configure the automatic launch of Nginx on startup.

```
systemctl enable nginx
```
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!](image)

**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 a database

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

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

   If the following appears, MariaDB has been installed.

   ![MariaDB packages](image)

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

   ```bash
   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/`.

   ```bash
   vi /etc/yum.repos.d/MariaDB.repo
   ```
3. Press i to switch to the editing mode and enter the following to add MariaDB.

Different operating systems use different versions of MariaDB. For installation information about other operating system versions, visit the MariaDB website.

```
# 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
```

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

5. Run the following command to install MariaDB. Please pay attention to the installation progress and wait for the installation to complete.

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

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

```
systemctl start mariadb
```

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

```
systemctl enable mariadb
```

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

```
mysql
```

If the following 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.

```bash
$q
```

### Step 4: Installing and configuring PHP

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

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

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

```bash
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 launch the PHP-FPM service.

```bash
systemctl start php-fpm
```

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

```bash
systemctl enable php-fpm
```

### Verifying Your Setup

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
http://<Public IP address of the CVM instance>
```
If the following results appear, the environment configuration was successful.

Relevant Operations

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

FAQs

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 Disks and Data Disks.
Setting up LNMP manually (CentOS 6)

Last updated : 2020-07-20 16:40:22

Overview

The LNMP environment is a website server architecture consisting of Nginx, MySQL or MariaDB, and PHP running on Linux. This document describes how to manually set up the LNMP environment on a Tencent Cloud CVM.

To manually set up the LNMP environment, you should familiarize yourself with common Linux commands such as installing software via YUM in CentOS, and understand the usage and version compatibility of the software to be installed.

Sample Software Versions

In this example, the following software versions are used to build the LNMP environment:
CentOS is a distribution of the Linux operating system. This document uses CentOS 6.9 as an example.
Nginx is a web server. This document uses Nginx 1.17.5 as an example.
MySQL is a database software. This document uses MySQL 5.1.73 as an example.
PHP is a scripting language. This document uses PHP 7.1.32 as an example.

Prerequisites

Setting up a LNMP environment requires a Linux CVM. If you have not purchased a Linux CVM yet, see Customizing Linux CVM Configurations.

Directions

Step 1: log in to a Linux instance

- Log in to a Linux instance using the standard login method (recommended). You can also use other login methods that you are more comfortable with:
- Log in to a Linux instance using remote login software.
- Log in to a Linux instance using SSH.
**Step 2: install 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/6/$basearch/
   gpgcheck=0
   enabled=1
   ```

3. Press `Esc` and enter `:wq` to save and close the file.

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 the editing mode, and edit the `nginx.conf` file.

7. Find `server{...}` and replace the content inside the curly brackets with the following. This is to cancel the listening of the IPv6 address and configure Nginx to realize linkage with PHP.
   ```
   server {
     listen 80;
     root /usr/share/nginx/html;
     server_name localhost;
     #charset koi8-r;
     #access_log /var/log/nginx/log/host.access.log main;
     #
     location / {
       index index.php index.html index.htm;
     }
     #error_page 404 /404.html;
     #redirect server error pages to the static page /50x.html
     #
     error_page 500 502 503 504 /50x.html;
     location = /50x.html {
       root /usr/share/nginx/html;
     }
     #pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000
     #
     location ~ .php$ {
       fastcgi_pass 127.0.0.1:9000;
   ```
fastcgi_index index.php;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
include fastcgi_params;
}
}

If you cannot find `server{...}` in the `nginx.conf` file, add the content of the `server{...}` at the top of `include /etc/nginx/conf.d/*conf;`, as shown below:

```
http {
    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    log_format main  '$remote_addr - $remote_user [$time_local] "$request" '
                    '$status $body_bytes_sent "$http_referer" '
                    '"$http_user_agent" "$http_x_forwarded_for"';

    access_log /var/log/nginx/access.log main;
    sendfile on;
    tcp_nopush on;
    keepalive_timeout 65;
    gzip on;

    include /etc/nginx/conf.d/*.conf;
}
```

--- INSERT ---

8. Press `Esc` and enter `:wq` to save and close the file.
9. Run the following command to start Nginx.

   ```
   service nginx start
   ```
0. Run the following commands to automatically launch Nginx at startup.

   ```
   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. Commercial support is available at nginx.com.

Thank you for using nginx.

Step 3: install a database

1. Run the following command to check whether MySQL has been already installed.

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

   - If the following appears, MySQL has already been installed.

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

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

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

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

2. Run the following command to install MySQL.

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

3. Run the following command to start MySQL.

   ```bash
   service mysqld start
   ```

4. Run the following commands to automatically launch MySQL at startup.

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

5. Run the following command to verify whether MySQL has been successfully installed.

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: install and configure 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 commands to automatically launch PHP-FPM at startup.

```
chkconfig --add php-fpm
```
Verifying the Environment Configuration

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

2. Run the following command to restart Nginx.
   ```bash
   service nginx restart
   ```

3. In a local browser, visit the following URL to check whether the environment has been successfully configured.
   ```plaintext
   http://[Public IP address of the CVM instance]
   ```
   If the following appears, the environment has been successfully configured.

![PHP Version 7.1.32](image)

Relevant Operations

After the LNMP environment is built, you can manually build a WordPress website to familiarize yourself with CVM and its features.
FAQs

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

- 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 Address and Port.
- 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:

```
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.

```
zypper ref
```

### Step 3: Installing and configuring Nginx

1. Run the following command to install Nginx.

```
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.

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

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

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

4. Press `i` to toggle edit mode.

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

```nginx
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;
    }
}
```
fastcgi_index index.php;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
include fastcgi_params;
}
}

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.

```
systemctl restart nginx
```

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

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

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

```
<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.

```
hello world!
```

### Step 4: Installing and configuring MySQL

1. Run the following command to install MySQL.

```
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.

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

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

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

If the following appears, you have successfully logged in.

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

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

5. Run the following command to apply the configuration:

```
flush privileges;
```

6. Run the following command to exit MySQL.

```
\q
```

**Step 5: Installing PHP**

Run the following command to install PHP:

```
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!](image)

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

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.

   ```bash
   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.

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

3. Run the following commands to create symbolic links.

   ```bash
   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.

   ```bash
   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.

   ```bash
   yum install -y git
   ```

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

   ```bash
   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.

```
[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:

```
[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.

```
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
```
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

Setting up Java Web Manually

Last updated : 2020-11-20 10:11:39

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 Windows, use WinSCP to upload the file.
   - 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 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/tomcat-8/v8.5.47/bin/apache-tomcat-8.5.47.tar.gz) for more information.
   ```

   ```shell
   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.

```
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.

    yum install httpd -y

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

    systemctl start httpd

    systemctl enable httpd

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

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

    The following appears if Apache is installed properly:

    ![Testing 123..](image)

    This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that this site is working properly. This server is powered by CentOS.

**Step 3: Installing MariaDB**

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

    rpm -qa | grep -i mariadb

   - If the following appears, MariaDB is already installed.

    ![MariaDB output](image)

    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/`.

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

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

   ```
   # 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](https://mariadb.org).

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
```

# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
# <Directory />
# AllowOverride none
# Require all granted
#</Directory>
#
#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#<IfModule dir_module>
# DirectoryIndex index.php index.html
#</IfModule>
#
#
# If the AddEncoding directives above are commented-out, then you
# probably should define those extensions to indicate media types:
#<AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz
# AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
#

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.

   ```url
   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.
Manually Building an WIPM Environment

Step1: Install and Configure IIS

Overview

This document describes how to add and install IIS roles on a CVM instance with Windows Server 2012 R2 or Windows Server 2008.

Directions

Windows Server 2012 R2

1. Log in to Windows CVM.
2. On the desktop, click and open **Server Manager**, as shown below:

![Server Manager](image)

3. Click **Add roles and features** and enter the “Add Roles and Features Wizard” window.
4. In the pop-up window, click **Next** and enter the “Select installation type” page.
5. Select **Role-based or feature-based installation** and click **Next** twice, as shown below:

6. Check **Web Server (IIS)** on the “Select server roles” page, as shown below:
   
The “Add features that are required for Web Server (IIS)** dialog box will pop up.
7. Click **Add Features** in the pop-up dialog box, as shown below:

8. Click **Next**.

9. On the **Features** page, check **.NET Framework 3.5 Features** and click **Next** twice, as shown below:
0. On the **Role Services** page, check **CGI** and click **Next**, as shown below:
1. Review your installation selections and click **Install**. Wait for the installation process to complete.

![Confirm installation selections](image)

2. When the installation has completed, open a browser on CVM and visit `http://localhost/` to verify if IIS has been successfully installed.
If the following page appears, it indicates that IIS has been successfully installed.

Windows Server 2008

1. Log in to Windows CVM.

2. On the desktop, click [image] and open Server Manager, as shown below:
3. Select **Roles** in the left sidebar, and click **Add Roles** in the right panel, as shown below:

![Add Roles Wizard](image)

4. Click **Next** in the “Add Roles Wizard” window, as shown below:

![Add Roles Wizard](image)
5. On the “Server Roles” page, check **Web Server (IIS)**, and click **Next** twice, as shown below:

![Select Server Roles](image1)

6. On the **Role Services** page, check **CGI** and click **Next**, as shown below:

![Select Role Services](image2)
7. Review your installation selections and click **Install**. Wait for the installation process to complete.

8. When the installation has completed, open a browser on CVM and visit [http://localhost/](http://localhost/) to verify if IIS has been successfully installed.
If the following page appears, it indicates that IIS has been successfully installed.
Step2: Install and Configure PHP

Scenario

This document uses a CVM running Windows Server 2012 R2 as an example to describe how to configure PHP 5.3 and earlier versions or versions later than 5.3 in a Windows CVM.

Prerequisites

- You have logged in to the Windows CVM and added and installed the IIS role in the CVM. For more information, see Step 1: Installing and Configuring IIS.
- You have obtained the public IP address of the Windows CVM. For more information, see Obtaining the Public IP Address of an Instance.

Directions

Installing PHP 5.3 or earlier

The PHP official website no longer provides the installation packages for versions earlier than PHP 5.2. If you require a version earlier than PHP 5.2, search for and download it from the CVM. Alternatively, download it locally and then upload the installation package to the CVM. For more information on how to upload files to a Windows CVM, see Uploading Files Through MSTSC to a Windows CVM from Windows. The following procedure uses PHP 5.2.13 as an example.

1. Open the PHP installation package in the CVM.
2. Click Next.
3. On the "Web Server Setup" page, select IIS FastCGI and click Next, as shown in the following figure:
4. Complete PHP installation as prompted.

5. Create a PHP file such as `hello.php` in `C:/inetpub/wwwroot`.

6. In the created `hello.php` file, add the following code and save the file.

   ```php
   <?php
   echo "<title>Test Page</title>";
   echo "hello world";
   ?>
   ```

7. On the desktop, open the browser and visit `http://<Public IP address of the Windows CVM>/hello.php` and check whether the environment is successfully configured.

   If the page shown below appears, the configuration was successful.
Installing a version later than PHP 5.3

Versions later than PHP 5.3 do not have an installation package and are installed by using a zip file or debug pack. The following demonstrates how to install PHP in a Windows Server 2012 R2 environment by using a zip file.

**Downloading software**

1. In the CVM, go to the [PHP official website](https://www.php.net) and download the compressed PHP installation package, as shown in the following figure:

   To run PHP under IIS, you must select the x86 installation package for Non Thread Safe. If your server is running Windows Server 32-bit (x86), replace IIS with Apache and select the x86 installation package for Thread Safe.
2. Based on the name of the downloaded PHP installation package, download and install the Visual C++ Redistributable installation package.
The following table lists the Visual C++ Redistributable installation packages that need to be downloaded and installed for the PHP installation package.

<table>
<thead>
<tr>
<th>PHP Installation Package Name</th>
<th>Download Address of the Visual C++ Redistributable Installation Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>php-x.x.x-nts-Win32-VC16-x86.zip</td>
<td>Microsoft Visual C++ Redistributable for Visual Studio 2019</td>
</tr>
<tr>
<td>php-x.x.x-nts-Win32-VC15-x86.zip</td>
<td>Microsoft Visual C++ Redistributable for Visual Studio 2017</td>
</tr>
<tr>
<td>php-x.x.x-nts-Win32-VC14-x86.zip</td>
<td>Microsoft Visual C++ Redistributable for Visual Studio 2015</td>
</tr>
</tbody>
</table>

For example, if the name of the downloaded PHP installation package is **PHP-7.1.30-nts-Win32-VC14-x86.zip**, download and install the Microsoft Visual C++ Redistributable for Visual Studio 2015 installation package.

**Installation and configuration**

1. Decompress the downloaded PHP installation package, for example, to `C:\PHP`.
2. Copy the `php.ini-production` file in `C:\PHP` and change the file extension to `.ini`, that is, rename it to `php.ini`, as shown in the following figure:

3. On the desktop, click to open **Server Manager**, as shown in the following figure:
4. In the left sidebar, click **IIS**.
5. In the right IIS management window, right-click the server name in the **Server** column and choose **Internet Information Services (IIS) Manager**, as shown in the following figure:
6. In the "Internet Information Service (IIS) Manager" window, click the server name in the left sidebar to go to the server homepage, as shown in the following figure:
For example, click the 10_141_9_72 server name to go to the 10_141_9_72 homepage.

7. On the **10_141_9_72 homepage**, double-click **Handler Mappings** to go to the "Handler Mappings" page, as shown in the following figure:
8. In the **Actions** column on the right, click **Add Module Mapping** to open the "Add Module Mapping" window.

9. In the "Add Module Mapping" window, enter the following information and click **OK**, as shown in the following figure:
The main parameters include:

- Request path: enter `*.php`.
- Module: select "FastCgiModule".
- Executable (optional): select the php-cgi.exe file in the PHP installation package, that is, `C:\php\php-cgi.exe`.
- Name: enter a custom name, such as FastCGI.

0. In the window that appears, click **OK**.
1. Click the **10_141_9_72** server name in the left sidebar to return to the 10_141_9_72 homepage.
2. On the **10_141_9_72 homepage**, double-click **Default Document** to go to the default document management page, as shown in the following figure:
3. In the **Actions** column on the right, click **Add** to open the "Add Default Document" window.

4. In the "Add Default Document" window, set **Name** to `index.php` and click **OK**, as shown in the following figure:
5. Click the 10_141_9_72 server name in the left sidebar to return to the 10_141_9_72 homepage.

6. On the **10_141_9_72 homepage**, double-click **FastCGI Settings** to open the FastCGI setting management page, as shown in the following figure:
7. On the FastCGI setting management page, select the FastCGI application and click **Edit**, as shown in the following figure:
8. In the "Edit FastCGI Application" window, set **Monitor changes to file** to the `php.ini` file path, as shown in the following figure:

![Edit FastCGI Application](image)

9. In `C:\inetpub\wwwroot`, create a PHP file, such as `index.php`.

0. In the created `index.php` file, add the following code and save the file.

```php
<?php
    phpinfo();
?>
```
1. On the desktop, open the browser and visit \texttt{http://localhost/index.php} to check whether the environment is configured successfully. If the page shown below appears, the configuration was successful.

![PHP Version 7.1.30](image-url)
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:
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:
7. In the **Apply Configuration** window, click **Execute**.

![MySQL Installer Apply Configuration 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**.

![MySQL Installer](image)

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:
Installation Complete

The installation procedure has been completed.

- [ ] Copy Log to Clipboard
- [x] Start MySQL Workbench after Setup
- [x] 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:

![MySQL Shell](image)

**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.
Building a Website
Setting up WordPress
Manually Building WordPress Website

Last updated : 2020-07-27 09:44:20

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 LNMP environment by referring to Manually Building an LNMP Environment (CentOS 7).

**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:
   ```
   
   ```

**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:

```
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:

```
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:

```
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:

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

3. Press \texttt{i} to enter the editing mode. Find the MySQL section in the file and modify the settings as described in \textit{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 \texttt{Esc} and enter :\texttt{wq}. Then, save the changes and close the file.

**Step 6: Verify WordPress installation**

1. In the address box of the browser, enter \texttt{http://\langle Domain name or public IP address of the CVM instance\rangle/\langle WordPress folder\rangle}, for example:

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

   Press \texttt{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 \textit{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</td>
</tr>
</tbody>
</table>
prone to be cracked.

<table>
<thead>
<tr>
<th>Password</th>
<th>Use the default strong password or a custom password. Do not use previous passwords and save the password in a secure place.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email address</td>
<td>Email address for receiving notifications</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](#).
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 the `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`.

   ```
   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 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.

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

1. Click Add Website.

2. 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`.

3. 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.
   - i. Find `extension_dir= "ext"` and delete the ; at the beginning.

14 Save `php.ini`.

**Step 4: Verifying the WordPress Configuration**

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](#).
Build Discuz! Forum
Manually Building 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:

```
[root@CVM_149_104_centos ~]# mysql -u root -p 123456
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)
[root@CVM_149_104_centos ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 27
Server version: 5.5.60-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)]>
```

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
```
If it is, the following appears:

![PHP Version 5.4.16](image)

<table>
<thead>
<tr>
<th>System</th>
<th>Linux VM_149.104.centos 3:10.0-862.el7.x86_64 #1 SMP Fri Apr 20 16:44:24 UTC 2018 x86_64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build Date</td>
<td>Oct 30 2018 19:31:42</td>
</tr>
<tr>
<td>Server API</td>
<td>Apache 2.0 Handler</td>
</tr>
<tr>
<td>Virtual Directory</td>
<td>disabled</td>
</tr>
<tr>
<td>Support</td>
<td></td>
</tr>
<tr>
<td>Configuration File</td>
<td>/etc</td>
</tr>
<tr>
<td>(php.ini) Path</td>
<td></td>
</tr>
</tbody>
</table>

**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**.
Setting up a Ghost Blog

Last updated : 2020-08-21 14:11:52

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 setup Ghost on a CVM.

To setup 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. If the domain name is used for Mainland China service, ICP filing is required.

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.

   ```
   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:

   ![Adduser Command Output]

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.
2. Run the following command to install Node.js.

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

### Install Ghost-CLI

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

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

### Step 5 Install and configure Ghost

1. Run the following commands.

```bash
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.

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

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

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.
```
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:

![Create your account form](image)

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

![Administration Page](image1)

Once finished, use a browser to visit your domain name `www.xxxxxxxx.xx` to see your blog, as shown below:

![Blog Page](image2)

**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:

```bash
# 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**.

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

5. Run the following command to reboot Apache service.

   ```bash
   systemctl restart httpd
   ```

**Configure a database for Drupal**

Instructions for configuring MariaDB user credentials may vary depending on different versions. Consult [official MariaDB website](http://example.com) for details.

1. Run the following command to enter MariaDB.
2. Run the following command to create a database named `drupal`.

   ```sql
   CREATE DATABASE drupal;
   ```

3. Run the following command to create a new user `user` and set its password to `123456`.

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

4. Run the following command and grant `user` all privileges to `drupal`.

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

5. Run the following command to apply all configurations.

   ```sql
   FLUSH PRIVILEGES;
   ```

6. Run the following command to exit MariaDB.

   ```bash
   \q
   ```

**Configure root**

1. Run the following command to enter MariaDB.

   ```bash
   mysql
   ```

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

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

3. Run the following command to exit MariaDB.

   ```bash
   \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.
Building an Application

Build the FTP Service

Building 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.

   ![FTP service started](image)

   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.

   - `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.

   ```
   #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.

   - `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:

   ```
   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:
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 \( \text{pasv\_min\_port} \) to \( \text{pasv\_max\_port} \) 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:

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

```bash
ls -l /home/test
# Here, /home/test indicates the FTP directory. Replace it with your actual FTP directory.
```
Building the FTP Service (Windows)

Overview

This document describes how to use IIS to build an FTP site on a Windows CVM instance.

Sample Software Versions

This document uses the following software versions as an example to build the FTP service.

- Operating system: Windows. This document uses Windows Server 2012 as an example.
- Web server: IIS. This document uses IIS 8.5 as an example.

Directions

Step 1: log in to the Windows CVM

- Log in to a Windows CVM instance using an RDP file (recommended).
  You can also use other login methods that you are more comfortable with: log in to a Windows CVM instance using a remote desktop.

Step 2: install the FTP service on IIS

1. On the desktop, click to open the server manager. The Server Manager window will appear.
2. Click Add roles and features, as shown below.
3. In the “Add Roles and Features Wizard” pop-up window, click Next to access the “Installation Type” page.

4. Select **Role-based or feature-based installation** and click **Next**.

5. On the “Select destination server” page, keep the default configurations and click **Next**.
6. On the “Select server roles” page, check **Web Server (IIS)** and click **Add Feature** in the window that pops up, as shown below:
7. Click **Next** 3 times to access the “Select role services” page.
8. Check **FTP Service** and **FTP Extensibility**, and click **Next**, as shown below:
9. Click **Install** to start installing the FTP service.
10. After the installation is completed, click **Close**.

">

**Step 3: create an FTP username and password**

**Note:**

The following steps create an FTP account with password authentication. If you plan to use anonymous access only, skip this section.

1. In the “Server Manager” window, select **Tools -> Computer Management** in the top-right navigation bar to open the “Computer Management” window.
2. Select **System Tools -> Local Users and Groups -> Users** in the left sidebar.
3. On the right panel of the **Users** interface, right-click the blank space and select **New User**, as shown below:
4. On the “New User” page, configure the username and password according to the following instructions. Click **Create**, as shown below:

Set the main parameters as follows:
- **User name**: custom. This document uses **ftpuser** as an example.
Password and Confirm password: custom. The password must contain uppercase and lowercase letters and digits. This document uses tf7295TFY as an example.

Clear User must change password at next logon, and check Password never expires. Select options based on your actual needs. This document uses Password never expires as an example.

5. Click Close. You can see the newly created user ftpuser in the list.

Step 4: set the shared folder permission

**Note:**

This document uses the C:\test folder as the shared folder of the FTP site. It contains the test.txt file you want to share with others. Create the C:\test folder and the test.txt file under it as instructed. You can also use any other folder as needed.

1. On the desktop, click to open the “This PC” window.
2. Select and right-click the test folder under the C drive. Select Properties.
3. In the “test Properties** window, select the Security tab.
4. Select Everyone and click Edit, as shown below:
   
   If “Group or user names” does not contain Everyone, refer to Adding Everyone to add the user.
5. On the “Permissions for test” page, set the permission for **Everyone** and click **OK**, as shown below:
This document uses granting **Everyone** all permissions as an example.

6. Click **OK** to complete the configuration.

**Step 5: add an FTP site**

1. In the “Server Manager” window, select **Tools -> *Internet Information Services (IIS) Manager*** in the top-right navigation bar.

2. In the **Internet Information Service (IIS) Manager** pop-up window, expand your server in the left sidebar, right-click **Sites**, and select **Add FTP Site**, as shown below:
3. On the “Site Information” page, enter the following information and click **Next**, as shown below:

- **FTP site name**: name of your FTP site. This document uses `ftp` as an example.
- **Physical path**: path of the shared folder with the permission configured. This document uses `C:\test` as an example.

4. On the “Binding and SSL Settings” page, enter the following information and click **Next**, as shown below:
Configure the main parameters as follows:

- **Binding**: the “IP Address” defaults to **All Unassigned**. The default FTP port number is 21. You can set a custom port number.

- **SSL**: select an option. In this document, **No SSL** is selected.
  - **No SSL**: no SSL is used.
  - **Allow SSL**: allow the FTP server to connect with clients with or without SSL.
  - **Require SSL**: SSL encryption is required for communication between the FTP server and clients.

  If you choose **Allow SSL** or **Require SSL**, you can select an existing SSL certificate in “SSL Certificates”, or create an SSL certificate.

5. On the “Authentication and Authorization Information” page, enter the following information and click **Next**, as shown below:
- **Authentication**: select an identity verification method. This document uses **Basic** as an example.
  - **Anonymous**: allow users that provide the anonymous or FTP username to access the content.
  - **Basic**: require users to provide valid user names and passwords to access the content. Under this mode, passwords are transmitted without encryption. Therefore, select this authentication mode only when you know that the connection between the clients and the FTP server is secure (for example, by using SSL).

- **Authorization**: select one of the following options from the **Allow access to** drop-down list. This document uses the specified **ftpuser** user as an example.
  - **All users**: all users, anonymous or identified, can access the content.
  - **Anonymous users**: anonymous users can access the content.
  - **Specified role or user group**: only the specified roles or members of the specified groups can access the content. If you choose this option, you need to specify the roles or user groups.
Specified users: only the specified user can access the content. If you choose this option, you need to specify the username.

Permissions: configure the permissions for the authorized users. This document takes setting the Read and Write permissions as an example.

- Read: allow the authorized user to read the shared content.
- Write: allow the authorized user to write into the directory.

6. Click Finish to successfully create the FTP site.

**Step 6: configure the security group and firewall**

1. After the FTP site is created, add an inbound rule that allows traffic to the FTP port based on the FTP access mode:
   - **Active mode**: open the ports 20 and 21.
   - **Passive mode**: open the ports 21 and 1024 - 65535.
     
     For more information, see Adding Security Group Rules.

2. (Optional) Refer to [Microsoft documentation](https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831655(v=ws.11)) on how to configure the firewall so that the FTP server is able to accept passive connections from the firewall.

**Step 7: test the FTP site**

You can use tools such as the FTP client software, browser, or file manager to verify the FTP server. This document uses the file manager of the client as an example.

1. Configure Internet Explorer as needed:
   - Firewall configured (active mode):
     
     Open an Internet Explorer window on the Client side and select Tools -> Internet Options -> Advanced. Uncheck Use Passive FTP for the firewall and the DSL modem compatibility and click OK.
   
   - Firewall has not been configured (passive mode):
     
     a. Open an Internet Explorer window on the FTP server side and select Tools -> Internet Options -> Advanced. Uncheck Use Passive FTP for the firewall and the DSL modem compatibility and click OK.
     
     b. Open an Internet Explorer window on the Client side and select Tools -> Internet Options -> Advanced. Check Use Passive FTP for the firewall and the DSL modem compatibility and click OK.

2. Open the PC where the client is installed, type the following address in the address box of the browser, and press Enter, as shown below:

   
   ftp://CVM public IP address:21

©2013-2019 Tencent Cloud. All rights reserved.
3. In the pop-up window, enter the username and password configured in creating the FTP username and password.

   In this document, the username is `ftpuser`, and the password is `tf7295TFY`.

4. You can upload and download files after a successful login.

Appendix

">

Adding Everyone
1. In the “test Properties” window, select the Security tab and click Edit, as shown below:

![Security tab in test Properties window]

2. On the “Permissions for test” page, click Add.
3. On the “Select Users or Groups” dialog box, click Advanced.
4. In the pop-up window, click Find Now.
5. Select **Everyone** under **Search results** and click **OK**, as shown below:
6. On the “Select Users or Groups” dialog box, click OK, as shown below:

![Select Users or Groups dialog box](image)

Go to Step 5 to configure the permission for Everyone.

">

**Creating a server certificate**

1. In the “Server Manager” window, select **Tools -> Internet Information Services (IIS) Manager** in the top-right navigation bar.

2. In the “Internet Information Services (IIS) Manager” pop-up window, select the server in the left sidebar and double-click **Server Certificates** on the right panel, as shown below:

![Server Certificates](image)

3. Select **Create Self-Signed Certificate** in the right operation column.
4. In the “Create Self-Signed Certificate” pop-up window, enter a certificate name and the storage type, as shown below:
   This document uses creating an SSL certificate for personal storage as an example.

5. Click **OK**.
The NTP Service

The NTP service of Tencent Cloud

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

The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over a network. NTP servers usually use Coordinated Universal Time (UTC).

Tencent Cloud provides a private NTP server for Tencent Cloud resources. For other devices, you can use the public NTP servers provided by Tencent Cloud.

**Private NTP server**

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

**Public NTP servers**

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

For more information on how to synchronize your clock over NTP on Linux, refer to [Setting NTP Service for Linux Instances](#).

For more information on how to synchronize your clock over NTP on Windows, refer to [Setting NTP Service for Windows Instances](#).
Set the NTP service on a Linux instance

Overview

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 CentOS 7.5 as an example to describe how to install and configure ntpd.

Notes

- Some operating systems use chrony as the default NTP service. Please make sure that ntpd is running and is configured to launch automatically at startup.
  - Run the `systemctl is-active ntpd.service` command to see if ntpd is running.
  - Run the `systemctl is-enabled ntpd.service` command to see if ntpd is configured to launch automatically at startup.
- 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 Rules to open it to the Internet.

Directions

**Installing ntpd**

Run the following command to check whether ntpd has been installed.

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

- If the following result is returned, 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, run the `yum install ntp` command to install it.

```bash
yum -y install ntp
```

ntpd uses the client mode by default.

**Configuring NTP**

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

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

2. Press `i` to switch to the editing mode and locate the `server` configurations. Change the value of `server` to the NTP clock source server you want to use (such as `time1.tencentyun.com`) and delete unwanted values, as shown below:

```bash
# Use public servers from the pool.ntp.org project.
# 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` and enter `:wq` to save and close the file.

**Launching ntpd**

Run the following command to restart the ntpd service.

```bash
systemctl restart ntpd.service
```

**Checking the status of ntpd**

Run the following commands to check the status of ntpd as needed.

- Run the following command to check whether the NTP is normally listening on the service port UDP 123.

```bash
netstat -nupl
```
If the following result is returned, the listening is normal.

```
[root@VM_0_136_centos ~]# netstat -npu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State          PID/Program name
udp   0      0 172.30.0.136:123            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
udp6  0      0 fe80::5054:ff:fe02::123    :::*              :::*            999/ntpd
udp6  0      0 ::1:1123                    :::*              :::*            999/ntpd
```

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

  `service ntpd status`

If the following result is returned, the ntpd status is normal.

```
[root@VM_0_136_centos ~]# service ntpd status
Redirecting to /bin/systemctl status ntpd.service
* ntpd.service - Network Time Service
 Loaded: loaded (/usr/lib/systemd/system/ntpd.service; enabled; vendor preset: disabled)
 Active: active (running) since Thu 2019-08-07 15:23:25 CST; 1 min ago
 Process: 997 ExecStart=/usr/sbin/ntpd -u ntp:ntp $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 999 (ntpd)
   CGroup: /system.slice/ntpd.service
             └─999 /usr/sbin/ntpd -u ntp:ntp
Aug 07 15:23:25 VM_0_136_centos ntpd[999]:  0.0.0.0 c01d 0d kern kernel time sync enabled
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: ntp_jo: estimated max descriptors: 1024, initial... 16
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 0 to 127.0.0.1 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:fe02:1123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listening on routing socket on fd #20 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 CPM
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.
```

- Run 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 that was configured earlier should be returned, as shown below:

```
[root@VM_0_136_centos ~]# ntpstat
synchronised to NTP server (185.35.50.50) at stratum 3
time correct to within 1060 ms
polling server every 64 s
[root@VM_0_136_centos ~]$
```
You can also get the IP address corresponding to the domain name by running the command `nslookup domain name`.

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

  `ntpq -p`

The following result will be returned:

<table>
<thead>
<tr>
<th>remote</th>
<th>refid</th>
<th>st</th>
<th>when</th>
<th>poll</th>
<th>reach</th>
<th>delay</th>
<th>offset</th>
<th>jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>108.12.99</td>
<td>INIT</td>
<td>16</td>
<td>u</td>
<td>64</td>
<td>6</td>
<td>0.000</td>
<td>3.940</td>
<td>5.588</td>
</tr>
<tr>
<td>193.14.34.194</td>
<td>194.14.34.194</td>
<td>2</td>
<td>u</td>
<td>64</td>
<td>17</td>
<td>277.831</td>
<td>1.729</td>
<td>0.263</td>
</tr>
<tr>
<td>193.14.34.194</td>
<td>194.14.34.194</td>
<td>2</td>
<td>u</td>
<td>64</td>
<td>16</td>
<td>201.280</td>
<td>1.003</td>
<td>0.441</td>
</tr>
<tr>
<td>165.14.34.194</td>
<td>194.14.34.194</td>
<td>2</td>
<td>u</td>
<td>64</td>
<td>17</td>
<td>6.507</td>
<td>9.897</td>
<td>0.461</td>
</tr>
</tbody>
</table>

- **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 through 16 from high to low. In order to relieve the load and network congestion, you should avoid connecting directly to a stratum 1 server.
- **when**: the number of seconds that have elapsed since the last successful request.
- **poll**: the synchronization interval (in seconds) between local and remote servers. At the beginning, the **poll** value will be smaller, which indicates a higher synchronization frequency, 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 decrease accordingly.
- **reach**: an octal value used to test whether the server can be connected. Its value increases every time 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 time difference in milliseconds (ms) between the host and the time source through NTP. The closer the offset is to 0, the closer the times of the host and the NTP server are.
- **jitter**: a value used for statistics that records the distribution of offsets over a particular number of consecutive connections. The smaller its absolute value is, the more accurate the host time is.

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

1. Run the following command to automatically launch ntpd at startup.
2. Run the following command to check whether chrony is set to launch at startup.

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

If chrony is set to launch at startup, run the following command to remove chrony from the auto-start list.

```
chrony is not compatible with ntpd, which may lead to ntpd start failure.
systemctl disable chronyd.service
```

**Enhancing ntpd security**

Run the following commands sequentially to enhance the security of the `/etc/ntp.conf` configuration file.

```
interface ignore wildcard

interface listen eth0
```
Transitioning from ntpdate to ntpd on a Linux Instance

Last updated : 2020-09-04 11:49:01

Overview

The ntpdate is a breakpoint update for the time synchronization of your new instances. The ntpd is a stepwise daemon for the time synchronization of your running instances. This document uses the CentOS 7.5 operating system as an example to introduce how to transition from ntpdate to ntpd on CVMs.

Prerequisites

The NTP service communicates on the port UDP 123. Please make sure that you have opened the port to the Internet before transitioning to the NTP service. If the port has not been opened, please refer to Adding Security Group Rules to open it to the Internet.

Directions

You can choose to transition from ntpdate to ntpd manually or automatically.

Transitioning from ntpdate to ntpd manually

Shutting down ntpdate

1. Run the following command to export the crontab configuration and filter ntpdate.
   
   ```
   crontab -l | grep -v ntpupdate > /tmp/cronfile
   ```

2. Run the following command to update the ntpdate configuration.
   
   ```
   crontab /tmp/cronfile
   ```

3. Run the following command to modify the rc.local file.
   
   ```
   vim /etc/rc.local
   ```
4. Press `i` to switch to the edit mode and delete the `ntupdate` configuration line.

5. Press `Esc` and enter `:wq` to save and close the file.

### Configuring ntpd

1. Run the following command to open the configuration file of the NTP service.
   ```
   vi /etc/ntp.conf
   ```

2. Press `i` to switch to the edit mode and locate the `server` configurations. Change the value of `server` to the NTP clock source server you want to use (such as `time1.tencentyun.com`) and delete unwanted values, as shown below:

   ```
   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` and enter `:wq` to save and close the file.

### Transitioning from ntpdate to ntpd automatically

1. Download the `ntpd_enable.sh` script.
   ```
   wget https://image-10023284.cos.ap-shanghai.myqcloud.com/ntpd_enable.sh
   ```

2. Run the following command to transition from ntpdate to ntpd using the `ntpd_enable.sh` script.
   ```
   sh ntpd_enable.sh
   ```

### Relevant Operations

#### Checking the status of ntpd

Run the following commands to check the status of ntpd as needed.

- Run the following command to check whether the NTP is listening normally on the service port UDP 123.
  ```
  netstat -nupl
  ```
If the following result is returned, the listening is normal.

```
[root@VM_0_136_centos ~]# netstat -nulp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp   0      0 172.30.0.136:123              0.0.0.0:*           LISTEN       999/ntpd
udp   0      0 127.0.0.1:123                 0.0.0.0:*           LISTEN       999/ntpd
udp6  0      0 fe80::5054:ff:fe62:123         :::*                  LISTEN       999/ntpd
udp6  0      0 ::1:123                        :::*                  LISTEN       999/ntpd
```

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

```
service ntpd status
```

If the following result is returned, the ntpd status is normal.

```
[root@VM_0_136_centos ~]# service ntpd status
Red Hat 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; 3 min ago
Main PID: 999 (ntpd)
    CGroup: /system.slice/ntpd.service
    -999 /usr/sbin/ntpd -u /ntpd $OPTIONS (code=exited, status=0/SUCCESS)
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c01d 0d kern kernel time sync enabled
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: ntpio: estimated max descriptors: 1024, initia... 16
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: listen normally on 0 lo 127.0.0.1 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:fe62:11...123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: listening on routing socket on fd #20 for inter...tes
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c01e 66 restart
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c012 02 freq set kernel 0.467 PPM
Aug 07 15:23:34 VM_0_136_centos ntpd[999]: 0.0.0.0 c615 05 clock_sync
```

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

```
ntpq -p
```
The following result will be returned:

```
[root@VM_0_136_centos ~]# ntpq -p
remote refid st t when poll reach delay offset jitter
100.11.2.24 .INIT. 16 u - 64 0 0.000 0.000 0.000
193.20.113.32 194.22.113.32 . 2 u 6 64 17 277.831 3.940 5.588
*185.20.113.32 194.22.113.32 . 2 u 68 64 16 201.280 1.729 0.263
193.20.113.32 194.22.113.32 . 2 u 69 64 16 293.382 1.003 0.441
169.20.113.32 100.11.2.24 . 2 u 3 64 17 6.607 9.897 0.461
```

- ***: the NTP server in use currently.
- **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 through 16 from high to low. In order to relieve the load and network congestion, you should avoid connecting directly to a stratum 1 server.
- **when**: the number of seconds that have elapsed since the last successful request.
- **poll**: the synchronization interval (in seconds) between the local and remote servers. At the beginning, the poll value will be smaller, which indicates a higher synchronization frequency, 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 decrease accordingly.
- **reach**: an octal value used to test whether the server can be connected. Its value increases every time 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 time difference in milliseconds (ms) between the host and the time source through NTP. The closer the offset is to 0, the closer the times of the host and the NTP server are.
- **jitter**: a value used for statistics that records the distribution of offsets over a particular number of consecutive connections. The smaller its absolute value is, the more accurate the host time is.
Set the NTP service on a Windows instance

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 menu: > 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.
The clock was successfully synchronized with ntpupdate.tencentyun.com on 7/24/2019 at 4:30 PM.
Building Microsoft SharePoint 2016

Last updated: 2020-07-02 18:00:37

Overview

This document introduces how to build Microsoft SharePoint 2016 on a CVM instance.

Software Versions

This document uses the CVM instance with the following hardware specification as an example:

- vCPU: 4 cores
- Memory: 8 GB

This document uses the following software versions as an example:

- Operating system: Windows Server 2012 R2 Datacenter 64-bit (Chinese)
- Database: SQL Server 2014

Prerequisites

You have purchased a Windows CVM. If you have not yet, see Customizing Windows CVM Configurations.

Directions

**Step 1: logging in to the Windows instance**

You can either logging in to a Windows instance using the RDP file (recommended) or logging into a Windows instance via remote desktop.

**Step 2: adding AD, DHCP, DNS and IIS services**

1. On the desktop, click to open Server Manager.
2. Select Local Server in the left sidebar, and locate IE Enhanced Security Configuration, as shown below:
### Server Manager - Local Server

**PROPERTIES**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer name</td>
<td>10.53.89.165</td>
</tr>
<tr>
<td>Workgroup</td>
<td>WORKGROUP</td>
</tr>
<tr>
<td>Last installed updates</td>
<td>Never</td>
</tr>
<tr>
<td>Windows Update</td>
<td>Not configured</td>
</tr>
<tr>
<td>Last check for updates</td>
<td>Never</td>
</tr>
<tr>
<td>Windows Firewall</td>
<td>Public: Off</td>
</tr>
<tr>
<td>Remote management</td>
<td>Enabled</td>
</tr>
<tr>
<td>Remote Desktop</td>
<td>Enabled</td>
</tr>
<tr>
<td>NIC Teaming</td>
<td>Disabled</td>
</tr>
<tr>
<td>IPv4 address assigned by DHCP, IPv6 enabled</td>
<td></td>
</tr>
<tr>
<td>Time zone</td>
<td>(UTC-0800) Beijing, China</td>
</tr>
<tr>
<td>Enhanced Security Configuration</td>
<td>Off</td>
</tr>
<tr>
<td>Hardware information</td>
<td>Sandrock KVM</td>
</tr>
<tr>
<td>Operating system version</td>
<td>Microsoft Windows Server 2012 R2 Datacenter</td>
</tr>
<tr>
<td>Processors</td>
<td>AMD EPYC 7K82 48-Cores</td>
</tr>
<tr>
<td>Installed memory (RAM)</td>
<td>1 GB</td>
</tr>
<tr>
<td>Total disk space</td>
<td>49.66 GB</td>
</tr>
</tbody>
</table>

**EVENTS**

<table>
<thead>
<tr>
<th>Server Name</th>
<th>ID</th>
<th>Severity</th>
<th>Source</th>
<th>Log</th>
<th>Date and Time</th>
</tr>
</thead>
</table>

- Filter: [ ]
- [ ]
- [ ]
- [ ]
3. Disable **IE Enhanced Security Configuration**, as shown below:

4. Select **Dashboard** in the left sidebar, and click **Add roles and features**.
5. In the “Add Roles and Features Wizard” window, keep the default configurations and click **Next** 3 times.
6. On the **Server Roles** page, select **Active Directory Domain Services, DHCP Server, DNS Server, Web Server (IIS)**, and click **Add Features** in the pop-up window, as shown below:
7. Click **Next**.
8. On the **Features** page, select **.NET Framework 3.5 Features** to add features, as shown below:

![Add Roles and Features Wizard]

9. Keep the default configurations and click **Next** until the **Confirmation** page appears.

0. Confirm the installation, and click **Install**.

1. After the installation is complete, restart the CVM.

2. On the desktop, click 📲 to open *Server Manager*. 
3. Click 🔄 and select **Promote this server to a domain controller**, as shown below:

![Promote this server to a domain controller](image)

4. In the **Active Directory Domain Services Configuration Wizard** window, select **Add a new forest**, enter a domain name in the **Root domain name** field, and click **Next**.
5. Under **Type the Directory Services Restore Mode (DSRM) password**, set the password, and click **Next**.
6. Keep the default configurations and click **Next** until the configuration is complete.
7. Click **Install**.
8. On the desktop, click 📸 to open **Server Manager**.
9. Click ! and select **Complete DHCP configuration**, as shown below:

![DHCP configuration wizard](image)

0. In the **DHCP Post-Install configuration wizard** window, click **Next**.
1. Keep the default configurations and click **Commit** to complete the installation.

2. Click **Close**.

**Step 3: installing SQL Server 2014 database**

1. Open the browser on CVM and download the SQL Server 2014 installation package from the SQL Server 2014 official site.

You may also obtain the SQL Server 2014 installation package from a third-party website or other valid channels.
2. Double click the “Setup.exe” file to start the installation wizard, as shown below:

3. Select **New SQL Server stand-alone installation or add features to an existing installation**.

4. On the **Product Key** page, enter the product key and click **Next**.

5. Select **I accept the license terms**, and click **Next**.

6. Keep the default configurations, and click **Next**.

7. After the installation check is complete, click **Next**.

8. Keep the default configurations, and click **Next**.
9. On the **Feature Selection** page, click **Select All** to select all features, and click **Next**.
0. On the **Instance Configuration** page, select **Default instance**, and click **Next**.

1. On the **Server Configuration -> Service Accounts** page, configure the account and password for SQL Server Database Engine and SQL Server Analysis Services, and click **Next**.
- Set the account name of **SQL Server Database Engine** to “NT AUTHORITY\NETWORK SERVICE”.
- Set the account name and password of **SQL Server Analysis Services** to the domain name and password configured in 14 to 15 in Step 2: adding AD, DHCP, DNS, and IIS services.

2. On the **Database Engine Configuration -> Server Configuration** page, select **Add Current User** to use the current account as the administrator account of SQL Server, and click **Next**.
3. On the **Analysis Services Configuration -> Account Provisioning** page, select **Add Current User** to grant the current account with administrator permissions for Analysis Services, and click
4. Keep the default configurations, and click **Next**.

5. On the **Distributed Replay Controller** page, click **Add Current User** to grant the current account with access permissions for the Distributed Replay controller service.
6. Keep the default configurations, and click **Next**.
7. Confirm the SQL Server configurations, and click **Install**.
8. After the installation is complete, click **Close**.

**Step 4: installing SharePoint 2016**

1. Open the browser on CVM and download the Microsoft SharePoint 2016 installation package from the Microsoft SharePoint 2016 official site.
2. Open the “Microsoft SharePoint 2016” image file, double-click the executable file `prerequisiteinstaller.exe` of the preparation tool to install the Microsoft SharePoint 2016.
Preparation Tool, as shown below:
3. Open the installation wizard of the Microsoft SharePoint 2016 Preparation Tool and click **Next**.

4. Select **I accept the terms of the License Agreement(s)**, and click **Next**.
5. After the preparation tool is installed, click **Finish** to restart the CVM.

6. Open the “Microsoft SharePoint 2016” image file, double-click the installation file **setup.exe** to install Microsoft SharePoint 2016.
7. Enter the product key, and click **Continue**.

8. Select **I accept the terms of this agreement**, and click **Continue**.

9. Select the installation directory (this example keeps the default configuration but you can specify a directory as needed), and click **Install Now**.
0. When the installation is complete, select **Run the SharePoint Products Configuration Wizard now**, and click **Close**.
Step 5: configuring SharePoint 2016
1. In the **SharePoint Products Configuration Wizard** window, click **Next**.

2. Click **Yes** in the pop-up dialog box to allow service restart during the configuration.
3. Select **Create a new server farm**, and click **Next**.

4. On the **Specify Configuration Database Settings** page, set the configuration database and the access account.
   The SharePoint database is on the local host, so you need to enter the local database and account.
Then, click **Next**.

5. Enter the password of the server farm and click **Next**.
6. Select **Front-end** for “Multiple-Server Farm” and click **Next**.

7. Specify the port number of SharePoint Central Administration Web Application (this example uses “10000” but you can configure the number as needed), and click **Next**.
Configure SharePoint Central Administration Web Application

A SharePoint Central Administration Web Application allows you to manage configuration settings for a server farm. The first server added to a server farm must host this web application. To specify a port number for the web application hosted on this machine, check the box below and type a number between 1 and 65535. If you do not specify a port number, a random one will be chosen.

**Specify port number:** 10001

Configure Security Settings

Kerberos is the recommended security configuration to use with Integrated Windows authentication. Kerberos requires special configuration by the domain administrator. NTLM authentication will work with any application pool account and the default domain configuration. Show more information.

Choose an authentication provider for this Web Application:

- NTLM
- Negotiate (Kerberos)

Next >
8. Confirm the SharePoint configurations, and click **Next**.

9. After the configuration is complete, click **Finish**.
Overview

PostgreSQL is an open source relational database management system emphasizing scalability and standard compliance. PostgreSQL is ideal for enterprise-level complex online transaction processing (OLTP) systems. It supports NoSQL (JSON/XML/hstore) and Geographic Information System (GIS) data types. Featuring strong reliability and data integrity, PostgreSQL is a suitable for websites, location application systems, complex data object processing and other use cases.

This document describes how to build a PostgreSQL system on a CVM instance running CentOS 7.

Software

This document uses the following software as an example to build PostgreSQL.
Linux: Linux operating system. This document uses CentOS 7.6 as an example.
PostgreSQL: Relational database management system. This document uses PostgreSQL 11.2 as an example.

Prerequisites

- Two created CVM instances. One CVM instance works as the primary node and the other works as the secondary node.
  - For more information, see Creating Instances via CVM Purchase Page.
- The security group rules for the two CVM instances have already been configured. Open the port 5432.
  - For more information, see Adding Security Group Rules.

Directions

Configuring primary node
1. Log in to the primary CVM instance.

2. Run the following command to upgrade all packages, system versions and kernels.
   
   ```
   yum update -y
   ```

3. Run the following command to install PostgreSQL storage repository.
   
   ```
   yum install https://download.postgresql.org/pub/repos/yum/reporpms/EL-6-x86_64/pgdg-redhat-repo-latest.noarch.rpm
   ```

4. Run the following command to install client package.
   
   ```
   yum install postgresql11
   ```

5. Run the following command to install server package.
   
   ```
   yum install postgresql11-server
   ```

6. Run the following command to initialize the database.
   
   ```
   /usr/pgsql-11/bin/postgresql-11-setup initdb
   ```

7. Run the following command to start the service.
   
   ```
   systemctl start postgresql-11
   ```

8. Run the following command to enable service autostart.
   
   ```
   systemctl enable postgresql-11
   ```

9. Run the following command to switch to the `postgres` user.
   
   ```
   su - postgres
   ```

10. Run the following command to enter the PostgreSQL terminal.
    
    ```
    psql
    ```

11. Run the following command to set password for the `postgres` user.
    
    ```
    ALTER USER postgres WITH PASSWORD 'Custom password';
    ```

12. Run the following command to create a database account (such as `postuser`) and set the password, login permission and backup permission.
    
    ```
    create role account name login replication encrypted password 'Custom password';
    ```
For example, use the following command to create a database account naming `postuser` with the password `postuser`:

```sql
create role postuser login replication encrypted password 'postuser';
```

3. Run the following command to check if the account has been created.

```sql
SELECT usename from pg_user;
```

If the following result is returned, it indicates that the account has been successfully created.

```
usename
---------
postgres
postuser
(2 rows)
```

4. Run the following command to check if the permission has been set.

```sql
SELECT rolname from pg_roles;
```

If the following result is returned, it indicates that the permission has been successfully set.

```
rolname
---------
postgres
postuser
(2 rows)
```

5. Enter `\q` and press Enter to exit the PostgreSQL terminal.

6. Enter `exit` and press Enter to exit PostgreSQL.

7. Run the following command to open the `pg_hba.conf` file.

```bash
vim /var/lib/pgsql/11/data/pg_hba.conf
```

8. Press `i` to switch to edit mode. Add the following two lines to `IPv4 local connections`:

```
host all all <IPv4 IP range of the secondary node’s VPC> md5 #Enable the MD5 password encryption for connections in the IP ranges of the VPC
host replication database account <IPv4 IP range of the secondary node’s VPC> md5 ##Allow data synchronization from the `replication` database.
```

For example, if the database account is `postuser` and the IPv4 IP range of the secondary node’s VPC is `192.10.0.0/16`, add the following content to `IPv4 local connections`:

```
host all all 192.10.0.0/16 md5
host replication postuser 192.10.0.0/16 md5
```
9. Press **Esc** and enter :**wq** to save the file.

0. Run the following command to open the **postgresql.conf** file.

```
vi /var/lib/pgsql/11/data/postgresql.conf
```

1. Press **i** to enter edit mode, locate and modify the following parameters.

```
listen_addresses = 'xxx.xxx.xxx.xxx'  # The private IP addresses that are listened on.
max_connections = 100  # The maximum connections. The value of `max_connections` for the secondary node must be greater than that for the primary node.
wal_level = 'hot_standby'  # Enable hot standby mode.
synchronous_commit = 'on'  # Enable synchronous replication.
max_wal_senders = 32  # The maximum number of synchronization processes.
wal_sender_timeout = 60  # The timeout value for the streaming replication instance to send data.
```

2. Press **Esc** and enter :**wq** to save and close the file.

3. Run the following command to restart the service.

```
systemctl restart postgresql-11
```

**Configuring secondary node**

1. Log in to the secondary CVM instance.

2. Run the following command to upgrade all packages, system versions and kernels.

```
yum update -y
```

3. Run the following command to install PostgreSQL storage repository.

```
yum install https://download.postgresql.org/pub/repos/yum/reporpms/EL-6-x86_64/pgdg-redhat-repo-latest.noarch.rpm
```

4. Run the following command to install client package.

```
yum install postgresql11
```

5. Run the following command to install server package.

```
yum install postgresql11-server
```

6. Run the following command and use the `pg_basebackup` utility to create a backup directory:

```
pg_basebackup -D /var/lib/pgsql/11/data -h Private IP of primary node -p 5432 -U Database account -X stream -P
```
For example, if the private IP of the primary node is 192.10.123.321, and the database account is `postuser`, run the following command:

```
```

Enter the password as prompted, and press **Enter**. If the following is returned, it indicates that the backup directory has been successfully created.

```
Password: 24526/24526 kB (100%), 1/1 tablespace
```

7. Run the following command to copy configuration files of the primary node.

```
cp /usr/pgsql-11/share/recovery.conf.sample /var/lib/pgsql/11/data/recovery.conf
```

8. Run the following command to open the `recovery.conf` file.

```
vim /var/lib/pgsql/11/data/recovery.conf
```

9. Press **i** to switch to edit mode, locate and modify the following parameters:

```
standby_mode = on #Declare the secondary node
primary_conninfo = 'host=<Private IP of the primary node> port=5432 user=Database account password=Database password' #Connection information of the primary node
recovery_target_timeline = 'latest' #Synchronize the latest data by using streaming replication
```

0. Press **Esc** and enter **:wq** to save the file.

1. Run the following command to open the `postgresql.conf` file.

```
vim /var/lib/pgsql/11/data/postgresql.conf
```

2. Press **i** to switch to edit mode, locate and modify the following parameters:

```
listen_addresses = 'xxx.xx.xx.xx' #The private IP addresses that are listened on.
max_connections = 1000 #The maximum connections. The value of `max_connections` for the secondary node must be greater than that for the primary node
hot_standby = on #Enable hot standby mode
max_standby_streaming_delay = 30s #The maximum delay for streaming replication
wal_receiver_status_interval = 1s #The maximum interval for the secondary node to report its status to the primary node
hot_standby_feedback = on #Enable the secondary node to report errors during replication.
```

3. Press **Esc** and enter **:wq** to save the file.

4. Run the following command to modify the group and owner of data directory:

```
chown -R postgres.postgres /var/lib/pgsql/11/data
```
5. Run the following command to start service.

```
systemctl start postgresql-11
```

6. Run the following command to enable service autostart.

```
systemctl enable postgresql-11
```

**Verifying deployment**

Perform the following to verify the deployment.

1. Run the following command to check the `sender` process on the primary node:

```
ps aux | grep receiver
```

If the following is returned, it indicates that the `sender` process is available.

```
[root@VM-0-107-centos ~]# ps aux | grep receiver
root  25800  0.0  0.0 112812  968 pts/0  S+   18:08  0:00 grep --color=auto receiver
```

2. Run the following command to check the `receiver` process on the secondary node:

```
ps aux | grep receiver
```

If the following is returned, it indicates that the `receiver` process is available.

```
[root@VM-0-99-centos ~]# ps aux | grep receiver
postgres 26947  0.0  0.3 428180 3640  7 Ss  18:05 0:00 postgres: walreceiver streaming 0/3000140
root  27832  0.0  0.0 112812  968 pts/0  A+   18:10  0:00 grep --color=auto receiver
```

3. On the primary node, run the following commands in sequence to check the secondary node status in the PostgreSQL terminal.

```
su - postgres
```

```
psql
```

```
select * from pg_stat_replication;
```
If the following is returned, it indicates that the secondary node status is available.

4. Verify that the secondary node synchronizes data with the primary node.
   i. On the primary node, run the following command to enter PostgreSQL terminal and create a database (such as `testdb`).

```
su - postgres

psql

create database testdb;
```

ii. On the secondary node, run the following commands in sequence to enter PostgreSQL terminal and check whether the secondary node is synchronized.

```
su - postgres

psql

"l",
```

If the following is returned, it indicates that the secondary node has been successfully synchronized.
Building the Docker

Overview

This document describes how to build and use Docker on a Tencent Cloud CVM instance, and is designed for new CVM developers who are familiar with the Linux operating system.

Software

This document uses the following software to build the Docker environment:

- Operating system: Linux operating system. This document uses CentOS 7.6 as an example.

**Note:**

Docker must be built on a 64-bit operating system with the kernel version 3.10 or later.

Prerequisites

A Linux CVM is required to set up a Docker environment. If you have not purchased a Linux CVM yet, see [Customizing Linux CVM Configurations](#).

**Note:**

Docker must be built on a 64-bit operating system with the kernel version 3.10 or later.

Directions

**Installing Docker**

1. See [Log into Linux Instance Using Standard Login Method](#). You can also use other login methods that you are more comfortable with:
   - [Log into Linux Instances via Remote Login Tools](#)
   - [Logging into Linux Instance via SSH Key](#)
2. Run the following commands in sequence to add the yum repository.

   ```
   yum update
   yum install epel-release -y
   yum clean all
   yum list
   ```

3. Run the following command to install Docker.

   ```
   yum install docker-io -y
   ```

4. Run the following command to run Docker.

   ```
   systemctl start docker
   ```

5. Run the following command to check the installation result.

   ```
   docker info
   ```

   If you see the following prompt, it indicates that Docker has been successfully installed.

   ![Docker info output]

   **Using Docker**

   You can use Docker with the following commands:

   - Manage the Docker daemon.
     - Run the Docker daemon.

   ```
   systemctl start docker
   ```
- Stop the Docker daemon.
  ```bash
  systemctl stop docker
  ```

- Restart the Docker daemon.
  ```bash
  systemctl restart docker
  ```

- Manage images. This document uses the Nginx image of Docker Hub as an example.
  ```bash
  docker pull nginx
  ```

- Modify image tag to help you identify the image.
  ```bash
  docker tag docker.io/nginx:latest tencentyun/nginx:v1
  ```

- Query existing images.
  ```bash
  docker images
  ```

- Forcibly delete an image.
  ```bash
  docker rmi -f tencentyun/nginx:v1
  ```

- Manage containers.
  
  - Enter a container.
    ```bash
    docker run -it ImageId /bin/bash
    ```
  
  - Run the `docker images` command to obtain the ImageId value.
  
  - Exit the container. Run the `exit` command to exit the container.
  
  - Enter a container running in the background.
    ```bash
    docker exec -it container ID /bin/bash
    ```
  
  - Create an image from the container.
    ```bash
    docker commit <container ID or container name> [repository name][:tag]
    ```

    For example:
    ```bash
    docker commit 1c23456cd7**** tencentyun/nginx:v2
    ```

### Creating images

1. Run the following command to open the “Dockerfile” file.
vim Dockerfile

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

```
FROM tencentyun/nginx:v2  #Declare a basic image.
MAINTAINER DTSTACK  #Declare the image owner.
RUN mkdir /dtstact  #Add the command that needs to be run before the container starts after the
  RUN command. Since Dockerfile files can only contain a maximum of 127 lines, we recommend that
  you write and run the commands in the script.
ENTRYPOINT ping https://cloud.tencent.com/  #The commands that run at startup. The last command
  must be a frontend command that runs constantly. Otherwise, the container will exit after runn
  ing all commands.
```

3. Press Esc and enter :wq to save the file.

4. Run the following command to build an image.

```
docker build -t nginxos:v1  #The single dot (.) specifies the path of the Dockerfile and must
  be included.
```

5. Run the following command to check if the image has been created.

```
docker images
```

6. Run the following commands in sequence to run and check the container.

```
docker run -d nginxos:v1  #Run the container in the background.
docker ps #Check the running container.
docker ps -a #Check all containers including those that are not running.
docker logs CONTAINER ID/IMAGE  #Check the startup log to troubleshoot the issue based on the c
  ontainer ID or name if you do not see the container in the returned results
```

7. Run the following commands in sequence to create an image.

```
docker commit fb2844b6**** nginxweb:v2  #Add the container ID and the name and version of the n
  ew image. after the commit command.
docker images  #List local images that have been downloaded and created.
```

8. Run the following command to push the image to the remote repository.

The image is pushed to Docker Hub by default. To push the image, log in to Docker, tag and name
the image in the following format: Docker username/image name: tag .

```
docker login  #Enter the username and password of the image registry after running the command
docker tag [image name]:[tag] [username]:[tag]
docker push [username]:[tag]
```

After the image is pushed, you can log in to Docker Hub to view the image.
Building GitLab

Last updated: 2020-08-27 15:42:55

Overview

GitLab is a Ruby-based open-source version management system. It provides the code management tool Git and the self-hosted Git repository to support your Web access to public and private projects. This document describes how to install and use GitLab on Tencent Cloud CVM.

Software

The CVM instance needs to be configured with:

- vCPU: 2 cores
- Memory: 4 GB
- Linux operating system: this document uses CentOS 7.7 as an example

Prerequisites

- A Linux CVM is required to install GitLab. If you have not purchased a Linux CVM yet, see Customizing Linux CVM Configurations.
- The security group rules for the Linux instance have already been configured. Open the port 80. For more information, see Adding Security Group Rules.

Directions

Installing GitLab

1. See Log in to Linux Instances Using the Standard Login Method. You can also use other login methods that you are more comfortable with:
   - Log in to Linux Instances via Remote Login Tools
   - Log in to Linux Instances via a SSH Key
2. Run the following command to install dependencies.

```bash
yum install -y curl policycoreutils-python openssh-server
```
3. Run the following commands in sequence to enable SSH service autostart and start the SSH service.

```bash
systemctl enable sshd
systemctl start sshd
```

4. Run the following command to install Postfix.

```bash
yum install -y postfix
```

5. Run the following command to enable Postfix service autostart.

```bash
systemctl enable postfix
```

6. Run the following command to open Postfix’s configuration file main.cf.

```bash
vim /etc/postfix/main.cf
```

7. Press `i` to enter the editing mode. Delete `#` before `inet_interfaces = all`, and add `#` before `inet_interfaces = localhost`, as shown below:

```ini
inet_interfaces = all
#inet_interfaces = $myhostname
#inet_interfaces = $myhostname, localhost
#inet_interfaces = localhost
```

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

9. Run the following command to start Postfix.

```bash
systemctl start postfix
```

10. Run the following command to add the GitLab software repository.

```bash
curl https://packages.gitlab.com/install/repositories/gitlab/gitlab-ce/script.rpm.sh | sudo bash
```

11. Run the following command to install GitLab.

```bash
sudo EXTERNAL_URL="Public IP address of the instance" yum install -y gitlab-ce
```

For more information about how to obtain the public IP of the instance, see Getting Public IP Addresses.

12. In a local browser, visit the public IP address that you have obtained. If the following page appears, GitLab has been installed successfully.
Creating projects

1. In a local browser, visit the public IP address of your CVM to access the GitLab login page. Enter your root account and the configured password, as shown below:

---

**Note:**

Configure the password for your GitLab account here.
2. Create a private project as instructed. This document uses `test` as an example in the following figure:
3. After the project is created, click **Add SSH Key** at the top of the page.

4. On the **SSH Keys** page, add a SSH key by performing the following steps:
   i. **Get the key** for the PC to be managed by the project and paste it in the **Key** field.
   ii. Enter the key name in the **Title** field.
iii. Click **Add key** as shown below:

If the result is similar to the following figure, the key has been added successfully:
5. On the project homepage, click **clone** to record the project address, as shown below:

![Cloning projects](image)

**Cloning projects**

1. Run the following command on the managed PC to configure the username of the Git repository.
   
   ```
   git config --global user.name "username"
   ```

2. Run the following command to configure the email for the username.
   
   ```
   git config --global user.email "xxx@example.com"
   ```

3. Run the following command to clone the project. Replace the project address with the actual values obtained in Step 5.
   
   ```
   git clone "Project address"
   ```

   After the project is successfully cloned, the same directory and all project files will be generated on your local computer.

**Uploading files**

1. Run the following command to access the project directory.
   
   ```
   cd test/
   ```

2. Run the following command to create the target file to be uploaded to GitLab. This document uses the test.sh file as an example.
   
   ```
   echo "test" > test.sh
   ```
3. Run the following command to add the test.sh file to the index.

```
  git add test.sh
```

4. Run the following command to submit the test.sh to the local repository.

```
  git commit -m "test.sh"
```

5. Run the following command to synchronize the test.sh file with the GitLab server.

```
  git push -u origin master
```

Go back to the test project page. You can now see the file on the page, as shown below:

![Test project page](image)

**Relevant Operations**

">

**Getting the key**

1. On the PC to be managed by the project, run the following command to install Git.

```
  yum install -y git
```
2. Run the following command to generate the key file ".ssh/id_rsa". During the key file generation process, press Enter to keep the default configurations.

```
ssh-keygen
```

3. Run the following command to view and record the key information.

```
cat .ssh/id_rsa.pub
```
Building RabbitMQ

Overview

RabbitMQ is an open-source message broker based on the Advanced Message Queuing Protocol (AMQP). It features usability, scalability, and high availability with an Erlang-programmed server, and supports multiple clients including Python, Ruby, .NET, Java, JMS, C, PHP, ActionScript, XMPP, STOMP, and AJAX. This document describes how to deploy RabbitMQ on Tencent Cloud CVM.

Software

This document uses the following software as an example to deploy RabbitMQ:

- Linux: Linux operating system. This document uses CentOS 7.7 as an example.
- RabbitMQ Server: open-source message broker. This document uses RabbitMQ Server 3.6.9 as an example.
- Erlang: programming language. This document uses Erlang 19.3 as an example.

Prerequisites

- A Linux CVM is required to deploy RabbitMQ. If you have not purchased a Linux CVM yet, see Customizing Linux CVM Configurations.
- The security group rules for the Linux instance have already been configured. Open the ports 80, 5672 and 15672. For more information, see Adding Security Group Rules.

Directions

Installing Erlang

1. See Log in to Linux Instances Using the Standard Login Method. You can also use other login methods that you are more comfortable with:
   - Log in to Linux Instances via Remote Login Tools
   - Log in to Linux Instances via a SSH Key
2. Run the following command to install dependencies.
yum -y install make gcc gcc-c++ m4 ncurses-devel openssl-devel unixODBC-devel

3. Run the following command to download the Erlang installation package.

   ```bash
   wget http://erlang.org/download/otp_src_19.3.tar.gz
   ```

4. Run the following command to decompress the Erlang installation package.

   ```bash
   tar xzf otp_src_19.3.tar.gz
   ```

5. Run the following command to create the erlang folder.

   ```bash
   mkdir /usr/local/erlang
   ```

6. Run the following commands in sequence to compile and install Erlang.

   ```bash
   cd otp_src_19.3
   ./configure --prefix=/usr/local/erlang --without-javac
   make && make install
   ```

7. Run the following command to open the profile configuration file.

   ```bash
   vi /etc/profile
   ```

8. Press `i` to enter the editing mode, and append the following at the end of the file.

   ```bash
   export PATH=$PATH:/usr/local/erlang/bin
   ```

9. Press `Esc` and enter `:wq` to save and close the file.

**Installing RabbitMQ Server**

1. Run the following command to download the RabbitMQ Server installation package.

   ```bash
   wget -P /root "https://www.rabbitmq.com/releases/rabbitmq-server/v3.6.9/rabbitmq-server-3.6.9-1.el7.noarch.rpm"
   ```

2. Run the following command to import the signature key.

   ```bash
   rpm --import https://www.rabbitmq.com/rabbitmq-release-signing-key.asc
   ```

3. Run the following commands in sequence to install RabbitMQ Server.

   ```bash
   cd
   ```
yum install rabbitmq-server-3.6.9-1.el7.noarch.rpm

4. Run the following commands in sequence to enable RabbitMQ autostart and start RabbitMQ.

   systemctl enable rabbitmq-server

   systemctl start rabbitmq-server

5. Run the following command to delete the default guest account of RabbitMQ.

   rabbitmqctl delete_user guest

6. Run the following command to create an account.

   rabbitmqctl add_user Username Password

7. Run the following command to set the new account as the admin account.

   rabbitmqctl set_user_tags Username administrator

8. Run the following command to grant the admin account all permissions.

   rabbitmqctl set_permissions -p / Username ".*" ".*" ".*"

Verifying installation

1. Run the following command to open the Web management page of RabbitMQ.

   rabbitmq-plugins enable rabbitmq_management

2. Open a browser and visit:

   http://Instance public IP:15672

For more information about how to obtain the public IP address of the instance, see Getting Public IP Addresses.
If you see the following page, it indicates that RabbitMQ has been successfully installed.

3. Log in to RabbitMQ with the admin account created in Step 6 and access the RabbitMQ management page, as shown below:
Network Performance Test

Last updated: 2020-09-10 17:41:51

Overview

This document describes how to test the CVM network performance with tools, which helps you stay on top of the CVM network performance based on the test result.

Network Performance Test Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bandwidth (Mbits/sec)</strong></td>
<td>Maximum amount of data (bits) transferred per unit time (1s)</td>
</tr>
<tr>
<td><strong>TCP-RR (times/sec)</strong></td>
<td>Response efficiency when multiple request/response communications are made during one TCP persistent connection. TCP-RR is widely used in database access links</td>
</tr>
<tr>
<td><strong>UDP-STREAM (packets/sec)</strong></td>
<td>Data throughput of UDP during batch data transfer, which reflects the maximum forwarding capacity of an ENI</td>
</tr>
<tr>
<td><strong>TCP-STREAM (Mbits/sec)</strong></td>
<td>TCP-based data throughput during batch data transfer</td>
</tr>
</tbody>
</table>

Tool Information

<table>
<thead>
<tr>
<th>Metric</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>iperf</td>
</tr>
<tr>
<td>PPS viewing</td>
<td>sar</td>
</tr>
<tr>
<td>ENI queue viewing</td>
<td>ethtool</td>
</tr>
</tbody>
</table>
Directions

Constructing a Test Environment

Preparing a test server

- Image: CentOS 7.4 64-bit
- Specifications: S3.2XLARGE16
- Quantity: 1

Assume that the IP address of the test server is 10.0.0.1.

Preparing companion training servers

- Image: CentOS 7.4 64-bit
- Specifications: S3.2XLARGE16
- Quantity: 8

Assume that the IP addresses of companion training servers are 10.0.0.2 to 10.0.0.9.

Deploying test tools

1. Run the following command to install the compiling environment and the system status detection tool:

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

2. Run the following command to download the netperf compression package:

   You can also download the latest version of netperf from GitHub: Netperf.

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

3. Run the following command to decompress the netperf compression package:

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

4. Run the following command to compile and install netperf:
5. Run the following commands to verify whether the installation was successful:

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

If “Help” appears, the installation was successful.

6. Run the following commands based on the OS type to install iperf:

For CentOS:
```
yum install iperf  #For CentOS. Ensure that you have root permissions.
```

For Ubuntu or Debian:
```
apt-get install iperf  #For Ubuntu or Debian. Ensure that you have root permissions.
```

7. Run the following command to verify whether the installation was successful:

```
iperf -h
```

If “Help” appears, the installation was successful.

**Bandwidth Test**

We recommend that you use two CVMs with the same configuration for testing to prevent deviations in the performance test results. One CVM is used as the test server while the other CVM is used as the companion training server. In this example, 10.0.0.1 and 10.0.0.2 are specified for testing.

**Test server**

Run the following command:

```
iperf -s
```

**Companion training server**

Run the following command:

```
iperf -c ${<Server IP address>} -b 2048M -t 300 -P ${<Number of ENI queues>}
```

For example, if the IP address of the companion training server is 10.0.0.1 and the number of ENI queues is 8, run the following command:

```
iperf -c 10.0.0.1 -b 2048M -t 300 -P 8
```

**UDP-STREAM Test**
We recommend that you use one test server and eight companion training servers for testing. 10.0.0.1 is the test server, and 10.0.0.2 to 10.0.0.9 are the companion training servers.

**Test server**

Run the following commands to view the network pps value:

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

**Companion training servers**

Run the following command:

```
./netperf -H <Private IP address of the test server> -l 300 -t UDP_STREAM -- -m 1 &
```

On the companion training servers, launch a few netperf instances. Based on experience, launching one instance should be sufficient. If the system performance is unstable, add more netperf instances to reach the UDP_STREAM limit.

For example, if the private IP address of the test server is 10.0.0.1, run the following command:

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

**TCP-RR Test**

We recommend that you use one test server and eight companion training servers for testing. 10.0.0.1 is the test server, and 10.0.0.2 to 10.0.0.9 are the companion training servers.

**Test server**

Run the following commands to view the network pps value:

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

**Companion training servers**

Run the following command:

```
./netperf -H <Private IP address of the test server> -l 300 -t TCP_RR -- -r 1,1 &
```

On the companion training servers, launch multiple netperf instances. Based on experience, at least 300 netperf instances should be launched to reach the TCP-RR limit.

For example, if the private IP address of the test server is 10.0.0.1, run the following command:
Test Data Analysis

Performance analysis of the sar tool

Sample analysis data

<table>
<thead>
<tr>
<th>Time</th>
<th>Interface</th>
<th>rxpck/s</th>
<th>txpck/s</th>
<th>rxkB/s</th>
<th>txkB/s</th>
<th>rxcmp/s</th>
<th>txcmp/s</th>
<th>rxmcst/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>02:41:03 PM</td>
<td>IFACE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:41:04 PM</td>
<td>eth0</td>
<td>1626689.00</td>
<td>8.00</td>
<td>68308.62</td>
<td>1.65</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>02:41:04 PM</td>
<td>lo</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>02:41:04 PM</td>
<td>IFACE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:41:05 PM</td>
<td>eth0</td>
<td>1599900.00</td>
<td>1.00</td>
<td>67183.30</td>
<td>0.10</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>02:41:05 PM</td>
<td>lo</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>02:41:05 PM</td>
<td>IFACE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:41:06 PM</td>
<td>eth0</td>
<td>1646689.00</td>
<td>1.00</td>
<td>69148.10</td>
<td>0.40</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>02:41:06 PM</td>
<td>lo</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>02:41:06 PM</td>
<td>IFACE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:41:07 PM</td>
<td>eth0</td>
<td>1605957.00</td>
<td>1.00</td>
<td>67437.67</td>
<td>0.40</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>02:41:07 PM</td>
<td>lo</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Field descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rxpck/s</td>
<td>Number of packets received per second; that is, the receiving pps</td>
</tr>
<tr>
<td>txpck/s</td>
<td>Number of packets sent per second; that is, the sending pps</td>
</tr>
<tr>
<td>rxkB/s</td>
<td>Receiving bandwidth</td>
</tr>
<tr>
<td>txkB/s</td>
<td>Sending bandwidth</td>
</tr>
</tbody>
</table>

Performance analysis of the iperf tool

Sample analysis data

```
[ ID] Interval Transfer Bandwidth
[ 5] 0.00-300.03 sec 0.00 Bytes 0.00 bits/sec sender
[ 5] 0.00-300.03 sec 6.88 GBytes 197 Mbits/sec receiver
```
Field descriptions

In SUM lines, sender represents the data volume sent and receiver represents the data volume received.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>Test duration</td>
</tr>
<tr>
<td>Transfer</td>
<td>Data transfer volume, including the sent and received data volumes</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Bandwidth, including the sending and receiving bandwidths</td>
</tr>
</tbody>
</table>

Relevant Operations

Script for Launching Multiple Netperf Instances

In TCP-RR and UDP-STREAM, multiple netperf instances need to be launched. The number of instances that need to be launched depends on the server configuration. 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 duration after -l. Set the duration to 10000 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
Recovering Data on Linux CVMs

Last updated: 2020-09-14 14:24:11

Overview

Extundelete is an open-source data recovery tool. With powerful features, it supports the ext3 and ext4 partition recovery of data disk files that are deleted accidentally, provided the disk is not written after the accident. This document describes how to use Extundelete to quickly recover the accidentally deleted data on a CentOS 7.7 Tencent Cloud CVM. Tencent Cloud also offers snapshots, custom images and Cloud Object Storage to store data. We recommend that you regularly back up data to enhance data security.

Software

- Linux: Linux operating system. This document uses CentOS 7.7 as an example.
- Extundelete: open-source data recovery tool. This document uses Extundelete 0.2.4 as an example.

Directions

⚠️ **Note:**
Refer to Creating Snapshots and Creating Custom Images to back up data before performing operations so that you can recover the instance to its initial status if a problem occurs.

**Installing Extundelete**

1. Run the following command to install the Extundelete dependencies and libraries.

⚠️ **Note:**
- Extundelete requires the libext2fs version 1.39 or later.
- To support the ext4 format, install the e1fsprogs version 1.41 or later. You may use the `dumpe2fs` command to view the version.
yum -y install bzip2 e2fsprogs-devel e2fsprogs gcc-c++ make

2. Download the Extundelete installation package.
3. Run the following commands in sequence to decompress the Extundelete installation package and access its directory.

    tar -xvjf extundelete-0.2.4.tar.bz2

    cd extundelete-0.2.4

4. Run the following commands in sequence to compile and install Extundelete.

    ./configure

    make && make install

After the installation is completed, you will be able to see the executable file “extundelete” in the /usr/local/bin directory.

**Testing the data recovery**

Recover data as needed by performing the following steps.

1. Initialize and partition the data disk by referring to Initializing Cloud Disks (Smaller than 2TB). Run the following command to view the existing disks and the available partitions.

    fdisk -l
The following information will appear:

2. Run the following commands in sequence to create a mount point and mount the partition. This document uses mounting the `/dev/vdb1` partition to `/test` as an example.

```
mkdir /test

mount /dev/vdb1 /test
```

3. Run the following commands in sequence to create the “hello” test file at the mount point.

```
cd /test

echo test > hello
```

4. Run the following command to record the MD5 value of the “hello” file. This value can be used to compare the original and recovered files.

```
md5sum hello
```

The following information will appear:

```
[root@VM-0-23-centos test]# md5sum hello
d8e8fca2d0675c2cb4cb0031ba249 hello
```

5. Run the following commands in sequence to delete the “hello” file.
6. Run the following command to unmount the partition.

   ```bash
   umount /dev/vdb1
   ```

7. Run the following command to search the partition for accidentally deleted files.

   ```bash
   extundelete --inode 2 /dev/vdb1
   ```

   The following information will appear:

   ```
   Direct blocks: 127754, 4, 0, 0, 1, 9251, 0, 0, 0, 0, 0, 0
   Indirect block: 0
   Double indirect block: 0
   Triple indirect block: 0
   
   File name          | Inode number | Deleted status
   --------------------+--------------+----------------
   .                   | 2            |               
   ..                  | 2            |               
   lost+found          | 11           |               
   WTEST.TMP           | 12           | Deleted       
   ```

8. Run the following command to use Extundelete to recover the file.

   ```bash
   /usr/local/bin/extundelete --restore-inode 12 /dev/vdb1
   ```

   After the file is recovered, you will see the `RECOVERED_FILES` folder in the same-level directory.

9. Access the `RECOVERED_FILES` folder, check the recovered file, and run the following command to obtain its MD5 value.

   ```bash
   md5sum Recovered file
   ```

   If the obtained MD5 value is the same as that of the “hello” file recorded in Step 4, the data has been recovered successfully.
Building a Visual Ubuntu Desktop

Overview

Virtual Network Console (VNC) is a remote control tool software developed by AT&T European Research Laboratory. An open-source software based on UNIX and Linux operating systems, VNC features robust remote control capability, high efficiency, and strong practicability. Its performance is comparable to any remote control software in Windows or Mac. This document will guide you through on how to build a visual Ubuntu desktop by using VNC.

Sample Software Versions

The following software is used to build a visual Ubuntu desktop.
Linux: Linux OS. This document uses Ubuntu Server 16.04.1 LTS 64-bit as an example.

Prerequisites

You have purchased a Linux CVM with the Ubuntu OS. If not, see Customizing Linux CVM Configurations.

Directions

1. Log in to a Linux instance using VNC.
2. Run the following command to switch to the “root” account.
   
   ```bash
   sudo su root
   ```
3. Run the following command to obtain and update to the latest version.
   
   ```bash
   apt-get update
   ```
4. Run the following command to install VNC.
   
   ```bash
   apt-get install vnc4server
   ```
5. Run the following command to launch VNC and set a password.
vncserver

If the result similar to the following is returned, it indicates that VNC has been launched successfully.

```bash
root@VM-0-133-ubuntu:/home/ubuntu# vncserver
You will require a password to access your desktop.
Password:
Verify:
xauth: file /root/.Xauthority does not exist
New 'VM-0-133-ubuntu:1 (root)' desktop is VM-0-133-ubuntu:1
Creating default startup script /root/.vnc/xstartup
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/VM-0-133-ubuntu:1.log
```

6. Run the following command to install the X-windows base package.

```bash
sudo apt-get install x-window-system-core
```

7. Run the following command to install the login manager.

```bash
sudo apt-get install gdm
```

8. Run the following command to install Ubuntu desktop.

```bash
sudo apt-get install ubuntu-desktop
```

During the installation, choose “gdm3” for Default display manager:

9. Run the following command to install the GNOME supporting software.

```bash
sudo apt-get install gnome-panel gnome-settings-daemon metacity nautilus gnome-terminal
```

10. Run the following command to access the VNC configuration file.

```bash
vi ~/.vnc/xstartup
```

1. Press i to enter edit mode, and modify the configuration file as follows.

```bash
#!/bin/sh
# Uncomment the following two lines for normal desktop:
export XKL_XMODMAP_DISABLE=1
unset SESSION_MANAGER
# exec /etc/X11/xinit/xinitrc
unset DBUS_SESSION_BUS_ADDRESS
gnome-panel &
gnome-settings-daemon &
```
2. Press **Esc** and enter **:wq**. Save and close the file.

3. Run the following commands to restart the desktop process.

```
metacity &
nautilus &
gnome-terminal &
```

4. Click [here](#) to download and install VNC Viewer. Select the version that matches your operating system.

5. Type **CVM IP address**: 1 into VNC Viewer, and press **Enter**.

6. Click **Continue** in the pop-out dialog box.

7. Enter the VNC password set in **Step 5** and click **OK**.
Changing Kernel of a Linux Instance Manually

Last updated : 2020-09-04 11:50:10

Overview

Bottleneck Bandwidth and Round-trip propagation time (BBR) is a TCP congestion control algorithm developed by Google in 2016. It helps significantly improve the throughput and the TCP connection latency of Linux servers. However, enabling BBR requires a Linux kernel version of 4.10 or later. If you use an earlier version, you need to upgrade your kernel. This document guides you through how to manually change the kernel and enable BBR on your Linux server.

Directions

**Updating the kernel package**

1. Run the following command to check the current kernel version.

   ```
   uname -r
   ```

2. Run the following command to update the software package.

   ```
   yum update -y
   ```

3. Run the following command to import the public key of ELRepo.

   ```
   rpm --import https://www.elrepo.org/RPM-GPG-KEY-elrepo.org
   ```

4. Run the following command to install the yum repository of ELRepo.

   ```
   yum install https://www.elrepo.org/elrepo-release-7.0-4.el7.elrepo.noarch.rpm
   ```

**Installing a new kernel**

1. Run the following command to check the supported kernel package in the ELRepo repository.

   ```
   yum --disablerepo="*" --enablerepo="elrepo-kernel" list available
   ```

2. Run the following command to install the latest mainline stable kernel.
yum --enablerepo=elrepo-kernel install kernel-ml

Modifying the grub configuration

1. Run the following command to open the `/etc/default/grub` file.

   ```
   vim /etc/default/grub
   ```

2. Press `i` to switch to the edit mode and change `GRUB_DEFAULT=saved` to `GRUB_DEFAULT=0`.

   
   ```
   GRUB_DEFAULT=0
   ```

3. Press `Esc` and enter `:wq` to save and close the file.

4. Run the following command to generate the kernel configuration again.

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

5. Run the following command to restart the server.

   ```
   reboot
   ```

6. Run the following command to check whether the modification is successful.

   ```
   uname -r
   ```

Deleting unnecessary kernels

1. Run the following command to view all kernels.

   ```
   rpm -qa | grep kernel
   ```

2. Run the following command to delete the older kernel.

   ```
   yum remove kernel-old_kernel_version
   ```

   For example:

   ```
   yum remove kernel-3.10.0-957.el7.x86_64
   ```

Enabling BBR
1. Run the following command to edit the `/etc/sysctl.conf` file.

   ```
   vim /etc/sysctl.conf
   ```

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

   ```
   net.core.default_qdisc=fq
   net.ipv4.tcp_congestion_control=bbr
   ```

3. Press `Esc` and enter `:wq` to save and close the file.

4. Run the following command to load the kernel parameter settings to the `/etc/sysctl.conf` configuration file.

   ```
   sysctl -p
   ```

5. Run the following commands to verify whether BBR has been successfully enabled.

   ```
   sysctl net.ipv4.tcp_congestion_control
   # The following appears if the configuration succeeds:
   # net.ipv4.tcp_congestion_control = bbr
   
   sysctl net.ipv4.tcp_available_congestion_control
   # The following appears if the configuration succeeds:
   # net.ipv4.tcp_available_congestion_control = reno cubic bbr
   ```

6. Run the following command to check whether the kernel module is loaded.

   ```
   lsmod | grep bbr
   ```

   If the following information is returned, BBR has been successfully enabled.

   ```
   [root@VM_0_51_centos ~]# lsmod | grep bbr
   tcp_bbr          20480  1
   ```
Managing Disk Space on Windows CVMs

Last updated : 2020-09-14 14:24:12

Overview

This document describes how to release disk space on a Windows Server 2012 R2-based Tencent Cloud CVM when the disk space is insufficient. It also describes how to perform routine disk maintenance.

Directions

Releasing disk space

You can delete large files or obsolete files to free up disk space. If the disk space is still insufficient after deleting large and obsolete files, you can expand the disk space. To do this, please see Cloud Disk Expansion Scenarios.

Deleting large files

1. Log in to a Windows instance using either the RDP file (recommended) or the remote desktop.
2. Click in the bottom toolbar and open the “This PC” window.
3. Select the disk in which you want to free up space, and press Ctrl + F to open the search tool.
4. Select Search -> Size and filter files by the system-defined size options, as shown below:
Deleting obsolete files

1. On the desktop, click to open Server Manager.
2. Click Add Roles and Features under Manage.
3. In the pop-up window, click Next.
4. Select Role-based or feature-based installation and click Next twice, as shown below:

5. On the Select features page, check Ink and Handwriting Services and Desktop Experience, as shown below. Click OK in the pop-up dialog box.

Note:
You can also enter a size in the search box in the upper-right corner of the This PC window. For example:
- Enter “Size: > 500 MB” to search the disk for files larger than 500 MB.
- Enter “Size: > 100 MB < 500 MB” to search the disk for files larger than 100 MB but less than 500 MB.
6. Click **Next** and then **Install**. Wait for the installation to complete, and restart CVM when prompted.
7. Select **Desktop Experience** and click in the top-right corner. Enter **Disk Management** and search.
8. In the pop-up **Disk Cleanup** window, select the target disk and start the cleanup, as shown below:

![Disk Cleanup Window](image)

**Routine disk maintenance**

**Removing programs regularly**

Select **Control Panel -> Programs and Features -> Uninstall or change a program** to regularly remove obsolete programs, as shown below:

![Programs and Features](image)

**Viewing disk usage on the console**

The Cloud Monitor feature is automatically enabled once a CVM instance is created. You can view the disk usage by following the steps below:

1. Log in to the **CVM console** and access the **Instances** page.
2. Select the ID/Name of the target instance to access the details page.
3. Select the **Monitoring** tab to view the instance disk usage, as shown below:
Using RemoteFx to Redirect USB Devices in Windows

Scenario

RemoteFx is an upgraded version of Windows Remote Desktop Protocol (RDP). From RDP 8.0, RemoteFx can be used to redirect local USB devices to a remote desktop through the RDP data channel, ensuring that the CVM can use these USB devices.

This document uses the following environment versions as examples to describe how to enable the RemoteFx USB redirection feature of RDP to redirect USB devices to a CVM.

- Client: Windows 10
- Server: Windows Server 2016

Use Limits

Because RDP 8.0 and later versions support the RemoteFx USB redirection feature, Windows 8, Windows 10, Windows Server 2016, and Windows Server 2019 all support this feature. If the operating system of your local PC has one of these versions, you do not need to install the RDP 8.0 update patch. If your local PC has Windows 7 or Windows Vista, please go to Microsoft official website to get and install the RDP 8.0 update patch.

Directions

**Configuring the server**

1. Logging in to a Windows instance using the RDP file (recommended).
2. On the desktop, click and select **Server Manager** to open Server Manager.
3. In the “Server Manager” window, click **Add roles and features**, as shown in the following figure:

![Server Manager window](image)

4. In the pop-up "Add Roles and Features Wizard" window, click **Next** to go to the "Select installation type" page.
5. On the "Select installation type" page, select **Role-based or feature-based installation** and click **Next**.
6. On the "Select destination server" page, keep the default configurations and click **Next**.
7. On the "Select server roles" page, select **Remote Desktop Services** and click **Next**, as shown in the following figure:
8. Keep the default configurations and click **Next** for 2 times.

9. On the "Select role services" page, select **Remote Desktop Session Host**, **Remote Desktop Connection Broker**, and **Remote Desktop Licensing**. In the pop-up window, click **Add**.
0. Click **Next**.
1. Click **Install**.
2. After the installation is completed, restart the CVM.
3. On the desktop, click 📱, enter **gpedit.msc**, and press Enter to open "Local Group Policy Editor".
4. In the leftside navigation tree, choose **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection**, and double-click **Do not allow supported Plug and Play**
device redirection, as shown in the following figure:
5. In the pop-up window, select **Disabled** and click **OK**, as shown in the following figure:

![Do not allow supported Plug and Play device redirection](image)

6. Restart the CVM.

**Configuring the client**

1. On the local PC, right-click "计算机" and choose **Run** to open the "Run" dialog box, as shown in the following figure:

2. In the "Run" dialog box, enter `gpedit.msc` and click **OK** to open "Local Group Policy Editor".

3. In the leftside navigation tree, choose **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Connection Client > RemoteFx USB Redirection** and double-click **Allow RDP redirection of other devices**.

©2013-2019 Tencent Cloud. All rights reserved.
supported RemoteFx USB devices, as shown in the following figure:

4. In the pop-up window, select **Enabled** and set the RemoteFx USB redirection access permission to **Administrators and Users**, as shown in the following figure:
5. Click **OK**.
6. Restart the local PC.

**Verifying the configuration result**

1. On your local PC, insert a USB device, right-click **Run** and choose **Run** to open the "Run" dialog box.
2. In the "Run" dialog box, enter **mstsc** and press Enter to open the remote desktop connection dialog box, as shown in the following figure:
3. Enter the Windows server's public IP address in **Computer**, and then click **Options**.

4. On the **Local Resources** tab page, click **More** under "Local devices and resources", as shown in the following figure:

![Remote Desktop Connection](image)

5. In the pop-up window, expand **Other supported RemoteFx USB devices**, select the inserted USB device, and click **OK**.
6. Click **Connect**.

7. In the pop-up **Windows Security** window, enter the instance's admin account and password, as shown in the following figure:
8. Click **OK** to log in to the Windows instance.
   If [ ] appears on the Windows instance operation page, the configuration was successful.

### Relevant Operations

Windows RDP provides optimized connection for standard USB devices. Devices such as drivers and cameras can be mapped directly without enabling the RemoteFX feature. The RemoteFX USB redirection feature is required for less commonly used USB devices. The following table lists the redirection methods for these USB devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Support Status</th>
<th>Redirection Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>All-in-One Printer</td>
<td>Supported</td>
<td>RemoteFX USB Redirection</td>
</tr>
<tr>
<td>Printer</td>
<td>Supported</td>
<td>Easy Print</td>
</tr>
<tr>
<td>Scanner</td>
<td>Supported</td>
<td>RemoteFX USB Redirection</td>
</tr>
<tr>
<td>Biometric</td>
<td>Supported while in session</td>
<td>RemoteFX USB Redirection</td>
</tr>
<tr>
<td></td>
<td>Not supported during login</td>
<td></td>
</tr>
<tr>
<td>PTP Camera</td>
<td>Supported</td>
<td>Plug and Play Device Redirection</td>
</tr>
<tr>
<td>MTP Media Player</td>
<td>Supported</td>
<td>Plug and Play Device Redirection</td>
</tr>
<tr>
<td>Webcam</td>
<td>Supported (LAN only)</td>
<td>RemoteFX USB Redirection</td>
</tr>
<tr>
<td>VoIP Telephone/Headset</td>
<td>Supported (LAN only)</td>
<td>RemoteFX USB Redirection</td>
</tr>
<tr>
<td>Audio (not a USB composite device)</td>
<td>Supported (LAN only)</td>
<td>Audio Redirection</td>
</tr>
<tr>
<td>CD or DVD Drive</td>
<td>Supported for read operations</td>
<td>Drive Redirection</td>
</tr>
<tr>
<td>Hard Drive or USB Flash Drive</td>
<td>Supported</td>
<td>Drive Redirection</td>
</tr>
<tr>
<td>Smart Card Reader</td>
<td>Supported</td>
<td>Smart Card Redirection</td>
</tr>
<tr>
<td>USB-to-Serial</td>
<td>Supported</td>
<td>RemoteFX USB Redirection</td>
</tr>
<tr>
<td>USB Network Adapter (also includes some personal digital assistants)</td>
<td>Blocked</td>
<td>N/A</td>
</tr>
<tr>
<td>USB Display</td>
<td>Blocked</td>
<td>N/A</td>
</tr>
<tr>
<td>USB Keyboard or Mouse</td>
<td>Supported</td>
<td>Input Redirection</td>
</tr>
</tbody>
</table>
Using USB/IP to Share USB Devices in Linux

Last updated: 2020-06-24 17:54:17

Scenario

USB/IP is an open-source project and has been incorporated in the kernel. In a Linux environment, you can use USB/IP to remotely share USB devices. This document uses the following environment versions as examples to describe how to use USB/IP to share USB devices.

USB client: CVM with CentOS 7.6
USB server: local PC with Debian

Notes

The USB/IP installation method and kernel module name vary by Linux OS versions. Check whether your current Linux OS supports the USB/IP feature.

Directions

Configuring the USB server

1. On the local PC, run the following commands in sequence to install USB/IP and load related kernel modules:

   ```
   sudo apt-get install usbip
   sudo modprobe usbip-core
   sudo modprobe vhci-hcd
   sudo modprobe usbip_host
   ```

2. Insert a USB device and run the following command to view available USB devices:

   ```
   usbip list --local
   ```

   For example, if a Feitian USB key is inserted to the local PC, the following result is returned:

   ```
   busid 1-1.3(096e:031b)
   Feitian Technologies, Inc.: unknown product(096e:031b)
   ```
3. Record the busid value and run the following commands in sequence to enable listening, specify the USB/IP port, and share the USB device:

```
sudo usbipd -D [--tcp-port PORT]
sudo usbip bind -b [busid]
```

For example, if the specified USB/IP port is port 3240 (default USB/IP port) and busid is 1-1.3, run the following commands:

```
sudo usbipd -D
sudo usbip bind -b 1-1.3
```

(Optional) 4. Run the following command to create an SSH tunnel and use port listening:

```
Skip this step if the local PC has a public IP address.
```

```
ssh -Nf -R specified USB/IP port:localhost:specified USB/IP port root@your_host
```

`your_host` indicates the CVM IP address.

For example, if the USB/IP port is port 3240 and the CVM IP address is 192.168.15.24, run the following command:

```
ssh -Nf -R 3240:localhost:3240 root@192.168.15.24
```

### Configuring the USB client

The following uses a local PC without a public IP as an example. If your local PC has a public IP, replace `127.0.0.1` in the following steps with the public IP of your local PC.

1. **Log into Linux instance using standard login method (recommended).**
2. Run the following commands in sequence to download the USB/IP source:

```
rpm --import https://www.elrepo.org/RPM-GPG-KEY-elrepo.org
```

3. Run the following commands in sequence to install USB/IP:

```
yum -y install kmod-usbip usbip-utils
modprobe usbip-core
```
modprobe vhci-hcd
modprobe usbip-host

4. Run the following command to query available USB devices of the CVM:

```bash
usbip list --remote 127.0.0.1
```

For example, if the Feitian USB key information is located, the following result is returned:

```
Exportable USB devices
-127.0.0.1 1-1.3: Feitian Technologies, Inc.: unknown
product(096e:031b):/sys/devices/platform/scb/fd500000.pcie/pci0000:00/0000:00:00.0/0000:01:00.0
/usb1/1-1/1-1.3:(Defined at Interface level)(00/00/00)
```

5. Run the following command to bind the USB device to the CVM:

```
usbip attach --remote=127.0.0.1 --busid=1-1.3
```

6. Run the following command to query the USB device list:

```bash
lsusb
```

If information similar to the following is returned, the USB device has been shared.

```
Bus 002 Device 002:ID096e:031b Feitian Technologies, Inc.
Bus 002 Device 001:ID1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 001:ID1d6b:0001 Linux Foundation 1.1 root hub
```