Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please contact Alibaba Cloud directly if you discover any errors in this document.
## Document conventions

<table>
<thead>
<tr>
<th>Style</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="danger.png" alt="Danger" /></td>
<td>A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.</td>
<td>Danger: Resetting will result in the loss of user configuration data.</td>
</tr>
<tr>
<td><img src="warning.png" alt="Warning" /></td>
<td>A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.</td>
<td>Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.</td>
</tr>
<tr>
<td><img src="note.png" alt="Notice" /></td>
<td>A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.</td>
<td>Notice: If the weight is set to 0, the server no longer receives new requests.</td>
</tr>
<tr>
<td><img src="note.png" alt="Note" /></td>
<td>A note indicates supplemental instructions, best practices, tips, and other content.</td>
<td>Note: You can use Ctrl + A to select all files.</td>
</tr>
<tr>
<td><img src="angle_brackets.png" alt="Closing angle brackets" /></td>
<td>Closing angle brackets are used to indicate a multi-level menu cascade.</td>
<td>Click Settings &gt; Network &gt; Set network type.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Bold formatting is used for buttons, menus, page names, and other UI elements.</td>
<td>Click OK.</td>
</tr>
<tr>
<td><strong>Courier font</strong></td>
<td>Courier font is used for commands.</td>
<td>Run the cd /d C:/window command to enter the Windows system folder.</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>Italic formatting is used for parameters and variables.</td>
<td>bae log list --instanceid Instance_ID</td>
</tr>
<tr>
<td>[] or [a</td>
<td>b]</td>
<td>This format is used for an optional value, where only one item can be selected.</td>
</tr>
<tr>
<td>Style</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>{} or {a</td>
<td>b}</td>
<td>This format is used for a required value, where only one item can be selected.</td>
</tr>
</tbody>
</table>
Contents

Legal disclaimer............................................................................................................. I
Document conventions.................................................................................................. I
1 Quick start................................................................................................................... 1
2 Build a software development environment......................................................... 3
  2.1 Build a LAMP environment..................................................................................... 3
  2.2 Deploy LNMP........................................................................................................... 17
    2.2.1 Use ROS to deploy an LNMP environment..................................................... 17
    2.2.2 Manually build an LNMP environment in CentOS 6........................................ 21
    2.2.3 Manually build an LNMP environment in CentOS 7........................................ 33
  2.3 Configure Java Web............................................................................................. 42
    2.3.1 Manually deploy a Java web environment....................................................... 42
    2.3.2 Use Cloud Toolkit to deploy a Java web environment..................................... 50
  2.4 Deploy Windows by changing the image............................................................ 64
  2.5 Deploy a Node.js project on CentOS.................................................................... 67
3 Build a website.......................................................................................................... 72
  3.1 Build a WordPress blog platform......................................................................... 72
    3.1.1 Build a WordPress website on a CentOS 7 ECS instance.............................. 72
    3.1.2 Build a WordPress website on a Windows ECS instance............................... 76
    3.1.3 Create a WordPress environment by using ROS............................................. 82
  3.2 Build a Drupal website.......................................................................................... 86
    3.2.1 Build a Drupal website based on an Alibaba Cloud Marketplace image........ 86
  3.3 Build a Magento e-commerce website on ECS.................................................... 89
  3.4 Deploy the Ghost blogging platform on CentOS................................................. 103
4 Build an application.................................................................................................. 115
  4.1 Build an FTP site on an ECS instance................................................................. 115
    4.1.1 Build an FTP site on a Linux instance........................................................... 115
    4.1.2 Build an FTP site on a Windows instance..................................................... 125
  4.2 Build Microsoft SharePoint 2016 on an ECS instance.......................................... 131
  4.3 Install SharePoint 2016........................................................................................ 144
  4.4 Build Docker......................................................................................................... 146
  4.5 Deploy databases based on ECS.......................................................................... 151
    4.5.1 Manually deploy a MySQL database on an ECS instance running CentOS 7......................................................................................................................... 151
    4.5.2 Manually deploy a MySQL database on Windows.......................................... 155
    4.5.3 Manage user-created databases hosted on an ECS instance......................... 160
  4.6 Build a primary/secondary PostgreSQL system.................................................. 162
  4.7 Deploy and use SVN............................................................................................. 168
    4.7.1 Overview........................................................................................................ 168
    4.7.2 Deploy SVN by using svnserve...................................................................... 169
4.7.3 Deploy SVN over HTTP........................................................................... 174
4.7.4 Use SVN................................................................................................. 181

5 Use the Vim editor....................................................................................... 183
# 1 Quick start

This topic describes a variety of methods on how to build websites on ECS.

**Procedure**

1. Select the ECS instance.
   
   The configurations of the ECS instance depend on the website type. You must determine the proper website size and estimate the number of visitors before you activate the ECS instance. For a small website, you can select an ECS instance with basic configurations. For more information about how to purchase an instance, see #unique_4.

   ECS instances support the subscription and pay-as-you-go billing methods. For more information, see #unique_5. For prices of different configurations, see Pricing of ECS.

2. Deploy a website.

3. Purchase a domain name.

   Enter the domain name that you want to purchase. If the domain name is not in use, you can purchase the domain name. For more information, see #unique_6.

   For the difference between the suffix .com and .net, see #unique_7.

4. Apply for an Internet Content Provider (ICP) filing for the domain name.

   - **Note:**
     If the instance that hosts your website is located in Mainland China, you must apply for an ICP filing for your domain name. Otherwise, you can skip this step.

   a. Prepare for the ICP filing.

      You must prepare the application materials based on the ICP filing regulations of the province, autonomous region, or municipality where you intend to submit the application. For more information, see #unique_8. For more information, see #unique_9.

   b. Apply for an ICP filing.

      For more information, see #unique_10.
5. Resolve the domain name.

You can resolve your domain name in Alibaba Cloud DNS. For more information, see [Configure the domain resolution](#). After you configure domain name resolution, users can visit your website through the configured domain name.

To map the domain name to an IP address, add an A record. For more information, see [Record types](#).

Now you have built a website on your own. After you built your website, you can visit the website and test its service by using the domain name.

**FAQ**

The following section describes the frequently asked questions and corresponding solutions for using ECS instances or building websites:

**Security groups and snapshots**

- [unique_11](#)
- [unique_12](#)

**Failure to visit a website you have built**

- What are the common causes and solutions of failures occurring when attempting to visit my website?
- How do I test the connection when the ping result shows packet loss or when the ping operation has failed?

**References**

- For information about how to select Alibaba Cloud services and configurations based on business needs, see [Architecture Design and Cloudification Consultation](#).
- If you want to migrate your business from an on-premises data center or a hosted data center to Alibaba Cloud, you can request technical support for cloud migration to Alibaba Cloud. Professional cloud migration solutions are provided to support your business. For more information, see [Cloud Migration Support](#).
2 Build a software development environment

2.1 Build a LAMP environment

This topic describes how to build a LAMP stack on an ECS instance. LAMP is an acronym of the names of its original four open-source components: the Linux operating system, Apache HTTP Server, MySQL relational database management system, and PHP programming language.

Prerequisites

An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud official website.

Context

An ECS instance with the following configurations is used as an example:

- Instance type: ecs.c6.large
- Operating system: CentOS 7.2 64-bit
- Network type: VPC
- IP address: public IP address

This topic uses the following software versions. When you build a LAMP stack, choose software versions as needed.

- Apache 2.4.43
- MySQL 5.6.24
- PHP 7.0.32
- phpMyAdmin 4.0.10.20

This topic is intended for individual users who are familiar with the Linux operating system, but new to using Alibaba Cloud ECS to build websites.

This topic describes how to manually build a LAMP stack. You can also purchase a LAMP image on Alibaba Cloud Marketplace and create an ECS instance from the image to build websites.

Procedure

Follow these steps to build a LAMP stack on an ECS instance:
1. **Step 1. Prepare the compilation environment**

2. **Step 2. Install Apache**

3. **Step 3. Install MySQL**

4. **Step 4. Install PHP**

5. **Step 5. Install phpMyAdmin**

### Step 1. Prepare the compilation environment

Follow these steps to prepare the compilation environment:

1. #unique_4.

2. #unique_15.

3. Run the `cat /etc/redhat-release` command to view the system version.

   ![Command Output]

   ```
   [root@test ~]# cat /etc/redhat-release
   CentOS Linux release 7.2.1511 (Core)
   ```

4. Disable the firewall.

   a) Run the `systemctl status firewalld` command to check the status of the firewall.

   ![Command Output]

   ```
   [root@test ~]# systemctl status firewalld
   firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor prefixed)
   Active: active (running) since Tue 2018-11-13 10:40:03 CST; 21s ago
   Docs: man:firewalld(1)
   Main PID: 20765 (firewalld)
   ```

   - If the firewall is in the inactive state, the firewall is disabled.
   - If the firewall is in the active state, the firewall is enabled. In this example, the firewall is in the active state. Therefore, you must disable the firewall.

   b) Disable the firewall. Skip this step if the firewall is already disabled.

   - To temporarily disable the firewall, run the `systemctl stop firewalld` command.

     ![Note]

     **Note:**

     After you run this command, the firewall is temporarily disabled. It will enter the active state when you restart the Linux operating system.

   - To permanently disable the firewall, run the `systemctl disable firewalld` command.

     ![Note]

     **Note:**

     You can re-enable the firewall after it is disabled. For more information, visit the firewalld website.
   
a) Run the `getenforce` command to check the status of SELinux.
   ```
   [root@test ~]# getenforce
   Enforcing
   ```
   - If SELinux is in the Disabled state, SELinux is disabled.
   - If SELinux is in the Enforcing state, SELinux is enabled. In this example, SELinux is in the Enforcing state. Therefore, you must disable SELinux.

b) Disable SELinux. Skip this step if SELinux is already disabled.
   - To temporarily disable SELinux, run the `setenforce 0` command.
   ```
   Note:
   After you run this command, SELinux is temporarily disabled. It will enter the
   Enforcing state when you restart the Linux operating system.
   ```
   - To permanently disable SELinux, run the `vi /etc/selinux/config` command to edit the SELinux configuration file. Press the Enter key. Move the pointer to the `SELINUX=enforcing` row and press the I key to edit the configuration file. Change `SELINUX=enforcing` to `SELINUX=disabled` and press the Esc key. Enter `:wq` and press the Enter key to save and close the SELinux configuration file.
   ```
   Note:
   You can re-enable SELinux after it is disabled. For more information, see the
   SELinux documentation.
   ```

c) Restart the system to apply the settings.

6. Add an inbound rule to the security group of the ECS instance to allow traffic on the required port. For more information, see #unique_16.

Step 2. Install Apache

Follow these steps to install Apache:
1. Run the following commands to install the dependency package:
   a. `yum groupinstall "Development Tools" -y`
   b. `yum install libtool -y`
   c. `yum install expat-devel pcre pcre-devel openssl-devel -y`

2. Run the following commands to download and decompress the Apache, APR, and APR-util source code packages:

   **Note:**
   Source code package versions are continuously upgraded. You can check available source code package versions from [httpd source code package](#) and [APR source code](#).
package, and replace the source code package versions in the command with the versions to be installed.


In this example, the Apache source code package version is 2.4.43. You can run the following command to download the package:

`wget https://mirrors.aliyun.com/apache/httpd/httpd-2.4.43.tar.gz`

b. `wget https://mirrors.aliyun.com/apache/apr/apr-<APR source code package version>.tar.gz`

In this example, the APR source code package version is 1.6.5. You can run the following command to download the package:

`wget https://mirrors.aliyun.com/apache/apr/apr-1.6.5.tar.gz`

c. `wget https://mirrors.aliyun.com/apache/apr/apr-util-<APR-util source code package version>.tar.gz`

In this example, the APR-util source code package version is 1.6.1. You can run the following command to download the package:

`wget https://mirrors.aliyun.com/apache/apr/apr-util-1.6.1.tar.gz`

d. `tar xvf httpd-<Apache source code package version>.tar.gz -C /usr/local/src`

In this example, the Apache source code package version is 2.4.43. You can run the following command to decompress the package:

`tar xvf httpd-2.4.43.tar.gz -C /usr/local/src`

e. `tar xvf apr-<APR source code package version>.tar.gz -C /usr/local/src`

In this example, the APR source code package version is 1.6.5. You can run the following command to decompress the package:

`tar xvf apr-1.6.5.tar.gz -C /usr/local/src`

f. `tar xvf apr-util-<APR-util source code package version>.tar.gz -C /usr/local/src`

In this example, the APR-util source code package version is 1.6.1. You can run the following command to decompress the package:

`tar xvf apr-util-1.6.1.tar.gz -C /usr/local/src`

3. Run the following commands to move the APR and APR-util source code packages to the Apache srclib folder:

a. `cd /usr/local/src`

b. `mv apr-<APR source code package version> httpd-<Apache source code package version>/srclib/apr`

In this example, the APR and Apache source code package versions are 1.6.5 and 2.4.43, respectively. You can run the following command to move the folders:

`mv apr-1.6.5 httpd-2.4.43/srclib/apr`

c. `mv apr-util-<APR-util source code package version> httpd-<Apache source code package version>/srclib/apr-util`

In this example, the APR and Apache source code package versions are 1.6.1 and 2.4.43, respectively. You can run the following command to move the folders:

`mv apr-util-1.6.1 httpd-2.4.43/srclib/apr-util`

4. Run the following commands to compile the source code:

a. `cd /usr/local/src/httpd-<Source code package version>`

In this example, the Apache source code package version is 2.4.43. You can run the following command to access the directory where the Apache source code is located:

`cd /usr/local/src/httpd-2.4.43`

b. `./buildconf`

c. `./configure --prefix=/usr/local/apache2`
4. make && make install

5. Run the following commands to set the PATH environment variable:
   a. echo "export PATH=$PATH:/usr/local/apache2/bin" > /etc/profile.d/httpd.sh
   b. source /etc/profile.d/httpd.sh

6. You can run the `httpd -v` command to view the Apache version number.

7. Add the Apache configuration file.
   a) Run the `vi /usr/lib/systemd/system/httpd.service` command to open the configuration file.
   b) Press the I key and add the following content to the configuration file:

```
[Unit]
Description=The Apache HTTP Server
After=network.target

[Service]
Type=forking
ExecStart=/usr/local/apache2/bin/apachectl -k start
ExecReload=/usr/local/apache2/bin/apachectl -k graceful
ExecStop=/usr/local/apache2/bin/apachectl -k graceful-stop
PIDFile=/usr/local/apache2/logs/httpd.pid
PrivateTmp=false

[Install]
WantedBy=multi-user.target
```
   c) Press the Esc key, enter :wq, and then press the Enter key to save and close the Apache configuration file.
8. Run the following commands to start Apache and enable Apache to start upon system startup:

a. `systemctl start httpd`

b. `systemctl enable httpd`

9. Check the installation status.

a) Log on to the ECS console.

b) In the left-side navigation pane, choose **Instances & Images > Instances**.

c) On the **Instances** page, find the target instance and copy its public IP address from the **IP address** column.

d) Enter `http://Public IP address of the ECS instance` in the address bar of your browser and press the Enter key.

If the following page is displayed, Apache is started.

```
It works!
```

### Step 3. Install MySQL

Follow these steps to install MySQL:
1. Run the following commands to prepare the compilation environment:
   a. `yum install ncurses-devel bison gnutls-devel -y`
   b. `yum install cmake -y`

2. Run the following commands to prepare a directory to store MySQL data:
   a. `cd`
   b. `mkdir /mnt/data`
   c. `groupadd -r mysql`
   d. `useradd -r -g mysql -s /sbin/nologin mysql`
   e. `id mysql`

3. Run the following command to change the owner and group of the data directory:
   ```
   chown -R mysql:mysql /mnt/data
   ```

4. Run the following commands to download, decompress, and compile the general availability (GA) version of the source code:

   **Note:**
   If an exception occurs to the official MySQL download link, we recommend that you download the MySQL source code package from a third-party link on your ECS instance. Alternatively, you can download the package from the MySQL official website or a third-party channel, and then use a remote connection tool such as PuTTY to upload the package to your ECS instance.

   a. Use one of the following methods to download the source code package. In this example, the MySQL source code package version is 5.6.24.
      - `wget https://dev.mysql.com/get/Downloads/mysql-5.6.24.tar.gz`
      - `wget https://cdn.mysql.com/archives/mysql-5.6/mysql-5.6.24.tar.gz`
   b. `tar xvf mysql-5.6.24.tar.gz -C /usr/local/src`
   c. `cd /usr/local/src/mysql-5.6.24`
   d. `cmake -DCMAKE_INSTALL_PREFIX=/usr/local/mysql \
      -DMYSQL_DATADIR=/mnt/data \
      -DSYSCONFDIR=/etc \
      -DWITH_INNODB_STORAGE_ENGINE=1 \
      -DWITH_ARCHIVE_STORAGE_ENGINE=1 \
      -DWITH_BLACKHOLE_STORAGE_ENGINE=1 \
      -DWITH_READLINE=1 \
      -DWITH_SSL=system`
-DWITH_ZLIB=system \ 
-DWITH_LIBWRAP=0 \ 
-DMYSQL_TCP_PORT=3306 \ 
-DDEFAULT_CHARSET=utf8 \ 
-DMYSQL_UNIX_ADDR=/usr/local/mysql/mysql.sock \ 
-DDEFAULT_COLLATION=utf8_general_ci \ 
-DWITH_SYSTEMD=1 \ 
-DINSTALL_SYSTEMD_UNITDIR=/usr/lib/systemd/system

e. make && make install

5. Run the following command to change the group of the installation directory to mysql:

chown -R mysql:mysql /usr/local/mysql/

6. Run the following commands to initialize the database and copy the configuration file:

a. cd /usr/local/mysql

b. /usr/local/mysql/scripts/mysql_install_db --user=mysql --datadir=/mnt/data/

c. mv /etc/my.cnf /etc/my.cnf.bak

d. cp /usr/local/mysql/support-files/my-default.cnf /etc/my.cnf

7. Run the following command to change the installation and data storage paths:

```
echo -e "basedir = /usr/local/mysql\ndatadir = /mnt/data\n" >> /etc/my.cnf
``` 

8. Modify the MySQL configuration file.

a) Run the `vi /usr/lib/systemd/system/mysql.service` command to open the MySQL configuration file.

b) Press the I key and add the following content to the configuration file:

```
[Unit]
Description=MySQL Community Server
After=network.target
After=syslog.target

[Install]
WantedBy=multi-user.target
Alias=mysql.service

[Service]
User=mysql
Group=mysql
PermissionsStartOnly=true
ExecStart=/usr/local/mysql/bin/mysqld
TimeoutSec=600
Restart=always
PrivateTmp=false
```

c) Press the Esc key, enter :wq, and then press the Enter key to save and close the MySQL configuration file.
9. Run the following commands to set the PATH environment variable:
   a. `echo "export PATH=$PATH:/usr/local/mysql/bin" > /etc/profile.d/mysql.sh`
   b. `source /etc/profile.d/mysql.sh`

10. Run the following commands to start MySQL and enable it to start upon system startup:
   a. `systemctl start mysql`
   b. `systemctl enable mysql`

11. Change the MySQL root password. Run the following command and set the password by following the instructions:
    `mysqladmin -u root password`

12. Run the following command to log on to the MySQL database:
    `mysql -uroot -p`

```
[root@test mysql]$ mysql -uroot -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \.g.
Your MySQL connection id is 2
Server version: 5.6.24 Source distribution

Copyright (c) 2000, 2015, 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.
```

13. Run the `\q` command to log off from the MySQL database.

Step 4. Install PHP

Follow these steps to install PHP:

1. Run the following command to install the dependency package:
   `yum install libmcrypt libmcrypt-devel mhash mhash-devel libxml2 libxml2-devel bzip2 bzip2-devel -y`

2. Run the following commands to download, decompress, and compile the GA version of the source code package:

   ![Note]
To download the GA version of the PHP source code package, ensure that the network environment is good. If the download fails, run the `cd` command and then run the `rm -rf mirror` command to download the GA version of the PHP source code package again.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>cd</td>
</tr>
<tr>
<td>b.</td>
<td>wget <a href="https://cn2.php.net/get/php-7.0.32.tar.bz2/from/this/mirror">https://cn2.php.net/get/php-7.0.32.tar.bz2/from/this/mirror</a></td>
</tr>
<tr>
<td>c.</td>
<td>cp mirror php-7.0.32.tar.bz2</td>
</tr>
<tr>
<td>d.</td>
<td>tar xvf php-7.0.32.tar.bz2 -C /usr/local/src</td>
</tr>
<tr>
<td>e.</td>
<td>cd /usr/local/src/php-7.0.32</td>
</tr>
<tr>
<td>f.</td>
<td>./configure --prefix=/usr/local/php \  --with-config-file-scan-dir=/etc/php.d \  --with-apxs2=/usr/local/apache2/bin/apxs \  --with-config-file-path=/etc \  --with-pdo-mysql=mysqlnd \  --with-mysql=/usr/local/mysql/bin/mysql_config \  --enable-mbstring \  --with-freetype-dir \  --with-jpeg-dir \  --with-png-dir \  --with-zlib \  --with-libxml-dir=/usr \  --with-openssl \  --enable-xml \  --enable-sockets \  --enable-fpm \  --with-bz2</td>
</tr>
<tr>
<td>g.</td>
<td>make &amp;&amp; make install</td>
</tr>
</tbody>
</table>

**Note:**

If the ECS instance does not have sufficient memory, terminate PHP extensions that you do not need when you configure PHP to save memory. For example, you can add the `--disable-fileinfo` option to the `./configure` command to terminate the fileinfo extension.
3. Run the following command to copy the PHP configuration file:

```bash
cp php.ini-production /etc/php.ini
```

4. Run the command `vi /usr/local/apache2/conf/httpd.conf` to open the Apache configuration file, and then press the I key to edit the configuration file.

   a) Find the `ServerName` parameter and add `ServerName localhost:80` to the parameter.

   ```
   ServerName example.com
   ServerName localhost:80
   ServerName www.example.com:80
   ```

   b) Find the `Directory` parameter. Add a number sign (#) before `Require all denied`, start a new line, and then add `Require all granted`.

   ```
   Directory /
   AllowOverride none
   # Require all denied
   Require all granted
   ```

   c) Find `DirectoryIndex index.html` and replace it with `DirectoryIndex index.php index.html`.

   ```
   <IfModule dir_module>
   DirectoryIndex index.php index.html
   </IfModule>
   ```

   d) Find the following content:

   ```
   # 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
   ```
Add the following content:

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

The configurations are as shown in the following figure.

![Apache configuration settings](image)

e) Press the Esc key, enter :wq, and press the Enter key to save and close the Apache configuration file.

**5. Add Apache support for PHP parsing.**

a) Run the following command to open the index.php file:

```
vi /usr/local/apache2/htdocs/index.php
```

b) Press the I key to edit the file. Add the following content to the file:

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

c) Press the Esc key, enter :wq, and then press the Enter key to save and close the index.php file.

d) Run the following command to restart Apache:

```
systemctl restart httpd
```

**6. Enter http://Public IP address of the ECS instance in the address bar of your browser and press the Enter key.**

If the following page is displayed, PHP parsing is working properly.

![PHP version 7.0.32](image)
Step 5. Install phpMyAdmin

Follow these steps to install phpMyAdmin:

1. Run the following commands to prepare a directory to store phpMyAdmin data:
   a. `cd`
   b. `mkdir -p /usr/local/apache2/htdocs/phpmyadmin`

2. Run the following commands to download and decompress the phpMyAdmin package:
   a. `wget https://files.phpmyadmin.net/phpMyAdmin/4.0.10.20/phpMyAdmin-4.0.10.20-all-languages.zip`
   b. `unzip phpMyAdmin-4.0.10.20-all-languages.zip`

3. Run the following command to copy the phpMyAdmin files to the prepared directory:
   
   ```
   mv phpMyAdmin-4.0.10.20-all-languages/* /usr/local/apache2/htdocs/phpmyadmin
   ```

4. Enter `http://Public IP address of the ECS instance/phpmyadmin` in the address bar of your browser and press the Enter key to go to the logon page of phpMyAdmin.
   If the following page is displayed, phpMyAdmin has been installed.
5. Enter the MySQL username and password. Click Go.

2.2 Deploy LNMP

2.2.1 Use ROS to deploy an LNMP environment

An LNMP environment is based on four major components: Linux, NGINX, MySQL, and PHP. This topic describes how to use Resource Orchestration Service (ROS) to deploy LNMP environments.

Prerequisites

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud official website.
- You will be prompted to activate ROS the first time you use the service. ROS is a free service and thus can be activated free of charge.

Context
ROS is a free service. You do not need to download or install anything to use ROS. You can use ROS to create resource stack templates in JSON format. In the ROS console, you can also use a sample template to create a resource stack. For more information, see Sample Templates.

You can also use other sample templates in the ROS console to build other environments, such as Java Web test environments, Node.js development and test environments, Ruby Web development and test environments, or Hadoop and Spark distributed systems. This topic employs the Deploy a LNMP (Linux, NGINX, MySQL, and PHP) Stack template to demonstrate how to use ROS to automatically create an ECS instance and deploy an LNMP environment on the instance.

For more information about ROS, see ROS documentation.

Procedure

1. Log on to the ROS console.
2. In the left-side navigation pane, choose Templates > Sample Templates.
3. In the top navigation bar, select a region.
4. Find the Deploy a LNMP (Linux, NGINX, MySQL, and PHP) Stack template.
5. Click **View Details** to check the template in JSON format. The following table lists the top-level fields in the JSON file.

<table>
<thead>
<tr>
<th>Top-level field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;ROSTemplateFormatVersion&quot;: &quot;2015-09-01&quot;</td>
<td>Specifies the version of the template.</td>
</tr>
<tr>
<td>&quot;Description&quot;: &quot;Deploy LNMP (Linux + Nginx + MySQL + PHP) stack on 1 ECS instance. <em><strong>WARNING</strong></em> Only support CentOS-7.&quot;</td>
<td>Describes the template and how it is used.</td>
</tr>
<tr>
<td>&quot;Parameters&quot;: {}</td>
<td>Specifies template parameters. For this example, this field specifies the default image ID and instance type.</td>
</tr>
<tr>
<td>&quot;Resources&quot;: {}</td>
<td>Specifies the resources that you can use the template to create. For this example, this field specifies that the resources to be created include an ECS instance and a security group. The properties of these resources are defined in the Parameters field.</td>
</tr>
<tr>
<td>&quot;Outputs&quot;: {}</td>
<td>Specifies the resource information that the stack outputs after ROS creates the specified resources. For this example, the stack outputs the ECS instance ID, public IP address, and security group ID.</td>
</tr>
</tbody>
</table>

6. Click **Create Stack**.

7. Set the parameters and click **Create Stack**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack Name</td>
<td>Specifies a unique stack name. You cannot change the stack name after ROS creates the stack.</td>
</tr>
<tr>
<td>Nginx Download Url</td>
<td>Use the default NGINX download URL.</td>
</tr>
<tr>
<td>DB Password</td>
<td>The password used to access the MySQL database. The password can only contain letters and digits.</td>
</tr>
<tr>
<td>Confirm DB Password</td>
<td>Confirm the password used to access the MySQL database.</td>
</tr>
<tr>
<td>Available Zone ID</td>
<td>The zone ID of the resource that you want to create.</td>
</tr>
<tr>
<td>Image ID</td>
<td>The ID of the image that ROS uses to create the ECS instance.</td>
</tr>
<tr>
<td>DB Name</td>
<td>The name of the MySQL database.</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DB Username</td>
<td>The username of the MySQL database.</td>
</tr>
<tr>
<td>DB Root Password</td>
<td>The password of a MySQL root user. The password can only contain letters and digits.</td>
</tr>
<tr>
<td>Confirm DB Root Password</td>
<td>Confirm the password of a MySQL root user.</td>
</tr>
<tr>
<td>Instance Type</td>
<td>The type of the ECS instance that you want to create.</td>
</tr>
<tr>
<td>System Disk Category</td>
<td>The disk category of the system disk.</td>
</tr>
<tr>
<td>Instance Password</td>
<td>The password used to log on to the ECS instance. The password can only contain letters and digits.</td>
</tr>
<tr>
<td>Confirm Instance Password</td>
<td>Confirm the password used to log on to the ECS instance.</td>
</tr>
</tbody>
</table>

8. In the left-side navigation pane, click **Stacks** to check the status of the stack that you have created.

9. Click the name of the new stack. Click the **Outputs** tab and check the **NginxWebsiteURL** value.

You can use the URL to connect to the LNMP environment that you have created.

- **Note:**
  - On the **Resources** tab, you can check all of the resources in the stack.
• On the **Events** tab, you can check the operations that ROS performs in the process of creating the stack. The causes of failed operations are also displayed in the list.

### 2.2.2 Manually build an LNMP environment in CentOS 6

This topic describes how to manually build an LNMP environment on an ECS instance that runs the CentOS 6 operating system. LNMP represents a combination of Linux, NGINX, MySQL, and PHP.

**Prerequisites**

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the [Alibaba Cloud official website](https://www.aliyun.com).
- An inbound rule is added to a security group of the ECS instance to allow traffic on port 80. If port 80 is not enabled, enable the port first. For more information, see [unique_16](#unique_16).

<table>
<thead>
<tr>
<th>Direction</th>
<th>Authorization policy</th>
<th>Protocol type</th>
<th>Port range</th>
<th>Priority</th>
<th>Authorization type</th>
<th>Authorized object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Allow</td>
<td>HTTP (80)</td>
<td>80/80</td>
<td>1</td>
<td>IPv4 CIDR block</td>
<td>The public IP addresses of clients to be allowed to access the LNMP environment. Separate multiple IP addresses with commas (,). A value of 0.0.0.0/0 indicates that all IP addresses are allowed to access the LNMP environment.</td>
</tr>
</tbody>
</table>

**Context**

This topic is intended for individual users who are familiar with Linux, but new to web development on Alibaba Cloud ECS instances.

This topic describes how to manually build an LNMP environment. You can also purchase an LNMP image on [Alibaba Cloud Marketplace](https://marketplace.aliyun.com) and create an ECS instance from the image to build websites.
The procedure described in this topic is applicable to the following instance configurations and software versions:

- **Instance type:** ecs.c6.large
- **Operating system:** public images running CentOS 6.8 32-bit

**Note:**
If you are using a 32-bit operating system, do not select instance types that have a memory capacity greater than 4 GiB.

- **NGINX:** nginx-1.10.2
- **MySQL:** MySQL 5.6.24
- **PHP:** PHP 5.6.23
- **Network type:** VPC
- **IP address:** public IP address

The commands and parameters used in this topic may vary based on your software version.

**Procedure**

Perform the following steps to build an LNMP environment on an ECS instance:

- **Step 1:** Prepare the compilation environment
- **Step 2:** Install and configure NGINX
- **Step 3:** Install and configure MySQL
- **Step 4:** Install PHP-FPM
- **Step 5:** Test the connection to the LNMP environment

**Step 1: Prepare the compilation environment**

1. Create an ECS instance.
   
   For more information, see #unique_4.
2. Connect to the Linux instance.
   
   For more information, see #unique_15.
3. Run the command `cat /etc/redhat-release` to check the system version.
Step 2: Install and configure NGINX

1. Run the following commands in sequence to add a user to run the NGINX service process:

   ```bash
   groupadd -r nginx
   useradd -r -g nginx nginx
   ```

2. Download the source code package, and decompress and compile the package.

   a) Run the following command to download the source code package:

   ```bash
   wget http://nginx.org/download/nginx-1.10.2.tar.gz
   ```

   b) Run the following command to decompress the source code package:

   ```bash
   tar xvf nginx-1.10.2.tar.gz -C /usr/local/src
   ```

   c) Run the following commands in sequence to install compilation tools:

   ```bash
   yum groupinstall "Development tools"
   ```

   ```bash
   yum -y install gcc wget gcc-c++ automake autoconf libtool libxml2-devel libxslt-devel perl-devel perl-ExtUtils-Embed pcre-devel openssl-devel
   ```

   d) Run the following command to go to the directory of the NGINX source code package:

   ```bash
   cd /usr/local/src/nginx-1.10.2
   ```

   e) Run the following commands in sequence to compile the source code:

   ```bash
   ./configure
   ```

   ```bash
   --prefix=/usr/local/nginx
   --sbin-path=/usr/sbin/nginx
   --conf-path=/etc/nginx/nginx.conf
   --error-log-path=/var/log/nginx/error.log
   --http-log-path=/var/log/nginx/access.log
   --pid-path=/var/run/nginx.pid
   --lock-path=/var/run/nginx.lock
   --http-client-body-temp-path=/var/tmp/nginx/client
   --http-proxy-temp-path=/var/tmp/nginx/proxy
   --http-fastcgi-temp-path=/var/tmp/nginx/fcgi
   --http-uwsgi-temp-path=/var/tmp/nginx/uwsgi
   --http-scgi-temp-path=/var/tmp/nginx/scgi
   --user=nginx
   --group=nginx
   --with-pcre
   --with-http_v2_module
   --with-http_ssl_module
   --with-http_realip_module
   --with-http_addition_module
   --with-http_sub_module
   --with-http_dav_module
   --with-http_flv_module
   --with-http_mp4_module
   --with-http_gunzip_module
   ```
Elastic Compute Service

Tutorials / 2 Build a software development environment

```
--with-http_gzip_static_module
--with-http_random_index_module
--with-http_secure_link_module
--with-http_stub_status_module
--with-http_auth_request_module
--with-mail
--with-mail_ssl_module
--with-file-aio
--with-ipv6
--with-http_v2_module
--with-threads
--with-stream
--with-stream_ssl_module
make && make install
```

f) Run the following command to create a directory:

```
mkdir -p /var/tmp/nginx/client
```

3. Add the SysV startup script.

a) Run the `vi /etc/init.d/nginx` command to open the SysV startup script file.

b) Press the I key and add the following content to the script file:

```bash
#!/bin/sh
#
# nginx - this script starts and stops the nginx daemon
#
# chkconfig:   - 85 15
# description: Nginx is an HTTP(S) server, HTTP(S) reverse \n#               proxy and IMAP/POP3 proxy server
# processname: nginx
# config:      /etc/nginx/nginx.conf
# config:      /etc/sysconfig/nginx
# pidfile:     /var/run/nginx.pid
# Source function library.
. /etc/rc.d/init.d/functions
# Source networking configuration.
. /etc/sysconfig/network
# Check that networking is up.
[ "$NETWORKING" = "no" ] && exit 0
nginx="/usr/sbin/nginx"
prog=$(basename $nginx)
NGINX_CONF_FILE="/etc/nginx/nginx.conf"
[-f /etc/sysconfig/nginx ] && . /etc/sysconfig/nginx
lockfile=/var/lock/subsys/nginx
start() {
   [-x $nginx ]|| exit 5
   [-f $NGINX_CONF_FILE ]|| exit 6
   echo -n "$prog: "
daemon $nginx -c $NGINX_CONF_FILE
   retval=$?
   echo
   [ $retval -eq 0 ] && touch $lockfile
   return $retval
}
stop() {
   echo -n "$prog: 
   killproc $prog -QUIT
   retval=$?
```

Issue: 20200628
c) Press the Esc key, enter :wq, and then press the Enter key to save and close the SysV startup script file.
4. Run the following command to grant executable permissions to the script:

   chmod a+x /etc/init.d/ossfs

5. Run the following commands in sequence to add NGINX to the service management list and enable it to run at system startup:

   chkconfig --add nginx

   chkconfig nginx on

6. Run the following command to start NGINX:

   service nginx start

7. Test whether NGINX is installed.
   a) Log on to the ECS console.
   b) In the left-side navigation pane, choose Instances & Images > Instances.
   c) On the Instances page, find the target instance, and copy the public IP address of the instance from the IP Address column.
   d) In the browser address bar, enter the IP address and press the Enter key.
      The following response indicates that NGINX is installed.

---

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 and configure MySQL

1. Run the following commands in sequence to prepare the compilation environment:

   yum groupinstall "Server Platform Development" "Development tools" -y

   yum install cmake -y

2. Create a directory to store MySQL data.

   a) Run the `mkdir /mnt/data` command to create a directory to store MySQL data.
   b) Run the `groupadd -r mysql` command to create a user group named `mysql`.
   c) Run the `useradd -r -g mysql -s /sbin/nologin mysql` command to create a user named `mysql`.
   d) Run the `id mysql` command to check whether the user is created.
   e) Run the `chown -R mysql:mysql /mnt/data` command to change the group and user of the MySQL data directory to `mysql`.

3. Download the latest stable version of the source code package, and decompress and compile it.

   a) Run one of the following commands to download the source code package:

      * `wget https://dev.mysql.com/get/Downloads/mysql-5.6.24.tar.gz`
      * `wget https://cdn.mysql.com/archives/mysql-5.6/mysql-5.6.24.tar.gz`

   b) Run the following command to decompress the source code package:

      `tar xvf mysql-5.6.24.tar.gz -C /usr/local/src`

   c) Run the following command to go to the directory of the MySQL source code package:

      `cd /usr/local/src/mysql-5.6.24`

   d) Run the following commands in sequence to compile the source code package:

      `cmake . -DCMAKE_INSTALL_PREFIX=/usr/local/mysql\`
      `   -DMYSQL_DATADIR=/mnt/data\`
      `   -DSYSCONFDIR=/etc\`
      `   -DWITH_INNODB_STORAGE_ENGINE=1\`
      `   -DWITH_ARCHIVE_STORAGE_ENGINE=1\`
      `   -DWITH_BLACKHOLE_STORAGE_ENGINE=1\`
      `   -DWITH_READLINE=1\`
      `   -DWITH_SSL=system\`
      `   -DWITH_ZLIB=system\`
      `   -DWITH_LIBWRAP=0\`
      `   -DMYSQL_TCP_PORT=3306\`
      `   -DMYSQL_UNIX_ADDR=/tmp/mysql.sock\`
      `   -DDEFAULT_CHARSET=utf8\`

   ```
4. Configure MySQL.
   a) Run the following command to change the group and user of the installation directory to mysql:
      ```bash
      chown -R mysql:mysql /usr/local/mysql/
      ```
   b) Run the following commands in sequence to initialize the database:
      ```bash
      cd /usr/local/mysql
      /usr/local/mysql/scripts/mysql_install_db --user=mysql --datadir=/mnt/data/
      ```

Note:
After MySQL is installed on CentOS 6.8, a file named my.cnf appears under the /etc directory. You must change the file name to another one such as /etc/my.cnf.bak.
Otherwise, the file will interfere with the configuration of MySQL and cause MySQL to fail to start.

c) Run the following commands in sequence to copy the configuration file of MySQL:

```
cp /usr/local/mysql/support-files/mysql.server /etc/init.d/mysqld

cp /usr/local/mysql/support-files/my-default.cnf /etc/my.cnf
```

d) Run the following command to grant executable permissions to the startup script of MySQL:

```
chmod a+x /etc/init.d/ossfs
```

e) Run the following commands in sequence to add MySQL to the service management list and enable it to run at system startup:

```
chkconfig --add mysqld

cchkconfig mysqld  on
```

f) Run the following command to change the installation and data storage paths:

```
echo -e "basedir = /usr/local/mysql\ndatadir = /mnt/data\n" >> /etc/my.cnf
```

g) Run the following commands in sequence to set the PATH environment variable:

```
echo "export PATH=$PATH:/usr/local/mysql/bin" > /etc/profile.d/mysql.sh

source /etc/profile.d/mysql.sh
```

5. Run the following command to start MySQL:

```
service mysqld start
```

6. Run the following command to connect to the MySQL database for testing:

```
mysql -h 127.0.0.1
```

Step 4: Install PHP-FPM

As a web server, NGINX does not directly call or parse external programs when it receives requests. It must use FastCGI to call such programs. However, in case of a PHP request, NGINX will transfer the request to a PHP interpreter, and return the result to the client. PHP-FPM is a FastCGI process manager that can parse PHP code. PHP-FPM provides better PHP process management methods, which can effectively control the memory and processes and smoothly reload PHP configurations.
1. Run the following command to install the dependency package:

```bash
yum install libmcrypt libmcrypt-devel mhash mhash-devel libxml2 libxml2-devel bzip2 bzip2-devel -y
```

2. Download the latest stable version of the source code package, and decompress and compile it.

   a) Run the following command to download the source code package:

   ```bash
   wget http://cn2.php.net/get/php-5.6.23.tar.bz2/from/this/mirror
   ```

   **Note:**
   To download the GA version of the PHP source code package, ensure that the network environment is good. If the download fails, run the `cd` command and then run the `rm -rf mirror` command to download the GA version of the PHP source code package again.

   b) Run the following commands in sequence to decompress the source code package:

   ```bash
   cp mirror php-5.6.23.tar.bz2
   tar xvf php-5.6.23.tar.bz2 -C /usr/local/src
   ```

   c) Run the following command to go to the directory of the PHP source code package:

   ```bash
   cd /usr/local/src/php-5.6.23
   ```

   d) Run the following commands in sequence to compile the source code package:

   ```bash
   ./configure --prefix=/usr/local/php \
   --with-config-file-scan-dir=/etc/php.d \ 
   --with-config-file-path=/etc \ 
   --with-mysql=/usr/local/mysql \ 
   --with-mysqli=/usr/local/mysql/bin/mysql_config \ 
   --enable-mbstring \ 
   --with-freetype-dir \ 
   --with-jpeg-dir \ 
   --with-png-dir \ 
   --with-zlib \ 
   --with-libxml-dir=/usr \ 
   --with-openssl \ 
   --enable-xml \ 
   --enable-sockets \ 
   --enable-fpm \ 
   --with-mcrypt
   ```
3. Configure PHP.
   a) Run the following commands in sequence to add the PHP and PHP-FPM configuration files:
      ```
      cp /usr/local/src/php-5.6.23/php.ini-production /etc/php.ini
      cd /usr/local/php/etc/
      cp php-fpm.conf.default php-fpm.conf
      sed -i 's@;pid = run/php-fpm.pid@pid = /usr/local/php/var/run/php-fpm.pid@' php-fpm.conf
      ```
   b) Run the following command to add the PHP-FPM startup script:
      ```
      ```
   c) Run the following command to grant executable permissions to the PHP-FPM startup script:
      ```
      chmod +x /etc/init.d/php-fpm
      ```
   d) Run the following commands in sequence to add PHP-FPM to the service management list and enable it to run at system startup:
      ```
      chkconfig --add php-fpm
      chkconfig --list php-fpm
      chkconfig php-fpm on
      ```
4. Run the following command to start PHP-FPM:
   ```
   service php-fpm start
   ```
5. Add the NGINX support for FastCGI.
   a) Run the following command to back up the default NGINX configuration file:
      ```
      cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.bak
      ```
   b) Run the following command to add the NGINX configuration file:
      ```
      cp /etc/nginx/nginx.conf.default /etc/nginx/nginx.conf
      ```
   c) Run the `vi /etc/nginx/nginx.conf` command to open the NGINX configuration file.
   d) Press the I key, and add a homepage in the PHP format to the supported homepages.
Example:

```
location / {
    root /usr/local/nginx/html;
    index index.php index.html index.htm;
}
```

e) Delete the annotation character in front of the following content:

```
location ~ \..php$ {
    root html;
    fastcgi_pass 127.0.0.1:9000;
    fastcgi_index index.php;
    fastcgi_param SCRIPT_FILENAME /scripts$fastcgi_script_name;
    include fastcgi_params;
}
```

f) Change `root html;` to `root /usr/local/nginx/html;`.

g) Change `fastcgi_param SCRIPT_FILENAME /scripts$fastcgi_script_name;` to `fastcgi_param SCRIPT_FILENAME /usr/local/nginx/html/$fastcgi_script_name;`.

h) Press the Esc key, enter :wq, and then press the Enter key to save and close the NGINX configuration file.

6. Run the service nginx reload command to reload the NGINX configuration file.

7. Modify the index.php file.


   b) Press the I key and enter the following content:

```
<?php
    $conn=mysql_connect('127.0.0.1','root','');
    if ($conn){
        echo "LNMP platform connect to mysql is successful!" ;
    }else{
        echo "LNMP platform connect to mysql is failed!" ;
    }
    phpinfo();
?>
```

c) Press the Esc key, enter :wq, and then press the Enter key to save and close the index.php file.

**Step 5: Test the connection to the LNMP environment**

1. Log on to the ECS console.

2. In the left-side navigation pane, choose Instances & Images > Instances.

3. On the Instances page, find the target instance, and copy the public IP address of the instance from the IP Address column.
4. In the browser address bar, enter the IP address and press the Enter key.
The following response indicates that the LNMP environment is built.

<table>
<thead>
<tr>
<th>LNMP platform connect to mysql is successful!</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHP Version 5.6.23</td>
</tr>
<tr>
<td>System</td>
</tr>
<tr>
<td>Linux 3.10.01 #1 SMP Wed Dec 17 11:19:07</td>
</tr>
<tr>
<td>Build Date</td>
</tr>
<tr>
<td>Oct 31 2018 17:16:07</td>
</tr>
<tr>
<td>Configure Command</td>
</tr>
<tr>
<td>Server API</td>
</tr>
<tr>
<td>FPM/Passenger</td>
</tr>
<tr>
<td>Virtual Directory Support</td>
</tr>
<tr>
<td>disabled</td>
</tr>
<tr>
<td>Configuration File (php.ini) Path</td>
</tr>
<tr>
<td>/etc</td>
</tr>
<tr>
<td>Loaded Configuration File</td>
</tr>
<tr>
<td>/etc/php.ini</td>
</tr>
<tr>
<td>Scan this dir for additional ini files</td>
</tr>
<tr>
<td>/etc/php.d</td>
</tr>
</tbody>
</table>

2.2.3 Manually build an LNMP environment in CentOS 7

NGINX is a small and efficient web server software that can be used to build an LNMP web service environment. LNMP is an acronym of the names of its original four open-source components: the Linux operating system, NGINX web server, MySQL relational database management system, and PHP programming language. This topic describes how to manually build an LNMP environment on an ECS instance that runs the CentOS 7 operating system.

Prerequisites

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud official website.
- An ECS instance that runs the CentOS 7 operating system is created and assigned a public IP address. For information about how to create an ECS instance, see #unique_22.
An inbound rule is added to the security group of the ECS instance to allow traffic on port 80. For information about how to allow traffic on port 80, see #unique_16.

<table>
<thead>
<tr>
<th>Rule direction</th>
<th>Action</th>
<th>Protocol type</th>
<th>Port range</th>
<th>Priority</th>
<th>Authorized object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Allow</td>
<td>HTTP (80)</td>
<td>80/80</td>
<td>1</td>
<td>The public IP addresses of clients to be allowed to access the LNMP environment. Separate multiple IP addresses with commas (,). The value of 0.0.0.0/0 indicates that all IP addresses are allowed to access the LNMP environment.</td>
</tr>
</tbody>
</table>

**Context**

This topic is intended for individual users who are familiar with the Linux operating system, but new to using Alibaba Cloud ECS to build websites.

You can also purchase an LNMP image on Alibaba Cloud Marketplace and create an ECS instance from the image to build websites.

An ecs.c6.large instance with the following configurations is used as an example. The actual operation depends on your instance configurations.

- CPU: 2 vCPUs
- Memory: 4 GiB
- Network type: VPC
- IP address: public IP address

**Limits**

The procedure described in this topic is applicable to the following software versions:

- OS: public image for CentOS 7.2 64-bit
- NGINX 1.16.1
- MySQL 5.7.28
- PHP 7.0.33

**Note:**

If you use software versions different from the ones listed, you may need to adjust the commands and parameter settings as needed.
Procedure

Follow these steps to manually build an LNMP environment on an ECS instance:

• Step 1. Prepare the compilation environment
• Step 2. Install NGINX
• Step 3. Install MySQL
• Step 4. Install PHP
• Step 5. Configure NGINX
• Step 6. Configure MySQL
• Step 7. Configure PHP
• Step 8. Test the connection to the LNMP environment

Step 1. Prepare the compilation environment

1. Connect to a Linux instance.

2. Disable the firewall.
   a) Run the `systemctl status firewalld` command to check the status of the firewall.

```
[root@test -]# systemctl status firewalld
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2018-11-13 10:40:03 CST; 21s ago
     Docs: man:firewalld(1)
     Main PID: 20705 (firewalld)
```

• If the firewall is in the inactive state, the firewall is disabled.
• If the firewall is in the active state, the firewall is enabled. In this example, the firewall is in the active state. Therefore, you must disable the firewall.

b) Disable the firewall. Skip this step if the firewall is already disabled.

• To temporarily disable the firewall, run the `systemctl stop firewalld` command.

Note:
After you run this command, the firewall is temporarily disabled. It will enter the active state when you restart the Linux operating system.

• To permanently disable the firewall, run the `systemctl disable firewalld` command.

Note:
You can re-enable the firewall after it is disabled. For more information, visit the firewalld website.
   a) Run the `getenforce` command to check the status of SELinux.

   ```
   [root@test ~]# getenforce
   Enforcing
   ```

   - If SELinux is in the Disabled state, SELinux is disabled.
   - If SELinux is in the Enforcing state, SELinux is enabled. In this example, SELinux is in the Enforcing state. Therefore, you must disable SELinux.

   b) Disable SELinux. Skip this step if SELinux is already disabled.

   - To temporarily disable SELinux, run the `setenforce 0` command.

   ```
   Note:
   After you run this command, SELinux is temporarily disabled. It will enter the Enforcing state when you restart the Linux operating system.
   ```

   - To permanently disable SELinux, run the `vim /etc/selinux/config` command to edit the SELinux configuration file. Press the Enter key. Move the pointer to the SELINUX=enforcing row and press the I key to edit the configuration file. Change SELINUX=enforcing to SELINUX=disabled and press the Esc key. Enter :wq and press the Enter key to save and close the SELinux configuration file.

   ```
   Note:
   You can re-enable SELinux after it is disabled. For more information, see #unique_23.
   ```

   c) Restart the system to apply the settings.
Step 2. Install NGINX

1. Run the following command to install NGINX:

   `yum -y install nginx`

2. Run the following command to check the NGINX version:

   `nginx -v`

   The following command output indicates that NGINX is installed:

   `nginx version: nginx/1.16.1`

Step 3. Install MySQL

1. Run the following command to update the YUM repository:

   `rpm -Uvh http://dev.mysql.com/get/mysql57-community-release-el7-9.noarch.rpm`

2. Run the following command to install MySQL:

   `yum -y install mysql-community-server`

3. Run the following command to check the MySQL version:

   `mysql -V`

   The following command output indicates that MySQL is installed:

   `mysql Ver 14.14 Distrib 5.7.28, for Linux (x86_64) using EditLine wrapper`

4. Run the following command to start MySQL:

   `systemctl start mysqld`

5. Run the following command to enable MySQL to start upon system startup:

   `systemctl enable mysqld`  
   `systemctl daemon-reload`

Step 4. Install PHP

1. Update the YUM repository.
   a) Run the following commands to add the EPEL repository:

   `yum install`  
   `https://repo.ius.io/ius-release-el7.rpm`
Elastic Compute Service

Tutorials / 2 Build a software development environment

b) Run the following command to add the Webtatic repository:

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

2. Run the following command to install PHP:

```
yum -y install php70w-devel php70w-x86_64 php70w-cli.x86_64 php70w-common.x86_64 php70w-gd.x86_64 php70w-ldap.x86_64 php70w-mbstring.x86_64 php70w-mcrypt.x86_64 php70w-pdo.x86_64 php70w-mysqlnd php70w-fpm php70w-opcache php70w-pecl-redis php70w-pecl-mongodb
```

3. Run the following command to check the PHP version:

```
php -v
```

The following command output indicates that PHP is installed.

```
PHP 7.0.33 (cli) (built: Dec 6 2018 22:30:44) ( NTS )
Copyright (c) 1997-2017 The PHP Group
Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies
with Zend OPcache v7.0.33, Copyright (c) 1999-2017, by Zend Technologies
```

Step 5. Configure NGINX

1. Run the following command to back up the NGINX configuration file:

```
cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.bak
```

2. Modify the NGINX configuration file to add NGINX support for PHP.

```
# Retain the default values for all settings except the following settings:
location / {
    # Add the following information to the location braces to configure the
default homepage when the website is accessed.
    index index.php index.html index.htm;
}
# Add the following information to enable NGINX to process your PHP requests
# by using Fast Common Gateway Interface (FastCGI).
location ~ .php$ {
    root /usr/share/nginx/html;  # Replace /usr/share/nginx/html with the
    # Replace /usr/share/nginx/html with the
    # root directory of your website, which in this example is /usr/share/nginx/html.
```

38

Note:

If you do not add this configuration, PHP-based pages cannot be displayed when you access them through a browser.

a) Run the following command to open the NGINX configuration file:

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

b) Press the I key to enter the edit mode.

c) Add the following configuration information to the server braces:
fastcgi_pass 127.0.0.1:9000;  # NGINX forwards your PHP requests to PHP FastCGI Process Manager (PHP-FPM) through port 9000 of the ECS instance.
fastcgi_index index.php;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
include fastcgi_params;  # NGINX calls the FastCGI operation to process the PHP requests.
}

The configurations are as shown in the following figure.

d) Press the Esc key, enter :wq, and then press the Enter key to save and close the configuration file.
3. Run the following command to start NGINX:

```
systemctl start nginx
```

4. Run the following command to enable NGINX to start upon system startup:

```
systemctl enable nginx
```

**Step 6. Configure MySQL**

1. Run the following command to check the `/var/log/mysqld.log` file, and obtain and record the initial password of the root user:

```
grep 'temporary password' /var/log/mysqld.log
```

The command output is as follows:

```
2016-12-13T14:57:47.535748Z 1 [Note] A temporary password is generated for root@localhost: p0/G28g>lsHD
```

**Note:**
You must use this initial password to reset the password of the root user.

2. Run the following command to make security configurations for MySQL:

```
mysql_secure_installation
```

Follow these steps:

a) Reset the password of the root user.

```
Enter password for user root: # Enter the initial password that you obtained in the previous step.
The 'validate_password' plugin is installed on the server.
The subsequent steps will run with the existing configuration of the plugin.
Using existing password for root.
Estimated strength of the password: 100
Change the password for root ? (Press y|Y for Yes, any other key for No) : Y # Enter Y to change the password of the root user.
New password: # Enter a new password that is 8 to 30 characters in length. It must contain lowercase and uppercase letters, digits, and special characters. Special characters include ) ~ ! @ # $ % ^ & * - + = | {} [ ] : ; ' <> , . ? /
Re-enter new password: # Enter the new password again for confirmation.
Estimated strength of the password: 100
Do you wish to continue with the password provided?( Press y|Y for Yes, any other key for No) : Y
```

b) Enter Y to delete anonymous users.

```
By default, a MySQL installation has an anonymous user, allowing anyone to log into MySQL without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment.
Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y
```
c) Enter Y to deny remote access from the root user.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : Y
Success.

d) Enter Y to delete the test database and access permissions on this database.

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : Y
- Dropping test database...
Success.

e) Enter Y to reload privilege tables.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : Y
Success.
All done!

For more information, see MySQL documentation.

Step 7. Configure PHP

1. Create the phpinfo.php file to display the PHP information.

a) Run the following command to create the file:

vim <Website root directory>/phpinfo.php  # Replace <Website root directory> with your website root directory.

The website root directory is the root value within the location ~ .php$ braces that you configured in the nginx.conf file as shown in the following figure.

In this example, the website root directory is /usr/share/nginx/html. You can run the following command:

vim /usr/share/nginx/html/phpinfo.php

b) Press the I key to enter the edit mode.

c) Enter the following content:

<? php echo phpinfo(); ?>

d) Press the Esc key, enter :wq, and then press the Enter key to save and close the configuration file.
2. Run the following command to start PHP-FPM:

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

3. Run the following command to enable PHP-FPM to start upon system startup:

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

### Step 8. Test the connection to the LNMP environment

1. Open your browser.

2. In the address bar, enter `http://<Public IP address of the ECS instance>/phpinfo.php`.

The following response indicates that the LNMP environment is deployed.

![PHP Version 7.0.33](image)

#### What’s next

After you confirm that the LNMP environment has been deployed, we recommend that you run the following command to delete the `phpinfo.php` file to ensure system security:

```bash
rm -rf <Website root directory>/phpinfo.php  # Replace the <Website root directory> with the website root directory that you configured in the nginx.conf file.
```

In this example, the website root directory is `/usr/share/nginx/html`. You can run the following command:

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

### 2.3 Configure Java Web

#### 2.3.1 Manually deploy a Java web environment

This topic describes how to manually deploy a Java web environment on an ECS instance. This topic is applicable to individual users who are new to website construction on ECS instances.

**Prerequisites**
Elastic Compute Service  

Tutorials / 2 Build a software development environment

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud official website.
- To use ECS instances that are located in mainland China regions, make sure that you have completed real-name verification for your account.
- An ECS instance is created. For more information, see #unique_4.

Context

The following instance type and software versions are used in this topic. The versions may be different in your actual running environment.

- Instance type: ecs.c6.large
- Operating system: CentOS 7.4
- Tomcat: Tomcat 8.5.53

**Note:**
Tomcat 8.5.53 is used in this example. The source code is constantly upgraded and you can obtain the appropriate version.

- JDK: JDK 1.8.0_241
- FTP tool: WinSCP

Procedure

Take the following steps to manually deploy a Java web environment:

1. **Step 1: Download the source code**
2. **Step 2: Prepare for installation**
3. **Step 3: Install JDK**
4. **Step 4: Install Apache Tomcat**

**Step 1: Download the source code**

1. Click here to download Apache Tomcat.
2. Download JDK.
   a) Click here to download the JDK installation package.

**Note:**
If you run the `wget` command to download the JDK installation package to the ECS instance, an error occurs when you decompress the package. You can download the
b) Log on to the ECS console.

c) In the left-side navigation pane, choose **Instances & Images > Instances**.

d) Select the region where the ECS instance is deployed.

 e) On the **Instances** page, find the purchased instance, and view the public IP address of the instance in the **IP Address** column.

f) Connect to the Linux instance by using the corresponding public IP address in WinSCP.

g) Upload the downloaded Apache Tomcat and JDK installation packages to the root directory of the Linux instance.

**Step 2: Prepare for installation**

1. Add an inbound rule to the security group of the ECS instance to allow traffic on the required ports. For more information, see #unique_16.

   In this example, SSH port 22 and HTTP port 8080 are enabled.

2. Connect to the Linux instance. For more information, see #unique_15.

3. Disable the firewall.

   a) Run the **systemctl status firewalld** command to check the status of the firewall.

   ```
   [root@test ~]# systemctl status firewalld
   firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2018-11-13 10:40:03 CST; 21s ago
   Docs: man:firewalld(1)
   Main PID: 20705 (firewalld)
   ```

   • If the firewall is in the inactive state, the firewall is disabled.

   • If the firewall is in the active state, the firewall is enabled. In this example, the firewall is in the active state. Therefore, you must disable the firewall.

   b) Disable the firewall. If the firewall is in the inactive state, skip this step.

   • To temporarily disable the firewall, run the **systemctl stop firewalld** command.

**Note:**
After you run this command, the firewall is temporarily disabled. It enters the active state after you restart the instance next time.

• To permanently disable the firewall, run the `systemctl disable firewalld` command.

**Note:**
You can enable the firewall again. For more information, see Firewalld documentation.


   a) Run the `getenforce` command to check the status of SELinux.

   ```
   [root@test ~]# getenforce
   Enforcing
   ```

   • If the status of SELinux is Disabled, SELinux is disabled.
   • If the status of SELinux is Enforcing, SELinux is enabled. In this example, SELinux is in the Enforcing state. You must disable SELinux.

   b) Disable SELinux. If SELinux is in the Disabled state, skip this step.

   • To temporarily disable SELinux, run the `setenforce 0` command.

   **Note:**
   After you run this command, SELinux is temporarily disabled. It enters the enforcing state after you restart Linux next time.

   • To permanently disable SELinux, do as follows: Run the `vi /etc/selinux/config` command, edit the SELinux configuration file, and press Enter. Move your pointer to the line of SELINUX=enforcing and press `i` to enter the edit mode. Change SELINUX=enforcing to SELINUX=disabled and press Esc. Then, enter `:wq` and press Enter to save and close the SELinux configuration file.

   **Note:**
   You can enable SELinux again. For more information, see SELinux documentation.

   c) Restart the system to make the changes take effect.
5. Run the following command to create a standard user named www to run Tomcat:

```
useradd www
```

6. Run the following command to create a root directory for the Java web project:

```
mkdir -p /data/wwwroot/default
```

7. Upload the WAR package of Java web project files to the root directory and change the owner of files under the root directory to www.

   In this example, the following commands are run to create a Tomcat test page under the root directory and change the owner of files under the root directory to www.

```
echo Tomcat test > /data/wwwroot/default/index.jsp
chown -R www.www /data/wwwroot
```

**Step 3: Install JDK**

1. Run the following command to create a directory:

```
mkdir /usr/java
```

2. Run the following commands in sequence to grant executable permissions to jdk-8u241-linux-x64.tar.gz and decompress it to /usr/java:

```
chmod +x jdk-8u241-linux-x64.tar.gz
```
```
tar xzf jdk-8u241-linux-x64.tar.gz -C /usr/java
```

3. Set environment variables.

   a) Run the `vi /etc/profile` command to open the /etc/profile file.

   b) Press the `I` key to add the following content:

   ```
   # set java environment
   export JAVA_HOME=/usr/java/jdk1.8.0_241
   export CLASSPATH=$JAVA_HOME/lib/tools.jar:$JAVA_HOME/lib/dt.jar:$JAVA_HOME/lib
   export PATH=$JAVA_HOME/bin:$PATH
   ```

   c) Press the `Esc` key, enter `:wq`, and then press the Enter key to save and close the configuration file.

4. Run the `source /etc/profile` command to load environment variables.
5. Run the `java -version` command to check the JDK version.
   The following response indicates that JDK is installed.

```
[root@javaweb conf]# java -version
Java version "1.8.0_241"
Java(TM) SE Runtime Environment (build 1.8.0_241-b07)
Java HotSpot(TM) 64-Bit Server VM (build 25.241-b07, mixed mode)
```

Step 4: Install Apache Tomcat

1. Run the following commands in sequence:
   a. Decompress `apache-tomcat-8.5.53.tar.gz`.

```
tar xzf apache-tomcat-8.5.53.tar.gz
```

   b. Rename the Tomcat directory.

```
mv apache-tomcat-8.5.53 /usr/local/tomcat/
```

   c. Configure the owner of the file.

```
chown -R www.www /usr/local/tomcat/
```

The `/usr/local/tomcat/` directory contains the following subdirectories:

- bin: stores some Tomcat script files, such as scripts used to enable and disable the Tomcat service.
- conf: stores various global configuration files of the Tomcat server, among which `server.xml` and `web.xml` are the most important files.
- webapps: the main web publishing directory of Tomcat. It stores web application files by default.
- logs: stores Tomcat operation log files.
2. Configure the server.xml file.
   a) Run the following command to switch to the /usr/local/tomcat/conf/ directory:

   ```bash
   cd /usr/local/tomcat/conf/
   ```

   b) Run the following command to rename the server.xml file:

   ```bash
   mv server.xml server.xml_bk
   ```

   c) Create a server.xml file.

   **A.** Run the `vi server.xml` command to create a server.xml file.

   **B.** Press the I key to add the following content:

   ```xml
   <?xml version="1.0" encoding="UTF-8"?>
   <Server port="8006" shutdown="SHUTDOWN">
   <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener"/>
   <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener"/>
   <Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener"/>
   <Listener className="org.apache.catalina.core.AprLifecycleListener"/>
   <GlobalNamingResources>
   <Resource name="UserDatabase" auth="Container" type="org.apache.catalina.users.MemoryUserDatabaseFactory" description="User database that can be updated and saved" factory="org.apache.catalina.users.MemoryUserDatabaseFactory" pathname="conf/tomcat-users.xml"/>
   </GlobalNamingResources>
   <Service name="Catalina">
   <Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443" maxThreads="1000" minSpareThreads="20" acceptCount="1000" maxHttpHeaderSize="65536" debug="0" disableUploadTimeout="true" useBodyEncodingForURI="true" enableLookups="false" URIEncoding="UTF-8"/>
   <Engine name="Catalina" defaultHost="localhost">
   <Realm className="org.apache.catalina.realm.LockOutRealm">
   <Realm className="org.apache.catalina.realm.UserDatabaseRealm" resourceName="UserDatabase"/>
   </Realm>
   <Host name="localhost" appBase="/data/wwwroot/default" unpackWARs="true" autoDeploy="true">
   <Context path="/" docBase="/data/wwwroot/default" debug="0" reloadable="false" crossContext="true"/>
   <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs" prefix="localhost_access_log." suffix=".txt" pattern="%h %l %u %t &quot;%r&quot; %s %b"/>
   </Host>
   </Engine>
   ```
C. Press the Esc key, enter :wq, and then press the Enter key to save and close the configuration file.

3. Configure the Java Virtual Machine (JVM) memory parameters.

   a) Run the vi /usr/local/tomcat/bin/setenv.sh command to create a file named /usr/local/tomcat/bin/setenv.sh.

   b) Press the I key to add the following content:

   ```
   JAVA_OPTS='-Djava.security.egd=file:/dev/./urandom -server -Xms256m -Xmx496m -Dfile.encoding=UTF-8'
   ```

   c) Press the Esc key, enter :wq, and then press the Enter key to save and close the configuration file.

4. Configure a script to enable Tomcat to run at startup.

   a) Run the following command to download the Tomcat startup script.

   ```
   Note:
   The script originates from the community and is for reference only. Alibaba Cloud does not make any guarantee, express or implied, with respect to the performance and reliability of the script, as well as potential impacts of operations on the script.
   ```

   ```
   ```

   b) Run the following command to rename Tomcat-init:

   ```
   mv Tomcat-init /etc/init.d/tomcat
   ```

   c) Run the following command to grant executable permissions to the /etc/init.d/tomcat file:

   ```
   chmod +x /etc/init.d/tomcat
   ```

   d) Run the following command to set the JAVA_HOME script for automatic startup.

   ```
   Notice:
   ```
The JDK version in the script must be the same as that you installed. Otherwise, Tomcat fails to start.

```
sed -i 's@^export JAVA_HOME=.*@export JAVA_HOME=/usr/java/jdk1.8.0_241@' /etc/init.d/tomcat
```

5. Run the following commands to enable Tomcat to run at startup:

```
chkconfig --add tomcat
chkconfig tomcat on
```

6. Run the following command to start Tomcat:

```
service tomcat start
```

7. Open your browser and enter a URL in the http://<Public IP address of the ECS instance>:8080 format in the address bar to connect to the ECS instance. The following response indicates that Tomcat is installed.

```
[ ] [ ] [ ] [ ]
 1:8080
```

**Tomcat test**

---

**What's next**

When Tomcat becomes available, we recommend that you configure websites on the instance and map domain names to the public IP address of the instance.

### 2.3.2 Use Cloud Toolkit to deploy a Java web environment

Alibaba Cloud Toolkit for Eclipse (Cloud Toolkit) is a free plug-in used for the integrated development environment (IDE). After you develop, debug, and test an application on a local server, you can use this plug-in to deploy the application to an ECS instance.

**Prerequisites**

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud official website.
- Java Development Kit (JDK) 1.8 or later is downloaded and installed.
- Eclipse IDE 4.5.0 or later is downloaded and installed. The program is suitable for Java Enterprise Edition (Java EE) developers.
• An AccessKey pair is created. For more information, see Create an AccessKey pair.
• An ECS instance is created. In this topic, a Linux instance is used as an example.
• A security group in a VPC is created and inbound rules are added to the security group to allow access from ports 21, 22, and 80. For more information, see #unique_16.
• WinSCP or other tools are installed to establish a remote connection to Linux.

Context

This topic describes how to install Cloud Toolkit in Eclipse in your local server that uses the Windows operating system and use Cloud Toolkit to deploy a Java application to an instance.

Procedure

To deploy a Java application to an ECS instance by using Cloud Toolkit, follow these steps:

1. Step 1: Install Cloud Toolkit
2. Step 2: Set the AccessKey pair
3. Step 3: Download and upload the JDK installation package
4. Step 4: Prepare for installation
5. Step 5: Install JDK
6. Step 6: Install Apache Tomcat
7. Step 7: Deploy a Java application to the ECS instance

Step 1: Install Cloud Toolkit

To install Cloud Toolkit in Windows, follow these steps:

1. Start Eclipse.
2. On the toolbar, choose **Help > Install New Software**....

3. Click **Add...** in the dialog box that appears.

4. Enter a name such as Cloud Toolkit for Eclipse, enter the http://toolkit.aliyun.com/eclipse software location, and click **Add**.
5. In the Name column, select Alibaba Cloud Toolkit Core and Alibaba Cloud Toolkit Deployment Tools, clear Contact all update sites during install to find required software in the Details section, and click Next.

![Image of the installation window showing selected software and options]

6. Click Next.

7. Select I accept the terms of the license agreement and click Finish.

8. Click Install anyway.
9. Click **Restart Now** to restart Eclipse.

![Restart Now](image)

**Step 2: Set the AccessKey pair**

An AccessKey ID is used to identify a user. An AccessKey secret is used to encrypt the signature string and is the key that the server uses to authenticate the signature string. The AccessKey secret must be kept confidential.

To set the AccessKey ID and AccessKey secret, follow these steps:

1. On the toolbar, choose **Window > Preferences**.

2. In the left-side navigation pane, choose **Alibaba Cloud Toolkit > Accounts**.
3. Set **Access Key ID** and **Access Key secret**, and click **Apply and Close**.

### Step 3: Download and upload the JDK installation package

To download and upload the JDK installation package, follow these steps:

1. Download **Apache Tomcat**.

   **Note:**
   The source code is constantly upgraded and you can obtain the appropriate version as needed.

2. Download the **JDK installation package**.

   **Note:**
   If you download a JDK installation package to a Linux instance, an error will occur when you decompress the package. You can download a JDK installation package for Linux to your computer and then upload it to the instance.

3. Log on to the **ECS console**.

4. In the left-side navigation pane, choose **Instances & Images > Images**.
5. In the top navigation bar, select a region.

6. Find the target instance on the Instances page, and obtain the public IP address of the instance from the **IP Address** column.

7. Start WinSCP, use the public IP address to connect to the Linux instance, and upload the JDK installation package to the root directory of the Linux instance.

**Step 4: Prepare for installation**

To prepare for installation, follow these steps:

1. Establish a remote connection to the ECS instance. For more information, see #unique_15.

2. Disable the firewall.
   a) Run the `systemctl status firewalld` command to check the status of the firewall.

   ```
   [root@test ~]# systemctl status firewalld
   firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor provided)
   Active: active (running) since Tue 2018-11-13 10:40:03 CST; 21s ago
   Docs: man:firewalld(1)
   Main PID: 20765 (firewalld)
   ```

   - If the firewall is in the inactive state, the firewall is disabled.
   - If the firewall is in the active state, the firewall is enabled. In this example, the firewall is in the active state, so you need to disable the firewall.

   b) Disable the firewall. Skip this step if the firewall is in the inactive state.

   - To temporarily disable the firewall, run the `systemctl stop firewalld` command.

   ```
   Note:
   The firewall is temporarily disabled, and will enter the active state when you restart the Linux operating system next time.
   ```

   - To permanently disable the firewall, run the `systemctl disable firewalld` command.

   ```
   Note:
   You can enable the firewall again. For more information, visit the firewalld.
   ```
3. Disable SELinux.
   a) Run the `getenforce` command to check the status of SELinux.

   ```
   [root@test ~]# getenforce
   Enforcing
   ```

   • If SELinux is in the Disabled state, SELinux is disabled.
   • If SELinux is in the Enforcing state, SELinux is enabled. In this example, SELinux is in the Enforcing state, so you need to disable SELinux.

   b) Disable SELinux. Skip this step if SELinux is in the Disabled state.

   • To temporarily disable SELinux, run the `setenforce 0` command.

   **Note:**
   SELinux is temporarily disabled, and will enter the Enforcing state when you restart the Linux operating system next time.

   • To permanently disable SELinux, run the `vi /etc/selinux/config` command and press the Enter key. Move the pointer over the line of SELINUX=enforcing, and press the I key to enter the edit mode. Change the SELinux state to Disabled. After that, press the Esc key, enter :wq, and press the Enter key to save and close the SELinux configuration file.

   **Note:**
   You can enable SELinux again. For more information, visit the Introduction to SELinux.

   c) Restart the system for the changes to take effect.

4. Create a user named www to run Tomcat.

   ```
   useradd www
   ```

5. Create a root directory for the Java web project.

   ```
   mkdir -p /data/wwwroot/default
   ```

6. Grant the file permission under the root directory of the website to www.

   ```
   chown -R www.www /data/wwwroot
   ```

**Step 5: Install JDK**

To install JDK, follow these steps in the instance:
1. Create a directory.

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

2. Decompress the JDK installation package that is jdk-8u191-linux-x64.tar.gz in this example to /usr/java.

```bash
chmod +x jdk-8u191-linux-x64.tar.gz
```

```bash
tar xzf jdk-8u191-linux-x64.tar.gz -C /usr/java
```

3. Configure environment variables.

   a) Run the `vi /etc/profile` command to open the /etc/profile file.

   b) Press the I key to enter the edit mode.

   c) Add the following lines into the /etc/profile file:

   ```bash
   # set java environment
   export JAVA_HOME=/usr/java/jdk1.8.0_191
   export CLASSPATH=$JAVA_HOME/lib/tools.jar:$JAVA_HOME/lib/dt.jar:$JAVA_HOME/lib
   export PATH=$JAVA_HOME/bin:$PATH
   ```

   d) Press the Esc key to exit the edit mode and enter :wq to save and close the file.

4. Run the `source /etc/profile` command to load environment variables.

5. Run the `java -version` command to check the JDK version.

If the JDK version information is returned as follows, JDK is installed.

```
[root@test ~]# java -version
java version "1.8.0_191"
Java(TM) SE Runtime Environment (build 1.8.0_191-b12)
Java HotSpot(TM) 64-Bit Server VM (build 25.191-b12, mixed mode)
```

**Step 6: Install Apache Tomcat**

To install Apache Tomcat, follow these steps in the instance:

1. Run the following commands in sequence to decompress the apache-tomcat-8.5.34.tar.gz package, rename the Tomcat directory, and configure user permissions:

```bash
tar xzf apache-tomcat-8.5.34.tar.gz
mv apache-tomcat-8.5.34 /usr/local/tomcat/
```
The `/usr/local/tomcat/` directory contains the following files:

- **bin**: stores some Tomcat script files, including scripts used to enable and disable the Tomcat service.
- **conf**: stores global configuration files for the Tomcat server, including the important files `server.xml` and `web.xml`.
- **webapps**: the main web publishing directory of Tomcat and stores web application files by default.
- **logs**: stores Tomcat log files.

2. Configure the `server.xml` file.

   a) Run the `cd /usr/local/tomcat/conf/` command to switch to the `/usr/local/tomcat/conf/` directory.

   b) Run the `mv server.xml server.xml_bk` command to rename the `server.xml` file.

   c) Run the `vi server.xml` command to open the file.

   d) Press the I key to enter the edit mode.

   e) Add the following code:

```
<?xml version="1.0" encoding="UTF-8"?>
<Server port="8006" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener"/>
  <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener"/>
  <Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener"/>
  <Listener className="org.apache.catalina.core.AprLifecycleListener"/>
  <GlobalNamingResources>
    <Resource name="UserDatabase" auth="Container" type="org.apache.catalina.users.MemoryUserDatabaseFactory" pathname="conf/tomcat-users.xml"/>
  </GlobalNamingResources>
  <Service name="Catalina">
    <Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443" maxThreads="1000" minSpareThreads="20" acceptCount="1000" maxHttpHeaderSize="65536" debug="0" disableUploadTimeout="true" useBodyEncodingForURI="true" enableLookups="false" URIEncoding="UTF-8"/>
    <Engine name="Catalina" defaultHost="localhost">
      <Realm className="org.apache.catalina.realm.LockOutRealm">
```

[Issue: 20200628]
f) Press the Esc key to exit the edit mode, enter :wq, and press the Enter key to save and close the file.

   a) Run the `vi /usr/local/tomcat/bin/setenv.sh` command to create a file named `/usr/local/tomcat/bin/setenv.sh`.
   b) Press the I key to enter the edit mode.
   c) Add the following code:
      ```bash
      JAVA_OPTS='-Djava.security.egd=file:/dev/./urandom -server -Xms256m -Xmx496m -Dfile.encoding=UTF-8'
      ```
   d) Press the Esc key to exit the edit mode, enter :wq, and press Enter to save and close the file.

4. Configure a script to run Tomcat at system startup.
   a) Run the `wget https://github.com/lj2007331/oneinstack/raw/master/init.d/Tomcat-init` command to download the script.
   b) Run the `mv Tomcat-init /etc/init.d/tomcat` command to rename the downloaded Tomcat-init file.
   c) Run the `chmod +x /etc/init.d/tomcat` command to assign the executable permission to the script file.
   d) Run the following command to set the JAVA_HOME startup script:

   ```bash
   Notice:
   ```
The JDK version information in the script must be the same as that of the JDK version you installed. Otherwise, Tomcat will fail to start.

```
sed -i 's@^export JAVA_HOME=.*@export JAVA_HOME=/usr/java/jdk1.8.0_191@' /etc/init.d/tomcat
```

5. Configure Tomcat to automatically start at system startup.

```
chkconfig --add tomcat
chkconfig tomcat on
```


```
service tomcat start
```

**Step 7: Deploy a Java application to the ECS instance**

You can use Cloud Toolkit to deploy a Java application to the ECS instance. Then, Tomcat test is displayed when you visit http://Public IP address of the ECS instance:8080. Follow these steps:
1. In Eclipse, right-click the name of the application project that you want to deploy, and choose Alibaba Cloud > Deploy to ECS... from the shortcut menu.

2. In the Deploy to Alibaba Cloud dialog box that appears, complete the following settings:

   - **Deploy File**: Select a deployment method. Select Upload File in this example. If you build the application project by using Maven, select Maven Build.
   - **Choose File**: Select the file that you want to deploy.
   - **Target Deploy ECS**: Specify the region where your instance is located and select an instance.
   - **Deploy Location**: Enter the directory that you deployed on the ECS instance, such as /data/wwwroot/default in this example.
   - **Command**: Click Select... and click Add... in the dialog box that appears. Enter a command in the field. The ECS instance runs the command automatically after Cloud Toolkit deploys the Java application to the directory on the ECS instance.
example, enter the `service tomcat restart` command to restart Tomcat. You can also enter other commands as needed.

3. Click **Deploy** to start deploying the Java application to the ECS instance.
4. In the **Console** section of Eclipse, view the progress of the deployment.

![Console output](image)

5. Open your browser and enter the `http://Public IP address of the ECS instance:8080` URL in the address bar to connect to the ECS instance.

If the page in the following figure is displayed, the Java application is deployed to the ECS instance by using the Alibaba Cloud Toolkit for Eclipse plug-in.

![Browser output](image)

**What's next**

You can modify the Java application in Eclipse, save the code, and use Cloud Toolkit to deploy the modified file to the ECS instance.

### 2.4 Deploy Windows by changing the image

You can deploy Windows on the ECS instance by using an image that integrates the OS and applications. This topic describes how to deploy Windows on an ECS instance by changing its image.

**Prerequisites**

An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud official website.

**Context**
You can deploy the application environment on an ECS instance manually or by using an image from Alibaba Cloud Marketplace based on your business needs. Images in Alibaba Cloud Marketplace integrate the OS and applications. We recommend that you use images from the Marketplace to deploy Windows.

You can select Windows images from Alibaba Cloud Marketplace to create ECS instances. For more information, see Create an instance. You can also switch the existing operating system of an ECS instance by changing the system disk to an image in Alibaba Cloud Marketplace. The procedure in the tutorial applies to existing ECS instances. You can deploy Windows by changing images from Alibaba Cloud Marketplace. The tutorial only describes the general procedure for using an Alibaba Cloud Marketplace image. An image software installation package generally includes an operation guide. For more information about installation and configuration, see Image Operation Guide.

**Note:**

- You cannot install or deploy virtualization software such as KVM, Xen, and VMware on ECS.
- When the system disk of an ECS instance is changed, its data disk is not affected. We recommend that you back up your personal data on the system disk to the data disk or elsewhere by using other methods.
- When the system disk of an ECS instance is changed, all data on the system disk is deleted. Automatic snapshots backed up by ECS might also be deleted depending on your settings. For more information, see Delete automatic snapshots when releasing a disk. Ensure that you have backed up your data before changing the system disk.
- The IP address of the ECS instance remains unchanged even when the system disk is changed.

**Procedure**

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Instances & Images > Instances.
3. Change the system disk of the ECS instance.
   
   a) In the **Actions** column of the **Instances** page, choose **More > Replace System Disk**.
   
   b) In the **Replace System Disk** dialog box that appears, click **OK**.

   c) In the **Image Type** section, select **Marketplace Image**, and click **Select from image market (including operating system)**.

   d) In the left-side navigation pane, select Image Category or enter the image that you want to use and click **Search**. Select the target image and click **Apply**.

   e) Set the logon password for the ECS instance. Enter the password in the **Login Password** field and enter the password again in the **Confirm Password** field.

   f) In the lower-right corner of the **Replace System Disk** page, select ECS Terms of Service and Image Product Terms of Use and click **Confirm to Change**.

**Result**

When the message **The system disk has been replaced** is displayed, the operating system of your ECS instance is successfully replaced with the Alibaba Cloud Marketplace image. Click **Back to Instance List** to return to the **Instances** page. After you log on to the ECS instance, you can use its application environment.
2.5 Deploy a Node.js project on CentOS

This topic describes how to install Node.js and deploy a project on an ECS instance that runs CentOS 7.2.

Prerequisites

- You have installed PuTTY on the computer that you use for connecting to the ECS instance. You can click here to download PuTTY.
- An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud official website.

Context

Node.js is a JavaScript runtime built on Chrome V8 engine. You can use Node.js to efficiently build an online application that supports easy extension. Node.js uses an event-driven and non-blocking I/O model. This lightweight and efficient model is suitable for data-intensive real-time applications that run on distributed devices. The Node.js package manager (npm) is the largest ecosystem of open source libraries in the world. Node.js is applicable to the following typical scenarios:

- Real-time applications: instant messaging and real-time notifications, such as Socket.IO.
- Distributed applications: efficient parallel I/O to consume existing data.
- Utilities: a variety of utilities from front-end compression and deployment applications such as grunt to desktop graphical user interface applications.
- Game applications: real-time and high-concurrency applications in the game field, such as the Pomelo framework of NetEase.
- Stable functions to improve the performance of rendering Web pages.
- Consistent front-end and back-end programming environments: applications that allow front-end developers to easily take on server-side development, such as the full-stack Javascript MongoDB, Express.js, AngularJS, and Node.js. (MEAN) framework.
Procedure

To install Node.js on an ECS instance and deploy a project, follow these steps:

1. **Step 1: Create and connect to an ECS instance**
2. **Step 2: Deploy the Node.js environment**
3. **Step 3: Deploy a test project**

**Step 1: Create and connect to an ECS instance**

To create and connect to an ECS instance, follow these steps:

1. Use the public image 64-bit CentOS 7.2 to create an ECS instance. For more information, see [Create an ECS instance](#).
2. Use the root user to connect to the ECS instance. For more information, see #unique_31.

**Step 2: Deploy the Node.js environment**

Deploy the Node.js environment in any of the following ways:

- Use a binary file to install the Node.js environment

  The installation package used in the deployment is a compiled binary file. After you decompress the package, the node and npm files already exist in the bin folder, so you do not need to recompile the binary file.

To deploy the Node.js environment by using the binary file, follow these steps:

1. Download the Node.js installation package.
   
   ```
   wget https://nodejs.org/dist/v6.9.5/node-v6.9.5-linux-x64.tar.xz
   ```

2. Decompress the file.
   
   ```
   tar xvf node-v6.9.5-linux-x64.tar.xz
   ```

3. After you create a soft link, you can run node and npm commands directly in any directory.
   
   ```
   ln -s /root/node-v6.9.5-linux-x64/bin/node /usr/local/bin/node
   ln -s /root/node-v6.9.5-linux-x64/bin/npm /usr/local/bin/npm
   ```

4. Check the versions of node and npm.
   
   ```
   node -v
   ```
npm -v

Then, the Node.js environment has been installed. By default, the software is installed in the directory `/root/node-v6.9.5-linux-x64/`.

5. To install the software in another directory such as `/opt/node/`, run the following commands in sequence:

```bash
mkdir -p /opt/node/
mv /root/node-v6.9.5-linux-x64/* /opt/node/
rm -f /usr/local/bin/node
rm -f /usr/local/bin/npm
ln -s /opt/node/bin/node /usr/local/bin/node
ln -s /opt/node/bin/npm /usr/local/bin/npm
```

- Use NVM to install multiple versions

Node Version Manager (NVM) is the software used to manage Node.js versions. You can use NVM to easily switch Node.js versions. NVM is suitable for developers that are dedicated to Node.js or that need to efficiently update or switch Node.js versions.

To install multiple Node.js versions by using NVM, follow these steps:

1. Use Git to clone source code to the local directory `~/.nvm`, and check the latest update.

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

2. Activate NVM.

```bash
echo ". ~/.nvm/nvm.sh" >> /etc/profile
source /etc/profile
```

3. Retrieve a list of all Node.js versions.

```bash
nvm list-remote
```

4. Install multiple Node.js versions.

```bash
nvm install v6.9.5
nvm install v7.4.0
```

5. Run the `nvm ls` command to check the version of the installed Node.js environment.

Node.js v7.4.0 is installed in this example. The response is as follows:

```
[root@iZXXXXZ .nvm]# nvm ls
v6.9.5
  -> v7.4.0
system
stable -> 7.4 (-> v7.4.0) (default)
```
unstable -> 6.9 (-> v6.9.5) (default)

6. Run the command `nvm use v7.4.0` to switch to Node.js v7.4.0. The response is as follows:

```
[root@iZXXXXZ .nvm]# nvm use v7.4.0
Now using node v7.4.0
```

**Step 3: Deploy a test project**

To deploy a test project, follow these steps:

1. Create the `example.js` project file.

   ```
   cd ~
   touch example.js
   ```

2. Use the `vim` editor to open the `example.js` project file.

   ```
   yum install vim
   vim example.js
   ```

   Press the `i` key to enter the edit mode, and copy the following code to the project file. Afterward, press the `Esc` key to exit the edit mode. Type `:wq` and press the `Enter` key to save and close the file.

   The code that you copy to the project file is as follows:

   ```
   const http = require('http');
   const hostname = '0.0.0.0';
   const port = 3000;
   const server = http.createServer((req, res) => {
     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}/`);
   });
   ```

   **Note:**

   In this example, you specify Port 3000 as the service port. You can also specify another port in your actual running environment. However, you must add an inbound rule to the security group of the ECS instance to support the specified port.
3. Run the project.

```
node ~/example.js &
```

4. Run the following command to check whether the deployed application is listening on the specified port.

```
netstat -tulpn
```

In this example, the response contains Port 3000, indicating that the application is listening on the port.

5. Log on to the ECS console, and add an inbound rule to the security group of the ECS instance to support the specified port, such as Port 3000 in this example.

For more information about how to add security group rules, see #unique_16.

6. Open your local browser, and in the address bar, enter the URL `http://<Public IP address of the ECS instance>:Port number` to access the project.

```
Hello World
```

Related topics
- Alibaba Cloud sandbox platform
- Alibaba Cloud Marketplace
3 Build a website

3.1 Build a WordPress blog platform

3.1.1 Build a WordPress website on a CentOS 7 ECS instance

WordPress is a blog-publishing system written in PHP. You can use WordPress to build your own websites on servers supporting PHP and MySQL databases or use WordPress as a content management system (CMS). This topic describes how to build a WordPress website on an ECS instance that is running the Linux operating system.

Prerequisites

- You must have registered an Alibaba Cloud account. If not, create a new Alibaba Cloud account first.
- A security group of the VPC type is created. Inbound rules are added for the security group to allow traffic from port 80. If you want to remotely connect to the Linux instance by using SSH, traffic from port 22 is allowed. For more information about how to add security group rules, see #unique_16.
- A Linux ECS instance is created and deployed with the LNMP environment. For more information, see Manually build an LNMP environment in CentOS 7. This tutorial uses the following software versions:
  - Operating system: public image running CentOS 7.2 64-bit
  - NGINX: 1.16.1
  - MySQL: 5.7.29
  - PHP: 7.0.33
  - WordPress: 5.0.4

Note:

If you use software versions different from the preceding versions, you may need to adjust parameter settings based on your needs.

Context

The tutorial is intended for enterprises or individuals who are familiar with Linux, but new to building WordPress websites on Alibaba Cloud ECS instances. You can also use the
WordPress image provided in Alibaba Cloud Marketplace to quickly build a WordPress website.

Build a WordPress website

1. Use the ECS console to remotely connect to the ECS instance that is deployed with the LNMP environment and configure a database for the WordPress website.
   a) Remotely connect to the ECS instance.
      For more information, see #unique_31.
   b) Log on to the MySQL database.

```
mysql -uroot -p
```
   c) Create a database for the WordPress website that you want to build.

```
create database wordpress;
```
   d) Create a user.

```
create user 'user'@'localhost' identified by 'password123';
```
   e) Grant the user all permissions on the wordpress database.

```
grant all privileges on wordpress.* to 'user'@'localhost' identified by 'password123';
```
   f) Make the configuration take effect.

```
flush privileges;
```
   g) Exit MySQL.

```
exit;
```

2. Download WordPress.

Note:
If you download WordPress on an ECS instance located in mainland China, an error 429 Too Many Requests will be reported. We recommend that you try multiple times or download the WordPress installation package from a third-party website.

a) Go to the /usr/share/nginx/html/ directory.

```
cd /usr/share/nginx/html
```

b) Download WordPress.

```
wget https://cn.wordpress.org/wordpress-<Version information>.tar.gz
```

The version used in this tutorial is 5.0.4.

c) Decompress the WordPress installation package.


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

b) Edit the wp-config.php file.

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

c) Press i to switch to the edit mode and modify MySQL-related configurations based on the wordpress database. An example of the modification code is as follows:

```
// ** MySQL settings - The information is based on the host in use. ** //
/** WordPress database name */
define('DB_NAME', 'wordpress');

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

/** MySQL database password */
define('DB_PASSWORD', 'password123');

/** MySQL host */
define('DB_HOST', 'localhost');
```

d) After the modification is complete, press Esc, type :wq, and press Enter to save and close the configuration file.
   
a) Enter http://Publich IP address of the ECS instance/wordpress in the browser of your computer to enter the WordPress installation page.

b) Enter basic information of the WordPress website and click Run the installation.
   The parameters are described as follows:
   
   • Site Title: The name of the WordPress website. Example: demowp.
   • Username: The username used to log on to WordPress. Keep your username secure. Example: testwp.
   • Password: We recommend that you choose a secure password. Example: Wp.123456.
   • Your Email: The email used to receive notifications. Example: 1234567890@aliyun.com.

c) Click Install Wordpress.

d) Enter the username testwp and password Wp.123456 that are used to install WordPress and click LOGIN.

You have logged on to your WordPress website.

Resolve the domain name of the WordPress website

Accessing your WordPress website by using the public IP address of the ECS instance compromises the security of the ECS instance. If you have a domain name or want to register a domain name for the WordPress website, follow these steps. The domain name to register in this tutorial is www.WordPress.EcsQuickStart.com.

1. Register the domain name.
   
   For more information, see #unique_6.

2. Apply for an ICP filing.
   
   If the website your domain name points to is hosted on an ECS instance located in mainland China, you must apply for an ICP filing. see #unique_10.

3. Resolve the domain name and bind it to the public IP address of the ECS instance.
   
   Domain name resolution is necessary for you to access your website by using a domain name. For more information, see Domain name resolution.
4. Return to the ECS console, remotely connect to the ECS instance on which the WordPress website is deployed, and log on to the MySQL database.

   mysql -uroot -p

5. Use the wordpress database.

   use wordpress;

6. Replace the public IP address of the ECS instance with the new domain name.


7. Exit MySQL.

   exit;

The new domain name is configured for your WordPress website.

### 3.1.2 Build a WordPress website on a Windows ECS instance

This topic describes how to build a WordPress website on an ECS instance that is running the Windows operating system.

**Prerequisites**

- You must have registered an Alibaba Cloud account. If not, [create a new Alibaba Cloud account](#).
- A security group of the VPC type is created. Inbound rules are added for the security group to allow traffic from port 80 and port 3389. For more information about how to add security group rules, see #unique_16.
- A Windows ECS instance is created and deployed with the Web environment. This tutorial uses the following software versions:
  - Operating system: Windows Server 2012 R2 64-bit
  - Internet Information Services (IIS): 7.5
  - PHP: 7.0.28
  - MySQL: 5.7
  - WordPress: 5.3.2

**Note:**

If you use software versions different from the preceding versions, you may need to adjust parameter settings based on your needs.
Build a WordPress website

1. Use the ECS console to remotely connect to the ECS instance that is deployed with the Web environment and download the WordPress installation package.
   a) Remotely connect to the ECS instance.
      For more information, see #unique_15.
   b) Download the WordPress installation package from the official WordPress website.
      The version used in this tutorial is 5.3.2.

   **Note:**
   If you download WordPress on an ECS instance located in mainland China, error 429 Too Many Requests will be reported. We recommend that you try multiple times or download the WordPress installation package from a third-party website.

   c) Decompress the WordPress installation package.
      In this tutorial, the WordPress installation package is decompressed to C:\wordpress.
2. Create a MySQL database for the WordPress website that you want to build.
   a) Go to the bin folder of the MySQL installation directory, hold the Shift key and right-click a blank area in this folder, and select Open command window here.
   b) Log on to the MySQL database.
      ```bash
      mysql -u root -p
      ```
   c) Create a database for the WordPress website.
      In this tutorial, the database created for the WordPress website is wordpress.
      ```sql
      create database wordpress;
      ```

3. Configure the WordPress website.
   a) In the C:\wordpress directory, find the wp-config-sample.php file, copy it, and name the copied file wp-config.php.
   b) Use the text editor to open the wp-config.php file and modify information related to the wordpress database.
      The following figure shows an example.

```php
// ** 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', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'password123');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```
   c) Save the wp-config.php file.
4. Add the WordPress website to Server Manager.
   a) Find and open Server Manager in the Windows taskbar.
   
   ![Server Manager image]
   
   b) In the right-side navigation pane of Server Manager, choose **Tools > Internet Information Services (IIS) Manager**.

c) In the **Connections** pane, click **Sites** under the name of the ECS instance.

d) Delete the website that is bound to port 80, or change the port number from 80 to an unused port, such as port 8080.

   ![Internet Information Services (IIS) Manager image]

   e) In the right-side **Actions** pane, click **Add Website** to add the WordPress website.

   The following figure shows an example.
The parameters are described as follows:

- Site name: the name of a custom website. In this tutorial, enter `wordpress`.
- Application pool: Select `DefaultAppPool`.
- Physical path: the directory where the WordPress installation package is decompressed. In this tutorial, select `C:\wordpress`.
- Port: Set it to 80.
5. Install WordPress and log on to the WordPress website.
   a) Visit http://localhost/ from the ECS instance. The WordPress installation page is displayed.
   b) Enter basic information of the website and click Run the installation.
      The parameters are described as follows:
      • Site Title: The name of the WordPress website. Example: demowp.
      • Username: The username used to log on to WordPress. Keep your username secure. Example: testwp.
      • Password: We recommend that you choose a secure password. Example: Wp.123456.
      • Your Email: The email used to receive notifications. Example: 1234567890@aliyun.com.
   c) Click Install WordPress.
   d) Enter the username and password used to install WordPress and click LOGIN.
      You have logged on to your WordPress website.

Resolve the domain name of the WordPress website

Accessing your WordPress website by using the public IP address of the ECS instance compromises the security of the ECS instance. If you have a domain name or want to register a domain name for the WordPress website, follow these steps. The domain name to register in this tutorial is www.WordPress.EcsQuickStart.com.

1. Register the domain name.
   For more information, see #unique_6.

2. Apply for an ICP filing.
   If the website your domain name points to is hosted on an ECS instance located in mainland China, you must apply for an ICP filing. see #unique_10.

3. Resolve the domain name and bind it to the public IP address of the ECS instance.
   Domain name resolution is necessary for you to access your website by using a domain name. For more information, see Domain name resolution.

4. Return to the ECS instance on which the WordPress website is deployed. Go to the bin folder of the MySQL installation directory, hold the Shift key and right-click a blank area in this folder, and select Open command window here.
5. Log on to the MySQL database.

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

6. Use the wordpress database.

```
use wordpress;
```

7. Replace http://localhost/ with the new domain name.

```
```

The new domain name is configured for your WordPress website.

### 3.1.3 Create a WordPress environment by using ROS

Alibaba Cloud Resource Orchestration Service (ROS) allows you to use templates to create a group of Alibaba Cloud resources. The ROS template is a JSON file used to specify the resources that you want to create. This topic describes how to use ROS templates to create a WordPress environment based on ECS and ApsaraDB for RDS services.

**Prerequisites**

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the [Alibaba Cloud official website](https://www.aliyun.com/).
- The first time that you use the ROS service, you are prompted to activate this service. ROS is a free service. Therefore, you can activate ROS free of charge.

**Context**

ApsaraDB for RDS is a stable, reliable, and scalable online database service provided by Alibaba Cloud. ApsaraDB for RDS supports database engines such as MySQL, SQL Server, and PostgreSQL. It provides a complete set of solutions for scenarios such as disaster recovery, backup, restoration, monitoring, and migration, freeing you from database O&M. For more information, see [What is ApsaraDB for RDS?](https://www.aliyun.com/product/apsaraodb.html).

This topic describes how to create a WordPress environment by using the **Create a WordPress Environment Based on ECS and ApsaraDB for RDS** template.

**Procedure**

1. Log on to the [ROS console](https://ros.console.aliyun.com/).
2. Select the target template.
   
a) In the left-side navigation pane, choose Templates > Sample Templates.
   
   The common templates provided by ROS are displayed on the Sample Templates page.
   
b) Find the Create a WordPress Environment Based on ECS and ApsaraDB for RDS template.
   
c) Optional: Click View Details to check the template in JSON format.
   
The following table lists the top-level fields in the JSON file.

<table>
<thead>
<tr>
<th>Top-level field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;ROSTemplateFormatVersion&quot; : &quot;2015-09-01&quot;</td>
<td>Specifies the version of the template.</td>
</tr>
<tr>
<td>&quot;Parameters&quot; : {}</td>
<td>Specifies some parameters of the template.</td>
</tr>
<tr>
<td></td>
<td>In this example, this field specifies the default image ID and instance type.</td>
</tr>
<tr>
<td>&quot;Resources&quot; : {}</td>
<td>Specifies the resources that you can use the template to create.</td>
</tr>
<tr>
<td></td>
<td>In this example, this field declares that the resources to be created include an ECS instance and a security group. The properties of these resources are defined in the Parameters field.</td>
</tr>
<tr>
<td>&quot;Outputs&quot; : {}</td>
<td>Specifies the resource information that the stack generates after ROS creates the specified resources.</td>
</tr>
<tr>
<td></td>
<td>In this example, the stack generates the ECS instance ID, public IP address, and security group ID.</td>
</tr>
</tbody>
</table>

3. Click Create Stack.
4. Configure the parameters.
   a) In the top navigation bar, select a region.
   b) Configure the parameters in the stack template.

The following table describes the stack template parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack Name</td>
<td>The name of the stack. The stack name must be unique and cannot be modified after the stack is created.</td>
</tr>
<tr>
<td>VPC</td>
<td>VPC CIDR Block</td>
</tr>
<tr>
<td></td>
<td>The private CIDR block of the VPC.</td>
</tr>
<tr>
<td></td>
<td>For more information, see #unique_38.</td>
</tr>
<tr>
<td>VSwitch CIDR Block</td>
<td>The CIDR block of the VSwitch.</td>
</tr>
<tr>
<td></td>
<td>The CIDR block of the VSwitch must fall within the CIDR block of the VPC and cannot overlap with the CIDR block of an existing VSwitch. For more information, see #unique_38.</td>
</tr>
<tr>
<td>Zone ID</td>
<td>The zone ID of the resource that you want to create.</td>
</tr>
<tr>
<td>ECS</td>
<td>Instance Type</td>
</tr>
<tr>
<td></td>
<td>The ECS instance type that you want to select.</td>
</tr>
<tr>
<td></td>
<td>For more information about ECS instance types, see #unique_39.</td>
</tr>
<tr>
<td></td>
<td>Image ID</td>
</tr>
<tr>
<td></td>
<td>The ID of the image that ROS uses to create the ECS instance.</td>
</tr>
<tr>
<td></td>
<td>Instance Password</td>
</tr>
<tr>
<td></td>
<td>The logon password of the ECS instance.</td>
</tr>
<tr>
<td></td>
<td>The password must be 8 to 30 characters in length and must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters.</td>
</tr>
<tr>
<td></td>
<td>Special characters include ( ) ` ~ ! @ # $ % ^ &amp; * - _ + =</td>
</tr>
</tbody>
</table>

Note:
Passwords of Windows instances cannot start with a forward slash (/).
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RDS</strong></td>
<td><img src="image.jpg" alt="Image" /></td>
</tr>
<tr>
<td>DB Instance Class</td>
<td>The type of the ApsaraDB for RDS instance.</td>
</tr>
<tr>
<td>Database Engine Version</td>
<td>The database engine that you want to use.</td>
</tr>
<tr>
<td>DB Instance Storage</td>
<td>The storage capacity of the ApsaraDB for RDS instance.</td>
</tr>
<tr>
<td>DB Name</td>
<td>The name of the WordPress database.</td>
</tr>
<tr>
<td>DB Username</td>
<td>The username of the WordPress database.</td>
</tr>
<tr>
<td>DB Password</td>
<td>The password used to access the WordPress database.</td>
</tr>
<tr>
<td></td>
<td>The password must be 6 to 32 characters in length and consist of letters, digits, and underscores (_).</td>
</tr>
</tbody>
</table>

c) Click Next.

d) Configure stack parameters.

The following table describes the stack parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack Policy (Optional)</td>
<td>The stack policy.</td>
</tr>
<tr>
<td>Rollback on Failure</td>
<td>Specifies whether to roll back the stack if the stack creation fails.</td>
</tr>
<tr>
<td></td>
<td>* If you select <strong>Enabled</strong>, ROS will delete the created resources when an error such as creation timeout occurs during the creation process.</td>
</tr>
<tr>
<td></td>
<td>* If you select <strong>Disabled</strong>, ROS will not delete the created resources when any error such as creation timeout occurs during the creation process.</td>
</tr>
<tr>
<td>Timeout Period</td>
<td>The timeout period that is specified for the stack creation request. If ROS fails to create the specified resources within the period, the creation operation will time out.</td>
</tr>
</tbody>
</table>

e) Click Next.

f) Check whether the stack parameters are configured correctly.

5. Click **Create Stack**.
Result

In the left-side navigation pane, click **Stacks**. In the top navigation bar, select the region of your created stack from the drop-down list to view stack information such as the status. If the status of the stack is **Created**, the stack is created.

What’s next

Click the stack name to go to the stack details page. Click the following tabs to view information about the stack.

- **Stack Information**: displays the basic information of the stack, such as the status and timeout period.
- **Events**: records the operations that ROS performs during the stack creation. The causes of failed operations are also displayed in the list.
- **Resources**: displays all resources of the stack.
- **Template**: displays the original template of the stack.

### 3.2 Build a Drupal website

#### 3.2.1 Build a Drupal website based on an Alibaba Cloud Marketplace image

This topic describes how to build a Drupal e-commerce website on an ECS instance based on an Alibaba Cloud Marketplace image.

**Prerequisites**

You must have registered an Alibaba Cloud account before you follow the instructions provided in the tutorial. If not, create a new Alibaba Cloud account first.

**Context**

Drupal is an open source content management framework (CMF) written in PHP. Drupal consists of a content management system (CMS) and a PHP development framework. You can use Drupal to build dynamic websites that provide various features and services. Drupal is commonly used in a variety of applications, from personal blogs to large communities.

The procedure described in this topic is applicable to users who are familiar with Linux, but new to web development on Alibaba Cloud ECS instances, and want to quickly build a website.
The following operating system and software versions are used in the example:

- Operating system: CentOS 7.3 64-bit
- Apache 2.4.45
- MySQL 5.6.36
- PHP 5.6.30
- Drupal 8.3.4

Procedure

To build a Drupal website based on an Alibaba Cloud Marketplace image, complete the following steps:

1. **Step 1. Create an ECS instance**
2. **Step 2. Select a Drupal website image**
3. **Step 3. Install Drupal**

**Step 1. Create an ECS instance**

Create an ECS instance to build a small-sized website for personal use. Then, you can upgrade the configurations of the instance or optimize the architecture to complete later development. An ECS instance of ecs.c6.large type is used in this example.

**Step 2. Select a Drupal website image**

1. Log on to the ECS console.
2. In the left-side navigation pane, choose *Instances & Images* > *Instances*.
3. In the top navigation bar, select a region.
4. On the *Instances* page, click *Create Instance*.
5. In the *Image* section of the *Custom Launch* tab, choose *Marketplace Image* > *Select from image market (including operating system)*.
6. Enter Drupal in the search bar, click *Search*, and select an image.
7. Click *Continue*.
8. On the *Custom Launch* tab, you can see that the Alibaba Cloud Marketplace image that you purchased is automatically selected in the *Image* section. Assign a public IP address to the instance and complete other settings to create the instance. For more information, see #unique_4.
Step 3. Install Drupal

1. Access http://the public IP address/phpMyAdmin through a local browser.
   
   You can obtain the public IP address of the instance from the instance list in the ECS console.

2. Use the username and password of MySQL provided by the Alibaba Cloud Marketplace image to log on to phpMyAdmin.

3. In the left-side navigation pane, click NEW. At the top of the page, click SQL.

4. Create a database and user for Drupal.
   
   Enter the following SQL statements in the field and configure the following parameters:
   
   - DrupalDBName: Specify a name for the database.
   - UserName: Specify the user for the database.
   - IP address: Specify localhost or 127.0.0.1 for a local host.
   - UserPassWord: Specify a password for the database.

```
CREATE DATABASE drupalDBName;
CREATE USER UserName;
GRANT ALL PRIVILEGES ON *. * TO 'UserName'@'IP' IDENTIFIED BY 'UserPassWord' WITH GRANT OPTION;
FLUSH PRIVILEGES;
```

5. Click Go.

6. Access http://the public IP address/drupal through a local browser to go to the Drupal installation page. Select the required language from the Choose language drop-down list, and then click Save and continue.

![Drupal 8.3.4](image)

7. Select the standard installation method and then click Save and continue.
8. Enter the information of the created database and then click **Save and continue**.

9. After the automatic installation is completed, enter the site information on the website settings page, and then click **Save and continue**.

After the installation is completed, you can log on to the Drupal website to customize the settings.

### 3.3 Build a Magento e-commerce website on ECS

Magento is an open source e-commerce platform. It is built on flexible modular architecture and extended features to provide premium solutions for large- and medium-sized websites. Magento supports PHP versions from 5.6 to 7.1. It uses MySQL databases to store data. This topic describes how to build a Magento e-commerce website on a CentOS 7 ECS instance.

**Prerequisites**

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the [Alibaba Cloud official website](https://www.alibabacloud.com).
• Inbound rules are added to the security group of the ECS instance and ports 80 and 3306 are allowed. For more information, see #unique_16.

\[ Table \]

<table>
<thead>
<tr>
<th>Rule direction</th>
<th>Action</th>
<th>Protocol type</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Allow</td>
<td>HTTP (80)</td>
<td>80/80</td>
<td>IPv4 CIDR block</td>
<td>The CIDR blocks containing the public IP addresses of all clients that need to access the Magento website. Separate multiple CIDR blocks with commas (,). To allow all clients to access the Magento website, authorize 0.0.0.0/0.</td>
</tr>
<tr>
<td>Inbound</td>
<td>Allow</td>
<td>MySQL (3306)</td>
<td>3306/3306</td>
<td>IPv4 CIDR block</td>
<td>The CIDR blocks containing the public IP addresses of all clients that need to access the MySQL database services. Separate multiple CIDR blocks with commas (,). To allow all clients to access the services, authorize 0.0.0.0/0.</td>
</tr>
</tbody>
</table>

\[ Context \]

The ECS instance used in this topic has the following configurations:

• Instance type: ecs.c6.large
• Operating system: public image CentOS 7.2 64-bit
• Number of vCPUs: 2
• Memory: 4 GiB

\[ Note: \]

Most clients reside within LANs and their private IP addresses are converted into public IP addresses when the clients access or are accessed by external devices. Therefore, the IP addresses returned by the `ipconfig` or the `ifconfig` command may not be the actual public IP addresses of the clients. If clients cannot access the Magento website after the Magento website is built, verify the public IP addresses of the clients.
If you want to build a Magento server, the memory of the selected instance type must be at least 2 GiB.

- Network type: VPC
- IP address: public IP address

The following software versions are used in the sample procedure:

- Apache HTTP Server 2.4.6
- MySQL 5.7
- PHP 7.0
- Composer 1.8.5
- Magento 2.1

If you use software versions different from the ones listed, you may need to adjust the commands and parameter settings.

**Procedure**

Complete the following steps to build a Magento e-commerce website on an Alibaba Cloud ECS instance:

- **Step 1. Install and configure Apache HTTP Server**
- **Step 2. Install and configure MySQL**
- **Step 3. Install and configure PHP**
- **Step 4. Create a Magento database**
- **Step 5. Install and configure Composer**
- **Step 6. Install and configure Magento**
- **Step 7. Configure the client of Magento**
- **Step 8. Add a cron job**
Step 1. Install and configure Apache HTTP Server

1. Install Apache HTTP Server.

   a) Run the following command to install Apache HTTP Server:

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

   b) Run the following command to check whether Apache HTTP Server is installed:

   ```bash
   httpd -v
   ```

   The following command output indicates that Apache HTTP Server is installed.

2. Configure Apache HTTP Server.

   a) Run the following command to open the configuration file of Apache HTTP Server:

   ```bash
   vim /etc/httpd/conf/httpd.conf
   ```

   b) Add `LoadModule rewrite_module modules/mod_rewrite.so` below `Include conf.modules.d/*.conf`. Complete the following steps:

   A. Move the pointer to the start of the line below the `Include conf.modules.d/*.conf` line.

   B. Press the I key to switch to the edit mode.

   C. Enter `LoadModule rewrite_module modules/mod_rewrite.so`.

   The following figure shows the added content.

   c) Replace `AllowOverride None` in the following content with `AllowOverride All`.

   ```sh
   # 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
   #
   # Add a number sign (#) at the beginning of the line to comment out this line.
   #AllowOverride None
   
   # Add the following content:
   ```
AllowOverride All

The following figure shows the replacement result.

```
AllowOverride None  # AllowOverride None
AllowOverride All   # AllowOverride All
```

d) Press the Esc key, enter :wq, and press the Enter key to save and close the configuration file.
3. Run the following command to start Apache HTTP Server:
   
   ```
   systemctl start httpd
   ```

4. Run the following command to configure Apache HTTP Server to run upon system startup:
   
   ```
   systemctl enable httpd
   ```

**Step 2. Install and configure MySQL**

1. Install MySQL.
   
   a) Run the following command to add a MySQL YUM repository:
   
   ```
   rpm -Uvh http://dev.mysql.com/get/mysql57-community-release-el7-8.noarch.rpm
   ```

   b) Run the following command to install MySQL:
   
   ```
   yum -y install mysql-community-server
   ```

2. Run the following command to start MySQL:
   
   ```
   systemctl start mysqld
   ```

3. Run the following command to configure MySQL to run upon system startup:
   
   ```
   systemctl enable mysqld
   ```

4. Configure MySQL.
   
   a) Run the following command to check the /var/log/mysqld.log file. Then, you can obtain and record the initial password of the root user.
   
   ```
   grep 'temporary password' /var/log/mysqld.log
   ```

   The following command output is returned:

   ```
   2016-12-13T14:57:47.535748Z 1 [Note] A temporary password is generated for root @localhost: p0/G28g>lsHD
   ```
You can use this initial password to reset the password of the root user in subsequent operations.

b) Run the following command to configure your MySQL databases and protect data:

```
mysql_secure_installation
```

Complete the following steps:

A. Set the password of the root user.

```
Enter password for user root: # Enter the initial password that you obtained in the previous step.
The 'validate_password' plugin is installed on the server.
The subsequent steps will run with the existing configuration of the plugin.
Using existing password for root.
Estimated strength of the password: 100
Change the password for root ? (Press y|Y for Yes, any other key for No): Y
New password: # Enter a new password. The password must be 8 to 30 characters in length and contain uppercase letters, lowercase letters, digits, and special characters. Special characters include ( ) ` ~ ! @ $ % ^ & * - + = | { } [ ] : ; '
< > , . ? /
Re-enter new password.
Estimated strength of the password: 100
Do you wish to continue with the password provided?( Press y|Y for Yes, any other key for No) : Y
```

B. Enter Y to delete anonymous users.

```
By default, a MySQL installation has an anonymous user, allowing anyone to log into MySQL without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment.
Remove anonymous users? (Press y|Y for Yes, any other key for No): Y
Success.
```

C. Enter Y to deny remote access by the root user.

```
Disallow root login remotely? (Press y|Y for Yes, any other key for No): Y
Success.
```

D. Enter Y to delete the test database and access permissions on this database.

```
Remove test database and access to it? (Press y|Y for Yes, any other key for No): Y
- Dropping test database...
Success.
```

E. Enter Y to reload privilege tables.

```
Reload privilege tables now? (Press y|Y for Yes, any other key for No): Y
Success.
All done!
```

For more information, visit MySQL documentation.
Step 3. Install and configure PHP

1. Installed PHP.
   a) Run the following command to add the IUS repository:

   ```
yum install \
https://repo.ius.io/ius-release-el7.rpm \
```

   b) Run the following command to add the Webtatic repository:

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

   c) Run the following command to install PHP 7 and all required extensions:

   ```
yum -y install php70w php70w-pdo php70w-mysqlnd php70w-opcache php70w-
-xml php70w-gd php70w-mcrypt php70w-devel php70w-intl php70w- mbstring
php70w-bcmath php70w-json php70w- iconv
```

   d) Run the following command to check the PHP version:

   ```
php -v
```

The following command output indicates that PHP is installed:

```
PHP 7.0.33 (cli) (built: Dec 6 2018 22:30:44) ( NTS )
Copyright (c) 1997-2017 The PHP Group
Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies
with Zend OPcache v7.0.33, Copyright (c) 1999-2017, by Zend Technologies
```

2. Configure PHP.
   a) Run the following command to open the PHP configuration file:

   ```
   vim /etc/php.ini
   ```

   b) Move the pointer to the end of the last line. Complete the following steps:

   A. Enter :$ and press the Enter key to move the pointer to the last line of the file.
   B. Press the $ key to move the pointer to the end of the line.

   c) Press the I key to switch to the edit mode.

   d) Add configurations for the memory limit and time zone at the end of the file.

   ```
   ; The maximum memory value allowed for the PHP script. You can increase or
decrease the memory limit.
   memory_limit = 1024M
   ; Set the time zone to Shanghai.
   ```
date.timezone = Asia/Shanghai

The following figure shows the result.

```
; ; End:
memory_limit = 1024M
date.timezone = Asia/Shanghai
```

e) Press the Esc key, enter :wq, and press the Enter key to save and close the configuration file.

f) Run the following command to restart Apache HTTP Server:

```
systemctl restart httpd
```

### Step 4. Create a Magento database

1. Run the following command and enter the password of the root user to log on to MySQL:

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

2. Run the following command to create the magento database:

```
mysql> CREATE DATABASE magento; # replace magento with the database name that you want to create.
```

3. Run the following commands in sequence to create a user for the magento database:

```
mysql> GRANT ALL ON magento. * TO <YourUser>@localhost IDENTIFIED BY '<YourPass>' ; # Replace <YourUser> with the account that you want to create and replace.<YourPass> with the password that you want to use.
mysql> FLUSH PRIVILEGES;
```

For example, to create an account named magentoUser and set its password to magentoUser1@3, run the following command:

```
mysql> GRANT ALL ON magento. * TO magentoUser@localhost IDENTIFIED BY 'magentoUser1@3';
mysql> FLUSH PRIVILEGES;
```

4. Type exit and press the Enter key to exit MySQL.

5. Optional: Verify whether the new Magento database and account are available.

Complete the following steps:

a) Run the following command to log on to MySQL with the new account and its password:

```
mysql -u <YourUser> -p # Replace <YourUser> with the account that you created.
```

b) Run the following command to view the new magento database:

```
mysql> show databases;
```
Step 5. Install and configure Composer

Composer is a dependency management tool of PHP. Composer can identify the code repository that is used as the basis for the project. It can also be used to install the depended code repository for the project.

1. Run the following command to install Composer:

```bash
curl -sS https://getcomposer.org/installer | php
```

2. Run the following command to configure Composer:

```bash
mv /root/composer.phar /usr/bin/composer
```

3. Run the `composer -v` command to check the Composer version.

The following command output indicates that Composer is installed.

```
/ ____/___  ____ ___  ____  ____  ________  _____
/ /   / __ / __ `__ / __ / __ / ___/ _ / ___/
/ /___/ /_/ / / / / / / /_/ / /_/ (__  )  __/ /
\____/\____/_/ /_/ /_/ . ___/
    /_/    Composer version 1.8.5 2019-04-09 17:46:47
```

Step 6. Install and configure Magento

You can install Magento by using different methods and decide whether to install sample data.

- If you install Magento for test purpose only, you can install sample data.
- If you install Magento for production purpose, we recommend that you install Magento and configure it from the start.

Git is used to download Magento and Composer is used to install Magento in this example.
1. Download Magento.
   a) Run the following command to install Git:
      
      ```
      yum -y install git
      ```
   b) Go to the default root directory of the web server.
      
      ```
      cd /var/www/html/
      ```
   c) Download Magento.
      
      ```
      git clone https://github.com/magento/magento2.git
      ```

2. Optional: Run the following command to switch Magento to a stable version:
   
   ```
   cd magento2 && git checkout tags/2.1.0 -b 2.1.0
   ```
   The output is as follows:
   
   ```
   Switched to a new branch '2.1.0'
   ```
   
   **Note:**
   By default, Git downloads and installs the latest Magento version. If you use Magento in a production environment, we recommend that you switch Magento to a stable version. Otherwise, issues may arise when you upgrade and install Magento in the future.

3. Run the following command to move the installation file to the root directory of the web server:
   
   ```
   shopt -s dotglob nullglob && mv /var/www/html/magento2/* /var/www/html/ && cd ..
   ```
   
   **Note:**
   After you run this command, you can access your Magento website through http://<the public IP address of the ECS instance>. Otherwise, you can access your Magento website only through http://<the public IP address of the ECS instance>/magento2.
4. Run the following commands in sequence to set appropriate permissions for the Magento file:

```bash
chown -R :apache /var/www/html
find /var/www/html -type f -print0 | xargs -r0 chmod 640
find /var/www/html -type d -print0 | xargs -r0 chmod 750
chmod -R g+w /var/www/html/{pub, var}
chmod -R g+w /var/www/html/{app/etc, vendor}
chmod 750 /var/www/html/bin/magento
```

5. Run the `composer install` command to install Magento.

**Step 7. Configure the client of Magento**

1. Open your browser.

2. In the browser address bar, enter `http://<the public IP address of the ECS instance>`. The following page indicates Magento is installed.

![Magento Configuration Page](image-url)
3. Click **Agree and Setup Magento** to start configuring Magento. Complete the following steps:

   a) Check readiness.

   A. Click **Start Readiness Check**.

   B. After the check is complete, click **Next**.

   ![Magento Installer](image)

   b) Add the database.

   A. Enter the account and password of the database that you created. In this example, the user account is `magentoUser` and the password is `magentoUser1@3`.

   B. Enter the name of the previously created database. In this example, the database name is `magento`.

   C. Click **Next**.

   c) Complete the settings for web access, and click **Next**.

   d) Fill in the custom store and click **Next**.

   e) Enter the administrator account information, and click **Next**.

   f) Click **Install Now** to install Magento.

The following page indicates that Magento is configured.
Step 8. Add a cron job

To add a cron job, complete the following steps:

1. Run the `crontab -u apache -e` command to configure the jobs to be operated by cron.
2. Press the I key to switch to the edit mode.
3. Enter the following configuration information:

   ```
   */10 * * * * php -c /etc /var/www/html/bin/magento cron:run
   */10 * * * * php -c /etc /var/www/html/update/cron.php
   */10 * * * * php -c /etc /var/www/html/bin/magento setup:cron:run
   ```

4. Press the Esc key, enter :wq, and press the Enter key to save and close the configuration.

   For more information about how to use cron jobs in Magento, visit Configure and run cron.

What's next
• Access http://<the public IP address of the ECS instance> to go to the following default homepage.

![Homepage](image)

• Access http://<the public IP address of the ECS instance>/admin and enter the username and password that you set during the installation. Log on to the management panel.

Related topics
Magento official documentation

3.4 Deploy the Ghost blogging platform on CentOS 7

Ghost is a free open source blogging platform developed on the basis of Node.js. The platform is used to simplify the online publishing process for individual blogs and online publications. This topic describes how to deploy the Ghost blogging platform.

Prerequisites

An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud official website.

Context

As your business scope is increasingly enlarged, you can use comprehensive services of Alibaba Cloud to scale up and scale out your business capacity. For example, you can optimize your business in the following ways:

• Scale up the vCPU and memory of a single ECS instance to enhance the processing performance.
• Add multiple ECS instances and implement load balancing among these instances.
• Use Auto Scaling to automatically increase or decrease the number of ECS instances based on business requirements.

• Use Object Storage Service (OSS) to store a large amount of data such as static web pages, images, and videos.

This topic describes how to deploy the Ghost blogging platform on an ECS instance that has basic configurations. The procedure described in this topic is applicable to individual users that are new to website construction with ECS instances.

Procedure

To deploy the Ghost blogging platform on an ECS instance, follow these steps:

1. **Step 1: Create a Linux-based ECS instance**

2. **Step 2: Deploy the Web environment**

3. **Step 3: Install Ghost**

4. **Step 4: Purchase a domain**

5. **Step 5: Apply for an ICP filing**

6. **Step 6: Resolve the domain name to the IP address of the instance**

**Step 1: Create a Linux-based ECS instance**

To build an individual website, you need only one ECS instance.

This section describes how to create an ECS instance. If you have a custom image, you can create an instance from this image. For more information, see #unique_44.

Create a Linux-based ECS instance. For more information, see #unique_4.

To set parameters, follow these rules:

- **Instance Type:** For an individual website, you can use an instance of 1 vCPU and 2 GiB or 2 vCPUs and 4 GiB to meet basic requirements. For more information about instance types, see #unique_39.

- **Network Type:** Click VPC in the Network Type section.

- **Network Billing Method:** To enable the ECS instance to connect to the Internet, you must configure an Elastic IP address (EIP) and attach the EIP to the ECS instance. If you do not select Assign Public IP Address, the ECS instance has no public IP address configured. The actual configurations depend on your requirements.

- **Image:** To build a website, you can click Public Image, and select a Linux operating system such as CentOS from the drop-down list.
After you create an instance, the system sends you an SMS message and an email to notify you of the information about the instance, such as the instance name, public IP address, and internal IP address. You can use the information to log on to the ECS console and manage the instance.

The system notifies you of most important information by sending SMS messages. To authenticate some important operations such as restarting or stopping the instance, you must use your mobile phone to receive verification codes. Therefore, after you bind a mobile number to your Alibaba Cloud account, you must keep the corresponding mobile phone in the normal running status.

**Step 2: Deploy the Web environment**

This section describes how to deploy the Web environment by installing NGINX.

The software package provides NGINX 1.10.2.

**Note:**

This version is used in the following example. The version that you download may be different in your actual running environment.

Prerequisites:

- Your instance can connect to the Internet.
- You have installed a tool for connecting to the Linux-based ECS instance. SecureCRT is used as the tool in this section.

To deploy the Web environment, follow these steps:
1. Open the SecureCRT client and specify the information of the instance that you want to log on to.
   a) Specify the name of the session for connecting to the ECS instance.
   b) Select SSH from the Protocol drop-down list.
   c) Enter the host IP address in the Hostname field and specify the username.
   d) Click Connect.

2. Enter the root username and the password.
3. Add the NGINX repository.

```
[root@localhost ~]# rpm -Uvh http://nginx.org/packages/centos/7/noarch/RPMS/
nginx-release-centos-7-0.el7.ngx.noarch.rpm
```

4. Install NGINX.

```
[root@localhost ~]# yum -y install nginx
```

5. Enable NGINX to run at startup.

```
[root@localhost ~]# systemctl enable nginx.service
```

6. Start NGINX and check the NGINX service status.

```
[root@localhost ~]# systemctl start nginx.service
[root@localhost ~]# systemctl status nginx.service
```

7. Open your browser, and in the address bar, enter the public IP address of the ECS instance to view the default NGINX web page.

![Welcome to nginx!](image)

Then, the NGINX environment is ready to run.

**Step 3: Install Ghost**

To install Ghost, follow these steps:
1. Run the following command to update system software to the latest versions.

```
[root@localhost ~]# yum -y update
```

2. Install Node.js.
   a) Install Extra Packages for Enterprise Linux (EPEL).

```
[root@localhost ~]# yum install epel-release -y
```

   b) Install Node.js and npm.

```
[root@localhost ~]# yum install nodejs npm --enablerepo=epel
```

c) Install the process manager to control Node.js applications. This process manager keeps the applications in the running state.

```
[root@localhost ~]# npm install pm2 -g
```

d) Run the commands node -v and npm -v to check the Node.js version.

3. Install Ghost.
   a) Create the Ghost installation directory.

```
[root@localhost ~]# mkdir -p /var/www/ghost
```

   b) Enter the Ghost installation directory, and run the following command to download the latest Ghost version.

```
[root@localhost ~]# cd /var/www/ghost
[root@localhost ghost]# curl -L https://ghost.org/zip/ghost-latest.zip -o ghost.zip
```

c) Decompress the Ghost package.

```
[root@localhost ghost]# yum install unzip -y
[root@localhost ghost]# yum install unzip -y
```

d) Use npm to install Ghost.

```
[root@localhost ghost]# unzip ghost.zip
```

e) Run the npm start command to start Ghost and check whether Ghost has been installed.

```
[root@localhost ghost]# npm install -production
```

f) Create a copy of the example configuration file config.example.js, and rename the file as config.js.

```
[root@localhost ghost]# cp config.example.js config.js
```

g) In the config.js file, specify the domain of the Ghost blogging platform as the URL.

```
[root@localhost ghost]# vim config.js
```

```javascript
var path = require('path'),
    config;

config = {
    // ### Production
    // When running Ghost in the wild, use the production environment.
    // Configure your URL and mail settings here
    production: {
        url: 'http://myghostblog.com',
        mail: {},
        database: {
            client: 'sqlite3',
            connection: {
                filename: path.join(__dirname, '/content/data/ghost.db')
            },
            debug: false
        },
        server: {
            host: '127.0.0.1',
            port: '2368'
        }
    }
};
```

h) Use the process manager to enable Ghost to run permanently.

```
[root@localhost ghost]# NODE_ENV=production pm2 start index.js --name "ghost"
```

i) Start, stop, and then restart Ghost.

```
[root@localhost ghost]# pm2 start ghost
[root@localhost ghost]# pm2 stop ghost
```
4. Install NGINX.
   
a) Add the NGINX repository.

   ```bash
   [root@localhost ~]# rpm -Uvh http://nginx.org/packages/centos/7/noarch/RPMS/nginx-release-centos-7-0.el7.ngx.noarch.rpm
   ```

   b) Install NGINX.

   ```bash
   [root@localhost ~]# yum -y install nginx
   ```

   c) Enable NGINX to run at startup.

   ```bash
   [root@localhost ~]# systemctl enable nginx.service
   ```

   d) Start NGINX and check the NGINX service status.

   ```bash
   [root@localhost ~]# systemctl start nginx.service
   [root@localhost ~]# systemctl status nginx.service
   ```

   e) Open your browser, and in the address bar, enter the public IP address of the ECS instance to view the default NGINX web page.

   ![Welcome to nginx!](Image)
5. Specify NGINX as the reverse proxy for Ghost.
   a) Enter the NGINX configuration directory, and create the NGINX configuration file for Ghost.
      
      [root@localhost ~]# vim /etc/nginx/conf.d/ghost.conf
   b) Add the following content to the ghost.conf file, and set server_name to the domain that is used in your actual running environment.

   ```
   upstream ghost {
   server 127.0.0.1:2368;
   }
   server {
   listen 80;
   server_name myghostblog.com;
   access_log /var/log/nginx/ghost.access.log;
   error_log /var/log/nginx/ghost.error.log;
   proxy_buffers 16 64k;
   proxy_buffer_size 128k;
   location / {
   proxy_pass http://ghost;
   proxy_next_upstream invalid_header http_500 http_502 http_503 http_504;
   proxy_redirect off;
   proxy_set_header Host $host;  # Ghost
   proxy_set_header X-Real-IP $remote_addr;
   proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
   proxy_set_header X-Forwarded-Proto $https;
   }
   }
   ```
   c) Change the name of the default configuration file default.conf to default.conf.bak, so NGINX is only applicable to ghost.conf.
      
      [root@localhost ~]# mv default.conf default.conf.bak
   d) Restart the NGINX service.
      
      [root@localhost conf.d]# systemctl restart nginx.service

6. Connect to the Ghost blogging platform.
   a) Open your browser, and in the address bar, enter the URL http://IP address of the ECS instance or http://Domain of the Ghost blogging platform to connect to the Ghost blogging platform.
Step 4: Purchase a domain

You can specify a unique domain for your website. Therefore, users can visit your website by using a simple domain instead of a complex IP address.

We recommend that you visit www.net.cn to purchase a domain.
1. Go to the Domains page, enter the domain that you want to use in the search bar, and then click Find A Domain. If the searched domain has not been registered, you can purchase the domain. Specify the domain that you want to purchase and the service duration for the domain, and click Buy Now.

2. When you confirm the order, you must specify the owner of the domain. To simplify the operation, we recommend that you select Person temporarily. You can change the owner in the follow-up management. In this example, a personal domain is specified.

3. If you purchase the domain for the first time, you must create the registrant profile. For more information, see Create the registrant profile.

4. Enter the authentic registrant profile.

5. To pass the real-name verification, upload the scanned image of your identity card. The profile verification takes one to five working days.

**Step 5: Apply for an ICP filing**

You must apply for an IPC filing for the domain that is associated with a website hosted on a server in Mainland China. Your website cannot provide services until you obtain the ICP license number for the domain.

The Alibaba Cloud ICP Filing system can help you simplify the ICP filing procedure. You can apply for an ICP filing free of charge. The review duration is approximately 20 days.

1. Log on to the ICP Filing Management console.

2. In the left-side navigation pane, choose ICP Filing Management > ICP No. Application, and click Apply to apply for the service identification number for the ECS instance that you have purchased. You will use the service identification number when you register an ICP filing.

3. In the dialog box that appears, click OK.

4. After the system issues the service identification number, the ICP No. Management tab appears and displays the service identification number that is associated with the ECS instance. For more information about ICP filing, click the Filing Introduction tab.

5. If you apply for an ICP filing for the first time, you must register an IPC filing account in the Alibaba Cloud ICP Filing system.
Step 6: Resolve the domain name to the IP address of the instance

You must resolve the domain name to the IP address of the ECS instance, so users can visit your website by using the domain name. Follow these steps:

1. Log on to the Domain console.
2. In the left-side navigation pane, choose Domain > Domain Names. Find the domain name that you want to resolve, and in the Actions column next to the domain name, click Resolve.
3. Click Getting Started.
4. Enter the public IP address of your Linux-based instance in the dialog box that appears, and click Submit.

Then, you can use the domain name to visit your website.
4 Build an application

4.1 Build an FTP site on an ECS instance

4.1.1 Build an FTP site on a Linux instance

vsftpd (very secure FTP daemon) is a light, safe, and easy-to-use File Transfer Protocol (FTP) server software for Linux. This topic describes how to install vsftpd on a Linux ECS instance.

Prerequisites

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud official website.
- You have created an ECS instance and assigned it a public IP address. If you have not, see #unique_22.

Context

FTP is a protocol used for transferring files. It is built on a client-server model architecture and supports the following two modes:

- Active mode: The client sends port information to the FTP server, and the server establishes a connection to the port.
- Passive mode: FTP server opens a port and sends the port information to the client. The client connects to the port, and the server accepts the connection.

Note:

Most FTP clients are located in local area networks (LANs), have no independent public IP addresses, and are protected by firewalls. This causes problems for FTP servers in active mode to establish a connection to the client. Therefore, we recommend that you use the passive mode for the FTP server unless there are special requirements.

FTP supports the following three authentication modes:

- Anonymous user mode: Anyone can log on to the FTP server without password verification. This is the least secure mode. We recommend that you use it to save only unimportant public files, but not files in a production environment.
- Local user mode: This authentication mode requires users to have Linux local accounts. This mode is more secure compared with the anonymous user mode.
• Virtual user mode: Virtual users are dedicated users of the FTP server. Virtual users can access only the FTP service provided by the Linux system and cannot access other resources of the system. This way, the security of the FTP server is further enhanced.

The following table lists the methods of configuring the FTP server.

<table>
<thead>
<tr>
<th>Working mode</th>
<th>Anonymous user</th>
<th>Local user</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active mode</td>
<td>Allow anonymous users to upload files to the FTP server in the active mode.</td>
<td>Allow local users to access to the FTP server in the active mode.</td>
</tr>
<tr>
<td>Passive mode</td>
<td>None.</td>
<td>Allow local users to access to the FTP server in the passive mode.</td>
</tr>
</tbody>
</table>

**Limits**

Procedures in this topic are applicable to the following software versions:

• Operating system: the CentOS 7.2 64-bit public image
• vsftpd: 3.0.2
• Internet Explorer: 11

The commands and parameters used in this topic may vary based on your software version.

**Procedure**

To build an FTP site on a Linux instance, perform the following steps:

• **Step 1: install vsftpd**
• **Step 2: configure vsftpd (anonymous user mode)**
• **Step 2: configure vsftpd (local user mode)**
• **Step 3: Set security groups**
• **Step 4: Test the client**

**Step 1: install vsftpd**

1. Connect to the target Linux instance.

   For more information, see #unique_48/unique_48_Connect_42_section_fjm_rgx_wdb.
2. Run the following command to install vsftpd.

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

   If the following page appears, the installation succeeds.

3. Run the following command to enable the FTP service to run at boot time:

   ```bash
   systemctl enable vsftpd.service
   ```

4. Run the following command to start the FTP service:

   ```bash
   systemctl start vsftpd.service
   ```

5. Run the following command to view the listening port of the FTP service:

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

   The following page appears, which indicates that the FTP service is started and is
   listening to port 21. The anonymous access function is enabled by default. You can log
   on to the FTP server without entering your username and password, but you do not have
   the permissions to modify or upload files.

Step 2: configure vsftpd (anonymous user mode)

To configure the file upload permission for anonymous users in active mode, perform the
following steps:
1. Modify the configuration file /etc/vsftpd/vsftpd.conf.
   a) Run the `vim /etc/vsftpd/vsftpd.conf` command to open the configuration file.
   b) Press I to enter the edit mode.
   c) Set `write_enable=YES`.
   d) Set `anon_upload_enable=YES`.
   e) Press Esc to exit the edit mode. Enter :wq and press Enter to save and close the file.
   The following figure shows the modified configuration file.
   
   ![Modified configuration file]

2. Run the following command to change the permissions of the /var/ftp/pub directory and grant write permissions to FTP users:
   
   `chmod o+w /var/ftp/pub/`

3. Run the following command to reload the configuration file:
   
   `systemctl restart vsftpd.service`

**Step 2: configure vsftpd (local user mode)**

To configure the permission for local users to access the FTP server, perform the following steps:
1. Run the following command to create a Linux user for the FTP service. In this example, the username is ftptest.

   useradd ftptest

2. Run the following command to modify the password of the ftptest user:

   passwd ftptest

3. Run the following command to create a file directory for the FTP service:

   mkdir /var/ftp/test

4. Run the following command to change the owner of the /var/ftp/test directory to ftptest:

   chown -R ftptest:ftptest /var/ftp/test

5. Modify the vsftpd.conf configuration file.

   a) Run the `vim /etc/vsftpd/vsftpd.conf` command to open the configuration file.
   
   b) Press I to enter the edit mode.
   
   c) Enable the active or passive mode for the FTP server as needed.

   • To enable the active mode for the FTP server, you need to set the following parameters:

   ```
   #Use the default values for all parameters except for the following parameters:
   #Modify the values of the following parameters:
   anonymous_enable=NO   #Disallows anonymous users to log on to the FTP server.
   local_enable=YES      #Allows local users to log on to the FTP server.
   listen=YES            #Listens to IPv4 sockets.
   #Add # to the beginning of the row to comment out the following parameter:
   #listen_ipv6=YES       #Disables listening to IPv6 sockets.
   #Add the following parameters:
   chroot_local_user=YES #Specifies all users who log on are limited to the home directory.
   chroot_list_enable=YES #Uses a list to specify users who are not limited to the home directory.
   chroot_list_file=/etc/vsftpd/chroot_list #Specifies the list file to contain users who are not limited to the home directory.
   allow_writeable_chroot=YES
   local_root=/var/ftp/test #Specifies the directory where local users reside after they log on.
   ```

   • To enable the passive mode for the FTP server, you need to set the following parameters:

   ```
   #Use the default values for all parameters except for the following parameters:
   ```
# Modify the values of the following parameters:
- `anonymous_enable=NO` # Disallows anonymous users from logging on to the FTP server.
- `local_enable=YES` # Allows local users to log on to the FTP server.
- `listen=YES` # Listens to IPv4 sockets.

# Add # to the beginning of the row to comment out the following parameter:
- `listen_ipv6=YES` # Disables listening to IPv6 sockets.

# Add the following parameters:
- `local_root=/var/ftp/test` # Specifies the directory where local users reside after they log on.
- `chroot_local_user=YES` # Specifies all users who log on are limited to the home directory.
- `chroot_list_enable=YES` # Uses a list to specify users who are not limited to the home directory.
- `chroot_list_file=/etc/vsftpd/chroot_list` # Specifies the list file to contain users who are not limited to the home directory.
- `allow_writeable_chroot=YES`
- `pasv_enable=YES` # Enables the passive mode.
- `pasv_address=<The public IP address of the FTP server>` # This topic uses the public IP address of a Linux instance.
- `pasv_min_port=<port number>` # Specifies the minimum value of the port range available for data transfer in the passive mode.
- `pasv_max_port=<port number>` # Specifies the maximum value of the port range available for data transfer in the passive mode.

**Note:**

We recommend that you use a relatively high port range, such as 50000 to 50010, which improves the security of the FTP server.

For more information about the parameters, see vsftpd configuration file and parameters.

d) Press Esc to exit the edit mode. Enter :wq and press Enter to save and close the file.

6. Create the chroot_list file, and write the exception user list to the file.

   a) Run the `vim /etc/vsftpd/chroot_list` command to create the chroot_list file.
   
   b) Press I to enter the edit mode.
   
   c) Enter the names of exception users. These users are not limited to the home directory and can access other directories.
   
   d) Press Esc to exit the edit mode. Enter :wq and press Enter to save and close the file.

**Note:**

Even if no exception users exist, you must also create the chroot_list file. The file can be empty.
7. Run the following command to restart vsftpd.

```
systemctl restart vsftpd.service
```

**Step 3: Set security groups**

After building the FTP site, add inbound security group rules to the instance security group and allow the following FTP ports. For more information, see #unique_16.

**Note:**

Most clients are located within LANs and their private IP addresses are converted into public IP addresses when the clients access or are accessed by external devices. Therefore, the IP addresses returned by the `ipconfig` or the `ifconfig` command may not be the actual public IP addresses of the clients. If you cannot log on to the FTP server on the client, verify the public IP address of your client is correct.

- When the FTP server is in the active mode: allow port 21. The following table lists the configuration details:

<table>
<thead>
<tr>
<th>Rule direction</th>
<th>Authorization policy</th>
<th>Protocol</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Allow</td>
<td>Custom TCP</td>
<td>21/21</td>
<td>IPv4 CIDR block</td>
<td>The CIDR blocks that contain the public IP addresses of all clients which need to access the FTP server. Separate multiple CIDR blocks with commas (,). To allow all clients to access the FTP server, authorize 0.0.0.0/0.</td>
</tr>
</tbody>
</table>
- When the FTP server is in the passive mode: allow port 21 and all the ports between the `pases_min_port` and the `pases_max_port` parameters in the `/etc/vsftpd/vsftpd.conf` configuration file. The following table lists the configuration details:

<table>
<thead>
<tr>
<th>Rule direction</th>
<th>Authorization policy</th>
<th>Protocol</th>
<th>Port range</th>
<th>Authorization type</th>
<th>Authorization object</th>
</tr>
</thead>
</table>
| Inbound        | Allow               | Custom TCP | 21/21      | IPv4 CIDR block    | The CIDR blocks that contain the public IP addresses of all clients which need to access the FTP server. Separate multiple CIDR blocks with commas (,).
|                |                     |          |            |                    | To allow all clients to access the FTP server, authorize 0.0.0.0/0. |
|                |                     |          | `pases_min_port`/`pases_max_port` | IPv4 CIDR block    | The CIDR blocks that contain the public IP addresses of all clients which need to access the FTP server. Separate multiple CIDR blocks with commas (,).
|                |                     |          |            |                    | To allow all clients to access the FTP server, authorize 0.0.0.0/0. |

**Step 4: Test the client**

FTP clients, Windows command-line tools, or browsers can be used to test FTP servers. This topic takes the IE browser that comes with Windows as an example to introduce the access steps when the FTP server is configured to the active mode or the passive mode.

**Note:**

If an error occurs when you use a browser to access the FTP server, clear the browser cache and try again.
• When the FTP server runs in the active mode

1. Open the IE browser of the client.
2. Perform the following operations to set the browser to the active access mode:
   Choose Settings > Internet Options > Advanced. Select Enable FTP Folder View and clear Use Passive FTP.
4. In the dialog box that appears, enter the username and password to access the FTP site and perform operations on the FTP file.

   **Note:**
   These steps apply only to local users. Anonymous users can log on to the FTP server without entering the user name and password.

• When the FTP server runs in the passive mode

1. Open the IE browser of the client.
2. Set the browser to the passive access mode. Choose Settings > Internet Options > Advanced. Select Enable FTP Folder View and Use Passive FTP.
4. In the dialog box that appears, enter the username and password to access the FTP site and perform operations on the FTP file.

   **Note:**
   These steps apply only to local users. Anonymous users can log on to the FTP server without entering the user name and password.

**vsftpd configuration file and parameters**

The files under the /etc/vsftpd directory:

• /etc/vsftpd/vsftpd.conf is the core configuration file of vsftpd.
• /etc/vsftpd/ftpusers is the blacklist file. Users in this file are not allowed to access the FTP server.
• `/etc/vsftpd/user_list` is the whitelist file. Users in this file are allowed to access the FTP server.

The `vsftpd.conf` configuration file:

• The following table describes the parameters for logon control.

<table>
<thead>
<tr>
<th>Parameter setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>anonymous_enable=YES</td>
<td>Accepts anonymous users.</td>
</tr>
<tr>
<td>no_anon_password=YES</td>
<td>No password is required when anonymous users log on to the FTP server.</td>
</tr>
<tr>
<td>anon_root= (none)</td>
<td>The home directory for anonymous users.</td>
</tr>
<tr>
<td>local_enable=YES</td>
<td>Accepts local users.</td>
</tr>
<tr>
<td>local_root= (none)</td>
<td>The home directory for local users.</td>
</tr>
</tbody>
</table>

• The following table describes the parameters used to control permissions of users.

<table>
<thead>
<tr>
<th>Parameter setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>write_enable=YES</td>
<td>Allows users to upload files (global control).</td>
</tr>
<tr>
<td>local_umask=022</td>
<td>Grants local users the permission to upload files.</td>
</tr>
<tr>
<td>file_open_mode=0666</td>
<td>Uses umask for file upload permissions</td>
</tr>
<tr>
<td>anon_upload_enable=YES</td>
<td>Allows anonymous users to upload files.</td>
</tr>
<tr>
<td>anon_mkdir_write_enable=YES</td>
<td>Allows anonymous users to create directories.</td>
</tr>
<tr>
<td>anon_other_write_enable=YES</td>
<td>Allows anonymous users to modify and delete files.</td>
</tr>
<tr>
<td>chown_username=lightwiter</td>
<td>Specifies the username of anonymously uploaded files.</td>
</tr>
</tbody>
</table>

**What's next**

Enhance the security of the FTP service. For more information, see [Security enhancement solution](#).
4.1.2 Build an FTP site on a Windows instance

This topic describes how to build an FTP site on a Windows instance. This method is applicable to Windows Server 2008 and later. In this example, Windows Server 2012 R2 is used.

Prerequisites

- You must have registered an Alibaba Cloud account. If not, create a new Alibaba Cloud account first.
- You must have created an ECS instance. The resources of the instance used in this topic are as follows:
  - Instance type: ecs.c6.large
  - Operating system: Windows Server 2012 R2 64-bit

Procedure

To build an FTP site on a Windows instance, perform the following operations:

1. Step 1: Add IIS and FTP server roles
2. Step 2: Create an FTP username and password
3. Step 3: Configure permissions for a shared file
4. Step 4: Create and configure an FTP site
5. Step 5: Configure security groups and the firewall
6. Step 6: Test the client

Step 1: Add IIS and FTP server roles

You must install IIS and FTP services before you build an FTP site.

1. Connect to the Windows ECS instance. For more information, see #unique_50.
2. In the taskbar, click the Server Manager icon.
3. In the top navigation bar, choose Manage > Add Roles and Features.
4. In the dialog box that appears, keep the default settings and click Next to go to the Select server roles step.
5. Select **Web Server (IIS)**. In the message that appears, click **Add Features** and then click **Next**.
6. In the **Select role services** step, select **IIS Management Console** and **FTP Server**, and then click **Next**.

![Select role services](image)

7. Click **Install**.

**Step 2: Create an FTP username and password**

To create a username and password for FTP, perform the following operations. If you want to allow access to the site from anonymous users, skip this step.

1. In the taskbar, click **Start**.

2. Click **Administrative Tools** and double-click **Computer Management**.

3. In the left-side navigation pane, choose **Local Users and Groups > Users**.

![Computer Management](image)
4. Right-click anywhere in the blank space in the middle and choose **New User...** from the shortcut menu.

In this example, the username is ftptest.

**Note:**
The password must contain uppercase letters, lowercase letters, and digits. Otherwise, the password is invalid.

**Step 3: Configure permissions for a shared file**

You must configure access and modification permissions on the folder shared to users on the FTP site.

1. Create a folder for FTP on the server disk. Right-click the folder and choose **Properties** from the shortcut menu.

In this example, a folder named ftp is created under Disk C.

2. Click the **Security** tab and click **Edit**.

3. Click **Add**.

4. In the dialog box that appears, enter **Everyone** for the object name and click **OK**.

5. In the **Group or user names** section, click **Everyone** and configure permissions for **Everyone** as needed. Then, click **OK**.

In this example, all permissions are granted.

**Step 4: Create and configure an FTP site**

After you install FTP and configure permissions on the shared folder, perform the following operations to create an FTP site:

1. In the taskbar, click the **Server Manager** icon.

2. In the top navigation bar, choose **Administrative Tools > Internet Information Services (IIS) Manager**.
3. In the left-side navigation pane, right-click Sites and choose Add FTP Site... from the shortcut menu.

4. In the dialog box that appears, enter the FTP site name and Physical path of the shared folder, and then click Next.

   In this example, the FTP site name is set to ftptest and the Physical path is set to the path of the FTP folder created in Step 3: Configure permissions for a shared file.

5. Keep the default All Assigned selection for the IP Address field. You can configure a port number as needed. The default FTP port is 21.

6. Select one of the following options for the SSL field and click Next.

   - Allow SSL: allows the FTP server to connect to the client in the both SSL encrypted and unencrypted states.
   - Require SSL: requires SSL encryption for communication between the FTP server and the client.
   - No SSL: does not require SSL encryption.

7. Select one or more authentication methods.

   - Anonymous: allows users that provide the anonymous or ftp username to access the content.
   - Basic: requires users to provide valid usernames and passwords to access the content. The basic authentication method transmits the unencrypted password through the network. Therefore, you must only use the basic authentication method when you are sure that the connection between the client and the FTP server is secure, such as when SSL encryption is used.
8. Select one of the following options from the **Allow access to:** drop-down list:

- **All users:** All users, both anonymous and identified users, can access the relevant content.
- **Anonymous users:** Anonymous users can access the relevant content.
- **Specified roles or user groups:** Only specific roles or members of the specified user group can access the relevant content. Enter the role or user group in the corresponding field.
- **Specified users:** Only specified users can access the relevant content. Enter the usernames in the corresponding field.

9. Select the **Read** and **Write** permissions for the authorized users. Click **Finish**.

After the preceding operations are complete, you can view information about the FTP site.

**Step 5: Configure security groups and the firewall**

After the FTP site is built, you must create an inbound rule for security groups of the instance to allow traffic on the FTP port. For more information, see #unique_16. For more information about specific configurations, see #unique_11 and #unique_51.

By default, the instance firewall allows traffic for the FTP service on TCP port 21. If you want to use other ports, you must create a new rule as an inbound rule of the firewall.

For more information about firewall configurations, visit Build an FTP Site on IIS.

**Step 6: Test the client**

To test the client, perform the following operations:

1. Configure Internet Explorer.
   a) Open Internet Explorer and choose **Tools > Internet options.**
   b) Click the **Advanced** tab. In the **Settings** section, select **Enable folder view for FTP sites** and clear **Use Passive FTP (for firewall and DSL modem compatibility).**

2. Double-click **This PC.** In the search box, enter ftp://IP address of the server:FTP port. If you do not specify a port, the default port 21 is used. For example, you can enter ftp://0.0.0.0:21.

   If a dialog box that prompts you to enter your username and password appears, the configuration is complete. After you enter the username and password, you can perform FTP file operations based on your permissions. In this example, the ftptest username
and the corresponding password configured in the Step 2: Create an FTP username and password section are used.

What's next

You can perform security hardening on the FTP service. For more information, see FTP anonymous logon and weak password vulnerabilities.

If you want to manage files stored on Object Storage Service (OSS) based on FTP, you can install ossftp. For more information, see Quick installation of ossftp. After ossftp receives a common FTP request, ossftp will map operations on files and folders as operations on OSS.

4.2 Build Microsoft SharePoint 2016 on an ECS instance

This topic describes how to build Microsoft SharePoint 2016 on an ECS instance.

Prerequisites

You must have registered an Alibaba Cloud account before you follow the instructions provided in the tutorial. If not, create a new Alibaba Cloud account first.

Context

Microsoft SharePoint Portal Server (Microsoft SharePoint) is a portal development environment that enables enterprises to develop intelligent portals. Microsoft SharePoint seamlessly connects to knowledge bases, individual users, and teams. Microsoft SharePoint empowers your business through efficient information processing and provides an enterprise-wide service solution. It allows you to integrate enterprise applications and flexibly choose deployment options and management tools to incorporate information from various systems.

The procedure described in this topic is applicable to users who are familiar with ECS instances and Windows Server operating systems.

The following software versions are used:

- Operating system: Windows Server 2012 R2 Datacenter
- Database: SQL Server 2014 SP1

The ECS instances described in this topic have the following specifications:

- vCPU: 4 vCPUs
- Memory: 8 GB
Procedure

To build Microsoft SharePoint 2016 on an ECS instance, follow these steps:

1. **Step 1: Add the AD, DHCP, DNS, and IIS services**
2. **Step 2: Install SQL Server 2014**
3. **Step 3: Install SharePoint 2016**
4. **Step 4: Configure SharePoint 2016**

**Step 1: Add the AD, DHCP, DNS, and IIS services**

1. Purchase an ECS instance. For more information, see #unique_4.
2. Establish a remote connection to the instance.
3. Find and open Server Manager from the Windows taskbar.
4. In the left-side navigation pane, click **Local Server** and find **IE Enhanced Security Configuration** in the PROPERTIES section.
5. Disable Internet Explorer Enhanced Security Configuration.
6. Add roles and features including DNS, DHCP, IIS, and .NET Framework 3.5.

a) Click **Add roles and features**.

![Add roles and features](image1)

b) Add the AD, DHCP, and DNS services. Select **Active Directory Domain Services**, **DHCP Server**, and **DNS Server**, and click **Next**.

![Add Roles and Features Wizard](image2)

c) Add the IIS service. Select **Web Server (IIS)** and click **Next**.
d) In the **Features** step, select **.NET Framework 3.5 Features**.

e) Click **Next** until the installation is complete.
7. Configure the AD service. Select **Add a new forest** and enter a domain name in the **Root domain name** field to create a domain environment.

8. Set and confirm a password and click **Next** until the configuration is complete.
9. Click **Complete DHCP configuration** to configure the DHCP feature.

   ![DHCP configuration](image)

   a) Check the DHCP configuration and click **Next**.
   b) Keep the default configuration and click **Commit** to complete the installation.

**Step 2: Install SQL Server 2014**

You can also download the database from a third-party website. Make sure that the downloaded software is secure.

2. Install SQL Server 2014 SP1. Open the SQL Server Installation Center window and click the first installation option.

3. Enter the product key and click Next.

4. Read and accept the license terms, and click Next.

5. Complete the installation check and click Next.
6. Keep the default configuration and click **Next**.

![SQL Server 2014 Setup: Setup Role](image)

7. Click **Select All** to select all features and click **Next**.

![SQL Server 2014 Setup: Feature Selection](image)
8. Configure the SQL Server instance. Click **Default instance** to use the default instance ID.
9. Specify the account names and passwords for **SQL Server Database Engine** and **SQL Server Analysis Services**.
10. Click **Add Current User** to add the current user and click **Next**.

11. Click **Add Current User** to add the current user and click **Next**.
12. Click **Next** until the installation is complete.

**Step 3: Install SharePoint 2016**

1. Install the SharePoint 2016 prerequisite installer. Open the image folder and double-click the executable file of the prerequisite installer.

   ![Image of prerequisite installer folder]

2. In the installation wizard, click **Next**.

3. Read and accept the license terms, and install necessary components.

4. Open the Setup.exe file, enter the product key in the dialog box that appears, read and accept the license terms, and then click **Continue**.

5. Specify the installation directory as needed or keep the default setting as shown in this example, and click **Install Now**.

6. After the installation is complete, select **Run the SharePoint Products Configuration Wizard now** and close the wizard.

**Step 4: Configure SharePoint 2016**

1. Select **Create a new server farm**.

2. Specify configuration database settings and the database access account. The database is installed on the local host. Therefore, you must specify the local IP address in the Database server field.
3. Specify the server role.

4. Select **Specify port number** and enter 10000 in the field. You can also specify another port number as needed.

5. Check the configurations and click **Next**.

Now, you can open the SharePoint Central Administration web application.

### 4.3 Install SharePoint 2016

This topic describes how to install SharePoint 2016.

**Prerequisites**

An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud official website.

**Context**

To install SharePoint 2016, you must meet the following environment requirements:

- **Basic configurations:**
  - Windows Server 2012
  - CPU: 4 vCPUs. Memory: 8 GB. You can design the architecture and purchase ECS instances according to actual environments.

- **Software environment:**
  - SQL Server 2012 Express
  - SharePoint 2016
  - Active Directory (AD)
  - Domain Name System (DNS)
  - Internet Information Services (IIS)

- **Required component:** .NET Framework 3.5 for installing SQL Server.

**Note:**

- When you install .Net Framework 3.5, an error may occur at the step of **adding roles and features**. For more information about how to fix this issue, see What can I do if I am unable to install .NET Framework 3.5.1, or a language package, on Windows Server 2012 R2/2016/2019?
- For more information about the required component of SharePoint, see Microsoft documentation. The system indicates that you need to install dependencies.
when you install SharePoint. If you fail to install dependencies, you cannot install SharePoint.

Procedure

1. Build AD.

   **Note:**
   Modify the Security Identifier (SID) before you add a client to a domain. In this topic, only one ECS instance is used to install SharePoint. Therefore, all roles and features are assigned to the instance. In your actual running environment, do not install SQL, AD, and SharePoint servers on the same instance.

2. Install SQL Server 2012 Express.

   Use the default method to install SQL Server. In this topic, the Express edition is used in the test environment. Follow these rules:

   **Note:**
   - The Express edition has the TCP/IP protocol disabled by default. You must manually enable the protocol.
   - The Express edition may have no console. You must install a SQL management tool.
   - We recommend that you use the SQL Server Enterprise edition that provides more features than the Express edition.


   a) Install the required components of SharePoint.

   **Note:**
   To use the installation wizard, your instance must be authorized to access the Internet. If your instance is not authorized, you have to download the components
and run commands to install these components. For more information, see Microsoft documentation.

b) Restart the ECS instance, and install Sharepoint.

c) Run the SharePoint 2016 installation wizard, enter the product key, and then click **Continue**.
   - Start to install SharePoint 2016.

d) Run the SharePoint configuration wizard.

e) Click **Create a new server farm**, and click **Next**.

f) Specify configuration database settings and the database access account.

g) Specify the server role.

h) Specify the port number for the SharePoint Central Administration Web application and configure security settings.

i) Complete the configuration wizard and start to install SharePoint.

j) Click **Finish**.

**What's next**

After you install SharePoint, you can configure the server farm in the SharePoint Central Administration Web application. When you configure the server farm, only enable the required services. Otherwise, unnecessary memory pressure may be incurred.

**4.4 Build Docker**

This topic describes how to deploy Docker on CentOS.

**Prerequisites**

You must have registered an Alibaba Cloud account before you follow the instructions provided in the tutorial. If not, create a new Alibaba Cloud account first.

**Context**

This topic is applicable to developers that are familiar with Linux but new to Alibaba Cloud ECS.

In the following example, the operating system version is CentOS 7.2 64 3.10.0-514.6.2.el7.x86_64.

**Note:**

Docker requires a 64-bit Linux system with kernel 3.10 or later.
**Procedure**

To build Docker on an ECS instance, perform the following steps:

1. **Deploy Docker**
2. **Use Docker**
3. **Create an image**

**Deploy Docker**

You can purchase the required image from [Alibaba Cloud Marketplace](https://marketplace.aliyun.com/), and easily deploy Docker. You can also install Docker manually as described in this topic.

To deploy Docker, perform the following steps:

1. Add a Yellowdog Updater, Modified (YUM) repository:
   
   ```
   yum install epel-release -y
   yum clean all
   yum list
   ```

2. Install and run Docker:
   
   ```
   yum install docker-io -y
   systemctl start docker
   ```

3. Check the installation result:
   
   ```
   docker info
   ```

   If the following information is displayed, Docker has been installed.

   ![docker_info_output]
Use Docker

You can use Docker in these ways:

1. Manage the Docker daemon:

   systemctl start docker  #Run the Docker daemon.
   systemctl stop docker   #Stop the Docker daemon.
systemctl restart docker  #Restart the Docker daemon.

2. Manage images. The following example uses Apache images from Alibaba Cloud image repository:

```bash
docker pull registry.cn-hangzhou.aliyuncs.com/lxepoo/apache-php5
```

- Modify the tag of an image in Alibaba Cloud image repository to simplify image identification:

```bash
docker tag registry.cn-hangzhou.aliyuncs.com/lxepoo/apache-php5:latest aliweb:v1
```

- Check existing images:

```bash
docker images
```

- Delete an image:

```bash
docker rmi -f registry.cn-hangzhou.aliyuncs.com/lxepoo/apache-php5
```

3. Manage containers:

- Enter a container. Run the `docker images` command to obtain the `ImageId` value of `e1xxxxxxxxx`. Then, run the `docker run` command to enter the container.

```bash
docker run -it e1xxxxxxxxx /bin/bash
```

- Exit the container. Run the `exit` command to exit the container.
• You can combine the run command with the -d parameter to run the container in the background. The --name parameter specifies apache as the container name.

```
docker run -d --name apache e1xxxxxxxxxe
```

• Enter the container that runs in the background:

```
docker exec -it apache /bin/bash
```

• Create an image from the container. Description of the parameters in the command:

```
docker commit <container ID or container name> [<repository name> [: <tag>]].
```

```
docker commit containerID/containerName repository:tag
```

• To easily test and restore an image, you can run the source image, create a new image with a simple name from the source image, and then test the new image.

```
# docker commit 4c8066cd8c01 apachephp:v1
```

• Run the container and map port 8080 of the host to the container:

```
# docker run -d -p 8080:80 apachephp:v1
```

In a browser, enter the IP address of the host followed by the port number 8080 to connect to the container. The following response indicates that the container runs normally.

Create an image

To create an image, perform the following steps:

1. Prepare the following content in a Dockerfile:

```
# vim Dockerfile
```
FROM apachephp:v1  #Declare a base image.
MAINTAINER DTSTACK #Declare the image owner.
RUN mkdir /dtstact #The commands that you want to run before the container starts.
You must add these commands to the end of the RUN command. The Dockerfile can contain only a maximum of 127 lines. If you have commands that exceed 127 lines in the Dockerfile, we recommend that you write these commands to a script.
ENTRYPOINT ping www.aliyun.com #The commands that run at startup. The last command must be a frontend command that runs constantly. Otherwise, the container will exit after running all commands.

2. Build an image:

docker build -t webcentos:v1 .   #The single dot (.) specifies the path of the Dockerfile and must be provided.
docker images                    #Check whether the image has been created.
docker run -d webcentos:v1       #Run the container in the background.
docker ps -a                     #Query all containers including those in the stopped state.
docker logs CONTAINER ID/IMAGE   #Check the startup log to troubleshoot the issue based on the container ID or name if the started container does not exist in the query result.
docker commit fb2844b6c070 dtstackweb:v1 #The container ID and the name and version of the new image. You must add the information to the end of the commit command.
docker images                    #Query images that have been downloaded and created on premises.
docker push fb2844b6c070 dtstackweb:v1 #Push an image to the remote image repository. Default value

3. Push the image to the registry.

Specify ImageId and image version.

docker login --username=dtstack_plus registry.cn-shanghai.aliyuncs.com #Specify the password of the image repository. Enter the information after you run this command.
docker tag [ImageId] registry.cn-shanghai.aliyuncs.com/dtstack123/test:[Image version]
docker push registry.cn-shanghai.aliyuncs.com/dtstack123/test:[Image version]

If you can view the image version in the image repository, it indicates that the image has been pushed to the registry.

4.5 Deploy databases based on ECS

4.5.1 Manually deploy a MySQL database on an ECS instance running CentOS 7

MySQL is a relational database management system and is often used to build the LAMP or LNMP environment. This topic describes how to install, configure, and remotely access a MySQL database on a Linux ECS instance.

Prerequisites
• To use ECS instances that are located in mainland China regions, make sure that you have completed real-name verification for your account.

• An ECS instance is created. For more information, see #unique_4.

Context

In this topic, the following instance type and software versions are used. The operations may vary depending on the versions of your software.

• Instance type: ecs.c6.large (2 vCPUs and 4 GiB memory)
• Operating system: public image CentOS 7.2 64-bit
• MySQL: 5.7.26

In this example, the MySQL installation paths are as follows:

- Configuration file: /etc/my.cnf
- Data storage: /var/lib/mysql
- Command files: /usr/bin and /usr/sbin

• Port: 3306

Note:
You must add inbound rules to the security group associated with the ECS instance and enable port 3306 for inbound traffic. For more information, see #unique_16.

Procedure

Follow these steps to deploy a MySQL database on a Linux ECS instance:

1. Step 1. Prepare the environment
2. Step 2. Install MySQL
3. Step 3. Configure MySQL
4. Step 4. Remotely access the MySQL database

Step 1. Prepare the environment

Connect to your ECS instance. For more information, see #unique_58 or #unique_31.
Step 2. Install MySQL

1. Run the following command to update the YUM repository:
   
rpm -Uvh http://dev.mysql.com/get/mysql57-community-release-el7-9.noarch.rpm

2. Run the following command to install MySQL:
   
yum -y install mysql-community-server

3. Run the following command to check the MySQL version:
   
   mysql -V

   The following command output indicates that MySQL is installed:
   
   mysql  Ver 14.14 Distrib 5.7.26, for Linux (x86_64) using EditLine wrapper

Step 3. Configure MySQL

1. Run the following command to start MySQL:
   
   systemctl start mysqld

2. Run the following command to enable MySQL to start upon system startup:
   
   systemctl enable mysqld

3. Run the following command to check the /var/log/mysqld.log file, and obtain and record the initial password of the root user:
   
   grep 'temporary password' /var/log/mysqld.log

   A command output similar to the following one is displayed:
   
   2020-04-08T08:12:07.893939Z 1 [Note] A temporary password is generated for root@localhost: xvlo1\Zs7>ui

   **Note:**
   
The initial password is used in the subsequent security configurations for MySQL.

4. Run the following command to make security configurations for MySQL:
   
   mysql_secure_installation

   a) Reset the password of the root user.

   Enter password for user root: #Enter the initial password that you obtained in the previous step.
   The 'validate_password' plugin is installed on the server.
   The subsequent steps will run with the existing configuration of the plugin.
Using existing password for root.
Estimated strength of the password: 100
Change the password for root? (Press y|Y for Yes, any other key for No) : Y
#Enter Y to change the password of the root user.
New password: #Enter a new password that is 8 to 30 characters in length. The
password must contain uppercase letters, lowercase letters, digits, and special
characters. Special characters include ()` ~ ! @ # $ % ^ & * - + = | {} \[\] : ; ' <> , . ? /
Re-enter new password: #Enter the new password again for confirmation.
Estimated strength of the password: 100
Do you wish to continue with the password provided? (Press y|Y for Yes, any other
key for No) : Y
#Enter Y to continue.

b) Delete anonymous users.

By default, a MySQL installation has an anonymous user, allowing anyone to
log into MySQL without having to have a user account created for them. This is
intended only for testing, and to make the installation go a bit smoother. You
should remove them before moving into a production environment.
Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y
#Enter Y to delete anonymous users.
Success.

c) Deny remote access from the root user.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : Y
#Enter Y to deny remote access from the root user.
Success.

d) Delete the test database and access permissions on this database.

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : Y
#Enter Y to delete the test database and access permissions on this database.
- Dropping test database...
Success.

e) Reload privilege tables.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : Y
#Enter Y to reload privilege tables.
Success.
All done!

For more information about the security configurations for MySQL, see MySQL
documentation.

Step 4. Remotely access the MySQL database

You can use a database client or Data Management Service (DMS) provided by Alibaba
Cloud to remotely access the MySQL database. In this topic, DMS is used to show how to
remotely access the MySQL database.
1. On the ECS instance, create an account for remote logon to the MySQL database.
   a) Run the following command and enter the password of the root user to log on to the MySQL database:

   ```bash
   mysql -uroot -p
   ```

   b) Run the following commands in sequence to create an account for remote logon to MySQL. In this example, the account is dms and the password is 123456.

   ```sql
   mysql> grant all on *.* to 'dms'@'%' IDENTIFIED BY '123456';
   mysql> flush privileges;
   ```

   **Note:**
   - We recommend that you use an account other than root to remotely log on to the MySQL database.
   - When you create an account, you must replace password 123456 with a password that meets the complexity requirements. The password must be 8 to 30 characters in length, and must contain uppercase letters, lowercase letters, digits, and special characters. Special characters include `( ) ^ ~ ! @ # $ % ^ & * - + = | {} [ ] : ; ' < > , . ? /`

2. Log on to the DMS console.

3. In the left-side navigation pane, click **User-Created Database (ECS, Internet)**.

4. Click **Add Database**.

5. Add the database that you have created. For more information, see **Manage user-created databases hosted on an ECS instance**.

6. Click **Log On**.
   After you are logged on, you can use the menu bar of DMS to create objects such as databases, tables, and functions.

**4.5.2 Manually deploy a MySQL database on Windows**

This topic describes how to manually deploy a MySQL database on a Windows-based Elastic Compute Service (ECS) instance.

**Prerequisites**

An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud official website.
Procedure

1. Activate an ECS instance running Windows Server 2012. For more information, see #unique_4.
2. Remotely connect to an ECS instance. For more information, see #unique_61.
3. Download and install the plug-in vcredist_x86.exe.
5. Install the MySQL database.
   
a) Double-click mysql-installer-community-5.6.15.0.msi to install MySQL.

   ![MySQL Installer]

b) Select **Install MySQL Products**.

![MySQL Installer]

c) Select I accept the license terms and skip the check for updates, click Next, and then select **Custom** to start custom installation. In the right pane, specify the MySQL installation location and the database location, and click **Next**.

   In this example, use the default MySQL installation location and database location.
d) Keep the default values unchanged, click **Next** and then click **Execute** to start the installation.

e) Click **Next** to go to the MySQL Server Configuration page, and select **Server Machine** from the Config Type drop-down list.
f) Keep the default values unchanged, click **Next**, and then enter the password of the root user to complete the installation.

After you install MySQL, the MySQL Command-Line Client icon appears on the start page.

6. Add an inbound rule to the security group of the activated ECS instance to open port 3306. For more information, see #unique_16.
4.5.3 Manage user-created databases hosted on an ECS instance

This topic describes how to use Alibaba Cloud Data Management Service (DMS) to manage user-created MySQL databases hosted on an ECS instance.

Prerequisites

1. **Purchase DMS.**
2. Create an ECS instance. For more information, see #unique_4.
3. Add an inbound security group rule to the ECS instance to enable the default port (port 3306) on which MySQL is listening.
4. Install a MySQL database on the ECS instance.
5. Create a non-root account for the MySQL database.

**Note:**
By default, MySQL does not allow remote access from the root account. If you have changed the default settings to allow remote access from the root account, you can skip this step.

In this example, run the following command to create an account named `dms` for the MySQL database and set the password to `123456`.

```
grant all on *.* to 'dms'@'%' IDENTIFIED BY '123456';
```

Context

DMS is a Web terminal developed by Alibaba Cloud to help manage your databases hosted on ECS instances that run Windows or Linux. You can use DMS by adding your databases through the SMS console. For example, you can create databases and tables. DMS supports such databases as MySQL, SQLServer, PostgreSQL, MongoDB, and Redis. For more information, see [DMS features](#).

Procedure

1. Log on to the Data Management Service console.
2. In the left-side navigation pane, click User-created Databases (ECS, Internet).
3. Click **Add Database**.
4. Set the database parameters as needed.

The following table describes the database parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>The type of the database hosted on the ECS instance. In this example, select MySQL.</td>
</tr>
<tr>
<td>undefinedInstance Source</td>
<td>Valid values: Internet-based User-Created; ECS-based User-Created. In this example, select ECS-based User-Created.</td>
</tr>
<tr>
<td>Region</td>
<td>The region to which the ECS instance belongs.</td>
</tr>
<tr>
<td>ECS InstanceID</td>
<td>The ID of the ECS instance.</td>
</tr>
<tr>
<td>Port</td>
<td>The number of the port used for listening to the database hosted on the ECS instance. In this example, the port configured for MySQL is 3306.</td>
</tr>
<tr>
<td>Databases Username</td>
<td>The username of the database hosted on the ECS instance. In this example, the username of the MySQL database is dms.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> We recommend that you use a non-root account.</td>
</tr>
<tr>
<td>Password</td>
<td>The password corresponding to the username of the database hosted on the ECS instance. In this example, the password of dms is 123456.</td>
</tr>
</tbody>
</table>

5. Click Logon.

After you log on, the data management page is displayed.

What's next

You can manage the database by using the following menus in the top navigation bar:

- **Create**: creates databases, tables, database users, procedures, functions, views, triggers, and events. For more information, see Database development.
- **SQL Operations**: opens the SQL window to run database management commands, including the ability to edit command results. For more information, see SQL operations.
- **Data Operation**: imports, exports, automatically generates, traces, backs up, and restores data, and clones databases and compares table structures. For more information, see Data management.
- **Instance Management**: manages the binlog file of the database and calculates the table data volume.
• **Monitoring Alarm & Diagnosis Optimization**: manages database diagnosis, slow SQL analysis, space diagnosis, instance sessions, real-time performance, and diagnosis reports through the **Performance** menu.

• **Tools**: manages databases, users, ER diagrams, and batch operations, and generates documents (Word/Excel/PDF).

### 4.6 Build a primary/secondary PostgreSQL system

PostgreSQL is one of the most advanced open source database. ApsaraDB RDS for PostgreSQL is compatible with NoSQL databases. It supports efficient queries and plug-in management, and provides secure and stable services. This topic describes how to build a primary/secondary PostgreSQL system on an ECS instance that runs CentOS 7.

#### Prerequisites

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the [Alibaba Cloud official website](#).
- You have added an inbound rule to the security group of the ECS instance to allow traffic from port 5432. For more information, see #unique_16.

#### Context

The procedure described in this topic is applicable to Alibaba Cloud users that are familiar with Alibaba Cloud ECS instances, Linux operating systems, and PostgreSQL databases.

The following software versions are used in this topic. The versions may be different in your actual running environment.

- Operating system: CentOS 7.2
- PostgreSQL: version 9.5.6

You can use one of the following methods to install PostgreSQL on an ECS instance:

- Image deployment: Go to [Alibaba Cloud Marketplace](#) and search for the required PostgreSQL image.
- Manual deployment: Install PostgreSQL by using the source code or Yellowdog Update, Modified (YUM).

#### Procedure

To install PostgreSQL by using YUM and build a primary/secondary architecture of PostgreSQL, perform the following steps:
1. Step 1: Create two ECS instances

To build a primary/secondary architecture of PostgreSQL, you must create two ECS instances that run in a Virtual Private Cloud (VPC). One ECS instance works as the primary node and the other ECS instance works as the secondary node. For more information, see #unique_4.

**Note:**
We recommend that you do not assign public IP addresses to the ECS instances. Instead, you can attach an Elastic IP Address (EIP) to each ECS instance. This allows you to upgrade the configurations or optimize the architecture later on. For more information, see Create an EIP.

2. Step 2: Configure the primary node of PostgreSQL

To configure the primary node of PostgreSQL, perform the following steps:

1. On the primary ECS instance, run the following commands in sequence to install PostgreSQL:

   a. `yum update -y`
   
   b. `yum install https://download.postgresql.org/pub/repos/yum/9.5/redhat/rhel-7-x86_64/pgdg-centos95-9.5-3.noarch.rpm -y`
   
   c. `yum install postgresql95-server postgresql95-contrib -y`
   
   d. `/usr/pgsql-9.5/bin/postgresql95-setup initdb`

**Note:**
The package pgdg-centos95-9.5-3.noarch.rpm is used in this topic. In your actual running environment, use the latest RPM package.

3. Step 3: Configure the secondary node of PostgreSQL

4. Step 4: Test the primary/secondary architecture of PostgreSQL
2. Run the following commands in sequence to start the PostgreSQL service and enable PostgreSQL to run at startup:
   a. systemctl start postgresql-9.5.service #Starts the PostgreSQL service.
   b. systemctl enable postgresql-9.5.service #Enables PostgreSQL to run at startup.

3. Create a database account named replica. This database is used for replication between the primary and secondary nodes. Then, specify the password, logon permission, and backup permission.
   a) Run the following command to log on to PostgreSQL:
      ```
      su - postgres
      ```
   b) Enter `psql` in the following command to go to the PostgreSQL interactive terminal:
      ```
      -bash-4.2$ psql
      ```
   c) Enter the following SQL statement to create the database account named replica, and specify the password, logon permission, and backup permission:
      ```
      postgres=# CREATE ROLE replica login replication encrypted password 'replica';
      ```
   d) Check whether the database account named replica is created:
      ```
      postgres=# SELECT usename from pg_user;
      ```
      The following response indicates that the account named replica has been created:
      ```
      usename
      ----------
      postgres
      replica
      (2 rows)
      ```
   e) Check whether the permissions are created:
      ```
      postgres=# SELECT rolname from pg_roles;
      ```
      The following response indicates that the permissions have been created:
      ```
      rolname
      ----------
      postgres
      replica
      ```
f) Enter \q in the command, and press the Enter key to exit the PostgreSQL interactive terminal:

    postgres=# \q


g) Enter exit in the command, and press the Enter key to exit PostgreSQL:

   -bash-4.2$ exit

logout

4. Run the following command to open the file pg_hba.conf, and set a whitelist for replica:

    vim /var/lib/pgsql/9.5/data/pg_hba.conf

Add the following lines of information to the IPv4 local connections field:

    host all all 192.168.1.0/24 md5              #Enables MD5 password encryption for connections in the CIDR block of the VPC.
    host replication replica 192.168.1.0/24 md5  #Enables data synchronization from the replication database.

5. Run the following command to open the postgresql.conf file:

    vim /var/lib/pgsql/9.5/data/postgresql.conf

Set the following parameters:

    wal_level = hot_standby  #Enables the hot standby mode.
    synchronous_commit = on  #Enables synchronization.
    max_wal_senders = 32    #The maximum number of synchronization processes.
    wal_sender_timeout = 60s #The timeout value for the streaming replication instance to synchronize data.
    max_connections = 100   #The maximum number of connections. The value of max_connections for the secondary node must be greater than that for the primary node.

6. Run the following command to restart the PostgreSQL service:

    systemctl restart postgresql-9.5.service

**Step 3: Configure the secondary node of PostgreSQL**

To configure the secondary node of PostgreSQL, perform the following steps:
1. Run the following commands in sequence to install PostgreSQL:

   a. `yum update -y`

   b. `yum install https://download.postgresql.org/pub/repos/yum/9.5/redhat/rhel-7-x86_64/pgdg-centos95-9.5-2.noarch.rpm -y`

   c. `yum install postgresql95-server postgresql95-contrib -y`

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

   ```
   # pg_basebackup -D /var/lib/pgsql/9.5/data -h <Primary node IP> -p 5432 -U replica -X stream -P
   Password: 30075/30075 kB (100%), 1/1 tablespace
   ```

3. Run the following commands in sequence to create and open the `recovery.conf` file:

   a. `cp /usr/pgsql-9.5/share/recovery.conf.sample /var/lib/pgsql/9.5/data/recovery.conf`

   b. `vim /var/lib/pgsql/9.5/data/recovery.conf`

   Set the following parameters:

   ```
   standby_mode = on       # Declares the secondary node.
   primary_conninfo = 'host=<Primary node IP> port=5432 user=replica password=replica'
   # Connection information of the primary node.
   recovery_target_timeline = 'latest' # Synchronizes the latest data by using streaming replication.
   ```

4. Run the following command to open the `postgresql.conf` file:

   ```
   vim /var/lib/pgsql/9.5/data/postgresql.conf
   ```

   Set the following parameters:

   ```
   max_connections = 1000       # The maximum number of connections. The value for the secondary node must be greater than that for the primary node.
   hot_standby = on             # Enables the 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 the running status to the primary node.
   ```
hot_standby_feedback = on          # Enables the secondary node to report errors during replication.

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

```
chown -R postgres.postgres /var/lib/pgsql/9.5/data
```

6. Run the following commands in sequence to start the PostgreSQL service and enable PostgreSQL to run at startup:

   a. `systemctl start postgresql-9.5.service`  # Starts the PostgreSQL service.

   b. `systemctl enable postgresql-9.5.service`  # Enables PostgreSQL to run at startup.

---

**Step 4: Test the primary/secondary architecture of PostgreSQL**

To test the primary/secondary architecture of PostgreSQL, perform the following steps:

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

```
ps aux |grep sender
```

   The following response indicates that the sender process is available:

   ```
   postgres  2916  0.0  0.3 340388  3220 ?        Ss   15:38   0:00 postgres: wal sender process replica 192.168.1.222(49640) streaming 0/F01C1A8
   ```

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

```
ps aux |grep receiver
```

   The following response indicates that the receiver process is available:

   ```
   postgres 23284  0.0  0.3 387100  3444 ?        Ss   16:04   0:00 postgres: wal receiver process streaming 0/F01C1A8
   ```

3. On the primary node, execute the following SQL statement to check the status of the secondary node:

   ```
   replication=# select * from pg_stat_replication;
   ```

   The following response indicates that the status of the secondary node is available:

   ```
   pid | usesysid | usename | application_name | client_addr | client_hostname | client_port | backend_start | backend_xmin | state | sent_location | write_location | flush_location | replay_location | sync_priority | sync_state
   +---------------+-----------------+---------------+----------------+-------------+-----------------+------------+-------------+-------------+-----+---------------+---------------+---------------+---------------+------------+--------
   +---------------+-----------------+---------------+----------------+-------------+-----------------+------------+-------------+-------------+-----+---------------+---------------+---------------+---------------+------------+--------
   2916 | 16393 | replica | walreceiver | 192.168.1.222 | | 49640 | 2017-05-02 15:38:06.188988+08 | 1836 | streaming | 0/F01C0C8 | 0/F01C0C8 | 0/F01C0C8 | 0/F01C0C8 | 0 | async
   ```
4.7 Deploy and use SVN

4.7.1 Overview

Apache Subversion (SVN) is an open source version control system that manages timeline-based data changes. This topic describes the terms and operations related to SVN.

SVN

The data that SVN manages is stored in a repository. This repository records all changes of files, so that you can reverse the data to an earlier version or review the change history of files. The terms and operations of SVN are listed as follows:

- Repository: stores source code.
- Checkout: checks out source code to a local directory.
- Commit: commits modified code to the repository.
- Update: synchronizes source code in the repository to a local directory.

To manage code in SVN, you typically need to perform these steps:

1. Checkout: Check out source code to a local directory.
2. Other users modify and commit the source code to the repository.
3. Update: Obtain the updates of the source code from the repository.
4. Modify and debug the source code.
5. Commit: Commit the debugged source code to the repository, so other users can view your modifications.

SVN manages source code by line. When you and other users modify the code in a file at the same time:

- If the modified code is in different lines, SVN automatically merges the modifications.
- If the modified code is in the same line, SVN indicates a file conflict. You must confirm the modification manually to resolve the conflict.

Procedure

SVN supports access over HTTP or based on svnserv. You can deploy the access to SVN in these ways:

- Deploy SVN by using svnserv
- Deploy SVN over HTTP
After you deploy SVN, you can commit modifications, obtain updates, and reverse files by using SVN. For more information, see Use SVN.

### 4.7.2 Deploy SVN by using svnserve

This topic describes how to deploy Apache Subversion (SVN) by using svnserve.

**Prerequisites**

- You must have registered an Alibaba Cloud account. If not, create a new Alibaba Cloud account first.
- An instance that is of the ecs.g6.large instance type and runs the CentOS operating system is created. For more information, see #unique_69.
- Inbound rules are added to instance security groups to allow traffic on port 3690, which is the default port of SVN. For more information, see #unique_16.

**Context**

In this topic, the following software versions are used to manually deploy SVN. Choose software versions as needed.

- Operating system: public image CentOS 7.2 64-bit
- Subversion: 1.7.14

**Procedure**

- **Step 1: Install SVN**
- **Step 2: Configure SVN**
- **Step 3: Use a Windows client to test the SVN service**

**Step 1: Install SVN**

1. #unique_15.
2. Run the following command to install SVN:
   ```bash
   yum install subversion
   ```

3. Run the following command to check the SVN version:
   ```bash
   svnserv --version
   ```

Step 2: Configure SVN

1. Run the following command to create a root directory for an SVN repository:
   ```bash
   mkdir /var/svn
   ```

2. Run the following commands in sequence to create an SVN repository:
   ```bash
   cd /var/svn
   svnadmin create /var/svn/svnrepos
   ```

3. Run the following commands in sequence to check files automatically generated in the SVN repository:
   ```bash
   cd svnrepos
   ls
   ```

The following table describes the SVN directories.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>db</td>
<td>Stores all version control data files.</td>
</tr>
</tbody>
</table>
### Directory | Description
--- | ---
hooks | Stores hook scripts.
locks | The client used to track access to the SVN repository.
format | A text file that contains only one integer, indicating the version number of the current SVN repository.
conf | The configuration file of the SVN repository, including the username and permissions for accessing the repository.

4. Set the username and password of the SVN repository.
   a) Run the `cd conf/` command.
   b) Run the `vi passwd` command to open the configuration file.
   c) Press the I key to enter the edit mode.
   d) Move the pointer over the `[users]` field, and add the username and password.
   
   **Note:**
   You can add the username and password in the `username = password` format, such as `userTest = passWDTes` in the following figure. There must be a space on both ends of the equal sign (=).

   ```
   # This file is an example password file for svnserv.
   # Its format is similar to that of svnserve.conf. As shown in the # example below it contains one section labelled [users].
   # The name and password for each user follow, one account per line.
   
   [users]
   # harry = harrysecret
   # sally = sallysecret
   userTest = passWDTes
   ```

   e) Press the Esc key to exit the edit mode, and enter `:wq` to save and close the file.

5. Set the read and write permissions for the account.
   a) Run the `vi authz` command to open the access control file.
   b) Press the I key to enter the edit mode.
   c) Move the pointer over the end of the file and add the following code. In the code, `userTest` specifies the username, `r` specifies the read permission, and `w` specifies the write permission.
userTest=rw

![Configuration file](image)

d) Press the `Esc` key to exit the edit mode, and enter `:wq` to save and close the file.

### 6. Modify the configurations of the SVN service.

a) Run the `vi svnserve.conf` command to open the configuration file of the SVN service.
b) Press the `I` key to enter the edit mode.
c) Move the pointer over the following lines, and delete the number sign (`#`) and space at the beginning of each line.

#### Note:

Each line cannot start with a space and there must be a space on both ends of the equal sign (`=`).

- `anon-access = read` # This assigns read permissions to anonymous users. You can also set `anon-access` to `none` to disable access by anonymous users, and then the revision history of the SVN service can show dates.
- `auth-access = write` # This authorizes write permissions.
- `password-db = passwd` # This specifies the password database file.
- `authz-db = authz` # This specifies the file that stores the authorization rules for path-based access control.
realm = /var/svn/svnrepos # This specifies the authorization realm of the repository

```bash
anon-access = none
auth-access = write

password-db = password

realm = /var/svn/svnrepos

# This option specifies the authentication realm of the repository.
# If two repositories have the same authentication realm, they should
# have the same password database, and vice versa. The default realm
# is repository's uid.
```

d) Press the Esc key to exit the edit mode, and enter :wq to save and close the file.

7. Run the following command to start the SVN repository:

   `svnserve -d -r /var/svn/`

   **Note:**
   Run the `killall svnserve` command to stop the SVN service.

8. Run the `ps -ef | grep svn` command to check whether the SVN service has been started.

   If the following code returned, the SVN service is started.

   ```bash
   [root@server ~]# ps -ef | grep svn
   root       19438  1 0 10:17 ?        00:00:00 svnserve -d -r /var/svn/
   root       19440 19354 0 10:17 ?        00:00:00 grep --color=auto svn
   ```

**Step 3: Use a Windows client to test the SVN service**

1. Download and install the [TortoiseSVN client](https://tortoisesvn.net/) on your local computer.

2. Right-click the blank area in the local project folder.

   In this example, the project folder is C:\KDR.
3. Choose **SVN Checkout**... from the shortcut menu.

4. Configure the following settings and click **OK**:

   - Set the **URL of repository**: field in the following format: svn://Public IP address of the ECS instance/SVN repository name. In this example, the SVN repository name is svnrepos.
   - Set the **Checkout directory**: field. In this example, the directory is C:\KDR.

   ![Checkout Window](image)

   **Note:**
   During the logon for the first time, you must provide the username and password that you have configured in the passwd file.

### 4.7.3 Deploy SVN over HTTP

This topic describes how to deploy Apache Subversion (SVN) over HTTP.

**Prerequisites**

- You must have registered an Alibaba Cloud account. If not, [create a new Alibaba Cloud account](#) first.
An instance that is of the ecs.c6.large instance type and runs the CentOS operating system is created. For more information, see #unique_69.

Inbound rules are added to security groups of the instance to allow traffic on port 3690, which is the default port of SVN. For more information, see #unique_16.

**Context**

In this topic, the following software versions are used to manually deploy SVN. We recommend that you choose the software versions as needed.

- Operating system: public image CentOS 7.2 64-bit
- Subversion: 1.7.14
- Apache HTTP Server: 2.4.6

You can also use images provided by Alibaba Cloud Marketplace to deploy SVN. For more information about how to use SVN images provided by Alibaba Cloud Marketplace to deploy SVN, see the "User guide" section in SVN images (CentOS 64-bit).

**Procedure**

To deploy SVN over HTTP, follow these steps:

1. **Step 1: Install SVN**
2. **Step 2: Install Apache**
3. **Step 3: Install mod_dav_svn**
4. **Step 4: Configure SVN**
5. **Step 5: Configure Apache**
6. **Step 6: Use a browser to test access to SVN**

**Step 1: Install SVN**

1. Connect to a Linux instance.
2. Run the following command to install SVN:

```
yum install subversion
```

3. Run the following command to check the SVN version:

```
svnserve --version
```

**Step 2: Install Apache**

1. Run the following command to install the Hypertext Transfer Protocol daemon (HTTPd):

```
yum install httpd
```

2. Run the following command to check the HTTPd version:

```
httpd -version
```

**Step 3: Install mod_dav_svn**

Run the following command to install mod_dav_svn:

```
yum install mod_dav_svn
```

**Step 4: Configure SVN**

1. Run the following commands in sequence to create an SVN repository:

```
mkdir /var/svn

cd /var/svn
```
Elastic Compute Service

Tutorials / 4 Build an application

svnadmin create /var/svn/svnrepos

2. Run the following command to change the user group of the SVN repository to apache:

chown -R apache:apache /var/svn/svnrepos

3. Run the following commands in sequence to check files automatically generated in the SVN repository:

cd svnrepos

ls

The following table describes the SVN directories.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>db</td>
<td>Stores all version control data files.</td>
</tr>
<tr>
<td>hooks</td>
<td>Stores hook scripts.</td>
</tr>
<tr>
<td>locks</td>
<td>The client used to track access to the SVN repository.</td>
</tr>
<tr>
<td>format</td>
<td>A text file that contains only one integer, indicating the version number of the current SVN repository.</td>
</tr>
<tr>
<td>conf</td>
<td>The configuration file of the SVN repository, including the username and permissions for accessing the repository.</td>
</tr>
</tbody>
</table>

4. Set the username and password of the SVN repository.

a) Run the cd conf/ command.

b) Run the vi passwd command to open the configuration file.

c) Press the I key to enter the edit mode.

d) Move the pointer over the [users] field, and add the username and password.

Note:
You can add the username and password in the username = password format, such as userTest = passWDTesT in the following figure. There must be a space on both ends of the equal sign (=).

```
### This file is an example password file for svnserve.
### Its format is similar to that of svnserve.conf. As shown in the
### example below it contains one section labelled [users].
### The name and password for each user follow, one account per line.

[users]
# harry = harryssecret
# sally = sallyssecret
userTest = passWDTesT
```

e) Press the Esc key to exit the edit mode, and enter :wq to save and close the file.

5. Generate a password for HTTP.

By default, the password for SVN is in plaintext. You must separately generate a passwd file for HTTP because HTTP does not support passwords in plaintext. In this example, the password is passWDTesT.

```
htpasswd /var/svn/svnrepos/conf/passwd userTest
```

6. Set the read and write permissions for the account.

a) Run the vi authz command to open the access control file.

b) Press the I key to enter the edit mode.

c) Move the pointer over the end of the file and add the following code. In the code, userTest specifies the username, r specifies the read permission, and w specifies the write permission.

```
[/]
userTest=rw
```

d) Press the Esc key to exit the edit mode, and enter :wq to save and close the file.
7. Modify the configurations of the SVN service.
   
a) Run the `vi svnserve.conf` command to open the configuration file of the SVN service.

b) Press the I key to enter the edit mode.

c) Move the pointer over the following lines, and delete the number sign (#) and space at the beginning of each line.

   **Note:**
   Each line cannot start with a space and there must be a space on both ends of the equal sign (=).

   `anon-access = read # This assigns read permissions to anonymous users. You can also set anon-access to none to disable access by anonymous users, and then the revision history of the SVN service can show dates.
auth-access = write # This authorizes write permissions.
password-db = passwd # This specifies the password database file.
authz-db = authz # This specifies the file that stores the authorization rules for path-based access control.
realm = /var/svn/svnrepos # This specifies the authorization realm of the repository.
`

d) Press the Esc key to exit the edit mode, and enter `:wq` to save and close the file.
8. Run the following command to start the SVN repository:

```
svnserve -d -r /var/svn/
```

**Note:**
Run the `killall svnserve` command to stop the SVN service.

9. Run the `ps -ef |grep svn` command to check whether the SVN service has been started.

If the following code returned, the SVN service is started.

![image]

**Step 5: Configure Apache**

1. Run the `vim /etc/httpd/conf.d/subversion.conf` command to open the HTTPd configuration file.

2. Press the `I` key to enter the edit mode.

3. Enter the following configuration information:

```
<Location /svn>
DAV svn
SVNParenPath /var/svn
AuthType Basic
AuthName "Authorization SVN"
AuthzSVNAccessFile /var/svn/svnrepos/conf/authz
AuthUserFile /var/svn/svnrepos/conf/passwd
Require valid-user
</Location>
```

4. Press the Esc key, and enter `:wq` to save and close the file.

5. Run the following command to start the Apache HTTP Server:

```
systemctl start httpd.service
```

**Step 6: Use a browser to test access to SVN**

1. Open the browser in the local computer.

2. In the address bar, enter a URL in the `http://<Public IP address of the ECS instance>/svn/<SVN repository name>` format, and press the Enter key. In this example, the SVN repository name is `svnrepos`. 


3. Enter your username and password that you configured in the passwd file. In this example, the username is userTest and the password is passWDTesT.

The following response indicates that you have accessed the created SVN repository.

```
svnrepos - Revision 0: /
```

### 4.7.4 Use SVN

After you deploy Apache Subversion (SVN), you can check out a project from the SVN repository to a local directory, commit local modifications to the repository, obtain updates from the repository, and reverse deleted files.

**Prerequisites**

You have deployed SVN. For more information, see Deploy SVN by using svnserv and Deploy SVN over HTTP.

**Commit modifications**

To commit local modifications to the repository, follow these steps:

1. Right-click the blank area in a project folder, and select **SVN Commit**.
2. Enter the revision comments, select the modifications that you want to commit, and then click **OK**. Then, the original project in the repository is overwritten by the project that you have committed.

**Note:**

A conflict occurs when two users modify the same object of the same version and commit the modifications. In this case, one of the commitments will fail due to the backward version. To avoid this issue, you can back up your local project, check out the latest project from the repository, overwrite the latest project with your local project, and then commit the modified project.

**Obtain updates**

After the project in the SVN repository is updated, you can right-click a blank area in the local project folder, and select **SVN Update** to download and display all updates.
**Note:**

When you right-click a blank area in the local project folder and select SVN Update, all files in the project folder are overwritten. Therefore, we recommend that you back up the original project folder before the update operation, in case some required content may be overwritten.

**Reverse deleted data**

To reverse deleted data, follow these steps:

1. Open a local project folder, right-click the blank area in the folder, and then select **SVN Checkout** to check out data.
2. Delete the data you checked out.
3. Choose between the following methods to reverse the deleted data based on your commitment conditions.
   - If you have not committed the delete operation, right-click the blank area in the folder, and choose **TortoiseSVN > SVN Revert**.
   - If you have committed the delete operation, the modification has been synchronized to the repository, and the corresponding data has also been deleted from the repository. Therefore, to reverse the deleted data, follow these steps:
     a. Check the revision history and determine the data that has been deleted.
     b. Right-click the deleted data and select Revert to this revision.
4. Open the original project folder, right-click the reversed data, and then select **SVN Commit** to synchronize the local reversed data to the repository.
5 Use the Vim editor

Vim is a text editor that is developed as an improved version of the vi editor. It can display text with extra format details, such as font color and underline. Vim is an essential tool in Linux. For example, you can use this tool to edit configuration files of Web applications. This topic describes the modes and commonly used commands of Vim.

Vim modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Function</th>
<th>Mode switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal mode</td>
<td>In this mode, you can copy, paste, and delete characters or lines.</td>
<td>• The tool enters normal mode when you run the <code>vim &lt;file name&gt;</code> command to open a file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To switch from other modes to this mode, press the Esc key.</td>
</tr>
<tr>
<td>Insert mode</td>
<td>In this mode, you can insert characters.</td>
<td>To switch from the normal mode to this mode, enter any of the following characters: ( i, I, a, A, o, O ).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> You will see -- INSERT -- in the lower-left corner of the editor after you switch to this mode.</td>
</tr>
<tr>
<td>Replace mode</td>
<td>In this mode, you can replace characters.</td>
<td>To switch from the normal mode to this mode, enter R.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> You will see -- REPLACE -- in the lower-left corner of the editor after you switch to this mode.</td>
</tr>
<tr>
<td>Visual mode</td>
<td>In this mode, you can select a range of text.</td>
<td>To switch from the normal mode to this mode, enter v.</td>
</tr>
<tr>
<td></td>
<td>You must select a range of text before running commands such as copy , replace, and delete on the specified text.</td>
<td><strong>Note:</strong> You will see -- VISUAL -- in lower-left corner of the editor after you switch to this mode.</td>
</tr>
<tr>
<td>Mode</td>
<td>Function</td>
<td>Mode switch</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Command mode</td>
<td>In this mode, you can search and replace strings, display line numbers, save file changes, and exit the editor.</td>
<td>To switch from the normal mode to this mode, enter .</td>
</tr>
</tbody>
</table>

**Insert**

**Commands**

- **i**: inserts a character to the left of the current character
- **I**: inserts a character at the start of the current line
- **a**: inserts a character to the right of the current character
- **A**: inserts a character at the end of the current line
- **o**: inserts a new line below the current line
- **O**: inserts a new line above the current line

**Examples**

Assume that you want to edit an example.conf file that contains the following content:

```plaintext
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by `httpd -l`) do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
# Include conf.modules.d/*.conf
```

Example 1: Insert Location as the first line of the example.conf file. To do this, follow these steps:

1. Run the `vim example.conf` command to open the file in normal mode.
2. Enter `i` to switch to the insert mode.
3. Enter `Location`.
4. Press the Enter key to switch to a new line.
5. Press the Esc key to exit the insert mode.
6. Enter the :wq command to save the changes to the file and then exit the editor.

After you make this insertion, the example.conf file contains the following content:

```
Location
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding `LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by `httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
# Include conf.modules.d/*.conf
```

Example 2: Insert # at the start of line ten in the example.conf file. To do this, follow these steps:

1. Run the vim example.conf command to open the file in normal mode.
2. Enter :10 to move the cursor to line ten.
3. Enter I to switch to the insert mode.
4. Enter #.
5. Press the Esc key to exit the insert mode.
6. Enter the :wq command to save the changes to the file and then exit the editor.

After you make this insertion, the example.conf file contains the following content:

```
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding `LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by `httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
# Include conf.modules.d/*.conf
```

Example 3: Insert LoadModule rewrite_module modules/mod_rewrite.so in the line below the Include conf.modules.d/*.conf line of the example.conf file. To do this, follow these steps:

1. Run the vim example.conf command to open the file in normal mode.
2. Run the /Include conf.modules.d/*.conf command to find the target line.
3. Enter o to switch to the insert mode.
4. Enter LoadModule rewrite_module modules/mod_rewrite.so.
5. Press the Esc key to exit the insert mode.
6. Enter the `:wq` command to save the changes to the file and then exit the editor.

After you make the insertion, the example.conf file contains the following content:

```plaintext
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by `httpd -l`) do not need
# to be loaded here.
# Example:
# LoadModule foo_module modules/mod_foo.so
# Include conf.modules.d/*.conf
LoadModule rewrite_module modules/mod_rewrite.so
```

**Replace Commands**

R: replaces the highlighted characters, until you press the Esc key to exit the replace mode.

**Example**

Assume that you want to edit an example.conf file that contains the following content:

```plaintext
# 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 None
```

For example, to replace `AllowOverride None` with `AllowOverride All` in the example.conf file, follow these steps:

1. Run the `vim example.conf` command to open the file in normal mode.
2. Run the `/AllowOverride None` command to find the target.
3. Move the cursor to the first letter of `None`.
4. Enter R to switch to the replace mode.
5. Enter All and a space.

**Note:**
The word None has four characters, but the word All has three characters. To replace all the four characters of None, you must type an extra white space following the three characters of All.

6. Press the Esc key to exit the replace mode.
7. Enter the :wq command to save the changes to the file and then exit the editor.

After you make the replacement, the example.conf file contains the following content:

```
# 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
```

Delete

Commands

- x: deletes the highlighted character.
- nx (n represents a number): deletes the highlighted character and the n-1 characters after it.
- dd: deletes the line in which the cursor is located.
- ndd (n represents a number): deletes the line in which the cursor is located and the n-1 lines below it.

Examples

Assume that you want to edit an example.conf file that contains the following contents:

```
# Listen: Allows you to bind Apache to specific IP addresses and/or ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
```

Example 1: Delete # at the start of the #Listen 12.34.56.78:80 line of the example.conf file.

To do this, follow these steps:

1. Run the `vim example.conf` command to open the file in normal mode.
2. Run the `/#Listen 12.34.56.78:80` command to find the target so that the cursor is on the `#` character.
3. Enter the `x` command to delete `#`.
4. Enter the `:wq` command to save the changes to the file and then exit the editor.

After you make the deletion, the example.conf file contains the following content:

```
# Listen: Allows you to bind Apache to specific IP addresses and/or ports, instead of the default. See also the <VirtualHost>
# directive.
#
```
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
Listen 12.34.56.78:80
Listen 80

Example 2: Delete the #Listen 12.34.56.78:80 line and the line below in the example.conf file. To do this, follow these steps:

1. Run the `vim example.conf` command to open the file in normal mode.
2. Run the `/#Listen 12.34.56.78:80` command to find the target.
3. Enter the `2dd` command to delete the following contents.

```
#Listen 12.34.56.78:80
Listen 80
```

4. Enter the `:wq` command to save the changes to the file and then exit the editor.

After you make the deletion, the example.conf file contains the following content:

```
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
```