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="" 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><img src="" alt="Danger" /> Danger: Resetting will result in the loss of user configuration data.</td>
</tr>
<tr>
<td><img src="" 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><img src="" alt="Warning" /> Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.</td>
</tr>
<tr>
<td><img src="" alt="Notice" /></td>
<td>A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.</td>
<td><img src="" alt="Notice" /> Notice: If the weight is set to 0, the server no longer receives new requests.</td>
</tr>
<tr>
<td><img src="" alt="Note" /></td>
<td>A note indicates supplemental instructions, best practices, tips, and other content.</td>
<td><img src="" alt="Note" /> Note: You can use Ctrl + A to select all files.</td>
</tr>
<tr>
<td><img src="closing_brackets" alt="&gt;" /></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 <code>cd /d C:/windows</code> 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><code>bae log list --instanceid Instance_ID</code></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 Deploy LAMP on ECS..................................................................................... 3
  2.2 Deploy LNMP............................................................................................... 17
    2.2.1 Use ROS............................................................................................... 17
    2.2.2 Build LNMP environment under CentOS 6............................................. 22
    2.2.3 Manually build an LNMP environment in CentOS 7............................ 31
  2.3 Configure Java Web....................................................................................... 42
    2.3.1 Deploy a Java Web project................................................................... 42
    2.3.2 Use Cloud Toolkit to deploy a Java web environment......................... 46
  2.4 Deploy Windows by changing the image....................................................... 60
  2.5 Deploy a Node.js project on CentOS............................................................. 63

3 Build a website.................................................................................................... 68
  3.1 Build a WordPress blog platform................................................................. 68
    3.1.1 Deploy a WordPress site based on ECS and RDS................................. 68
  3.2 Build a Magento website on ECS................................................................. 72
  3.3 Deploy the Ghost blogging platform on CentOS 7......................................... 79
  3.4 Build a Drupal website.................................................................................. 89

4 Build an application............................................................................................. 94
  4.1 Build Microsoft SharePoint 2016 on an ECS instance................................... 94
  4.2 Install SharePoint 2016................................................................................ 106
  4.3 Build Docker............................................................................................... 108
  4.4 Deploy databases based on ECS................................................................. 113
    4.4.1 Manually deploy a MySQL database on a Linux ECS instance............ 113
    4.4.2 Manually deploy a MySQL database on Windows............................. 117
  4.5 Build a primary/secondary PostgreSQL system.......................................... 121
  4.6 Deploy and use SVN.................................................................................... 128
    4.6.1 Overview............................................................................................. 128
    4.6.2 Deploy access to SVN by using svnserv............................................. 129
    4.6.3 Deploy access to SVN over HTTP....................................................... 134
    4.6.4 Use SVN........................................................................................... 138
  4.7 Build an FTP site on an ECS instance.......................................................... 139
    4.7.1 Build an FTP site on a Linux instance.............................................. 139
    4.7.2 Build an FTP site on a Windows ECS instance................................. 149

5 Use the Vim editor.............................................................................................. 152
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 Deploy LAMP on ECS

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

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 example uses an ECS instance with the following configuration:

• Uses the 64-bit CentOS 7.2 operating system
• Uses a VPC network
• Uses the public IP address of the ECS instance

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

• Apache 2.4.37
• 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 start the ECS instance to quickly build a website.

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 HTTP Server
3. Step 3. Install the MySQL database management system
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.

   ```
   [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 firewall status.

      ```
      [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 status is inactive, the firewall is disabled.
      
      • If the firewall status is active, the firewall is enabled. In this example, the firewall is enabled. Therefore, you must disable the firewall.

   b) The firewall must be disabled. If the firewall has already been disabled, skip this step.

      • If you want to temporarily disable the firewall, run the `systemctl stop firewalld` command.

      ![Note:](#)

      *This command temporarily disables the firewall. After you restart the Linux operating system, the firewall is enabled.*

      • If you want to permanently disable the firewall, run the `systemctl disable firewalld` command.

      ![Note:](#)

      *You can enable the firewall again. For more information, see the firewall site.*
5. Disable SELinux.
   a) Run the `getenforce` command to check the SELinux status.

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

   • If the SELinux status is Disabled, SELinux is disabled.
   • If the SELinux status is Enforcing, SELinux is enabled. In this example, SELinux is enabled. Therefore, you must disable SELinux.

   b) Disable SELinux. If SELinux has already been disabled, skip this step.

   • If you want to temporarily disable SELinux, run the `setenforce 0` command.

   **Note:**
   This command temporarily disables SELinux. After you restart the Linux operating system, SELinux is enabled.

   • If you want to permanently disable SELinux, run the `vi /etc/selinux/config` command to edit the configuration file of SELinux. Press Enter to run the command, move the cursor to the SELINUX=enforcing row, and press I to edit the configuration file. Change SELINUX=enforcing to SELINUX=disabled, press Esc, enter :wq, and then press Enter to save and close the configuration file.

   **Note:**
   You can enable SELinux again. 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 open the required port. For more information, see #unique_16.

Step 2. Install Apache HTTP Server

Follow these steps to install Apache HTTP Server.
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:
   
   a. `wget https://mirrors.aliyun.com/apache/httpd/httpd-2.4.37.tar.gz`
   
   b. `wget https://mirrors.aliyun.com/apache/apr/apr-1.6.5.tar.gz`
   
   c. `wget https://mirrors.aliyun.com/apache/apr/apr-util-1.6.1.tar.gz`
   
   d. `tar xvf httpd-2.4.37.tar.gz -C /usr/local/src`
   
   e. `tar xvf apr-1.6.5.tar.gz -C /usr/local/src`
   
   f. `tar xvf apr-util-1.6.1.tar.gz -C /usr/local/src`

   **Note:**
   
   The source code version is continuously upgraded. You can obtain the installation package path in the [httpd source code installation package](https://mirrors.aliyun.com) or the [APR source code installation package](https://mirrors.aliyun.com).

3. Run the following commands to move the APR and APR-util folders to the Apache srclib folder:
   
   a. `cd /usr/local/src`
   
   b. `mv apr-1.6.5 httpd-2.4.37/srclib/apr`
   
   c. `mv apr-util-1.6.1 httpd-2.4.37/srclib/apr-util`

4. Run the following commands to compile the source code:
   
   a. `cd /usr/local/src/httpd-2.4.37`
   
   b. `./buildconf`
   
   c. `./configure --prefix=/usr/local/apache2 \ 
      --enable-ssl \ 
      --enable-so \ 
      --with-mpm=event \ 
      --with-included-apr \ 
      --enable-cgi \ 
      --enable-rewrite \ 
      --enable-mods-shared=most \`
Elastic Compute Service

Tutorials / 2 Build a software development environment

```
--enable-mpms-shared=all
d.
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.

```
[root@test httpd-2.4.37]# httpd -v
Server version: Apache/2.4.37 (Unix)
Server built: Nov 30 2018 15:42:54
```

7. Add the Apache configuration file.
   a) Run the `vi /usr/lib/systemd/system/httpd.service` command to open the
      configuration file.
   b) Press I 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 Esc, enter `:wq`, and then press Enter to save and close the Apache configuration
      file.
8. Run the following commands to start Apache HTTP Server and enable Apache HTTP Server to automatically start when the operating system is started.

   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**.
   d) Enter `http://` The public IP address of the ECS instance into the address bar of your browser, and then press Enter.

   If the following page is displayed, it indicates that Apache HTTP Server has been started.

   ![It works!](image)

**Step 3. Install the MySQL database management system**

Follow these steps to install the MySQL database management system:
1. Run the following commands to prepare the compiling 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 GA version of the source code:
   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 \
      -DSYSTEMD=1 \
      -DMYSQL_UNIX_ADDR=/usr/local/mysql/mysql.sock \
      -DDEFAULT_CHARSET=utf8 \
      -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
datadir = /mnt/data/" >> /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 I and enter the following content:

     ```
     [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 Esc, enter :wq, and then press Enter 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 automatically start when the operating system is started:
    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`

13. Run the `\q` command to log out of MySQL.

**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:

   a. `cd`

   b. `wget http://cn2.php.net/get/php-7.0.32.tar.bz2/from/this/mirror`

   c. `cp mirror php-7.0.32.tar.bz2`

   d. `tar xvf php-7.0.32.tar.bz2 -C /usr/local/src`

   e. `cd /usr/local/src/php-7.0.32`

   f. `./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-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-bz2`

   g. `make && make install`

**Note:**

If the ECS instance does not have sufficient memory space, terminate PHP extensions that you do not need when you configure PHP to save memory space. For example, you can add `--disable-fileinfo` 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 vi /usr/local/apache2/conf/httpd.conf command to open the Apache configuration file, and then press I to edit the configuration file.

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

```ini
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
# If your host doesn't have a registered DNS name, enter its IP address here.
# ServerName: www.example.com:80
ServerName: localhost:80
```

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

```xml
<Directory />
  AllowOverride none
  #Require all denied
  Require all granted
</Directory>
```

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

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

d) Find the following content:

```ini
# 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
```

After you add the content, the configuration is as follows.

```
# AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
```

e) Press Esc, enter :wq, and then press Enter 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 I to edit the file. Add the following content to the file:

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

c) Press Esc to exit the edit mode. Enter :wq to save and close the index.php file.

d) Run the following command to restart Apache HTTP Server.

```
systemctl restart httpd
```

6. Enter `http://` The public IP address of the ECS instance into the address bar of your browser and press Enter.

If the following page is displayed, it indicates that PHP parsing is working properly.
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 command 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 file to the prepared storage directory:
   `mv phpMyAdmin-4.0.10.20-all-languages/* /usr/local/apache2/htdocs/phpmyadmin`

4. Enter `http://The public IP address of the ECS instance/phpmyadmin` into the address bar of your browser, and press Enter to go to the logon page of phpMyAdmin.
   If the following page is displayed, it indicates that phpMyAdmin has been installed.
5. Enter the MySQL username and password, and click Go.

2.2 Deploy LNMP

2.2.1 Use ROS

An LNMP environment is based on four major components required in this architecture: Linux, NGINX, MySQL, and PHP. This topic describes how to use Alibaba Cloud Resource Orchestration Service (ROS) to efficiently deploy the LNMP environment.

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

ROS is a free service. You do not need to download or install any package. 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 Template. For example, you can use the LNMP_basic template in the ROS console to automatically create an ECS instance, and deploy the LNMP environment on this instance.

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.

For more information about ROS, see ROS documentation.

Procedure

1. Log on to the ROS console.

   ![Note]
   
   The first time that you use the ROS service, you are prompted to activate this service. ROS is a free service, so you can activate ROS free of charge.

2. In the left-side navigation pane, choose Key Help > ECS Instance Information, click the ECS Instance Type tab to find the target instance type in the Instance Type column, click the ECS Zone tab to find the target zone ID in the ZoneId column, and then click the ECS Image tab to find the target image ID in the Image List column.

3. In the left-side navigation pane, click Sample Template.

4. Find the sample template LNMP_basic.
5. Click **Preview** 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 use of the template.</td>
</tr>
<tr>
<td>&quot;Parameters&quot;: {}</td>
<td>Specifies some parameters. 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. In 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. In 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. Select the region where the ECS instance is located from the **Region** drop-down list, such as **China (Hangzhou)**, and click **Next**.

8. Set stack parameters, and click **Create**.

   - **Stack Name**: specifies a unique stack name. You cannot change the stack name after ROS creates the stack.
   - **Creation timeout (minutes)**: specifies a period. If ROS fails to create the specified resources within the period, the creation operation will time out. You can select or
clear Roll back. If you select Roll back, ROS will delete the created resources when an error such as creation timeout occurs during the creation process.

- **Nginx Download Url**: specifies the default NGINX download URL.
- **DB Password** and **(Please Confirm) DB Password**: specify the password for accessing a MySQL database and confirm the password. The password must contain only letters and digits.
- **The ECS Available Zone ID**: the zone ID of the resource that you want to create. For more information, see Step 2.
- **ECS Image Id**: the ID of the image that ROS uses to create the ECS instance. For more information, see Step 2.
- **DB Name**: the name of the MySQL database.
- **DB Username**: the username of the MySQL database.
- **DB Root Password** and **(Please Confirm) DB Root Password**: specify the password of a MySQL root user and confirm the password. The password must contain only letters and digits.
- **ECS Instance Type**: the type of the ECS instance that you want to create. For more information, see Step 2.
- **System Disk Category**: the type of the disk.
- **Instance Password** and **(Please Confirm) Instance Password**: specify the password for logon to the ECS instance and confirm the password. The password must contain only letters and digits.
Create Stack

Stack Name: LNMP-ROS-TEST

Parameters:
- Nginx Download URL: http://nginx.org/packages/centos/7/noarch/RPMS/nginx-1.18.0-1.el7.centos.noarch.rpm
  - The download path of nginx-*rpm
- DB Password: ******
  - Password MySQL database access
- Confirm DB Password: ******
  - Password MySQL database access
- The ECS Available Zone ID: cn-beijing-h
  - The ECS Available Zone ID, Notice: Whether cloned ecs Type is supported in the available zone, View zoneid info
- ECS Image ID: centos_7
  - Image Id, represents the image resource to startup one ECS instance, View image resources
- DB Name: MyDatabase
  - MySQL database name
- DB Username: dms
  - Username for MySQL database access
- DB Root Password: ******
  - Root password for MySQL
- Confirm DB Root Password: ******
  - Root password for MySQL
- ECS Instance Type: ecs.s5.large
  - The ECS instance type, View instance types
- System Disk Category: cloud_ssd
  - System disk category: average cloud disk(cloud), efficient cloud disk(cloud_efficiency) or SSD cloud disk(cloud_ssd)
- Instance Password: ******
  - The login password of ECS instances
- Confirm Instance Password: ******
  - The login password of ECS instances
9. In the left-side navigation pane, click **Stack Management** to check the state of the stack that you have created.

![Stacks](image)

10. Click the name of the created stack. In the **Output** section on the **Stack Overview** page, check the value of `NginxWebsiteURL`. You can use the URL to connect to the LNMP environment that you have created.

![Stack Overview](image)

**Note:**

- On the **Resource List** page, you can check all resources of the stack.
- On the **Event List** page, 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.
- On the **Stack Template** page, you can check the original template of the stack.

### 2.2.2 Build LNMP environment under CentOS 6

This article describes how to build LNMP environment under CentOS on an ECS instance with the basic configuration.

- **Linux**: A family of free and open-source UNIX-like software operating systems (OS).
- **Nginx**: A lightweight HTTP and reverse proxy server.
- **MySQL**: A relational database management system.
- **PHP**: A scripting language that is especially suited for web development.
Audience

This method is applicable to individual users who are familiar with Linux, but new to website construction by using Alibaba Cloud ECS.

Procedure

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

1. Prepare the compiling environment.
2. Install Nginx.
3. Install MySQL.
4. Install MySQL.
5. Test.

**Step 1: Prepare the compiling environment**

Follow these steps to prepare the compiling environment. You can also buy LNMP images at the Cloud Market to start your ECS instance for website quick building.

1. Check the version of the operating system.

```bash
# cat /etc/redhat-release
CentOS release 6.5 (Final)
```

*Note:*

This article is based on a Linux instance running CentOS 6.5. You may have different OS versions. The same is applicable to the Nginx, MySQL, and PHP versions mentioned in the following paragraphs.

2. Disable SELINUX.

Run the command to modify the configuration file, which permanently takes effect after you restart the service.

```bash
# sed -i 's/SELINUX=. */SELINUX=disabled/g' /etc/selinux/config
```

Run the command to make the configuration take effect immediately.

```bash
# setenforce 0
```


Add a security rule to accept Internet access to the Web server on the instance.

**Step 2: Install Nginx**
Nginx is a small and highly-efficient Web server based on Linux. Follow these steps to install Nginx:

1. Add a user to run the Nginx service process.

   ```
   # groupadd -r nginx
   # useradd -r -g nginx
   ```

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

   ```
   # wget http://nginx.org/download/nginx-1.10.2.tar.gz
   # tar xvf nginx-1.10.2.tar.gz -C /usr/local/src
   # yum groupinstall "Development tools"
   # yum -y install gcc wget gcc-c++ automake autoconf libxml2-devel libxslt-devel perl-devel perl-ExtUtils-Embed pcre-devel openssl-devel
   # cd /usr/local/src/nginx-1.10.2
   # ./configure
   --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
   --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
   --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
   # mkdir -pv /var/tmp/nginx/client
   ```

3. Add a SysV startup script.

   ```
   # vim /etc/init.d/nginx
   #!/bin/sh
   ```
# nginx - this script starts and stops the nginx daemon
#
# chkconfig:   - 85 15
# description: Nginx is an HTTP(S) server, HTTP(S) reverse \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
demon $nginx -c $NGINX_CONF_FILE
   retval=$?
   echo
   [ $retval -eq 0 ] && touch $lockfile
   return $retval
}
stop() {
   echo -n "$prog: 
   killproc $prog -QUIT
   retval=$?
   echo
   [ $retval -eq 0 ] && rm -f $lockfile
   return $retval
killall -9 nginx
}
restart() {
   configtest || return $?
   stop
   sleep 1
   start
}
reload() {
   configtest || return $?
   echo -n "$prog: 
   killproc $prog -HUP
   RETVAL=$?
   echo
   [ RETVAL -eq 0 ] && touch $lockfile
   return $retval
}
force_reload() {
   restart
}
configtest() {
   $nginx -t -c $NGINX_CONF_FILE
}
rh_status() {
   status $prog
}
rh_status_q() {
   rh_status >/dev/null 2>&1
4. Grant the permission to run the script.

   # chmod +x /etc/init.d/nginx

5. Add Nginx to the service management list, and set it to automatically start on startup.

   # chkconfig --add nginx
6. Start the service.

# service nginx start

7. Access the instance by using http://Public IP address. If the following page appears, Nginx is installed successfully.

```
Welcome to nginx on EPEL!

This page is used to test the proper operation of the nginx HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly.

Website Administrator

This is the default index.html page that is distributed with nginx on EPEL. It is located in /usr/share/nginx/html.

You should now put your content in a location of your choice and edit the root configuration directive in the nginx configuration file /etc/nginx/nginx.conf.
```

Step3: Install MySQL

1. Prepare the compiling environment.

```bash
# yum groupinstall "Server Platform Development" "Development tools" -y
# yum install cmake -y
```

2. Create a directory to store the data of MySQL.

```bash
# mkdir /mnt/data
# groupadd -r mysql
# useradd -r -g mysql -s /sbin/nologin mysql
# id mysql
uid=497(mysql) gid=498(mysql) groups=498(mysql)
```

3. Change the owner and group of the data directory.

```bash
# chown -R mysql:mysql /mnt/data
```

4. Decompress and compile the stable source code package downloaded from MySQL official website. In this article, we use version 5.6.24.

```bash
# tar xvf mysql-5.6.24.tar.gz -C /usr/local/src
```
5. Change the group of the installation directory to mysql.

```bash
# chown -R mysql:mysql /usr/local/mysql/
```

6. Initializes the database.

```bash
# /usr/local/mysql/scripts/mysql_install_db --user=mysql --datadir=/mnt/data/
```

**Note:**
After completing the minimum installation of the CentOS 6.5 operating system, a my.cnf file is generated under the /etc directory. You must rename this file. For example, rename it as /etc/my.cnf.bak. Otherwise, this file will interfere with the correct configuration for MySQL source code installation, leading to MySQL start failure.

7. Copy the configuration file and startup script.

```bash
# cp /usr/local/mysql/support-files/mysql.server /etc/init.d/mysqld
# chmod +x /etc/init.d/mysqld
# cp support-files/my-default.cnf /etc/my.cnf
```

8. Set automatic start on startup.

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

9. Modify the installation path and data storage path in the configuration file.

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

10. Set the PATH environment variable.

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

11. Start the service.

```bash
# service mysqld start
```
**Step 4: Install PHP-FPM**

Nginx cannot process PHP. As a Web server, when Nginx receives a request, it does not support directly calling or parsing the external program. It must use FastCGI to call such programs. However, in case of PHP requests, Nginx will transfer the request to a PHP interpreter, and return the result to the client. PHP-FPM is a FastCGI process manager that supports parsing PHP code. PHP-FPM provides better PHP process management methods, which can effectively control the memory and process, and can support smoothly reloading PHP configuration.

1. Install dependency package.

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

2. Decompress the source code package downloaded from the official website, and then compile and install it.

   ```bash
   # tar xvf php-5.6.23.tar.bz2 -C /usr/local/src
   # cd /usr/local/src/php-5.6.23
   # ./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 
   --with-bz2
   # make && make install
   ```

3. Add the PHP and PHP-FPM configuration files.

   ```bash
   # 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
   ```

4. Add the PHP-FPM startup script.

   ```bash
   # cp /usr/local/src/php-5.6.23/sapi/fpm/init.d.php-fpm /etc/init.d/php-fpm
   ```
5. Add PHP-FPM to the service list, and set it to automatically start on startup.

```
# chmod +x /etc/init.d/php-fpm
# chkconfig --add php-fpm
# chkconfig --list php-fpm
# chkconfig php-fpm on
```

6. Start the service.

```
# service php-fpm start
```

7. Follow these steps to configure Nginx to support fastcgi: Back up the default configuration file.

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

Edit `/etc/nginx/nginx.conf`: Add a home page in the PHP format into the supported home page formats as follows.

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

Delete comments in front of the following content.

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

Reload the Nginx configuration file.

```
# service nginx reload
```

Create an index.php test page under `/usr/local/nginx/html/`, the content of which is shown as follows.

```
# cat index.php
<?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();
```
Access the instance by using http://Public IP address/index.php. If the following page appears, LNMP environment is built successfully.

<table>
<thead>
<tr>
<th>System</th>
<th>Linux (Zoe66JhT57vr202hrp7i2GJ2.6.22-575.22.1.x6.x86_64)</th>
<th>21.SMP Thu Mar 23 03:35:29 UTC 2023 x86_64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build Date</td>
<td>Dec 17 2016 21:17:58</td>
<td></td>
</tr>
</tbody>
</table>
| Configure Command | `./configure --prefix=/usr/local/php` 
                        `--with-config-file-path=/etc/php` 
                        `--with-config-file-path=/usr/local/etc/php` |                                             |
| Server API | PHP/Perl/CGI                                         |                                             |
| Virtual Directory Support | disabled                           |                                             |
| Configuration File (php.ini) Path | /etc  |                                             |

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. The LNMP environment is based on the four major components required in this architecture: Linux, NGINX, MySQL, and PHP. This topic describes how to manually build an LNMP environment on an ECS instance.

Prerequisites

- You must have registered an Alibaba Cloud account. If not, create a new Alibaba Cloud account first.
- You have created an ECS instance and assigned a public IP address to the instance. For information about how to create an instance, see #unique_22.
You have added an inbound rule 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>Authorization policy</th>
<th>Protocol</th>
<th>Port range</th>
<th>Priority</th>
<th>Authorization type</th>
<th>Authorization object</th>
</tr>
</thead>
</table>
| Inbound        | Allow                | HTTP (80)| 80/80      | 1        | IPv4 CIDR block    | 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.

**Context**

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.

You can also create a website by purchasing an LNMP image from Alibaba Cloud Marketplace and launching an ECS instance from the image.

This example uses an ECS instance with the following configurations: The actual operation depends on your instance configuration.

- 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:

- Operating system: public image for CentOS 7.2 64-bit
- NGINX version: 1.16.1
- MySQL version: 5.7.28
• PHP: version: 7.0.33

Note:
When you use software versions different from the preceding versions, you may need to adjust the commands and parameter settings as needed.

Procedure

To manually build an LNMP environment on an ECS instance, follow these steps:

• Step 1: Prepare the compiling 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 compiling 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.

   ```bash
   [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: 20705 (firewalld)
   
   Stopping 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 the firewall must be disabled.

   b) Disable the firewall. Skip this step if the firewall is already in the inactive state.
      • To temporarily disable the firewall, run the `systemctl stop firewalld` command.
After running this command, the firewall is temporarily disabled. It will enter the active state when you next restart the instance.

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

**Note:**
You can re-enable the firewall after it has been disabled. For more information, see the firewalld website.

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

   ```bash
   [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 SELinux must be disabled.

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

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

   **Note:**
   After running this command, SELinux is temporarily disabled. It will enter the Enforcing state when you next restart the instance.

   - To indefinitely disable SELinux, follow these steps: Run the `vim /etc/selinux/config` command. 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. Type `:wq` and then press the Enter key to save and close the SELinux configuration file.

   **Note:**
   You can re-enable SELinux after it has been disabled. For more information, see the SELinux website.

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

1. Run the following command to install NGINX:

   ```bash
   yum -y install nginx
   ```

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

   ```bash
   nginx -v
   ```

   The following response indicates that NGINX has been installed:

   ```bash
   nginx version: nginx/1.16.1
   ```

Step 3: Install MySQL

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

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

2. Run the following command to install MySQL:

   ```bash
   yum -y install mysql-community-server
   ```

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

   ```bash
   mysql -V
   ```

   The following response indicates that MySQL has been installed:

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

Step 4: Install PHP

1. Update the YUM Repository.

   a) Run the following command to add the IUS repository:

   ```bash
   # Before running the command, replace <Version number> with the currently available version number.
   ```
This example uses ius-release 1.0-15, so the command is as follows:

```
```

You can take the following steps to check available version numbers of IUS:

A. Visit the ius community website.

B. Enter ius-release in the search box.

C. Select the version number with the centos7 characters. The content in the following red box is the available version number.

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-mysqli php70w-fpm php70w-opcache php70w-pecl-redis php70w-pecl-mongodb
```

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

```
php -v
```

The following response indicates that PHP has been 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.

Note:
If you do not add this configuration, the PHP page cannot be displayed when accessed through a browser later.

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

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

b) Press the I key to enter editing mode.

c) Within the Server braces, add the following configuration information:

```
# Retain the default values for all settings except the following settings:
location / {
  # Add the following information in 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
  fastcgi_pass 127.0.0.1:9000;  # NGINX forwards PHP requests to PHP FastCGI
  fastcgi_index index.php;
  fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
  include fastcgi_params;  # NGINX calls the FastCGI operation to process PHP
  requests.
}
```
The configurations are as shown in the following figure.

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    server_name ;
    root /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf:

    location / {
        index index.php index.html index.htm;
    }
    location ~ .php$ {
        root /usr/share/nginx/html;
        fastcgi_pass 127.0.0.1:9000;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        include fastcgi_params;
    }
    error_page 404 /404.html;
    location = /40x.html {
    }

    error_page 500 502 503 504 /50x.html;
    location = /50x.html {
    }
}
```

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

```
systemctl start nginx
```

4. Run the following command to enable the NGINX service to run during startup:

```
systemctl enable nginx
```

**Step 6: Configure MySQL**

1. Run the following command to launch MySQL:

```
systemctl start mysqld
```

2. Run the following command to enable the MySQL service to run during 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
```

The response 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 the initial password to reset the password of the root user.

4. Run the following command to configure your MySQL databases and secure data:

```
mysql_secure_installation
```

Continue with these steps for the security configuration:

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  
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: # Re-enter the new password 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 the anonymous user account.

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, see MySQL documentation.
Step 7: Configure PHP

1. Create the phpinfo.php file to display phpinfo information.
   a) Run the following command to create the file:

   ```
   vim <Website root directory>/phpinfo.php  # Replace <Website root directory> with your configured 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:

   ![Location configuration example]

   In this example, the website root directory is /usr/share/nginx/html, so the command is as follows:

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

   b) Press the I key to enter editing mode.

   c) Enter the following content:

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

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

2. Run the following command to start PHP-FPM:

   ```
   systemctl start php-fpm
   ```

3. Run the following command to enable PHP-FPM to run during startup:

   ```
   systemctl enable php-fpm
   ```

Step 8: Test the connection to the LNMP environment

1. Open your browser.
2. In the address bar, enter the URL http://<Public IP address of the ECS instance>/phpinfo.php.

The following response indicates that the LNMP environment has been deployed.

![PHP Version 7.0.33](image)

What's next

Afterward, we recommend that you run the following command to delete the phpinfo.php file to ensure system security:

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

The website root directory configured in this example is /usr/share/nginx/html, so the command is as follows:

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

2.3 Configure Java Web

2.3.1 Deploy a Java Web project

This article describes how to deploy a Java Web project on a Linux instance with the basic configuration. This method is applicable to individual users who are new to website construction by using ECS.

Configuration requirements

The following programs are used as examples to deploy the Java Web project:

- OS: CentOS 7.4
- Tomcat: Tomcat 8.5.23
- JDK: JDK 1.8.0_141
Preparations

- The firewall is enabled by default for CentOS 7.4. You can disable the firewall, or add rules on the firewall by referring to official documents to open Ports 80, 443, or 8080 for inbound access.
  - Disable the firewall.
    
    ```bash
    systemctl stop firewalld.service
    ```
  - Set the firewall not to be enabled automatically at startup.
    
    ```bash
    systemctl disable firewalld.service
    ```
- Create a user www to run Tomcat.
  
  ```bash
  useradd www
  ```
- Add a security group rule to open Port 8080 for HTTP access. For more information, see add a security group rule.
- Creates a root directory for the Java Web project.
  
  ```bash
  mkdir -p /data/wwwroot/default
  ```
- Create a Tomcat test page.
  
  ```bash
  echo Tomcat test > /data/wwwroot/default/index.jsp
  chown -R www.www /data/wwwroot
  ```

Download source code

```bash
wget https://mirrors.aliyun.com/apache/tomcat/tomcat-8/v8.5.23/bin/apache-tomcat-8.5.23.tar.gz
```

The source code is constantly upgraded. You can find the installation package at https://mirrors.aliyun.com/apache/tomcat/tomcat-8/.

```bash
wget http://mirrors.linuxeye.com/jdk/jdk-8u141-linux-x64.tar.gz
```

The source code is constantly upgraded. You can find the installation package at http://mirrors.linuxeye.com/jdk/.

Install JDK

To install JDK, follow these steps:
1. Run `mkdir /usr/java` to create a directory.

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

2. Run the following command to decompress `jdk-8u141-linux-x64.tar.gz` to the `/usr/java` directory.

   ```bash
   tar xzf jdk-8u141-linux-x64.tar.gz -C /usr/java
   ```

3. Follow these steps to set environment variables:
   a. Run `vi /etc/profile`:

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

   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_141
   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, and then type `:wq` to save and close the file.

4. Run `source /etc/profile` to load the new environment variable.

5. Check the version of JDK. When the JDK version is displayed, it indicates that JDK has been installed successfully.

   ```bash
   java -version
   ```

   ```bash
   java -version
   java version "1.8.0_141"
   Java(TM) SE Runtime Environment (build 1.8.0_141-b15)
   Java HotSpot(TM) 64-Bit Server VM (build 25.141-b15, mixed mode)
   ```

**Install Tomcat**

To install Tomcat, follow these steps:

1. Run the following commands one by one to decompress `apache-tomcat-8.5.23.tar.gz`, rename the Tomcat directory, and set user permissions.

   ```bash
   tar xzf apache-tomcat-8.5.23.tar.gz
   mv apache-tomcat-8.5.23 /usr/local/tomcat/
   chown -R www.www /usr/local/tomcat/
   ```

**Note:**

In the `/usr/local/tomcat/` directory:
The bin directory stores some Tomcat script files, including scripts for enabling and disabling Tomcat service.

The conf directory stores various global configuration files for Tomcat server, the most important of which are server.xml and web.xml.

The webapps directory is the main Web publishing directory of Tomcat, which stores Web application files by default.

The logs directory stores Tomcat log files.

2. Follow these steps to configure the server.xml file:
   

b. Rename the server.xml file: mv server.xml server.xml_bk.

c. Create a new server.xml file:
   
   A. Run vi server.xml.
   
   B. Press the i key to enter the Edit mode.

   C. 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.UserDatabase" 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" 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>
  </Service>
</Server>
```

3. Follow these steps to set JVM memory parameters:
   
a. Run vi /usr/local/tomcat/bin/setenv.sh.

b. Press the i key to enter the Edit mode.

c. Add the following content.

```bash
JAVA_OPTS='-Djava.security.egd=file:/dev/urandom -server -Xms256m -Xmx496m -Dfile.encoding=UTF-8'
```
d. Press the Esc key, and then type :wq to save and close the file.

4. Follow these steps to set Tomcat automatic startup script:

   a. Run the command to download the script:
      ```bash
      ```
   b. Run the command to rename Tomcat-init:
      ```bash
      mv Tomcat-init /etc/init.d/tomcat
      ```
   c. Add the permission:
      ```bash
      chmod +x /etc/init.d/tomcat
      ```
   d. Set the startup script JAVA_HOME.
      ```bash
      sed -i 's@^export JAVA_HOME=.*@export JAVA_HOME=/usr/java/jdk1.8.0_141@' /etc/init.d/tomcat
      ```

5. Set automatic startup.

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


   ```bash
   service tomcat start
   ```

7. Access the instance by using http://Public IP address:8080. If the following page appears, Tomcat is installed successfully.

   ![Tomcat test](image)

### 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**

- You must have registered an Alibaba Cloud account. If not, create a new Alibaba Cloud account first.
• 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 Install window showing selected software and contact option cleared]

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.

![Software Updates](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**.

![Image of Access Key ID and Access Key secret](image)

**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 - firewall - 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: 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
cd /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
<? 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">
```

   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:

   ```
   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:

   ```
   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.

![Eclipse Deploy to ECS](image)

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. In this
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]

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]

**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**

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**
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.
- You must have registered an Alibaba Cloud account. If not, create a new Alibaba Cloud account first.

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](#unique_30).
2. Use the `root` user to connect to the ECS instance. For more information, see [#unique_30](#unique_30).

**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.**
   ```bash
   wget https://nodejs.org/dist/v6.9.5/node-v6.9.5-linux-x64.tar.xz
   ```
2. **Decompress the file.**
   ```bash
   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.**
   ```bash
   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.**
   ```bash
   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:

- 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.

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

2. Activate NVM.

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

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

   nvm list-remote

4. Install multiple Node.js versions.

   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@iZXXXZ .nvm]# nvm ls
   v6.9.5
   -> v7.4.0
   system
   stable -> 7.4 (-> v7.4.0) (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:

   ```javascript
   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.

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

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

```bash
netstat -tpln
```

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](http://<Public IP address of the ECS instance>:3000)
```

Related topics

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

3.1 Build a WordPress blog platform

3.1.1 Deploy a WordPress site based on ECS and RDS

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 text file used to specify the resources that you want to create. This topic describes how to use a template in ROS to deploy a WordPress site based on Elastic Compute Service (ECS) and Relational Database Service (RDS).

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.

Procedure

1. Log on to the ROS console.

   **Note:**
   - The first time that you use the ROS service, you are prompted to activate this service.
   - ROS is a free service, so you can activate ROS free of charge.

2. In the left-side navigation pane, choose Key Help > ECS Instance Information, click the ECS Instance Type tab to find the target instance type in the Instance Type column, click the ECS Zone tab to find the target zone ID in the ZoneId column, and then click the ECS Image tab to find the target image ID in the Image List column.

3. In the left-side navigation pane, click Sample Template to display common templates that ROS provides.
4. Find the sample template `wordpress_instance`.

![Sample Template](image)

5. Click **Preview** 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. 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. In 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. In 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. Select the region where the ECS instance is located from the **Region** drop-down list, and click **Next**. In this example, **China (Beijing)** is specified.

8. Set stack parameters.

The following table lists the stack parameters.

<table>
<thead>
<tr>
<th>Parameter name</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>Parameter name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Creation timeout</td>
<td>Specifies a period. If ROS fails to create the specified resources within the period, the creation operation will time out. You can select or clear <strong>Roll back</strong>.</td>
</tr>
<tr>
<td></td>
<td>• If you select Roll back, 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 clear Roll back, ROS will not delete the created resources when any error such as creation timeout occurs during the creation process.</td>
</tr>
<tr>
<td>ECS Image Id</td>
<td>The ID of the image that ROS uses to create the ECS instance. For more information, see Step 2.</td>
</tr>
<tr>
<td>ECS Instance Type</td>
<td>The type of the ECS instance that you want to create. For more information, see Step 2.</td>
</tr>
<tr>
<td>ECS Instance Password and (Please Confirm) ECS Instance Password</td>
<td>Specify the password for logon to the ECS instance and confirm the password. The password must be 8 to 30 characters in length and must contain at least three of these character categories: letters, digits, and special characters. Special characters include parentheses (( )), grave accents (’), tildes (~), exclamation points (!), at signs (@), number signs (#), dollar signs ($), percent signs (%), carets (^), ampersands (&amp;), asterisks (*), hyphens (-), underscores (_), plus signs (+), equal signs (=), vertical bars (</td>
</tr>
<tr>
<td>The VPC Cidrblock</td>
<td>The private CIDR block of a Virtual Private Cloud (VPC). For more information, see #unique_34.</td>
</tr>
<tr>
<td>The VSwitch 2 Cidrblock</td>
<td>The CIDR block of a VSwitch. 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_34.</td>
</tr>
<tr>
<td>DB Instance Class</td>
<td>The type of the ApsaraDB for RDS instance.</td>
</tr>
<tr>
<td>DB Instance Storage</td>
<td>The storage capacity of the ApsaraDB for RDS instance.</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ECS Zone Id</td>
<td>The zone ID of the resource that you want to create. For more information, see Step 2.</td>
</tr>
<tr>
<td>Database Instance Engine Type</td>
<td>The engine of the database that you want to use.</td>
</tr>
<tr>
<td>Database Engine Version</td>
<td>The version of the database engine that you want to use.</td>
</tr>
<tr>
<td>DB Name</td>
<td>The name of the MySQL database.</td>
</tr>
<tr>
<td>DB Username</td>
<td>The username of the MySQL database.</td>
</tr>
<tr>
<td>DB Password</td>
<td>The password for accessing the MySQL database. The password must be 8 to 32 characters in length.</td>
</tr>
</tbody>
</table>

The following figure shows the configured parameters.

![Create Stack Figure]
9. Click Create.

10. In the left-side navigation pane, click Stack Management, select the specified region in the top navigation bar, and then find the created stack.

11. Click the stack name, and in the left-side navigation pane, click the following tabs to check the information about the stack:
   - **Overview**: displays basic information, startup parameters, status, output, and stack parameters.
   - **Resource**: displays all resources of the stack.
   - **Event**: records the operations that ROS performs when creating the resource stack. The causes of failed operations are also displayed in the list.
   - **Template**: displays the original template of the stack.

### 3.2 Build a Magento website on ECS

Magento is an open-source e-commerce platform written in PHP. Many customers use it to build their B2B or B2C e-commerce platforms. This tutorial explains how to build a Magento platform on a single ECS instance.

In this tutorial, we will install the following tools:

- MySQL version: 5.7
- PHP version: 7.0
- Magento version: 2.2

**Prerequisites**

*[Create an ECS instance]. Make sure the instance meets the following requirements:
Operating system: CentOS 7.2 64bit. Minimum specifications include 2 Core CPU, 4 GiB RAM, and a 40 GiB Ultra Cloud Disk as the system disk. VPC-connected. If you do not have
a VPC network, one will be created when you create an ECS instance. A public IP address is assigned to the instance.

Inbound Internet traffic to the TCP Port 80 of the ECS instance is allowed. For more information, see create an ECS instance and add a security group rule.

<table>
<thead>
<tr>
<th>Service</th>
<th>Rule Direction</th>
<th>Authorization Policy</th>
<th>Protocol Type</th>
<th>Port Range</th>
<th>Authorization Type</th>
<th>Authorization Object</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Inbound</td>
<td>Allow</td>
<td>User-defined TCP</td>
<td>80/80</td>
<td>Address Field Access</td>
<td>0.0.0.0/0</td>
<td>1</td>
</tr>
<tr>
<td>MySQL</td>
<td>Inbound</td>
<td>Allow</td>
<td>User-defined TCP</td>
<td>3306/3306</td>
<td>Address Field Access</td>
<td>0.0.0.0/0</td>
<td>1</td>
</tr>
</tbody>
</table>

**Procedure**

To build a Magento website using ECS, follow these steps:

**Step 1: Install LAMP on ECS.**

**Step 2: Configure the database.**

**Step 3: Install and configure Composer.**

**Step 4: Install and configure Magento.**

**Step 5: Test the installation.**

**Step 1: Install LAMP (Linux, Apache, MySQL, and PHP) on ECS**

This section describes how to manually install the LAMP platform. You can also start the ECS instance directly from the cloud market by purchasing LAMP images so that you can quickly build a website.

1. Connect to the ECS instance and install Apache and MySQL.

   ```bash
   # yum -y update
   # yum -y install httpd
   # rpm -Uvh http://dev.mysql.com/get/mysql57-community-release-el7-8.noarch.rpm
   # yum -y install mysql-community-server
   ``

2. Start Apache and MySQL service and enable them at startup.

   ```bash
   # systemctl start httpd
   # systemctl enable httpd
   # systemctl start mysqld
   ```
# systemctl enable mysqld

3. Configure the Apache configuration file: /etc/httpd/conf/httpd.conf.

   a. Run `vim /etc/httpd/conf/httpd.conf`.
   b. Press the i key.
   c. Add the `LoadModule rewrite_module modules/mod_rewrite.so` line below Include `conf.modules.d/*.conf`, and replace `AllowOverride None` with `AllowOverride all` in the following section.

   ```
   Options Indexes FollowSymLinks
   #
   # AllowOverride controls what directives may be placed in .htaccess files.
   # It can be "All", "None", or any combination of the keywords:
   # Options FileInfo AuthConfig Limit
   #
   AllowOverride None
   ```
   d. Press the Esc key and type `:wq` to save and exit the file.

4. Obtain the temporary password of the root account at the installation of MySQL by running the following.

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

5. Finish the MySQL security configuration, including:

   - Resetting the root account password
   - Disabling remote root logon
   - Removing anonymous users
   - Removing test database and test database access

   For more information, see the official documentation.

   ```
   # mysql_secure_installation
   Securing the MySQL server deployment.
   Enter password for user root: # Enter your temporary root password that is recorded 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 strong password. The password can be [8, 30] characters in length. It must contain uppercase letters, lowercase letters, and numbers. The following special characters are allowed: ()~! @#$%^&*-+=|{}[]():;'<>,.? /
   Re-enter new password: # Repeat the new password to confirm it
   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
   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 \text{y}|Y for Yes, any other key for No): \text{Y}
Success.
Normally, root should only be allowed to connect from 'localhost'.
This ensures that someone cannot guess at the root password from the network.
Disallow root login remotely? (Press \text{y}|Y for Yes, any other key for No): \text{Y}
Success.
By default, MySQL comes with a database named 'test' that anyone can access.
This is also intended only for testing, and should be removed before moving into a production environment.
Remove test database and access to it? (Press \text{y}|Y for Yes, any other key for No): \text{Y}
- Dropping test database...
Success.
- Removing privileges on test database...
Success.
Reloading the privilege tables will ensure that all changes made so far will take effect immediately.
Reload privilege tables now? (Press \text{y}|Y for Yes, any other key for No): \text{Y}
Success.
All done!

6. Install PHP 7.

\begin{verbatim}
# yum install -y http://dl.iuscommunity.org/pub/ius/stable/CentOS/7/x86_64/ius-
release-1.0-14.ius.centos7.noarch.rpm
# yum -y update
# yum -y install php70u php70u-pdo php70u-mysqld php70u-opcache php70u-xm
php70u-gd php70u-mcrypt php70u-devel php70u-intl php70u-mbstring php70u-bcmath php70u-json php70u-ic
\end{verbatim}

7. Validate PHP installation.

\begin{verbatim}
# php -v
PHP 7.0.13 (cli) (built: Nov 10 2016 08:44:18) ( NTS )
Copyright (c) 1997-2016 The PHP Group
Zend Engine v3.0.0, Copyright (c) 1998-2016 Zend Technologies
with Zend OPcache v7.0.13, Copyright (c) 1999-2016, by Zend Technologies
\end{verbatim}

8. Edit the /etc/php.ini file to set your time zone:

\begin{itemize}
\item[a.] Run \text{vim} /etc/php.ini.
\item[b.] Press the \text{i} key.
\item[c.] Find the line starting with \textbf{date.timezone} which is commented out by default, and add the correct time zone. If your site is in China, add \texttt{date.timezone = Asia/Shanghai}.
\end{itemize}

9. Restart httpd by running the following.

\begin{verbatim}
systemctl start httpd
\end{verbatim}

\textbf{Step 2: Configure the database}

Follow these steps to configure a database:
1. Create a database and a user. Run the following commands, including those typed in the mysql> prompt.

```
# mysql -u root -p
Enter password:
mysql> CREATE DATABASE magento;
Query OK, 1 row affected (0.00 sec)
mysql> GRANT ALL ON magento. * TO YourUser@localhost IDENTIFIED BY 'YourPass';
Query OK, 0 rows affected, 1 warning (0.00 sec)
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

2. Run exit to exit MySQL.

3. Test the new user.

```
# mysql -u YourUser -p
mysql> show databases;
+--------------------+
| Database |
+--------------------+
| information_schema |
| magento |
+--------------------+
2 rows in set (0.00 sec)
mysql> exit
```

**Step 3: Install and configure Composer**

1. Install Composer.

```
# curl -sS https://getcomposer.org/installer | php
All settings correct for using Composer
Downloading 1.2.4...
Composer successfully installed to: /root/composer.phar
Use it: php composer.phar
```

2. Configure Composer.

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

3. Test Composer.

```
# composer -v
Composer version 1.2.4 2016-12-06 22:00:51
```

**Step 4: Install and configure Magento**

1. Download Magento from github using the following commands through git clone.

```
# yum -y install git
# cd /var/www/html/
```
2. Switch the version of Magento to the stable production version.

   # cd magento2 && git checkout tags/2.1.0 -b 2.1.0
   Switched to a new branch '2.1.0'

3. Move the installation files to the Apache root directory. If you skip this step, you will only be able to access your Magento service at http://your-server-ip/magento2.

   # shopt -s dotglob nullglob && mv /var/www/html/magento2/* /var/www/html/ && cd ..

4. Set Magento file permissions.

   # 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 composer install to install Magento.

6. Use your browser to access your server at http://public IP address of your ECS instance.

   You will see a welcome screen like this one.
7. Click **Agree and Setup Magento** and fill in the database information, web configuration, and accounts as follows. When you get a page like this, the installation is successful.

![Success](image)

**Magento Admin Info:**
- Username: [Redacted]
- Email: [Redacted]
- Password: [Redacted]
- Your Store Address: [Redacted]
- Magento Admin Address: [Redacted]

Be sure to bookmark your unique URL and record it offline.

**Database Info:**
- Encryption Key: [Redacted]
- Database Name: [Redacted]

**Step 5: Configure the cron job**

1. Run `crontab -u apache -e`.
2. Add the following in the `/etc/crontab` file.

```bash
*/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
```

For more information, see the [official documentation](https://magento.com/docs).

**What to do next**

Visit http://public IP address of your ECS instance to see the default home page.

Visit http://public IP address of your ECS instance/admin, and use the user name and password you set during the installation to log on to the Dashboard.
For more information about Magento configuration, see the official documentation.

3.3 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

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

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_37.

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_38.
- **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.

![Enter Secure Shell Password]

3. 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
```

4. Install NGINX.

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

5. Enable NGINX to run at startup.

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

6. Start NGINX and check the NGINX service status.

```bash
[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!]

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
d) Use npm to install Ghost.

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

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

```
[root@localhost ghost]# npm start
```

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 = {
      // ### 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.
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_set_header Host $host;
        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 $http_x_forwarded_proto;
    }
}
```

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.

3.4 Build a Drupal website

This topic describes how to use Drupal to deploy an e-commerce website on an ECS instance that runs CentOS 7.

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 a free and 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 that are familiar with Alibaba Cloud ECS instances and Linux, but new to website construction on ECS instances.

Project configuration

The following software versions are used in this procedure. The operations may vary depending on the versions of your software.
Operating system: CentOS 7.2
Apache: Apache 2.4.25
MySQL: MySQL 5.7.17
PHP: 7.1.1
Drupal: 8.1.1

Procedure
To build a Drupal website on an ECS instance, perform the following steps:

1. Step 1: Activate an ECS instance
2. Step 2: Deploy the web environment
3. Step 3: Install Drupal

Step 1: Activate an ECS instance
Activate an ECS instance to build a small-sized website for personal use. Later, you can upgrade the instance or optimize the architecture based on your needs.

Step 2: Deploy the web environment
You can deploy the web environment on the ECS instance in any of the following ways:

- Image deployment
- Deployment by using an installation package
- Manual deployment: Build the environment by using the source code or Yellowdog Update, Modified (YUM).

For new users, we recommend that you use an image to deploy the web environment. This is an easy way to set up a web environment. If you have some basic knowledge of Linux operations and maintenance, you can use an installation package, the source code, or the YUM utility to customize the web environment. This topic describes how to build a Drupal website by using an 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 **LAMP** in the search bar and select the image that matches your operating system. Select a LAMP image that is suitable for CentOS 7.2.

   You can also go to Alibaba Cloud Marketplace to search for and purchase the images that you want to use.

7. Click **Apply**.

8. On the **Custom Launch** page, scroll down to the **Image** section. The custom image you purchased is automatically selected. Complete other settings and activate the ECS instance as instructed. For more information, see #unique_4.

**Step 3: Install Drupal**

To install Drupal, perform the following steps:
1. Download the Drupal installation package:
   
   ```bash
   ```

2. Decompress the package to your website root directory:
   
   ```bash
   unzip drupal-8.1.1.zip
   mv drupal-8.1.1/* /var/www/html/
   ```

3. Specify the owner and group of the sites directory:
   
   ```bash
   chown -R apache:apache /var/www/html/sites
   ```

4. Restart the Apache service:
   
   ```bash
   # /etc/init.d/httpd restart
   ```

5. In the address bar of your browser, enter <Public IP address of an ECS instance>/index.php to go to the Drupal installation page. Select the required language from the Choose Language drop-down list, and click **Save and continue**.

   ![Drupal installation page]

6. Select Standard, and click **Save and continue**.

7. Enter database information, and click **Save and continue**.

   **Note:**
   After you log on to the MySQL database, you can run the following commands to set the database information:

   - DBNAME: database name
• UAERNAME: username
• IP: localhost or 127.0.0.1 for a local host
• YOURPASSWORD: database password

```sql
mysql> CREATE DATABASE DBNAME;
mysql> CREATE USER UAERNAME;
mysql> GRANT ALL PRIVILEGES ON *. * TO 'UAERNAME'@'IP' IDENTIFIED BY 'YOURPASSWORD' WITH GRANT OPTION;
mysql> FLUSH PRIVILEGES;
```

8. After the installation is complete, go to the website settings page, enter site information, and then click **Save and continue**.

What's next

After the installation, you can customize your website pages.
4 Build an application

4.1 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 allows enterprises to develop intelligent portals. Microsoft SharePoint can be seamlessly integrated with knowledge bases and individual users and teams can easily connect to the environment. Microsoft SharePoint empowers your business by means of efficient information processing. Microsoft SharePoint provides an enterprise-wide service solution. Based on the feature of integrating enterprise applications, you can flexibly choose deployment options and management tools to integrate information from various systems into this solution.

The procedure described in this topic is applicable to users that 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 use the following configurations:

- CPU: 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
4. Step 4: Configure SharePoint 2016

Step 1: Add the AD, DHCP, DNS, and IIS services

To add the Active Directory (AD), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and Internet Information Services (IIS) services, follow these steps:

1. Purchase an ECS instance. For more information, see #unique_4.
2. Disable Internet Explorer Enhanced Security Configuration.
3. Add roles and features of DNS, DHCP, IIS, and .NET Framework 3.5.

   a) Click **Add roles and features**.

   ![Add roles and features](image1.png)

   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.png)

   c) Add the IIS service. Select **Web Server IIS**, and click **Next**.
d) In the **Features** section, select **.NET Framework 3.5 Features**.

e) Click **Next** until the end of installation.
4. Configure the AD service. Click **Add a new forest**, and enter a domain name in the **Root domain name** field to create a domain environment.

5. Set the password, and click **Next** until the end of the configuration.
6. Click **Complete DHCP configuration** to set the DHCP feature.

   a) Check the DHCP configuration description, and click **Next**.
   
   b) Keep the default configuration, and click **Commit** to complete the installation.

---

**Step 2: Install SQL Server 2014**

To install the SQL Server 2014 database, follow these steps:
1. Install SQL Server 2014 SP1, go to the SQL Server Installation Center window, and click the first installation option.

2. Enter the product key, and click **Next**.

3. Accept the license terms, and click **Next**.

4. Complete the installation check, and click **Next**.
5. Keep the default option, and click **Next**.

![SQL Server 2014 Setup](image)

6. Click **Select All** to select all features, and click **Next**.

![Feature Selection](image)
7. Configure the SQL Server instance: Click **Default instance** to use the default instance ID.
8. Specify the account names and passwords for **SQL Server Database Engine** and **SQL Server Analysis Services**.
9. Click **Add Current User** to add the current user, and click **Next**.

10. Click **Add Current User** to add the current user again, and click **Next**.
11. Click **Next** until the end of the installation.

**Step 3: Install SharePoint 2016**

To install SharePoint 2016, follow these steps:

1. Install the SharePoint 2016 prerequisite installer: Open the image folder, and double-click the executable file of the prerequisite installer.

2. In the installation wizard, click **Next**.

3. Accept the license terms, and install necessary components.

4. Open the Setup.exe file, enter the product key in the dialog box that appears, accept the license terms, and then click **Continue**.

5. Specify the installation directory, or keep the default setting as shown in this example, and then click **Install Now**.

6. At the end of the installation, select **Run the SharePoint Products Configuration Wizard now** and close the wizard.

**Step 4: Configure SharePoint 2016**

To configure SharePoint 2016, follow these steps:

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 as the database server.

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.

4.2 Install SharePoint 2016

This topic describes how to install SharePoint 2016.

**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**

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.

**4.3 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, 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.
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:

   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:

     docker tag registry.cn-hangzhou.aliyuncs.com/lxepoo/apache-php5:latest aliweb:v1

   • Check existing images:

     docker images

   • Delete an image:

     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 `e1xxxxxxxxxe`. Then, run the `docker run` command to enter the container.

     docker run -ti e1xxxxxxxxxe /bin/bash

   • Exit the container. Run the `exit` command to exit the container.
• You can combine the run command with the \texttt{-d} parameter to run the container in the background. The \texttt{--name} parameter specifies apache as the container name.

\begin{verbatim}
docker run -d --name apache e1xxxxxxxxxe
\end{verbatim}

• Enter the container that runs in the background:

\begin{verbatim}
docker exec -it apache /bin/bash
\end{verbatim}

• Create an image from the container. Description of the parameters in the command:

\begin{verbatim}
docker commit <container ID or container name> [<repository name> [: <tag>]].
\end{verbatim}

\begin{verbatim}
docker commit containerID/containerName repository:tag
\end{verbatim}

• 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.

\begin{verbatim}
# docker commit 4c8066cd8c01 apachephp:v1
\end{verbatim}

• Run the container and map port 8080 of the host to the container:

\begin{verbatim}
# docker run -d -p 8080:80 apachephp:v1
\end{verbatim}

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.

\begin{figure}
\centering
\includegraphics[width=\textwidth]{phpinfo.png}
\caption{PHP Version 5.6.28}
\end{figure}

\begin{figure}
\centering
\includegraphics[width=\textwidth]{system.png}
\caption{System Build Date}
\end{figure}

**Create an image**

To create an image, perform the following steps:

1. Prepare the following content in a Dockerfile:

\begin{verbatim}
# vim Dockerfile
\end{verbatim}
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         #Push an image to the remote image repository. Default value
: Docker Hub.

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.

4.4 Deploy databases based on ECS

4.4.1 Manually deploy a MySQL database on a Linux ECS instance

MySQL is a relational database management system. It provides tools to build web
applications, such as applications based on the LAMP (Linux, Apache, MySQL, PHP) or
LNMP (Linux, NGINX, MySQL, PHP) stack. This topic describes how to install, configure, and
remotely access a MySQL database on a Linux 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.

You have added inbound rules to the security group associated with the ECS instance. Port 3306 is open for inbound traffic. For more information, see #unique_16.

**Context**

This topic is based on the following software versions. The operations may vary depending on the versions of your software.

- Operating system: public image for CentOS 7.2 64-bit
- MySQL: 5.7.26

This topic is based on an ECS instance with the following configuration. The operations may vary depending on the configuration of your ECS instance.

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

The basic procedure for deploying a MySQL database on a Linux ECS instance is as follows:

- **Step 1: Prepare the environment**
- **Step 2: Install MySQL**
- **Step 3: Configure MySQL**
- **Step 4: Remotely access the MySQL database**

**Step 1: Prepare the environment**

Connect to your ECS instance. For more information, see #unique_46 or #unique_30.

**Step 2: Install MySQL**

Perform the following operations to install MySQL:
1. Run the following command to update the YUM repository:

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

2. Run the following command to install MySQL:

   ```bash
   yum -y install mysql-community-server
   ```

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

   ```bash
   mysql -V
   ```

   MySQL is installed if the following result is returned:

   ```
   mysql  Ver 14.14 Distrib 5.7.26, for Linux (x86_64) using EditLine wrapper
   ```

**Step 3: Configure MySQL**

Perform the following operations to configure MySQL:

1. Run the following command to start MySQL:

   ```bash
   systemctl start mysqld
   ```

2. Run the following command to configure MySQL to run upon system startup:

   ```bash
   systemctl enable mysqld
   ```

3. Run the following command to view the `/var/log/mysqld.log` file and record the temporary password of the root user:

   ```bash
   # grep 'temporary password' /var/log/mysqld.log
   2019-04-28T06:50:56.674085Z 1 [Note] A temporary password is generated for root@localhost: 3w)WqGlM7-o,
   ```

   **Note:**
   You need the temporary password when you reset the password for the root user.

4. Run the following command to configure the security settings of MySQL:

   ```bash
   mysql_secure_installation
   ```

   The security settings of MySQL involve the following operations:

   a) Reset the password for the root user.

   Enter password for user root: #Enter the temporary password for the root user that you previously obtained.
   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 #Specify whether to change the password of the root user. Press the Y key.
New password: #Enter a new password that must be 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: #Re-enter the new password for confirmation.
Estimated strength of the password: 100
Do you wish to continue with the provided password?( Press y|Y for Yes, any other key for No) : Y

b) Enter Y to disable the anonymous user account.

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 #Specify whether to delete anonymous users. Press the Y key.
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 #Specify whether to disable remote logon as a root user. Press the Y key.
Success.

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

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : Y #Specify whether to delete the test database and permissions to access this database. Press the Y key.
- 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 #Specify whether to reload privilege tables. Press the Y key.
Success.
All done!

For more information about security settings of MySQL, see MySQL documentation.

Step 4: Remotely access the MySQL database

You can use a database client or Data Management (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 access to MySQL.
   a) Run the following command and enter the password for the root user to log on to MySQL:
   ```
   mysql -uroot -p
   ```
   b) Run the following commands in the sequence to create an account for remote logon to MySQL. In this example, the account is dms and the password is 123456.
   ```
   mysql> grant all on *.* to 'dms'@'%' IDENTIFIED BY '123456'; #Replace dms with root to enable remote logon with the root account.
   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 need to replace the 123456 password with a password that meets the complexity requirements. It must be 8 to 30 characters in length. The password 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, select User-created Databases (ECS, Internet).

4. Click **Add Database**.

5. Configure the database that you have created. For more information, see Configure user-created databases.

6. Click **Log On**.
   After logging on, you can use the menu bar of DMS to create objects such as databases, tables, and functions. For more information, see Manage user-created databases hosted on ECS.

### 4.4.2 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**

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.
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_49.

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**.

   ![MySQL Installer]

   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 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

- You must have registered an Alibaba Cloud account. If not, create a new Alibaba Cloud account first.
- 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
2. Step 2: Configure the primary node of PostgreSQL
3. Step 3: Configure the secondary node of PostgreSQL
4. Step 4: Test the primary/secondary architecture of PostgreSQL

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.

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.
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  
      ```
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:

```bash
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:

   ```bash
   ps aux |grep sender
   ```

   The following response indicates that the sender process is available:

   ```bash
   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:

   ```bash
   ps aux |grep receiver
   ```

   The following response indicates that the receiver process is available:

   ```bash
   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:

   ```sql
   replication=# select * from pg_stat_replication;
   ```

   The following response indicates that the status of the secondary node is available:

   ```sql
   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 15:38:06.18898408 | 1836 | streaming | 0/F01C0C8 | 0/F01C0C8 | 0/F01C0C8 | 0 | async
   ```
4.6 Deploy and use SVN

4.6.1 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 access to SVN by using svnserv
- Deploy access to 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.

4.6.2 Deploy access to SVN by using svnserv

This topic describes how to deploy access to Apache Subversion (SVN) by using svnserv.

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

In this topic, the following software versions are used to manually deploy SVN. The versions may be different in your actual running environment.

- Operating system: public image 64-bit CentOS 7.2
- Subversion: version 1.7.14
- Apache HTTP Server: version 2.4.6

Procedure

To deploy access to SVN by using svnserv, follow these steps:

1. **Step 1: Install SVN**
2. **Step 2: Configure SVN**
3. **Step 3: Configure the security group rules**
4. **Step 4: Use a Windows client to test the SVN service**

**Step 1: Install SVN**

You can install SVN in any of the following ways:

- Use an SVN image from Alibaba Cloud Marketplace
  1. Click here to purchase an SVN image in Alibaba Cloud Marketplace.
  2. Click Choose Your Plan.
  3. Enter the account and password to log on to the ECS console.
  4. In the Image section, the Selected Image field shows the specified SVN image.
     - Continue with other settings and activate the ECS instance. For more information, see #unique_4.
• Install SVN manually

1. Connect to a Linux instance by using a password.
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: Configure SVN

To configure SVN, follow these steps:

1. Run the following command to create a root directory for an SVN repository.
   
   `mkdir /var/svn`

2. Run the following commands in sequence to create an SVN repository.
   
   ```
   # cd /var/svn
   # svnadmin create /var/svn/svnrepos
   ```

3. Run the following commands in sequence to check files in the SVN repository.
   
   ```
   # cd svnrepos
   ```
The SVN directories are described as follows:

<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 to the `[users]` field, and add the username and password.

   **Note:**
   You can add the username and password in the following format: `username = password`. For example, `suzhan (username) = redhat (password)`, as shown in the following figure. There must be a space on both ends of the equal sign (`=`).

   e) Press the `Esc` key to exit the edit mode, and type `:wq` to save and close the file.
5. Set the read and write permissions for the username.
   a) Run the `vi authz` command to open the permission control file.
   b) Press the i key to enter the edit mode.
   c) Move the pointer to the end of the file, and add the following code. In the code, 
suzhan specifies the username, r specifies the read permission, and w specifies the 
write permission.

```
[/]
suzhan=rw
```

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

6. Modify the configurations of the SVN service.
   a) Run the command `vi svnserve.conf` to open the configuration file of the SVN service.
   b) Press the i key to enter the edit mode.
   c) Move the pointer to the following lines, and delete the number sign (#) and space at 
the beginning of each line:

```
anon-access = read #Assigns read permissions to anonymous users. You can also 
specify anon-access = none to disable access by anonymous users. If you set anon-
access to none, the revision history of the SVN service shows dates.
auth-access = write #Authorizes the write permission.
password-db = passwd #Specifies the password database file.
authz-db = authz #Specifies the file that stores the authorization rules for path-
based access control.
realm = /var/svn/svnrepos #Specifies the authorization realm of the repository.
```

**Note:**

issue: 20200416
Each line cannot start with a space and there must be a space on both ends of the equal sign (=).

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

7. Run the following command to start the SVN repository.

```
svnserve -d -r /var/svn/
```

8. Run the command `ps -ef |grep svn` to check whether the SVN service has been started.

The following response indicates that the SVN service has been started.

```
[...]
```

**Note:**
Run the command `killall svnservice` to stop the SVN service.

**Step 3: Configure the security group rules**

The SVN server listens on TCP Port 3690 by default. You must log on to the ECS console to add TCP Port 3690 to the security group. For more information, see #unique_16.
Step 4: Use a Windows client to test the SVN service

To test the SVN service by using a Windows client, follow these steps:

1. Download and install a TortoiseSVN client on your local computer.
2. Right-click the local project folder. In this example, the project folder is C:\KDR.
3. On the menu that appears, select SVN Checkout.
4. Apply the following settings, and click OK.
   - Set the URL of repository field in this 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](image)

Note:
During the logon for the first time, you must provide the username and password that you have configured in the passwd file.

4.6.3 Deploy access to SVN over HTTP

This topic describes how to deploy access to Apache Subversion (SVN) over HTTP.

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

In this topic, the following software versions are used to manually deploy SVN. The versions may be different in your actual running environment.

- Operating system: public image 64-bit CentOS 7.2
- Subversion: version 1.7.14
- Apache HTTP Server: version 2.4.6

Procedure

To deploy access to SVN over HTTP, follow these steps:

1. Install SVN
2. Install Apache
3. Install mod_dav_svn
4. Configure SVN
5. Configure Apache
6. Configure the security group rules
7. Use a browser to test access to SVN

Step 1: Install SVN

To install SVN, follow these steps:

1. Connect to a Linux instance by using a password.
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: Install Apache

To install Apache, follow these steps:
1. Run the following command to install the Hypertext Transfer Protocol daemon (HTTPd).

```bash
yum install httpd
```

2. Run the following command to check the HTTPd version.

```bash
httpd -version
```

**Step 3: Install mod_dav_svn**

Run the following command to install mod_dav_svn.

```bash
yum install mod_dav_svn
```

**Step 4: Configure SVN**

To configure SVN, follow these steps:

1. Run the following command to create a root directory for an SVN repository.

```bash
mkdir /var/svn
```

2. Run the following command to create an SVN repository.

```bash
svnadmin create /var/svn/svnrepo
```

3. Run the following command to specify apache as the user group of the SVN repository.

```bash
chown -R apache:apache /var/svn/svnrepo
```

4. Run the following command to create a configuration file named passwd.

```bash
touch /var/svn/passwd
```

5. Run the following command to create the admin user and set the password. In this example, set the password to admin123.

```bash
htpasswd /var/svn/passwd admin
```

6. Run the following command to create an access permission file.

```bash
cp /var/svn/svnrepo/conf/authz /var/svn/authz
```

**Step 5: Configure Apache**

To configure Apache, follow these steps:

1. Run the command `vim /etc/httpd/conf.d/subversion.conf` to open the HTTPd configuration file.

2. Press the `i` key to enter the edit mode.
3. Enter the following configuration information:

```xml
<Location /svn>
  DAV svn
  SVNParentPath /var/svn
  AuthType Basic
  AuthName "Authorization SVN"
  AuthzSVNAccessFile /var/svn/authz
  AuthUserFile /var/svn/passwd
  Require valid-user
</Location>
```

4. Press the Esc key, and type :wq to save and close the file.

5. Run the following command to start the Apache HTTP Server.

```bash
systemctl start httpd.service
```

**Step 6: Configure the security group rules**

The SVN server listens on TCP Port 3690 by default. You must log on to the ECS console to add TCP Port 3690 to the security group. For more information, see #unique_16.

**Step 7: Use a browser to test access to SVN**

To test access to SVN in a browser, follow these steps:

1. Open your browser.
2. In the address bar, enter the URL `http://<Public IP address of the ECS instance>/svn/<SVN repository name>`, and press the Enter key. In this example, the SVN repository name is `svnrepo`.
3. Enter your username and password that you have configured in the passwd file. In this example, the username is `admin` and the password is `admin123`.

The following response indicates that you have accessed the SVN repository that you have created.

```
svnrepo - Revision 0: /
```
4.6.4 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 access to SVN by using svnservice and Deploy access to 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.

4.7 Build an FTP site on an ECS instance

4.7.1 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

- You must have registered an Alibaba Cloud account. If not, create a new Alibaba Cloud account first.
- 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 1: install vsftpd

1. Connect to the target Linux instance.
   For more information, see #unique_59/unique_59_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.

   ![Installation success](image)

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.

   ![Listening port](image)
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.

   ![Configuration File](image)

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.

   \texttt{useradd ftptest}

2. Run the following command to modify the password of the \texttt{ftptest} user:

   \texttt{passwd ftptest}

3. Run the following command to create a file directory for the FTP service:

   \texttt{mkdir /var/ftp/test}

4. Run the following command to change the owner of the /var/ftp/test directory to ftptest:

   \texttt{chown -R ftptest:ftptest /var/ftp/test}

5. Modify the vsftpd.conf configuration file.
   a) Run the \texttt{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:

      \begin{verbatim}
      #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.
      \end{verbatim}

   • To enable the passive mode for the FTP server, you need to set the following parameters:

      \begin{verbatim}
      #Use the default values for all parameters except for the following parameters:
      \end{verbatim}
#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>
</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. |
• When the FTP server is in the passive mode: allow port 21 and all the ports between the `pasv_min_port` and the `pasv_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>
<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>
<tr>
<td>Inbound</td>
<td>Allow</td>
<td>Custom TCP</td>
<td><code>pasv_min_port</code>/<code>pasv_max_port</code></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>

**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=lightwriter</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.
4.7.2 Build an FTP site on a Windows ECS instance

This topic describes how to build an FTP site on a Windows ECS instance. This method is applicable to Windows Server 2008 and later versions. In this topic, Windows Server 2008 R2 is used.

The procedure for building an FTP site on a Windows ECS instance is as follows:

- Step 1. Add IIS and FTP service roles
- Step 2. Create FTP user name and password
- Step 3. Set permissions for shared files
- Step 4. Add and configure an FTP site
- Step 5. Configure a security group and firewall
- Step 6. Test

Step 1. Add IIS and FTP service roles

You must install IIS and FTP services before building an FTP site.

1. #unique_61.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Server Manager**.
3. In the left-side navigation pane, click **Roles**, and then click **Add Roles**.
4. In the dialog box, click **Next**.
5. Select **Web Server (IIS)**, and then click **Next**.
6. Select **IIS Management Console** and **FTP Server**, click **Next**, and then click **Install**.

Step 2. Create FTP user name and password

If you want to allow anonymous users to access the FTP, skip this step.

1. Click **Start** > **Administrative Tools** > **Server Manager**.
2. Click **Configuration** > **Local Users and Groups** > **Users**, right click the blank space, and select **New User**. In the **New User** dialog box, type the new user information. For example, ftptest is used in this topic.

   **Note:**
   The password must contain a mixture of upper-case letters, lower-case letters, and numbers. Otherwise, the password is invalid.
Step 3. Set permissions for shared files

You must set permissions to read, write, or execute for folders shared to users on the FTP site.

1. Create a folder for the FTP site, right click the folder, and then select **Properties**.
2. Click **Security**, select **Users**, and then click **Edit**.
3. Edit **Permissions for Users**. In this example, we grant **all permissions**.

Step 4. Add and configure an FTP site

Follow these steps to install an FTP site:

1. Click **Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the left-side navigation pane, click the instance ID, right click **Sites**, and then click **Add FTP Site**.
3. In the dialog box, specify the FTP site name and the physical path of the shared folder, and then click **Next**.
4. Use the **default value** for the IP address, and then type the port number of this instance. The default FTP port number is 21.
5. Select SSL settings.
   - **Allow SSL**: Allows the FTP site to support both non-SSL and SSL connections with the client.
   - **Require SSL**: Requires SSL encryption for communication between the FTP server and the client.
   - **No SSL**: If No SSL encryption is required, select **No SSL**.
6. Select one or more authentication methods.
   - **Anonymous**: Allows any user to access the shared content, by entering the user name **anonymous** or **ftp**.
   - **Basic**: Requires users to enter the valid user name and password before they can access the shared content. The basic authentication method transmits the unencrypted password through the network. Therefore, use this authentication method only when you are sure that the connection between the client and the FTP server is secure, for example, when SSL is used.
7. Select one of the following options from the **Authorization** list, and set permissions:

- **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 members of the specific role group or user group can access the relevant content. Enter the role group or user group in the corresponding field.
- **Specified users**: Only the specified users can access the relevant content. Enter the user name in the corresponding field.

8. Select **read** and **write** permissions for the authorized users, and then click **Finish**.

**Step 5. Configure a security group and firewall**

After building the FTP site, you must add a rule in the security group to allow inbound traffic on the FTP port. For more information, see [add a security group rule](#).

By default, TCP port 21 is open on the server firewall by default for the FTP service. If you have entered another port number, you must add an inbound rule to open this port on the firewall.

**Step 6. Test**

On your **local computer**, access the FTP site by using `ftp://IP address:FTP port` (the default port 21 is used if you do not enter the port). For example, you can enter `ftp://0.0.0.0:20`. You are prompted for your user name and password if the configuration was successful. After entering the user name and password correctly, you can perform the relevant FTP file operations according to your permissions.

**Note:**

If you use this method to access the FTP site from the client, you must adjust the Internet Explorer settings to open FTP folders. Open Internet Explorer, and then select **Tools > Internet Options > Advanced**. Select **Enable folder view for FTP sites**, and then clear **Use Passive FTP**.

**What to do next**

You can take actions to **improve your FTP service security**.

For more information, see [FTP anonymous logon and weak password vulnerabilities](#).
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>
</table>
| Normal mode        | In this mode, you can copy, paste, and delete characters or lines.       | • The tool enters normal mode when you run the `vim <file name>` command to open a file.  
<p>| [DO NOT TRANSLATE] |                                                                          | • To switch from other modes to this mode, press the Esc key.                |
| Insert mode        | In this mode, you can insert characters.                                 | To switch from the normal mode to this mode, enter any of the following characters: <code>i</code>, <code>I</code>, <code>a</code>, <code>A</code>, <code>o</code>, <code>O</code>. |
| [DO NOT TRANSLATE] |                                                                          | <strong>Note:</strong> You will see -- INSERT -- in the lower-left corner of the editor after you switch to this mode. |
| Replace mode       | In this mode, you can replace characters.                                | To switch from the normal mode to this mode, enter <code>R</code>.                     |
| [DO NOT TRANSLATE] |                                                                          | <strong>Note:</strong> You will see -- REPLACE -- in the lower-left corner of the editor after you switch to this mode. |
| Visual mode        | In this mode, you can select a range of text. You must select a range of text before running commands such as copy, replace, and delete on the specified text. | To switch from the normal mode to this mode, enter <code>v</code>.                     |
| [DO NOT TRANSLATE] |                                                                          | <strong>Note:</strong> You will see -- VISUAL -- in lower-left corner of the editor after you switch to this mode. |</p>
<table>
<thead>
<tr>
<th>Mode</th>
<th>Function</th>
<th>Mode switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command mode [DO NOT TRANSLATE]</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:

```
# 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:

```bash
# 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:

```bash
# 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.
```

## Elastic Compute Service

### Tutorials / 5 Use the Vim editor

# 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.

```