Alibaba Cloud
Elastic Compute Service

Tutorials

Issue: 20190904

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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

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

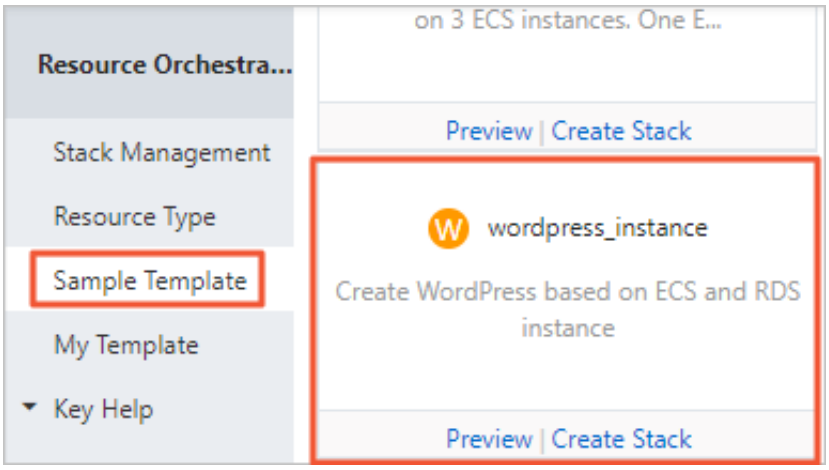
You must have an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

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.



5. Click Preview to check the template in JSON format.

   The following table lists the top-level fields in the JSON file.

Top-level field	Description
`" ROSTemplat eFormatVer sion " : " 2015 - 09 - 01 "`	Specifies the version of the template.
`" Parameters " : { }`	Specifies some parameters. In this example, this field specifies the default image ID and instance type.
`" Resources " : { }`	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.
`" Outputs ": { }`	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.

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.

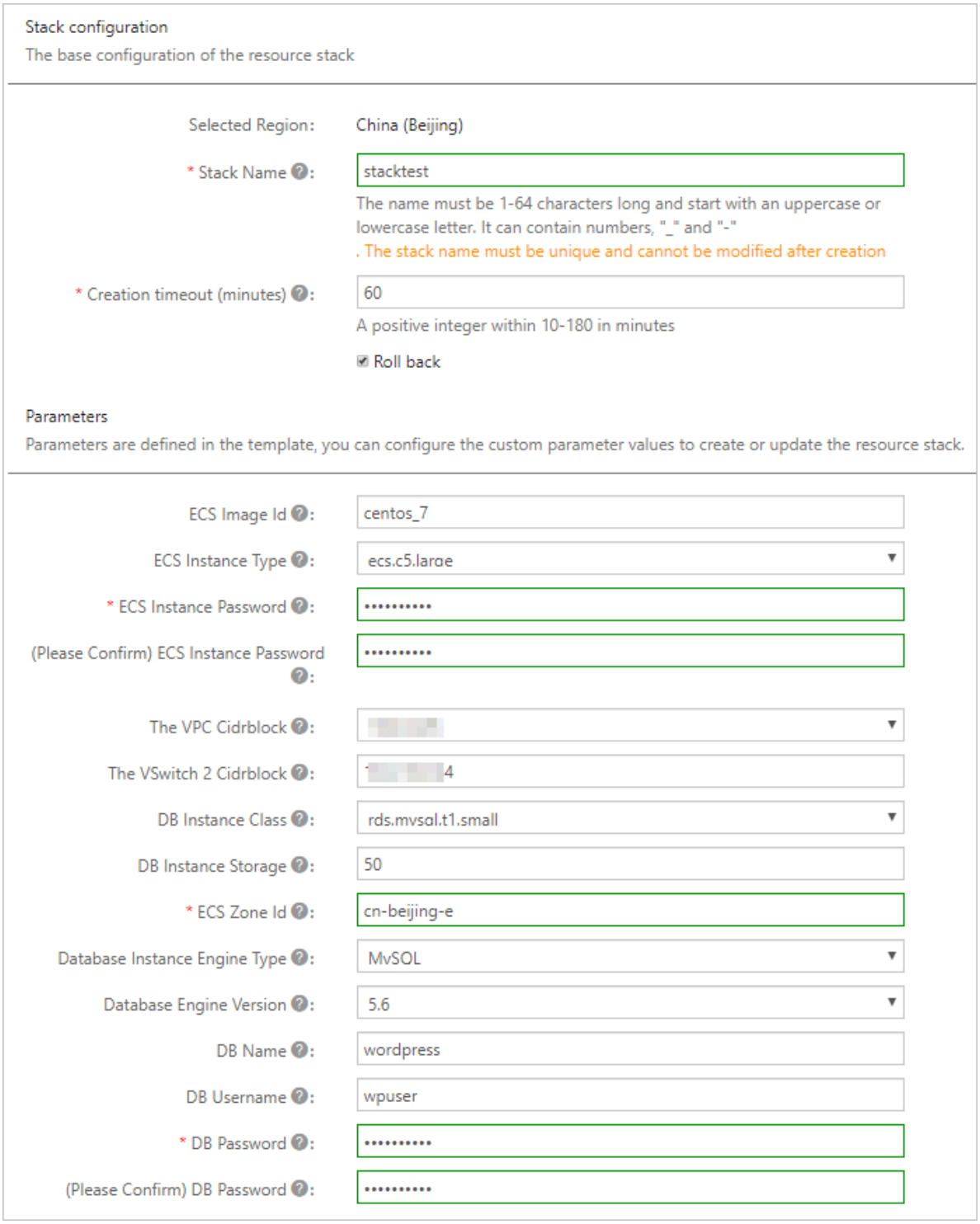
Parameter name	Description
Stack Name	Specifies a unique stack name. You cannot change the stack name after ROS creates the stack.
Creation timeout	Specifies a period. If ROS fails to create the specified resources within the period, the creation operation will time out. You can select or clear Roll back. · If you select Roll back, ROS will delete the created resources when an error such as creation timeout occurs during the creation process. · If you clear Roll back, ROS will not delete the created resources when any error such as creation timeout occurs during the creation process.

Parameter name	Description
ECS Image Id	The ID of the image that ROS uses to create the ECS instance. For more information, see Step 2.
ECS Instance Type	The type of the ECS instance that you want to create. For more information, see Step 2.
ECS Instance Password and (Please Confirm) ECS Instance Password	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 (&), asterisks (*), hyphens (-), underscores (_), plus signs (+), equal signs (=), vertical bars (|), braces ({}), brackets ([]), colons (:), semicolons (;), apostrophes ('), angle brackets (<>), commas (,), periods (.), question marks (?), and forward slashes (/). Note: Passwords for Windows-based instances cannot start with a forward slash (/).
The VPC Cidrblock	The private CIDR block of a Virtual Private Cloud (VPC). For more information, see #unique_4.
The VSwitch 2 Cidrblock	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_4.
DB Instance Class	The type of the ApsaraDB for RDS instance.
DB Instance Storage	The storage capacity of the ApsaraDB for RDS instance.
ECS Zone Id	The zone ID of the resource that you want to create. For more information, see Step 2.
Database Instance Engine Type	The engine of the database that you want to use.

Parameter name	Description
Database Engine Version	The version of the database engine that you want to use.
DB Name	The name of the MySQL database.
DB Username	The username of the MySQL database.

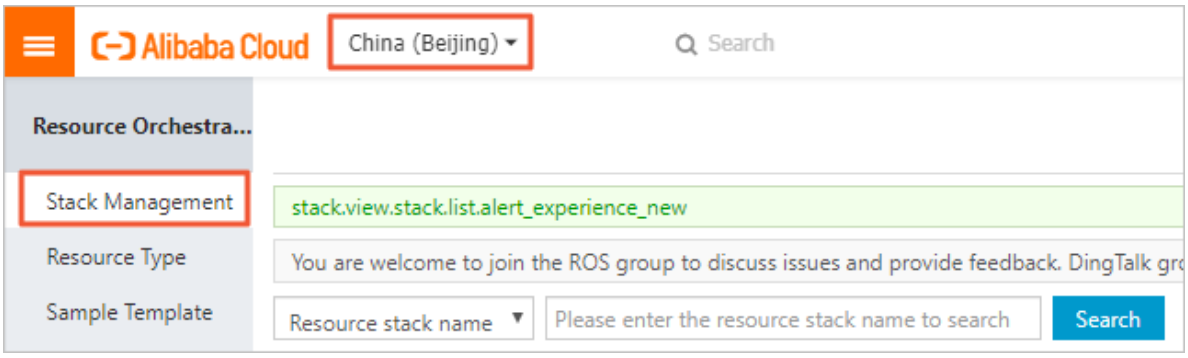
Parameter name	Description
DB Password	The password for accessing the MySQL database. The password must be 8 to 32 characters in length.

The following figure shows the configured parameters.



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.

2 Deploy LNMP

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 an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

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

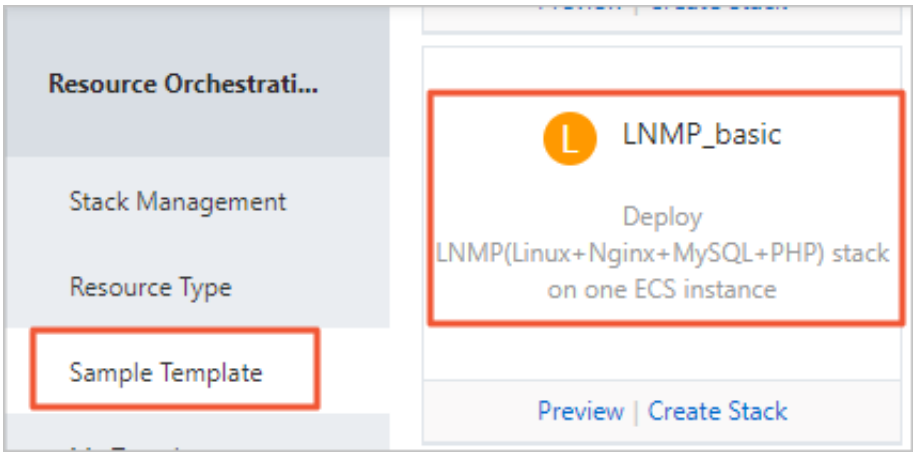
1. Log on to the ROS console.

   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.

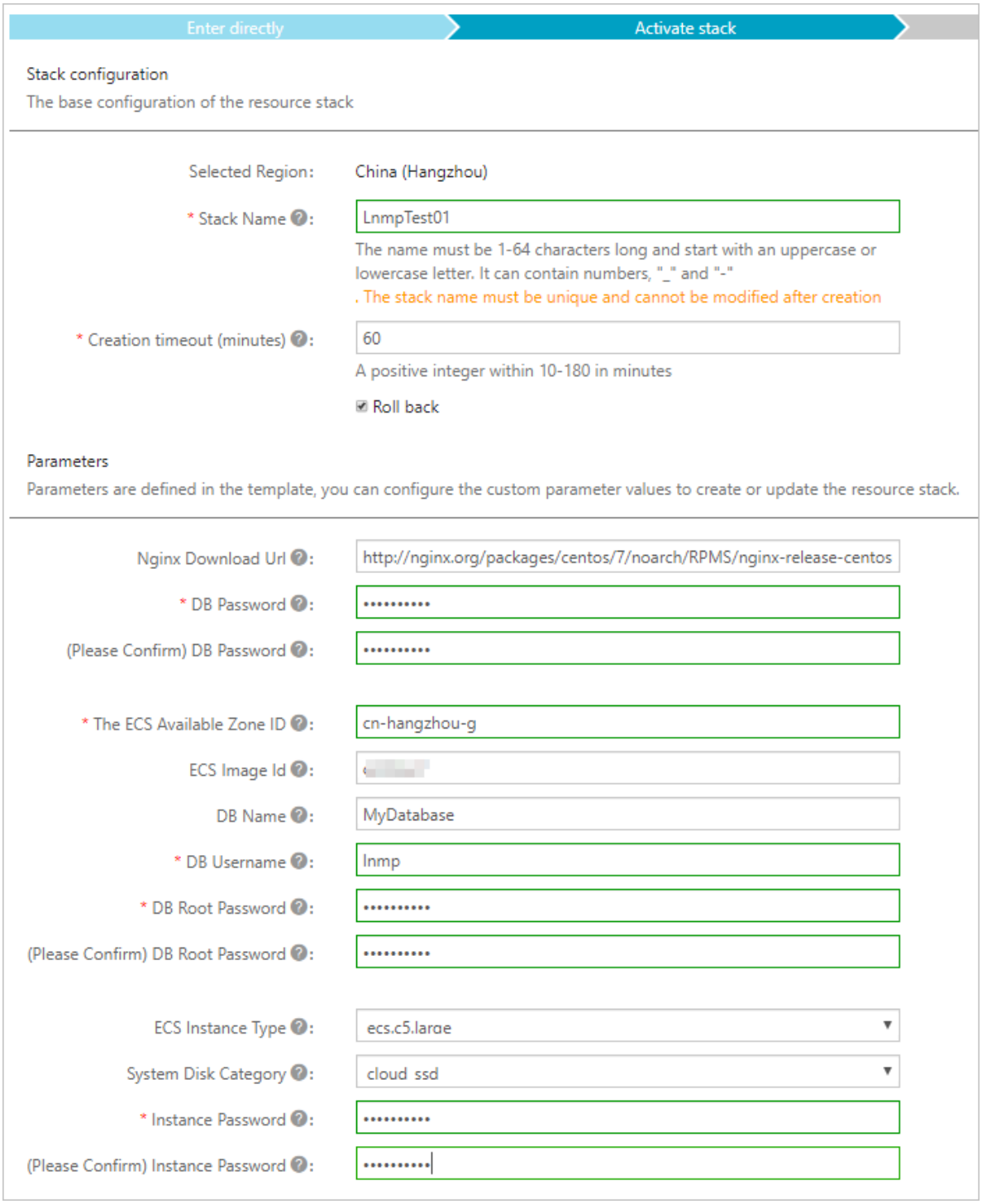
Top-level field	Description
`" ROSTemplat eFormatVer sion " : " 2015 - 09 - 01 "`	Specifies the version of the template.
`" Descriptio n ": " Deploy LNMP ( Linux + Nginx + MySQL + PHP ) stack on 1 ECS instance . *** WARNING *** Only support CentOS - 7 ."`	Describes the use of the template.
`" Parameters " : { }`	Specifies some parameters. In this example, this field specifies the default image ID and instance type.
`" Resources " : { }`	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.

Top-level field	Description
" Outputs ": { }	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 .

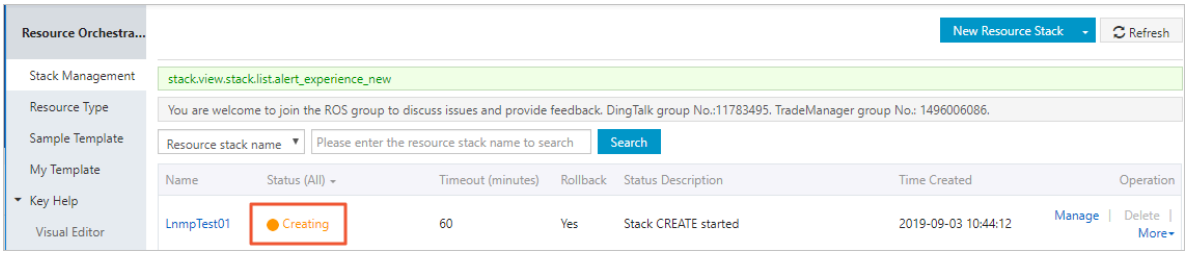
6. Click Create Stack.
7. Select the region where the ECS instance is located from the Region drop-down list, such as China (Hangzhou), and click Next.
8. Set stack parameters, and click Create.
   - Stack Name: specifies a unique stack name. You cannot change the stack name after ROS creates the stack.
   - 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.

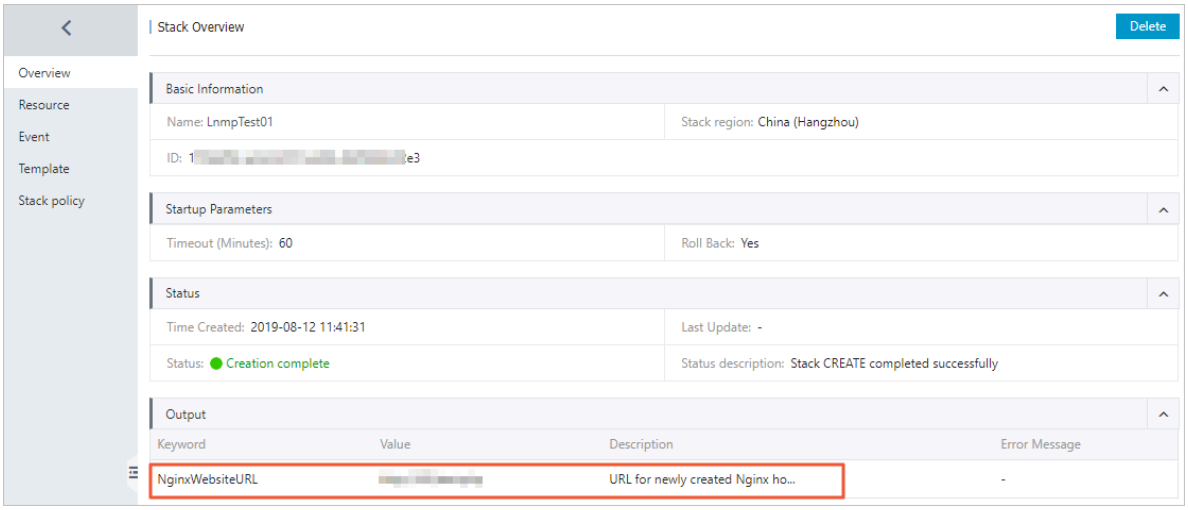
- Nginx Download Url: specifies the default NGINX download URL.
- DB Password and (Please Confirm) DB Password: specify the password for accessing a MySQL database and confirm the password. The password must contain only letters and digits.
- The ECS Available Zone ID: the zone ID of the resource that 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.



9. **In the left-side navigation pane, click Stack Management to check the state of the stack that you have created.**



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



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 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.

```
# 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.

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

   Run the command to make the configuration take effect immediately.

```
# setenforce 0
```

3. Security group setting.

   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 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 libtool 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 \
--http-fastcgi-temp-path=/var/tmp/nginx/fcgi \
--http-uwsgi-temp-path=/var/tmp/nginx/uwsgi \
--http-scgi-temp-path=/var/tmp/nginx/scgi \
--user=nginx \
--group=nginx \
--with-pcre \
--with-http_v2_module \
--with-http_ssl_module \
--with-http_realip_module \
--with-http_addition_module \
--with-http_sub_module \
--with-http_dav_module \
--with-http_flv_module \
--with-http_mp4_module \
--with-http_gunzip_module \
--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
#  descriptio  n :  Nginx   is   an   HTTP ( S )  server ,  HTTP ( S
 )  reverse  \
#               proxy   and   IMAP / POP3   proxy   server
#  processnam  e :  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   configurat  ion .
. / etc / sysconfig / network
#  Check   that   networking   is   up .
[ "$ NETWORKING " = " no " ] &&  exit   0
 nginx ="/ usr / sbin / nginx "
 prog =$( basename  $ nginx )
 NGINX_CONF  _FILE ="/ etc / nginx / nginx . conf "
[ - f  / etc / sysconfig / nginx  ] && . / etc / sysconfig / nginx
 lockfile =/ var / lock / subsys / nginx
 start () {
 [ - x  $ nginx  ] ||  exit   5
 [ - f  $ NGINX_CONF  _FILE  ] ||  exit   6
  echo  - n  $" Starting  $ prog : "
  daemon  $ nginx  - c  $ NGINX_CONF  _FILE
  retval =$?
  echo
 [ $ retval  - eq   0  ] &&  touch  $ lockfile
  return  $ retval
}
 stop () {
  echo  - n  $" Stopping  $ 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  $" Reloading  $ prog : "
  killproc  $ nginx  - HUP
 RETVAL =$?
  echo
}
 force_relo  ad () {
  restart
}
 configtest () {
$ nginx  - t  - c  $ NGINX_CONF  _FILE
}
 rh_status () {
  status  $ prog
}
 rh_status_  q () {
  rh_status  >/ dev / null   2 >& 1
}
 case  "$ 1 "  in
```

```
 start )
     rh_status_  q  &&  exit   0
$ 1
    ;;
 stop )
     rh_status_  q  ||  exit   0
    $ 1
    ;;
 restart | configtest )
    $ 1
    ;;
 reload )
     rh_status_  q  ||  exit   7
    $ 1
    ;;
 force - reload )
     force_relo  ad
    ;;
 status )
     rh_status
    ;;
 condrestar  t | try - restart )
     rh_status_  q  ||  exit   0
        ;;
*)
   echo  $" Usage : $ 0  { start | stop | status | restart
| condrestar  t | try - restart | reload | force - reload |
configtest }"
     exit   2
esac
```

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
```

```
# chkconfig nginx on
```

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.

Step3: Install MySQL

1. Prepare the compiling environment.

```
# yum groupinsta ll " Server Platform Developmen t " "
 Developmen t tools " - y
# yum install cmake - y
```

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

```
# 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.

```
#  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.

```
#  tar   xvf   mysql - 5 . 6 . 24 . tar . gz  - C   / usr / local /
 src
#  cd  / usr / local / src / mysql - 5 . 6 . 24
#  cmake  . - DCMAKE_INS  TALL_PREFI  X =/ usr / local / mysql  \
- DMYSQL_DAT  ADIR =/ mnt / data  \
- DSYSCONFDI  R =/ etc  \
- DWITH_INNO  BASE_STORA  GE_ENGINE = 1  \
- DWITH_ARCH  IVE_STORAG  E_ENGINE = 1  \
- DWITH_BLAC  KHOLE_STOR  AGE_ENGINE = 1  \
- DWITH_READ  LINE = 1  \
- DWITH_SSL = system  \
- DWITH_ZLIB = system  \
- DWITH_LIBW  RAP = 0  \
- DMYSQL_TCP  _PORT = 3306  \
- DMYSQL_UNI  X_ADDR =/ tmp / mysql . sock  \
- DDEFAULT_C  HARSET = utf8  \
- DDEFAULT_C  OLLATION = utf8_gener  al_ci
#  make  &&  make   install
```

5. Change the group of the installation directory to mysql.

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

6. Initializes the database.

```
# / usr / local / mysql / scripts / mysql_inst  all_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.

```
#  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.

```
#  chkconfig   mysqld   on
```

```
#  chkconfig  -- add   mysqld
```

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

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

10. Set the PATH environment variable.

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

11. Start the service.

```
#  service   mysqld   start
#  mysql  - h   127 . 0 . 0 . 1
```

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.

```
#  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.

```
#  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_conf  ig  \
-- 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.

```
#  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.

```
#  cp  / usr / local / src / php - 5 . 6 . 23 / sapi / fpm / init .
 d . php - fpm  / etc / init . d / php - fpm
#  chmod  + x  / etc / init . d / php - fpm
```

5. Add PHP-FPM to the service list, and set it to automatically start on startup.

```
#  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 .
 confbak
#  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_pa  ss      127 . 0 . 0 . 1 : 9000 ;
   fastcgi_in  dex     index . php ;
   fastcgi_pa  ram    SCRIPT_FIL  ENAME   / usr / local / nginx /
 html /$ fastcgi_sc  ript_name ;
   include          fastcgi_pa  rams ;
```

```
}
```

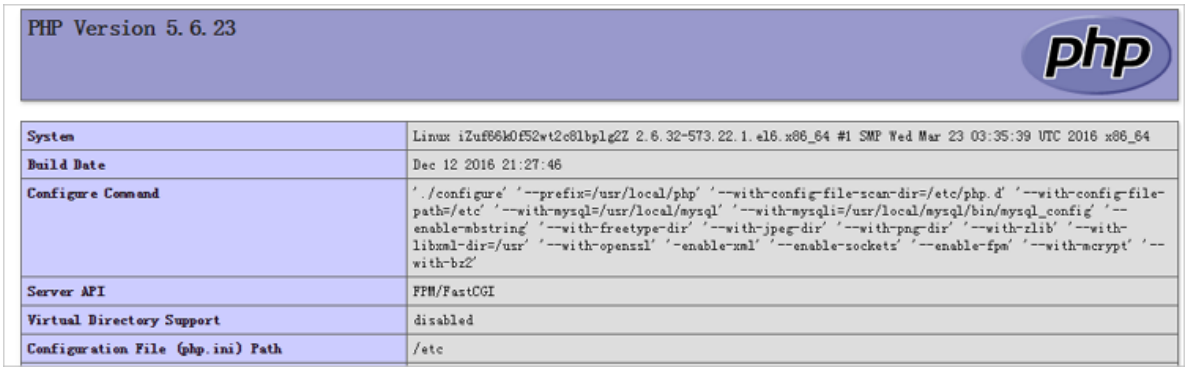
Reload the Nginx configuration file.

```
#  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_conn  ect (' 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.



2.3 Build an LNMP environment on CentOS 7

NGINX is a small and efficient Web server software for Linux. NGINX allows you to easily build an LNMP Web service environment. The LNMP environment is based on four major components required in this architecture: Linux, NGINX, MySQL, and PHP. This topic describes how to manually build the LNMP environment on an ECS instance.

Prerequisites

- You must have an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

- You have added an inbound rule to the security group of the ECS instance to support Ports 80 and 3306. For more information, see #unique_10.

Context

The procedure described in this topic is applicable to individual users that are familiar with Linux, but new to website construction by using Alibaba Cloud ECS instances.

The following software versions are used:

- Operating system: public image 64-bit CentOS 7.2
- NGINX: version 1.12.2
- MySQL: version 5.7.25
- PHP: version 7.0.33

The ECS instances described in this topic use the following configurations:

- CPU: 2 vCPUs
- Memory: 4 GiB
- Network type: Virtual Private Cloud (VPC)
- IP address: public IP address

You can also purchase an LNMP image in Alibaba Cloud Marketplace and launch an ECS instance from the image to efficiently build a website.

Procedure

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

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

Step 1: Prepare the compiling environment

To prepare the compiling environment, follow these steps:

1. Connect to a Linux ECS instance. For more information, see #unique_11 or #unique_12.
2. Disable the firewall.
   a) Run the command `systemctl status firewalld` to check the state of the firewall.

```
[root@test ~]# systemctl status firewalld
   firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor pr
eset: enabled)
   Active: active (running) since Tue 2018-11-13 10:40:03 CST; 21s ago
     Docs: man:firewalld(1)
 Main PID: 20785 (firewalld)
```

   - If the firewall stays in the `inactive` state, the firewall is disabled.
   - If the firewall stays in the `active` state, the firewall is enabled. In this example, the firewall is in the active state, so you must 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 command `systemctl stop firewalld`.

     Note:
     Therefore, the firewall is temporarily disabled, and will remain in the active state when you restart Linux next time.

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

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

3. Disable Security-Enhanced Linux (SELinux).

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

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

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

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

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

> Note:
> Therefore, SELinux is temporarily disabled, and will remain in the Enforcing state when you restart Linux next time.

- To permanently disable SELinux, follow these steps: Run the command `vi /etc/selinux/config`, and press the Enter key. Move the pointer to the line of `SELINUX=enforcing`, and press the `i` key to enter the edit mode. Edit the SELinux state in this way: `SELINUX=disabled`. Afterward, press the `Esc` key, type `:wq`, and then press the `Enter` key to save and close the SELinux configuration file.

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

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

Step 2: Install NGINX

To install NGINX, follow these steps:

1. Run the following command to install NGINX.

```
yum -y install nginx
```

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

```
nginx -v
```

The following response indicates that NGINX has been installed.

```
nginx version: nginx/1.12.2
```

Step 3: Install MySQL

To install MySQL, follow these steps:

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

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

2. Run the following command to install MySQL.

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

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

```
mysql -V
```

The following response indicates that MySQL has been installed.

```
mysql Ver 14.14 Distrib 5.7.25, for Linux (x86_64) using EditLine wrapper
```

Step 4: Install PHP

To install PHP, follow these steps:

1. Run the following commands in sequence to update the YUM repository.

```
# yum install -y http://dl.iuscommunity.org/pub/ius/stable/CentOS/7/x86_64/ius-release-1.0-15.ius.centos7.noarch.rpm
# rpm -Uvh https://mirror.webtatic.com/yum/el7/webtatic-release.rpm
```

Note:

The package `ius-release-1.0-15.ius.centos7.noarch.rpm` is used in this topic. In your actual running environment, use the latest ius-release package.

2. Run the following command to install PHP.

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

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
  Technologi es
    with Zend OPcache v7 . 0 . 33 , Copyright ( c ) 1999 -
2017 , by Zend Technologi es
```

Step 5: Configure NGINX

To configure NGINX, follow these steps:

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

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

2. Run the following command to open the NGINX configuration file.

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

3. Press the `i` key to enter the edit mode.
4. Add the following configurations between the braces of the *server* field so that NGINX can support PHP requests.

```
        location / {
            index index . php index . html index . htm ;
       }
       # Enables NGINX to process your PHP requests
by using Fast Common Gateway Interface ( FastCGI ).
        location ~ . php $ {
            root / usr / share / php ;
            fastcgi_pa ss 127 . 0 . 0 . 1 : 9000 ; # NGINX
forwards PHP requests to PHP FastCGI Process Manager
( PHP - FPM ) through Port 9000 of the ECS instance .
            fastcgi_in dex index . php ;
            fastcgi_pa ram SCRIPT_FIL ENAME $ document_r
oot $ fastcgi_sc ript_name ;
            include fastcgi_pa rams ; # NGINX uses the
FastCGI interface to process PHP requests .
```

```
        }
```

Note:
If you do not add the configurations, NGINX cannot process your PHP requests. As a result, you will not open the requested PHP-enabled page.

5. Run the following command to start the NGINX service.

```
systemctl start nginx
```

6. Run the following command to enable the NGINX service to run at startup.

```
systemctl enable nginx
```

Step 6: Configure MySQL

To configure MySQL, follow these steps:

1. Run the following command to start the MySQL service.

```
systemctl start mysqld
```

2. Run the following command to enable the MySQL service to run at startup.

```
systemctl enable mysqld
```

3. Run the following command to check the file */ var / log / mysqld . log* and obtain the initial password of the root user.

```
# 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
```

Note:
You must use the initial password to reset the password as the root user.

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

```
mysql_secu re_install ation
```

Continue with these steps for the security configuration:

a) Reset the password as the root user.

```
Enter password for user root : # Specifies the
initial password that you obtained in the previous
  step .
The ' validate_p assword ' plugin is installed on the
  server .
```

```
The subsequent steps will run with the existing
configurat ion 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 # Specifies whether
to change the password of the root user . Press
the Y key .
New password : # Specifies a new password . The
password must be 8 to 30 characters in length
and must contain letters , digits , and special
characters at the same time . The following special
characters are allowed : parenthese s ((()), grave
accents (`), tildes (~), exclamatio n points (!), at
signs (@), number signs (#), dollar signs ($), percent
signs (%), carets (^), ampersands (&), asterisks (*),
hyphens (-), underscore s ( _ ), plus signs (+), equal
signs (=), vertical bars (|), braces ({}), brackets
([]), colons (:), semicolons (;), apostrophe s ('), angle
brackets (<>), commas (,), periods (.), question marks
(?), and forward slashes (/).
Re - enter new password : # Confirms the new password .
Estimated strength of the password : 100
Do you wish to continue with the password
provided ?( Press y | Y for Yes , any other key for
No ) : Y
```

b) Press the `Y` key to delete anonymous users.

```
By default , a MySQL installati on 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 installati on go a bit smoother . You
should remove them before moving into a production
environmen t .
Remove anonymous users ? ( Press y | Y for Yes , any
other key for No ) : Y # Specifies whether to
delete anonymous users . Press the Y key .
Success .
```

c) Press the `Y` key to disable remote logon as the root user.

```
Disallow root login remotely ? ( Press y | Y for Yes
, any other key for No ) : Y # Specifies whether
to disable remote logon as a root user . Press
the Y key .
Success .
```

d) Press the `Y` key to delete the test database and the permission for accessing the test database.

```
Remove test database and access to it ? ( Press y |
Y for Yes , any other key for No ) : Y # Specifies
whether to delete the test database and the
permission for accessing the test database . Press
the Y key .
- Dropping test database ...
```

```
Success .
```

e) Press the `Y` key to reload the grant table.

```
Reload privilege tables now ? ( Press y | Y for Yes
, any other key for No ) : Y # Specifies whether
to reload the grant table . Press the Y key .
Success .
All done !
```

For more information, see MySQL documentation.

Step 7: Configure PHP

To configure PHP, follow these steps:

1. In the */ usr / share / php* directory, create a *phpinfo . php* file to show PHP version information. Continue with these steps:
   a) Run the command `vim / usr / share / php / phpinfo . php` to open the file.
   b) Press the `i` key to enter the edit mode.
   c) Enter the following code:

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

   d) Type `: wq` to save and close the 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 at startup.

```
systemctl enable php - fpm
```

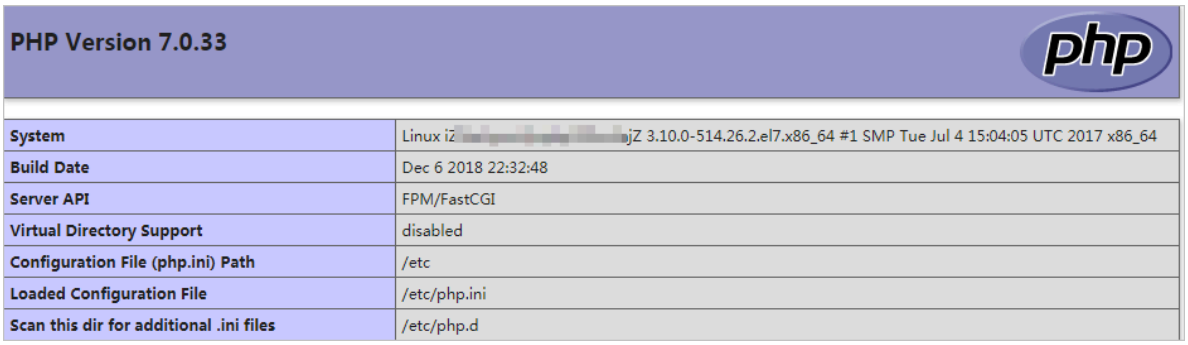
Step 8: Test the connection to the LNMP environment

To test the connection to the LNMP environment, follow these steps:

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.



What's next

Afterward, we recommend that you run the following command to delete */ usr / share / php / phpinfo . php* and secure your system.

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

3 Configure Java Web

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.

    ```
    systemctl stop firewalld . service
    ```

  - Set the firewall not to be enabled automatically at startup.

    ```
    systemctl disable firewalld . service
    ```

- Create a user www to run Tomcat.

  ```
  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.

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

- Create a Tomcat test page.

  ```
  echo Tomcat test > / data / wwwroot / default / index . jsp
  ```

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

Download source code

```
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/*.

```
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.

   ```
   mkdir /usr/java
   ```

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

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

3. Follow these steps to set environment variables:

   a. Run vi /etc/profile: `vi /etc/profile`

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

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

   ```
   # 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.

```
java  - version
```

```
java  - version
java   version  " 1 . 8 . 0_141 "
Java ( TM )  SE   Runtime   Environmen  t  ( 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.

```
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:
   a. Switch to the /usr/local/tomcat/conf/ directory: `cd / usr / local / tomcat / conf /`.
   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 version =" 1 . 0 " encoding =" UTF - 8 "? > < Server
port =" 8006 " shutdown =" SHUTDOWN "> < Listener className
=" org . apache . catalina . core . JreMemoryL eakPrevent
ionListene r "/> < Listener className =" org . apache .
catalina . mbeans . GlobalReso urcesLifec ycleListen er
"/> < Listener className =" org . apache . catalina . core
. ThreadLoca lLeakPreve ntionListe ner "/> < Listener
className =" org . apache . catalina . core . AprLifecyc
leListener "/> < GlobalNami ngResource s > < Resource name
=" UserDataba se " auth =" Container " type =" org . apache
. catalina . UserDataba se " descriptio n =" User database
that can be updated and saved " factory =" org
. apache . catalina . users . MemoryUser DatabaseFa ctory
" pathname =" conf / tomcat - users . xml "/> </ GlobalNami
ngResource s > < Service name =" Catalina "> < Connector
port =" 8080 " protocol =" HTTP / 1 . 1 " connection Timeout
=" 20000 " redirectPo rt =" 8443 " maxThreads =" 1000 "
minSpareTh reads =" 20 " acceptCoun t =" 1000 " maxHttpHea
derSize =" 65536 " debug =" 0 " disableUpl oadTimeout =" true
" useBodyEnc odingForUR I =" true " enableLook ups =" false
" URIEncodin g =" UTF - 8 "/> < Engine name =" Catalina "
defaultHos t =" localhost "> < Realm className =" org . apache
. catalina . realm . LockOutRea lm "> < Realm className =" org
. apache . catalina . realm . UserDataba seRealm " resourceNa
me =" UserDataba se "/> </ Realm > < Host name =" localhost
" appBase ="/ data / wwwroot / default " unpackWARs =" true
" autoDeploy =" true "> < Context path ="" docBase ="/ data
/ wwwroot / default " debug =" 0 " reloadable =" false "
crossConte xt =" true "/> < Valve className =" org . apache
. catalina . valves . AccessLogV alve " 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.

```
 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: `wget https :// github . com /
   lj2007331 / oneinstack / raw / master / init . d / Tomcat - init`
   b. Run the command to rename Tomcat-init: `mv Tomcat - init / etc /
   init . d / tomcat`
   c. Add the permission: `chmod  + x  / etc / init . d / tomcat`
   d. Set the startup script JAVA_HOME.

```
sed  - i  ' s @^ export  JAVA_HOME =.*@ export  JAVA_HOME =/
usr / java / jdk1 . 8 . 0_141 @' / etc / init . d / tomcat
```

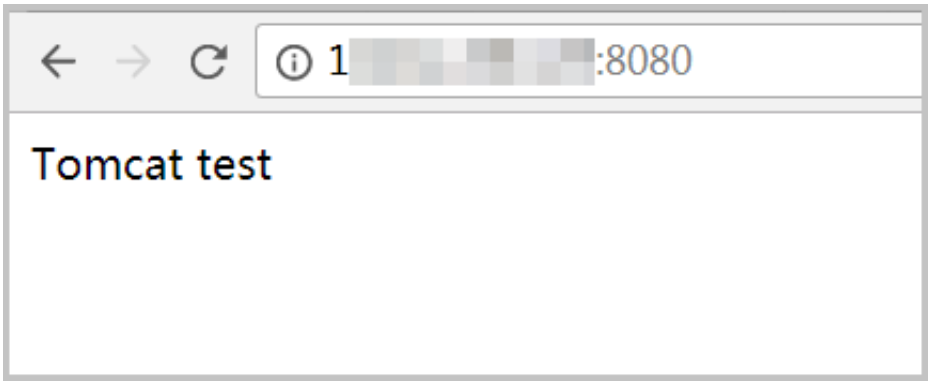
5. Set automatic startup.

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

6. Start Tomcat.

```
service  tomcat  start
```

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



3.2 Use the Eclipse plug-in to deploy applications

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

Prerequisites

- You have downloaded and installed Java Development Kit (JDK) 1.8 or later.
- You have downloaded and installed Eclipse IDE 4.5.0 or later. The program must be suitable for Java Enterprise Edition (Java EE) developers.
- You must have an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

Context

This topic describes how to install Cloud Toolkit in Eclipse on Windows, and efficientl y deploy an application by using Cloud Toolkit.

Procedure

To deploy a Java application by using the Eclipse plug-in on an ECS instance, follow these steps:

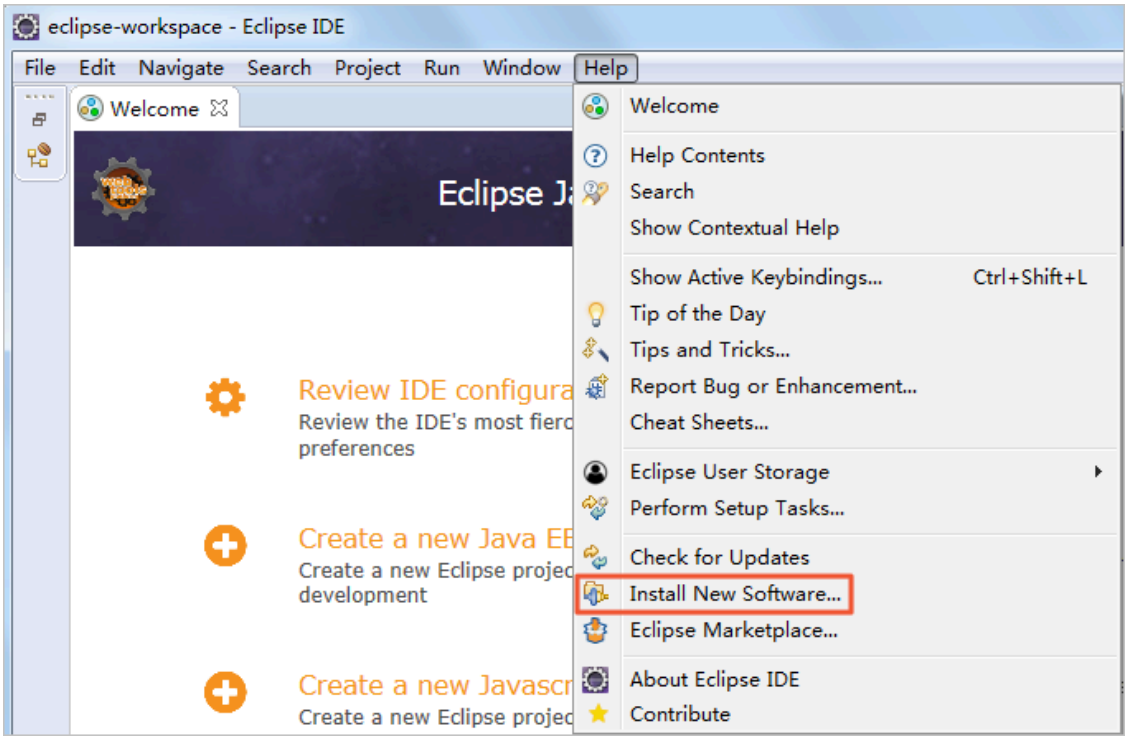
1. Step 1: Install Cloud Toolkit
2. Step 2: Set the AccessKey pair
3. Step 3: Download and upload the JDK installation package
4. Step 4: Prepare for installation
5. Step 5: Install JDK
6. Step 6: Install Apache Tomcat
7. Step 7: Deploy a Java application to the ECS instance

Step 1: Install Cloud Toolkit

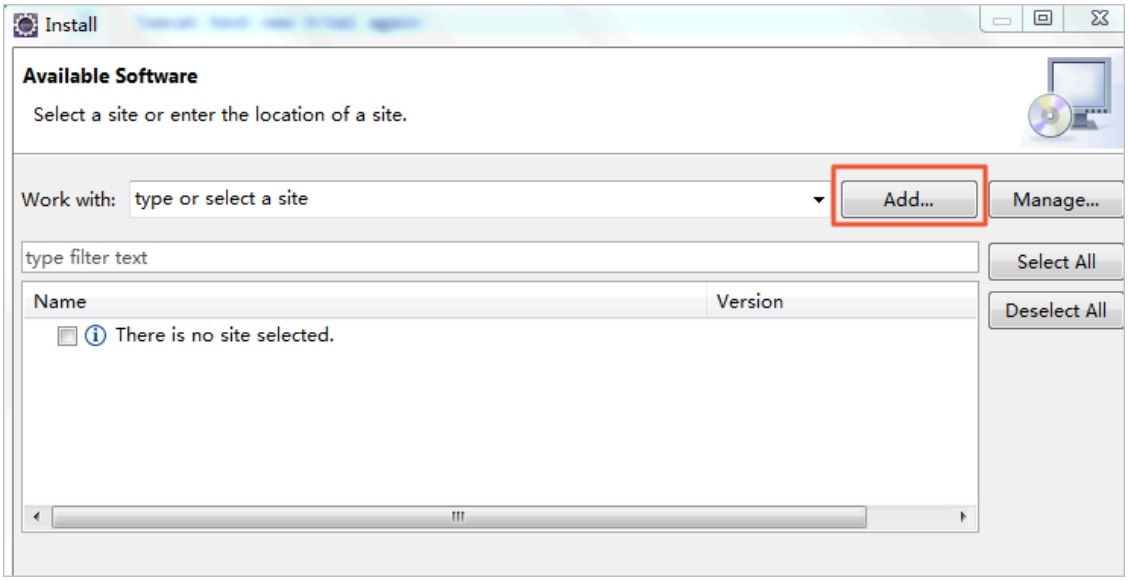
To install Cloud Toolkit, follow these steps:

1. Start Eclipse.

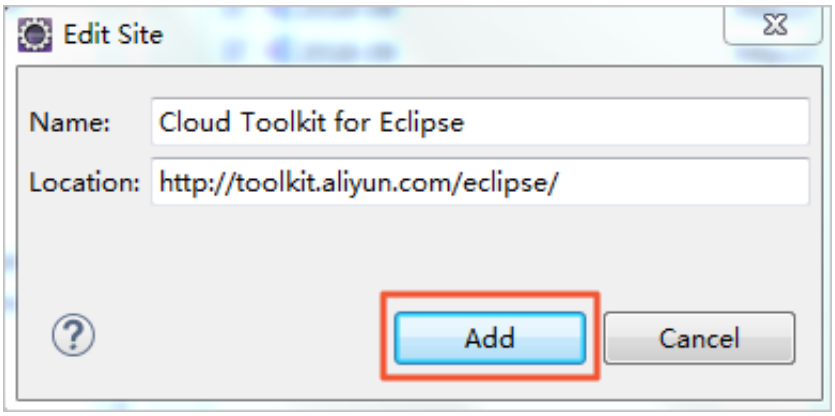
2. On the menu, choose Help > Install New Software....



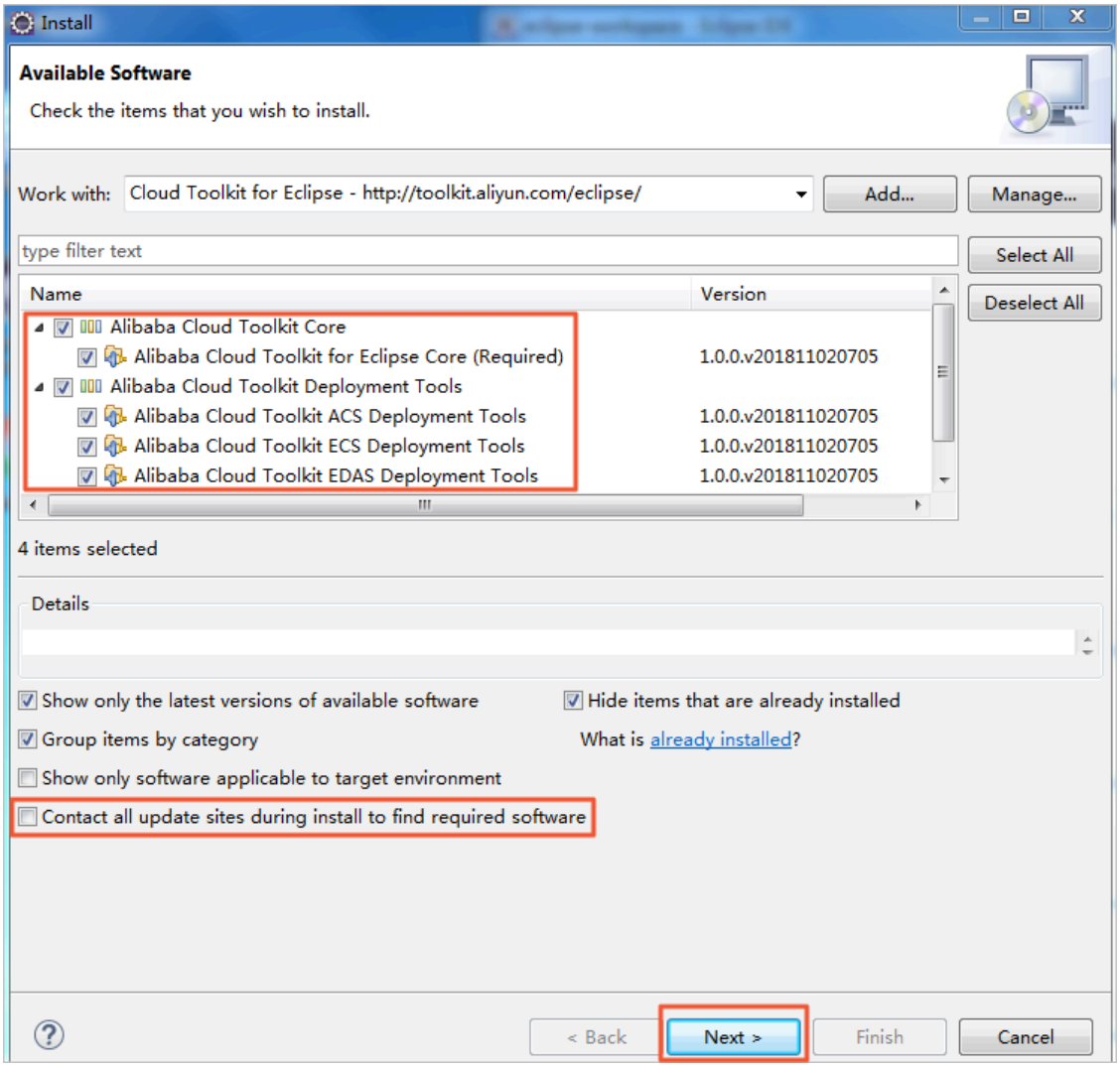
3. Click Add... in the window that appears.



4. Enter a name such as `Cloud Toolkit for Eclipse` and the software location `http://toolkit.aliyun.com/eclipse`, and click Add.

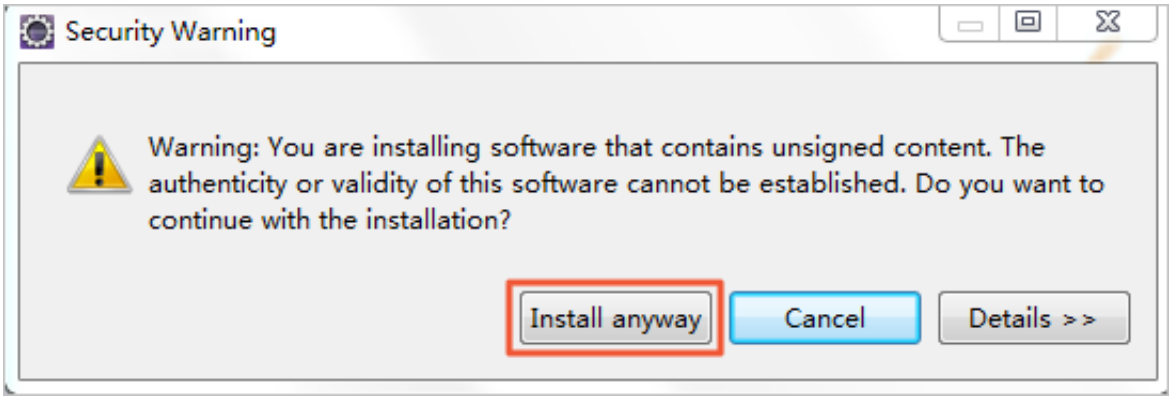


5. In the Name column, select Alibaba Cloud Toolkit Core and Alibaba Cloud Toolkit Deployment Tools, and clear Contact all update sites during install to find required software in the Details section, and then click Next.

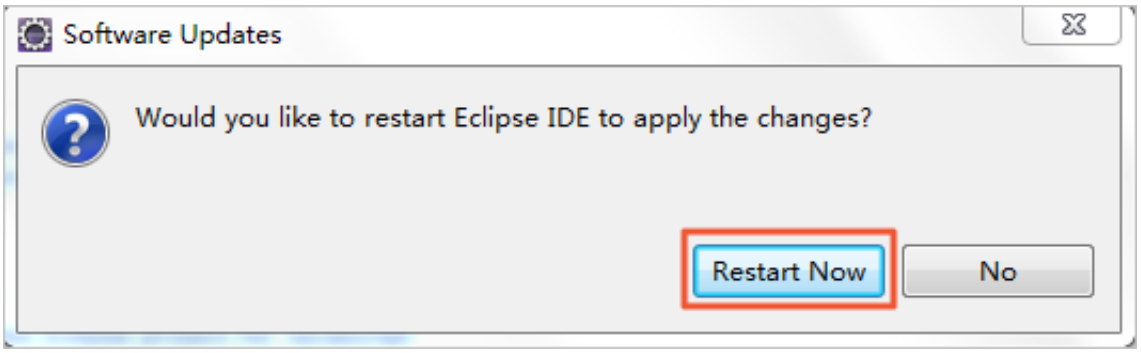


6. Click Next.

7. Select I accept the terms of the license agreement, and click Finish.
8. Click Install anyway.



9. Click Restart Now to restart Eclipse.

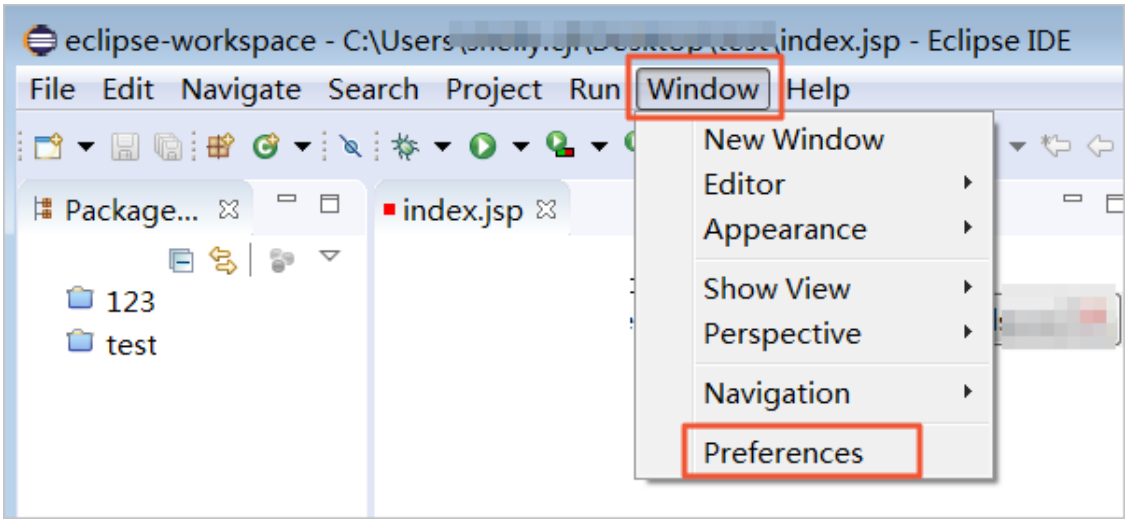


Step 2: Set the AccessKey pair

The AccessKey ID and AccessKey Secret are issued to users by Alibaba Cloud. 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 pair must be kept confidential.

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

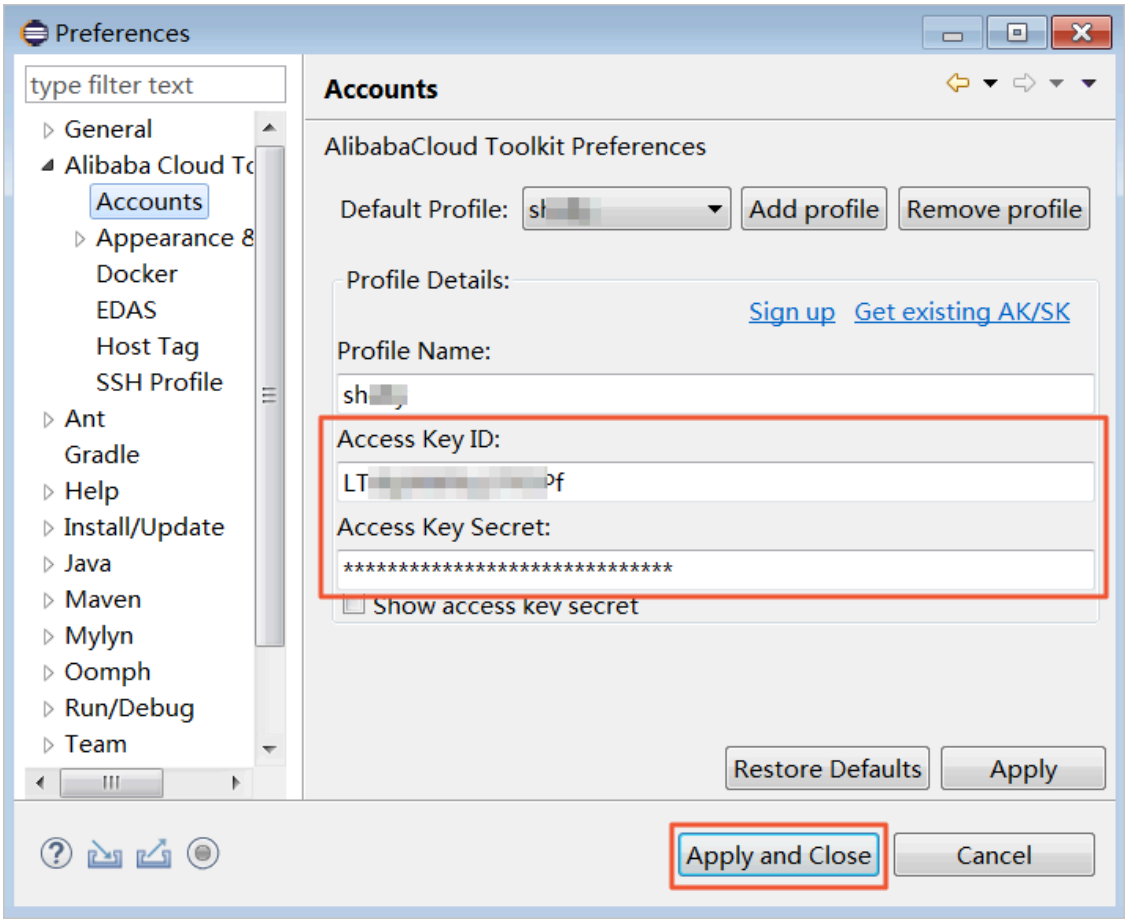
1. On the toolbar, choose Window > Preferences.



2. In the left-side navigation pane, choose Alibaba Cloud Toolkit > Accounts.
3. Enter the AccessKey ID and AccessKey Secret, and click Apply and Close.

> Note:
>
> · If you have an account but have not generated any AccessKey pair, click Get existing AK/SK, and log on to the Alibaba Cloud console to generate an AccessKey pair. For more information, see Create an AccessKey pair.

· If you have not created any account, click Sign up.



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. You can click here to obtain the required installation package address.

2. Download the JDK installation package.

   Note:
   If you download the JDK package on an ECS instance, an error occurs during decompression. You can download the JDK installation package to your local directory and upload the package to the ECS 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 ECS instance, and obtain the public IP address of the instance from the IP Address column.
7. Start Windows Secure Copy (WinSCP), use the public IP address to connect to the Linux ECS instance, and then upload the JDK installation package to the root directory of the Linux ECS instance.

Step 4: Prepare for installation

To prepare for installation, follow these steps:

1. #unique_17.
2. Add inbound rules to support the required ports. For more information, see #unique_10.
3. Disable the firewall.
   a) Run the command `systemctl status firewalld` to check the state of the firewall.

```
[root@test ~]# systemctl status firewalld
   firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor pr
eset: enabled)
   Active: active (running) since Tue 2018-11-13 10:40:03 CST; 21s ago
     Docs: man:firewalld(1)
 Main PID: 20785 (firewalld)
```

   - If the firewall stays in the `inactive` state, the firewall is disabled.
   - If the firewall stays in the `active` state, the firewall is enabled. In this example, the firewall is in the active state, so you must 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 command `systemctl stop firewalld`.

     Note:
     Therefore, the firewall is temporarily disabled, and will remain in the active state when you restart Linux next time.

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

     Note:

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

4. Disable Security-Enhanced Linux (SELinux).

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

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

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

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

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

Note:
Therefore, SELinux is temporarily disabled, and will remain in the Enforcing state when you restart Linux next time.

- To permanently disable SELinux, follow these steps: Run the command `vi /etc/selinux/config`, and press the Enter key. Move the pointer to the line of `SELINUX=enforcing`, and press the `i` key to enter the edit mode. Edit the SELinux state in this way: `SELINUX=disabled`. Afterward, press the `Esc` key, type `:wq`, and then press the `Enter` key to save and close the SELinux configuration file.

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

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

5. Create a user named www to run Tomcat.

```
useradd   www
```

6. Creates a root directory for the Java Web project.

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

7. Assign 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:

1. Run mkdir /usr/java to create a directory.

```
mkdir  / usr / java
```

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

```
chmod  + x   jdk - 8u191 - linux - x64 . tar . gz
tar   xzf   jdk - 8u191 - linux - x64 . tar . gz  - C  / usr / java
```

3. Set environment variables.

   a) Run the command `vi / etc / profile` 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.

```
#  set   java   environmen  t
 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 type `: wq` to save and close the file.

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

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

   The following response indicates that JDK has been 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:

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

```
tar   xzf   apache-tomcat-8.5.34.tar.gz
mv   apache-tomcat-8.5.34  /usr/local/tomcat/
chown  -R   www.www  /usr/local/tomcat/
```

The directory */usr/local/tomcat/* contains the following files:

- The *bin* directory stores some Tomcat script files, including scripts for enabling and disabling the Tomcat service.
- The *conf* directory stores various global configuration files for the Tomcat server, including the important files *server.xml* and *web.xml*.
- The *webapps* directory is the main Web publishing directory of Tomcat to store Web application files by default.
- The *logs* directory stores Tomcat log files.

2. Configure the *server.xml* file.
   a) Run the command `cd  /usr/local/tomcat/conf/` to switch to the directory */usr/local/tomcat/conf/*.
   b) Run the command `mv  server.xml  server.xml_bk` to rename the *server.xml* file.
   c) Run the `vi  server.xml` command.
   d) Press the `i` key to enter the edit mode.
   e) Add the following code:

```
<?  xml   version =" 1.0 "  encoding =" UTF-8 "? >
< Server   port =" 8006 "  shutdown =" SHUTDOWN ">
< Listener   className =" org.apache.catalina.core.
 JreMemoryL  eakPrevent  ionListene  r "/>
< Listener   className =" org.apache.catalina.mbeans.
 GlobalReso  urcesLifec  ycleListen  er "/>
< Listener   className =" org.apache.catalina.core.
 ThreadLoca  lLeakPreve  ntionListe  ner "/>
< Listener   className =" org.apache.catalina.core.
 AprLifecyc  leListener "/>
< GlobalNami  ngResource  s >
< Resource   name =" UserDataba  se "  auth =" Container "
  type =" org.apache.catalina.UserDataba  se "
  descriptio  n =" User   database   that   can   be   updated
 and   saved "
```

```
  factory =" org . apache . catalina . users . MemoryUser
 DatabaseFa  ctory "
  pathname =" conf / tomcat - users . xml "/>
</ GlobalNami  ngResource  s >
< Service   name =" Catalina ">
< Connector   port =" 8080 "
  protocol =" HTTP / 1 . 1 "
  connection  Timeout =" 20000 "
  redirectPo  rt =" 8443 "
  maxThreads =" 1000 "
  minSpareTh  reads =" 20 "
  acceptCoun  t =" 1000 "
  maxHttpHea  derSize =" 65536 "
  debug =" 0 "
  disableUpl  oadTimeout =" true "
  useBodyEnc  odingForUR  I =" true "
  enableLook  ups =" false "
  URIEncodin  g =" UTF - 8 "/>
< Engine   name =" Catalina "  defaultHos  t =" localhost ">
< Realm   className =" org . apache . catalina . realm .
 LockOutRea  lm ">
< Realm   className =" org . apache . catalina . realm .
 UserDataba  seRealm "
   resourceNa  me =" UserDataba  se "/>
</ Realm >
< Host   name =" localhost "  appBase ="/ data / wwwroot / default
 "  unpackWARs =" true "  autoDeploy =" true ">
< Context   path =""  docBase ="/ data / wwwroot / default "
 debug =" 0 "  reloadable =" false "  crossConte  xt =" true "/>
< Valve   className =" org . apache . catalina . valves .
 AccessLogV  alve "  directory =" logs "
 prefix =" localhost_  access_log ."  suffix =". txt "  pattern
 ="% h  % l  % u  % t  & quot ;% r & quot ; % s  % b " />
</ Host >
</ Engine >
</ Service >
</ Server >
```

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

3. Set Java virtual machine (JVM) memory parameters.

a) Run the command `vi  / usr / local / tomcat / bin / setenv . sh` 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, and type `: wq` to save and close the file.

4. Set a script to enable Tomcat to run at startup.
   a) Run the command `wget https://github.com/lj2007331/oneinstack/raw/master/init.d/Tomcat-init` to download the script.
   b) Run the command `mv Tomcat-init /etc/init.d/tomcat` to rename the *Tomcat-init* file.
   c) Run the command `chmod +x /etc/init.d/tomcat` to assign the execute permission to the script file.
   d) Run the following code to set the JAVA_HOME script for automatic startup.

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

5. Set automatic startup.

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

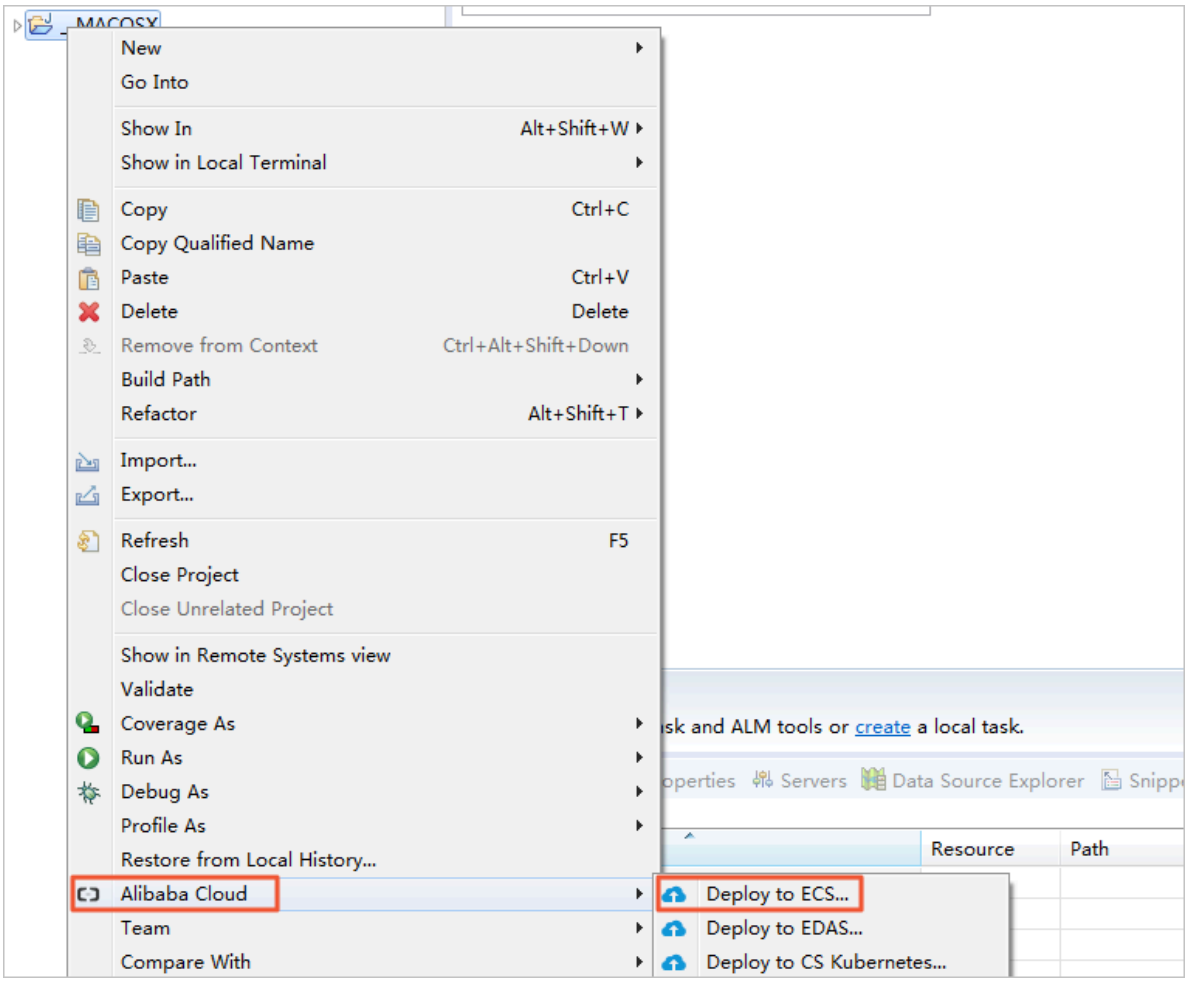
6. Start Tomcat.

```
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, you connect to *http://Public IP address of the ECS instance:8080* to view `Tomcat test`. Follow these steps:

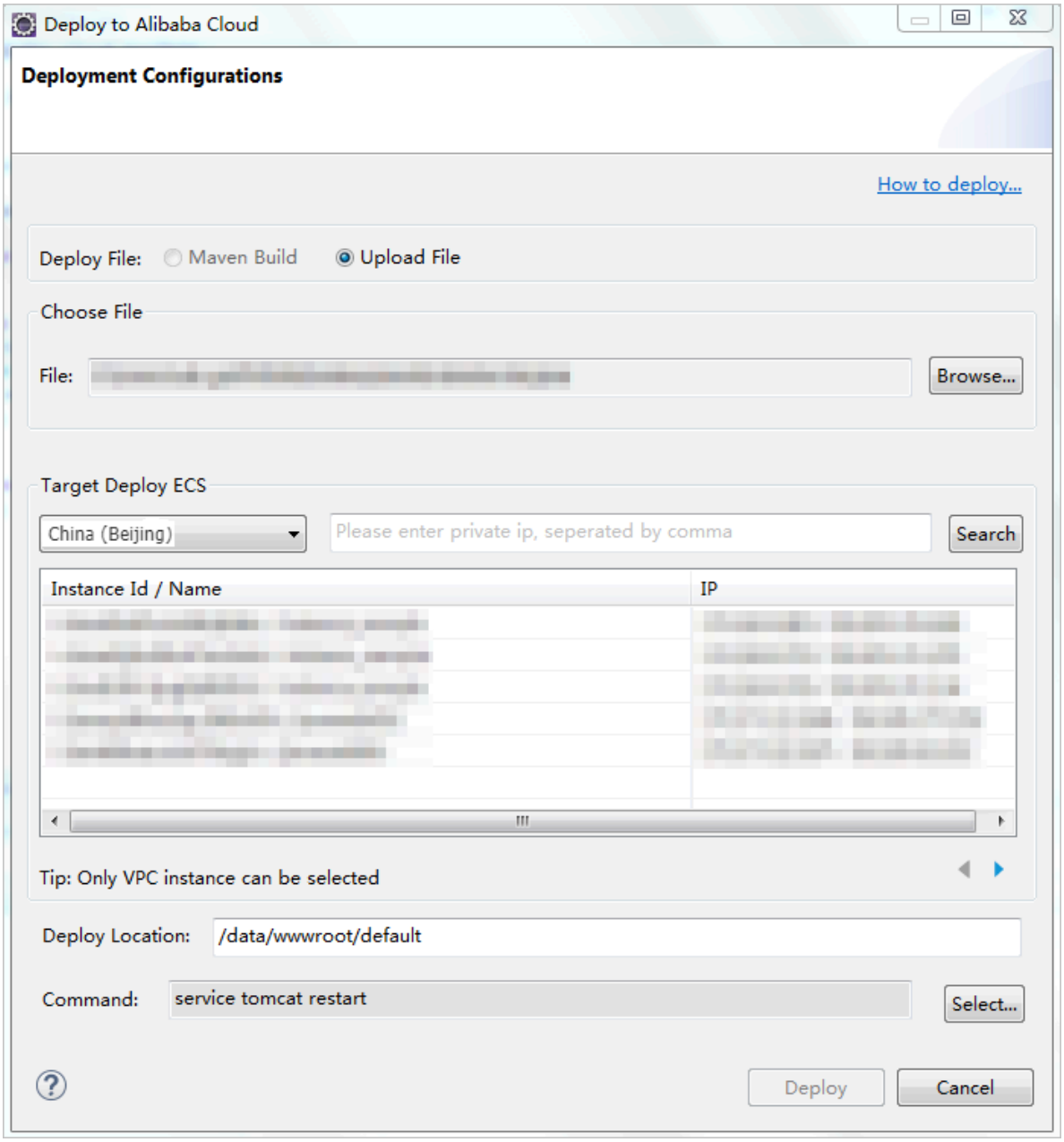
1. In Eclipse, right-click the name of the application project that you want to deploy, and choose Alibaba Cloud > Deploy to ECS....



2. In the window Deploy to Alibaba Cloud that appears, follow these settings:

   - Deploy File: the deployment method, such as Upload File in this example. If you build the application project by using Maven, select Maven Build.
   - Choose File: the file that you want to deploy.
   - Target Deploy ECS: specifies the region where your instance is located and the target instance.
   - Deploy Location: the directory that you deploy on the ECS instance, such as `/data/wwwroot/default` in this example.
   - Command: Click Select..., and in the dialog box that appears, click Add.... Enter a command in the text box. The ECS instance runs the command automatically after the Cloud Toolkit plug-in 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 another command as needed.



3. Click Deploy to start deploying the Java application to the ECS instance.

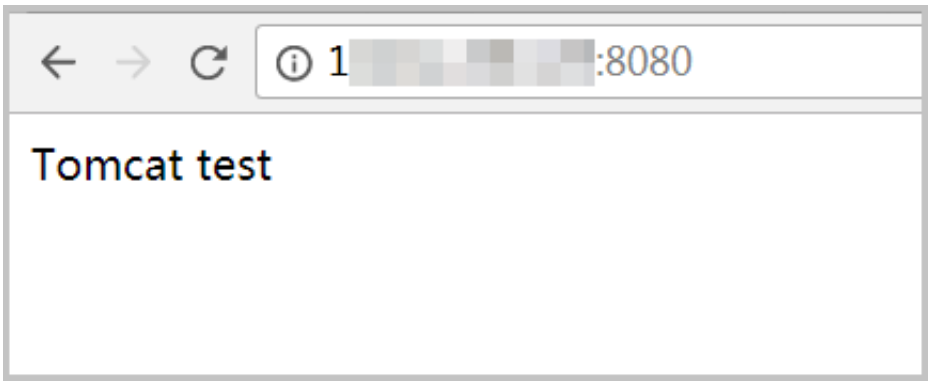
4. In the Console section of Eclipse, you can view the progress of the deployment.

```
Console

[INFO] Target Deploy ECS: {                    }
[INFO] Command: {service tomcat restart }
[INFO] Result: {[00;31mStoping Tomcat[00m
[00;31mwaiting for processes to exit[00m
[00;32mStarting tomcat[00m
Tomcat started.
[00;32mTomcat is running with pid:      [00m }
[INFO] Finished at: 2018-11-07T16:12:00+8:00
[INFO] File Upload Total time: 7.345 s
```

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

   The following response indicates that the Java application has been deployed to the ECS instance by using the Alibaba Cloud Toolkit for Eclipse plug-in.



What's next

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

4 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 an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

Context

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

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

Procedure

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

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

Step 1: Create and connect to an ECS instance

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

1. Use the public image 64-bit CentOS 7.2 to create an ECS instance. For more information, see Create an ECS instance.
2. Use the `root` user to connect to the ECS instance. For more information, see #unique_12.

Step 2: Deploy the Node.js environment

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

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

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

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

  1. Download the Node.js installation package.

     ```
     wget  https :// nodejs . org / dist / v6 . 9 . 5 / node - v6 . 9
     . 5 - linux - x64 . tar . xz
     ```

  2. Decompress the file.

     ```
     tar  xvf  node - v6 . 9 . 5 - linux - x64 . tar . xz
     ```

  3. After you create a soft link, you can run node and npm commands directly in any directory.

     ```
     ln  - s  / root / node - v6 . 9 . 5 - linux - x64 / bin / node  /
     usr / local / bin / node
     ln  - s  / root / node - v6 . 9 . 5 - linux - x64 / bin / npm  /
     usr / local / bin / npm
     ```

  4. Check the versions of node and npm.

     ```
     node  - v
     ```

```
npm  - v
```

Then, the Node.js environment has been installed. By default, the software is installed in the directory */ root / node - v6 . 9 . 5 - linux - x64 /*.

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

```
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 @ iZXXXXZ  . nvm ]#  nvm  ls
       v6 . 9 . 5
```

```
->        v7 . 4 . 0
        system
 stable  ->  7 . 4  (->  v7 . 4 . 0 ) ( default )
 unstable  ->  6 . 9  (->  v6 . 9 . 5 ) ( default )
```

6. Run the command `nvm use v7 . 4 . 0` to switch to Node.js v7.4.0. The response is as follows:

```
[ root @ iZXXXXZ  . nvm ]#  nvm  use  v7 . 4 . 0
 Now  using  node  v7 . 4 . 0
```

Step 3: Deploy a test project

To deploy a test project, follow these steps:

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

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

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

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

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

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

```
 const  http  =  require (' http ');
 const  hostname  = ' 0 . 0 . 0 . 0 ';
 const  port  =  3000 ;
 const  server  =  http . createServ  er (( req ,  res ) => {
     res . statusCode  =  200 ;
     res . setHeader (' Content - Type ', ' text / plain ');
     res . end (' Hello  World \ n ');
});

 server . listen ( port ,  hostname , () => {
     console . log (` Server  running  at  http ://${ hostname }:
${ port }/`);
});
```

Note:

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

3. Run the project.

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

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

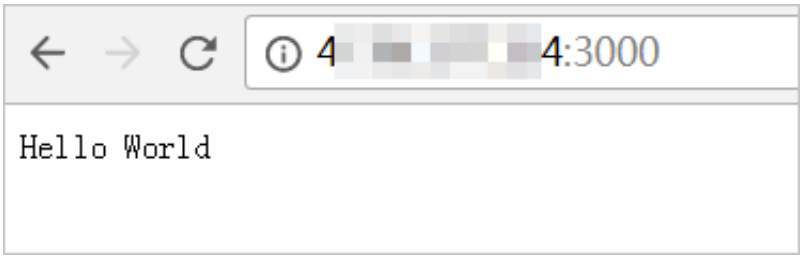
```
netstat -tpln
```

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_20.

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.



More information

Alibaba Cloud sandbox platform

Alibaba Cloud Marketplace

5 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 insgtance.

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.

Service	Rule Direction	Authorization Policy	Protocol Type	Port Range	Authorization Type	Authorization Object	Priority
HTTP	Inbound	Allow	User-defined TCP	80/80	Address Field Access	0.0.0.0/0	1
MySQL	Inbound	Allow	User-defined TCP	3306/3306	Address Field Access	0.0.0.0/0	1

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.

```
# 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.

```
# 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_secu  re_install  ation
 Securing   the   MySQL   server   deployment .
 Enter   password   for   user   root :  #  Enter   your   temporary
   root   password   that   is   recorded   in   the   previous
 step
 The  ' validate_p  assword '  plugin   is   installed   on   the
 server .
 The   subsequent   steps   will   run   with   the   existing
 configurat  ion   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
 : ()`~! @#$%^& amp ;*-+=|{}[]:;‘& lt ;>,.? /
 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   installati  on   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   installati  on   go   a   bit   smoother .  You
 should   remove   them   before   moving   into   a   production
 environmen  t .
 Remove   anonymous   users ? ( Press   y | Y   for   Yes ,  any
 other   key   for   No ):  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   y | Y   for   Yes ,
 any   other   key   for   No ):  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
 environmen  t .
```

```
 Remove   test   database   and   access   to   it ? ( Press   y | Y
   for   Yes ,  any   other   key   for   No ):  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   immediatel  y .
 Reload   privilege   tables   now ? ( Press   y | Y   for   Yes ,
 any   other   key   for   No ):  Y
 Success .
 All   done !
```

6. Install PHP 7.

```
#  yum   install  - y   http :// dl . iuscommuni  ty . 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 - mysqlnd
   php70u - opcache   php70u - xml   php70u - gd   php70u - mcrypt
   php70u - devel   php70u - intl   php70u - mbstring   php70u -
 bcmath   php70u - json   php70u - iconv
```

7. Validate PHP installation.

```
#  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
   Technologi  es
 with   Zend   OPcache   v7 . 0 . 13 ,  Copyright  ( c )  1999 -
 2016 ,  by   Zend   Technologi  es
```

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

   a. Run `vim  / etc / php . ini` .

   b. Press the `i` key.

   c. Find the line starting with `date . timezone` which is commented out by default, and add the correct time zone. If your site is in China, add `date . timezone  =  Asia / Shanghai` .

9. Restart httpd by running the following.

```
systemctl   start   httpd
```

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 |
+--------------------+
| informatio n_schema |
| magento |
+--------------------+
2 rows in set (0.00 sec)
mysql> exit
```

Step 3: Install and configure Composer

1. Install Composer.

```
# curl -sS https://getcompose r.org/installer | php
All settings correct for using Composer
Downloadin g 1.2.4 ...
Composer successful ly 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/
# git clone https://github.com/magento/magento2.git
```

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 ..
```

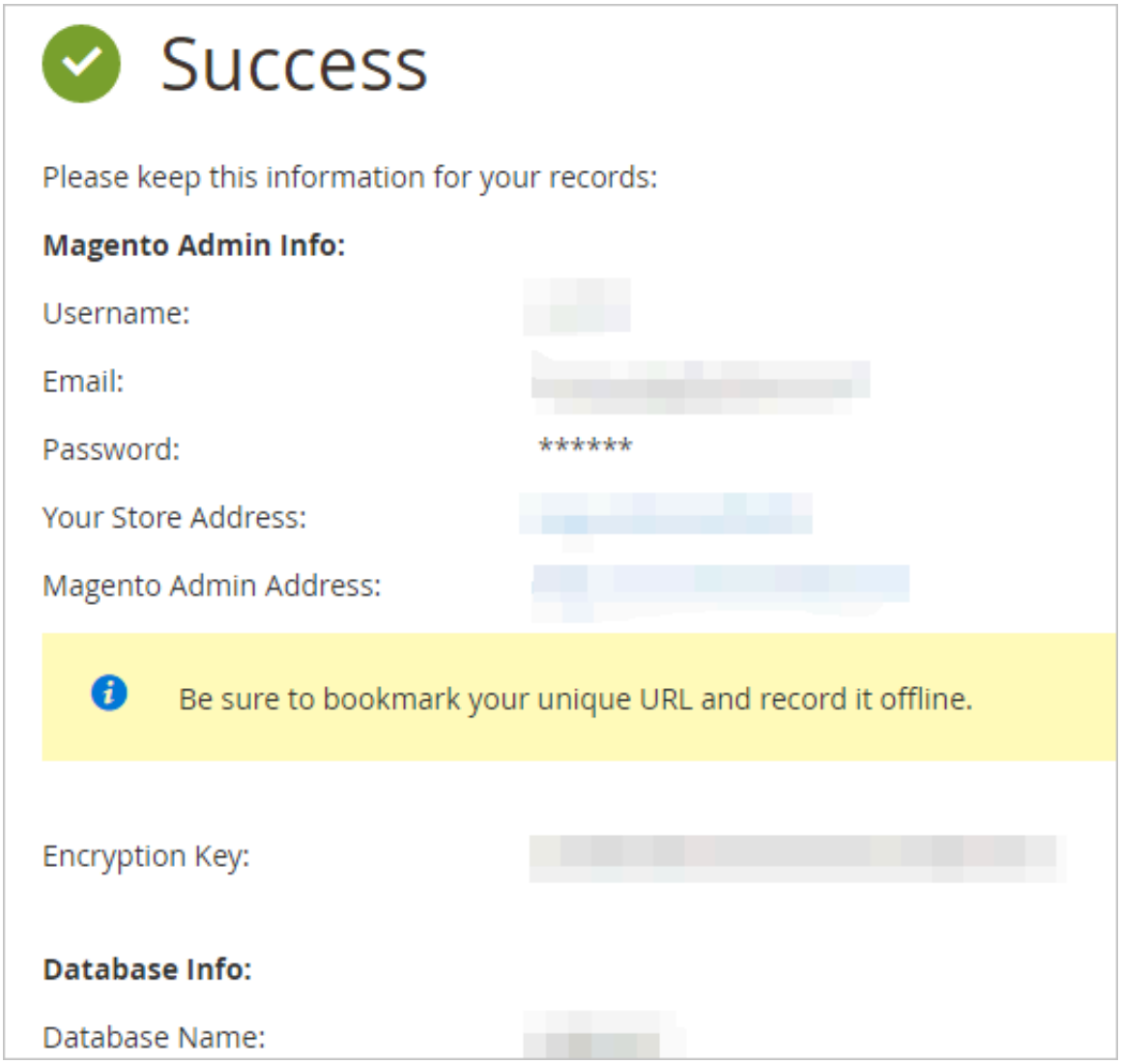
4. Set Magento file permissions.

```
# 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.



Step 5: Configure the cron job

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

```
*/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.

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.

6 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 an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

Context

Microsoft SharePoint Portal Server (Microsoft SharePoint) is a portal developmen t 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:

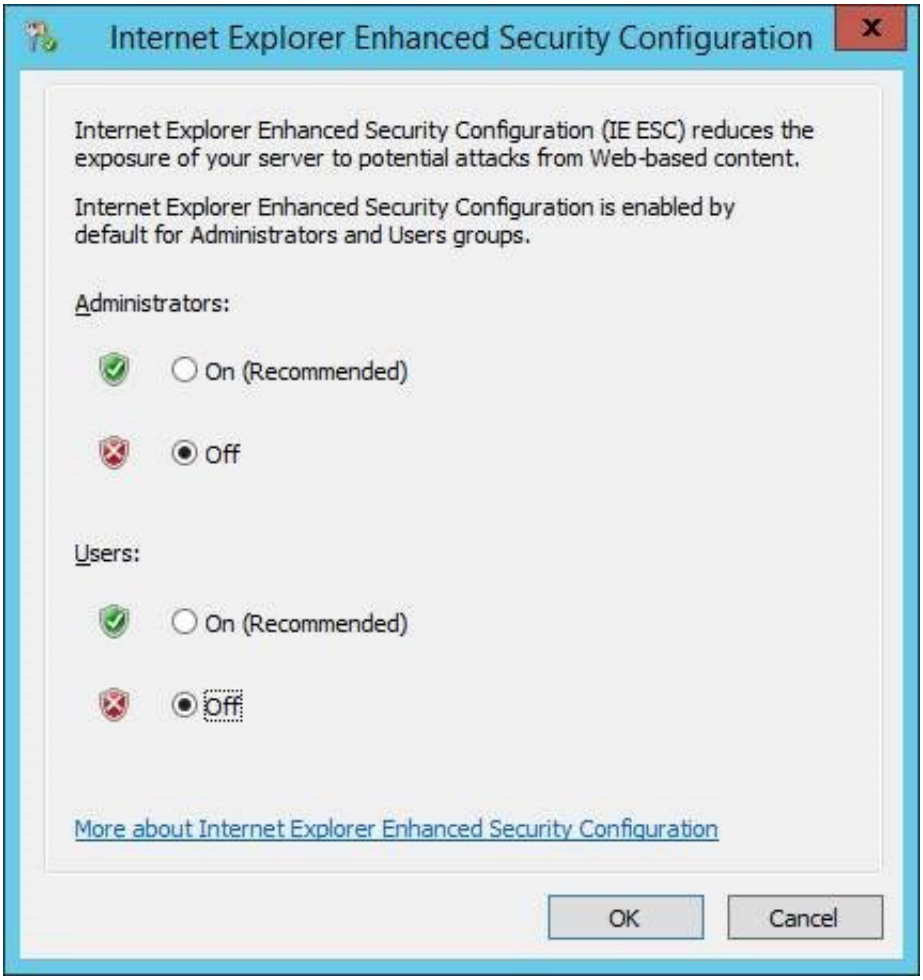
1. Step 1: Add the AD, DHCP, DNS, and IIS services
2. Step 2: Install SQL Server 2014
3. Step 3: Install SharePoint 2016

4. Step 4: Configure SharePoint 2016

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

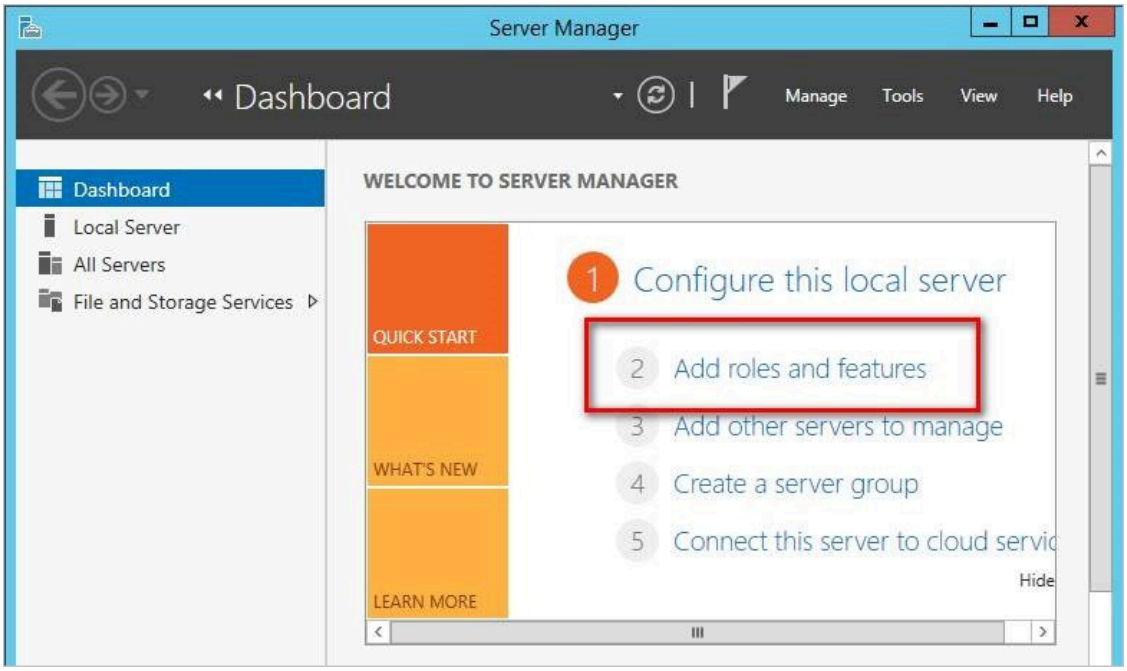
To add the Active Directory (AD), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and Internet Information Services (IIS) services, follow these steps:

1. Purchase an ECS instance. For more information, see #unique_23.
2. Disable Internet Explorer Enhanced Security Configuration.

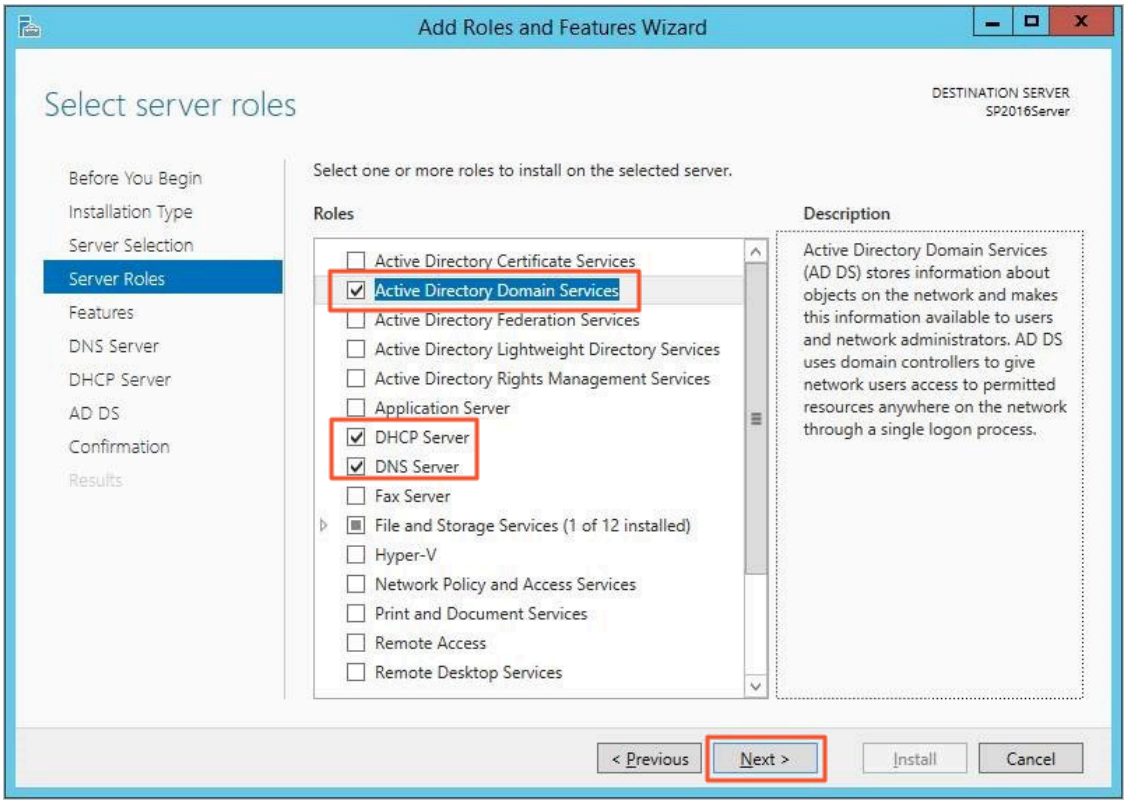


3. Add roles and features of DNS, DHCP, IIS, and .NET Framework3.5.

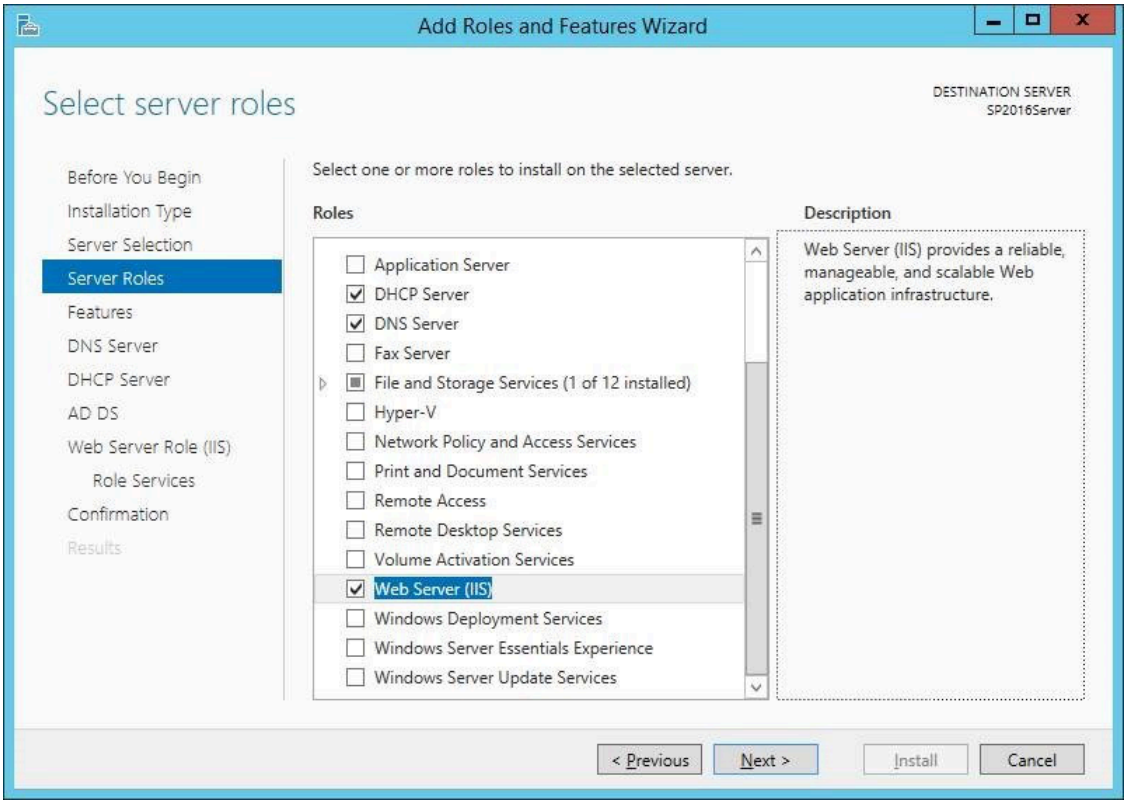
   a) Click Add roles and features.



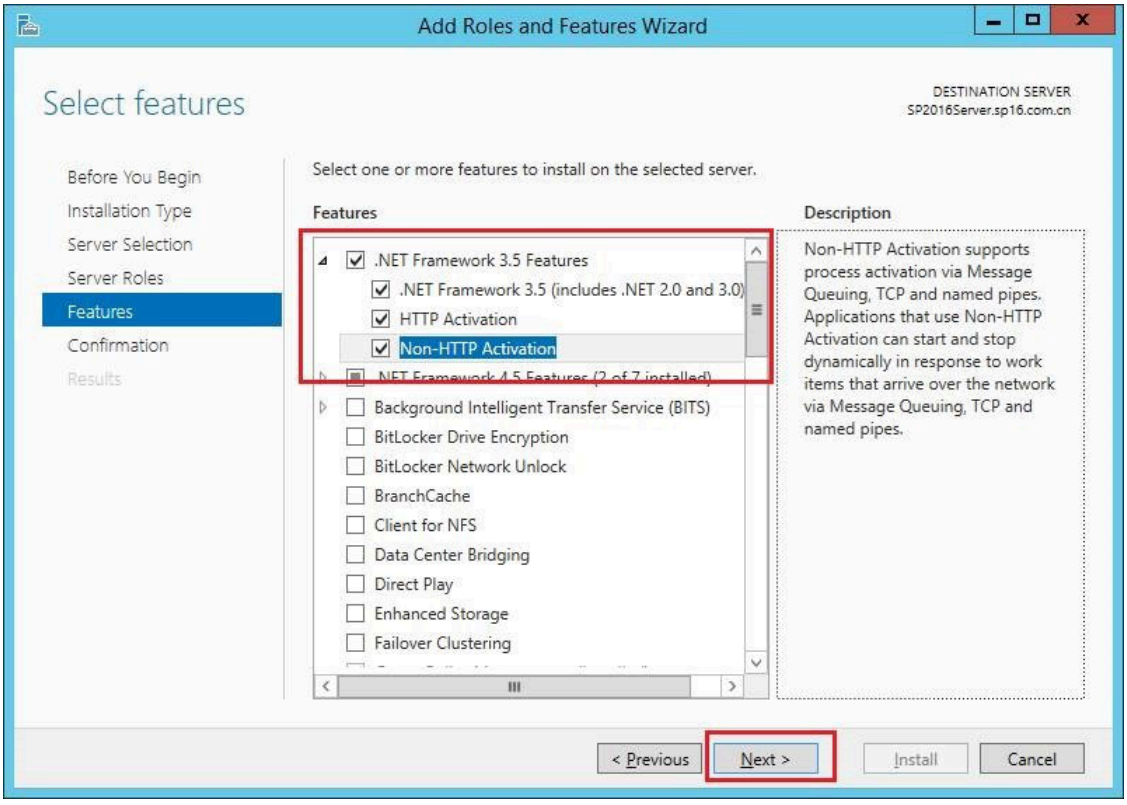
   b) Add the AD, DHCP, and DNS services. Select Active Directory Domain Services, DHCP Server, and DNS Server, and click Next.



   c) Add the IIS service. Select Web Server IIS, and click Next.

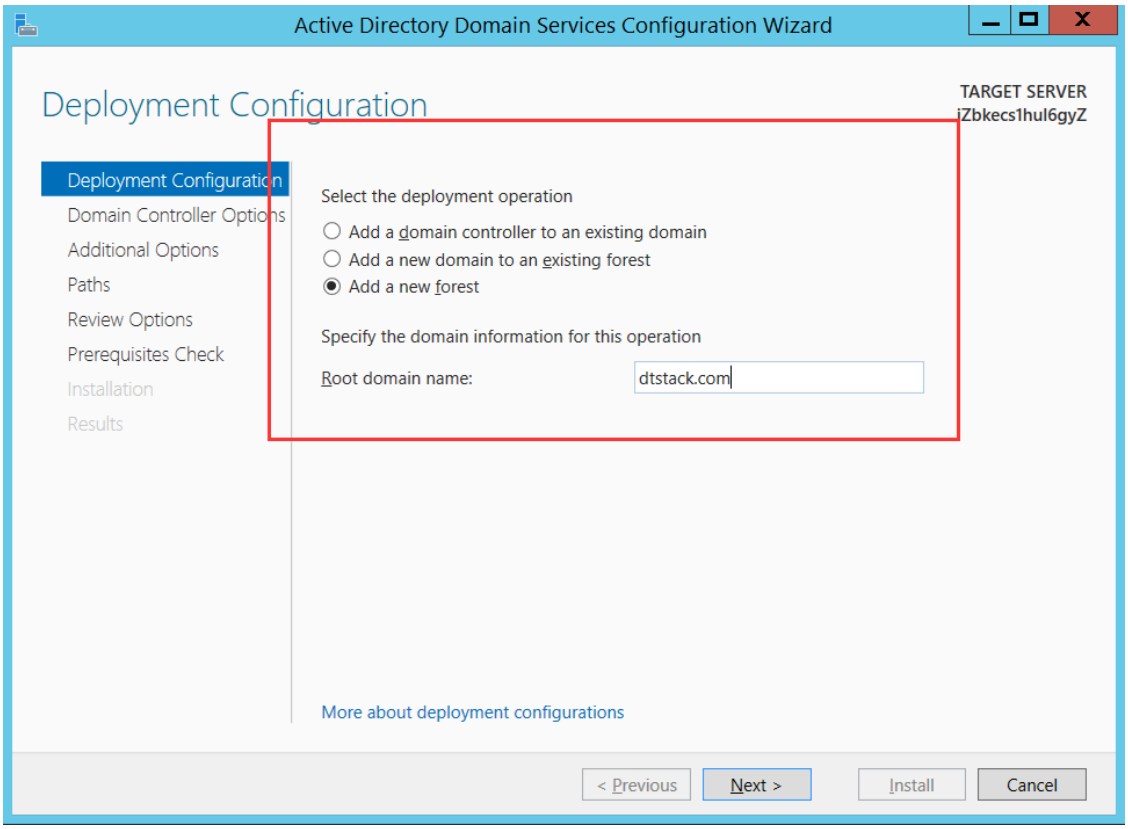


d) In the Features section, select .NET Framework 3.5 Features.

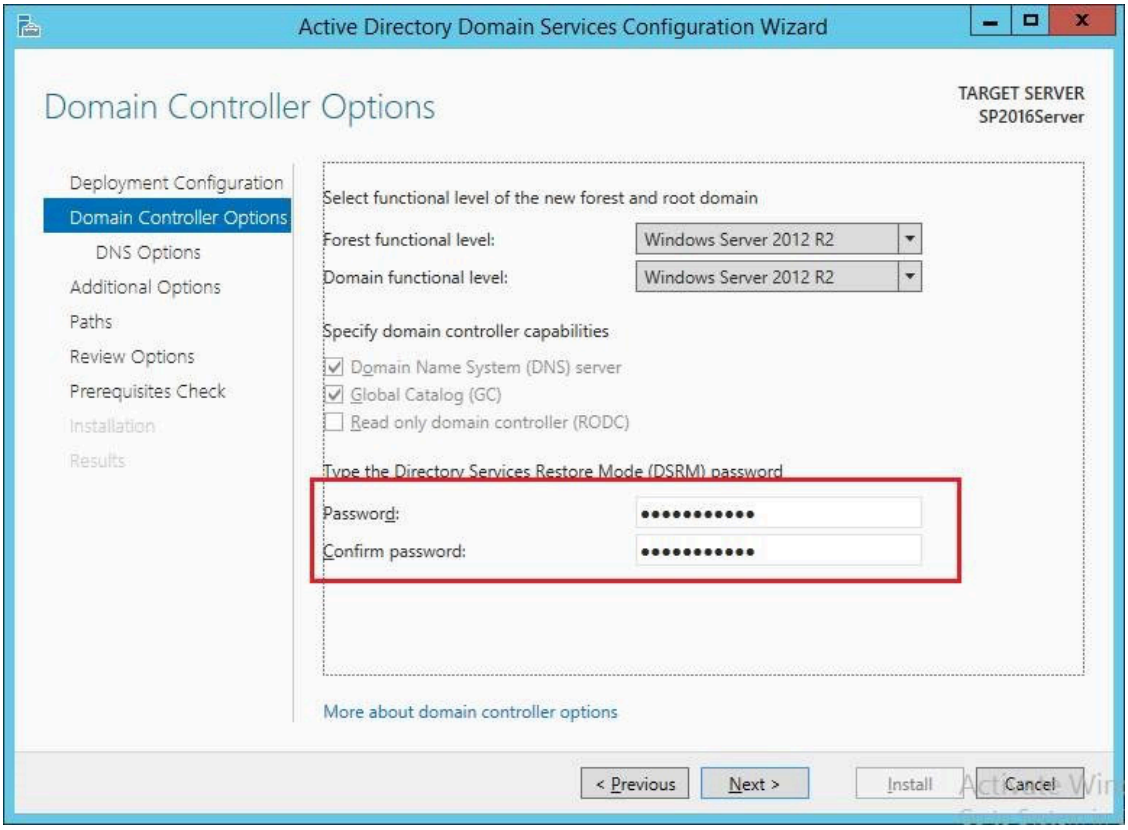


e) Click Next until the end of installation.

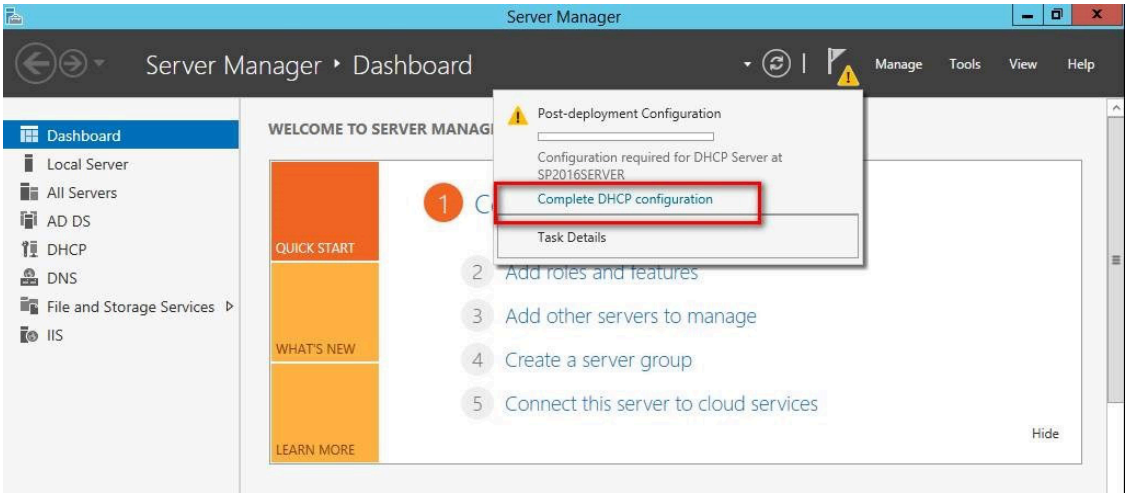
4. Configure the AD service. Click Add a new forest, and enter a domain name in the Root domain name field to create a domain environment.



5. Set the password, and click Next until the end of the configuration.

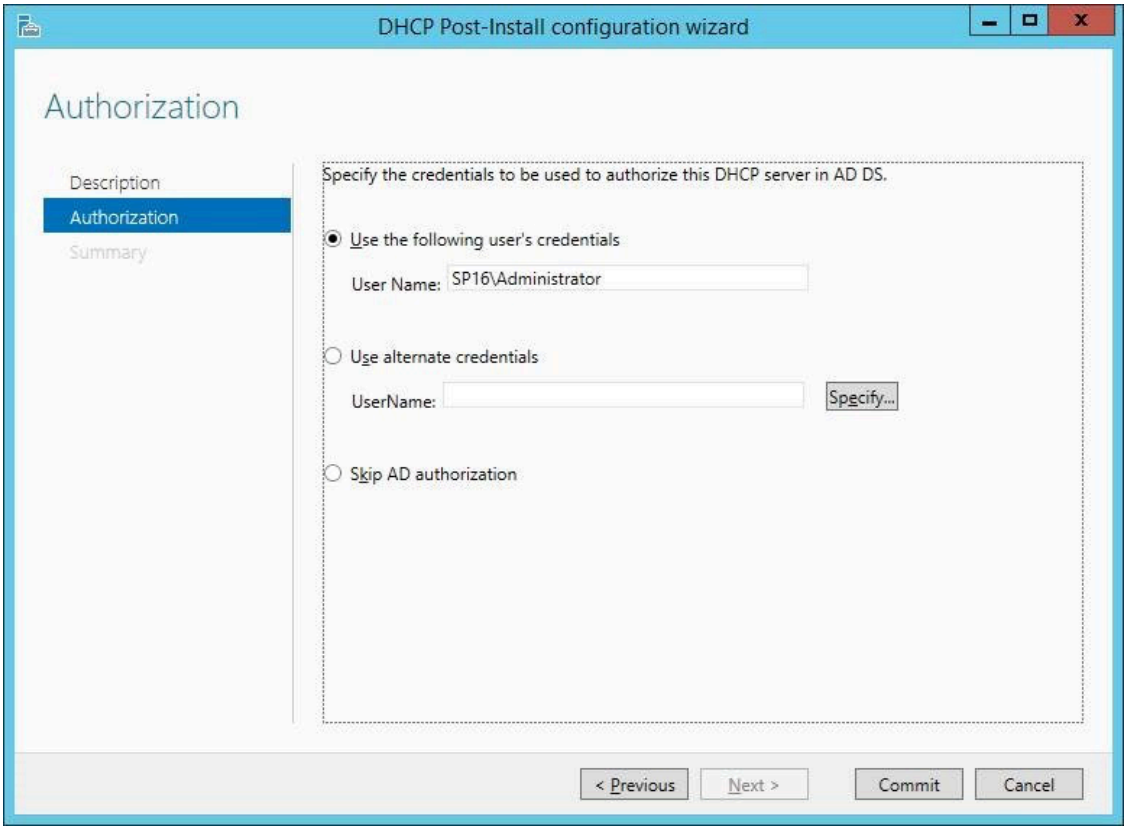


6. Click Complete DHCP configuration to set the DHCP feature.



a) Check the DHCP configuration description, and click Next.

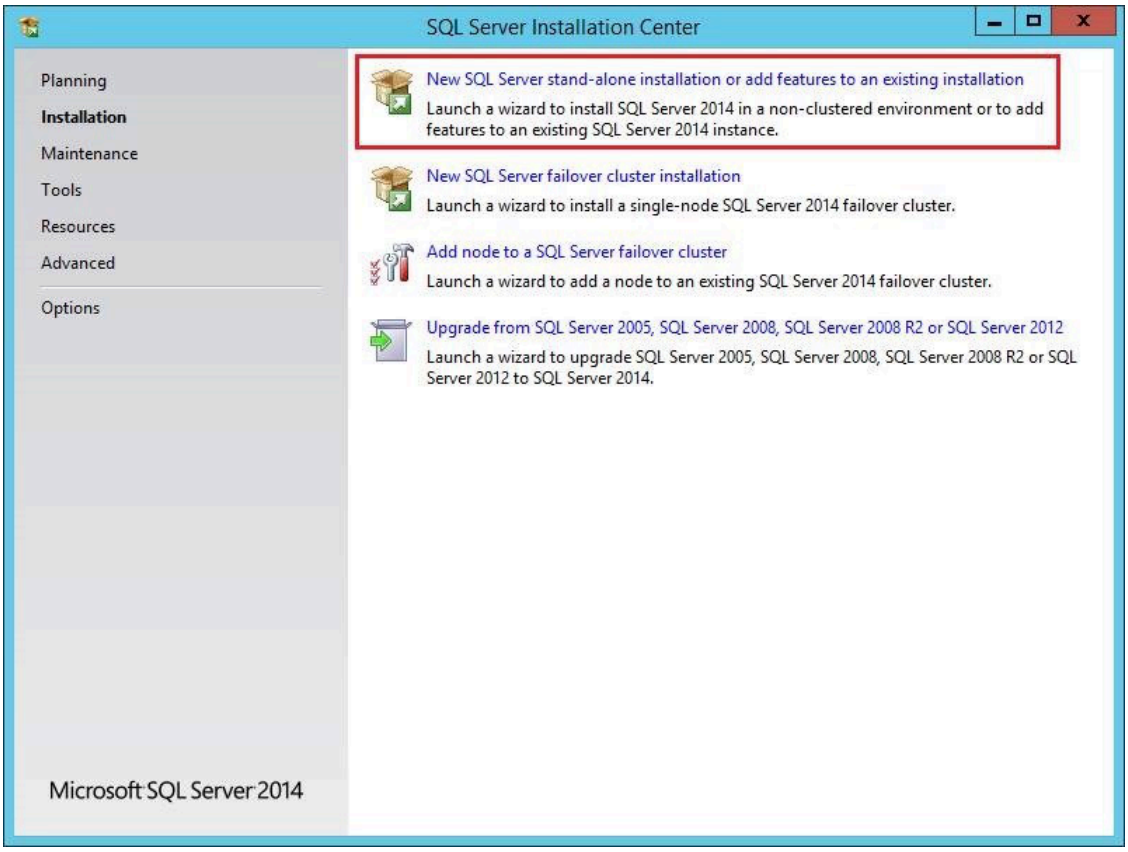
b) Keep the default configuration, and click Commit to complete the installation.



Step 2: Install SQL Server 2014

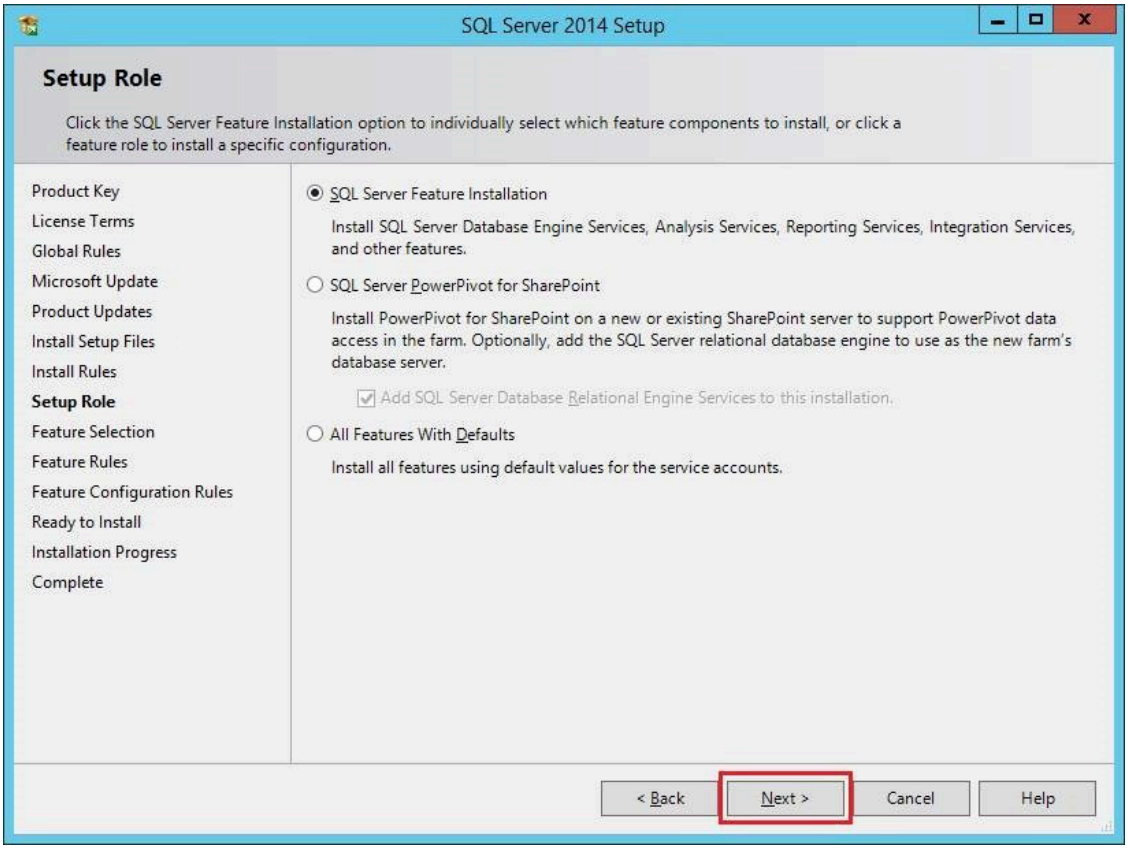
To install the SQL Server 2014 database, follow these steps:

1. Install SQL Server 2014 SP1, go to the SQL Server Installation Center window, and click the first installation option.

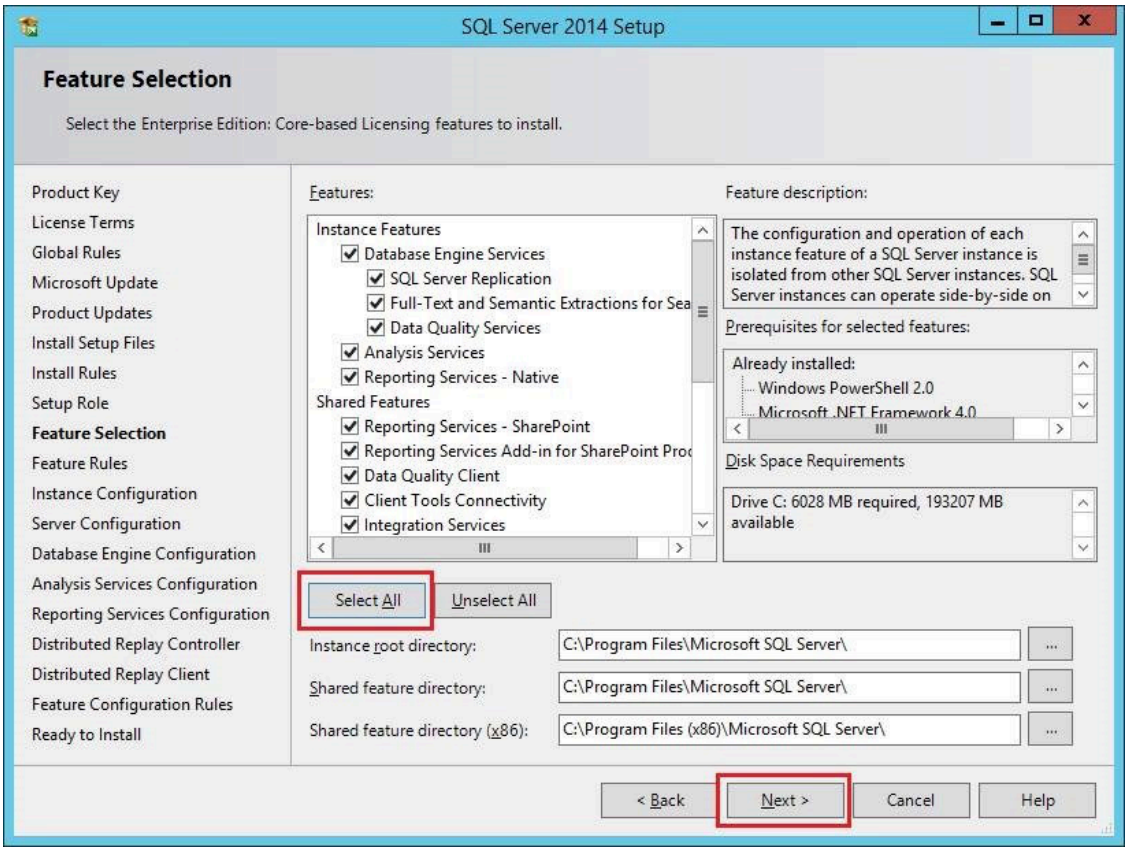


2. Enter the product key, and click Next.
3. Accept the license terms, and click Next.
4. Complete the installation check, and click Next.

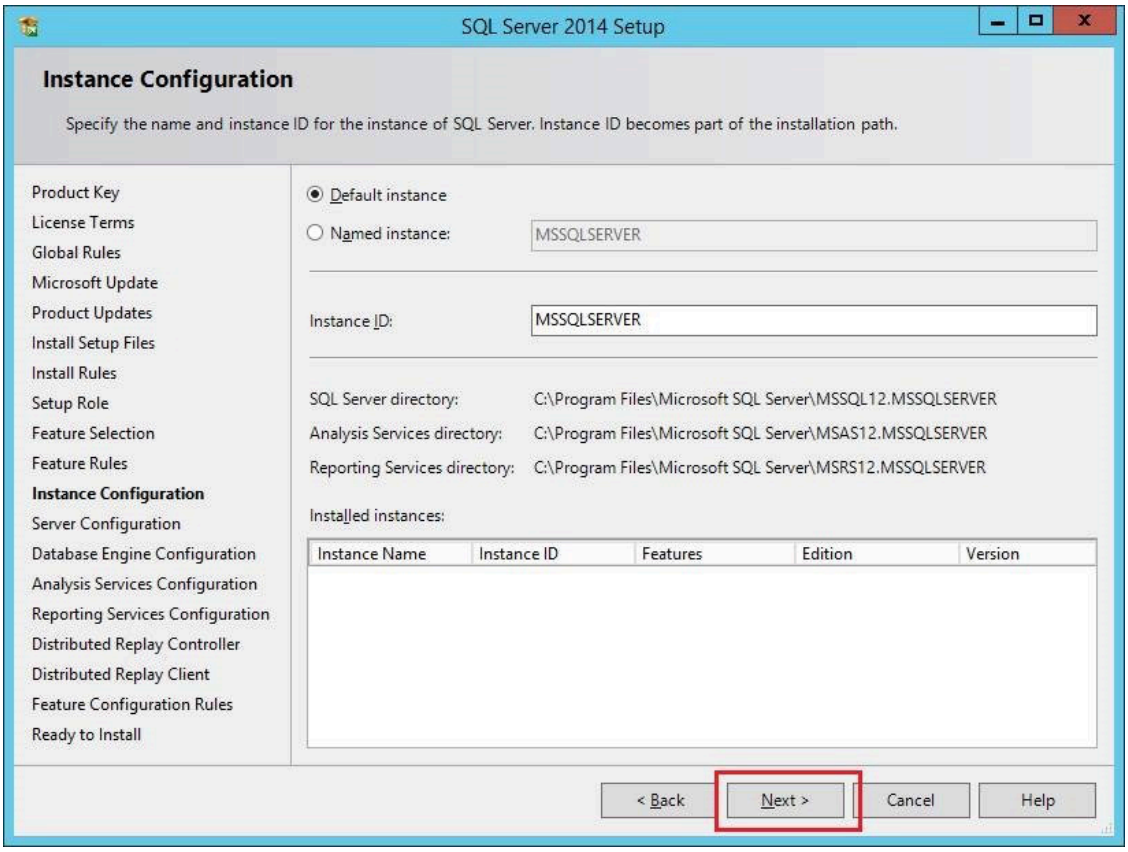
5. Keep the default option, and click Next.



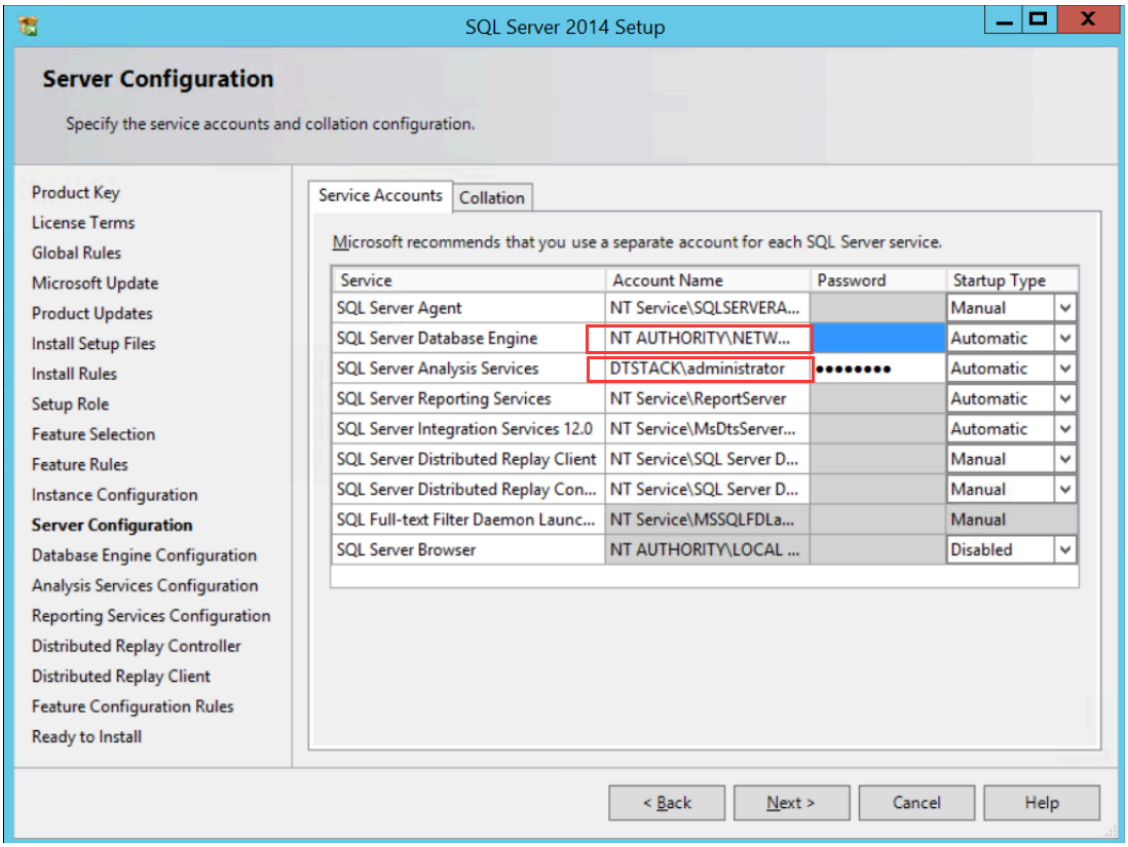
6. Click Select All to select all features, and click Next.



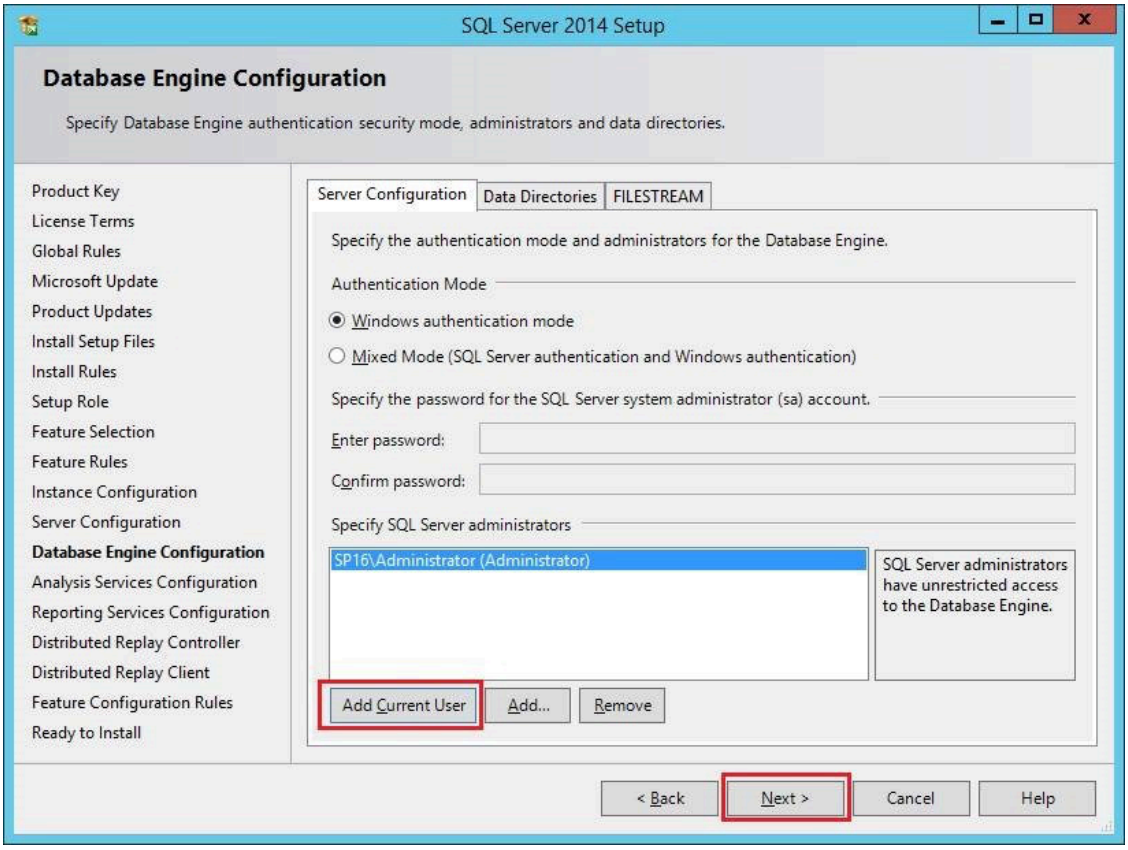
7. **Configure the SQL Server instance: Click Default instance to use the default instance ID.**



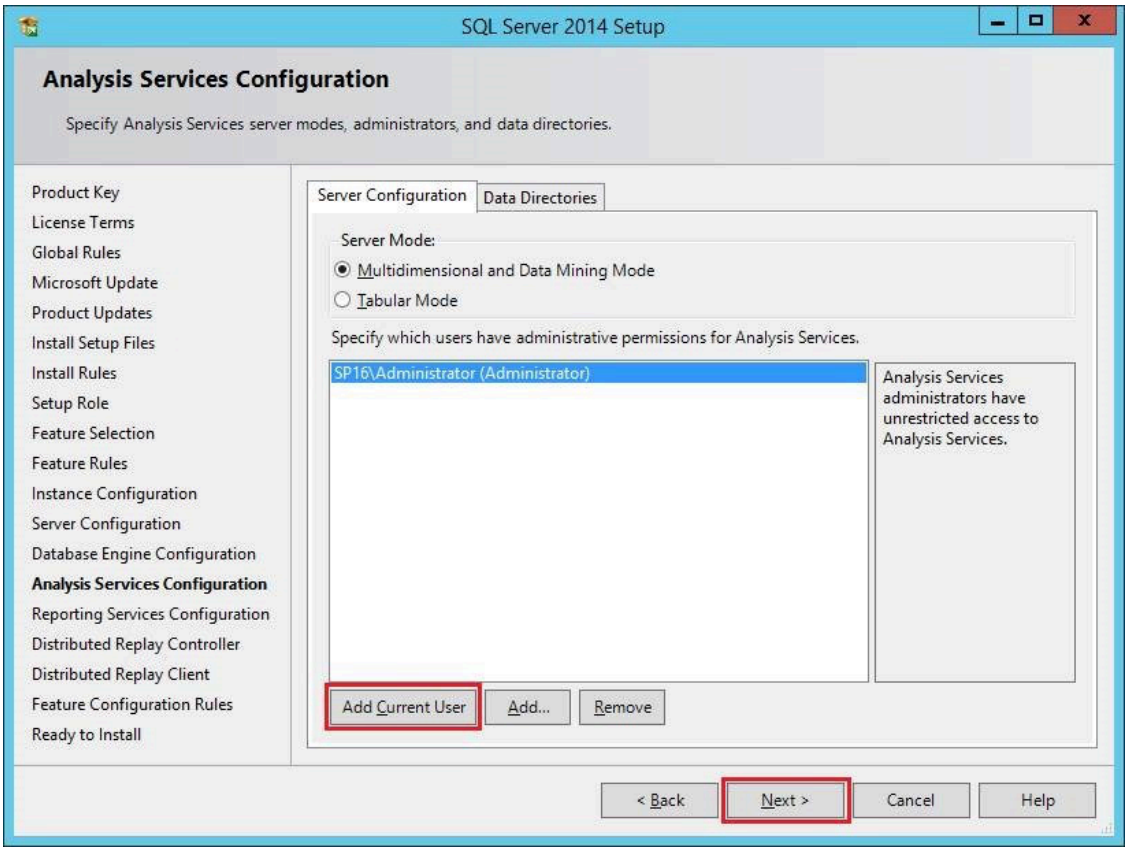
8. Specify the account names and passwords for SQL Server Database Engine and SQL Server Analysis Services.



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.

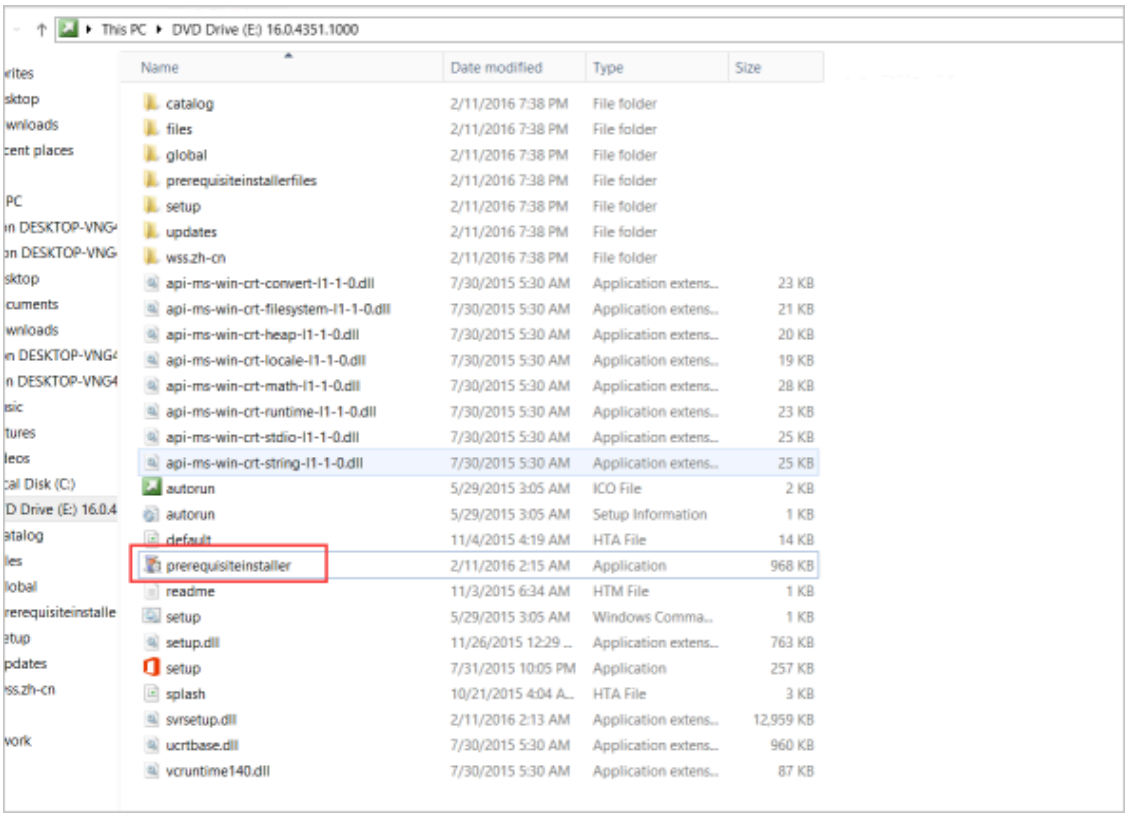


11. Click Next until the end of the installation.

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.

7 Build Docker on a CentOS 7-based ECS instance

This topic describes how to deploy Docker on CentOS.

Prerequisites

You must have an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

Context

The procedure described in this topic is applicable to developers that are familiar with Linux, but new to Alibaba Cloud ECS instances.

Procedure

To build Docker on a CentOS 7-based ECS instance, follow these steps:

1. Deploy Docker
2. Use Docker
3. Create an image

Deploy Docker

You can purchase a required image from Alibaba Cloud Marketplace, and easily deploy Docker. You can also install Docker manually as described in this topic.

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.

To deploy Docker, follow these 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
```

The following response indicates that Docker has been installed.

Use Docker

You can use Docker in these ways:

1. Manage the Docker daemon.

```
# systemctl start docker      # Runs the Docker daemon .
# systemctl stop docker       # Stops the Docker daemon .
```

```
# systemctl restart docker # Restarts 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 from Alibaba Cloud image repository to memorize the image easily.

```
# 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 image ID e1xxxxxxxxxe. Afterward, run the `docker run` command to enter the container corresponding the image ID.

```
# docker run - ti e1xxxxxxxx xe / bin / bash
```

   - Exit the container. Run the `exit` command to exit the container.

- You can combine the `run` command with the `-d` parameter to run the container in the background. The `--name` parameter specifies apache as the container name.

```
# docker run -d --name apache e1xxxxxxxx xe
```

- Enter the container that runs in the background.

```
# docker exec -ti apache /bin/bash
```

- Create an image from the container.

```
# docker commit containerID/containerName newImageName:tag
```

- To easily test and restore an image, you can run the source image, create a new image with a simple name from the source image, and then test the new image.

```
# docker commit 4c8066cd8c01 apachephp:v1
```

- Run the container and map Port 8080 of the host with the container.

```
# docker run -d -p 8080:80 apachephp:v1
```

In a browser, enter the IP address of the host followed by Port 8080 to connect to the container. The following response indicates that the container runs normally.

Create an image

To create an image, follow these steps:

1. **Prepare the following content in a Dockerfile.**

```
#  vim   Dockerfile
 FROM   apachephp : v1   # Declares   a   base   image .
 MAINTAINER   DTSTACK  # Declares   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   only   contain   127   lines   or
 less .  Therefore ,  we   recommend   that   you   write   the
 required   commands   that   you   have   not   written   in   the
   Dockerfile   to   a   script   if   the   Dockerfile   cannot
 contain   these   commands .
 ENTRYPOINT   ping   www . aliyun . com  # The   commands   that
 run   at   startup .  The   last   command   must   be   a   front
 - end   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                      # Checks   whether   the
 image   has   been   created .
 docker   run  - d   webcentos : v1        # Runs   the   container
   in   the   background .
 docker   ps                          # Queries   the   container
 in   operation .
 docker   ps  - a                       # Queries   all   containers
   including   those   in   the   stopped   state .
 docker   logs   CONTAINER   ID / IMAGE    # Checks   the   startup
   log   to   troublesho  ot   the   issue   based   on   the
 container   ID   or   name   if   the   started   container   does
   not   exist   in   the   query   result .
 docker   commit   fb2844b6c0  70   dtstackweb : v1  # The
 container   ID   and   the   name   and   version   of   the   new
   image .  You   must   add   the   informatio  n   to   the   end
   of   the   commit   command .
 docker   images                      # Queries   images   that
 have   been   downloaded   and   created   on   the   premises .
 docker   push                        # Pushes   an   image   to
 the   default   remote   image   repository ,  Docker   Hub .
```

3. **Push the image to the registry.**

   Enter your own `ImageId` **and** `image  version .`

```
 docker   login  -- username = dtstack_pl  us   registry . cn -
 shanghai . aliyuncs . com  # Specifies   the   password   of   the
   image   repository .  You   enter   the   informatio  n   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 ]
```

   The image has been pushed to the registry if you can view the image version in the image repository.

8 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 an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

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_26.
2. #unique_17.
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 pr
eset: enabled)
   Active: active (running) since Tue 2018-11-13 10:40:03 CST; 21s ago
     Docs: man:firewalld(1)
 Main PID: 20785 (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.

```
[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_10.

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 groupinsta ll " Developmen t 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 or the APR source code installation package.

3. Run the following commands to move the APR and APR-until 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  \
-- 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 ]
 Descriptio  n = 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.

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:
   a.
   ```
   wget https://downloads.mysql.com/archives/get/file/mysql-5.6.24.tar.gz
   ```
   b.
   ```
   tar xvf mysql-5.6.24.tar.gz -C /usr/local/src
   ```
   c.
   ```
   cd /usr/local/src/mysql-5.6.24
   ```
   d.
   ```
   cmake . -DCMAKE_INSTALL_PREFIX=/usr/local/mysql \
   -DMYSQL_DATADIR=/mnt/data \
   -DSYSCONFDIR=/etc \
   -DWITH_INNOBASE_STORAGE_ENGINE=1 \
   -DWITH_ARCHIVE_STORAGE_ENGINE=1 \
   -DWITH_BLACKHOLE_STORAGE_ENGINE=1 \
   -DWITH_READLINE=1 \
   -DWITH_SSL=system \
   -DWITH_ZLIB=system \
   -DWITH_LIBWRAP=0 \
   -DMYSQL_TCP_PORT=3306 \
   -DDEFAULT_CHARSET=utf8 \
   -DMYSQL_UNIX_ADDR=/usr/local/mysql/mysql.sock \
   -DDEFAULT_COLLATION=utf8_general_ci \
   -DWITH_SYSTEMD=1 \
   ```

```
- DINSTALL_S  YSTEMD_UNI  TDIR =/ 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_inst  all_db  -- user =
mysql  -- datadir =/ mnt / data /
```

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

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

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

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

8. Modify the MySQL configuration file.

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

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

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

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

[ Service ]
User = mysql
Group = mysql
Permission  sStartOnly = 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
    ```

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

    Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

    Oracle is a registered trademark of Oracle Corporation and/or its
    affiliates. Other names may be trademarks of their respective
    owners.

    Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
    ```

13. Run the `\ q` command to log 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
```

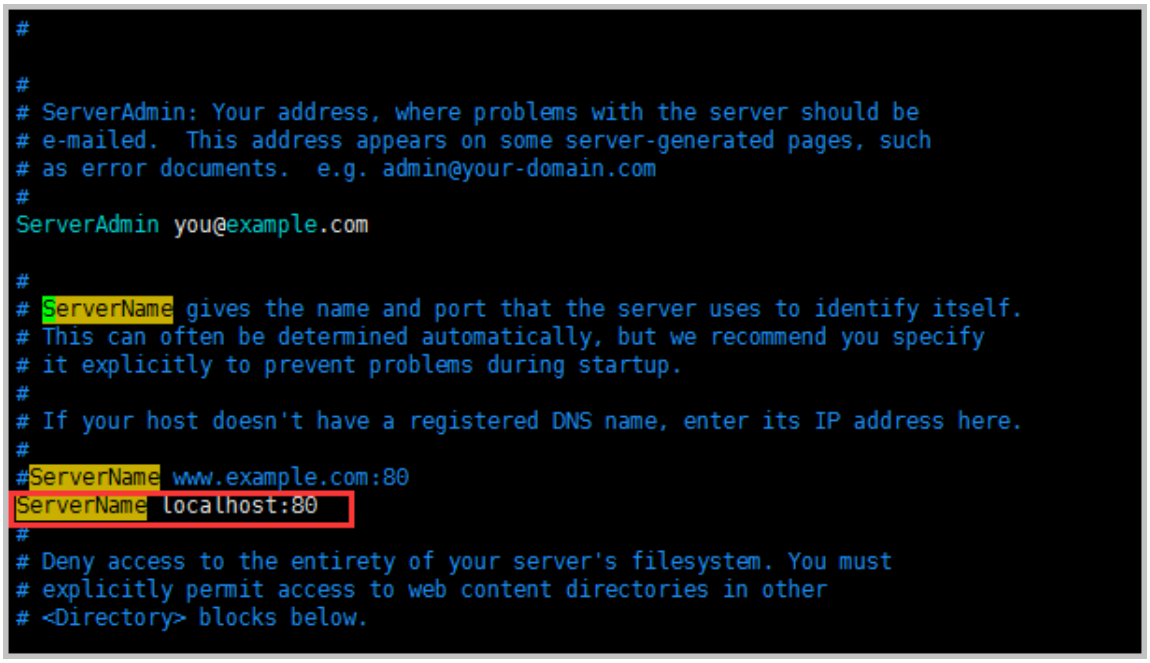
Note:
If the ECS instance does not have sufficient memory space, terminate PHP extensions that you do not need when you configure PHP to save memory space. For example, you can add `--disable-fileinfo` to the `./configure` command to terminate the fileinfo extension.

3. Run the following command to copy the PHP configuration file:

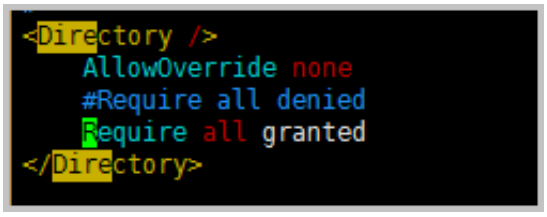
```
cp  php.ini-production  /etc/php.ini
```

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.

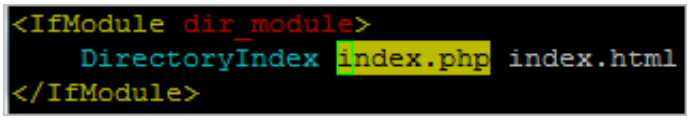
   a) Find the `ServerName` parameter and add `ServerName localhost:80` to the parameter.



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



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



   d) Find the following content:

```
# If the AddEncoding directives above are commented-out, then you
# probably should define those extensions to indicate media types:
#
AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz
```

Add the following content:

```
AddType   applicatio  n / x - httpd - php  . php
AddType   applicatio  n / 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 ();
```

```
? >
```

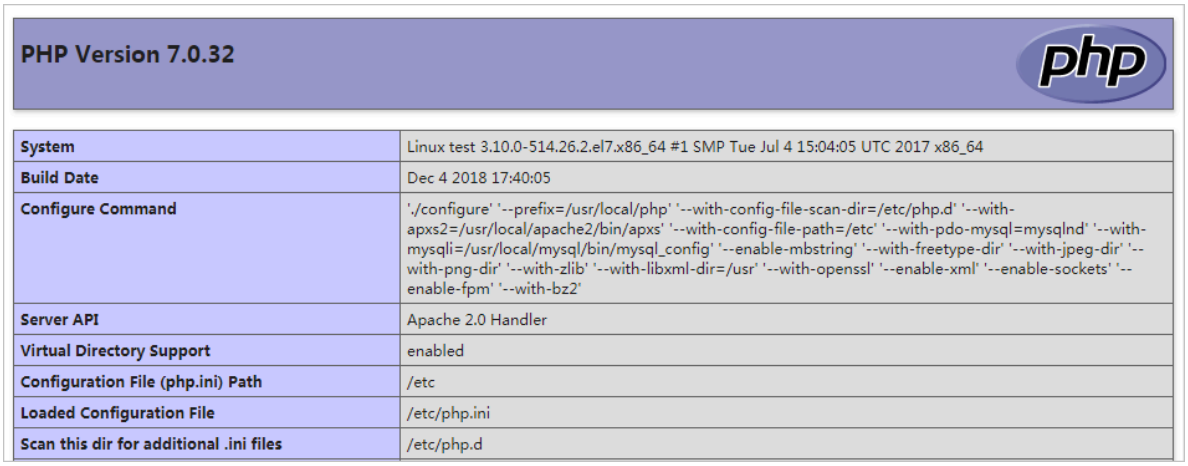
c) Press `Esc` to exit the edit mode. Enter `:wq` to save and close the *index.php* file.

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.



PHP Version 7.0.32

System	Linux test 3.10.0-514.26.2.el7.x86_64 #1 SMP Tue Jul 4 15:04:05 UTC 2017 x86_64
Build Date	Dec 4 2018 17:40:05
Configure Command	'./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'
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d

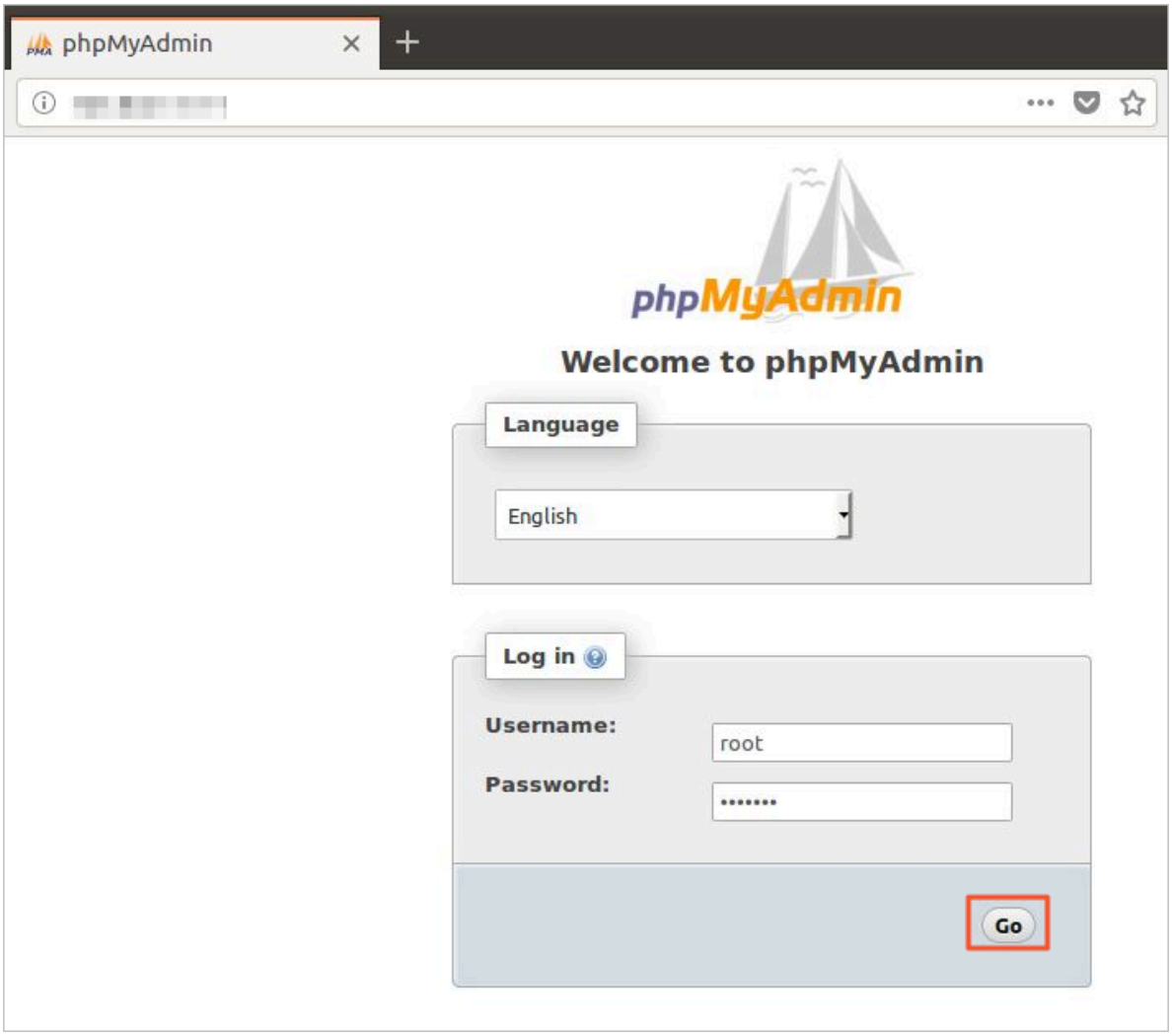
Step 5. Install phpMyAdmin

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.


phpMyAdmin
Welcome to phpMyAdmin
Language
English
Log in
Username:
root
Password:
••••••

5. Enter the MySQL username and password, and click Go.



9 Install SharePoint 2016

This topic describes how to install SharePoint 2016.

Prerequisites

You must have an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

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.

3. Install SharePoint 2016.

   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.

10 Build a primary/secondary PostgreSQL system based on ECS

PostgreSQL is regarded as the most advanced open source database. ApsaraDB RDS for PostgreSQL is compatible with NoSQL databases, supports efficient queries and plug-in management, and provides secure and stable services. This topic describes how to build a primary/secondary PostgreSQL system based on ECS.

Prerequisites

- You must have an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.
- You have added an inbound rule to the security group of the ECS instance to support Port 5432. For more information, see #unique_20.

Context

The procedure described in this topic is applicable to Alibaba Cloud users that are familiar with Alibaba Cloud ECS instances, the Linux operating system, 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 install PostgreSQL on an ECS instance in either of the following ways:

- Image deployment: Go to the Alibaba Cloud Marketplace page, and search for the required PostgreSQL image for installation.
- Manual deployment: Install PostgreSQL by using source code or Yellowdog Update , Modified (YUM).

Procedure

To install PostgreSQL by using YUM and build the primary/secondary architecture of PostgreSQL, follow these steps:

1. Step 1: Activate 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: Activate two ECS instances

To build the primary/secondary architecture of PostgreSQL, you must activate two ECS instances that run in a Virtual Private Cloud (VPC). One ECS instance works as a primary node and the other ECS instance works as a secondary node. For more information, see #unique_23.

> **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 in the follow-up management. For more information, see Create an EIP.

Step 2: Configure the primary node of PostgreSQL

To configure the primary node of PostgreSQL, follow these 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 that is used for replication between the primary and secondary nodes. Afterward, specify the password, logon permission, and backup permission.

   a) Run the following command to log on to PostgreSQL.

   ```
   su - postgres
   ```

   b) Type `psql` in the following command to enter 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 replicatio n 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
   ```

```
( 2   rows )
```

f) Type `\ q` in the command, and press the `Enter` key to exit the PostgreSQL interactive terminal.

```
 postgres =# \ q
```

g) Type `exit` in the command, and press the `Enter` key to exit PostgreSQL.

```
- bash - 4 . 2 $  exit
 logout
```

4. Run the following command to open the file *pg_hba . conf* , and set a whitelist for replica.

```
vim  / var / lib / pgsql / 9 . 5 / data / pg_hba . conf
```

Add the following lines to the `IPv4  local  connection  s` field.

```
host   all   all   192 . 168 . 1 . 0 / 24   md5              #
Enables   MD5   password   encryption   for   connection  s   in
the   CIDR   block   of   the   VPC .
host   replicatio  n   replica   192 . 168 . 1 . 0 / 24   md5   #
Enables   data   synchroniz  ation   from   the   replicatio  n
database .
```

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

```
vim  / var / lib / pgsql / 9 . 5 / data / postgresql . conf
```

Set the following parameters:

```
wal_level  =  hot_standb  y   # Enables   the   hot   standby
mode .
synchronou  s_commit  =  on   # Enables   synchroniz  ation .
max_wal_se  nders  =  32      # The   maximum   number   of
synchroniz  ation   processes .
wal_sender  _timeout  =  60s  # The   timeout   value   for   the
streaming   replicatio  n   instance   to   synchroniz  e   data .
max_connec  tions  =  100     # The   maximum   number   of
connection  s .  The   value   of   max_connec  tions   for   the
  secondary   node   must   be   larger   than   that   for   the
primary   node .
```

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

```
systemctl   restart   postgresql - 9 . 5 . service
```

Step 3: Configure the secondary node of PostgreSQL

To configure the secondary node of PostgreSQL, follow these 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 larger 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_standb  y_feedback  =  on          #  Enables   the
secondary   node   to   report   errors   during   replicatio  n .
```

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

```
chown  - R   postgres . postgres  / var / lib / pgsql / 9 . 5 /
data
```

6. Run the following commands in sequence to start the PostgreSQL service and enable PostgreSQL to run at startup.

   a.
   ```
   systemctl   start   postgresql - 9 . 5 . service    # Starts
   the   PostgreSQL   service .
   ```

   b.
   ```
   systemctl   enable   postgresql - 9 . 5 . service   # Enables
   PostgreSQL   to   run   at   startup .
   ```

Step 4: Test the primary/secondary architecture of PostgreSQL

To test the primary/secondary architecture of PostgreSQL, follow these steps:

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

```
ps   aux  | grep   sender
```

The following response indicates that the sender process is available.

```
postgres    2916    0 . 0    0 . 3   340388    3220  ?         Ss
    15 : 38     0 : 00   postgres :  wal   sender       process
replica   192 . 168 . 1 . 222 ( 49640 )  streaming   0 / F01C1A8
```

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

```
ps   aux  | grep   receiver
```

The following response indicates that the receiver process is available.

```
postgres   23284    0 . 0    0 . 3   387100    3444  ?         Ss
    16 : 04     0 : 00   postgres :  wal   receiver   process
streaming   0 / F01C1A8
```

3. On the primary node, run the following SQL statement to check the status of the secondary node.

```
replicatio  n =#  select  *  from   pg_stat_re  plication ;
```

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

```
pid  |  usesysid  |  usename  |  applicatio  n_name  |  client_add
r  |  client_hos  tname  |  client_por  t  |  backend_st  art  |
backend_xm  in  |  state  |  sent_locat  ion  |  write_loca  ti
on  |  flush_loca  tion  |  replay_loc  ation  |  sync_prior  ity
|  sync_state
```

```
------+----------+---------+------------------+--------------
+-----------------+------------ +------------------------------
+--------------+-----------+---------------+-------------
---+----------------+-----------------+--------------+------------
 2916  |  16393  |  replica  |  walreceive  r  |  192 . 168 . 1 .
 222  | |  49640  |  2017 - 05 - 02   15 : 38 : 06 . 188988 + 08  |
 1836  |  streaming  |  0 / F01C0C8  |  0 / F01C0C8
|  0 / F01C0C8  |  0 / F01C0C8  |  0  |  async
( 1   rows )
```

11 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 an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

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_30.

Create a Linux-based ECS instance. For more information, see #unique_23.

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_31.
- 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 correspond ing mobile phone in the normal running status.

Step 2: Deploy the Web environment

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

The software package provides NGINX 1.10.2.

 Note:

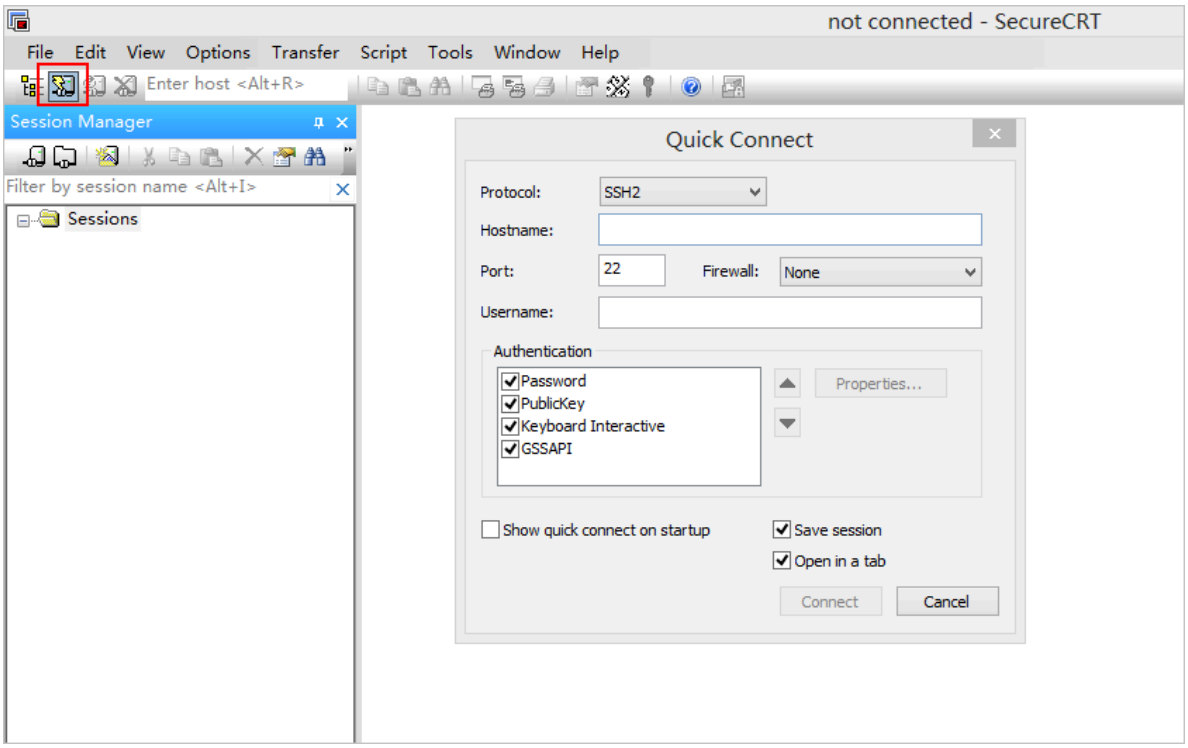
This version is used in the following example. The version that you download may be different in your actual running environment.

Prerequisites:

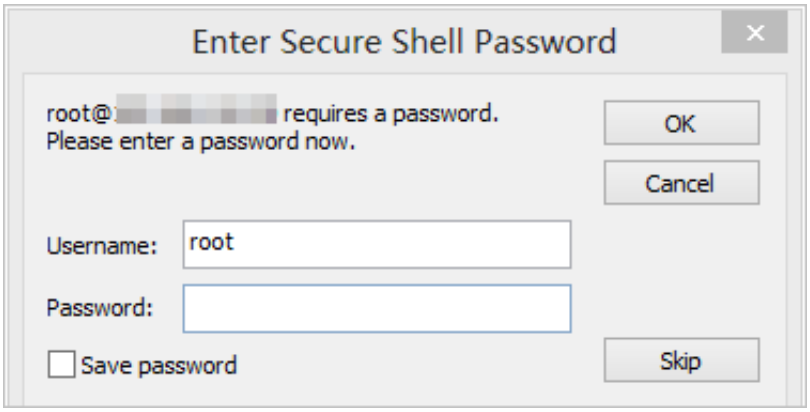
- **Your instance can connect to the Internet.**
- **You have installed a tool for connecting to the Linux-based ECS instance. SecureCRT is used as the tool in this section.**

To deploy the Web environment, follow these steps:

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



2. Enter the root username and the password.



3. Add the NGINX repository.

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

4. Install NGINX.

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

5. Enable NGINX to run at startup.

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

6. Start NGINX and check the NGINX service status.

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

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

Then, the NGINX environment is ready to run.

Step 3: Install Ghost

To install Ghost, follow these steps:

1. Run the following command to update system software to the latest versions.

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

2. Install Node.js.

   a) Install Extra Packages for Enterprise Linux (EPEL).

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

   b) Install Node.js and npm.

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

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

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

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

3. Install Ghost.

   a) Create the Ghost installation directory.

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

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

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

   c) Decompress the Ghost package.

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

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

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.

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
```

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

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

        server: {
            host: '127.0.0.1',
            port: '2368'
        }
    },
```

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

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

i) Start, stop, and then restart Ghost.

```
[ root @ localhost   ghost ]#  pm2   start   ghost
[ root @ localhost   ghost ]#  pm2   stop   ghost
```

```
[ root @ localhost   ghost ]#  pm2   restart   ghost
```

4. Install NGINX.

   a) Add the NGINX repository.

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

   b) Install NGINX.

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

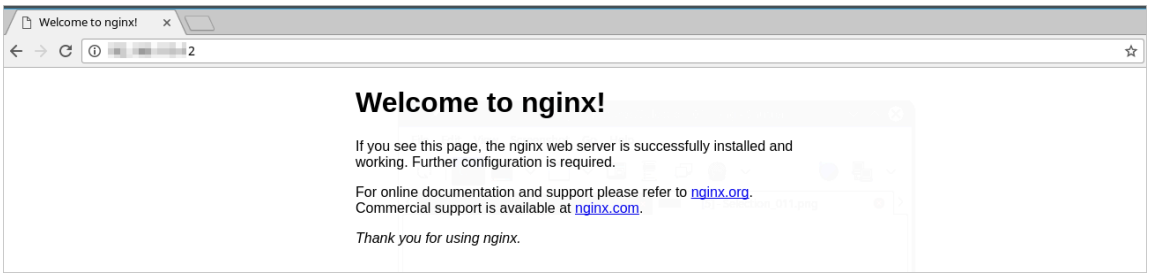
   c) Enable NGINX to run at startup.

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

   d) Start NGINX and check the NGINX service status.

```
[ 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_nam e to the domain that is used in your actual running environment.

```
upstream ghost {
    server 127.0.0.1:2368;
}

server {
    listen      80;
    server_name myghostblog.com;

    access_log  /var/log/nginx/ghost.access.log;
    error_log   /var/log/nginx/ghost.error.log;

    proxy_buffers 16 64k;
    proxy_buffer_size 128k;

location / {
        proxy_pass  http://ghost;
        proxy_next_upstream error timeout invalid_header http_500 http_502 http_503 http_504;
        proxy_redirect off;

        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 https;
    }

}
```

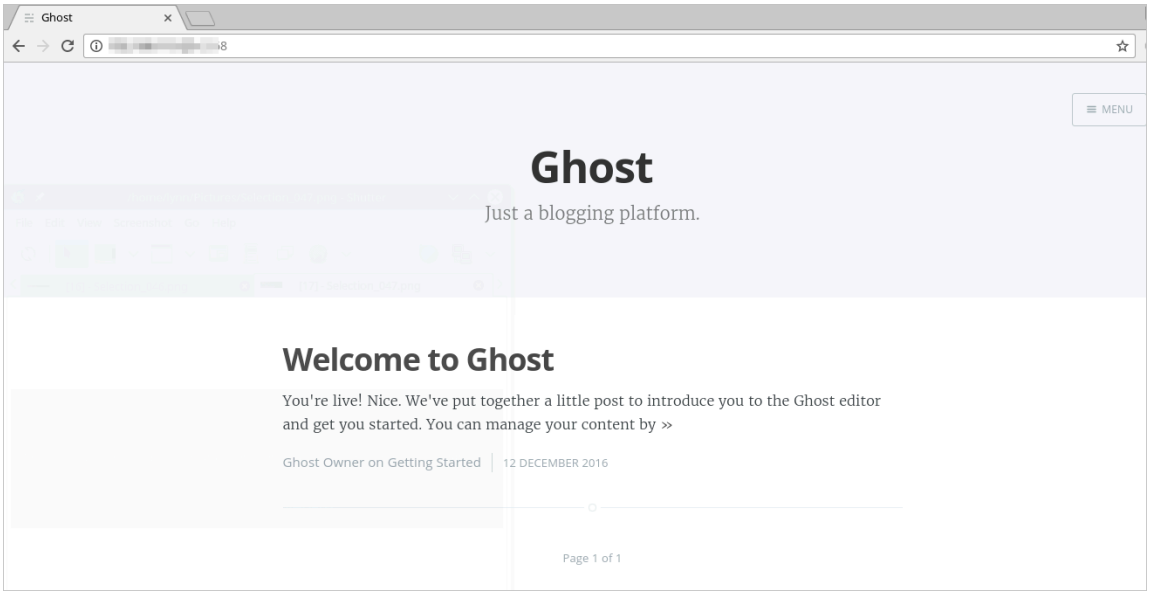
   c) Change the name of the default configuration file *default . conf* to *default . conf . bak* , so NGINX is only applicable to *ghost . conf* .

```
[ root @ localhost  ~]# mv   default . conf   default . conf . bak
```

   d) Restart the NGINX service.

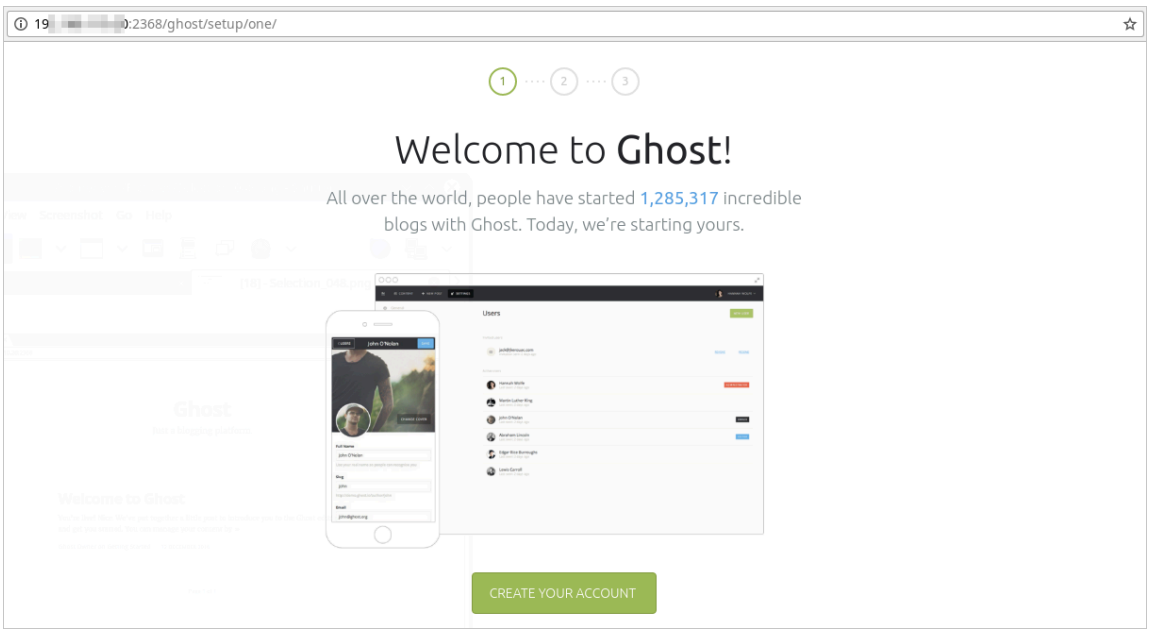
```
[ root @ localhost   conf . d ]#  systemctl   restart   nginx .
 service
```

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



Note:
If the system returns Error Code 502, check whether you have disabled the firewall.

b) To edit your Ghost blogging platform, open your browser, and in the address bar, enter the URL *http :// IP address of the ECS instance / ghost .*



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 .

> Note:
> The IPC filing account is used only for ICP filing and different from an Alibaba Cloud account.

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.

12 Build a Drupal-based website on CentOS 7

This topic describes how to build a Drupal-based website on an ECS instance that runs CentOS 7.

Prerequisites

You must have an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

Context

Drupal is a free and open source content management framework (CMF) written in Hypertext Preprocessor (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, and to support website projects in different 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 with ECS instances.

Procedure

To build a Drupal-based website on an ECS instance, follow these steps:

1. Activate an ECS instance
2. Build the Web environment
3. Install Drupal

Step 1: Activate an ECS instance

You can activate an ECS instance to build a personal website. In the follow-up management, you can upgrade the instance or optimize the architecture as needed.

Step 2: Build the Web environment

You can build the Web environment on the ECS instance in any of the following ways:

- Image deployment
- Easy deployment with an installation package

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

We recommend that you use an image. This is an easy way to build the Web environment for the first time. 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 the Drupal website by using an image.

1. When you create an ECS instance, in the Image section, choose Marketplace Image > Select from image market including operating system. For more information, see Create an ECS instance.
2. Type LAMP in the search bar, click Search, and then select the first matched image in this example.
3. Click Continue.

   You can also go to Alibaba Cloud Marketplace, and search for and purchase the required images.

   In this topic, the software versions used in the environment include: `CentOS 7.2 | Apache 2.4.25 | MySQL 5.7.17 | PHP 7.1.1 | Drupal8.1.1`.

   > **Note:**
   > The versions that you download may be different in your actual running environment.

Step 3: Install Drupal

To install Drupal, follow these steps:

1. Download the Drupal installation package.

```
# wget http://ftp.drupal.org/files/projects/drupal-8.1.1.zip
```

2. Decompress the package to your website root directory.

```
# unzip drupal-8.1.1.zip
# mv drupal-8.1.1/* /var/www/html/
```

3. Download the Chinese translation package.

```
# cd /var/www/html/
```

```
# wget -P profiles/standard/translations http://ftp.drupal.org/files/translations/8.x/drupal/drupal-8.26.zh-hans.po
```

4. Specify the owner and group of the *sites* directory.

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

5. Restart the Apache service.

```
# /etc/init.d/httpd restart
```

6. Open your browser, and in the address bar, enter the URL "Public IP address of the 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.
7. Select Standard, and click Save and continue.
8. Enter database information, and click Save and continue.

> Note:
> After you log on to the MySQL database, you can run the following commands to customize the database information:
>
> - DBNAME: database name
> - UAERNAME: username
> - IP: localhost or 127.0.0.1 for a local host
> - YOURPASSWORD: database password

```
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;
```

9. At the end of automatic installation, go to the website settings page, enter site information, and then click Save and continue.

What's next

Afterward, you can customize your website pages.

13 Deploy and use SVN

13.1 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 modificati ons.
- 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 svnserve. You can deploy the access to SVN in these ways:

- #unique_35
- #unique_36

After you deploy SVN, you can commit modifications, obtain updates, and reverse files by using SVN. For more information, see #unique_37.

13.2 Deploy access to SVN by using svnserve

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

Prerequisites

You must have an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

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 svnserve, 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_23.

- 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
     ```

     ```
     [root@iZb      Z conf]# svnserve --version
     svnserve, version 1.7.14 (r1542130)
       compiled Nov 20 2015, 19:25:09

     Copyright (C) 2013 The Apache Software Foundation.
     This software consists of contributions made by many people; see the NOTICE
     file for more information.
     Subversion is open source software, see http://subversion.apache.org/

     The following repository back-end (FS) modules are available:

     * fs_base : Module for working with a Berkeley DB repository.
     * fs_fs : Module for working with a plain file (FSFS) repository.

     Cyrus SASL authentication is available.
     ```

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
# ls
```

```
[root@iZ[redacted]beZ svnrepos]# ls
conf  db  format  hooks  locks  README.txt
```

The SVN directories are described as follows:

Directory	Description
db	Stores all version control data files.
hooks	Stores hook scripts.
locks	The client used to track access to the SVN repository.
format	A text file that contains only one integer, indicating the version number of the current SVN repository.
conf	The configuration file of the SVN repository, including the username and permissions for accessing the repository.

4. Set the username and password of the SVN repository.

a) Run the `cd conf/` command.

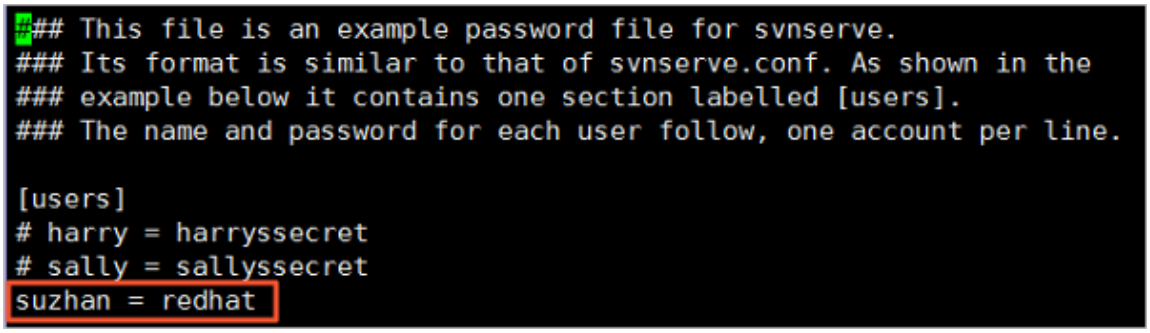
b) Run the `vi passwd` command to open the configuration file.

c) Press the `i` key to enter the edit mode.

d) Move the pointer 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.

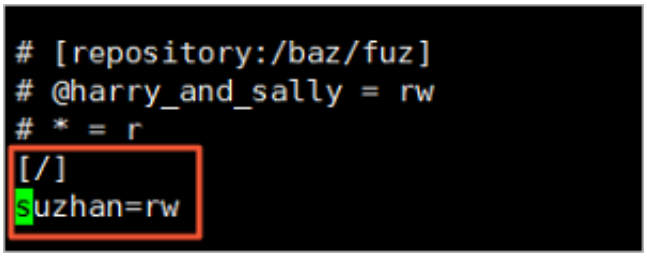
a) Run the `vi authz` command to open the permission control file.

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 permission s 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 authorizat ion rules for path-based access
control.
realm = /var/svn/svnrepos # Specifies the authorizat
ion realm of the repository.
```

Note:

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

```
anon-access = none
auth-access = write
### The password-db option controls the location of the password
### database file.  Unless you specify a path starting with a /,
### the file's location is relative to the directory containing
### this configuration file.
### If SASL is enabled (see below), this file will NOT be used.
### Uncomment the line below to use the default password file.
password-db = passwd
### The authz-db option controls the location of the authorization
### rules for path-based access control.  Unless you specify a path
### starting with a /, the file's location is relative to the the
### directory containing this file.  If you don't specify an
### authz-db, no path-based access control is done.
### Uncomment the line below to use the default authorization file.
authz-db = authz
### This option specifies the authentication realm of the repository.
### If two repositories have the same authentication realm, they should
### have the same password database, and vice versa.  The default realm
### is repository's uuid.
realm = /var/svn/svnrepos
### The force-username-case option causes svnserve to case-normalize
### usernames before comparing them against the authorization rules in the
### authz-db file configured above.  Valid values are "upper" (to upper-
### case the usernames), "lower" (to lowercase the usernames), and
### "none" (to compare usernames as-is without case conversion, which
### is the default behavior).
# force-username-case = none
```

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.

```
[root@ ~]# ps -ef|grep svn
root     19438     1  0 10:17 ?        00:00:00 svnserve -d -r /var/svn/
root     19440 19354  0 10:17 pts/0    00:00:00 grep --color=auto svn
```

Note:

Run the command `killall svnserve` to stop the SVN service.

Step 3: Configure the security group rules

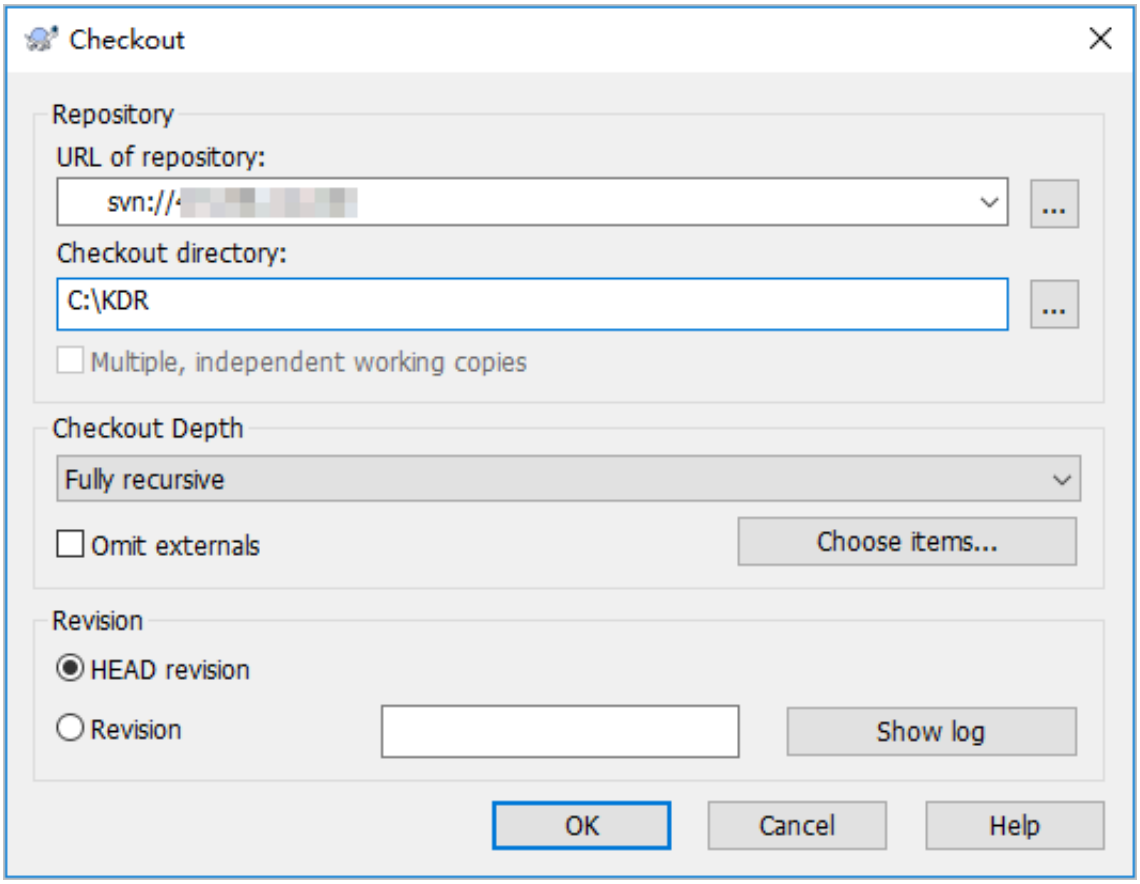
The SVN server listens on TCP Port 3690 by default. You must log on to the ECS console to add TCP Port 3690 to the security group. For more information, see #unique_10.

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` .



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

13.3 Deploy access to SVN over HTTP

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

Prerequisites

You must have an Alibaba Cloud account before you follow the instructions provided in the tutorial. To create an Alibaba Cloud account, click Create an Alibaba Cloud account.

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.

```
yum   install   subversion
```

3. Run the following command to check the SVN version.

```
svnserve  -- version
```

Step 2: Install Apache

To install Apache, follow these steps:

1. Run the following command to install the Hypertext Transfer Protocol daemon (HTTPd).

```
yum install httpd
```

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

```
httpd -version
```

Step 3: Install mod_dav_svn

Run the following command to install mod_dav_svn.

```
yum install mod_dav_svn
```

Step 4: Configure SVN

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 command to create an SVN repository.

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

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

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

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

```
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.

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

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

```
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:

```
< Location / svn >
 DAV svn
 SVNParentP ath / var / svn
 AuthType Basic
 AuthName " Authorizat ion SVN "
 AuthzSVNAc cessFile / var / svn / authz
 AuthUserFi le / 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.

```
systemctl start httpd . service
```

Step 6: Configure the security group rules

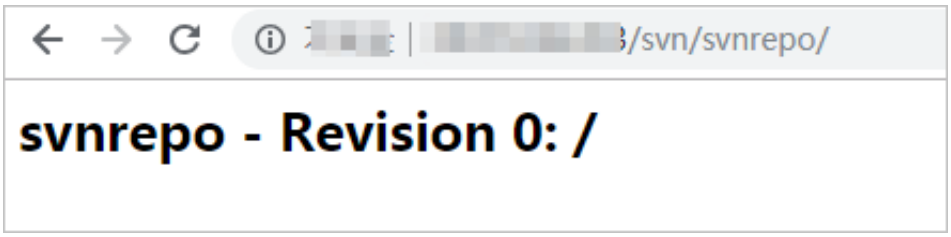
The SVN server listens on TCP Port 3690 by default. You must log on to the ECS console to add TCP Port 3690 to the security group. For more information, see #unique_10.

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.



13.4 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 #unique_35 and #unique_36.

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.

14 Build an FTP site on an ECS instance

14.1 Build an FTP site on a Linux ECS instance

vsftpd is a light, safe, and easy-to-use FTP server for Linux. It is the most popular FTP server across all Linux versions. This topic describes how to install vsftpd on a Linux ECS instance running CentOS 7.2 x64.

To build an FTP site on a Linux ECS instance, follow these steps:

- Step 1. Install vsftpd
- Step 2. Configure vsftpd
- Step 3. Configure a security group
- Step 4. Test

Step 1. Install vsftpd

1. #unique_43.
2. Run the following command to install vsftpd.

```
yum   install  - y   vsftpd
```

3. Run the following command to open and view `etc / vsftpd` .

```
cd  / etc / vsftpd
ls
```

Note:

- `/ etc / vsftpd / vsftpd . conf` is the core configuration file.
- `/ etc / vsftpd / ftpusers` is the blacklist. Users on the blacklist are prevented from accessing the FTP server.
- `/ etc / vsftpd / user_list` is the whitelist. Only the users on the whitelist are allowed to access the FTP server.

4. Run the following command to set vsftpd to automatically start on startup.

```
systemctl enable vsftpd . service
```

5. Run the following command to start the FTP service.

```
systemctl start vsftpd . service
```

6. Run the following command to view the FTP service port.

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

Step 2. Configure vsftpd

After vsftpd is installed, the anonymous FTP function is enabled by default. Using the anonymous FTP function, users can log on to the FTP server without the user name and password, but do not have the permission to modify or upload files.

This section describes the following vsftpd configuration methods and the corresponding parameter descriptions for your reference.

- Grant the file upload permission to anonymous users
- Configure local user logon
- Introduction to vsftpd.conf parameters

Grant the file upload permission to anonymous users

You can grant more permissions to anonymous users by modifying the options in the `vsftpd . conf` configuration file.

1. Follow these steps to modify `/ etc / vsftpd / vsftpd . conf` :
   a. Run `vim / etc / vsftpd / vsftpd . conf` .
   b. Press the i key to enter Edit mode.
   c. Set `write_enab le = YES` .
   d. Set `anon_uploa d_enable = YES` .
   e. Press the Esc key and then type `: wq` to save and close the file.
2. Run the following command to change the permissions of the `/ var / ftp / pub` directory, grant write permissions to the FTP users, and reload the configuration file.

```
chmod o + w / var / ftp / pub / systemctl restart vsftpd .
service
```

Configure local user logon

Local user logon refers to a user logging on to the FTP server by using the user name and password for the Linux operation system.

After vsftpd is installed, only anonymous FTP logon is supported. If you attempt to log on to the FTP server with the Linux user name, your access to vsftp will be denied . However, you can adjust the vsftpd configuration to allow logon with a user name and password. Follow these steps:

1. Run the following command to create the ftptest user.

```
useradd   ftptest
```

2. Run the following command to modify the password for the ftptest user.

```
passwd   ftptest
```

3. Follow these steps to modify `/ etc / vsftpd / vsftpd . conf` :
   a. Run `vim  / etc / vsftpd / vsftpd . conf` .
   b. Press the i key to enter edit mode.
   c. Set `anonymous   enable = NO` .
   d. Set `local_enab  le = YES` .
   e. Press the Esc key and then type `: wq` to save and close the file.
4. Run the following command to reload the configuration file.

```
systemctl   restart   vsftpd . service
```

Introduction to vsftpd.conf parameters

Run `cat  / etc / vsftpd / vsftpd . conf` to view content in the configuration file.

The following table lists all the parameters related to user logon control.

Parameter	Description
anonymous_enable=YES	Allows anonymous logon.
no_anon_password=YES	Anonymous users are not prompted for a password when logging on.
anon_root=(none)	Root directory for anonymous users.
local_enable=YES	Allows local user logon.
local_root=(none)	Root directory for local user.

The following table lists all the parameters related to user permission control.

Parameter	Description
write_enable=YES	Allows file upload (global control).
local_umask=022	Umask for the local user to upload files.
file_open_mode=0666	Uses umask for file upload permission.
anon_upload_enable=NO	Allows anonymous users to upload files.
anon_mkdir_write_enable=NO	Allows anonymous users to create directories.
anon_other_write_enable=NO	Allows anonymous users to modify and delete files and directories.
chown_username=lightwiter	Anonymous Upload File belongs User Name.

Step 3. Configure a security group

After building the FTP site, you must add a rule to open the FTP port. For more information, see add a security group rule.

Step 4. Test

On your local computer, access the FTP site by using `ftp :// public IP address : FTP port` (the default port 21 is used if you do not enter the port). For example, `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.

14.2 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_45.
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.