Elastic Cloud Server

Best Practices

Issue	01
Date	2020-08-31

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Migrating Servers to the Cloud

Background

As the public cloud is agile, flexible, secure, reliable, easy to use, and cost-effective, more and more enterprises migrate their IT applications and loads to the public cloud. It is important to quickly migrate existing server systems from on-premises IT systems or other public clouds to HUAWEI CLOUD. HUAWEI CLOUD supports migration of x86 physical servers or VMs on private clouds or other public cloud platforms to HUAWEI CLOUD ECSs.

Two migration methods are available for you.

- Server Migration Service (Recommended)
- Image import

This section describes how to use the preceding methods to migrate applications and data from your existing servers to HUAWEI CLOUD.

Server Migration Service (Recommended)

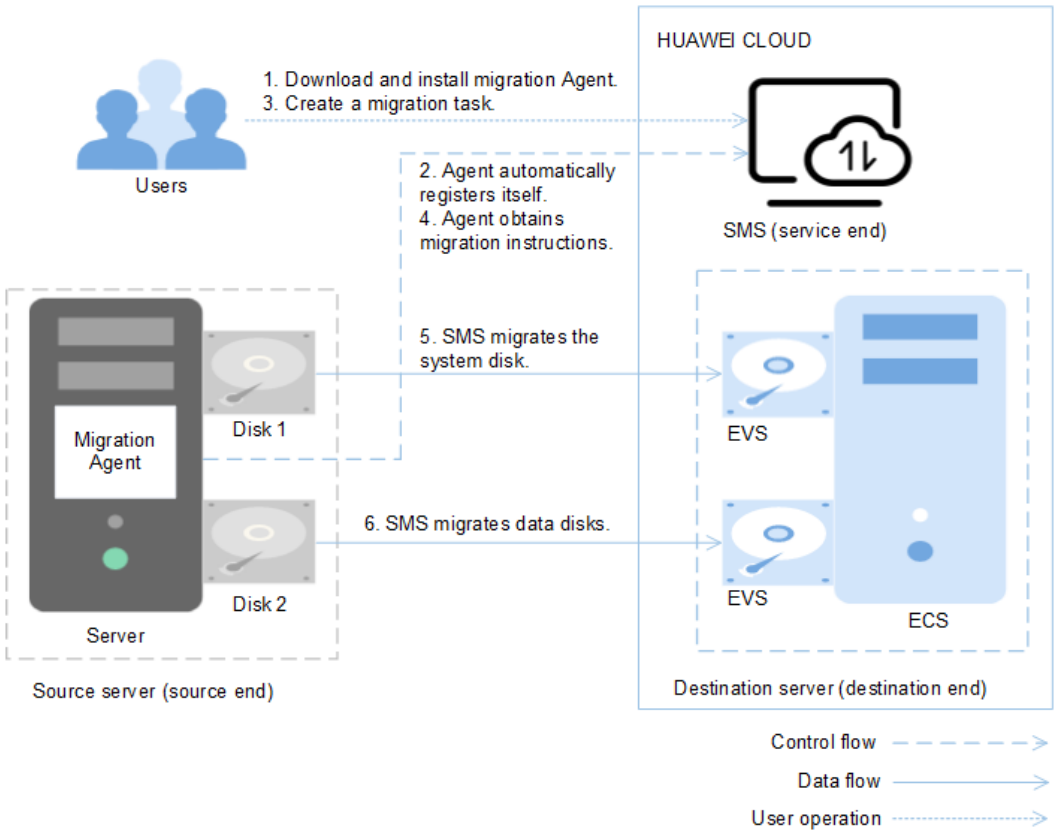
Service Overview

Server Migration Service (SMS) provides P2V and V2V migration services to help you migrate applications and data from on-premises x86 physical servers or VMs on private or public clouds to HUAWEI CLOUD Elastic Cloud Servers (ECSs).

SMS supports a wide range of OS types. For details, see **Supported Source Server OSs**.

Before using SMS, you need to know **Constraints and Limitations on Source Servers**.

Figure 1-1 SMS working principle



SMS works as follows. SMS automatically performs the migration, and you only need to perform **1** and **3** by yourself.

1. Install the migration Agent on the source server. For details, see **Installing the Agent on Source Servers**.
2. The migration Agent installed on the source server registers its connection status with SMS and reports the information about the source server to SMS. Then, SMS completes the migration feasibility check.
3. After the migration feasibility check is passed, you can create a migration task. For details, see **Creating a Migration Task**.
4. The migration Agent obtains and executes the migration instruction sent by SMS.
5. SMS starts to migrate system disk of the source server.
6. SMS starts to migrate data disks of the source server.

NOTE

- **Source end**: indicates the source server in a migration task.
- **Destination end**: indicates the destination server in the migration task.
- **Service end**: indicates the SMS service.

Service entry

SMS procedure: **Creating a Migration Task**.

SMS introduction: **Server Migration Service**

Image Import

1. Create an image. For example, you can use QEMU to create an image. See **details**.
2. Create a private image. See **details**.
3. Create an ECS based on the private image. See **Purchasing an ECS**.

2 Hardening Security for SSH Logins to Linux ECSs

Linux ECSs are generally logged in using SSH. How can I ensure login security for password-authenticated Linux ECSs? This section uses CentOS 7.6 as an example to describe how to harden security for SSH logins.

Table 2-1 ECS configurations

Parameter	Example Value
Name	ecs-f5a2
OS	CentOS 7.6 64bit
EIP	119.3.*xxx.x*
Login mode	Password

Changing the Default Login Port

1. Remotely log in to the ECS using its password through SSH. For details, see **Login Using an SSH Password** .
2. Run the following command to change the default port for SSH logins, for example, to **5000**:

   vim /etc/ssh/sshd_config

   Press **i** to enter the editing mode. In line 17, delete the comment character (#) and change the port number to **5000**.

   Figure 2-1 Before the change

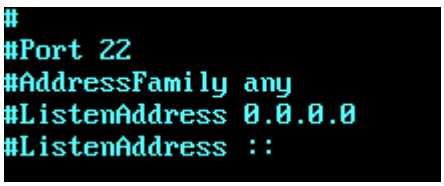
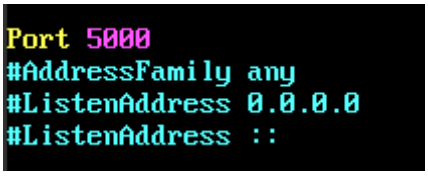
   

Figure 2-2 After the change



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

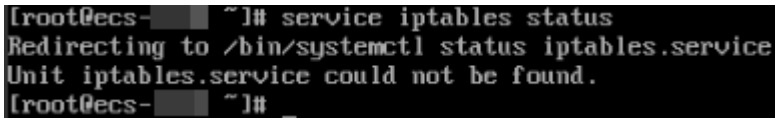
Adding a Firewall Rule to Allow the Access of a Specified Port

CentOS 7 series use Fireware firewalls, but not Iptables by default. Perform the operations described in this section only if Iptables has been installed on your ECS to allow the access of port 5000 for SSH logins.

1. Run the following command to check whether Iptables has been installed:

   service iptables status

   - If information similar to the following is displayed, Iptables has not been installed. In such a case, skip this section and proceed with **Adding a Security Group Rule**.

   - If information similar to the following is displayed, Iptables has been installed, and it is in **active** state. Then, go to step 2.

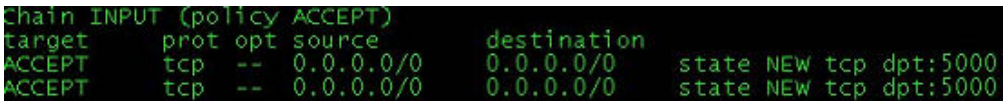
     

2. Run the following command to add an Iptables rule to allow the access of port 5000:

   iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 5000 -j ACCEPT

3. Run the following command to check whether port 5000 is contained in the existing Iptables rules:

   iptables -L -n

Adding a Security Group Rule

By default, port 22 is enabled in the inbound direction of a security group. After changing the SSH login port on your ECS to port 5000, add a rule for port 5000 to the security group.

1. Log in to the management console.

2. Under **Computing**, click **Elastic Cloud Server** to switch to the ECS console.
3. Click the ECS name **ecs-f5a2** to go to the page providing details about the ECS.
4. Click the **Security Groups** tab and then to show details about the security group rules. Click **Modify Security Group Rule** in the upper right corner of the table for the security group rules.
5. Add an inbound rule, as shown in **Figure 2-3**.

Figure 2-3 Security group rules

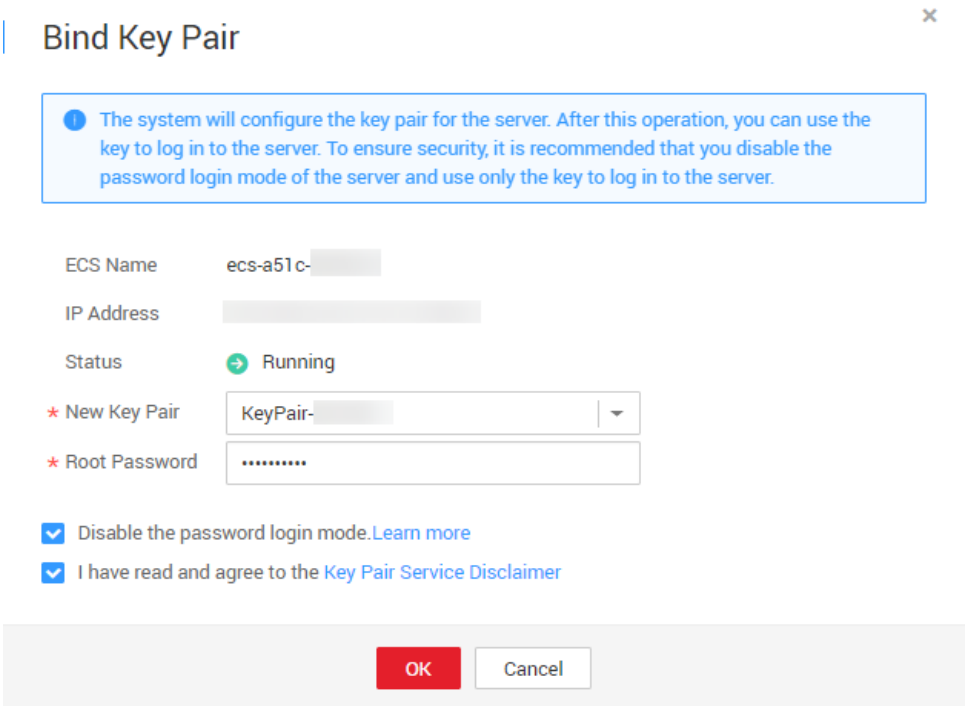
Type	Protocol	Port/Range	Source	Description
IPv4	All	All	sg-9341	--
IPv4	TCP	22	0.0.0.0/0	Permit default Linux SSH port.
IPv4	TCP	3389	0.0.0.0/0	Permit default Windows remote desktop port.
IPv4	TCP	5000	0.0.0.0/0	--

Changing Password Authentication to Key-Pair Authentication

Create a key pair on the management console and bind the key pair to your ECS. Edit the **sshd_config** file to disable password authentication.

1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server** to switch to the ECS console.
3. Create a key pair by following the instructions provided in **Creating a Key Pair** and securely keep the private key file.
4. Choose **Service List** > **Security** > **Data Encryption Workshop**. In the navigation pane on the left, click **Key Pair Service**.
5. Click the **ECS List** tab, locate the row containing **ecs-f5a2**, and click **Bind** in the **Operation** column. Set parameters and click **OK**.

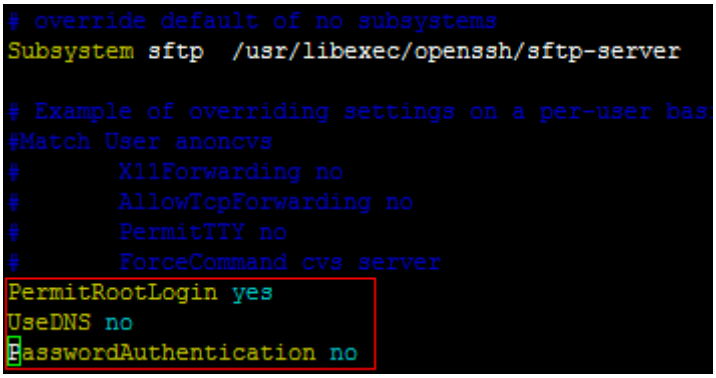
Figure 2-4 Binding a key pair



6. Log in to the ECS and edit the **sshd_config** configuration file to disable password authentication.

   vim /etc/ssh/sshd_config

   Press **i** to enter the editing mode and configure the data in last several lines, as shown in the following figure.



   Parameter description:

   - **PermitRootLogin**: specifies whether to allow the **root** user to log in to the ECS. Set this parameter to **yes**.
   - **UseDNS**: specifies whether DNS resolution is allowed. Set this parameter to **no**.
   - **PasswordAuthentication**: specifies whether a login is authenticated using a password. Set this parameter to **no**.

   NOTE

   During key pair binding in step 5, you have selected "Disable the password login mode". Therefore, the **PasswordAuthentication** value should be **no**. You only need to verify it.

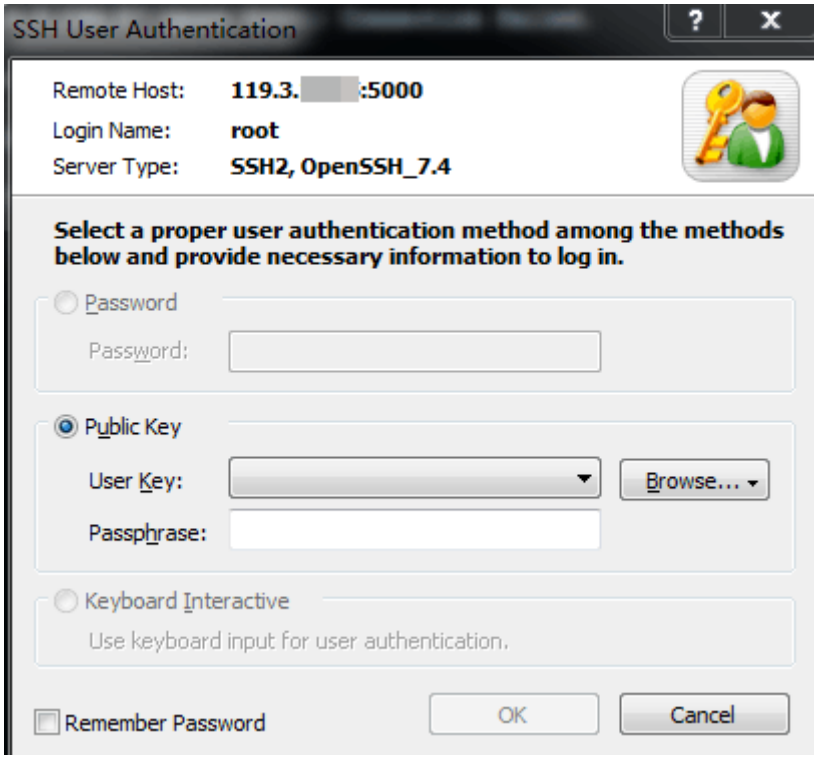
Press **Esc** and enter **:wq** to save the changes and exit.

7. Run the following command to restart sshd:

   systemctl restart sshd

8. Attempt to log in to the ECS using Xshell or an SSH client. If password input is unavailable, as shown in **Figure 2-5**, the configuration is successful.

Figure 2-5 Logging in to the ECS using Xshell



Editing hosts.allow and hosts.deny

The **/etc/hosts.allow** and **/etc/hosts.deny** files control remote access. You can configure these files to allow or deny the access of certain IP addresses or IP address segments to a process running on the Linux ECS.

For example, if SSH is available only to the administrator, allow the access of only the IP address segments that may be used by the administrator.

The ECS may be logged in anywhere. Therefore, you are advised to allow the access of all IP addresses in **/etc/hosts.allow**.

vim /etc/hosts.allow

Add **sshd:ALL** in the last line.

```
#           either use the tcp_wrappers library or that have been
#           started through a tcp_wrappers-enabled xinetd.
#
#           See 'man 5 hosts_options' and 'man 5 hosts_access'
#           for information on rule syntax.
#           See 'man tcpd' for information on tcp_wrappers
sshd:ALL
```


Identify ECS security risks using certain methods, for example, checking the SSH status, to detect risky IP addresses, and add them to **/etc/hosts.deny** to deny the access of these IP addresses.

3 Using VNC Viewer to Access a Linux ECS

Linux ECSs are generally accessed through SSH, allowing you to securely log in to your ECSs using key pairs. However, SSH connections use a character-based user interface, which does not support complex operations that are supported on the GUI. This section uses the Ubuntu 18.04 OS as an example to describe how to install VNC Server on a Linux ECS and how to use VNC Viewer to access the ECS.

Preparations

- Create an ECS running the Ubuntu 18.04 OS. Bind an EIP to the ECS and ensure that the ECS can access the Internet.

  For details, see **Purchasing an ECS** and **Assigning an EIP and Binding It to an ECS**.
- Install the VNC Viewer client on a local computer.

  NOTE

  To download VNC Viewer, log in at **https://www.realvnc.com/en/connect/download/viewer/**.

Installing VNC Server

The Ubuntu 18.04 OS has no GUI or VNC Server installed by default. In this example, Xfce, a compact lightweight desktop is used. Compared with Gnome and KDE, Xfce features compact and user-friendly. It applies to remote ECS access.

1. Remotely log in to the ECS.

   The username is **root**, and the password is set during ECS creation.
2. Run the following command to update software:

   sudo apt update
3. Install Xfce.

   sudo apt install xfce4 xfce4-goodies
4. Install the TightVNC server.

   sudo apt install tightvncserver
5. Run the **vncserver** command to configure the TightVNC server.

   After the first running of the **vncserver** command, the system automatically creates a default startup script. Then, configure parameters as prompted.


```
root@ecs-9240-          :~# vncserver

You will require a password to access your desktops.

Password:
Verify:
Would you like to enter a view-only password (y/n)? n
xauth:  file /root/.Xauthority does not exist

New 'X' desktop is ecs-9240-          :1

Creating default startup script /root/.vnc/xstartup
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/ecs-9240-          :1.log

root@ecs-9240-          :~#
```

- **Password**: consists of 6 to 8 characters. When the number of characters reaches the upper limit, no more characters can be entered. Securely keep the password, which will be used by VNC Viewer to access an ECS.
- **Verify**: Enter the password again.
- **Would you like to enter a view-only password**: If you select **y**, you are not allowed to use the mouse or keyboard to control your ECS. Press **n**.

Configuring VNC Server

1. Stop the first virtual desktop.

   vncserver -kill :1

   ```
   root@ecs-9240-          :~# vncserver -kill :1
   Killing Xtightvnc process ID 2738
   root@ecs-9240-          :~#
   ```

2. Modify the **xstartup** file.

   vim ~/.vnc/xstartup

   Press **i** to enter editing mode and enter the following data to the file:

   ```
   #!/bin/sh
   xrdb $HOME/.Xresources
   startxfce4 &
   ```

   In the preceding terminal display:

   - The first command **xrdb $HOME/.Xresources** is used to have the VNC GUI framework read the .Xresources file of VNC Server. You can modify GUI settings in the .Xresources file, such as the color display, cursor theme, and font rendering.
   - The second command **startxfce4 &** have VNC Server start Xfce.

   ```
   #!/bin/sh

   xrdb $HOME/.Xresources
   xsetroot -solid grey
   #x-terminal-emulator -geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" &
   #x-window-manager &
   # Fix to make GNOME work
   export XKL_XMODMAP_DISABLE=1
   /etc/X11/Xsession
   startxfce4 &
   ~
   ```


3. Assign executable permissions to the file to ensure proper VNC running.

   sudo chmod +x ~/.vnc/xstartup

4. Restart VNC Server.

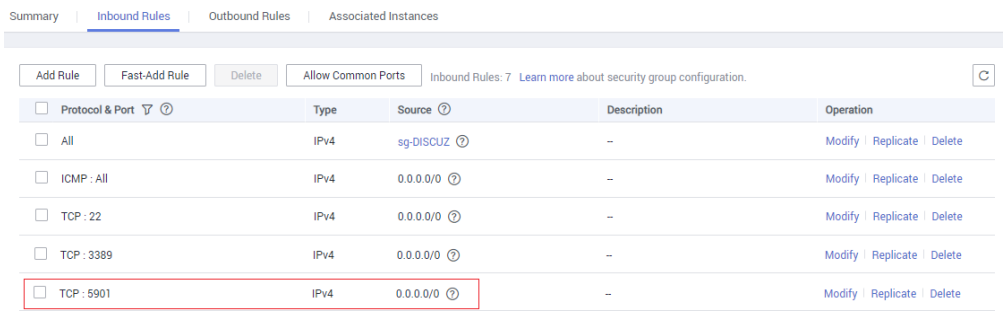
   vncserver

   After the second running of the **vncserver** command, the system automatically creates a log file.

   The information similar to "Log file is /root/.vnc/xxx:1.log" is displayed. **1** indicates that the current user is allocated with the first VNC desktop. The VNC port number is "5900+virtual desktop number", which is used by the VNC Viewer agent to access your ECS.

Configuring the ECS on the Management Console

1. Log in to the management console.
2. Click the name of your ECS to switch to the page providing details about the ECS.
3. On the **Security Groups** tab page, click **Modify Security Group Rule** to permit port 5901.



NOTE

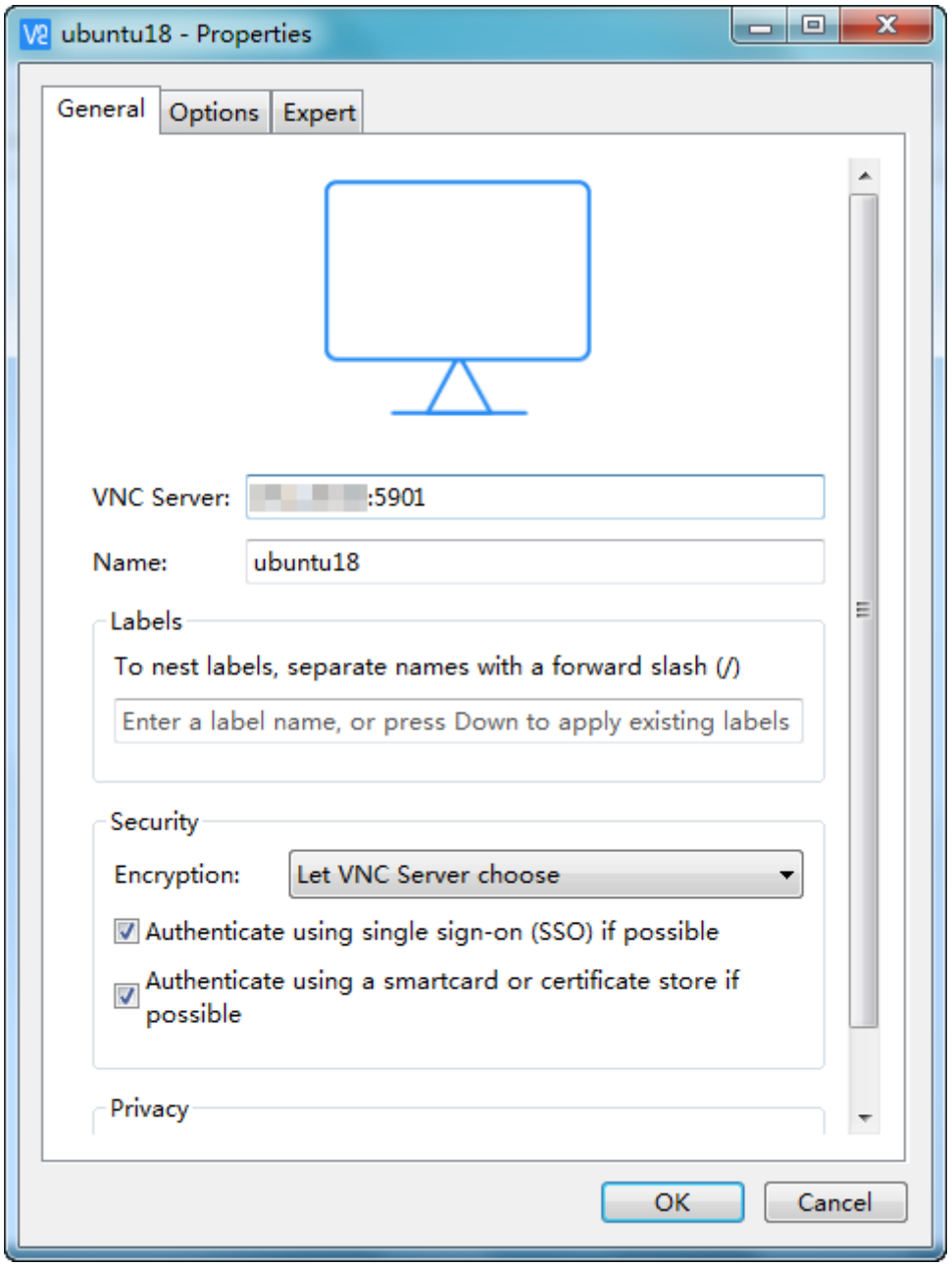
If the log file displayed in the command output of step 4 is **xxx:2.log**, permit port 5902. If the log file is **xxx:3.log**, permit port 5903. Apply the rule to other ports.

Using VNC Viewer to Access the ECS

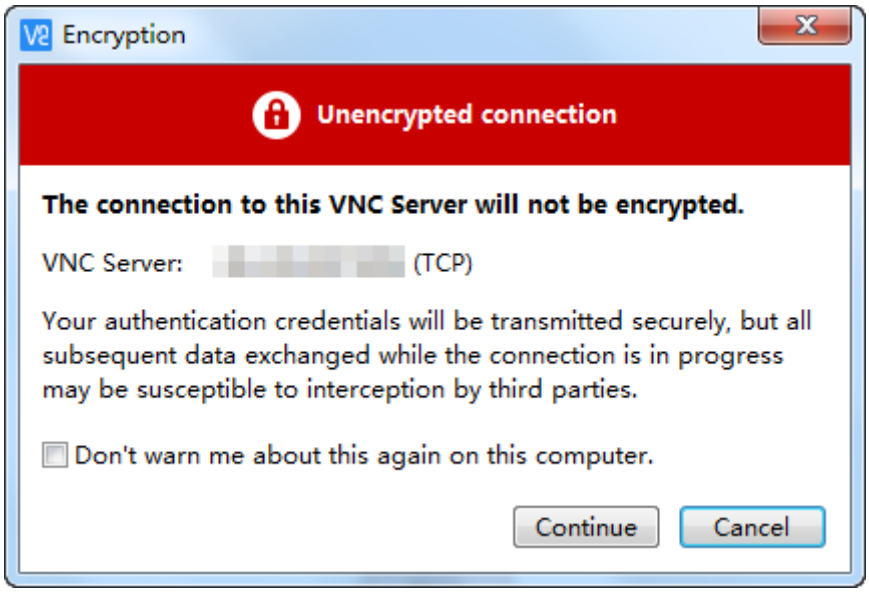
1. Start the VNC Viewer client on the local computer, enter **EIP:5901**, set the name, and click **OK**.

NOTE

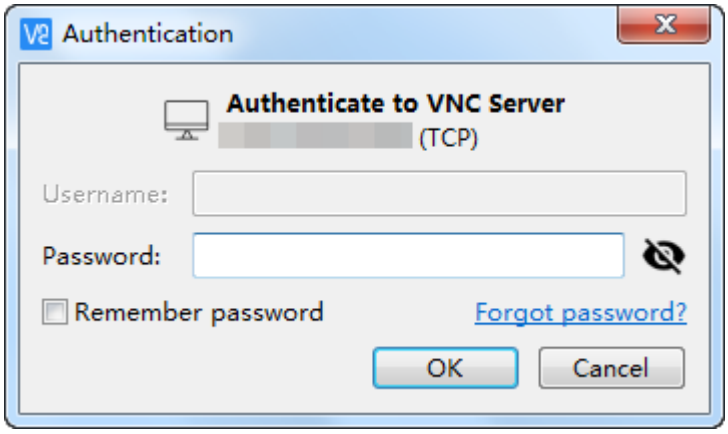
The port number is determined by the log file name displayed in the command output of step 4. If the log file name is **xxx:1.log**, enter **5901**.



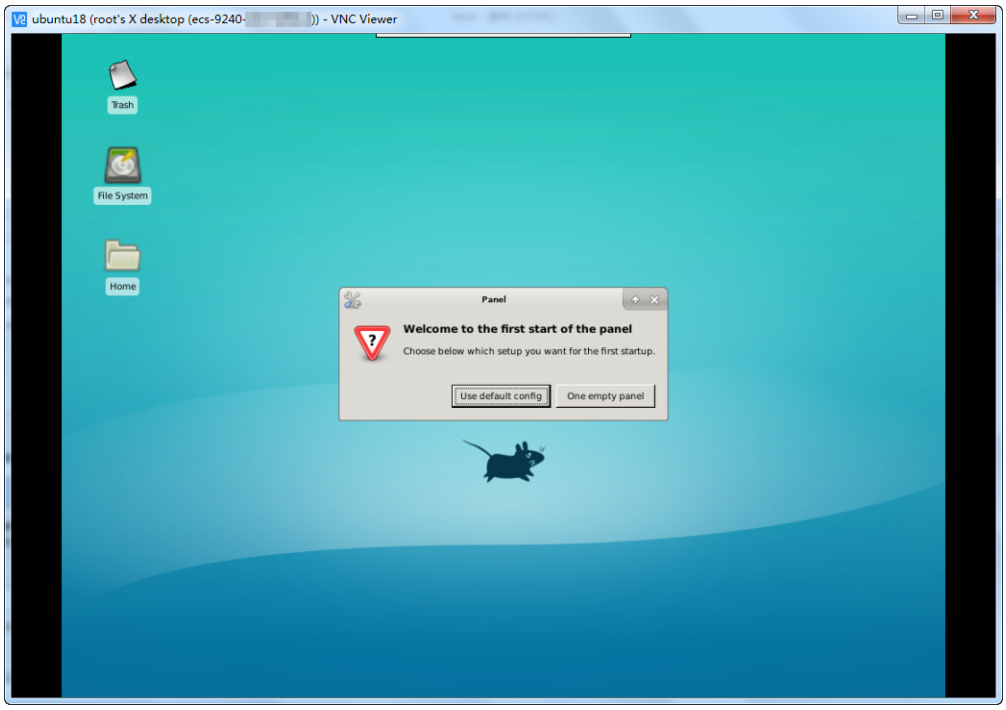
2. In the displayed dialog box, click **Continue**.



3. Enter the password set in step 5 and click **OK**.



4. Verify the GUI of the Ubuntu 18.04 OS.



4 Getting Started with Website Setup

Overview

This section describes how to set up a website on HUAWEI CLOUD. You can select a proper mode that best suits your needs.

Setup Modes

HUAWEI CLOUD provide you with four ways to set up a website, as described in Table 4-1. This section describes the self-service setup mode. For details about website setup using CloudSite, see the help documentation for CloudSite. For details about other two modes, see the user guides provided by the cloud service providers.

Table 4-1 Setup modes

Mode	Characteristics	Application Scenario
Self-service setup	The deployment process is complex and time-consuming. You need to purchase ECSs and build and maintain the websites by yourself. But it can meet your personalized needs.	This mode is applicable to experienced users who intend to design and build websites for individual or small businesses, or to users who are new to public cloud and hope to explore it by setting up personal or small enterprise websites.

Mode	Characteristics	Application Scenario
Setup using CloudSite	CloudSite is a HUAWEI CLOUD service for individuals and small- and medium-sized enterprises to set up websites, online stores, and WeChat stores. It provides a five-in-one template and enables you to build websites for PCs, mobile phones, WeChat public accounts, mini programs, and applications without any coding.	CloudSite provides more than 60 marketing tools applicable to websites for B2C transactions and cross-border e-commerce businesses of trade enterprises, achieving simple, cost-effective deployment.
Setup using templates	Templates available in the HUAWEI CLOUD Marketplace are professional website setup templates provided by HUAWEI CLOUD partners. You can purchase templates here for a time-saving, easy deployment. The websites deployed can be easily managed at the backend, and are maintained by technical personnel.	This mode is applicable to individuals or small- and medium-sized enterprises that have simple requirements. Templates for various channels are available, such as PC, mobile phone, and WeChat. The deployment process is simple and cost-effective.
Setup using customization services	Website customization services on the HUAWEI CLOUD Marketplace provide dedicated and customized experience for you. The websites deployed can be easily managed at the backend, and are maintained and supported by technical personnel.	This mode is applicable to enterprise users who have unique requirements on websites and sufficient funds. One-to-one professional development enables you to sleep peacefully at night and save time and labor resources.

Self-Service Setup

Step 1 Create one or more ECSs.

When you create an ECS, you need to specify ECS specifications, including vCPU, memory, disk, and bandwidth. The ECS specifications you specified must meet the minimum requirements for running website-related software. In addition, you must consider the website type, scale, and estimated access traffic.

- An ECS can be billed on a pay-per-use, yearly/monthly, or spot price basis. You can select an appropriate billing mode based on your demands. For details, see **ECS Billing**. You can also use the **price calculator** to learn the prices of ECSs with different specifications.
- If you already have an ECS of proper specifications, you can use it to deploy your website. Otherwise, purchase an ECS. For details, see **Methods of Purchasing ECSs**.

Step 2 Set up a website.

A website can be set up either manually or using an image. For details, see **Best Practices for Setting Up Websites**.

Step 3 Purchase a domain name.

To make the website accessible and usable, configure a unique domain name for the website. If a domain name is available, you can directly use it after authentication. If no domain name is available, follow the HUAWEI CLOUD domain registration process to purchase one.

Step 4 Obtain an ICP license.

If your website has not obtained an ICP license and needs to be hosted on HUAWEI CLOUD, use the HUAWEI CLOUD ICP license service to obtain a license.

Step 5 Enable domain name resolution.

Your website can be visited using the registered domain name only after domain name resolution is enabled. For details, see **Configuring Record Sets for a Website**.

For example, if the domain name is www.example.com, enter http// www.example.com in the address bar of the browser to access the website.

----End

Common FAQs

When deploying a website using an ECS, you may encounter some problems due to various reasons. The common problems and troubleshooting methods are as follows:

- ECS login
  - **What Should Be Prepared for Logging In to an ECS?**
  - **What Should I Do If I Cannot Log In to My Windows ECS?**
  - **What Should I Do If I Cannot Log In to My Linux ECS?**

  For more information, see **FAQs about ECS Login**.

- Security group
  - **Does a Security Group Rule or a Network ACL Rule Immediately Take Effect for Its Original Traffic After It Is Modified?**
  - **Can I Change the Security Group of an ECS?**

  For more information, see **FAQs about security group**.
- Network
  - **How Do I Handle the ECS IP Address Obtaining Failure?**
  - **How Do I Handle EIP Connection Failure?**
  - **What Do I Do If a Virtual IP Address Cannot Be Pinged After It Is Bound to an ECS NIC?**

  For more information, see **FAQs about VPC**.
- OS
  - **Troubleshooting High Bandwidth or CPU Usage of a Windows ECS**
  - **Troubleshooting High Bandwidth or CPU Usage of a Linux ECS**

  For more information, see **FAQs about OSs**.
- DNS
  - **How Do I Test Whether a Record Set Has Taken Effect?**
  - **How Do I Test Whether a Record Set Has Taken Effect?**

  For more information, see **FAQs about DNS**.
- Others
  - **Troubleshooting a Website Access Error Occurred on an ECS**
  - **Troubleshooting an Unreachable ECS Port**

Related Services

- If you want to quickly and smoothly migrate existing services to or deploy new services on HUAWEI CLOUD using professional migration solutions and dedicated migration tools, Cloud Migration Service on HUAWEI CLOUD can help you.
- If your services have been deployed on HUAWEI CLOUD, and need dedicated assurance service from professional engineers, Event Management Service on HUAWEI CLOUD can help you.

5 Best Practices for Setting Up Websites

Overview

This section provides guidance on how to set up frequently used websites using HUAWEI CLOUD services. In addition to operation guides, this section provides links to desired images, facilitating your website setup.

You can set up a website manually or using an image.

- Image-based setup: Marketplace images are used, featuring short, simple setup. This mode applies to mainstream website setup scenarios with professional after-sales support from image providers.
- Manual setup: This mode is time-consuming and complex. You must select suitable software, such as OS, database, and middleware for installation and configuration. The website maintenance relies on the experience of O&M personnel. This setup mode is suitable for custom requirements.

Summary

Table 5-1 Summary on website setups

Setup Mode	Website Requirement	OS	Image and Resources	Description
Manual setup	Setting Up a Discuz Forum	CentOS 6.3	Public image	Discuz is a common community forum software system. Its basic architecture is based on the popular web programming combination of PHP +MySQL.
Manual setup	Setting Up an FTP Site (Windows)	Windows Server 2012 R2	Public image	Use FTP delivered with Windows to set up an FTP site.

Setup Mode	Website Requirement	OS	Image and Resources	Description
Manual setup	**Setting Up an FTP Site (Linux)**	CentOS 7.2	Public image	Use the very secure FTP daemon (vsftpd) software to set up an FTP site. vsftpd is an FTP server software that is widely used in Linux releases.
Manual setup	**Manually Setting Up a Java Website**	CentOS 7.3	Public image • Tomcat 8.5.31 • JDK 8u171	Tomcat is a commonly used open source web application that is free of charge. It can be used to host common Java web applications.
Manual setup	**Manually Setting Up a Magento E-Commerce Website (Linux)**	CentOS 7.2	Public image • MySQL 5.7 • PHP 7.0 • Magento 2.1	Magento is an open source e-commerce system that features flexible design, modular architecture, and rich functions. It provides solutions for medium- and large-sized sites.
Manual setup	**Setting Up a Microsoft SharePoint Server 2016 Website**	Windows Server 2012 R2	Public image • Microsoft SQL Server 2014 • SharePoint Server 2016	Microsoft SharePoint Server is a portal that enables enterprises to develop intelligent portal websites. These sites are seamlessly accessible to users, teams, and knowledge libraries.
Manual setup	**Manually Setting Up an LNMP Website**	CentOS 7.2	Public image • Nginx 1.14.0 • MySQL 5.7 • PHP 7.0.31	LNMP indicates the Nginx+MySQL+PHP website server architecture in Linux. Nginx is compact, efficient web server software in Linux.

Setup Mode	Website Requirement	OS	Image and Resources	Description
Manual setup	**Manually Deploying WordPress (Linux)**	CentOS 7.2	Public image • Nginx 1.14.0 • MySQL 5.7 • PHP 7.0.31 • WordPress 4.9.8	A Linux ECS is used to manually set up an LNMP website and deploy WordPress on it. WordPress (WP for short) is initially a blog system and gradually evolved to a CMS or website setup system that is free of charge.
Manual setup	**Manually Deploying Docker (CentOS 7.5)**	CentOS 7.5	Public image	Docker is deployed on a Linux ECS. Additionally, common Docker operations and the process of creating a Docker image are provided.
Manual setup	**Deploying an ECS for Transceiving Text Messages from an Official WeChat Account**	CentOS 7.4	Public image	An ECS is deployed as an official WeChat account server so that it receives text messages from the WeChat server and sends processing results to end users. On this ECS, Python is used to compile the logic code for processing WeChat messages.
Manual setup	**Manually Deploying GitLab (CentOS 7.2)**	CentOS 7.2	Public image	A Linux ECS is used for manually deploying GitLab. GitLab is an open source version management system that uses Git as the code management tool.

Setup Mode	Website Requirement	OS	Image and Resources	Description
Manual setup	**Manually Deploying RabbitMQ (CentOS 7.4)**	CentOS 7.4	Public image • Erlang 8.3 • RabbitMQ 3.6.9	A Linux ECS is used for deploying RabbitMQ. RabbitMQ is a message middleware that uses the Erlang programming language for the Advanced Message Queuing Protocol (AMQP). It originates from the financial system and is used to store and forward messages in the distributed system. Featuring high reliability, scalability, availability, and rich functions, RabbitMQ is widely used.
Manual setup	**Manually Building a Ghost Blog**	Ubuntu 16.04	Public image • Nginx 1.14.0 • MySQL 5.7	Ghost is an open source blog platform based on Node.js and makes writing and release more convenient. This section walks you through the deployment of a Ghost blog on an ECS running Ubuntu 16.04.

Setup Mode	Website Requirement	OS	Image and Resources	Description
Manual setup	**Manually Deploying Node.js (CentOS 7.2)**	CentOS 7.2	Public image	A Linux ECS is used for deploying Node.js. Node.js is a JavaScript runtime environment based on the Google Chrome V8 engine. It enables simple deployment of network applications that feature fast response and easy-to-expand. Based on the event-driven and non-blocking I/O model, Node.js is lightweight and efficient. It is ideal for running data-intensive real-time applications on distributed devices.
Manual setup	**Setting Up a Local Slave PostgreSQL Database**	CentOS 7.6 64bit	PostgreSQL (11.2)	PostgreSQL is an open source object relational DBMS (ORDBMS) with an emphasis on extensibility and standards compliance. This section helps you use HUAWEI CLOUD ECSs to set up PostgreSQL.

Setup Mode	Website Requirement	OS	Image and Resources	Description
Manual setup	**Manually Installing a BT Panel (CentOS 7.2)**	CentOS 7.2 64bit	BT Linux panel 6.9	BT panel is easy-to-use, powerful, and free server management software that supports Linux and Windows. You can configure LAMP, LNMP, website, database, FTP, and SSL with a few clicks, and easily manage the server through web pages.

6 Setting Up a Discuz Forum

6.1 Introduction

Application Scenarios

HUAWEI CLOUD provides a variety of solutions. The following describes how HUAWEI CLOUD can help you build a website.

Small websites are often deployed on a single server, which handles user access, static and dynamic content, and database use, and data computing. As website services develop, database access traffic drastically increases, and a single server fails to meet the service requirements. Therefore, website applications and the database need be deployed on different servers to balance their work loads. According to national regulations, if the servers used to deploy the website are located in the Chinese mainland, Internet Content Provider (ICP) licensing is required. The domain name that is not licensed cannot be used to access the website.

To build a website, for example, a forum, the following requirements must be met:

1. Database nodes and service nodes are deployed on different servers.
2. The number of servers is dynamically adjusted based on service volume.
3. Traffic is automatically distributed to multiple servers.
4. The website must be licensed.

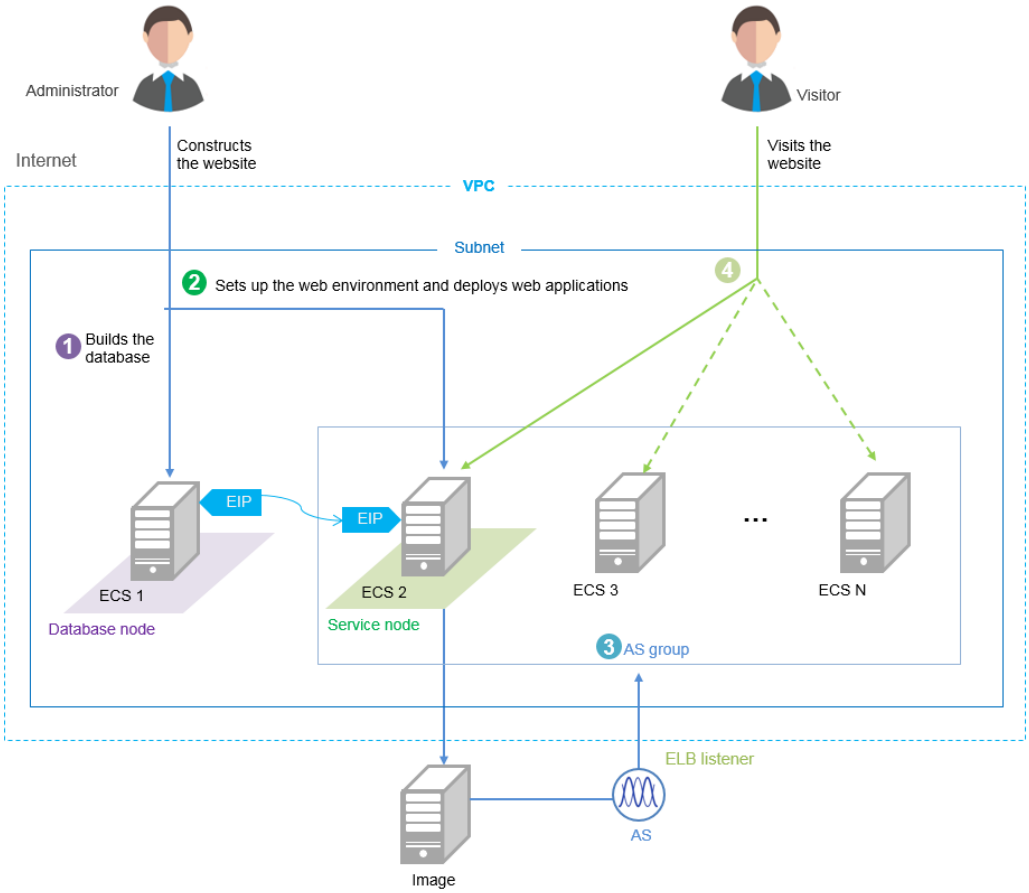
Solutions

HUAWEI CLOUD provides the following solutions for building a forum.

Table 6-1 HUAWEI CLOUD solutions

Requirement	Solution	Service
Database nodes and service nodes are deployed on different servers.	**Building the website**: Two Elastic Cloud Servers (ECSs) are required to replace traditional servers. One ECS works as the database node, and the other as the service node. A Virtual Private Cloud (VPC) is required to provide network resources for the two ECSs. An Elastic Volume Service (EVS) disk can be attached to the ECS as a data disk as required.	ECS VPC (Optional) EVS
The number of servers is dynamically adjusted based on service volume.	**Configuring features**: Auto Scaling (AS) policies are set based on service requirements. AS dynamically adds and removes ECSs created from the image of the service node as required to ensure stable and efficient service running.	AS
Service traffic is automatically distributed to multiple servers.	**Configuring features**: Elastic Load Balance (ELB) automatically distributes access traffic to multiple service nodes, achieving better fault tolerance and expanding service capabilities for applications.	ELB

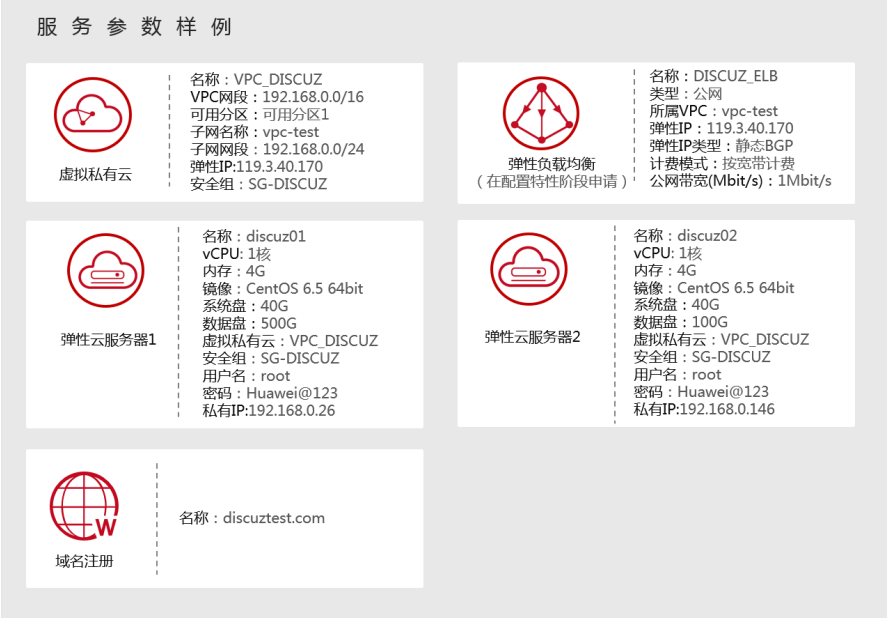
Logical Architecture



1. Bind an elastic IP address (EIP) to ECS 1 and build the database.
2. Unbind the EIP from ECS 1, bind it to ECS 2, set up the web environment, and deploy web applications.
3. As service traffic increases, AS adds ECSs created from the image of ECS 2 to the AS group.
4. Visitors access the website via the EIP of the load balancer, which automatically distributes traffic to multiple ECSs.

6.2 Purchasing Services

Required Services

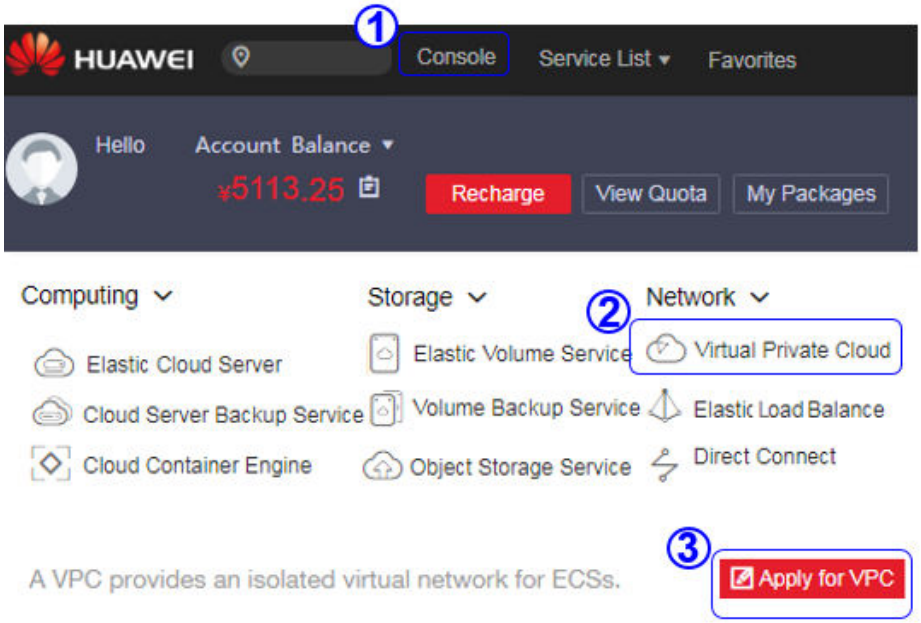


NOTE

Retain default settings for parameters not highlighted in the figures when buying services and configuring features.

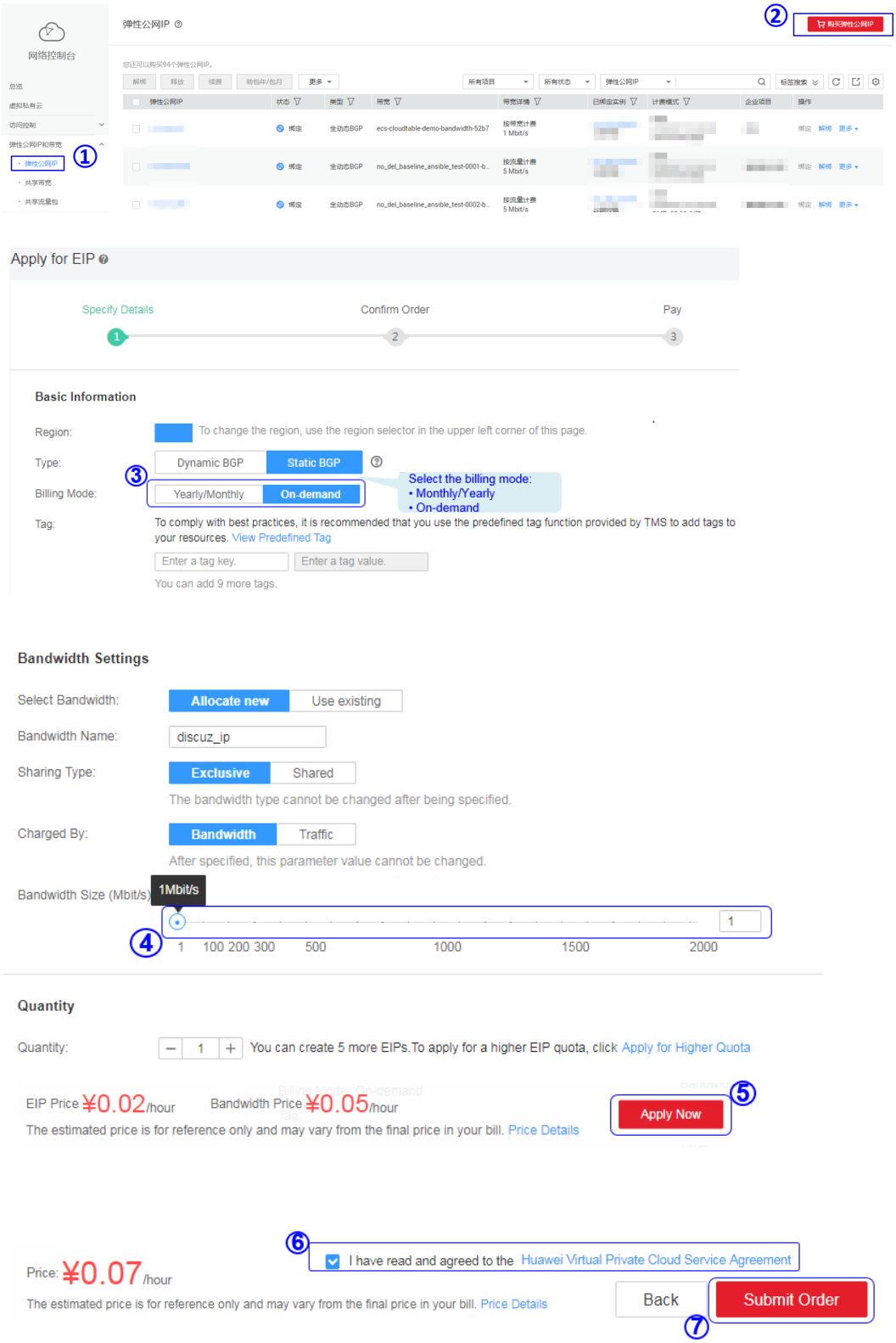
Applying for a VPC

1. On the displayed page, click **Apply for VPC**.

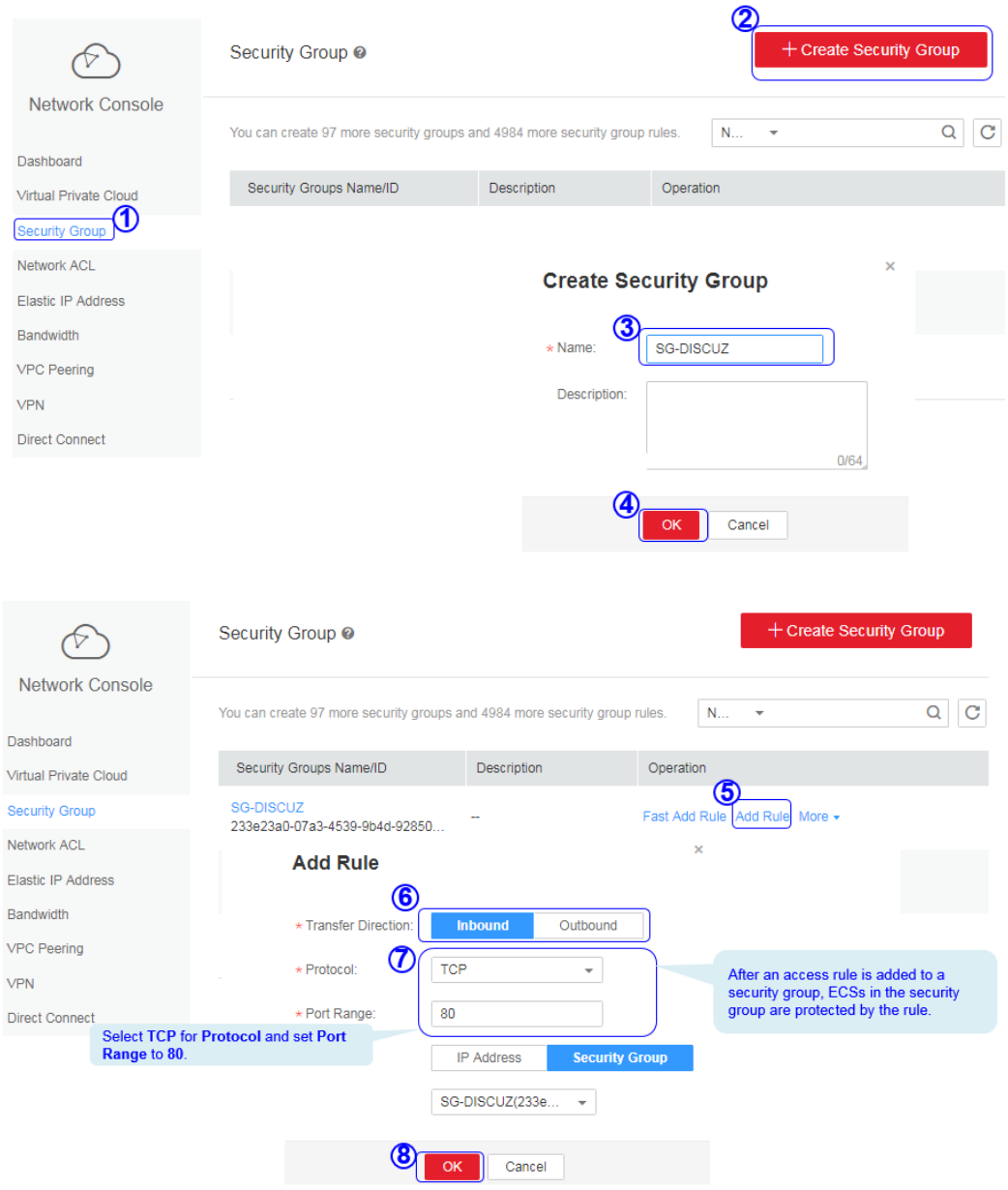


2. Specify the parameters and click **Create Now**.

Applying for an EIP



Creating a Security Group and Adding Rules

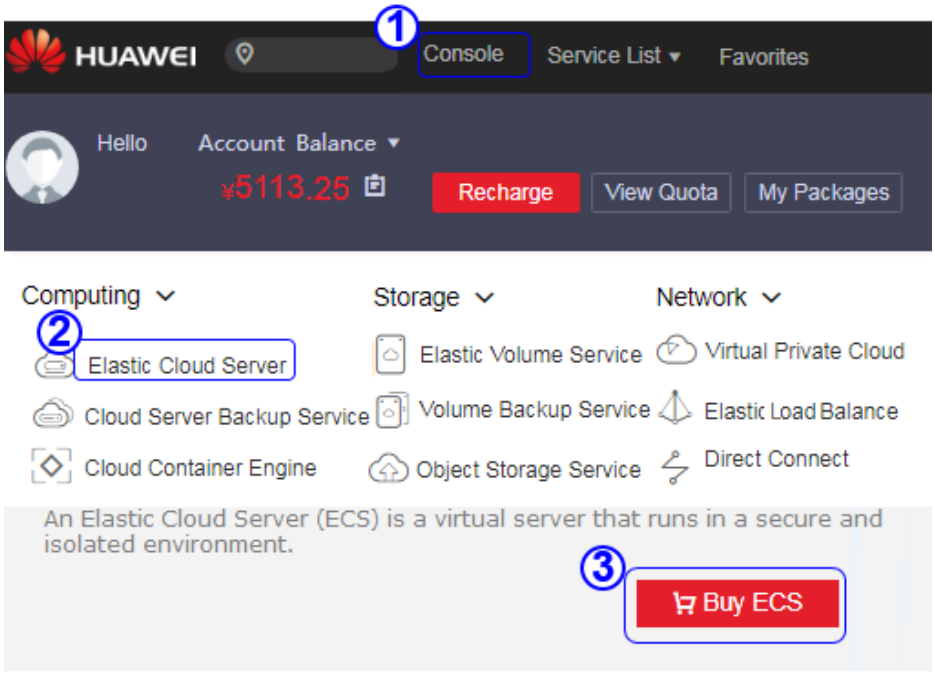


NOTE

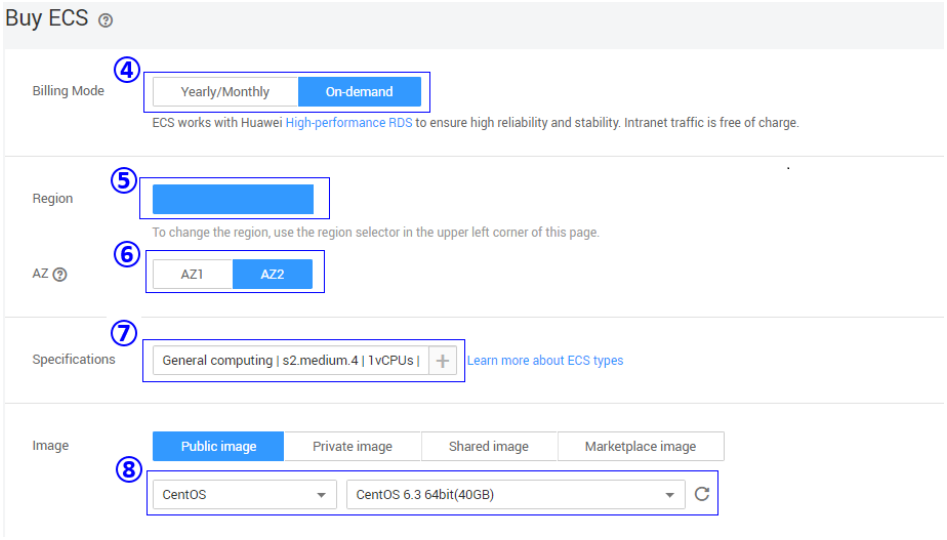
The default rules of the security group cannot be deleted. Otherwise, two servers cannot communicate with each other.

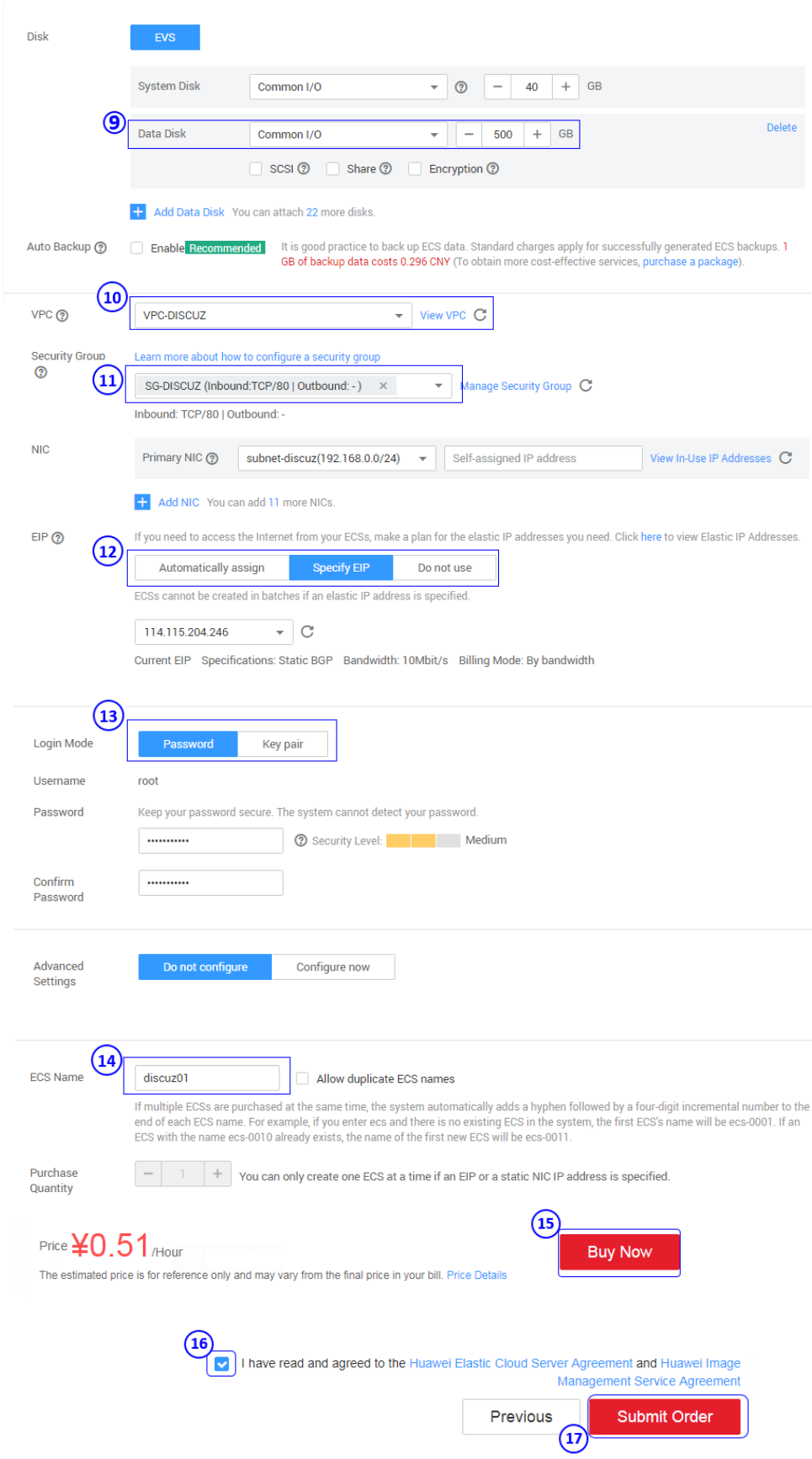
Purchasing ECSs

1. Under **Computing**, click **Elastic Cloud Server**. On the page that is displayed, click **Buy ECS**.



2. Specify the parameters and submit the request.



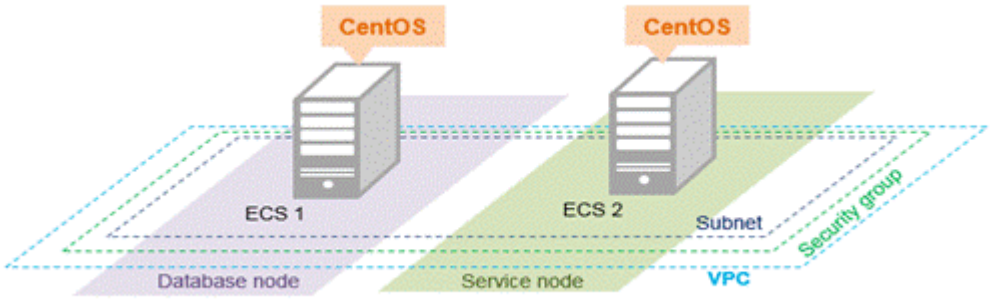


NOTE

You need to buy two ECSs. For details about their configuration, see "Example parameters".

6.3 Building the Website

Purchased Services



Example parameters

VPC

A VPC can connect to the Internet through an EIP.

- Name: VPC-DISCUZ
- VPC network segment: 192.168.0.0/16
- AZ: AZ 2
- Subnet: subnet-discuz
- Subnet network segment: 192.168.0.0/24
- EIP: 114.115.138.223
- Security group: SG-DISCUZ

ECS 1

Serves as a database node to deploy the database.

- Name: discuz01
- vCPU: 1 vCPU
- Memory: 4 GB
- Image: CentOS6.3 64-bit
- System disk: 40 GB
- Data disk: 500 GB
- VPC: VPC-DISCUZ
- Security group: SG-DISCUZ
- Username: root
- Password: Huawei@123
- Private IP address: 192.168.0. 3

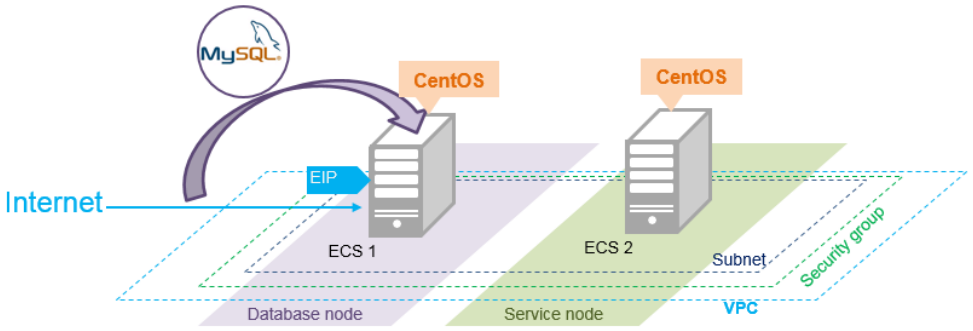
ECS 2

Serves as a service node to set up the website environment and deploy website code.

- Name: discuz02
- vCPU: 1 vCPU
- Memory: 4 GB
- Image: CentOS 6.3 64-bit
- System disk: 40 GB
- Data disk: 100 GB
- VPC: VPC-DISCUZ
- Security group: SG-DISCUZ
- Username: root
- Password: Huawei@123
- Private IP address: 192.168.0.138

Building Process

Building the Database

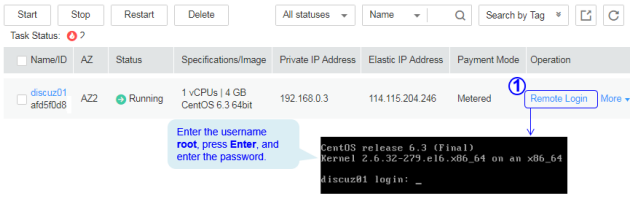


Install the database.

NOTE

- CentOS 6.5 64bit (40 GB) is used as the OS of the database node, and the MySQL version is 5.1.73.
- For CentOS 7 and later versions, MySQL is removed from the default program list. You need to run the **sudo rpm -Uvh http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm** command to manually download MySQL. After the download is complete, perform **2** to install the software.

1. Log in to ECS discuz01 remotely and enter the username and password.



2. Run the following command to deploy the MySQL database server, MySQL client, and all required libraries and files:

   yum install -y mysql-server mysql mysql-devel

   If the following information is displayed, the installation is successful.

   ```
   Complete!
   ```

Configure MySQL.

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

   service mysqld start

2. Run the following command to set the administrator username and password. The password is self-defined. In this command, **Huawei@123** is used an example.

   mysqladmin -u root password '*Huawei@123***'**

3. Run the following command and enter the password of user root to enter the database:

   mysql -u root -p

4. Run the following command to use the database:

use mysql

5. Run the following command to query the user list:

   select host,user from user;

   NOTE

   This command and the following database commands must end with a semicolon (;).

6. Run the following command to refresh the user list and allow all IP addresses to access the database:

   update user set host='%' where user='root' LIMIT 1;

7. Run the following command to forcibly update the permissions: and allow ECSs in the same subnet to access the MySQL database using private IP addresses.

   flush privileges;

8. Run the following command to exit the database:

   quit

9. Run the following command to restart the MySQL service:

   service mysqld restart

10. Run the following command to enable the MySQL service to automatically start upon system boot:

    chkconfig mysqld on

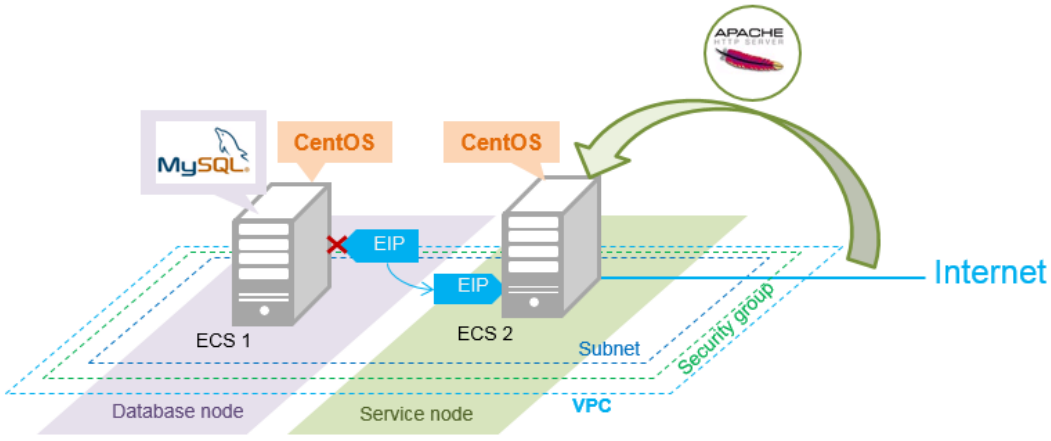
11. Run the following command to disable the firewall:

    service iptables stop

12. Run the following command to permanently disable the firewall after restarting the ECS:

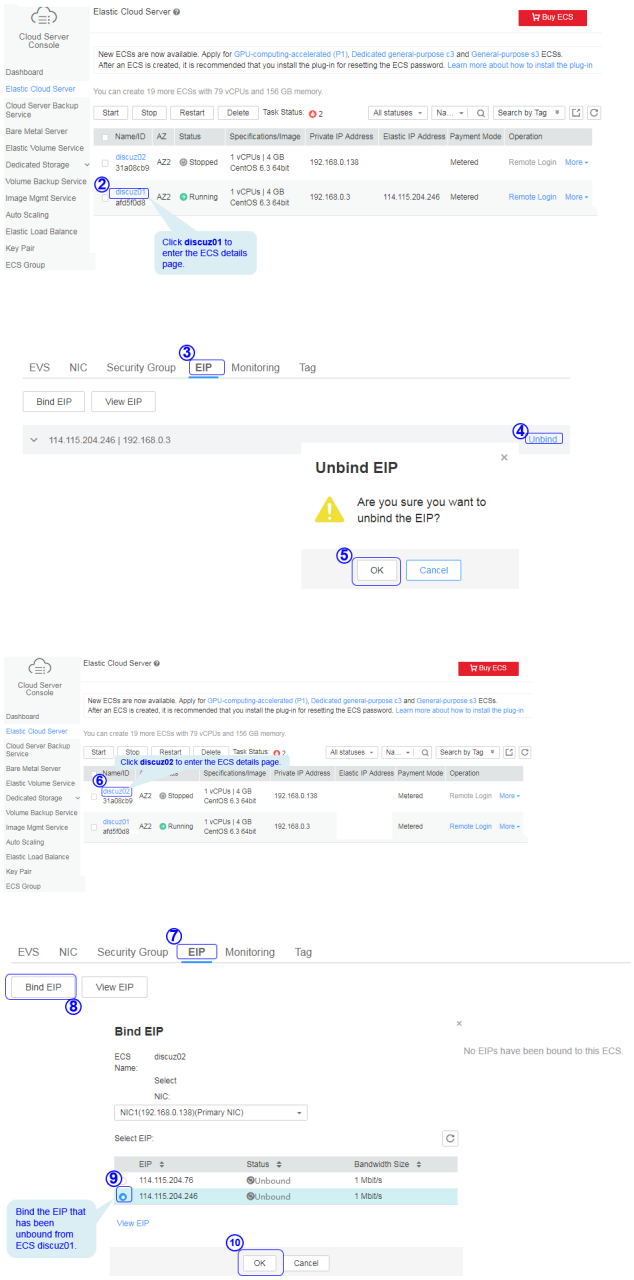
    chkconfig iptables off

Setting Up the Web Environment



Install the web environment.

1. Unbind the EIP from ECS discuz01 and bind it to ECS discuz02.



2. Log in to ECS discuz02 remotely and enter the username and password. For details, see the operations for logging in to ECS discuz01.
3. Run the following command to install the Apache server, PHP FastCGI manager, MySQL client, and MySQL database server:

   yum install -y httpd php php-fpm mysql mysql-server php-mysql

   If the following information is displayed, the installation is successful.

   ```
   Complete!
   ```

4. Run the following command to reinstall the Apache server, PHP FastCGI manager, MySQL client, and MySQL database server:

   yum reinstall -y httpd php php-fpm mysql mysql-server php-mysql

   If the following information is displayed, the installation is successful.

   ```
   Complete!
   ```

Configure the web environment.

1. Run the following command to start the httpd service:

   service httpd start

2. Run the following command to enable the httpd service to automatically start upon system boot:

   chkconfig httpd on

3. Run the following command to start the php-fpm service:

   service php-fpm start

4. Run the following command to enable the php-fpm service to automatically start upon system boot:

   chkconfig php-fpm on

5. Run the following command to disable the firewall:

   service iptables stop

6. Run the following command to permanently disable the firewall after restarting the ECS:

   chkconfig iptables off

7. Run the following command to start the MySQL service:

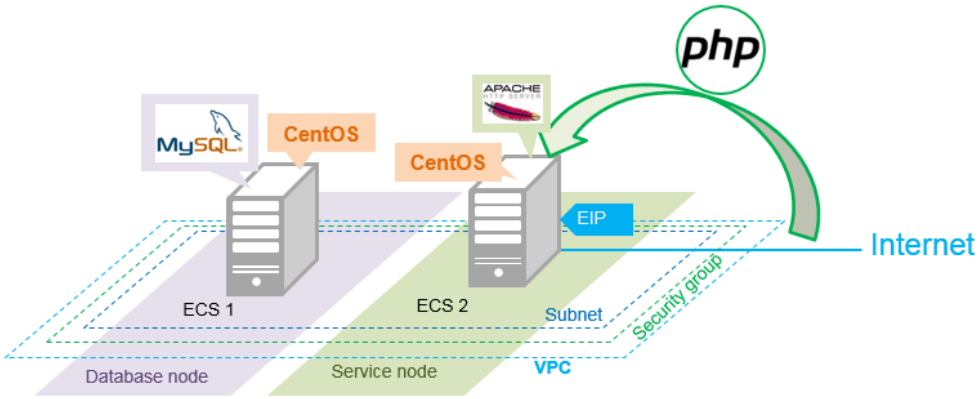
   service mysqld start

8. Run the following command to enable the MySQL service to start upon system boot.

   chkconfig mysqld on

9. Enter **http://***EIP* in a browser to query the default page of the ECS.

Deploying the Website Code



1. Log in to ECS discuz02 remotely and run the following command to install the Discuz software:

   wget http://download.comsenz.com/DiscuzX/3.3/Discuz_X3.3_SC_UTF8.zip

   NOTE

   - The recommended English version of Discuz X3.3 (UTF-8) is not free. Refer to the provided page for payment details.
   - The software packages are only used to construct the forum. To deploy a commercial website, download the applications as needed.

2. Run the following command to decompress the Discuz installation package:

   unzip Discuz_X3.3_SC_UTF8.zip

3. Run the following command to copy all files in the decompressed upload folder to the **var/www/html** directory:

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

4. Run the following command to grant write permissions to other users.

   chmod -R 777 /var/www/html

5. Enter **http://***EIP* in the address box and install Discuz following the guidance.

   a. Confirm the agreement and click **I Agree**.

   b. After the installation starts, check the installation environment and click **Next**.

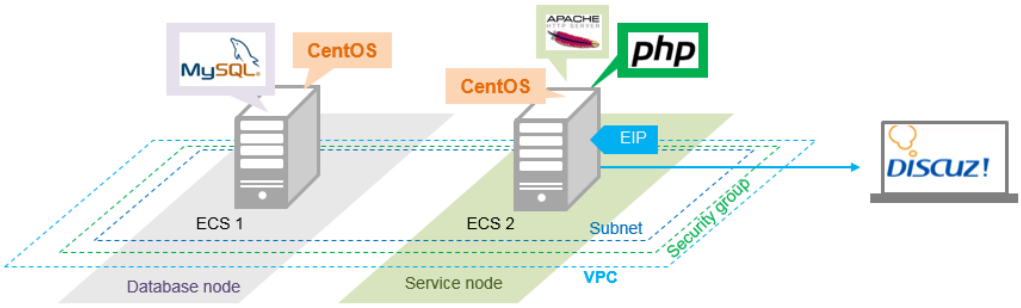
   c. Set the running environment and click **Next**.

   d. Enter the database information and click **Next** to complete the installation.

      - The database address is the private IP address of discuz01.
      - The database password is the password of the database administrator account (username **root**) configured on discuz01.
      - The administrator information is required.

Verifying the Website

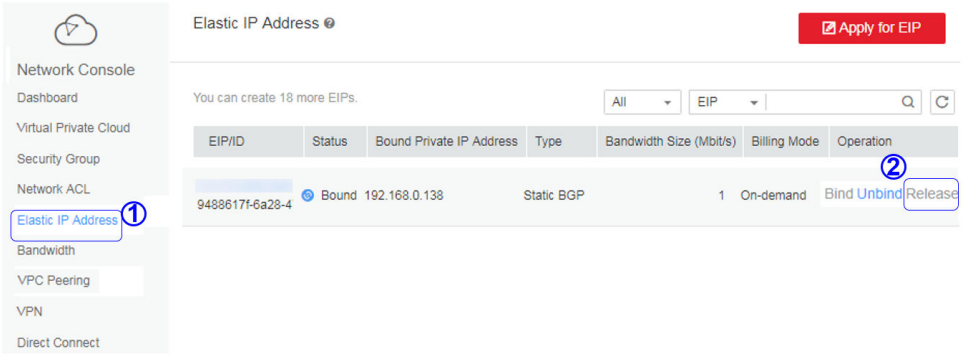
In the browser address bar, enter **http://*EIP*/forum.php**. If the forum homepage is displayed, the website is successfully built.



6.4 Configuring Features

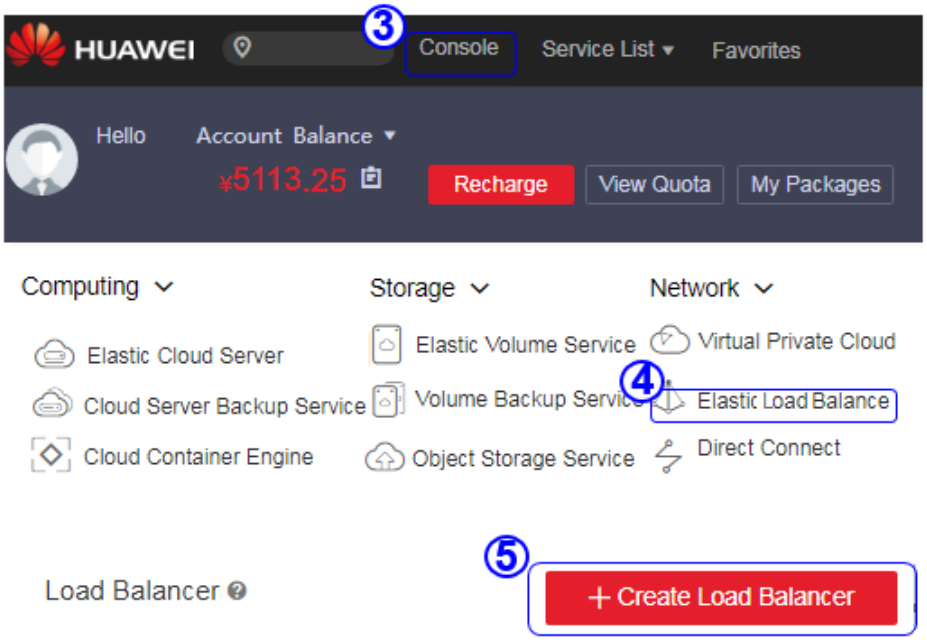
Unbinding the EIP

An EIP can be bound to only one resource. If you create a load balancer on a public network, the system will automatically bind an EIP to the load balancer. To ensure that an EIP can be bound to the load balancer, unbind the EIP bound to the ECS before you create the load balancer if you have only one EIP.

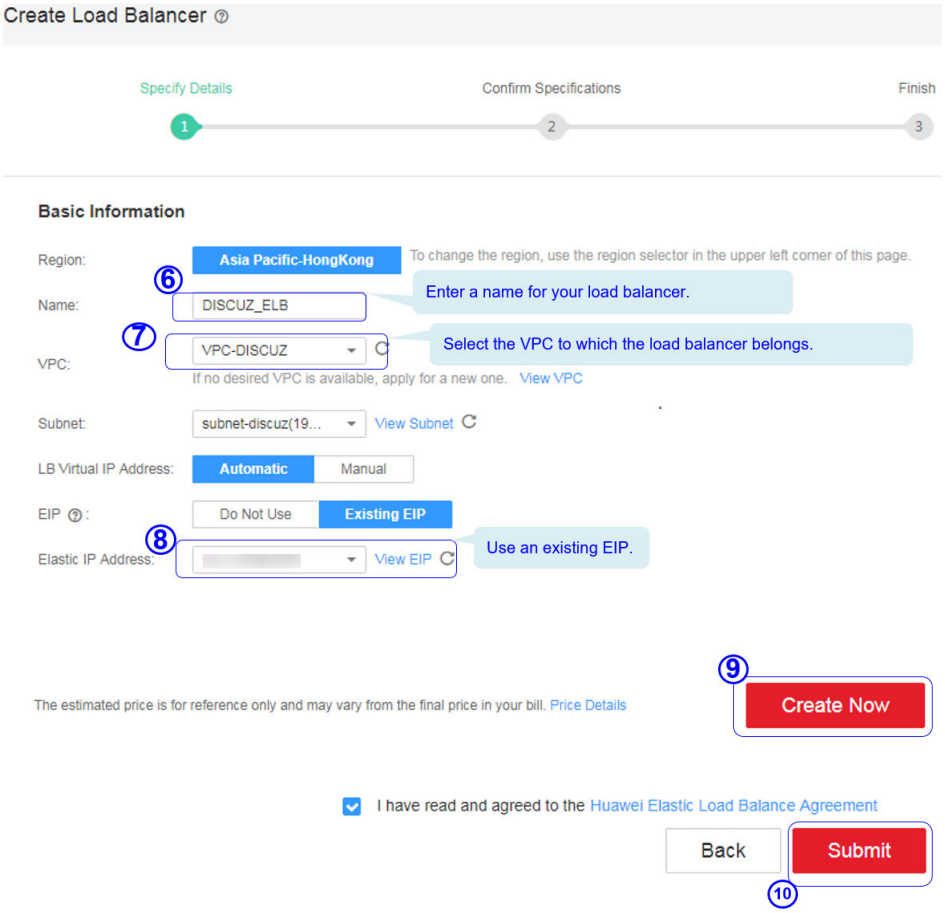


Creating a Load Balancer

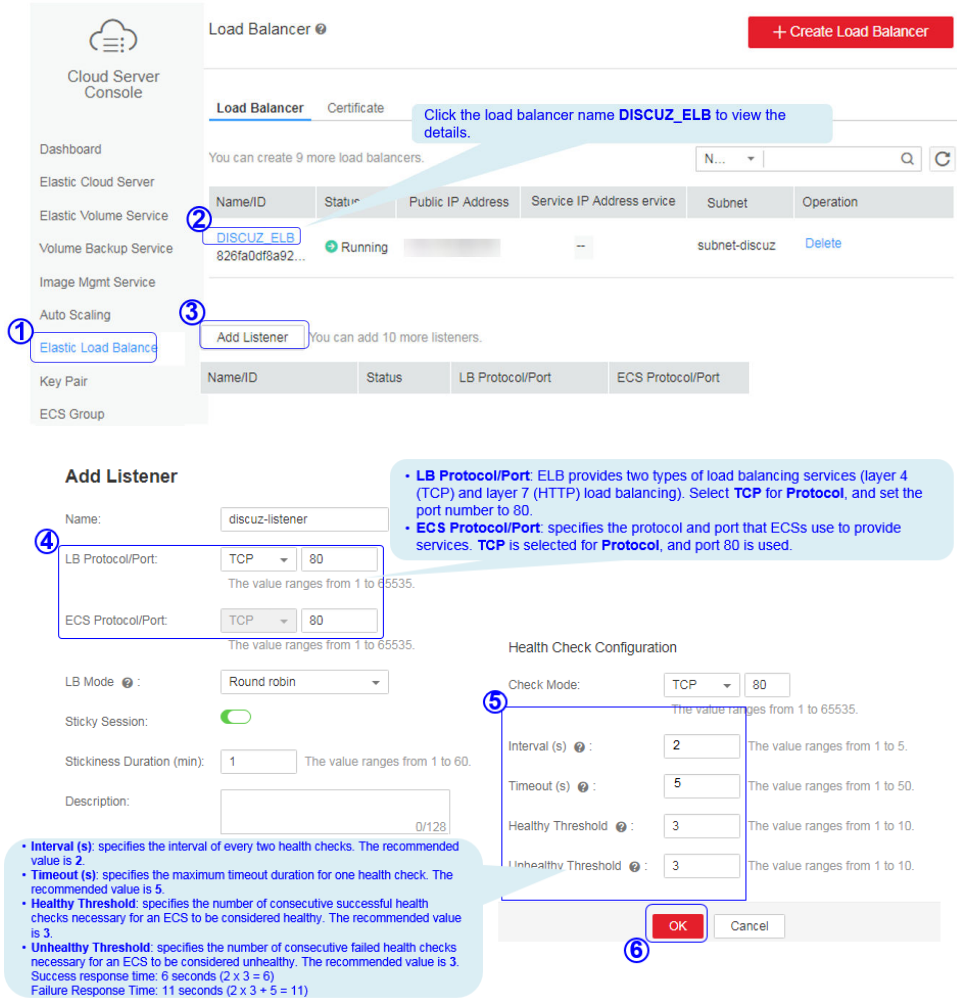
1. On the displayed page, click **Create Load Balancer**.



2. Specify the parameters and submit the application.

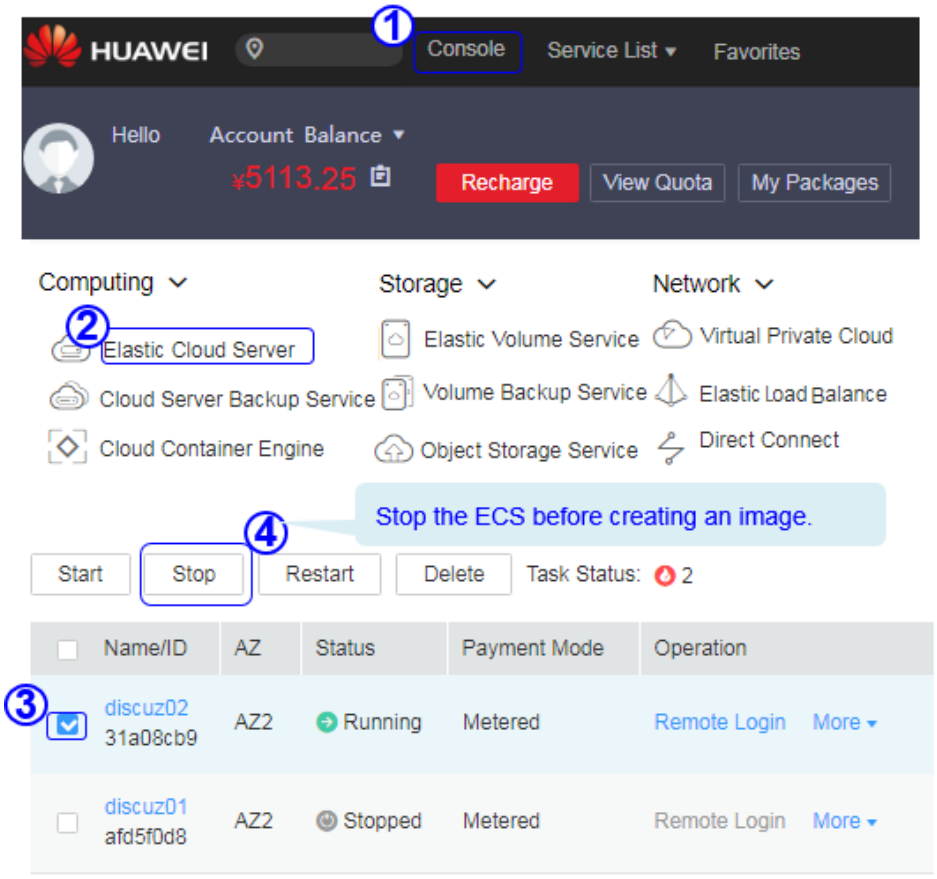


Configuring the Load Balancer

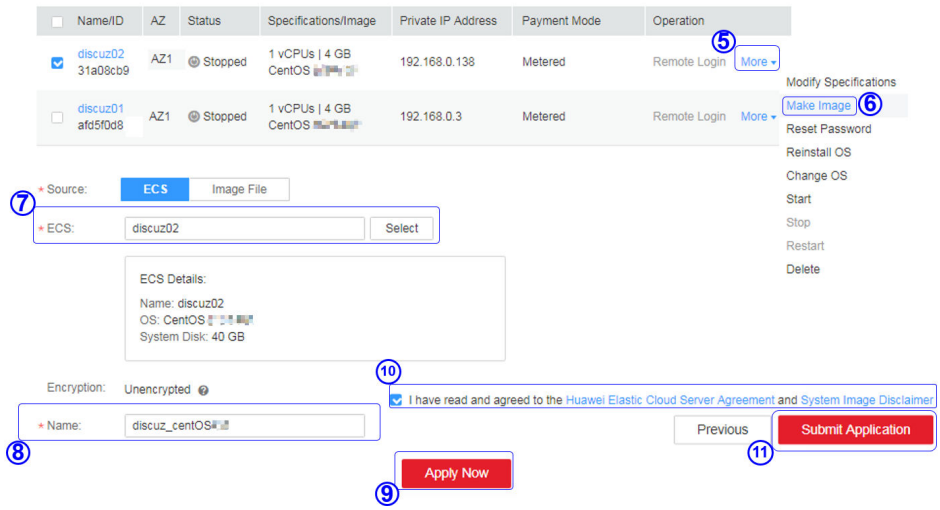


Creating Images

1. Under **Computing**, click **Elastic Cloud Server**. On the page that is displayed, locate and stop the ECS.

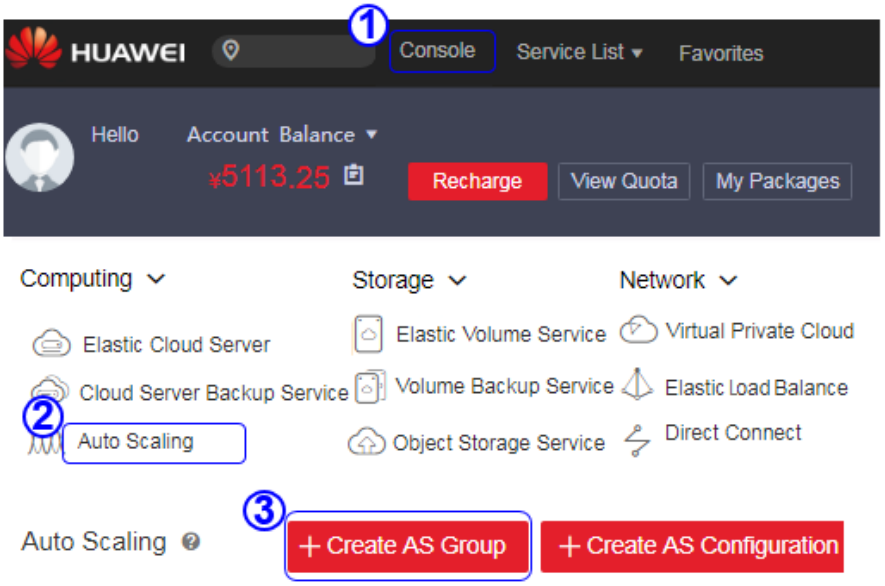


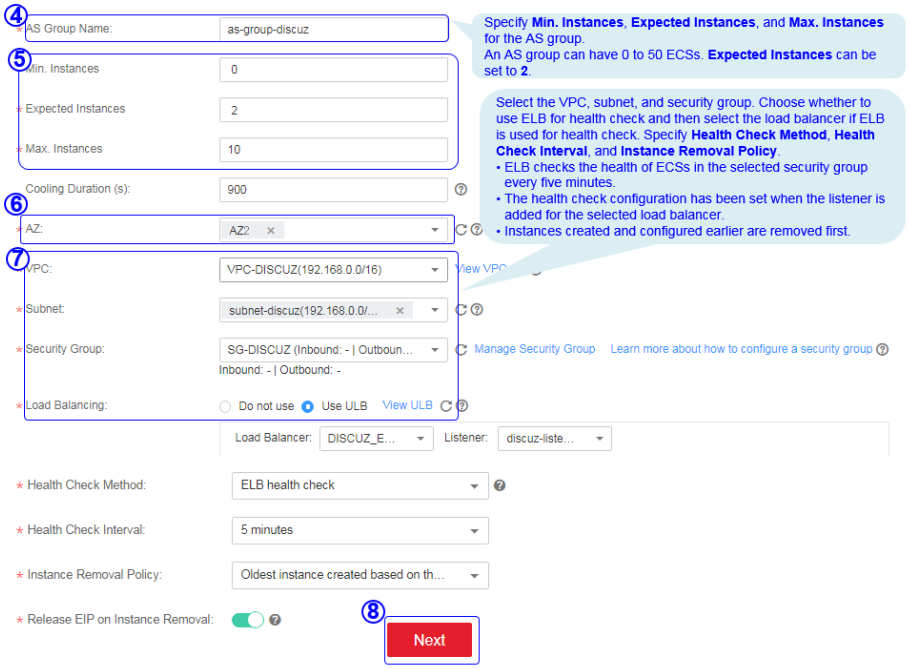
2. Configure the parameters and submit your request.

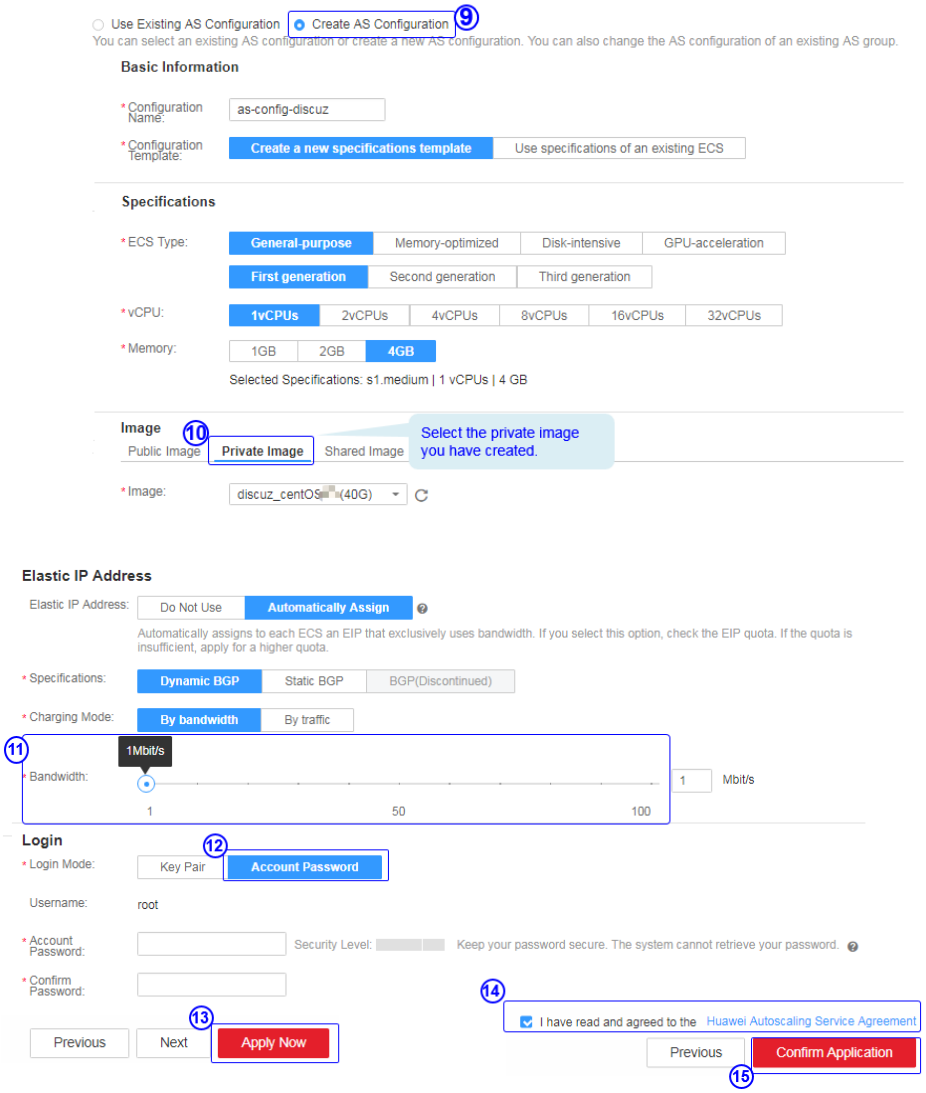


Configuring AS

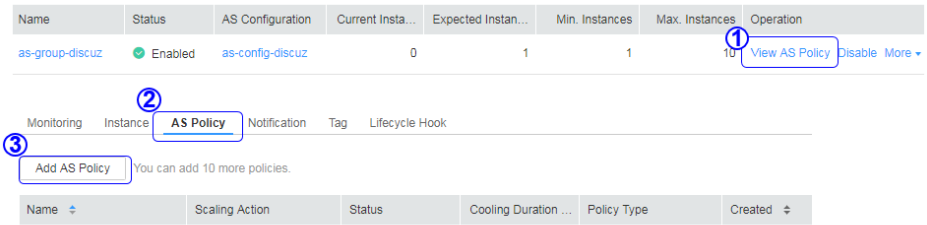
1. Under **Computing**, click **Auto Scaling**. Create an AS group and AS configuration.

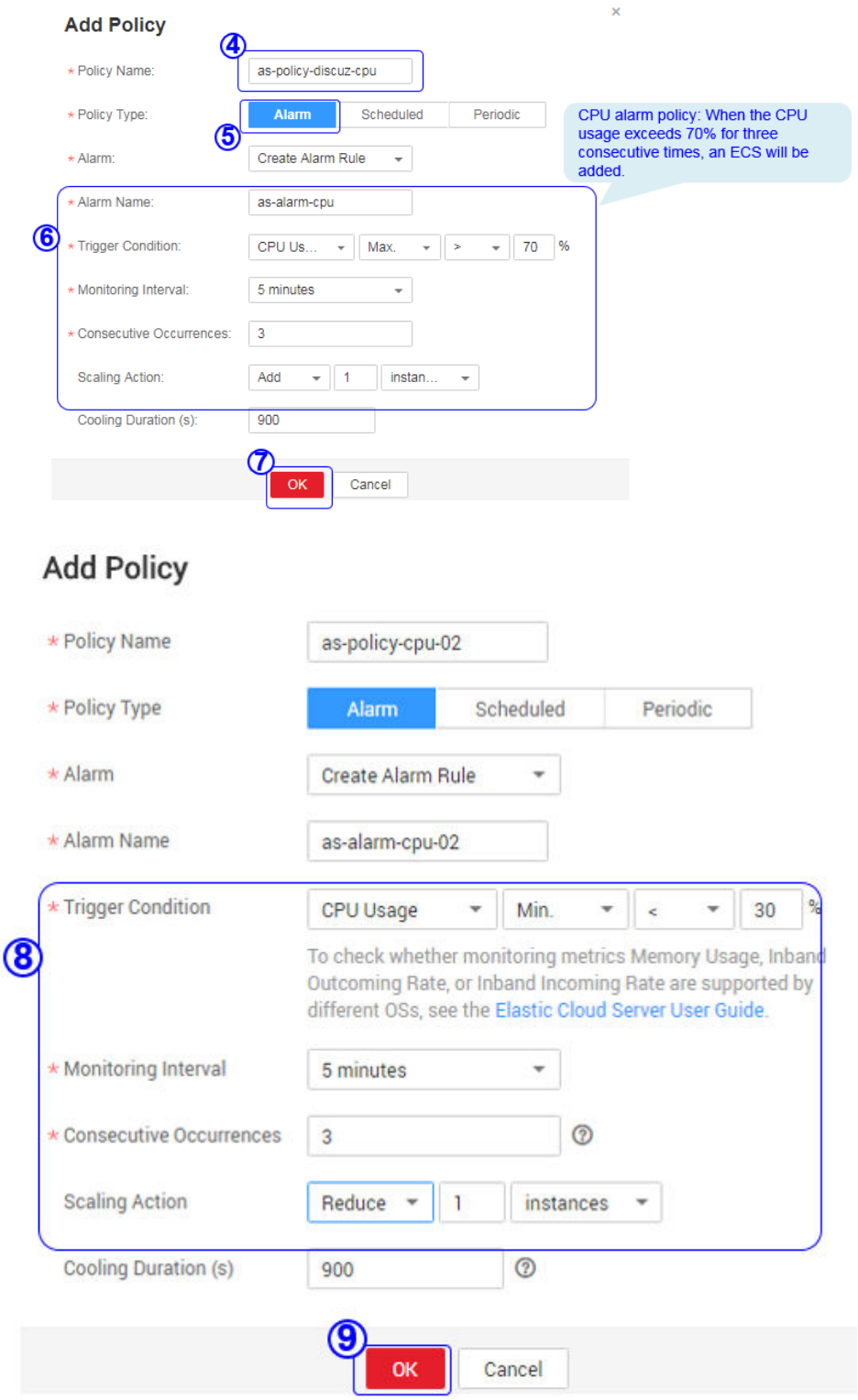




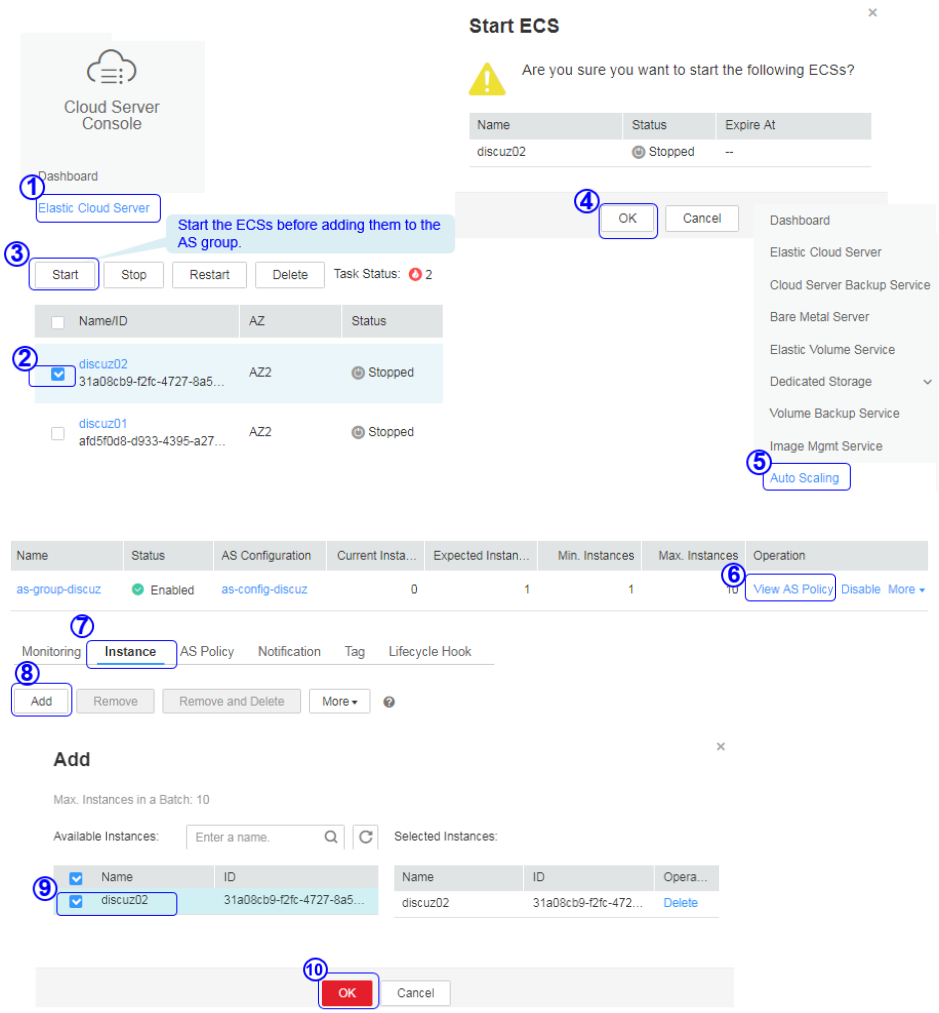


2. Configure AS policies.

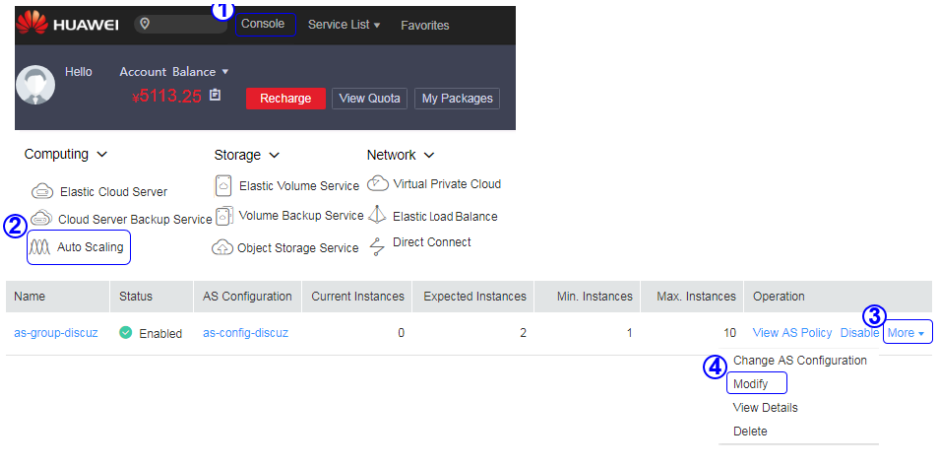


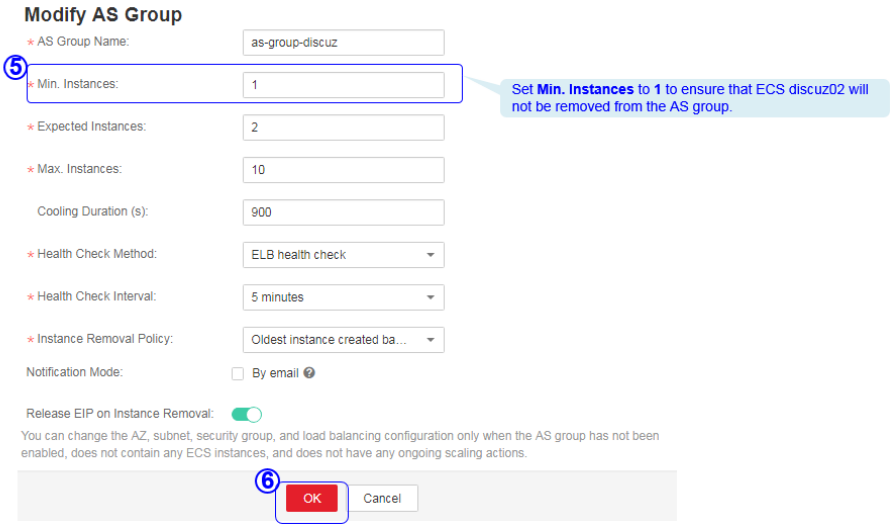


3. Add AS instances.



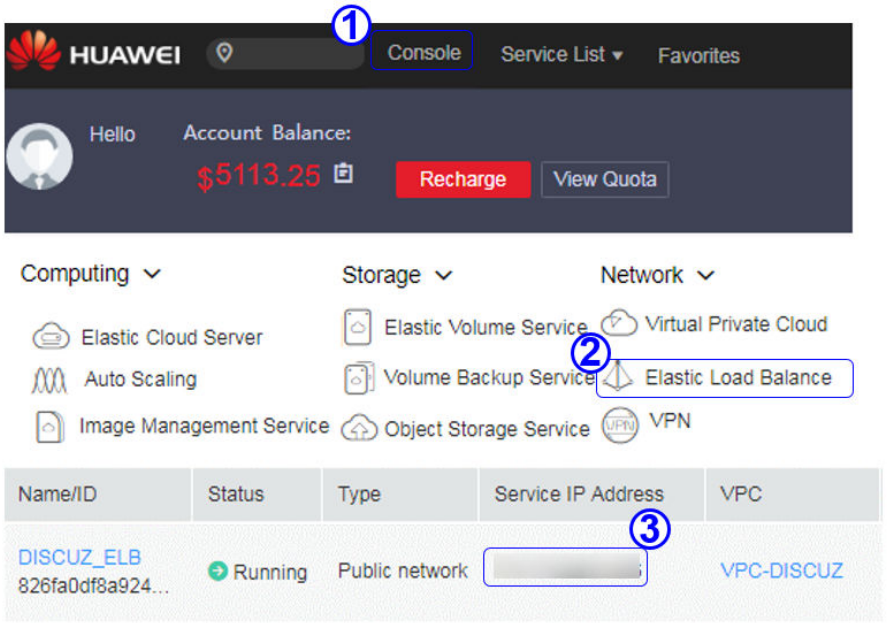
4. Modify AS policies.





Verifying the Configuration

1. Obtain the EIP of the load balancer.



2. In the browser address box, enter **http://***EIP of the load balancer*/**forum.php** to access the website, for example, **http://114.115.138.223/forum.php**.

6.5 Visiting the Website

Filing the Website

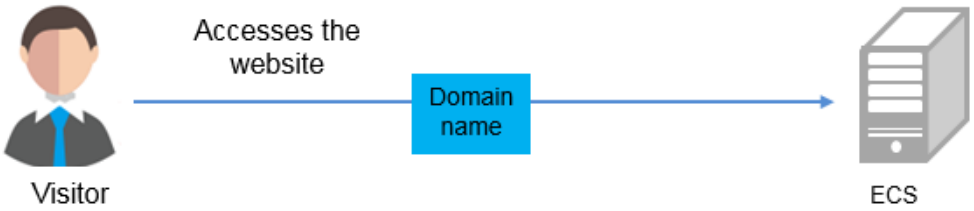
According to national regulations, if the servers used to deploy the website are located in the Chinese mainland, Internet Content Provider (ICP) licensing is required. The domain name that is not licensed cannot be used to access the website.

The prerequisites for ICP licensing are as follows:

- The domain name has been registered.
- Ensure that the IP address is possessed by Huawei.
- The website is a non-operating one.

Accessing the Website

Visitors can access the Internet using the domain name.



7 Manually Deploying WordPress (Linux)

Overview

The best practices for ECS guide you through the setup of an LNMP website on a Linux ECS and deploy WordPress on the website. WordPress (WP for short) is initially a blog system and gradually evolved to a content management system (CMS) or website setup system that is free of charge. The CentOS 7.2 64bit OS is used as an example in this section.

The process is as follows:

1. **Install Nginx.**
2. **Install MySQL.**
3. **Install PHP.**
4. **Test the LNMP website.**
5. **Create a database.**
6. **Install WordPress.**
7. **Purchase a domain name.**
8. **Obtain an ICP license.**
9. **Enable domain name resolution.**

Prerequisites

- A VPC and an EIP are available.
- A domain name is available if you plan to configure a domain name for the website.
- The rule listed in the following table has been added to the security group to which the target ECS belongs. For details, see **Configuring Security Group Rules**.

Table 7-1 Security group rule

Transfer Direction	Protocol	Port	Source End
Inbound	HTTP(80)	80	0.0.0.0/0

Procedure

Step 1 Install Nginx.

1. Log in to the target ECS.
2. Run the following command to download the Nginx package:

   wget http://nginx.org/packages/centos/7/noarch/RPMS/nginx-release-centos-7-0.el7.ngx.noarch.rpm
3. Run the following command to create the Nginx yum repository:

   rpm -ivh nginx-release-centos-7-0.el7.ngx.noarch.rpm
4. Run the following command to install Nginx:

   yum -y install nginx
5. Run the following commands to start Nginx and configure automatic Nginx enabling upon ECS startup:

   systemctl start nginx

   systemctl enable nginx
6. Check the startup status.

   systemctl status nginx.service
7. Enter http://*IP address of the Nginx server* in the address bar to access Nginx. If the following page is displayed, Nginx has been installed.

   Figure 7-1 Accessing Nginx

Step 2 Install MySQL.

1. Install MySQL.

   wget -i -c http://dev.mysql.com/get/mysql57-community-release-el7-10.noarch.rpm

   yum -y install mysql57-community-release-el7-10.noarch.rpm

   yum -y install mysql-community-server
2. Run the following commands to start MySQL and configure automatic MySQL enabling upon ECS startup:

   systemctl start mysqld

   systemctl enable mysqld
3. Query the running status of MySQL.

   systemctl status mysqld.service

   ```
   [root@ecs-adc3 ~]# systemctl status mysqld.service
   ● mysqld.service - MySQL Server
   ```



```
  Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; vendor preset: disabled)
  Active: active (running) since Mon 2021-08-16 19:33:40 CST; 36s ago
    Docs: man:mysqld(8)
          http://dev.mysql.com/doc/refman/en/using-systemd.html
 Main PID: 7916 (mysqld)
  CGroup: /system.slice/mysqld.service
          └─7916 /usr/sbin/mysqld --daemonize --pid-file=/var/run/mysqld/mysqld.pid

Aug 16 19:33:35 ecs-adc3 systemd[1]: Starting MySQL Server...
Aug 16 19:33:40 ecs-adc3 systemd[1]: Started MySQL Server.
```

4. Run the following command to obtain the password of user **root** that is automatically set during MySQL installation:

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

   Information similar to the following is displayed:

   ```
   2021-08-16T11:33:37.790533Z 1 [Note] A temporary password is generated for root@localhost: ;
   8nPd29lhs,k
   ```

5. Run the following command and perform operations as prompted to harden MySQL:

   mysql_secure_installation

   ```
   Securing the MySQL server deployment.

   Enter password for user root:    #Enter the obtained password of user root.
   The existing password for the user account root has expired. Please set a new password.

   New password:  #Enter the new password.

   Re-enter new password:   #Enter the new password again.
   The 'validate_password' plugin is installed on the server.
   The subsequent steps will run with the existing configuration of the plugin.
   Using existing password for root.

   Estimated strength of the password: 100
   Change the password for root ? ((Press y|Y for Yes, any other key for No) : N   #Asks you whether to
   change the password of user root. Press n.

    ... skipping.
   By default, a MySQL installation has an anonymous user,
   allowing anyone to log into MySQL without having to have
   a user account created for them. This is intended only for
   testing, and to make the installation go a bit smoother.
   You should remove them before moving into a production
   environment.

   Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y   #Asks you whether to
   remove anonymous users. Press 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   #Asks you whether to
   forbid remote login of user root. Press y.
   Success.

   By default, MySQL comes with a database named 'test' that anyone can access. This is also intended
   only for testing, and should be removed before moving into a production environment.

   Remove test database and access to it? (Press y|Y for Yes, any other key for No) : Y   #Asks you
   whether to delete the test database and cancel access permissions to it. Press y.
    - Dropping test database...
   Success.

    - Removing privileges on test database...
   Success.
   ```



```
Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : Y   #Asks you whether to reload privilege tables. Press y.
Success.

All done!
```

Step 3 Install PHP.

1. Run the following commands to install PHP 7 and PHP extensions required for installing LNMP:

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

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

   yum -y install php70w-tidy php70w-common php70w-devel php70w-pdo php70w-mysql php70w-gd php70w-ldap php70w-mbstring php70w-mcrypt php70w-fpm

2. Run the following command to check the PHP installation:

   php -v

   If information similar to the following is displayed, PHP has been installed:

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

3. Run the following commands to start PHP and configure automatic PHP enabling upon ECS startup:

   systemctl start php-fpm

   systemctl enable php-fpm

4. Modify the Nginx configuration file to support PHP.

   a. Run the following command to open the **/etc/nginx/nginx.conf** file:

      vim /etc/nginx/nginx.conf

   b. Press **i** to enter editing mode.

   c. Modify the **nginx.conf** file.

      Find the **server** paragraph and modify the following configuration information:

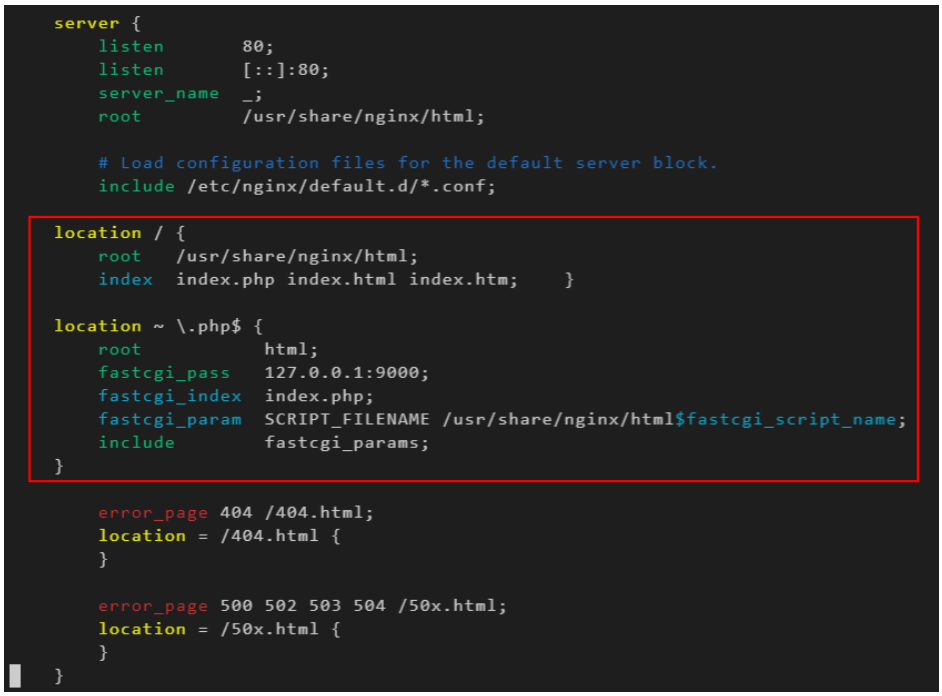
      ```
      server {
          listen       80;
          listen       [::]:80;
          server_name  _;
          root         /usr/share/nginx/html;

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

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

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

          error_page 404 /404.html;
      ```



```
    location = /404.html {
    }

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

Figure 7-2 shows the configuration after modification.

Figure 7-2 Configuration after modification



d. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the configuration file.

5. Run the following command to reload the Nginx configuration file:

   service nginx reload

Step 4 Test the LNMP website.

1. Create the **info.php** test page in **/usr/share/nginx/html**.

   a. Run the following command to create and open the **info.php** test file:

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

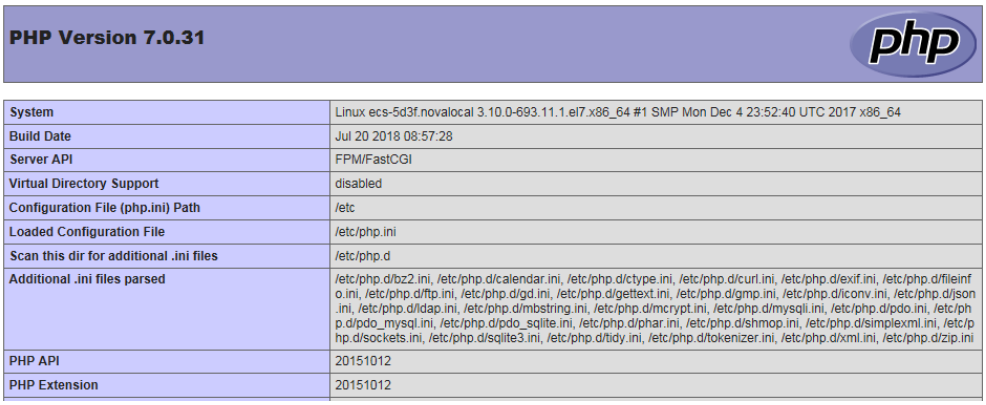
   b. Press **i** to enter editing mode.

   c. Modify the **info.php** file and add the following data to the file:

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

   d. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the configuration file.

2. Enter http://*Server IP address*/info.php in the address bar. If the following page is displayed, the LNMP website has been set up.



PHP Version 7.0.31

System	Linux ecs-5d3f.novalocal 3.10.0-693.11.1.el7.x86_64 #1 SMP Mon Dec 4 23:52:40 UTC 2017 x86_64
Build Date	Jul 20 2018 08:57:28
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/bz2.ini, /etc/php.d/calendar.ini, /etc/php.d/ctype.ini, /etc/php.d/curl.ini, /etc/php.d/exif.ini, /etc/php.d/fileinfo.ini, /etc/php.d/ftp.ini, /etc/php.d/gd.ini, /etc/php.d/gettext.ini, /etc/php.d/gmp.ini, /etc/php.d/iconv.ini, /etc/php.d/json.ini, /etc/php.d/ldap.ini, /etc/php.d/mbstring.ini, /etc/php.d/mcrypt.ini, /etc/php.d/mysqli.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/shmop.ini, /etc/php.d/simplexml.ini, /etc/php.d/sockets.ini, /etc/php.d/sqlite3.ini, /etc/php.d/tidy.ini, /etc/php.d/tokenizer.ini, /etc/php.d/xml.ini, /etc/php.d/zip.ini
PHP API	20151012
PHP Extension	20151012

Step 5 Create a database.

1. Run the following command and enter the user **root** password of MySQL as prompted to log in to the MySQL CLI:

   mysql -u root -p

2. Run the following command to create a new database:

   CREATE DATABASE *wordpress*;

   In the preceding command, *wordpress* is the database name, which is configurable.

3. Run the following command to create a user for the database and assign the full-access permission to the user:

   GRANT ALL ON *wordpress*.* **TO** *wordpressuser*@localhost **IDENTIFIED BY** '*BLOck@123*';

   In the preceding command, *wordpressuser* is the username for logging in to the database, and *BLOck@123* is the configurable user password.

4. Run the following command to exit the MySQL CLI:

   exit

5. (Optional) Run the following commands to verify the creation of the database and account and exit the MySQL CLI:

   mysql -u *wordpressuser* **-p**

   SHOW DATABASES;

   exit

   In the preceding command, *wordpressuser* is the created username for logging in to the database.

Step 6 Install WordPress.

1. Obtain the WordPress software package and upload it to the **/usr/share/nginx/html** directory.

   The WordPress software package **wordpress-4.9.8.tar.gz** is used as an example.

2. Run the following command to decompress the software package:

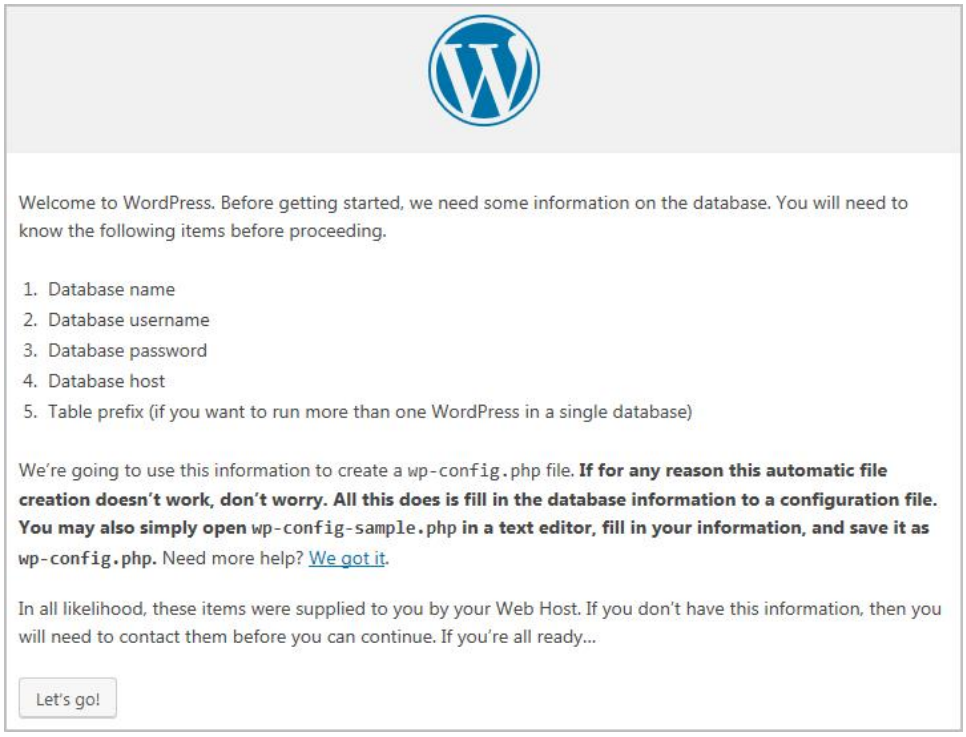
   tar -xvf wordpress-4.9.8.tar.gz

   After the decompression, the folder **wordpress** is obtained.

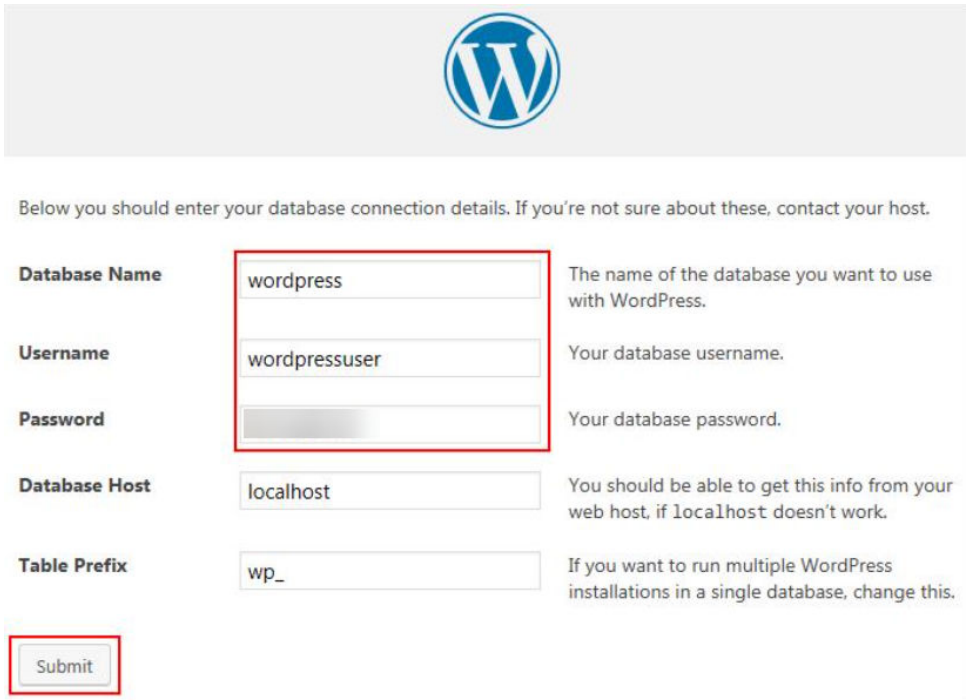
3. Run the following command to assign permissions to the **wordpress** folder:

   chmod -R 777 wordpress

4. Enter http://*Server IP address*/wordpress in the address bar of the browser to access the installation wizard.

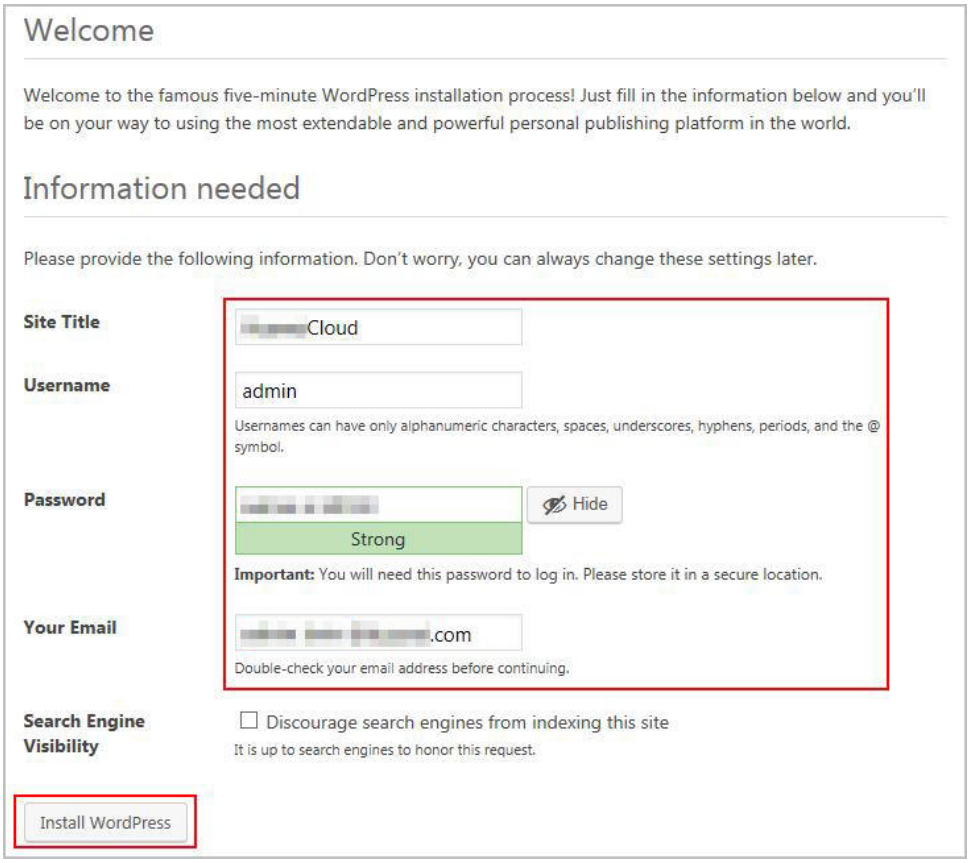


5. Configure the database as prompted and click **Let's go**.
6. Enter the database access information, including the database name, username, and password.

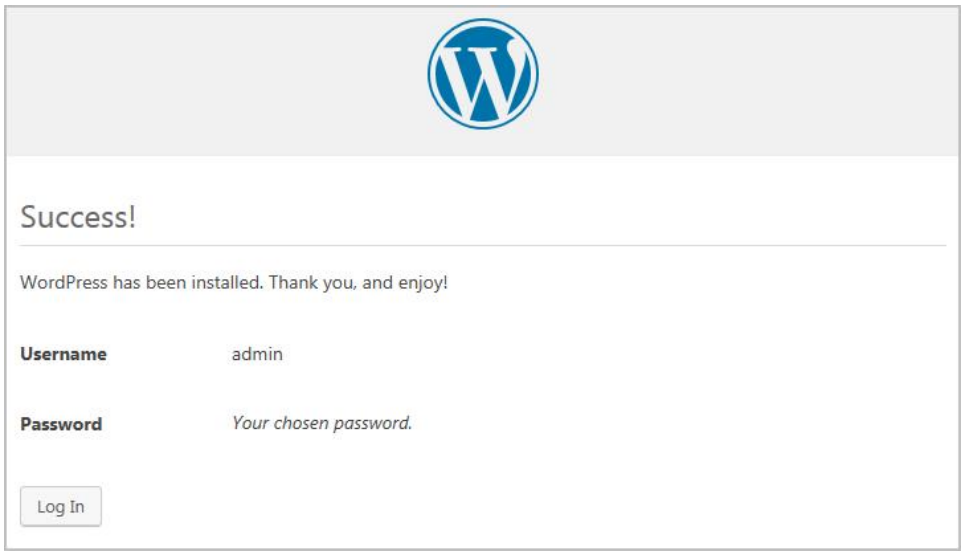


7. After the verification, the installation page is displayed. Then, click **Run the installation**.

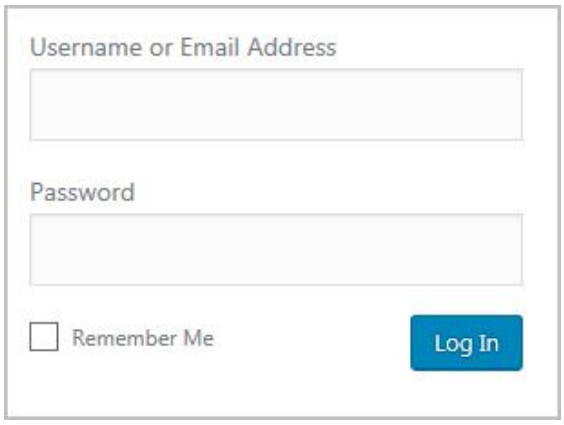
8. Set the site title, administrator username, password, and email address. Then, click **Install WordPress**.

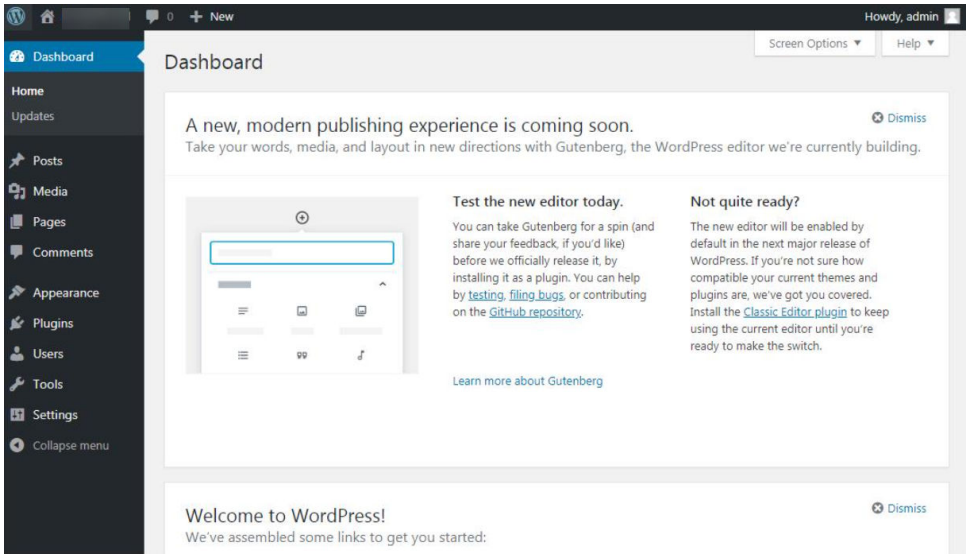


9. Verify that the following page is displayed, indicating that the installation is successful.



10. Click **Log In**. Alternatively, enter http//*Server IP address*/wordpress/wp-admin in the address bar of the browser, enter the username and password, and click **Log In**.





Step 7 Purchase a domain name.

To make the website accessible and usable, configure a unique domain name for the website. You are required to obtain an authorized domain name from the domain name registrar for the website.

Step 8 Obtain an ICP license.

If your website has not obtained an ICP license and needs to be hosted on HUAWEI CLOUD, use the HUAWEI CLOUD ICP license service to obtain a license.

Step 9 Enable domain name resolution.

Your website can be visited using the registered domain name only after domain name resolution is enabled. For details, see **Configuring a Public Zone**.

For example, if the domain name is www.example.com, enter http//www.example.com in the address bar of the browser to access the website.

----End

8 Setting Up an FTP Site (Windows)

Overview

The best practices for ECS guide you through the setup of an FTP site on a Windows ECS. The Windows Server 2012 R2 OS is used as an example in this section.

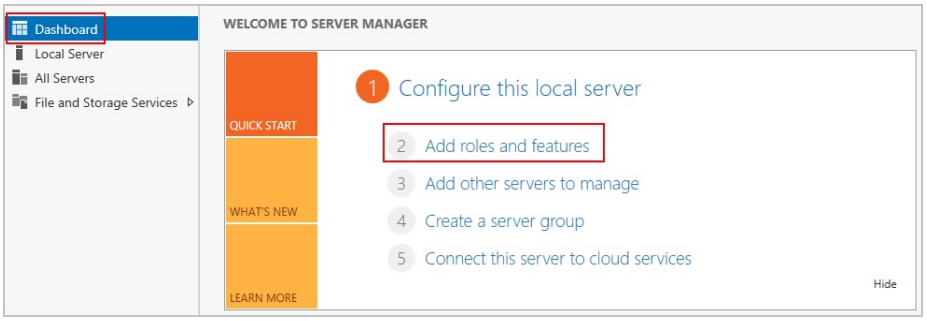
The process is as follows:

1. **Add IIS and FTP service roles.**
2. **Create a username and password.**
3. **Assign permissions to shared files.**
4. **Add and set the FTP site.**
5. **(Optional) Configure the FTP firewall.**
6. **Set the security group and firewall.**
7. **Verify the configuration on the client.**

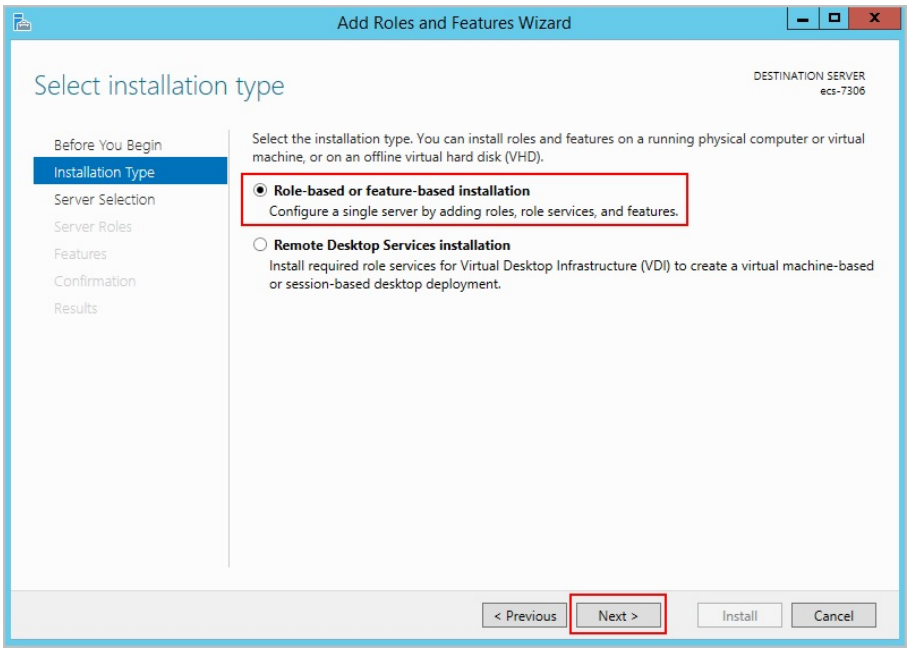
Procedure

Step 1 Add IIS and FTP service roles.

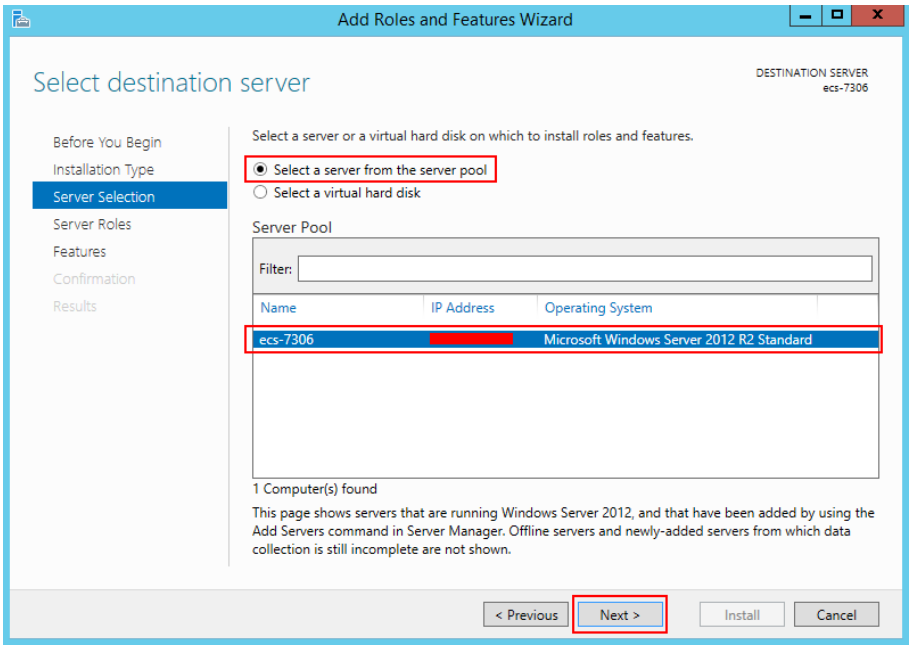
1. Log in to the ECS.
2. Choose **Start** > **Server Manager**.
3. Click **Add roles and features**.



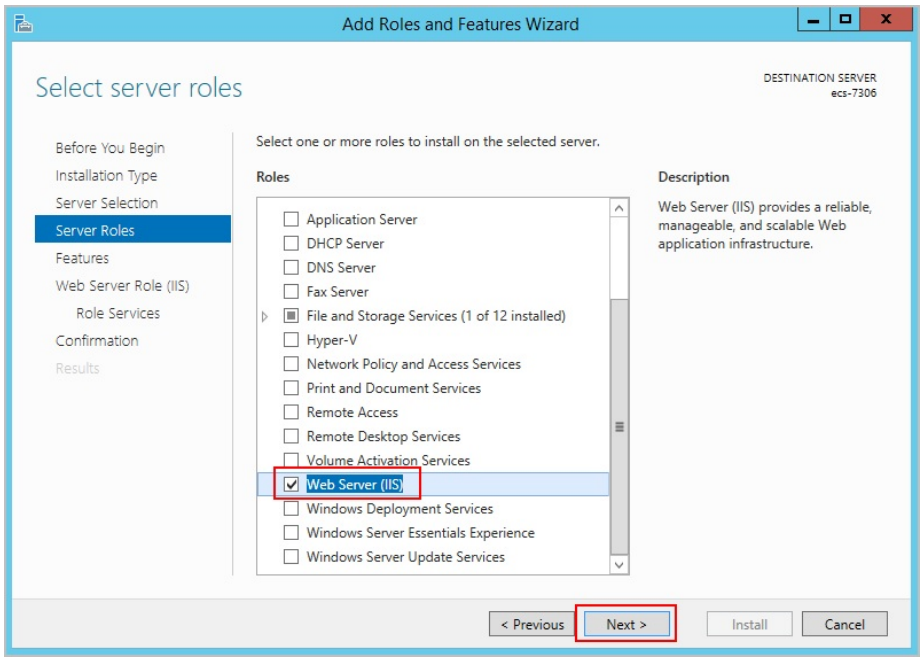
4. In the **Before you begin** dialog box, click **Next**.
5. Select **Role-based or feature-based installation** and click **Next**.

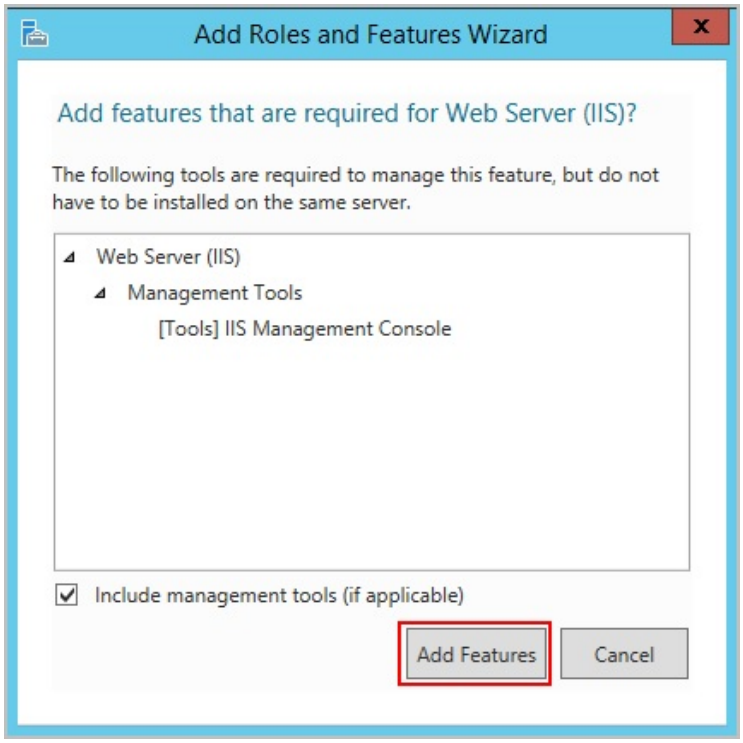


6. Select the ECS where FTP is to be deployed and click **Next**.

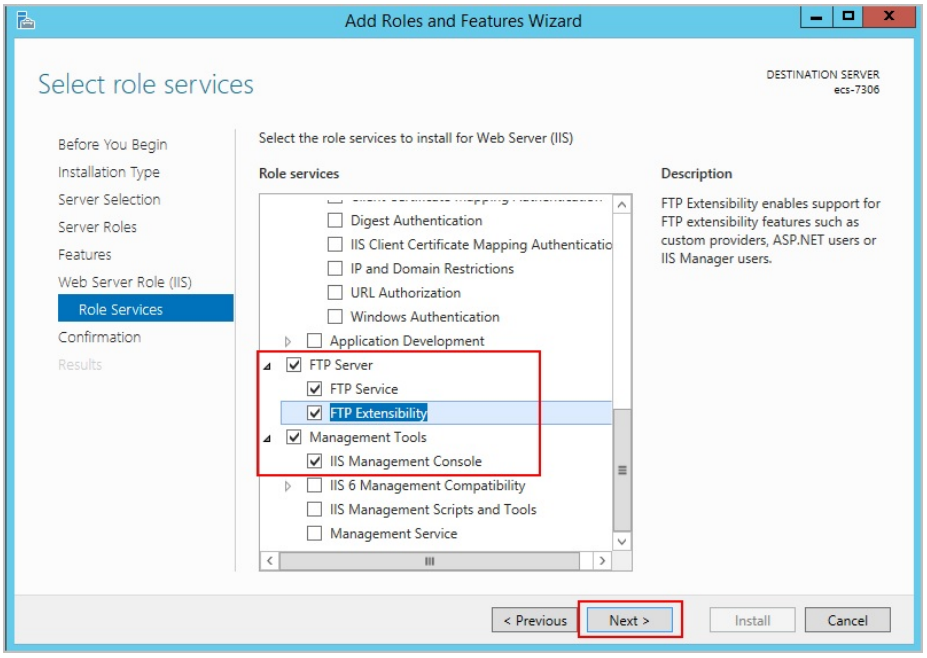


7. Select **Web Server (IIS)**. In the dialog box that is displayed, click **Add Features** and then **Next**.





8. Click **Next** until the **Role Service** page is displayed.
9. Select **FTP Server** and **IIS Management Console**. Then, click **Next**.

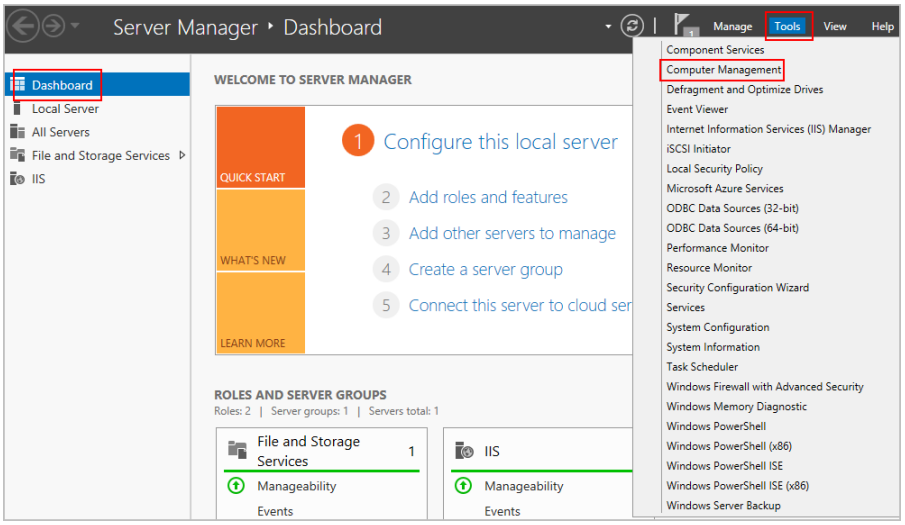


10. Click **Install** to assign the service roles.
11. After the installation is complete, click **Close**.

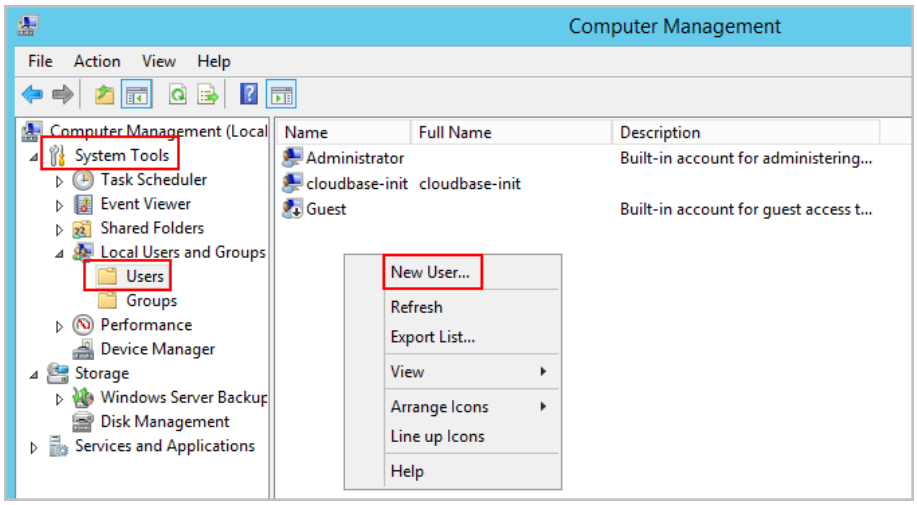
Step 2 Create a username and password.

The Windows username and password are used for FTP. If you allow anonymous users to access FTP, you do not need to create an FTP username and password.

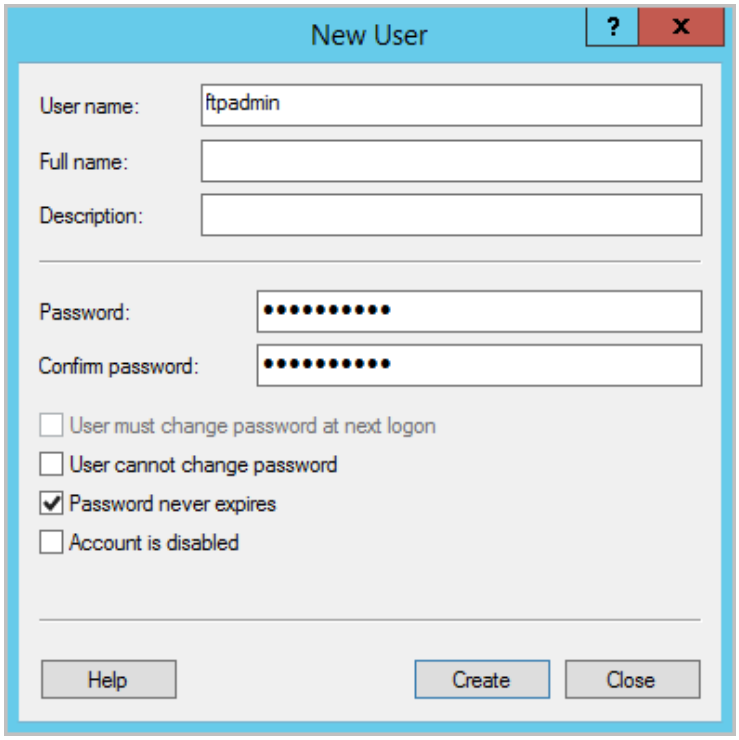
1. In **Server Manager**, choose **Dashboard** > **Tools** > **Computer Manager**.



2. Choose **System Tools** > **Local Users and Groups** > **Users**, right-click the blank area on the right, and choose **New User** from the shortcut menu.



3. Set **User name** (**ftpadmin** is used as an example) and **Password**.



Step 3 Assign permissions to shared files.

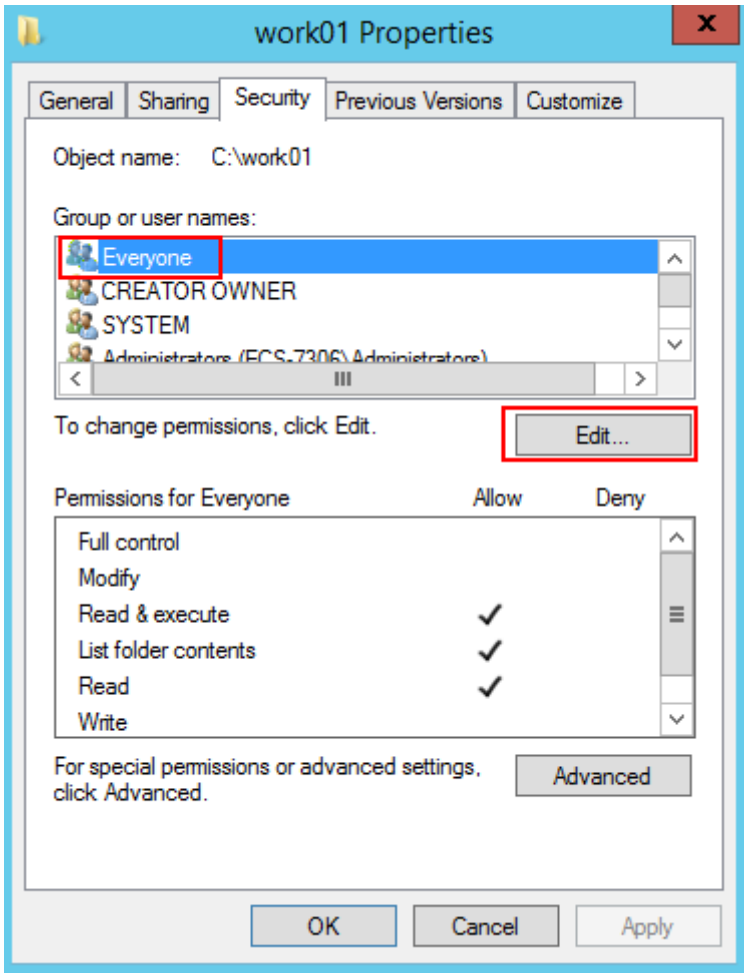
Set access and edit permissions for the files shared to users on the FTP site.

1. Create a folder for FTP on the ECS, right-click the folder, and choose **Properties** from the shortcut menu.

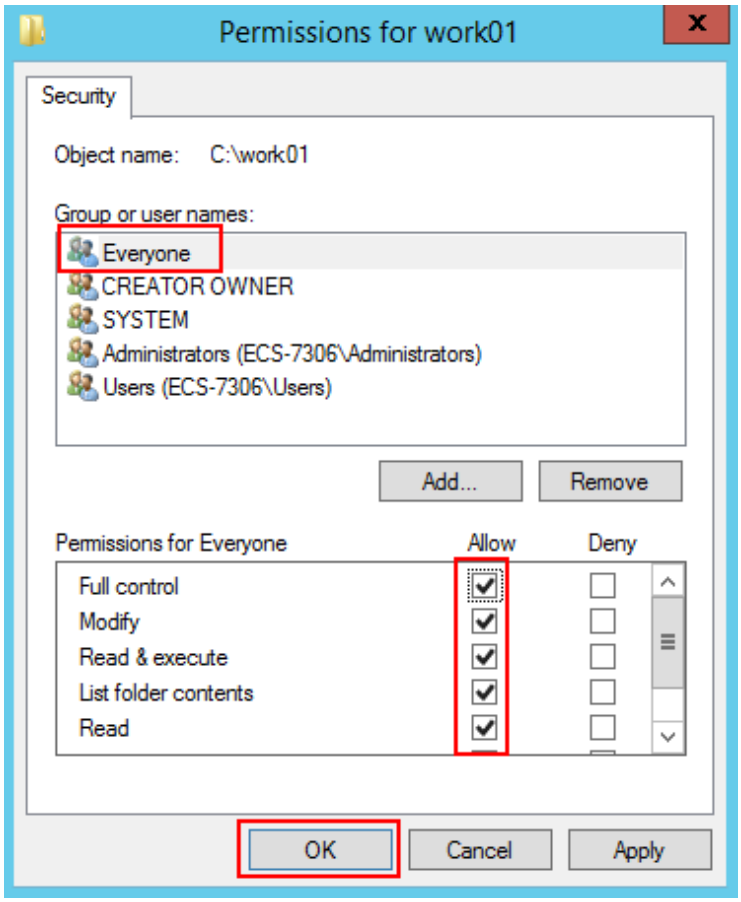
   The **work01** folder is used as an example.

2. On the **Security** tab, select **Everyone** and click **Edit**.

   If **Everyone** is unavailable, add it. For details, see **FAQs**.

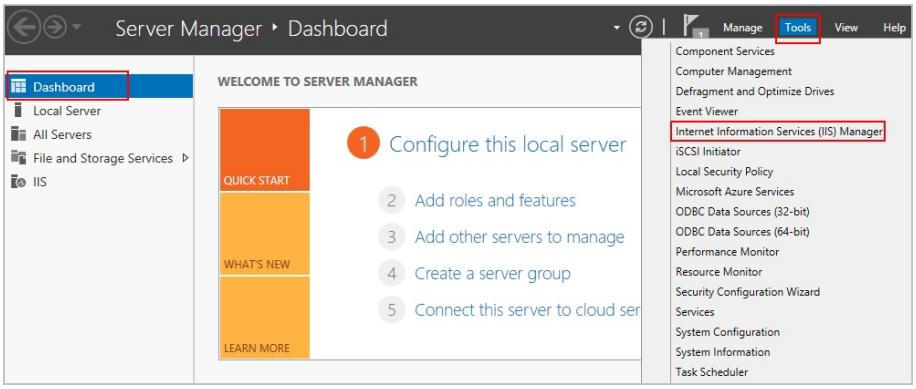


3. Select **Everyone**, assign permissions as needed, and click **OK**.
   In this example, all permissions are allowed.

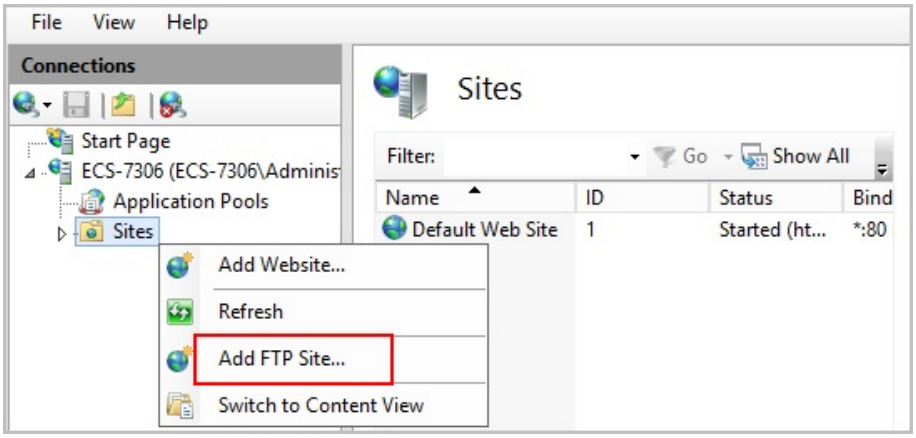


Step 4 Add and set the FTP site.

1. In **Server Manager**, choose **Dashboard** > **Tools** > **Internet Information Services (IIS) Manager**.

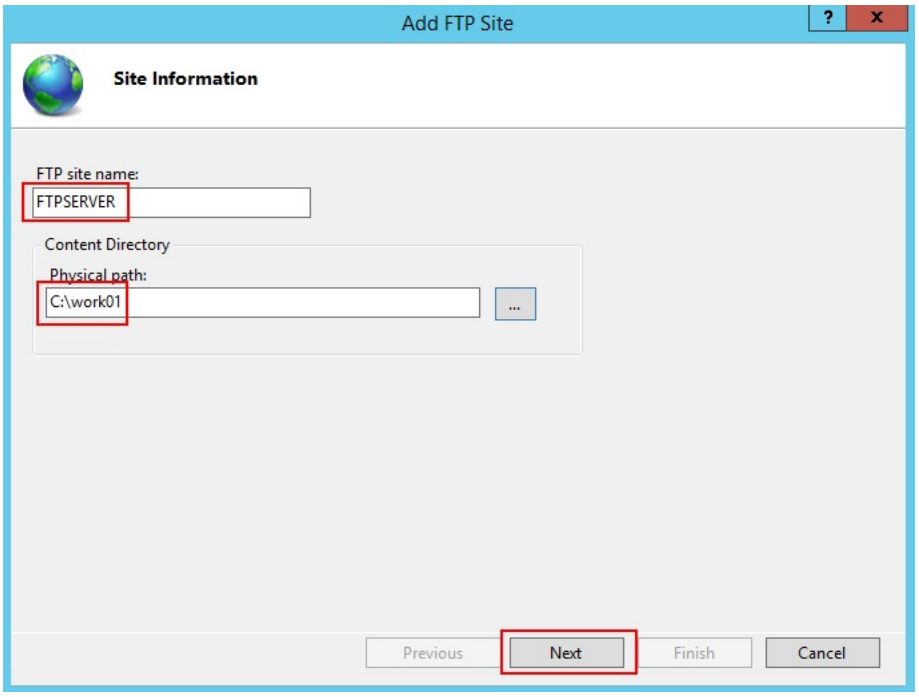


2. Right-click **Sites** and choose **Add FTP Site** from the shortcut menu.



3. In the dialog box that is displayed, set the FTP site name and the physical path in which the shared folder is stored. Then, click **Next**.

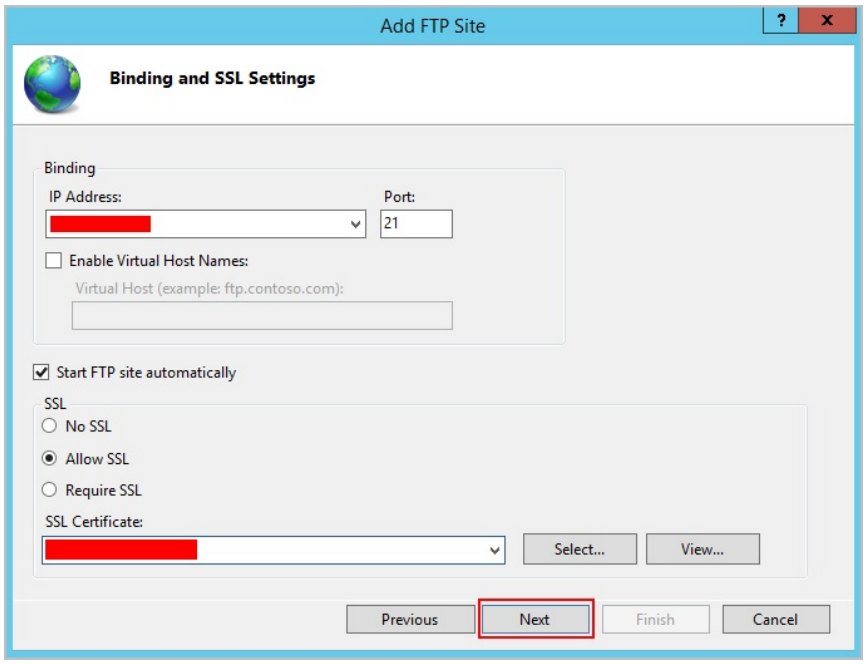
   Site name **FTPSERVER** is used as an example.



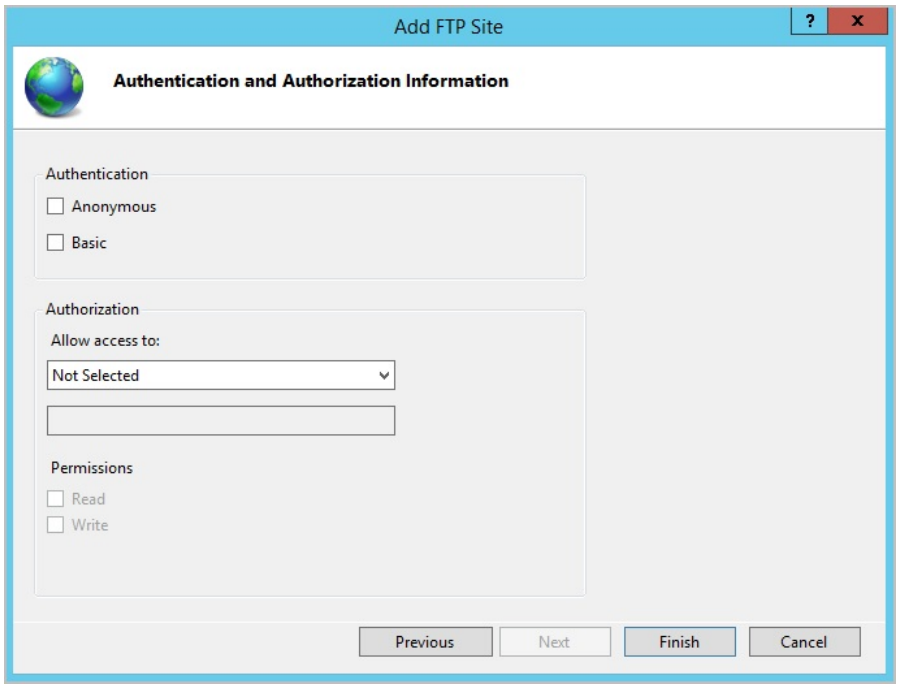
4. Enter the public IP address and port number of the ECS, set SSL, and click **Next**.
   - The default port number is 21. You can set the port number as required.
   - Set SSL as required.
     - **No SSL**: SSL encryption is not required.
     - **Allow SSL**: allows non-SSL and SSL connections between the FTP server and the client.
     - **Required SSL**: SSL encryption is required for the communication between the FTP server and the client.

       NOTE

       When **Allow SSL** and **Require SSL** are selected, select an existing SSL certificate or create one. For details, see **Creating a server certificate**.

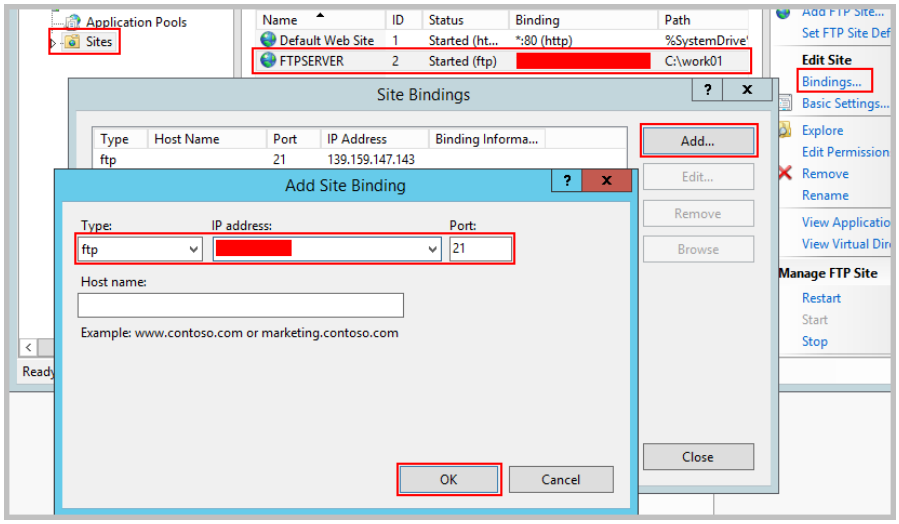


5. Configure authentication and authorization and click **Finish**.
   - Authentication
     - **Anonymous**: allows any user with username **anonymous** or **ftp** to access.
     - **Basic**: allows only users with authorized usernames and passwords to access. However, the passwords transmitted over the network are not encrypted. Therefore, you are advised to use this authentication method after confirming that the network connection between the client and the FTP server is secure.
   - Authorization
     - Allow access to:
       - **All users**: All users are allowed.
       - **Anonymous users**: Anonymous users are allowed.
       - **Specified roles or user groups**: Only specified roles or user group members are allowed. If you select this option, you are required to enter the specified roles or user group in the text box.
       - **Specified users**: Only specified users are allowed. If you select this option, you are required to enter the specified users in the text box.
     - **Permissions**: specifies permissions for the authorized users.



6. Add the private IP address of the ECS to the FTP site.

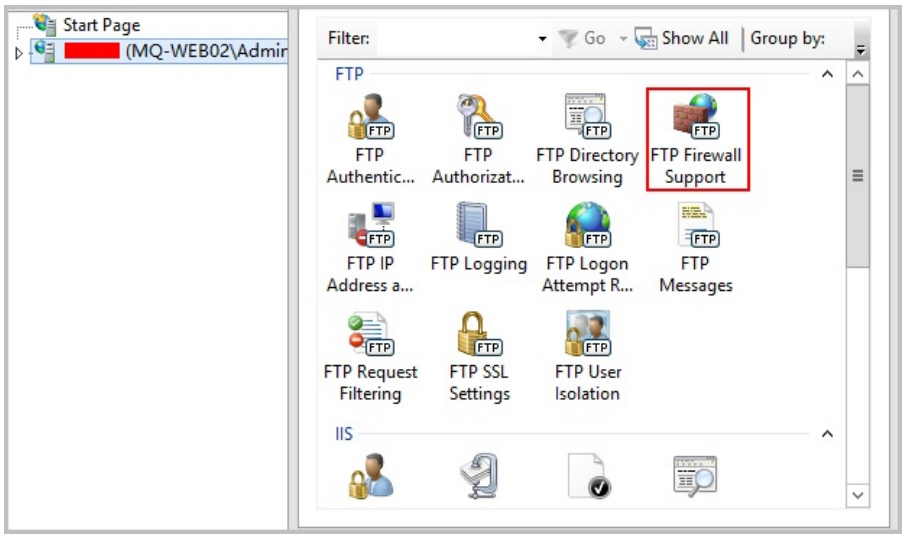
   Choose **Sites**, select the FTP site, and click **Bindings**. In the **Site Bindings** dialog box, click **Add**. Then, add the private IP address of the ECS in the displayed dialog box add click **OK**.



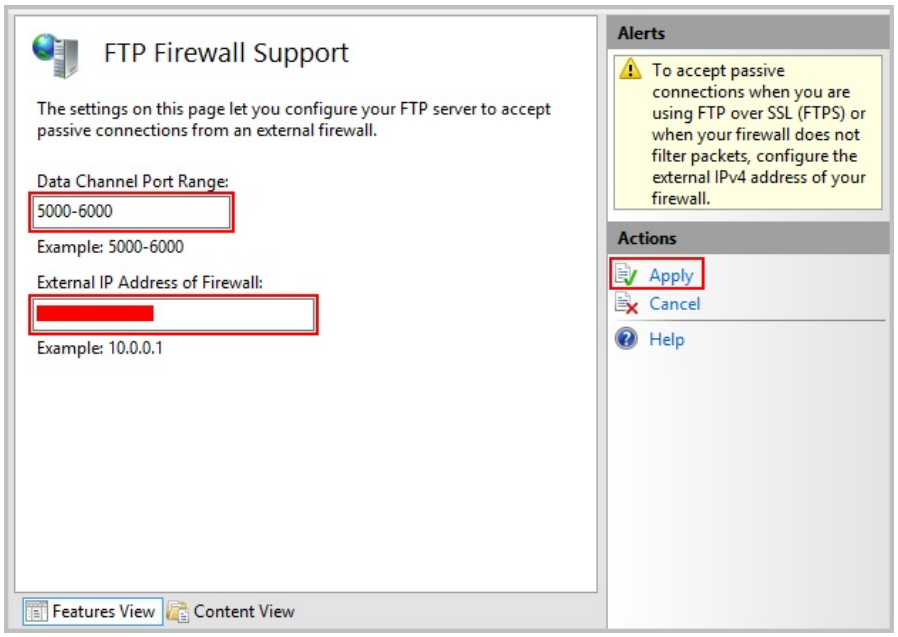
Step 5 (Optional) Configure the FTP firewall.

- To enable the passive mode on the FTP server, configure the FTP firewall.
- If HUAWEI CLOUD servers use public IP addresses to access the FTP site that is set up on a HUAWEI CLOUD ECS, the passive mode must be enabled on the FTP server.

1. Double-click **FTP Firewall Support**.



2. Set parameters and click **Apply**.
   - **Data Channel Port Range**: specifies the range of ports used for passive connections. The port range is 1025-65535. Configure this parameter based on site requirements.
   - **External IP Address of Firewall**: Enter the public IP address of the ECS.



3. Restart the ECS for the firewall configuration to take effect.

Step 6 Set the security group and firewall.

After setting up the FTP site, add a rule in the inbound direction of the security group to allow packets to pass through the FTP port. For details, see **Configuring Security Group Rules**.

If **FTP Firewall Support** is configured, enable the ports used by the FTP site and the data channel ports used by the FTP firewall in the security group.

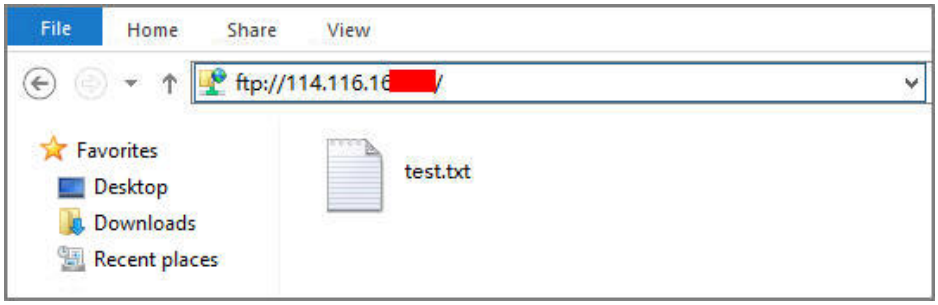
By default, the firewall allows packets to pass through TCP port 21 for FTP. If another port is used, add an inbound rule that allows packets to pass through the port on the firewall.

Step 7 Verify the configuration on the client.

On the computer with the client installed, enter fttp://*IP address of the FTP server*:*FTP port number* in the Internet Explorer address bar. If you do not specify the port number, default port number 21 is used. If a dialog box is displayed for you to enter the username and password, the configuration is correct. After entering the username and password, you can perform operations on the FTP folder with assigned permissions.

NOTE

If **FTP Firewall Support** is not configured, configure the Internet Explorer browser. Otherwise, the FTP folder will be inaccessible. To configure the Internet Explorer browser, choose **Tools** > **Internet Options** > **Advanced**, select **Enable FTP folder view**, and deselect **Use Passive FTP**.

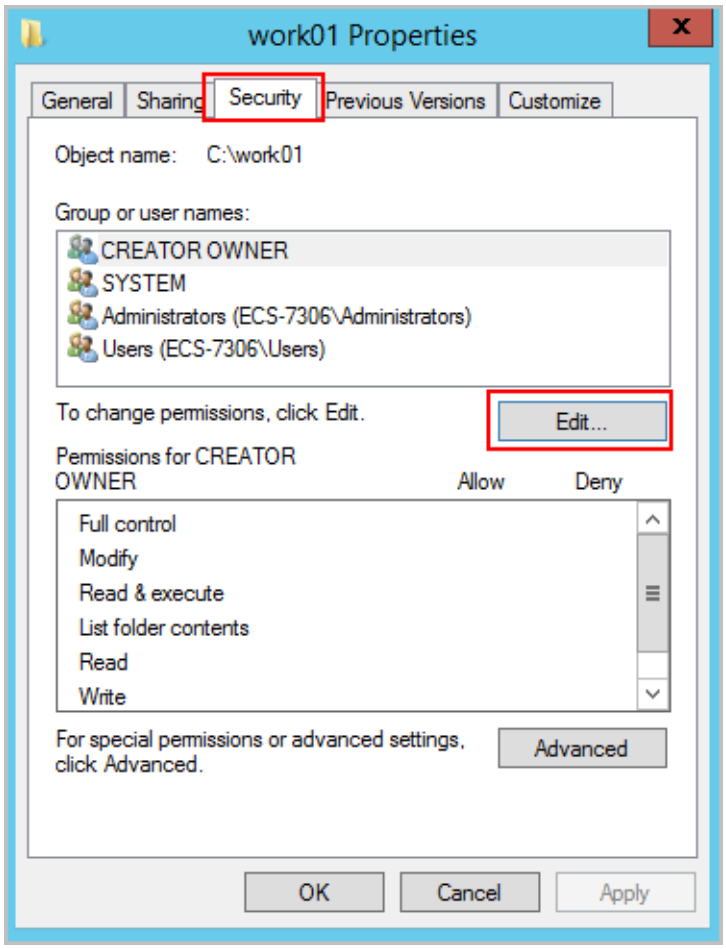


----End

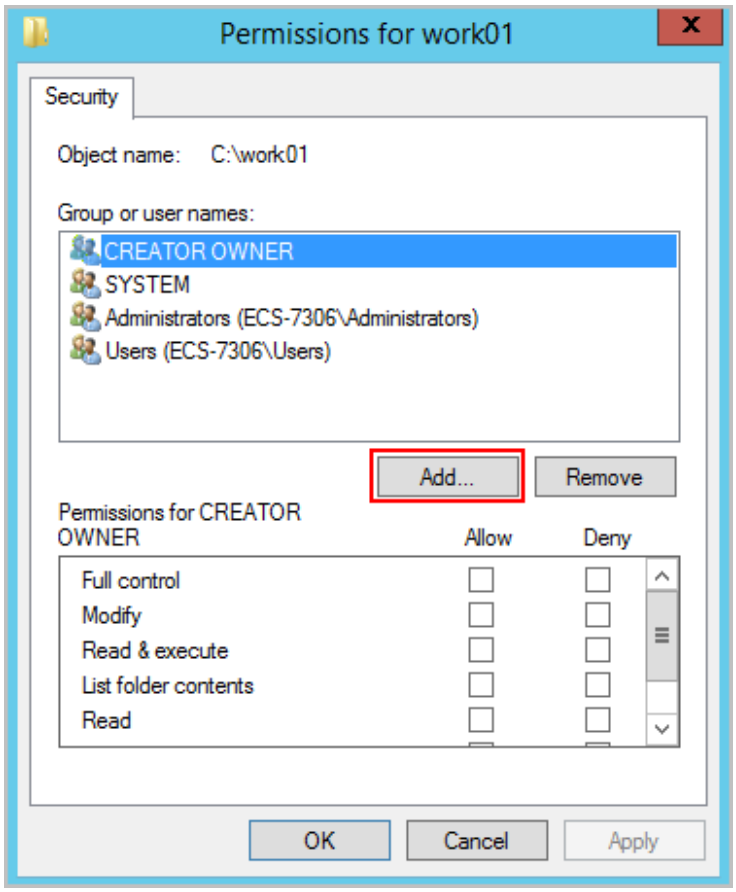
FAQs

- For more information about setting up an FTP site on a Windows ECS, see **Microsoft official documents**.
- When configuring the properties of a folder, if **Everyone** is unavailable, perform the following operations to add it:

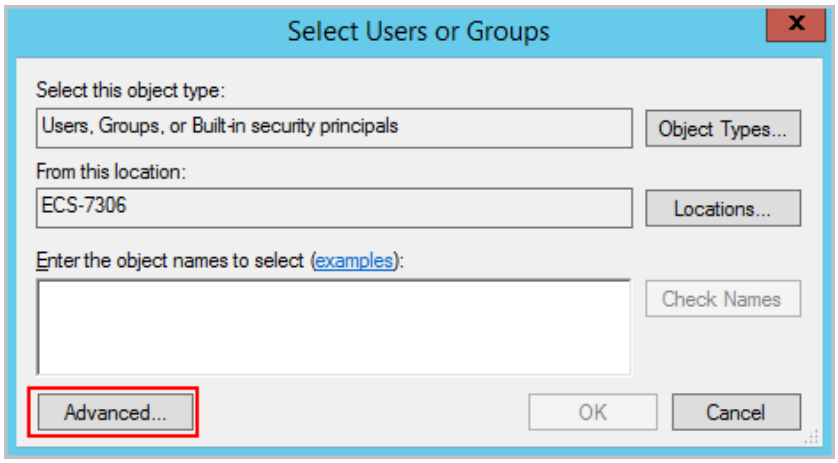
  a. On the **Security** tab, click **Edit**.



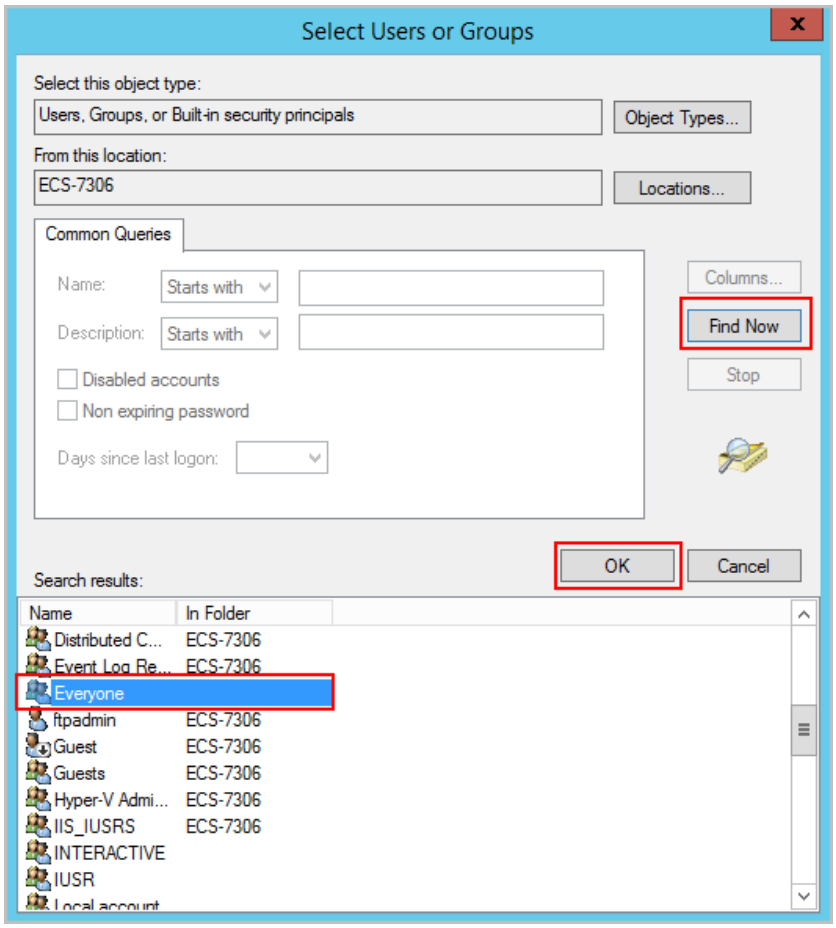
b. In the dialog box that is displayed, click **Add**.



c. In the dialog box that is displayed, click **Advanced**.



d. In the dialog box that is displayed, click **Find Now**, select **Everyone** in search results, and click **OK**.

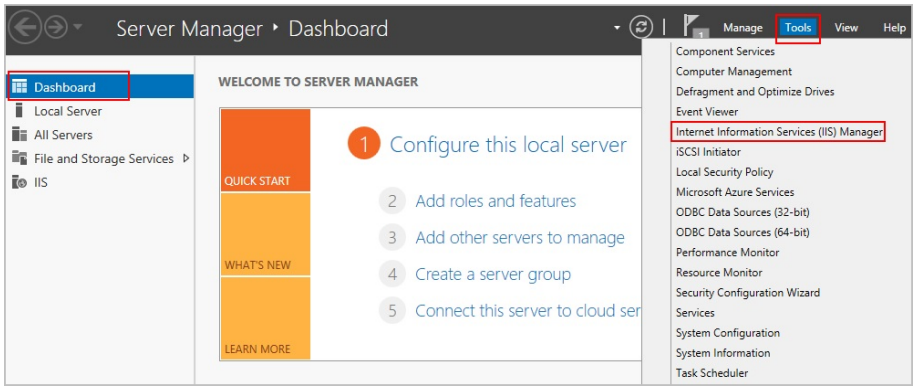


e. Click **OK** to return to the permissions page.

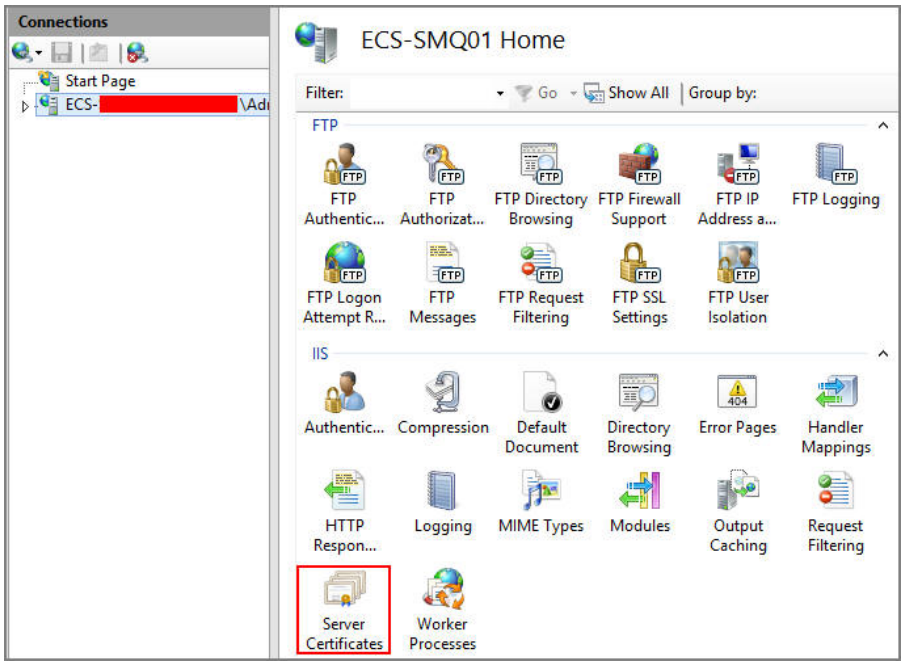
f. Click **OK**.

- Create a server certificate.

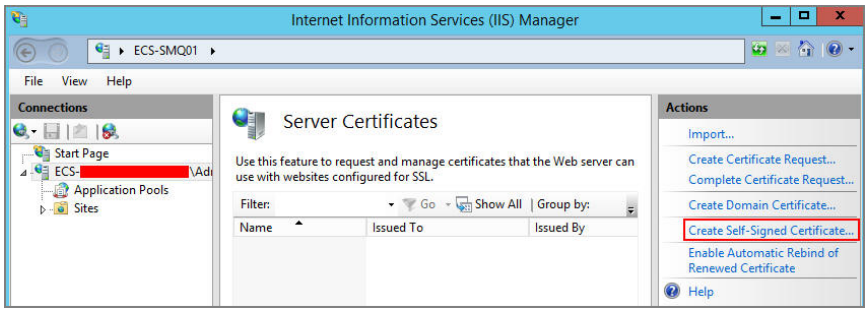
  a. In **Server Manager**, choose **Dashboard** > **Tools** > **Internet Information Services (IIS) Manager**.



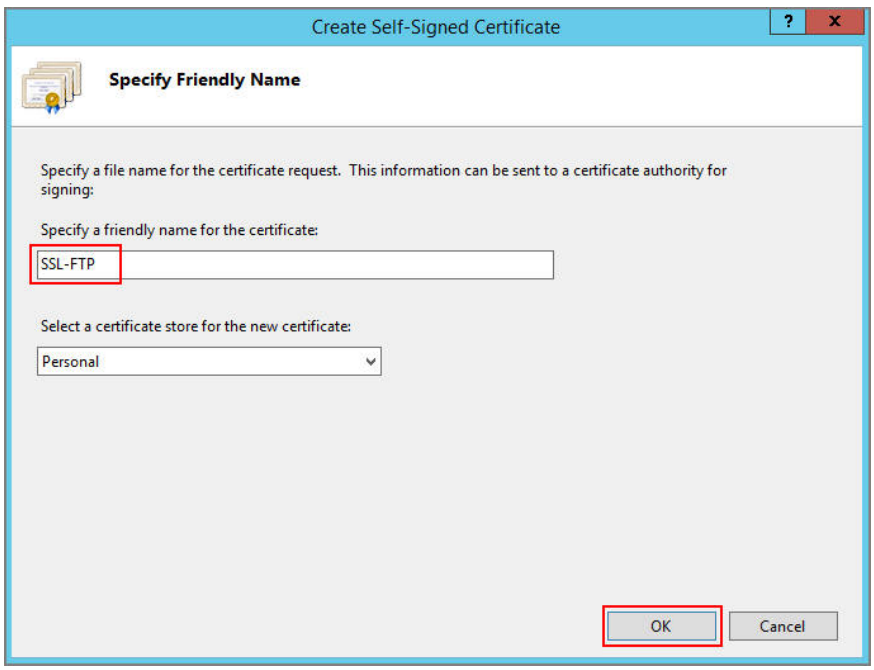
  b. In the list on the left, click the server. Under **IIS**, double-click **Server Certificates**. The **Server Certificates** page is displayed.



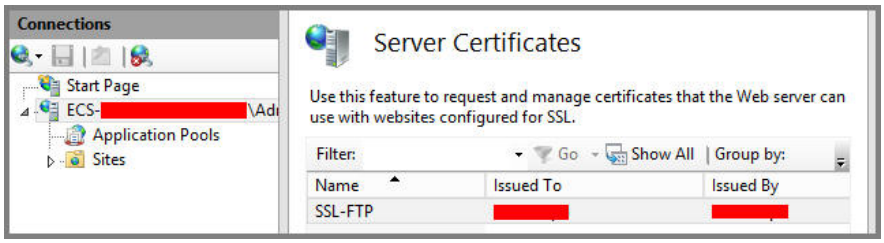
c. Click **Create Self-Signed Certificate**.



d. Specify a certificate name, select a certificate storage type, and click **OK**.



The created certificate is displayed on the **Server Certificates** page.



9 Setting Up an FTP Site (Linux)

Overview

The best practices for HUAWEI CLOUD ECS guide you through the setup of an FTP site on a Linux ECS using very secure FTP daemon (vsftpd). vsftpd is widely used in Linux releases, featuring compact and secure. The CentOS 7.2 64bit OS is used as an example in this section.

The process is as follows:

1. **Install vsftpd.**
2. **Configure vsftpd.**
3. **Configure a security group.**
4. **Verify the configuration on the client.**

Procedure

Step 1 Install vsftpd.

1. Log in to the ECS.
2. Run the following command to install vsftpd:

   yum install -y vsftpd

   If information similar to the following is displayed, vsftpd has been installed.

```
Dependencies Resolved

================================================================================
 Package              Arch              Version                 Repository   Size
================================================================================
Installing:
 vsftpd               x86_64            3.0.2-22.el7            base        169 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 169 k
Installed size: 348 k
Downloading packages:
vsftpd-3.0.2-22.el7.x86_64.rpm                             | 169 kB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : vsftpd-3.0.2-22.el7.x86_64                                   1/1
  Verifying  : vsftpd-3.0.2-22.el7.x86_64                                   1/1

Installed:
  vsftpd.x86_64 0:3.0.2-22.el7
```

3. Run the following command to configure automatic FTP enabling upon ECS startup:

systemctl enable vsftpd.service

4. Run the following command to start FTP:

   systemctl start vsftpd.service

5. Run the following command to obtain the port running FTP:

   netstat -antup | grep ftp

   Information similar to the following is displayed.

   ```
   tcp6       0      0 :::21                   :::*                    LISTEN      11836/vsftpd
   ```

Step 2 Configure vsftpd.

After vsftpd is installed, anonymous FTP is enabled by default, allowing you to log in to the FTP server without requiring the login username and password. However, you are not allowed to modify or upload files. If you attempt to log in to the FTP server using the Linux OS account, your request will be rejected by vsftpd, but you are allowed to configure the username and password in vsftpd for logging in to the FTP server. To do so, perform the following operations:

1. Create a user.

   For example, to create user **ftpadmin**, run the following command:

   useradd ftpadmin

2. Run the following command to configure the password of user **ftpadmin**:

   passwd ftpadmin

3. Run the following command to create a file directory for the FTP server, **/var/ftp/work01** is used as an example:

   mkdir /var/ftp/work01

4. Run the following command to change the owner of the created file directory to the local user for logging in to the FTP server:

   chown -R ftpadmin:ftpadmin /var/ftp/work01

5. Modify the **vsftpd.conf** configuration file.

   a. Run the following command to open the file:

      vi /etc/vsftpd/vsftpd.conf

   b. Press **i** to enter editing mode.

   c. Modify the **vsftpd.conf** file.

      Set the active or passive FTP mode based on site requirements. If other HUAWEI CLOUD ECSs are required to use public IP addresses to access the FTP site that is set up on a HUAWEI CLOUD ECS, set the passive FTP mode.

      - Parameters to be configured for the active FTP mode:

        ```
        #No anonymous login to the FTP server is allowed. Local users are allowed to log in to the FTP server with their local file directories specified.
        anonymous_enable=NO             #No anonymous login to the FTP server is allowed.
        local_enable=YES                #Local users are allowed to log in to the FTP server.
        local_root=/var/ftp/work01      #Specifies the file directory used by a local FTP user.

        #The following parameter allows login users to visit their own home directories:
        chroot_local_user=YES                   #The directory access rule applies to all users.
        chroot_list_enable=YES                  #The directory access rule does not apply to exclusive users.
        chroot_list_file=/etc/vsftpd/chroot_list   #Specifies exclusive users.
        allow_writeable_chroot=YES
        ```


- Additional parameters to be configured for the passive FTP mode, excluding all the parameters configured in the active FTP mode:

```
#The public IP address of the FTP server and the range of accessible ports must also be configured.
listen=YES
listen_ipv6=NO
pasv_address=xx.xx.xx.xx     #Public IP address of the FTP server

pasv_min_port=3000           #Minimum port number in the passive FTP mode
pasv_max_port=3100           #Maximum port number in the passive FTP mode
```

d. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the configuration file.

e. Create the **chroot_list** file in **/etc/vsftpd/**.

touch chroot_list

The **chroot_list** file contains exclusive users to whom the home directory access rules do not apply. To allow a user to access non-home directories, add the username to this file. If there is no exclusive user, the **chroot_list** file can be left blank, but the file must be available.

6. Run the following command to restart vsftpd for the configuration to take effect:

systemctl restart vsftpd.service

Step 3 Configure a security group.

After setting up the FTP site, add a rule in the inbound direction of the security group to allow packets to pass through the FTP port. For details, see **Adding a Security Group Rule**.

Enable ports based on active or passive FTP mode:

- Active FTP mode: Port 21
- Passive FTP mode: Port 21 and all ports from parameters **pasv_min_port** to **pasv_max_port** specified in the **/etc/vsftpd/vsftpd.conf** file

Step 4 Verify the configuration on the client.

On the computer with the client installed, enter fttp://*IP address of the FTP server*:*FTP port number* in the Internet Explorer address bar. If you do not specify the port number, default port number 21 is used. If a dialog box is displayed for you to enter the username and password, the configuration is correct. After entering the username and password, you can perform operations on the FTP folder with assigned permissions.

NOTE

- If the active FTP mode is selected, use this method to configure the Internet Explorer browser. Otherwise, the FTP folder will be inaccessible. To configure the Internet Explorer browser, choose **Tools** > **Internet Options** > **Advanced**, select **Enable FTP folder view**, and deselect **Use Passive FTP**.
- If an error occurs when you use a browser to access the FTP server, you are advised to clear the browser caches and try again.

----End

10 Manually Deploying Java Web

Introduction

Tomcat is a widely used Java Web application server. This section describes how to deploy Java Web on an ECS. To do so, you need to download the Java Web installation package, upload the package to the ECS, and set security rules for the ECS. After installing Java Web, you need to configure related software.

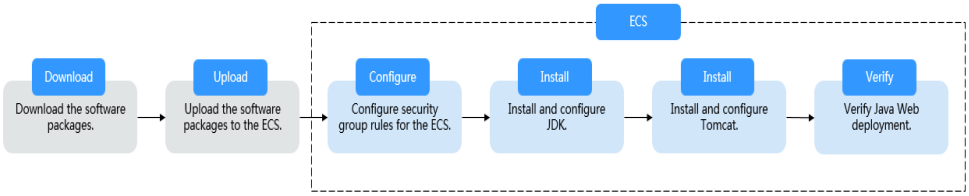
Intended Audience

Any one who wants to deploy Java Web on their ECSs can refer to this section.

The ECS in this chapter uses CentOS 7.3 64bit as OS.

Deployment Process

Figure 10-1 Deployment Process



Related Software and Tools

Table 10-1 Software packages

Software Package	How to Obtain
jdk	http://www.oracle.com/technetwork/java/javase/downloads
tomcat	http://tomcat.apache.org/download-80.cgi

NOTE

Table 10-1 lists the official paths to download JDK and Tomcat installation packages. You can also obtain the installation packages from other open-source image paths.

Table 10-2 Tool packages

Tool	Description	How to Obtain
PuTTY	A cross-platform remote access tool, which is used to access various nodes from a Windows OS during software installation	**http://www.putty.org/**
WinSCP	File transfer across platforms, which is used for transferring files between Windows and Linux systems	**http://winscp.net/**

Prerequisites

- An ECS with an EIP bound is available.
- The **jdk** directory has been created on the ECS. The commands are as follows:

  cd /home/

  mkdir webDemo

  cd webDemo/

  mkdir jdk
- The **tomcat** directory has been created on the ECS. The commands are as follows:

  cd webDemo/

  mkdir tomcat
- The installation packages have been downloaded to the local PC and uploaded to the ECS through the file transfer tool. Alternatively, you can run the **wget** command to download the installation packages to the ECS. The details of both methods are described as follows:
  - Method 1: Upload the installation packages to the ECS using the file transfer tool.
    - Use WinSCP to upload the JDK software package to the **jdk** directory.
    - Use WinSCP to upload the Tomcat software package to the **tomcat** directory.
  - Method 2: Run the **wget** command to download the installation packages to the ECS.
    i. Run the following command to switch to the **jdk** directory:

    cd /home/webDemo/jdk

ii. Running the following command to download the JDK installation package:

wget *JDK package download address*

Download the JDK installation package from the path listed in **Table 10-1** or from other open-source image paths.

Check the available **JDK 8** software package versions. The JDK installation package **jdk-8u261-linux-x64.tar.gz** is used as an example. Run the following command to download the package:

wget http://mirrors.linuxeye.com/jdk/jdk-8u261-linux-x64.tar.gz

iii. Run the following command to switch to the **tomcat** directory:

cd /home/webDemo/tomcat

iv. Running the following command to download the Tomcat installation package:

Download the Tomcat installation package from the path listed in **Table 10-1** or from other open-source image paths.

Run the following command to download the installation package, for example, **apache-tomcat-8.5.58.tar.gz**:

wget http://mirrors.tuna.tsinghua.edu.cn/apache/tomcat/tomcat-8/v8.5.58/bin/apache-tomcat-8.5.58.tar.gz

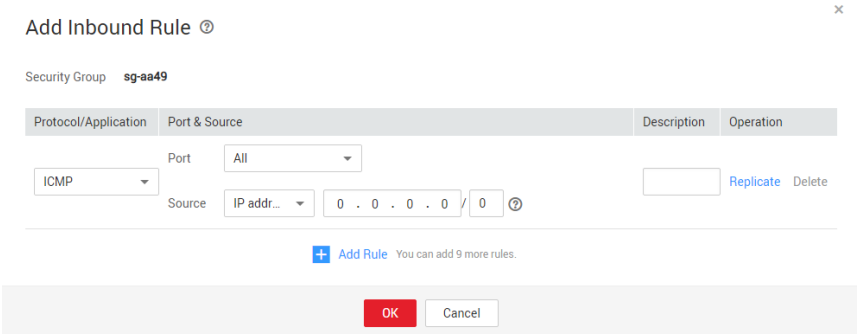
Configuring Security Group Rules for the ECS

1. Click the ECS name to switch to the ECS details page and click **Security Groups**.
2. In the upper right corner of the security group rule list, click **Modify Security Group Rule**.
3. On the displayed page showing security group details, click **Add Rule**.
4. In the **Add Inbound Rule** dialog box, add a security group rule as prompted.

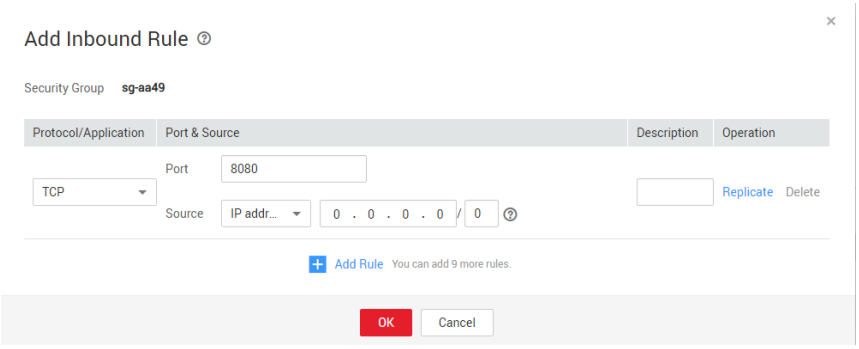
   To deploy the Java Web environment, you need to add two security group rules for the ECS.

   a. Set **Protocol** to **ICMP**.

   If ICMP is disabled by default, pinging the ECS EIP will time out. Therefore, you must add a rule that allows access to the ECS over ICMP.



   b. Set an appropriate port. You can set the port number only when **TCP** or **UDP** is selected for **Protocol**. 8080 is used as an example here.



Installing JDK

1. Run the following command to decompress the JDK installation package to the **jdk** directory:

   tar -xvf jdk-8u261-linux-x64.tar.gz -C /home/webDemo/jdk/

2. Run the following command to configure environment variables:

   vi /etc/profile

3. Add the following content to the end of the file:

   ```
   #set java environment
   export JAVA_HOME=/home/webDemo/jdk/jdk1.8.0_261
   export JRE_HOME=/home/webDemo/jdk/jdk1.8.0_261/jre
   export CLASSPATH=.:$JAVA_HOME/lib/dt.jar:$JRE_HOME/lib/tools.jar
   export PATH=$JAVA_HOME/bin:$PATH
   ```

4. Run the following command to save the configuration and exit:

   :wq

5. Run the following command to make the **/etc/profile** configurations take effect:

   source /etc/profile

6. Run the following command to verify the installation.

   java -version

   JDK is successfully installed if the following information is displayed:

   ```
   [root@ecs-c525-web ~]# java -version
   java version "1.8.0_261"
   Java(TM) SE Runtime Environment (build 1.8.0_261-b11)
   Java HotSpot(TM) 64-Bit Server VM (build 25.261-b08, mixed mode
   ```

Installing Tomcat

1. Run the following command to decompress the Tomcat installation package to the **tomcat** directory:

   tar -xvf apache-tomcat-8.5.58.tar.gz -C /home/webDemo/tomcat/

2. Run the following commands to install Tomcat:

   cd /home/webDemo/tomcat/apache-tomcat-8.5.58/

   cd bin/

3. Run the following command to edit the setclasspath.sh script:

   vi setclasspath.sh

   Add the following content to the setclasspath.sh script:

   ```
   export JAVA_HOME=/home/webDemo/jdk/jdk1.8.0_261
   export JRE_HOME=/home/webDemo/jdk/jdk1.8.0_261/jre
   ```


4. Save the file and exit. Run the following command to start Tomcat:
   ./startup.sh

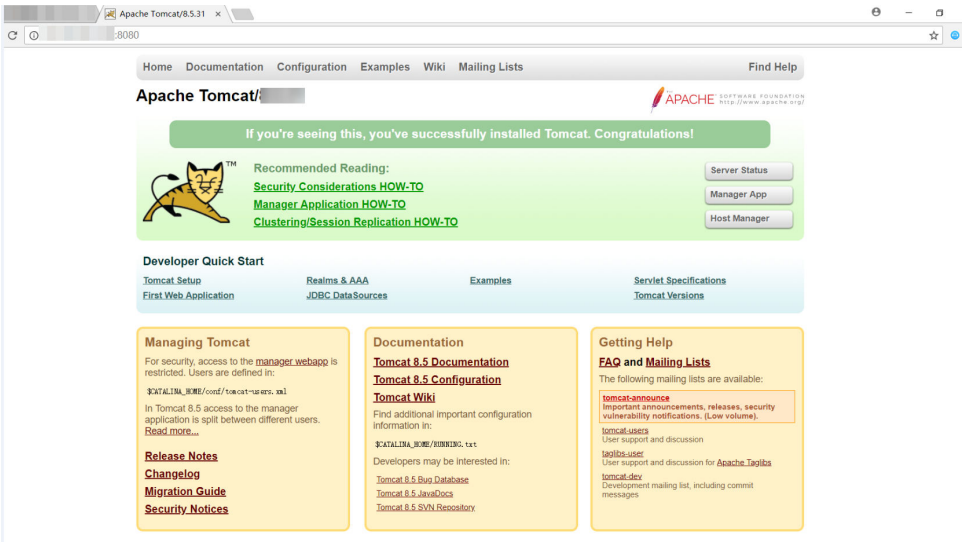
Verifying Java Web Deployment

Enter the following content in the address box of a browser:

http://EIP bound to the ECS:8080

If the Tomcat page is displayed, Java Web has been set up. Port 8080 of ECSs can be accessed over the public network.

Figure 10-2 Accessing port 8080



11 Manually Setting Up a Magento E-Commerce Website (Linux)

Overview

The best practices for ECS guide you through the setup of a Magento e-commerce website on a Linux ECS. Magento is an open source e-commerce system that features flexible design, modular architecture, and rich functions. It provides solutions for medium- and large-sized sites. Magento uses PHP for developing and MySQL for data storage. The CentOS 7.2 OS is used as an example in this section.

The process is as follows:

1. **Install and configure the LAMP platform.**
2. **Start Apache and MySQL.**
3. **Create a database.**
4. **Install and configure Composer.**
5. **Install Magento.**
6. **Configure Magento.**
7. **Set cron to run scheduled jobs.**
8. **Test the Magento website.**
9. **Purchase a domain name.**
10. **Obtain an ICP license.**
11. **Enable domain name resolution.**

Prerequisites

The rule listed in the following table has been added to the security group to which the target ECS belongs. For details, see **Adding a Security Group Rule**.

Table 11-1 Security group rules

Transfer Direction	Protocol/Application	Port/Range	Source End
Inbound	HTTP (80)	80	0.0.0.0/0

Transfer Direction	Protocol/Application	Port/Range	Source End
Inbound	MySQL (3306)	3306	0.0.0.0/0

Procedure

Step 1 Install and configure the LAMP platform.

1. Log in to the ECS.
2. Run the following commands as user **root** to update the software package 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

   NOTE

   During command execution, if an error message is displayed indicating a domain name resolution failure, add a DNS server to the **/etc/resolv.conf** configuration file.

Step 2 Run the following commands to start Apache and MySQL and configure automatic Apache and MySQL enabling upon ECS startup:

systemctl start httpd

systemctl enable httpd

systemctl start mysqld

systemctl enable mysqld

1. Modify the Apache configuration file.
   a. Run the following command to open the **httpd.conf** file:

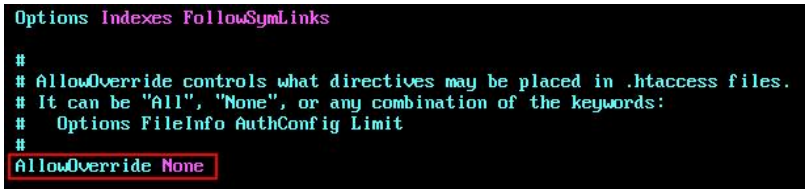
      vim /etc/httpd/conf/httpd.conf

      NOTE

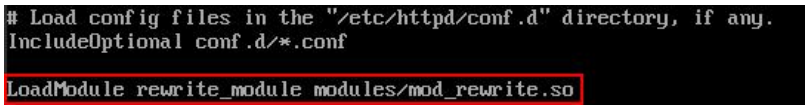
      If vim is not installed, run the **yum install -y vim*** command to install it.

   b. Press **i** to enter editing mode.
   c. Modify the **httpd.conf** file.

      - Change the **AllowOverride** value from **None** to **all**.



- Add **LoadModule rewrite_module modules/mod_rewrite.so** to the end of the configuration file.



d. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the configuration file.

2. Run the following command to obtain the password of user **root** that is automatically set during MySQL installation:

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

   Information similar to the following is displayed:

   ```
   2019-05-09T11:29:42.365419Z 1 [Note] A temporary password is generated for root@localhost: (n?K7jP#cirM
   ```

3. Run the following command and perform operations as prompted to harden MySQL:

   mysql_secure_installation

   ```
   Securing the MySQL server deployment.

   Enter password for user root:    #Enter the obtained password of user root.
   The existing password for the user account root has expired. Please set a new password.

   New password:                    #Set the password of user root.

   Re-enter new password:           #Enter the new password again.
   The 'validate_password' plugin is installed on the server.
   The subsequent steps will run with the existing configuration of the plugin.
   Using existing password for root.

   Estimated strength of the password: 100
   Change the password for root ? ((Press y|Y for Yes, any other key for No) : Y   #Asks you whether to change the password of user root. Press y.

   New password:    #Enter a new password containing 8 to 30 characters, including uppercase letters, lowercase letters, digits, and special characters. The special characters can be any of the following: ()`~!@#$%^&*-+=|{}[]:;'<>,.?/
   Re-enter new password:    #Enter the new password again.
   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   #Press y.
   By default, a MySQL installation has an anonymous user, allowing anyone to log into MySQL without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment.

   Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y   #Asks you whether to remove anonymous users. Press 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   #Asks you whether to forbid remote login of user root. Press y.
   Success.

   By default, MySQL comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment.

   Remove test database and access to it? (Press y|Y for Yes, any other key for No) : Y   #Asks you whether to delete the test database and cancel access permissions to it. Press y.
    - Dropping test database...
   Success.
   ```



```
 - Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : Y    #Asks you whether to reload privilege tables. Press y.
Success.

All done!
```

4. Run the following commands to install PHP 7 and PHP extensions required for installing Magento:

   yum install -y http://dl.iuscommunity.org/pub/ius/stable/CentOS/7/x86_64/ius-release-1.0-15.ius.centos7.noarch.rpm

   yum -y update

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

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

5. Run the following command to check the PHP installation:

   php -v

   If information similar to the following is displayed, PHP has been installed:

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

6. Modify the PHP configuration file.

   a. Run the following command to open the **php.ini** file:

      vim /etc/php.ini

   b. Press **i** to enter editing mode.

   c. Modify the **php.ini** file.

      - Change the **memory_limit** value based on site requirements for memory limit.

        ```
        ; Maximum amount of memory a script may consume (128MB)
        ; http://php.net/memory-limit
        memory_limit = 256M
        ```

      - Comment out the following content and set **date.timezone** for the PHP time zone.

        ```
        [Date]
        ; Defines the default timezone used by the date functions
        ; http://php.net/date.timezone
        date.timezone = Asia/Shanghai
        ```

   d. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the configuration file.

7. Run the following command to restart the web process:

   systemctl restart httpd

Step 3 Create a database.

1. Run the following command and enter the user **root** password of MySQL as prompted to log in to the MySQL CLI:

   mysql -u root -p

2. Run the following command to create a new database:

   CREATE DATABASE *magento***;**

   In the preceding command, *magento* is the database name, which is configurable.

3. Run the following command to create a user for the database and assign the full-access permission to the user:

   GRANT ALL ON *magento***.* TO** *magentouser***@localhost IDENTIFIED BY '***BLOck@123***' ;**

   In the preceding command, *magentouser* is the username for logging in to the database, and *BLOck@123* is the configurable user password.

4. Run the following command to exit the MySQL CLI:

   exit

5. (Optional) Run the following commands to verify the creation of the database and account and exit the MySQL CLI:

   mysql -u *magentouser* **-p**

   SHOW DATABASES;

   exit

   In the preceding command, *magentouser* is the created username for logging in to the database.

Step 4 Install and configure Composer.

Composer is a package manager for the PHP programming language. It manages PHP software dependencies and provides standard formats for dependent libraries.

1. Run the following command to install Composer:

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

   Information similar to the following is displayed:

   ```
   All settings correct for using Composer
   Downloading...

   Composer (version 1.8.5) successfully installed to: /root/composer.phar
   Use it: php composer.phar
   ```

2. Run the following command to globally enable Composer:

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

3. Run the following command to check whether Composer has been installed:

   composer -v

   If information similar to the following is displayed, Composer has been installed:

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


Step 5 Install Magento.

When installing Magento, you can determine whether to configure example data. If Magento is only used for testing, it is optional for you to configure example data. If Magento is installed in a production environment, you are advised to install the latest Magento version and perform initial configurations.

1. Run the following command to install git:

   yum -y install git

2. Run the following commands to download Magento using git:

   cd /var/www/html/

   git clone https://github.com/magento/magento2.git

3. Switch Magento to a stable version.

   By default, the latest Magento version is installed. If Magento running in a production environment is not stable, switch it to a stable version. Otherwise, Magento will not be able to upgrade.

   cd magento2 && git checkout tags/2.1.0 -b 2.1.0

   Information similar to the following is displayed:

   ```
   Switched to a new branch '2.1.0'
   ```

4. Move the installation files to the root directory of the web server.

   After the files are moved, enter http://*IP address of the Magento server* in the address bar to visit the Magento website. If the files are not moved, enter http://*IP address of the Magento server*/magento2 in the address bar to visit the Magento website.

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

5. Run the following commands to assign permissions to the Magento files:

   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

6. Run the following commands to install Magento:

   yum install -y unzip zip

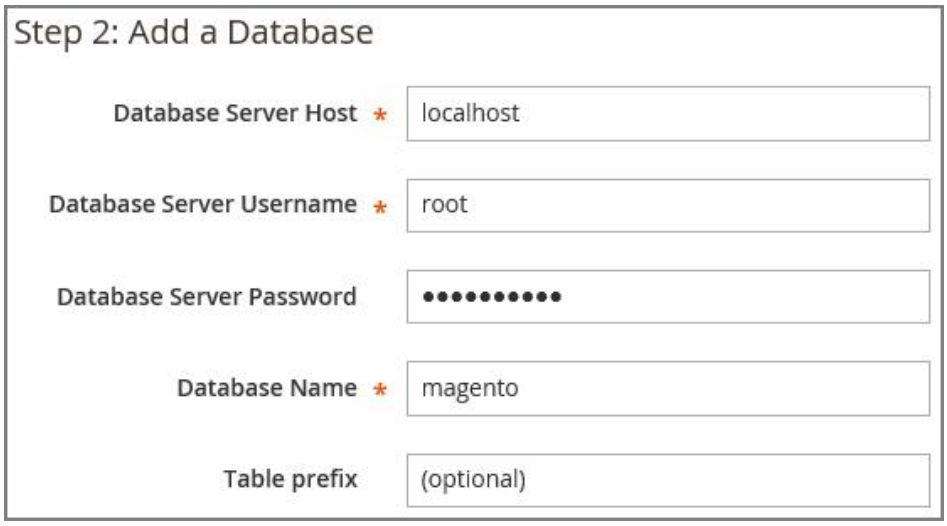
   composer install

7. Enter http://*IP address of the Magento server* in the address bar to visit Magento. If the following page is displayed, Magento has been installed.

Step 6 Configure Magento.

1. Click **Agree and Setup Magento** and configure Magento.
2. Click **Start Readiness Check** to check the environment. After the environment is ready, click **Next**.
3. Specify parameters, such as the database name and the **root** account for logging in to the MySQL database, and click **Next**.

   The following figure shows an example.



4. Set the website URL and server management address. Then, click **Next**.

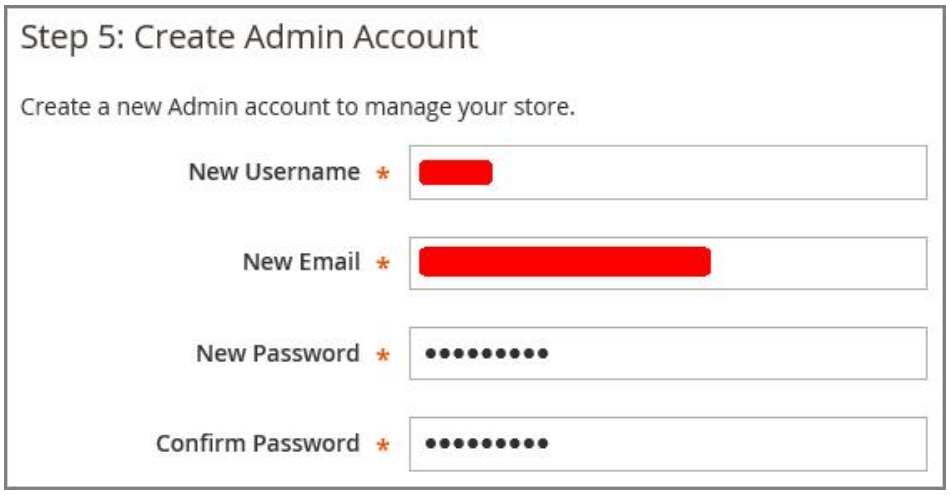
   The following figure shows an example.

NOTICE

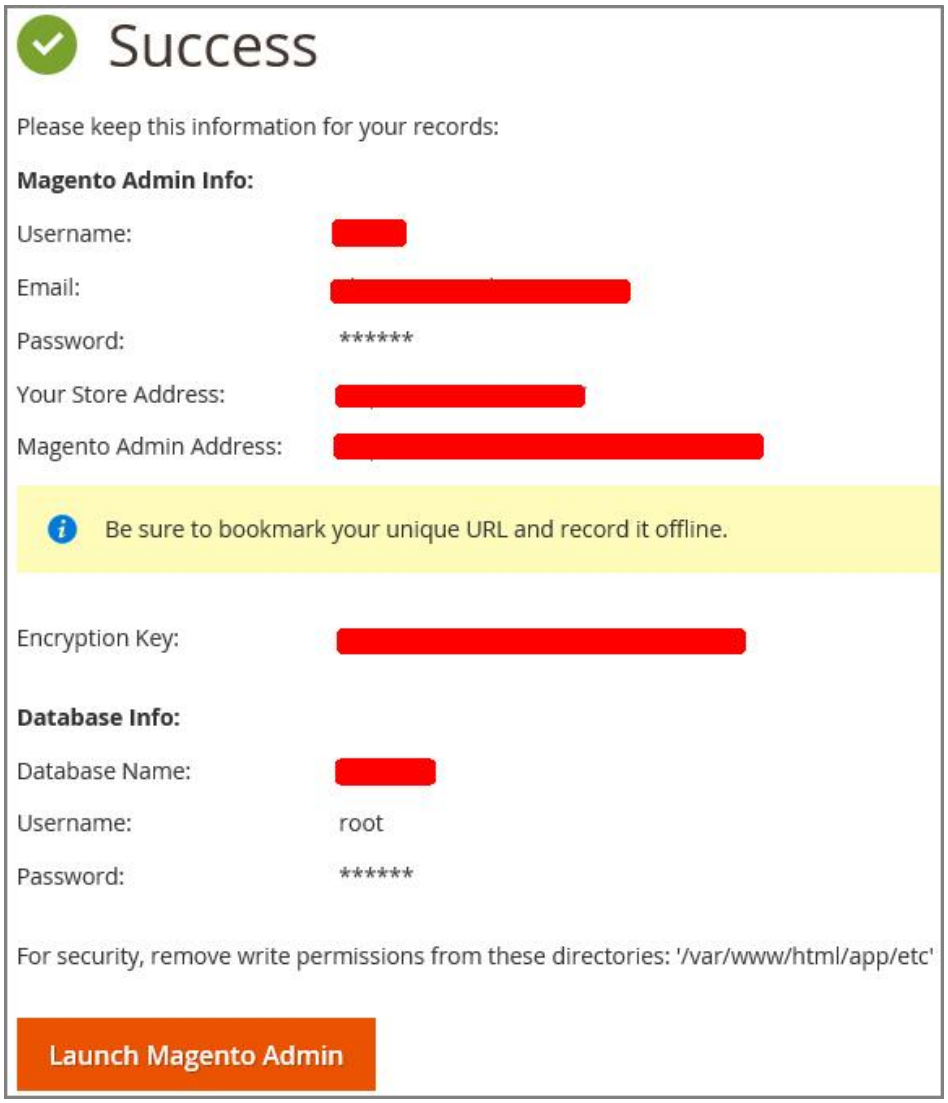
Securely keep the server management address.

5. Set the language and time zone. Then, click **Next**.
   The following figure shows an example.

6. Set the management account. Then, click **Next**.
   The following figure shows an example.



7. Click **Install Now**.
   If the following page is displayed, Magento has been installed.



Step 7 Set cron to run scheduled jobs.

1. Run the following command to configure a cron job:

   crontab -u apache -e

2. Press **i** to enter editing mode.
3. Add the following data to the file:

   ***/10 * * * * php -c /etc /var/www/html/bin/magento cron:run**

   ***/10 * * * * php -c /etc /var/www/html/update/cron.php**

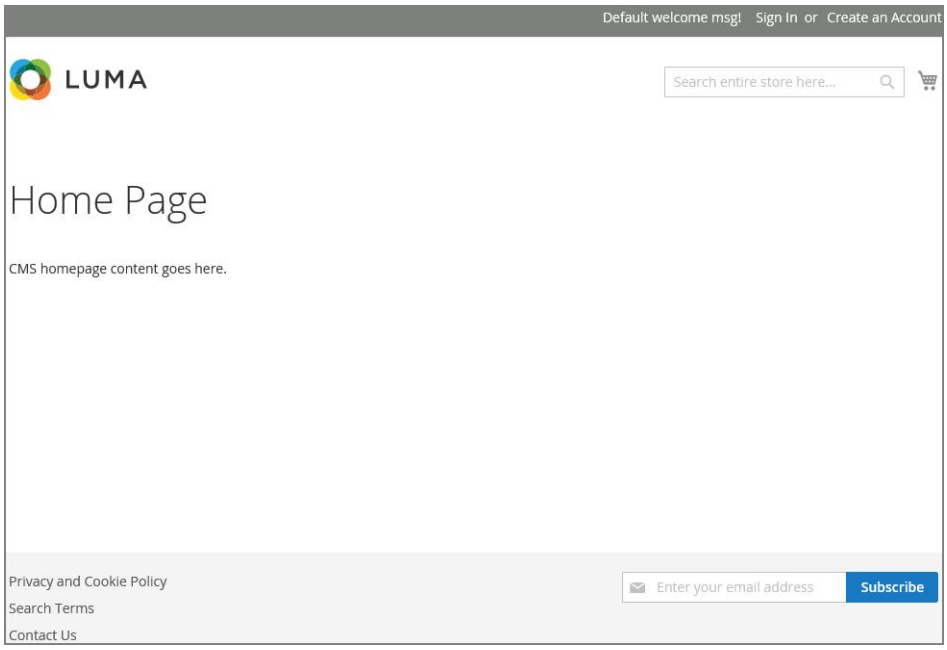
   ***/10 * * * * php -c /etc /var/www/html/bin/magento setup:cron:run**

4. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the configuration file.

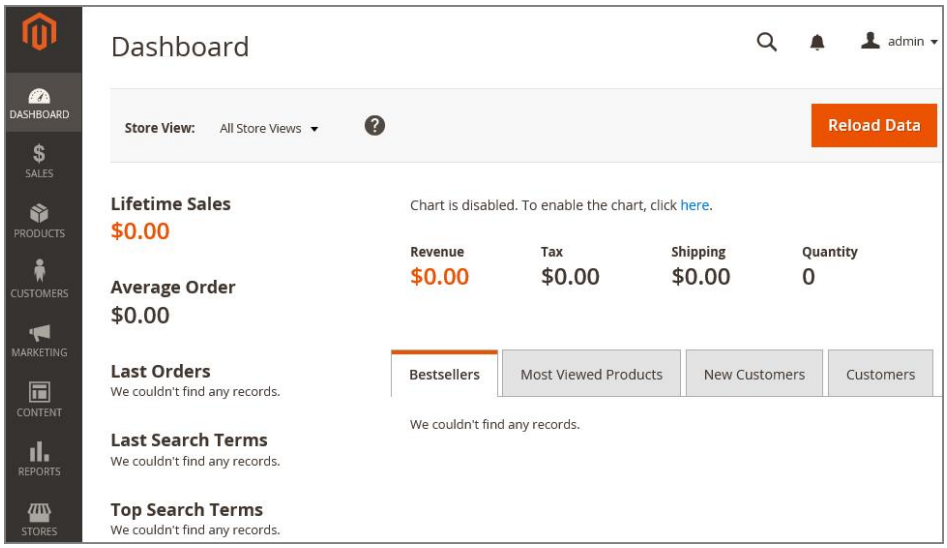
   For more information about how to run cron jobs on Magento, see **official Magento documents**.

Step 8 Test the Magento website.

1. In the address bar of the computer with client installed, enter http://*IP address of the Magento server*. The default page shown in the following figure is displayed.



2. Visit http://*Management IP address of the Magento server* and use the configured management account to log in to Magento. The following figure is displayed after a successful login.



NOTE

After the login, if the system displays error message "One or more indexers are invalid. Make sure your Magento cron job is running", run the **php bin/magento indexer:reindex** command in Magento root directory **/var/www/html**.

For more information about Magento configurations, see **official Magento documents**.

Step 9 Purchase a domain name.

To make the website accessible and usable, configure a unique domain name for the website. You are required to obtain an authorized domain name from the domain name registrar for the website.

Step 10 Obtain an ICP license.

If your website has not obtained an ICP license and needs to be hosted on HUAWEI CLOUD, use the HUAWEI CLOUD ICP license service to obtain a license.

Step 11 Enable domain name resolution.

Your website can be visited using the registered domain name only after domain name resolution is enabled. For details, see **Configuring a Public Zone**.

For example, if the domain name is www.example.com, enter http// www.example.com in the address bar of the browser to access the website.

----End

12 Building Microsoft SharePoint Server 2016

12.1 Purchasing and Logging In to an ECS

Purchase an ECS on HUAWEI CLOUD with specified specifications and OS.

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Elastic Cloud Server**.
4. Click **Buy ECS**.
   The **Buy ECS** page is displayed.
5. Configure ECS parameters.
   For details, see **Purchasing an ECS**.

Figure 12-1 Setting ECS specifications

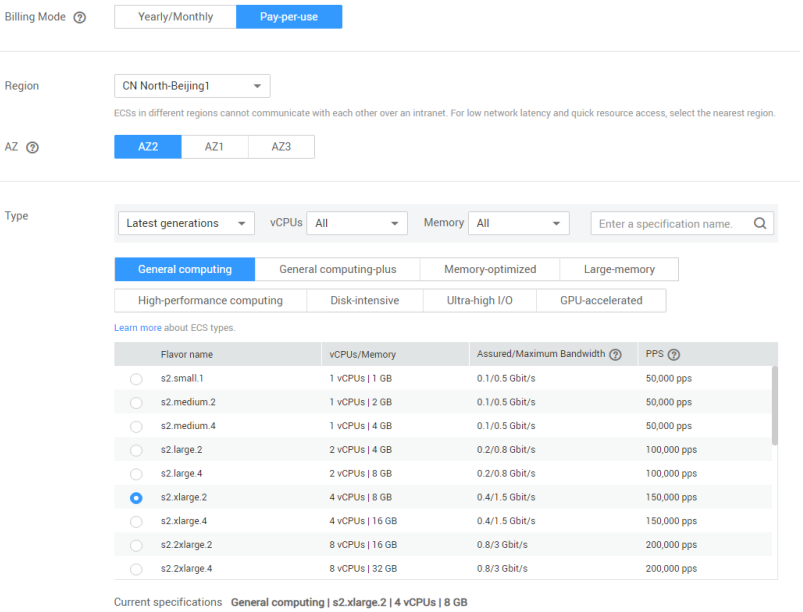


Figure 12-2 Setting the image and disk

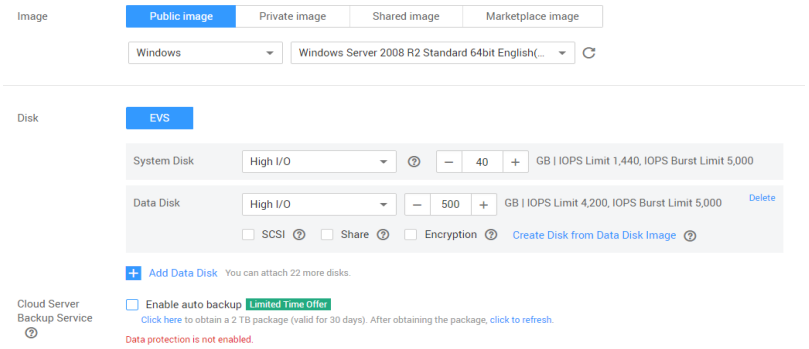


Figure 12-3 Setting the network

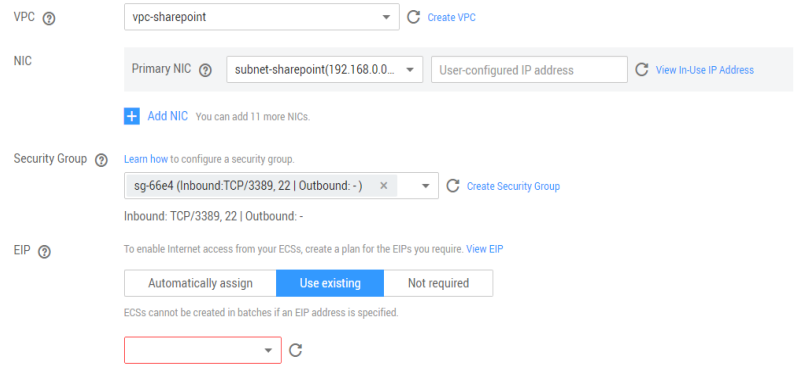
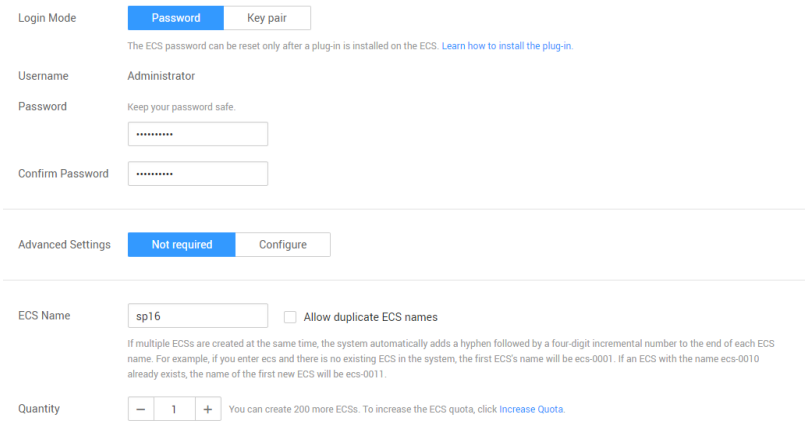


Figure 12-4 Setting the login mode and ECS name

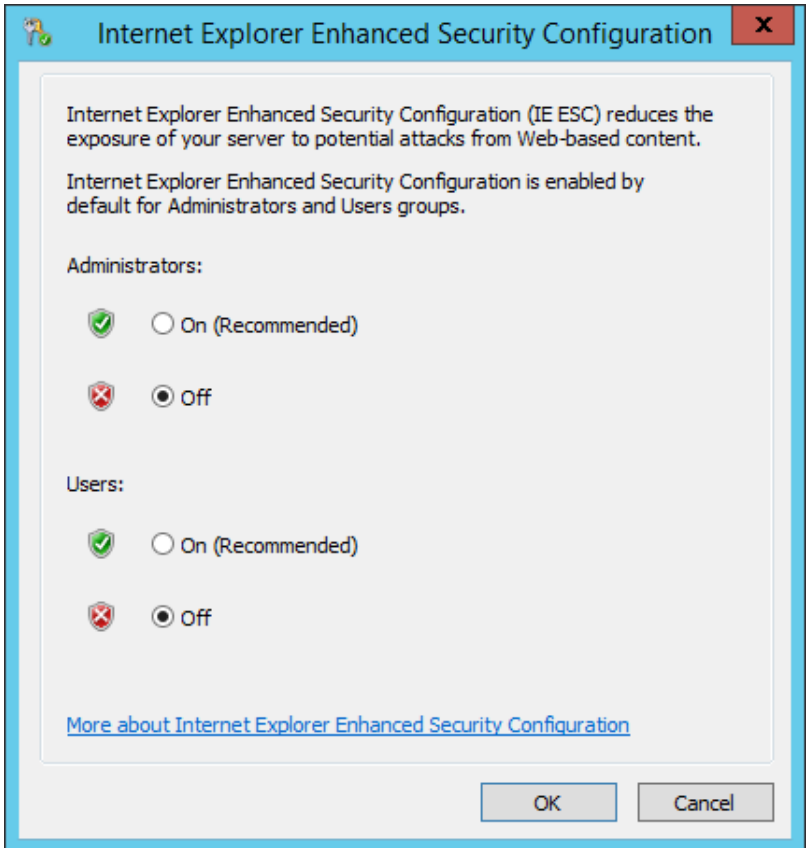


6. Click **Next**.
7. Confirm the ECS specifications and select **I have read and agree to Huawei Image Disclaimer**.
8. Click **Submit** and wait for the ECS creation to complete.
9. In the ECS list, locate the ECS you created and click **Remote Login** in the **Operation** column.
10. Click **Send CtrlAltDel** in the upper right of the remote login screen.
11. Enter the password of the ECS to log in.

12.2 Adding AD, DHCP, DNS, and IIS Services

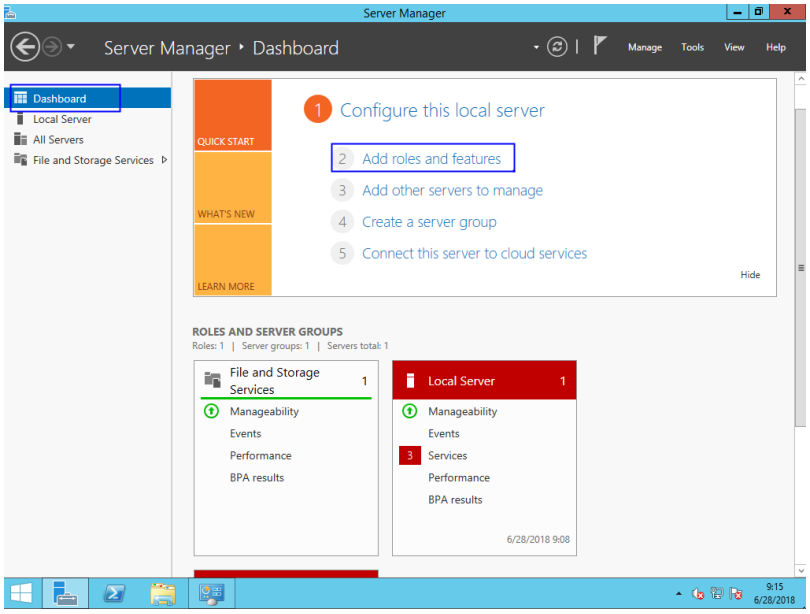
1. Choose **Server Manager** > **Local Server** and set **IE Enhanced Security Configuration** to **Off**.

   Figure 12-5 Internet Explorer Enhanced Security Configuration

2. Choose **Server Manager** > **Dashboard**.
3. Click **Add roles and features** to add roles and functions for the server, including DNS, DHCP, IIS, and Net Framework 3.5.

Figure 12-6 Add roles and features



4. On the **Server Roles** page, select **Active Directory Domain Services**, **DHCP Server**, **DNS Server**, and **Web Server (IIS)**.

Figure 12-7 Server role 1

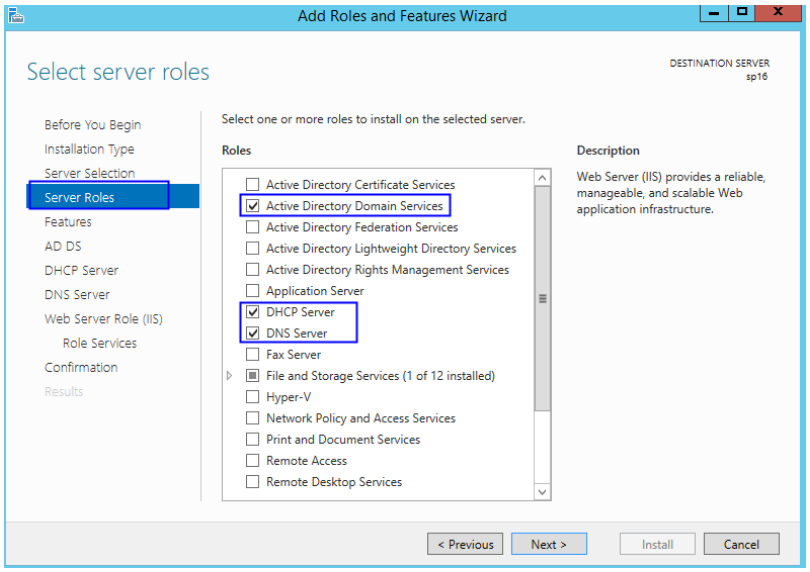
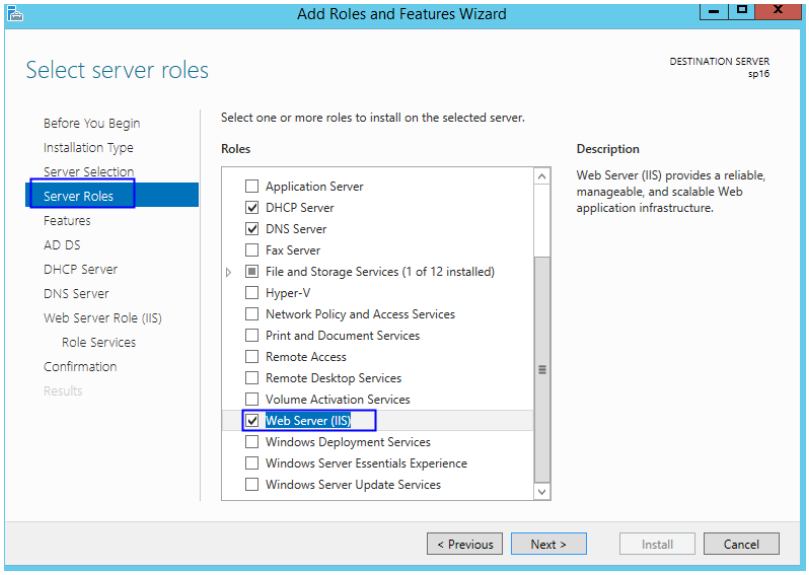
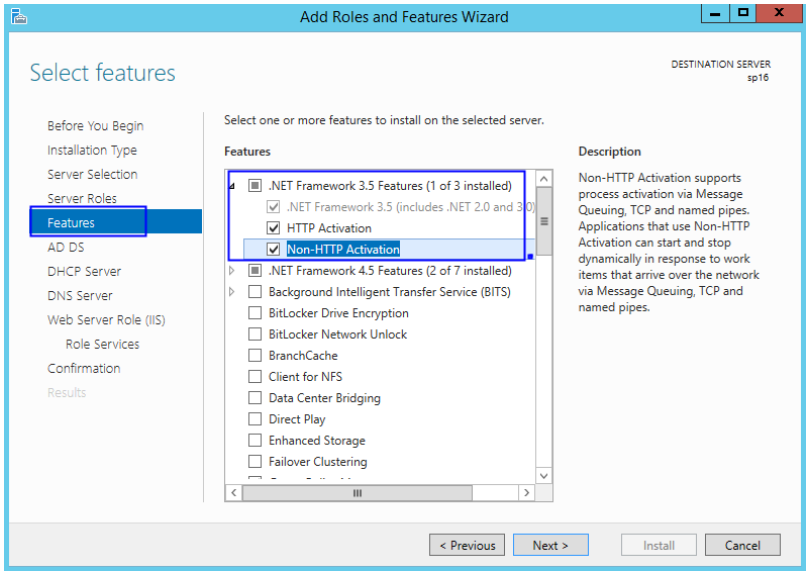


Figure 12-8 Server role 2



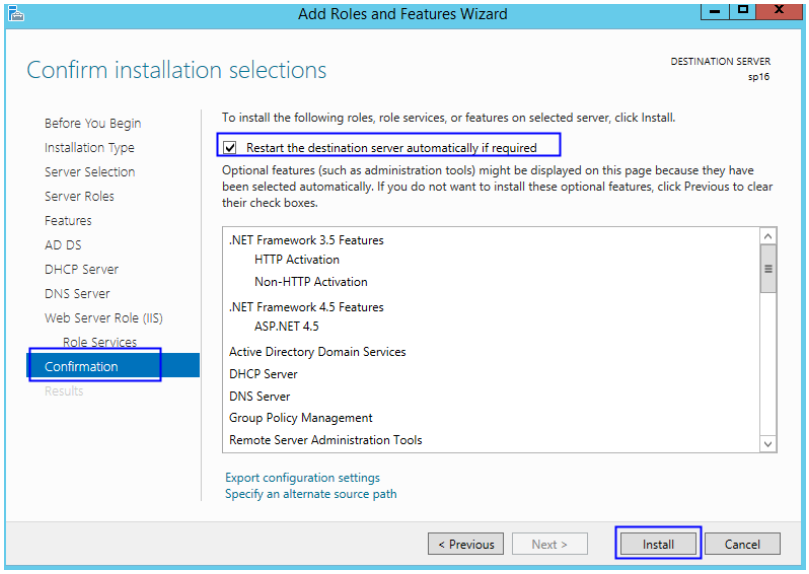
5. Click **Next**.
6. On the **Features** page, select **.NET Framework 3.5 Features**.

Figure 12-9 Features



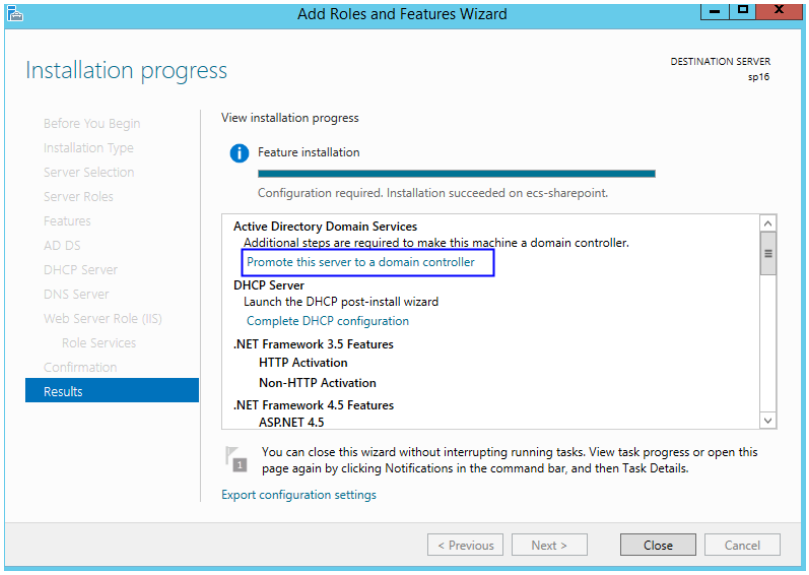
7. Click **Next** the configuration is complete.
8. On the **Confirmation** page, select **Restart the destination server automatically if required**.

Figure 12-10 Confirm installation selections



9. Click **Install** to start installation.
10. After the installation is complete, click **Promote this server to a domain controller** to configure the AD service.

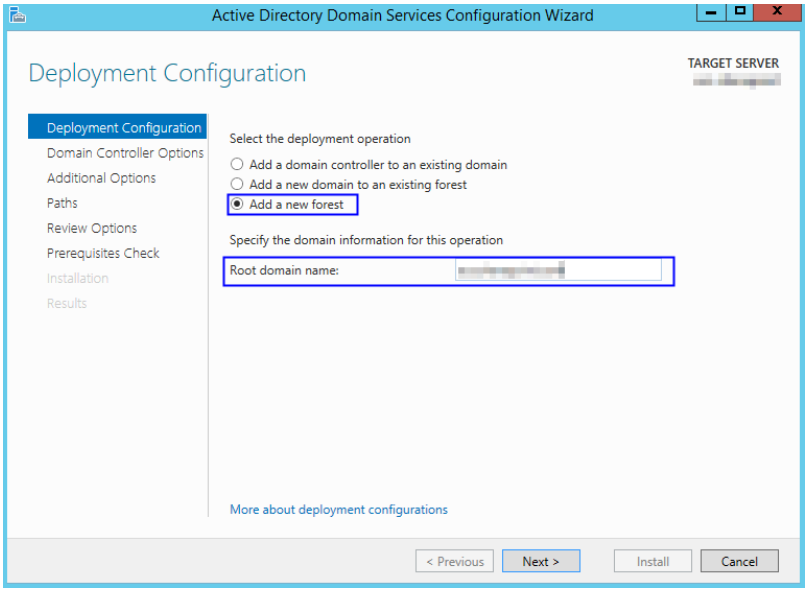
Figure 12-11 AD configuration



11. Choose **Add a new forest**.

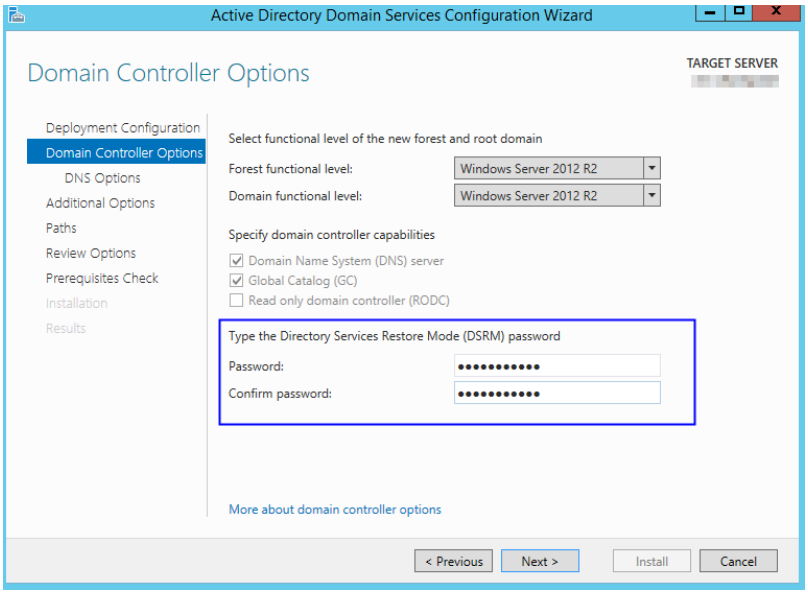
    Set **Root domain name** to **sp160.com.cn**.

Figure 12-12 Add a new forest



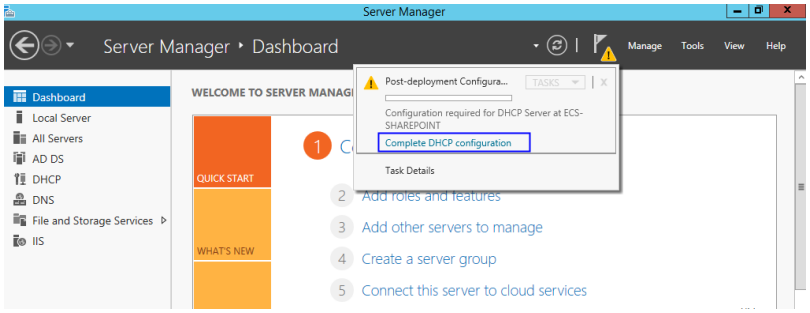
12. Click **Next**.
13. Set the password, which is used to back up and restore the domain controller.

Figure 12-13 Password setting



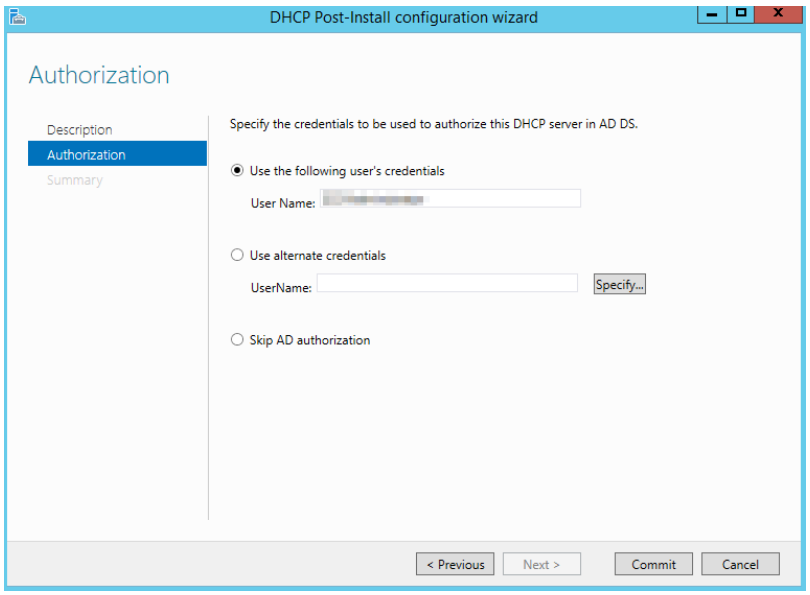
14. Click **Next** until the installation is complete.
15. Click **Complete DHCP configuration** to configure the DHCP function.

Figure 12-14 DHCP configuration 1



16. Retain the default settings and click **Next**.

Figure 12-15 DHCP configuration 2

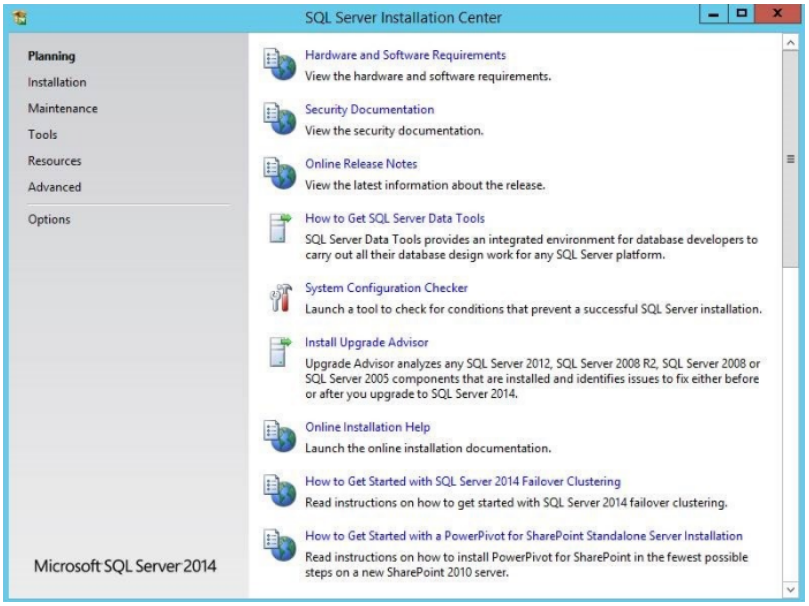


17. Click **Commit**.
18. After the configuration is complete, click **Close**.

12.3 Installing SQL Server

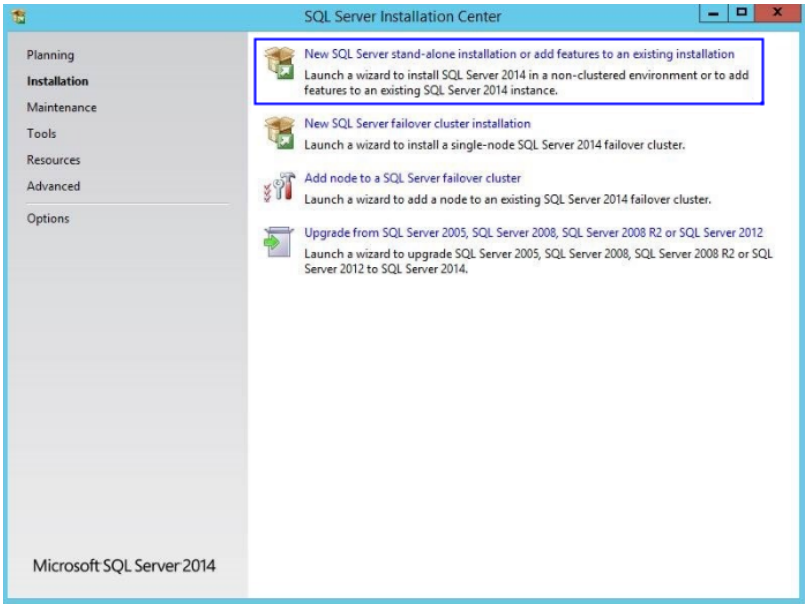
1. Double-click **Setup.exe** to open the SQL Server installation center.

Figure 12-16 SQL Server installation center



2. On the **Installation** page, click the first option.

Figure 12-17 SQL Server installation options

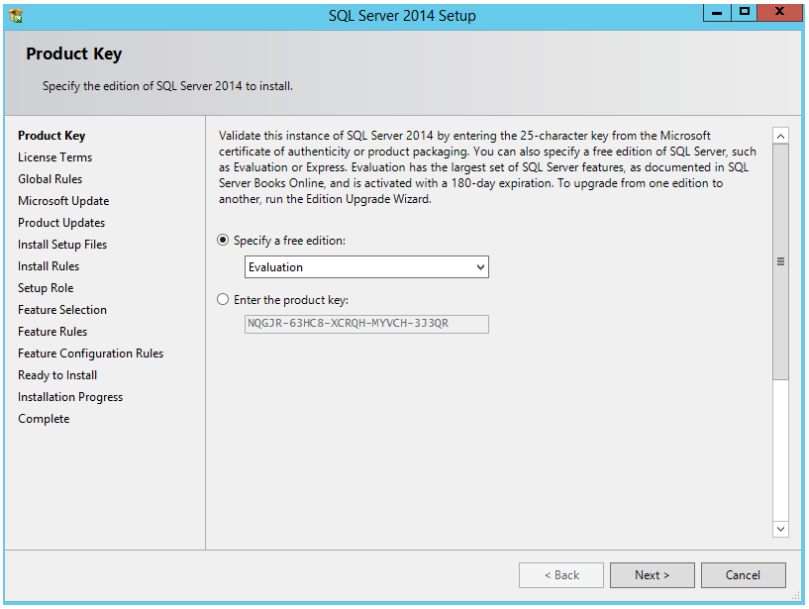


3. Select **Specify a free edition** to install SQL Server with a free image.

NOTE

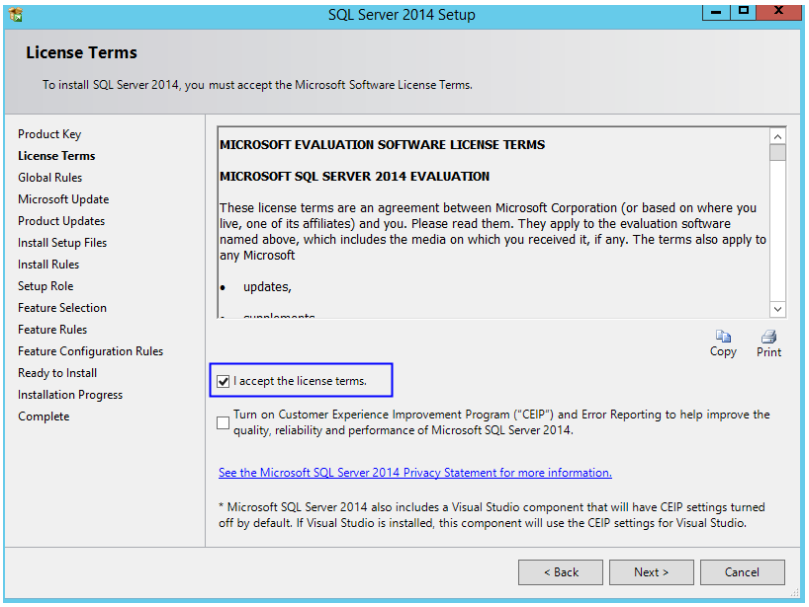
To set up an official SharePoint environment, you need to enter a key to install a full edition of SQL Server.

Figure 12-18 SQL Server free edition



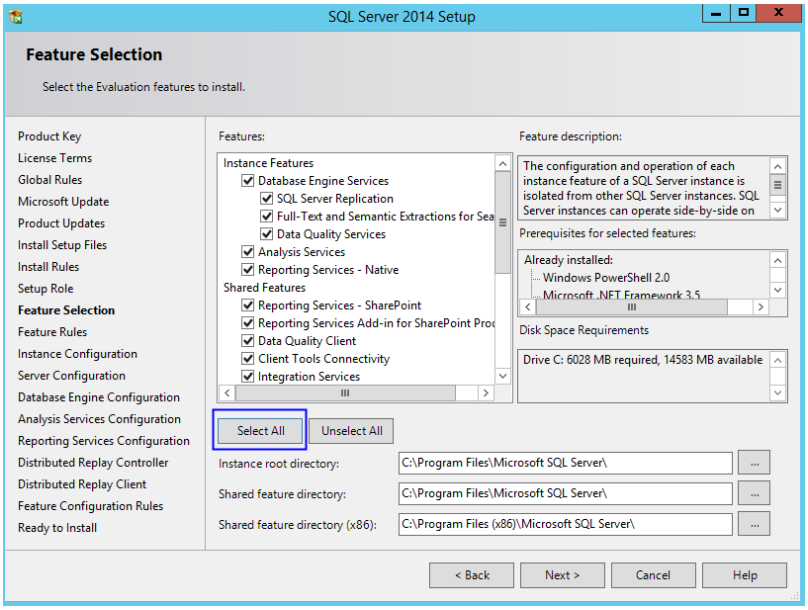
4. Select **I accept the license terms** and click **Next**.

Figure 12-19 SQL Server license option



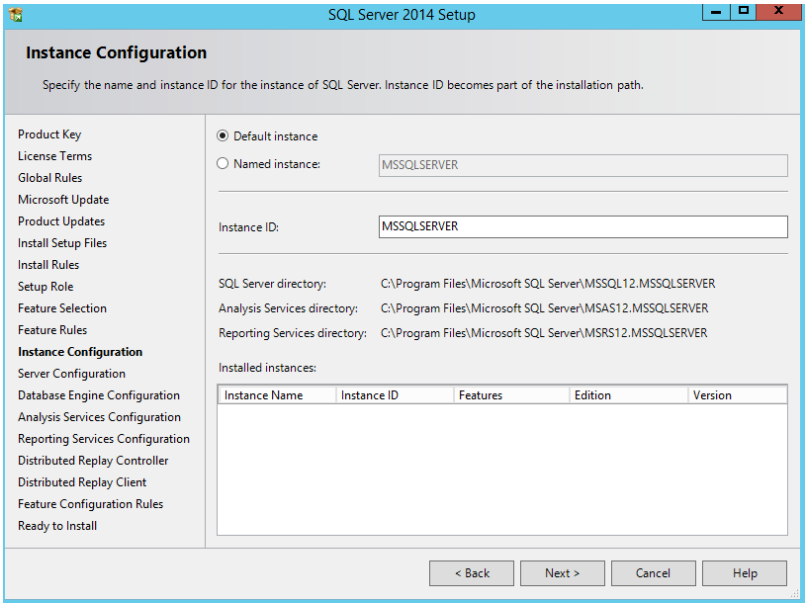
5. Click **Next** to install **Microsoft Updates**, **Install Rules**, and **Setup Role** using the default settings.
6. Click **Select All** to select all features and click **Next**.

Figure 12-20 SQL Server features



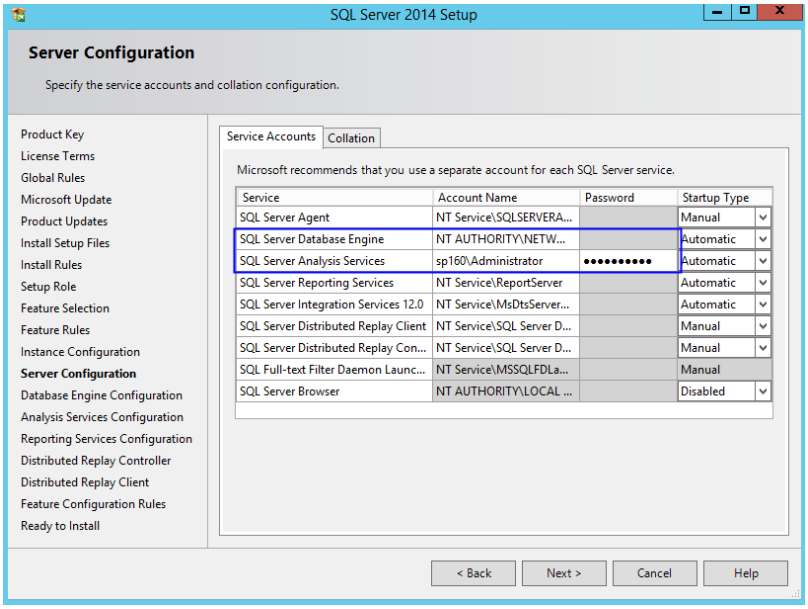
7. Select **Default instance**.

Figure 12-21 SQL Server instance



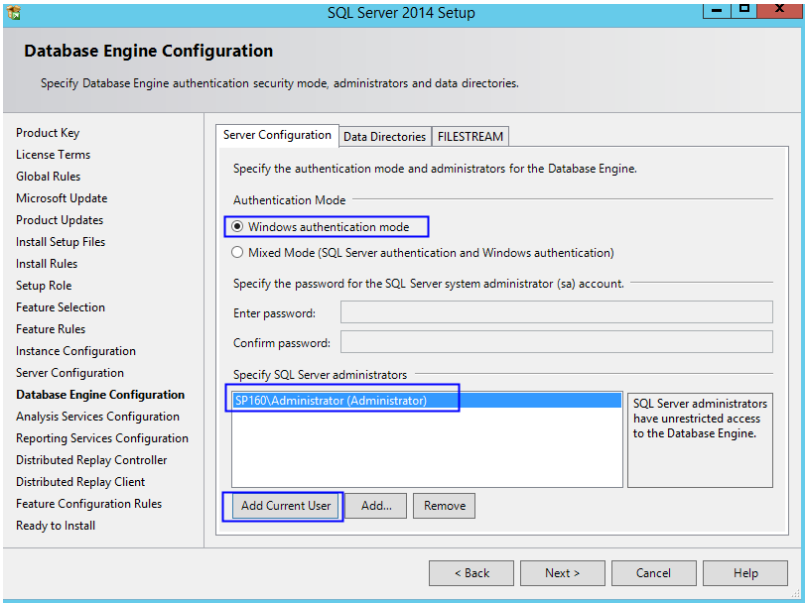
8. Set SQL Server configurations.
   - Change the account name of **SQL Server Database Engine** to **NT AUTHORITY\NETWORK SERVICE**.
   - Set the account and password of **SQL Server Analysis Services** to those configured in steps **11** to **13** in **Adding AD, DHCP, DNS, and IIS Services**.

Figure 12-22 SQL Server service accounts



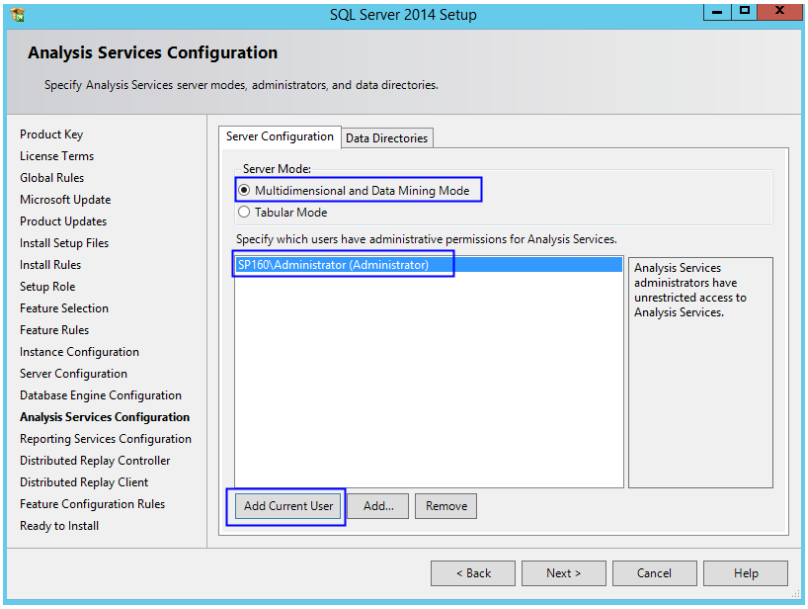
9. Click **Add Current User**, use the current account as the SQL Server administrator account, and click **Next**.

Figure 12-23 SQL Server administrator account 1



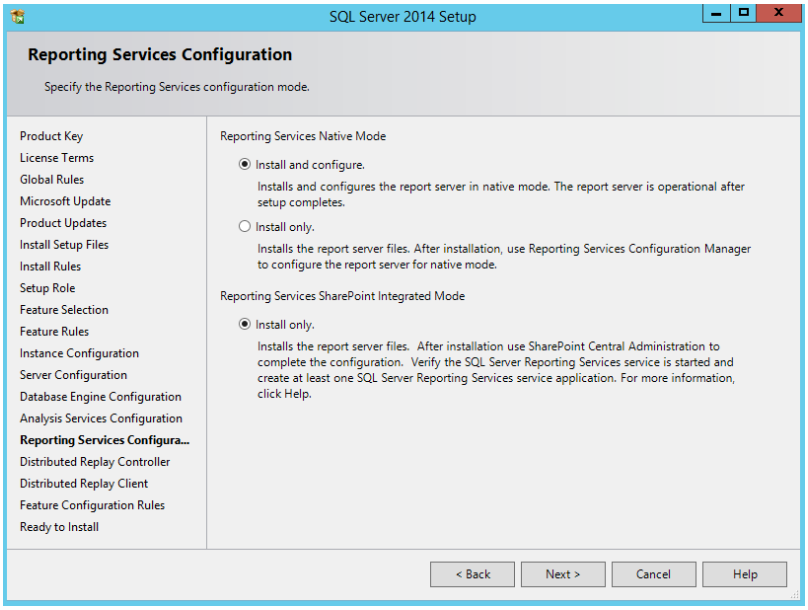
10. Click **Add Current User**, add Analysis Services administrator permissions for the current account, and click **Next**.

Figure 12-24 SQL Server administrator account 2



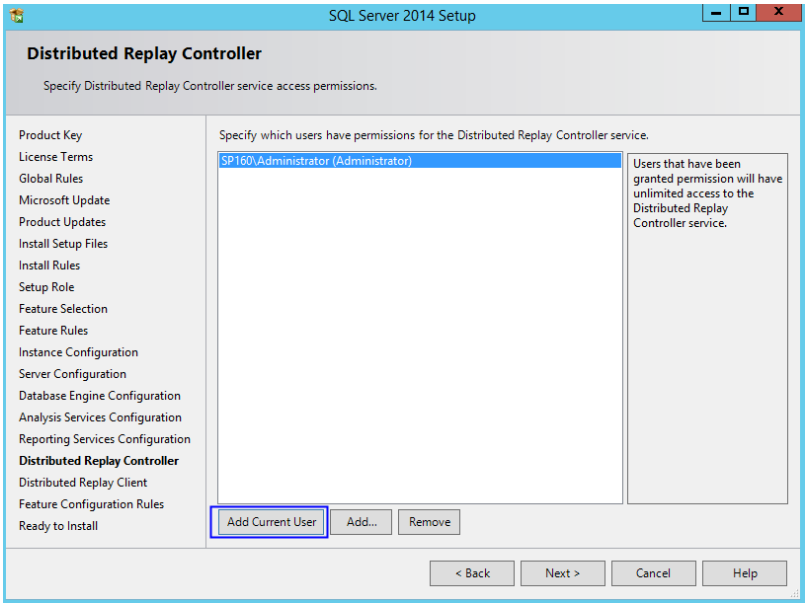
11. Retain the default setting in **Reporting Services Configuration** and click **Next**.

Figure 12-25 Reporting Services Configuration



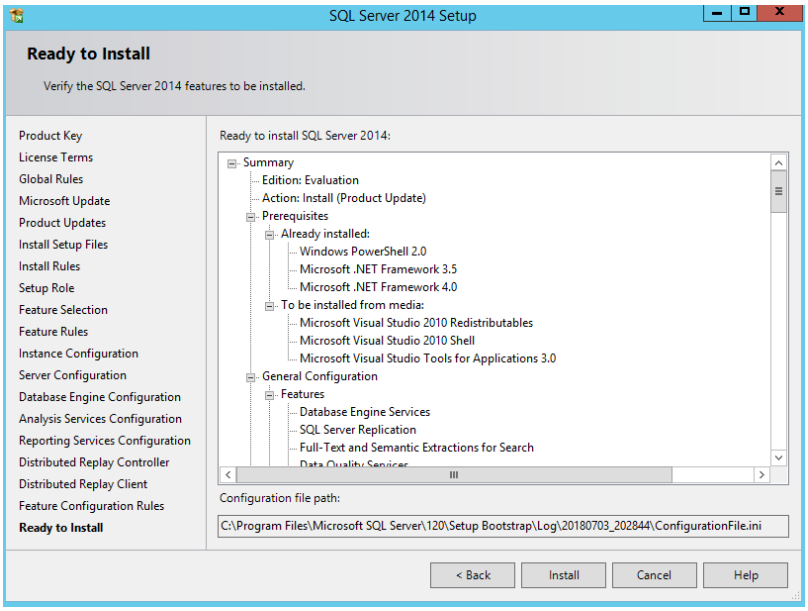
12. Click **Add Current User**, add Distribution Replay Controller service permissions for the current account, and click **Next**.

Figure 12-26 Distribution Replay Controller service



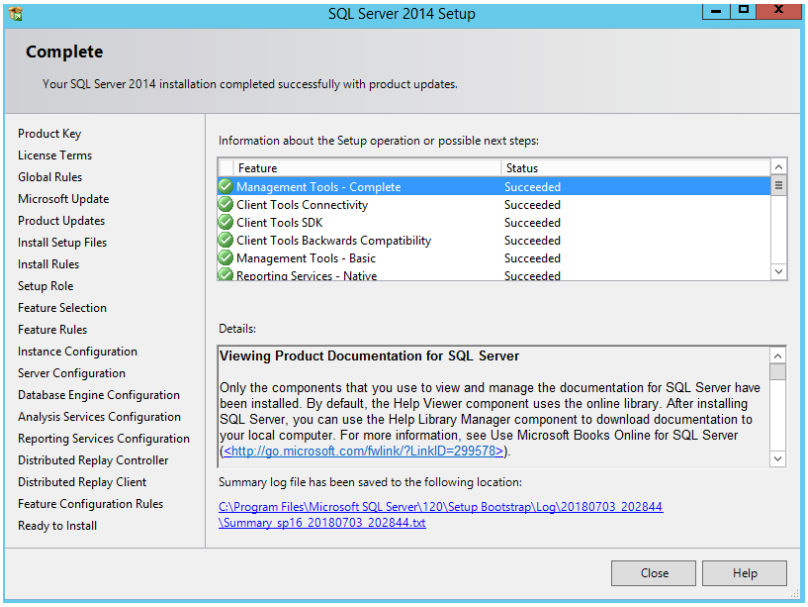
13. Confirm SQL Server configurations and click **Install**.

Figure 12-27 SQL Server installation



14. Click **Close**. The SQL Server installation is complete.

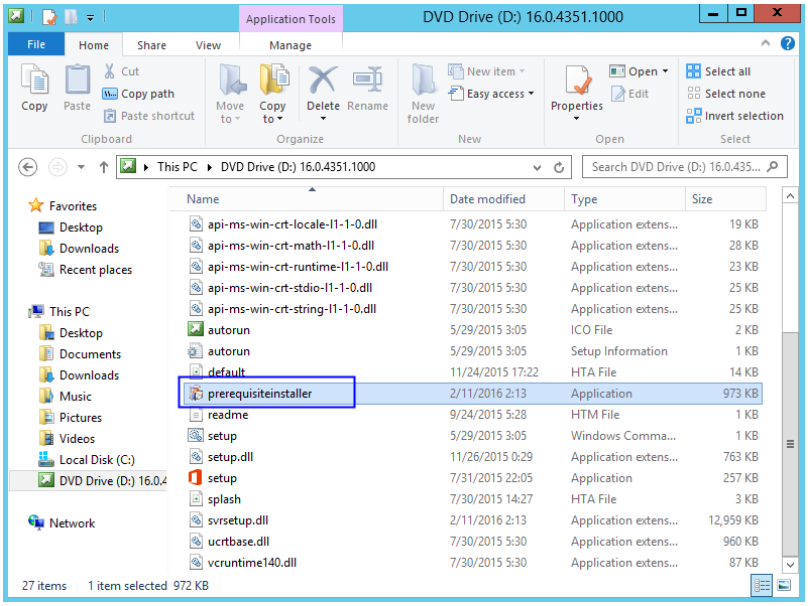
Figure 12-28 Finish SQL Server installation



12.4 Installing Microsoft SharePoint Server 2016

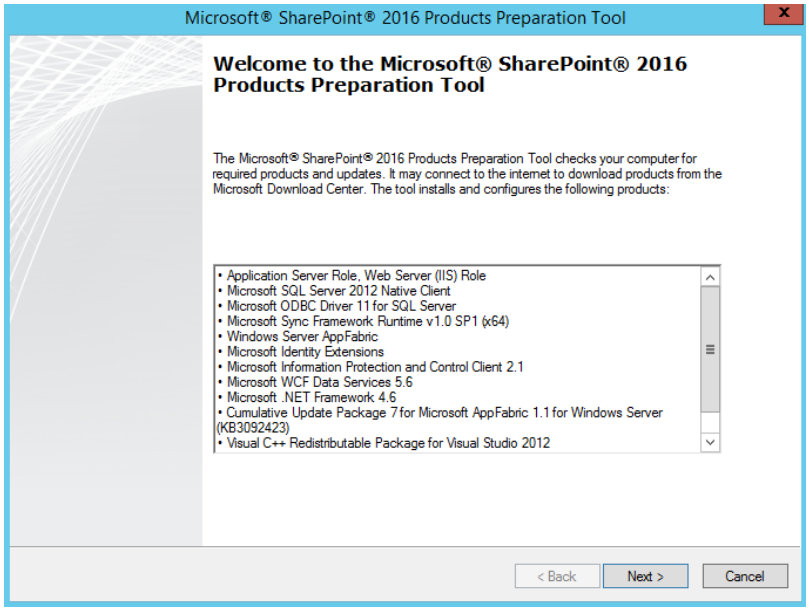
1. Open the image file and double-click the executable file of the preparation tool to install SharePoint 2016 preparation tool.

Figure 12-29 SharePoint preparation tool



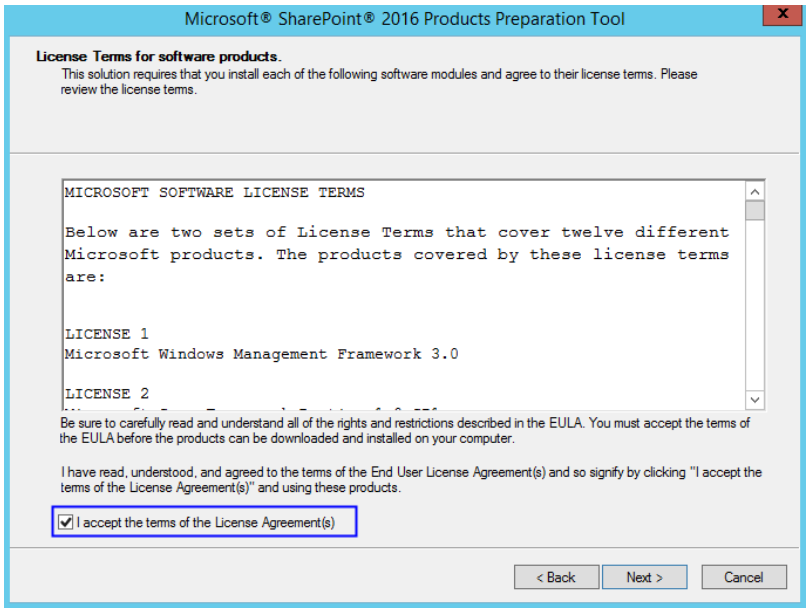
2. Open the installation wizard of the SharePoint preparation tool and click **Next**.

Figure 12-30 SharePoint preparation tool installation wizard



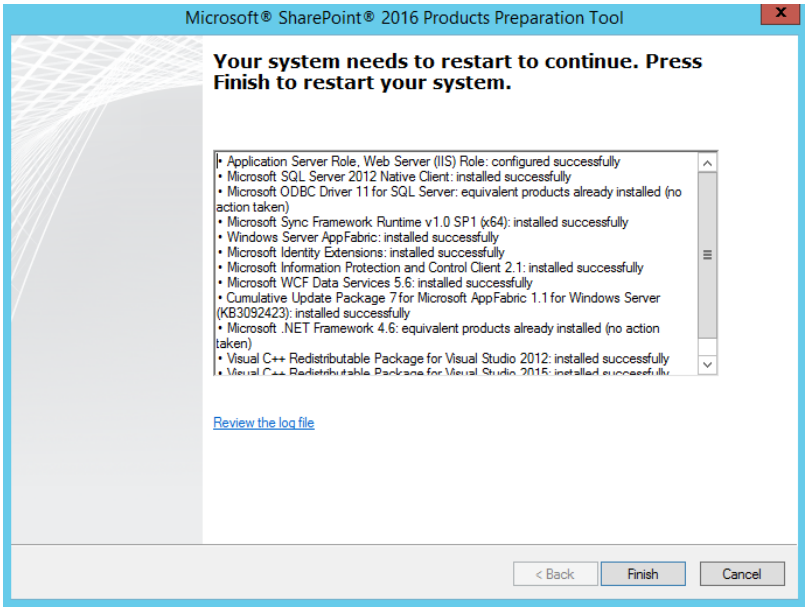
3. Select **I accept the terms of the License Agreement(s)** and click **Next**.

Figure 12-31 SharePoint preparation tool license



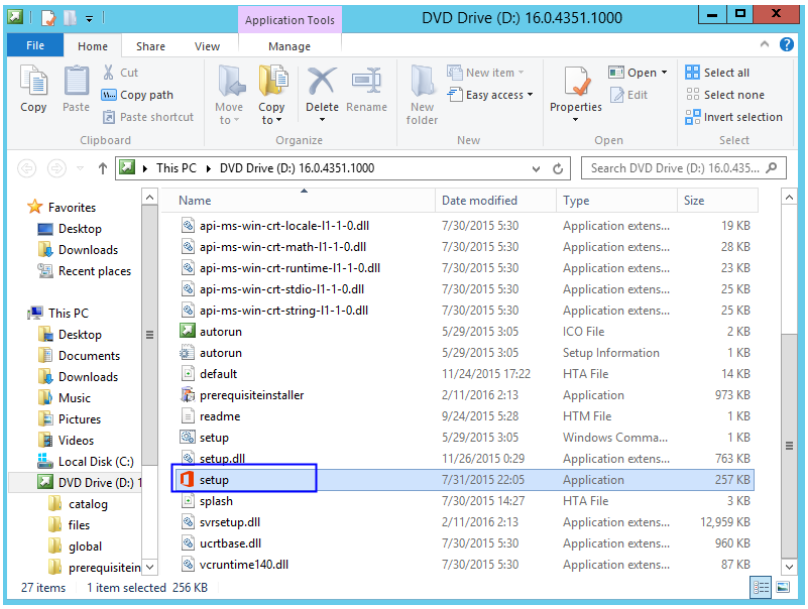
4. After the preparation tool is installed, click **Finish** to restart the system.

Figure 12-32 Successful preparation tool installation



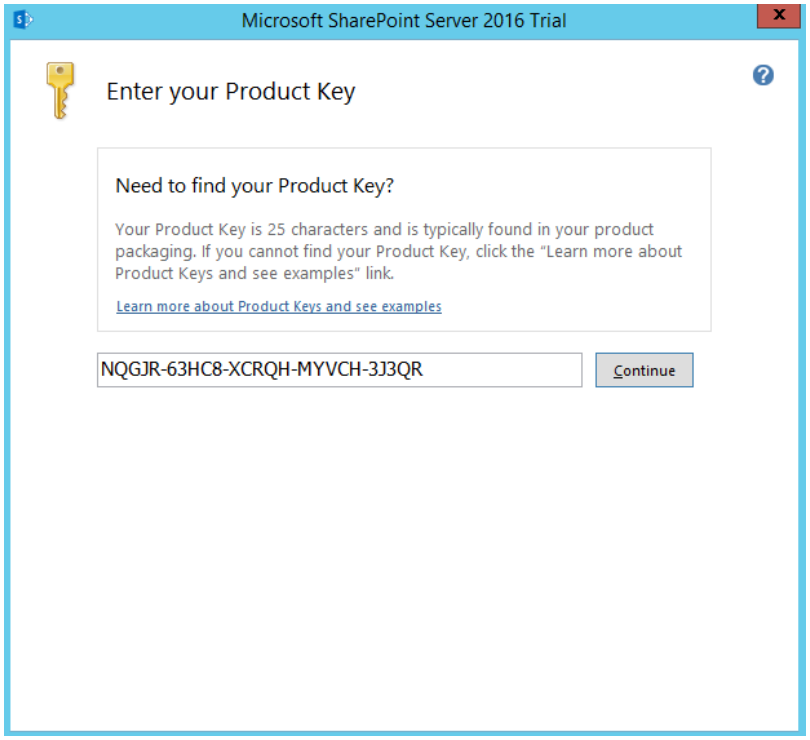
5. Double-click the installation file to install SharePoint.

Figure 12-33 Installing SharePoint



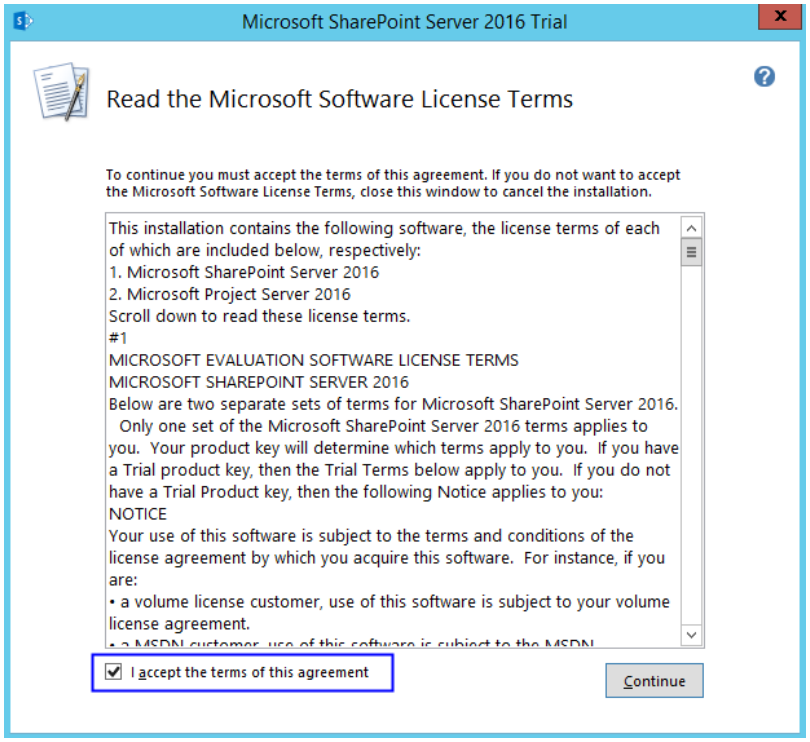
6. Enter the key of the SharePoint product. The key of the 180-day trial edition is **NQGJR-63HC8-XCRQH-MYVCH-3J3QR**.

Figure 12-34 SharePoint product key



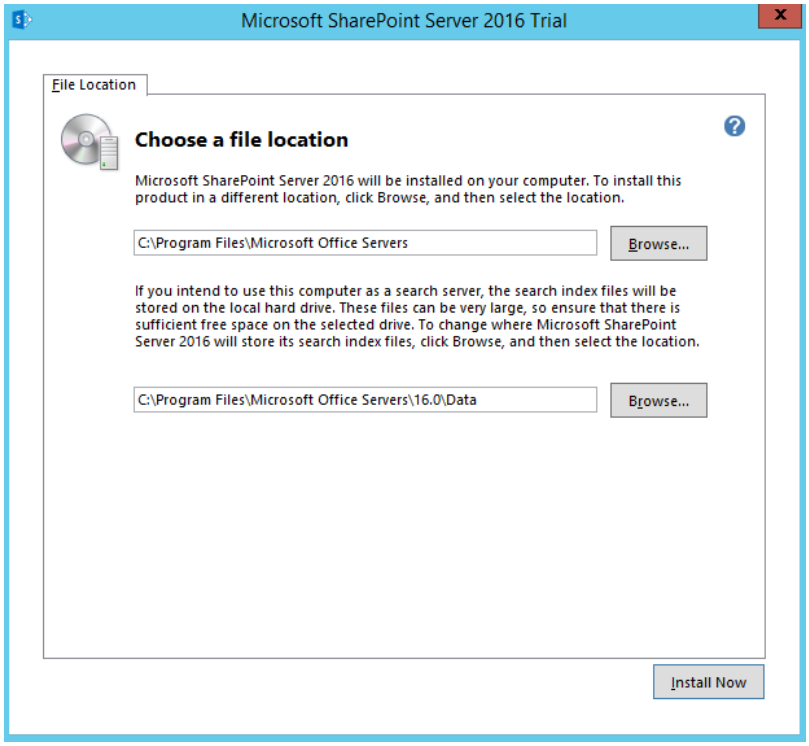
7. Accept the license and click **Continue**.

Figure 12-35 SharePoint license terms



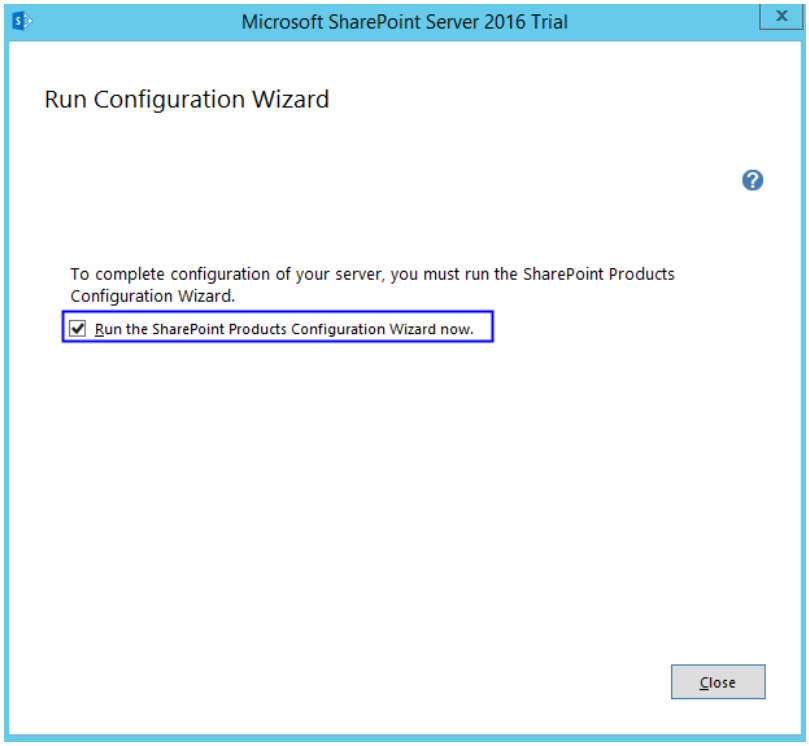
8. Retain the default installation paths.

Figure 12-36 SharePoint installation paths



9. Click **Install Now**.
10. After **SharePoint** is installed, select **Run the SharePoint Products Configuration Wizard now.** to run the SharePoint configuration wizard.

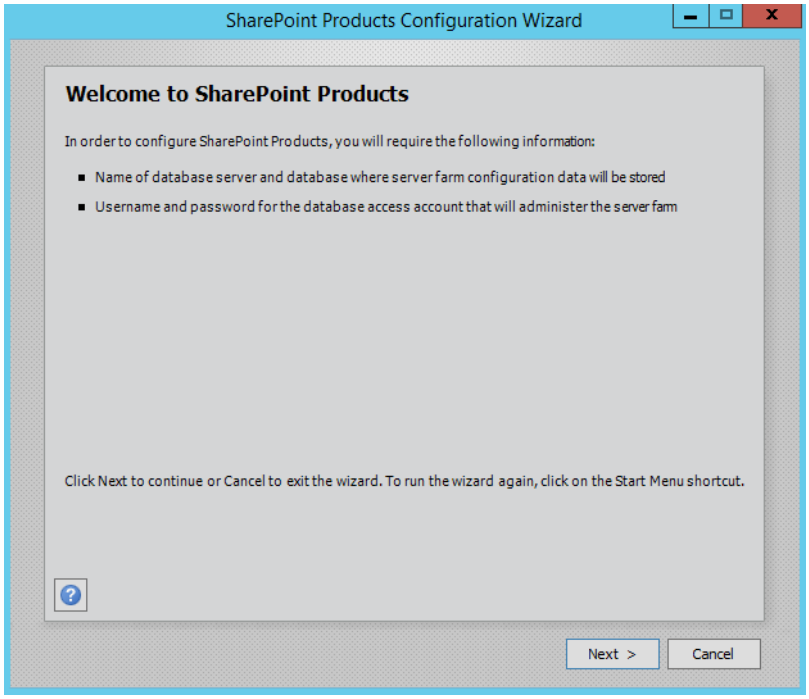
Figure 12-37 Successful SharePoint installation



12.5 Configuring Microsoft SharePoint Server 2016

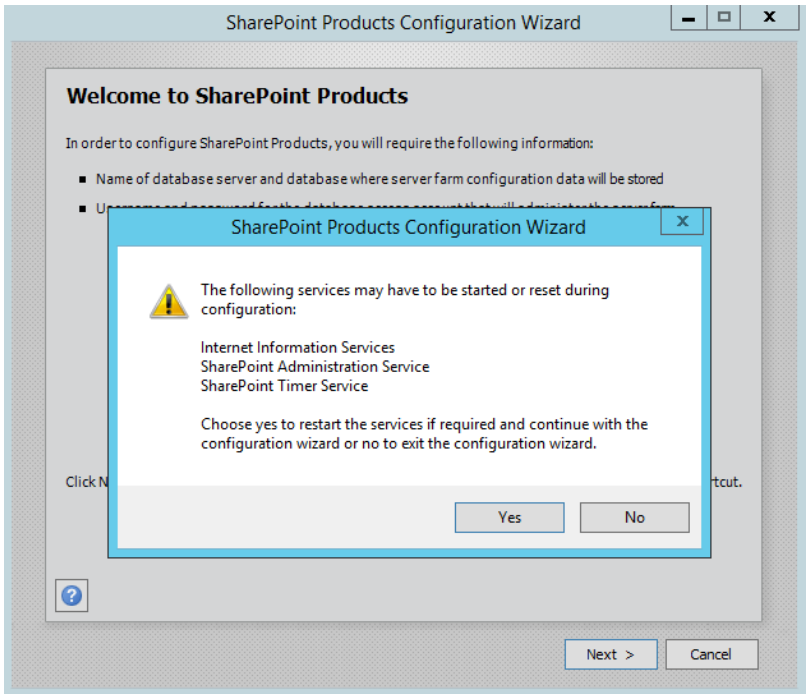
1. In the SharePoint products configuration wizard, click **Next**.

Figure 12-38 SharePoint Products Configuration Wizard



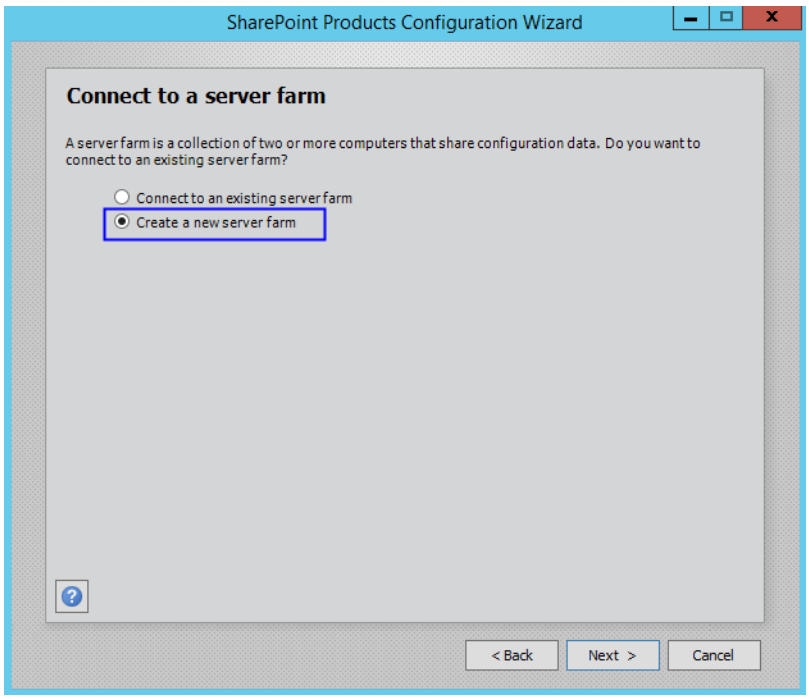
2. Click **Yes** to allow service restart during the configuration.

Figure 12-39 Service restart prompt



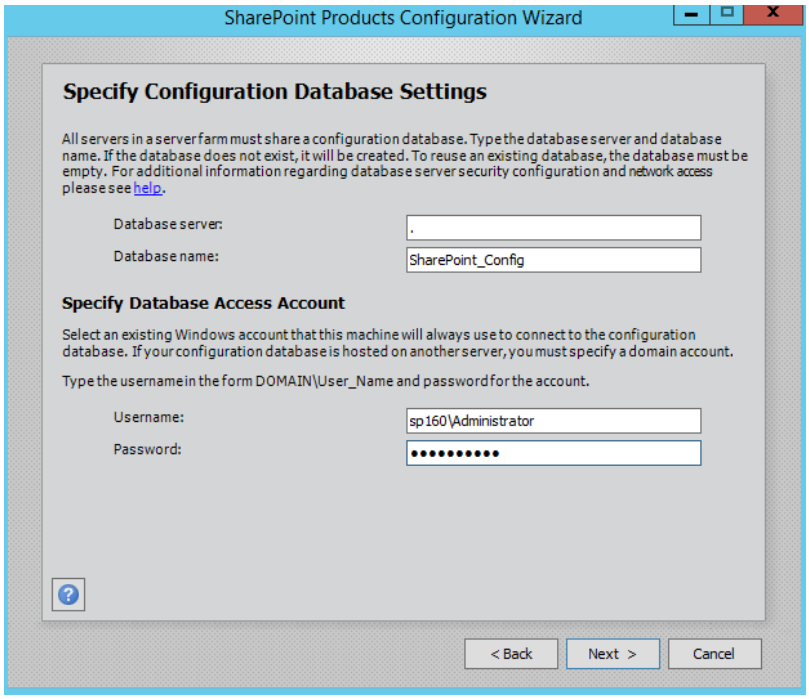
3. Select **Create a new server farm**.

Figure 12-40 Create a new server farm



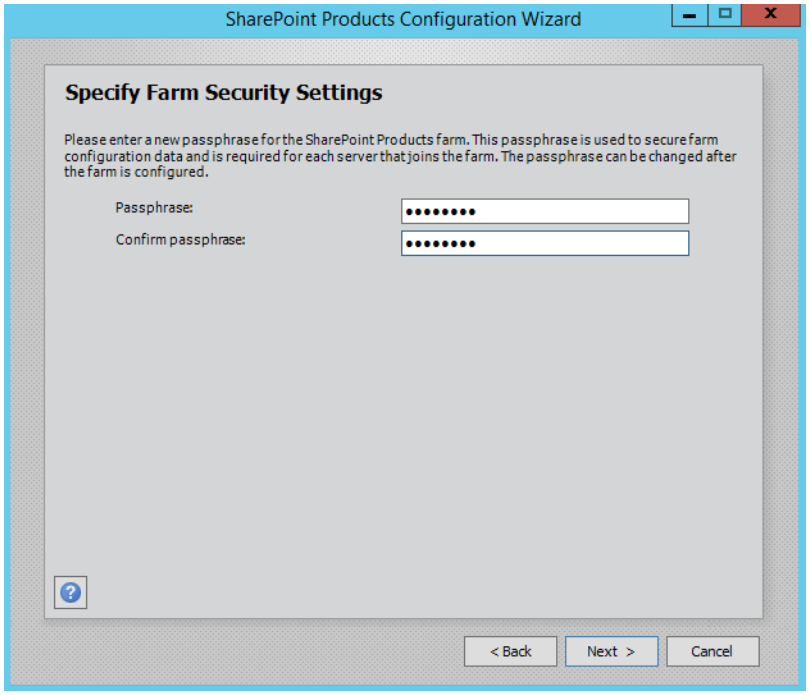
4. Configure the configuration database. The SharePoint database is on the local host. Therefore, you need to enter the local database and account. Then, click **Next**.

Figure 12-41 Configuring the SharePoint database



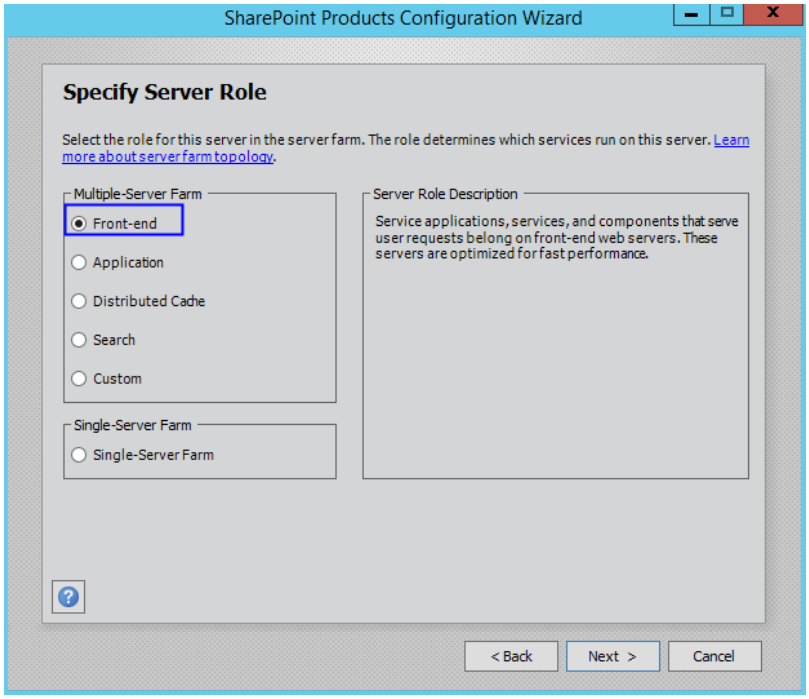
5. Enter the password of the server farm and click **Next**.

Figure 12-42 Setting the password for the SharePoint server farm



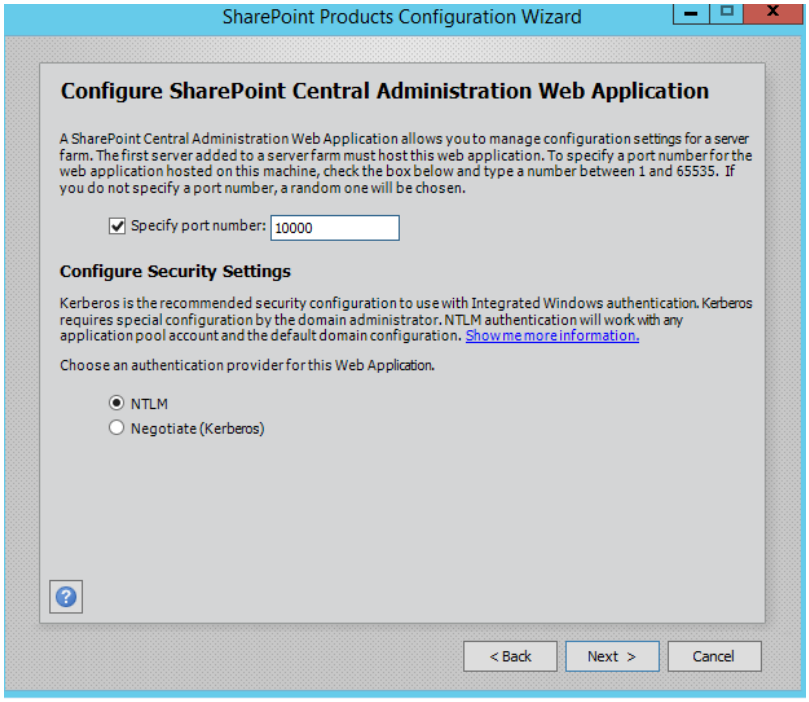
6. Select **Front-end** and click **Next** to specify the server role.

Figure 12-43 Setting the SharePoint server role



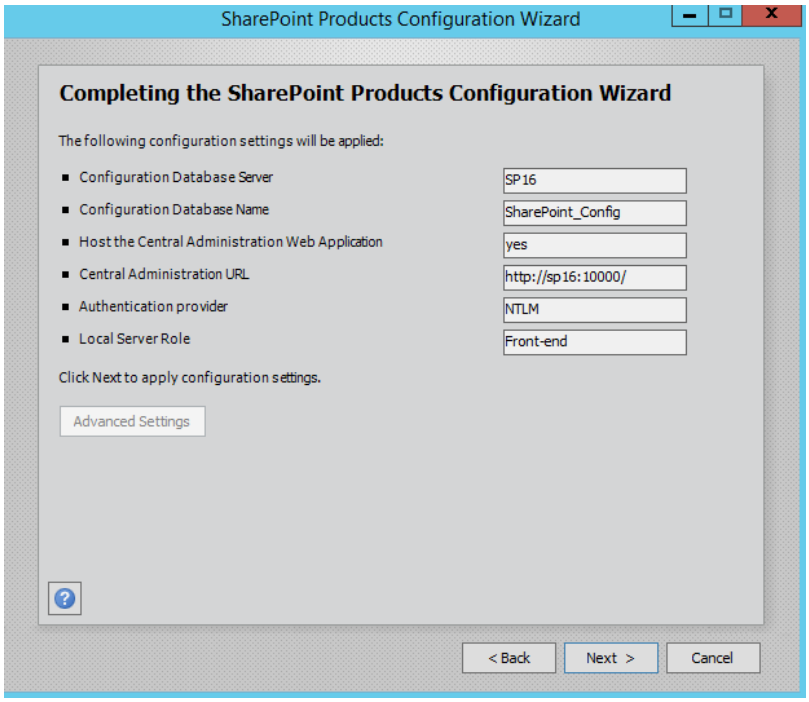
7. Set the port number of SharePoint Central Administration Web Application to **10000**.

Figure 12-44 Port number of SharePoint Central Administration Web Application



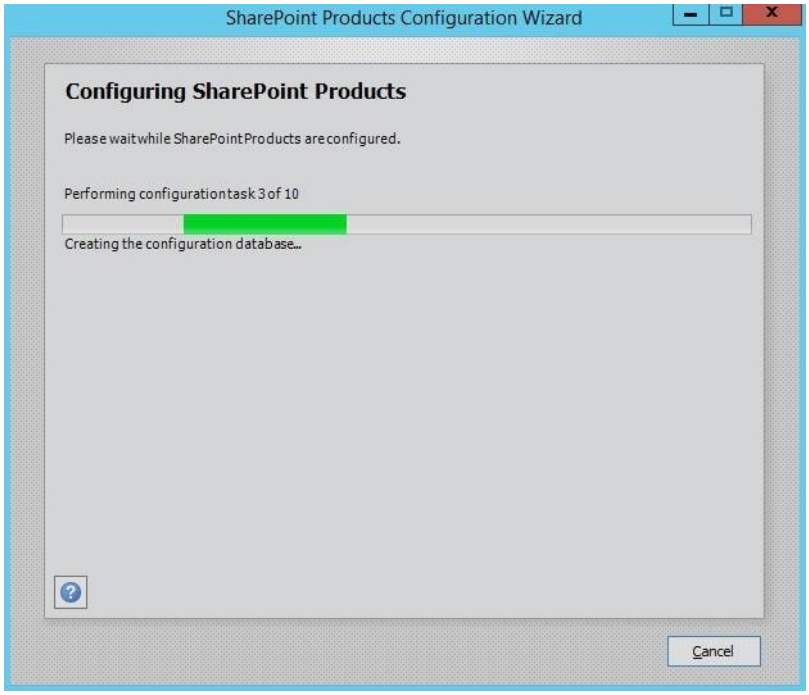
8. Check and confirm the SharePoint configurations.

Figure 12-45 SharePoint configurations



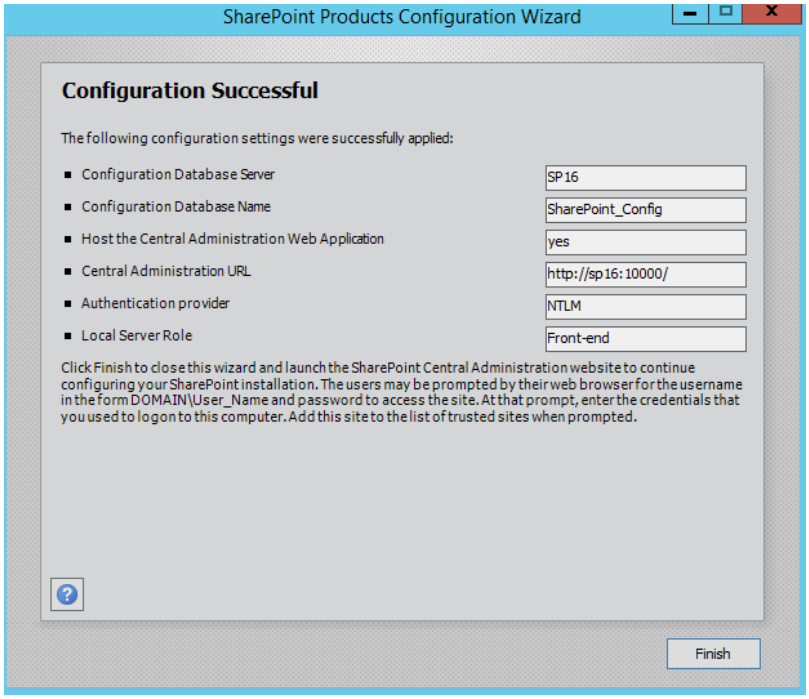
9. Click **Next** to start configuring SharePoint.

Figure 12-46 Configuration progress



10. After SharePoint is configured successfully, click **Finish**.

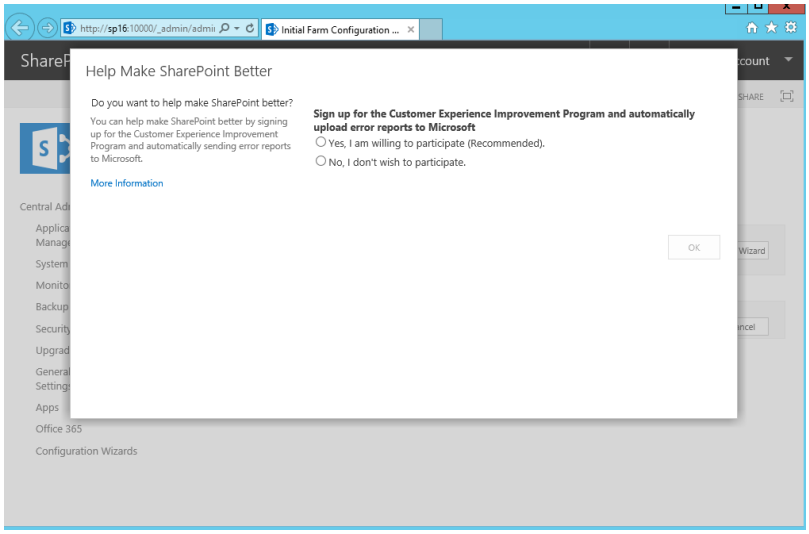
Figure 12-47 Successful SharePoint configuration



12.6 Verifying Microsoft SharePoint Server 2016

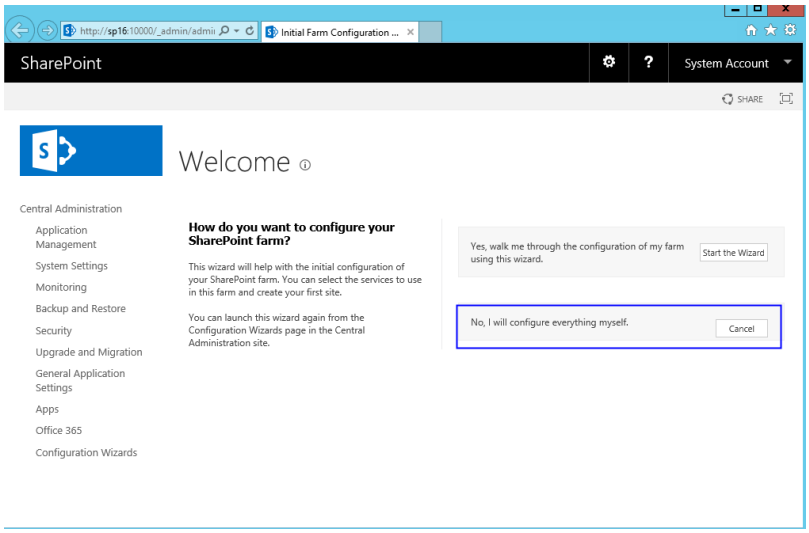
1. Open the SharePoint central administration.

Figure 12-48 SharePoint central administration



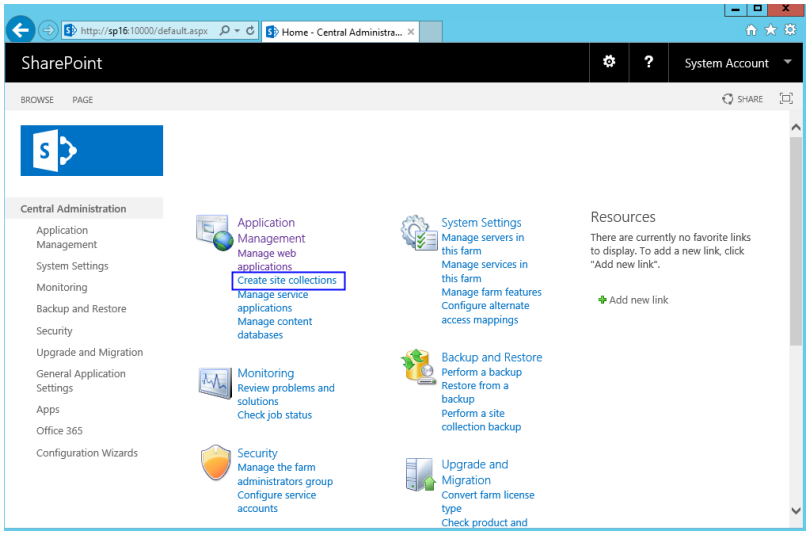
2. Select the method to configure the SharePoint farm. Click **Cancel**.
   To configure the SharePoint farm through the wizard, click **Start the Wizard**.

Figure 12-49 SharePoint farm configuration



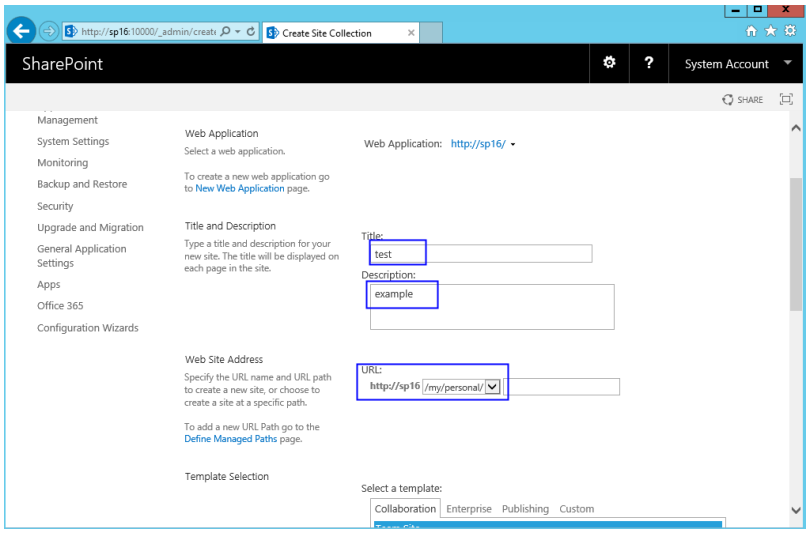
3. In the SharePoint central administration, click **Create site collections** to create a SharePoint site.

Figure 12-50 Creating a SharePoint site



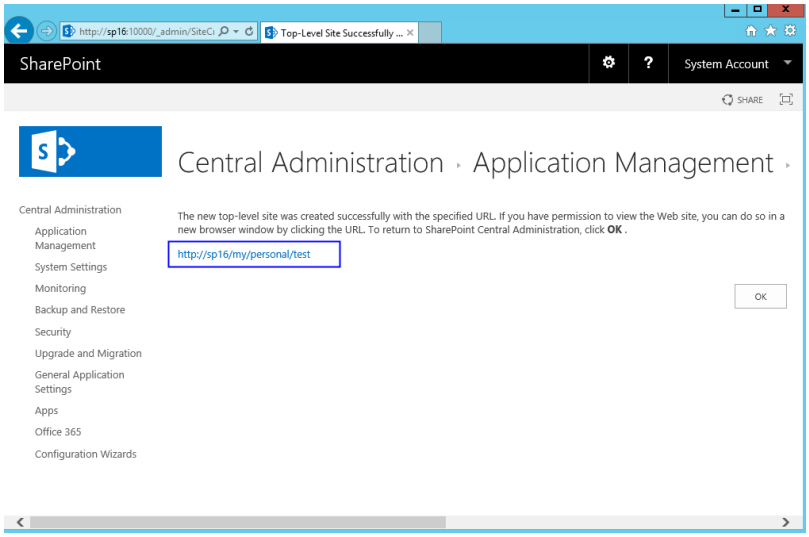
4. Set SharePoint site parameters.

Figure 12-51 Setting SharePoint site parameters



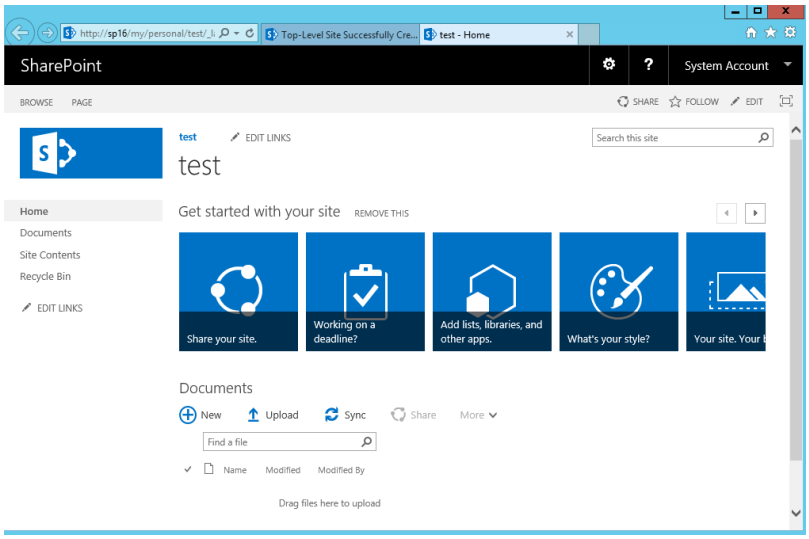
5. The SharePoint top-level site is created successfully. Click the link to open the page.

Figure 12-52 SharePoint top-level site created successfully



6. Open the SharePoint site, where you can design your web pages.

Figure 12-53 SharePoint verification



13 Manually Deploying LNMP (CentOS 7.2, PHP 7.0)

Overview

The best practices for HUAWEI CLOUD ECS guide you through the deployment of LNMP on a Linux ECS. The CentOS 7.2 64bit OS is used as an example in this section.

The process is as follows:

1. **Install Nginx.**
2. **Install MySQL.**
3. **Install PHP.**
4. **Test the LNMP deployment.**

Prerequisites

1. The ECS has had an EIP bound.
2. The rule listed in the following table has been added to the security group to which the target ECS belongs. For details, see **Adding a Security Group Rule**.

Table 13-1 Security group rule

Transfer Direction	Protocol/Application	Port/Range	Source End
Inbound	HTTP (80)	80	0.0.0.0/0

Procedure

Step 1 Install Nginx.

1. Log in to the ECS.
2. Run the following command to download the Nginx package:

   wget http://nginx.org/packages/centos/7/noarch/RPMS/nginx-release-centos-7-0.el7.ngx.noarch.rpm

3. Run the following command to create the Nginx yum repository:

   rpm -ivh nginx-release-centos-7-0.el7.ngx.noarch.rpm

4. Run the following command to install Nginx:

   yum -y install nginx

5. Run the following commands to start Nginx and configure automatic Nginx enabling upon ECS startup:

   systemctl start nginx

   systemctl enable nginx

6. Enter http://*IP address of the Nginx server* in the address bar to visit Nginx. If the following page is displayed, Nginx has been installed.

Step 2 Install MySQL.

1. Run the following commands to install MySQL:

   rpm -Uvh http://dev.mysql.com/get/mysql57-community-release-el7-8.noarch.rpm

   yum -y install mysql-community-server

2. Run the following commands to start MySQL and configure automatic MySQL enabling upon ECS startup:

   systemctl start mysqld

   systemctl enable mysqld

3. Run the following command to obtain the password of user **root** that is automatically set during MySQL installation:

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

   Information similar to the following is displayed:

   ```
   2018-08-29T07:27:37.541944Z 1 [Note] A temporary password is generated for root@localhost: 2YY?3uHUA?Ys
   ```

4. Run the following command and perform operations as prompted to harden MySQL:

   mysql_secure_installation

   ```
   Securing the MySQL server deployment.

   Enter password for user root:    #Enter the obtained password of user root.
   The existing password for the user account root has expired. Please set a new password.

   New password:  #Enter the new password.

   Re-enter new password:   #Enter the new password again.
   The 'validate_password' plugin is installed on the server.
   The subsequent steps will run with the existing configuration of the plugin.
   ```



```
Using existing password for root.

Estimated strength of the password: 100
Change the password for root ? ((Press y|Y for Yes, any other key for No) : N    #Asks you whether to change the password of user root. Press n.

 ... skipping.
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y    #Asks you whether to remove anonymous users. Press 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    #Asks you whether to forbid remote login of user root. Press y.
Success.

By default, MySQL comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : Y    #Asks you whether to delete the test database and cancel access permissions to it. Press y.
 - Dropping test database...
Success.

 - Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : Y    #Asks you whether to reload privilege tables. Press y.
Success.

All done!
```

Step 3 Install PHP.

1. Run the following commands to install PHP 7 and PHP extensions required for installing LNMP:

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

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

   yum -y install php70w-tidy php70w-common php70w-devel php70w-pdo php70w-mysql php70w-gd php70w-ldap php70w-mbstring php70w-mcrypt php70w-fpm

2. Run the following command to check the PHP installation:

   php -v

   If information similar to the following is displayed, PHP has been installed:

   ```
   PHP 7.0.31 (cli) (built: Jul 20 2018 08:55:22) ( NTS )
   Copyright (c) 1997-2017 The PHP Group
   Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies
   ```

3. Run the following commands to start PHP and configure automatic PHP enabling upon ECS startup:

   systemctl start php-fpm

systemctl enable php-fpm

4. Modify the Nginx configuration file to support PHP.
   a. Run the following command to open the **default.conf** file:

      vim /etc/nginx/conf.d/default.conf

   b. Press **i** to enter editing mode.
   c. Modify the **default.conf** file.

      - Add PHP to the supported homepage formats.

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

      - Comment out the following content and set the data in bold as the default Nginx path:

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

   d. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the configuration file.
5. Run the following command to reload the Nginx configuration file:

   service nginx reload

Step 4 Test the LNMP deployment.

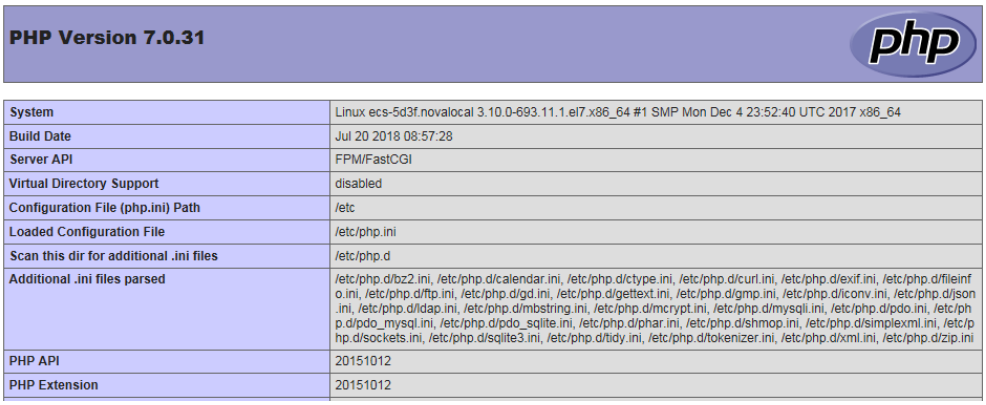
1. Create the **info.php** test page in **/usr/share/nginx/html/**.
   a. Run the following command to create and open the **info.php** test file:

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

   b. Press **i** to enter editing mode.
   c. Modify the **info.php** file and add the following data to the file:

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

   d. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the configuration file.
2. Enter http://*Server IP address*/info.php in the address bar. If the following page is displayed, the LNMP environment has been deployment.



PHP Version 7.0.31

System	Linux ecs-5d3f.novalocal 3.10.0-693.11.1.el7.x86_64 #1 SMP Mon Dec 4 23:52:40 UTC 2017 x86_64
Build Date	Jul 20 2018 08:57:28
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/bz2.ini, /etc/php.d/calendar.ini, /etc/php.d/ctype.ini, /etc/php.d/curl.ini, /etc/php.d/exif.ini, /etc/php.d/fileinfo.ini, /etc/php.d/ftp.ini, /etc/php.d/gd.ini, /etc/php.d/gettext.ini, /etc/php.d/gmp.ini, /etc/php.d/iconv.ini, /etc/php.d/json.ini, /etc/php.d/ldap.ini, /etc/php.d/mbstring.ini, /etc/php.d/mcrypt.ini, /etc/php.d/mysqli.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/shmop.ini, /etc/php.d/simplexml.ini, /etc/php.d/sockets.ini, /etc/php.d/sqlite3.ini, /etc/php.d/tidy.ini, /etc/php.d/tokenizer.ini, /etc/php.d/xml.ini, /etc/php.d/zip.ini
PHP API	20151012
PHP Extension	20151012

----End

14 Manually Deploying Docker (CentOS 7.5)

Overview

The best practices for HUAWEI CLOUD ECS guide you through the deployment of Docker on a Linux ECS. Additionally, common Docker operations and the process of creating a Docker image are provided.

Table 14-1 Docker terminologies

Term	Description
Docker	Docker is a platform for developers and system administrators to develop, deploy, and run applications using containers.
Docker image	Docker image is a special file system, which provides the programs, libraries, resources, and configuration files required for running containers. A Docker image also contains configuration parameters, for example, for anonymous disks, environment variables, and users. A Docker image does not contain any dynamic data, and its content remains unchanged after being built.
Container	The relationship between a Docker image and a container is similar to that between a class and an instance in object-oriented programming. Images are static, and containers are entities for running images. A container can be created, started, stopped, deleted, and suspended.

For more information about Docker, image, and container, see **Docker Documentation**.

Docker requires 64bit OSs with a kernel version being 3.10 or later. This section uses CentOS 7.5 64 3.10.0-862.9.1.el7.x86_64 as an example.

Prerequisites

- The target ECS has an EIP bound. For instructions about how to bind an EIP to an ECS, see **Assigning an EIP and Binding It to an ECS**.
- The rule listed in the following table has been added to the security group to which the target ECS belongs. For details, see **Adding a Security Group Rule**.

Table 14-2 Security group rule

Transfer Direction	Type	Protocol	Port/Range	Remote End
Inbound	IPv4	TCP	80	0.0.0.0/0

Deploying Docker

1. Log in to the ECS.
2. Add a yum source.

   yum install epel-release -y

   yum clean all
3. Install and run Docker.

   yum install docker-io -y

   systemctl enable docker

   systemctl start docker
4. Check the installation.

   docker --version

   If the information similar to the following is displayed, Docker has been installed:

   ```
   Docker version 1.13.1, build 8633870/1.13.1
   ```

Basic Operations on Docker

1. Managing Docker processes
   - Start Docker.

     systemctl start docker
   - Stop Docker.

     systemctl stop docker
   - Restart Docker.

     systemctl restart docker
2. Managing Docker images
   a. Pull docker images, taking official Apache and CentOS images as an example.

      docker pull *httpd*

      docker pull *centos*

   b. View existing images.

docker images

```
[root@ecs-b67a-docker ~]# docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
docker.io/httpd     latest              55a118e2a010        2 weeks ago         132 MB
docker.io/centos    latest              75835a67d134        5 weeks ago         200 MB
[root@ecs-b67a-docker ~]#
```

c. Forcibly delete an image.

docker rmi *centos*

3. Managing containers

a. Create a container and run it.

docker run -it -d -p *80:80* **--name** *datahttpd* **-v** */data/:/var/www/httpd/* **httpd**

The parameters are as follows:

- **-i**: runs the container in interactive mode, which is usually used with **-t**.
- **-t**: reallocates a pseudo input terminal to the container. This parameter is usually used with **-i**.
- **-d**: runs the container at the backend and returns the container ID.
- **-p**: port mapping, in the format of "Host port:Container port".
- **--name**: specifies a name for the container.
- **-v**: mounts an absolute directory on the host to the image, in the format of "Directory on the host:Mount path in the image".

NOTE

In the preceding parameters, the host is the target ECS.

For example, use image **httpd** to start a container in interactive mode, map port 80 on the container to port 80 on the host, and map **/data** on the host to **/var/www/httpd** on the container, and have the container ID returned. Then, run the following command:

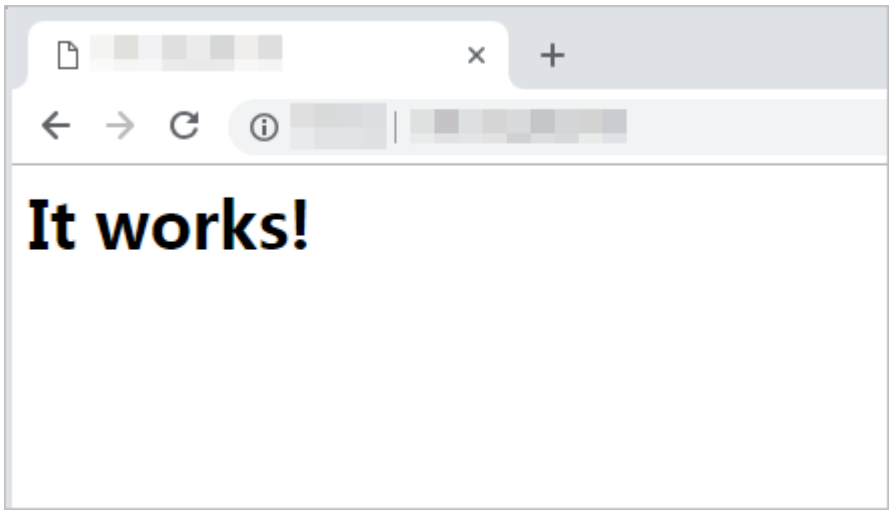
```
[root@ecs-b67a-docker ~]# docker run -it -d -p 80:80  --name datahttpd -v /data/:/var/www/httpd/ httpd
6a514dea52a9465c1f6863c0f17ff41debda231ccff8bf66e3c0dbcc5f33cb20
[root@ecs-b67a-docker ~]#
```

b. Check whether the container has been started.

docker ps -a

```
[root@ecs-b67a-docker ~]# docker ps -a
CONTAINER ID        IMAGE               COMMAND              CREATED             STATUS              PORTS               NAMES
6a514dea52a9        httpd               "httpd-foreground"   4 minutes ago       Up 4 minutes        0.0.0.0:80->80/tcp  datahttpd
[root@ecs-b67a-docker ~]#
```

c. In the address bar of the browser, enter the EIP bound to the ECS and check the running status of the container. If the following information is displayed, the container is running properly.



Creating an Image

Use **Dockerfile** to custom a simple Nginx image.

1. Create a file named **Dockerfile**.

   mkdir mynginx

   cd mynginx

   touch Dockerfile

2. Edit the file.

   vim Dockerfile

   Add the following data to **Dockerfile**:

   ```
   FROM nginx
   RUN echo '<h1>Hello, Docker!</h1>' > /usr/share/nginx/html/index.html
   ```

   Simple **Dockerfile** commands are as follows (for more information, log in at **https://hub.docker.com/**):

   - **FROM** statement: mandatory and must be the first instruction in **Dockerfile**, indicating that the Nginx image is used as a basic image.
   - **RUN** statement: indicates that the echo command is executed in the format of "RUN <Command>", and message "Hello, Docker!" is displayed on the screen.

3. Build the image.

   docker build -t nginx:v3 .

   - **-t nginx:v3**: specifies the image name and version.
   - **.**: specifies the context path. After the image built command is executed, all data in the path will be packed to the Docker engine to build the image.

4. Check the created Nginx image, the version of which is v3.

   docker images

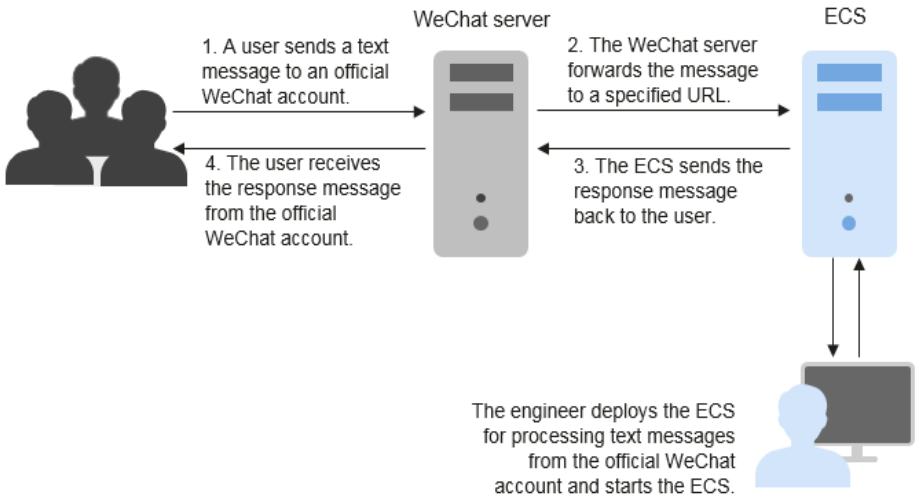
   ```
   REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
   nginx               v3                  09422e465d96        10 seconds ago      109 MB
   ```


15 Deploying an ECS for Transceiving Text Messages from an Official WeChat Account

Overview

The best practices for HUAWEI CLOUD ECS guide you through the deployment of an ECS as an official WeChat account server so that the ECS receives text messages from the WeChat server and sends processing results to end users. On this ECS, Python is used to compile the logic code for processing WeChat messages. **Figure 15-1** shows the service flow.

Figure 15-1 Flowchart for processing text messages

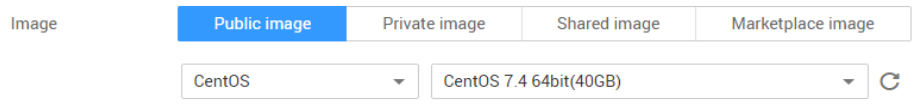


Before performing the operations described in this section, you are required to have basic knowledge on the CentOS (Linux), Python language, Web.py framework, and HTTP/XML protocol.

Preparations

- Apply for an official WeChat account.
  URL: **https://mp.weixin.qq.com/**
  This section uses the Service Infographics WeChat account as an example.
- Purchase an ECS.
  If you have not obtained a HUAWEI CLOUD account, register with HUAWEI CLOUD and complete real-name authentication.
  This section uses an ECS running CentOS 7.4 as an example.

  Figure 15-2 Public image

- Purchase an EIP.
  Purchase an EIP with your ECS. The EIP will be configured in the official WeChat account.

  Figure 15-3 EIP

Installing Basic Software

This section uses Python and Web.py to develop the official WeChat account. You are required to install or upgrade Python, pip, Web.py framework, and WinSCP software.

Upgrade the default Python version.

The Python version delivered with CentOS 7.4 is too early to use. You are advised to upgrade it to Python3.

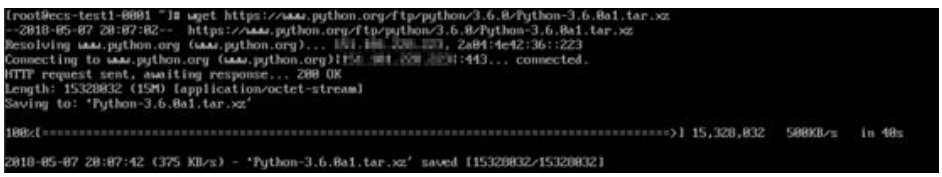
1. Run the following command to view the Python version:
   ```
   python --version
   ```

   Figure 15-4 Viewing the Python version

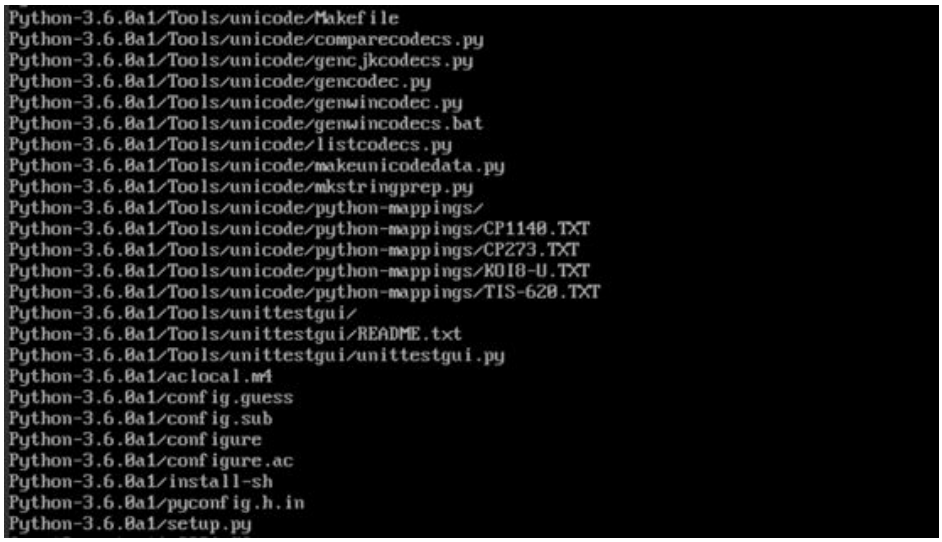
2. Download the Python installation package, taking Python 3.6.0 as an example.
   ```
   wget https://www.python.org/ftp/python/3.6.0/Python-3.6.0a1.tar.xz
   ```

   Figure 15-5 Downloading the Python installation package

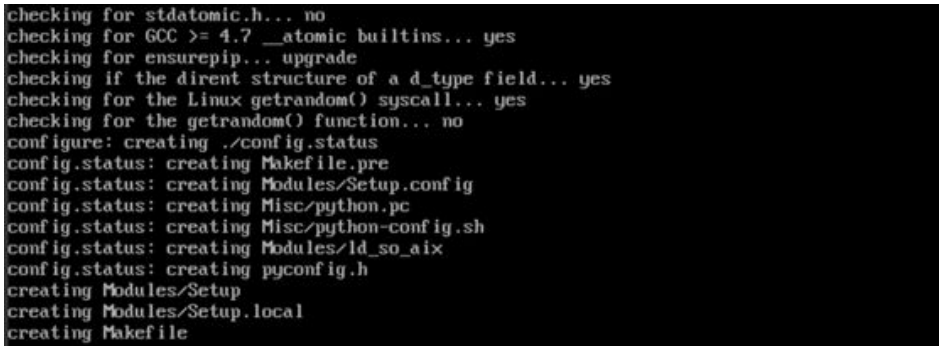
3. Run the following command to decompress the installation package:
```
tar xvf Python-3.6.0a1.tar.xz
```

Figure 15-6 Decompressing the installation package



4. Run the following command to configure the environment:
```
./configure
```
   - If the command output shown in **Figure 15-7** is displayed, the command has been successfully executed.

     Figure 15-7 Successful execution

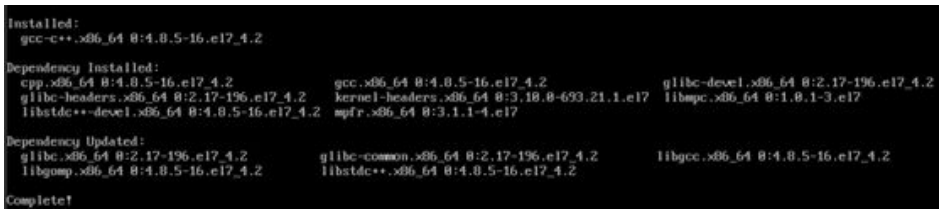
     

   - If the message "configure: error: no acceptable C compiler found in $PATH" is displayed, no proper compiler has been installed.

     To resolve this issue, perform the following operations:

     Run the following command to install or upgrade GCC and its dependent package:
     ```
     sudo yum install gcc-c++
     ```
     Enter **y** and press **Enter** as prompted. If information shown in **Figure 15-8** is displayed, the dependency package has been installed.

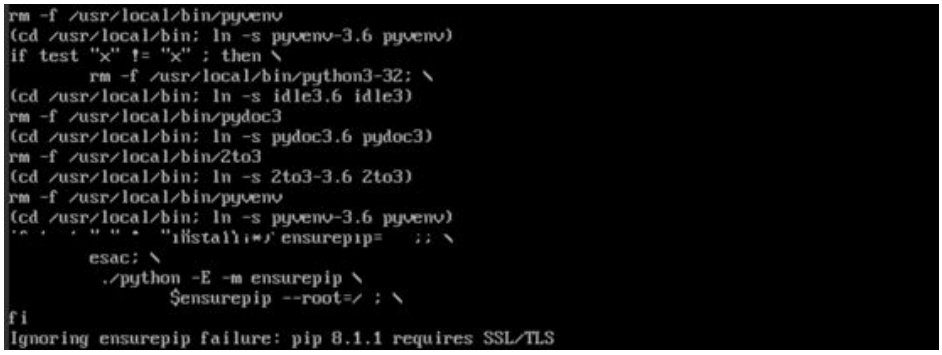
Figure 15-8 Successful installation



Run the **./configure** command again.

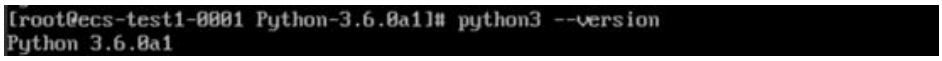
5. Run the following command to install Python:
   ```
   make && make install
   ```
   If the system displays a pip error after the command execution, the openssl-devel package is unavailable. Ignore the error.

   Figure 15-9 Successful execution

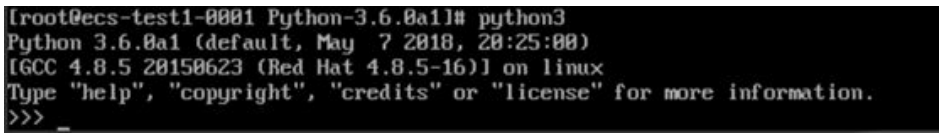
6. Run the following command to view the Python3 version:
   ```
   python3 --version
   ```

   Figure 15-10 Viewing the Python3 version

7. Run the following command to verify the Python3 installation:
   ```
   python3
   ```
   If information shown in the following figure is displayed, Python3 has been installed.

   Figure 15-11 Successful installation

Upgrade the default pip version.

pip is a common Python package management tool, which allows you to search for, download, install, and uninstall Python packages. pip3 is delivered with Python3, but the version is too early to use. Upgrade pip to the latest version. During Python3 installation, the error message "Ignoring ensurepip failure: pip 8.1.1 requires SSL/TLS" indicates a pip installation failure. Therefore, pip must be reinstalled.

1. Run the following command to install the openssl-devel package:
```
yum install openssl-devel -y
```

Figure 15-12 Installing the openssl-devel package

```
Installed:
  openssl-devel.x86_64 1:1.0.2k-8.el7

Dependency Installed:
  keyutils-libs-devel.x86_64 0:1.5.8-3.el7   krb5-devel.x86_64 0:1.15.1-8.el7
  libcom_err-devel.x86_64 0:1.42.9-10.el7    libkadm5.x86_64 0:1.15.1-8.el7
  libselinux-devel.x86_64 0:2.5-11.el7       libsepol-devel.x86_64 0:2.5-6.el7
  libverto-devel.x86_64 0:0.2.5-4.el7        pcre-devel.x86_64 0:8.32-17.el7
  zlib-devel.x86_64 0:1.2.7-17.el7

Complete!
```

2. Run the following command to verify the package installation:
```
make && make install
```
If information shown in the following figure is displayed, pip has been installed.

Figure 15-13 Successful installation

```
Collecting setuptools
Collecting pip
Installing collected packages: setuptools, pip
Successfully installed pip-8.1.1 setuptools-20.10.1
```

3. Run the following command to upgrade pip3:
```
pip3 install --upgrade pip
```
If information shown in the following figure is displayed, pip has been upgraded to the latest version.

Figure 15-14 Successful upgrade

```
Installing collected packages: pip
  Found existing installation: pip 8.1.1
    Uninstalling pip-8.1.1:
      Successfully uninstalled pip-8.1.1
Successfully installed pip-10.0.1
```

Install the Web.py framework.

To obtain the official Web.py installation tutorial, log in at **http://webpy.org/**. Run the following command to install Web.py:

```
pip3 install web.py==0.40.dev0
```

Figure 15-15 Installing Web.py

```
[root@ecs-test1-0001 home]# pip3 install web.py==0.40.dev0
Collecting web.py==0.40.dev0
  Downloading https://files.pythonhosted.org/packages/47/15/c011b80de6c2df69be46
    100% |                                | 122kB 216kB/s
Installing collected packages: web.py
  Running setup.py install for web.py ... done
Successfully installed web.py-0.40.dev0
```

Install WinSCP.

Code is generally edited on a local Windows OS and uploaded to the CentOS ECS. WinSCP is an SSH-based open source SFTP client for Windows and supports SCP.

Its main function is file transfer between a local and a remote computer. Additionally, WinSCP offers scripting and basic file manager functionality.

For more details about WinSCP, see **https://winscp.net/eng/docs/introduction**.

Uploading Code

1. Create the **main.py** file and copy the following data:

```
# -*- coding: utf-8 -*-
# filename: main.py
import web
from handle import Handle

urls = (
    '/wx', 'Handle',
)

if __name__ == '__main__':
    app = web.application(urls, globals())
    app.run()
```

2. Create the **handle.py** file and copy the following data:

```
# -*- coding: utf-8 -*-
# filename: handle.py

import hashlib
import web
import receive
import time
import os

class Handle(object):

    def __init__(self):
        self.app_root = os.path.dirname(__file__)
        self.templates_root = os.path.join(self.app_root, 'templates')
        self.render = web.template.render(self.templates_root)

    def GET(self):
        try:
            data = web.input()
            if len(data) == 0:
                return "hello, this is handle view"
            signature = data.signature
            timestamp = data.timestamp
            nonce = data.nonce
            echostr = data.echostr
            token = "Use the taken value obtained in the basic configuration of the official WeChat
account."

            list = [token, timestamp, nonce]
            list.sort()
            s = list[0] + list[1] + list[2]
            hashcode = hashlib.sha1(s.encode('utf-8')).hexdigest()
            print( "handle/GET func: hashcode, signature: ", hashcode, signature)
            if hashcode == signature:
                return echostr
            else:
                return echostr
        except (Exception) as Argument:
            return Argument

    def POST(self):
        try:
            webData = web.data()
            print("Handle Post webdata is:\n", webData)
            #Print message body logs.
            recMsg = receive.parse_xml(webData)
```



```
            if isinstance(recMsg, receive.Msg) and recMsg.MsgType == 'text':
                toUser = recMsg.FromUserName
                fromUser = recMsg.ToUserName
                content = "Welcome to Service Infographics." + str(recMsg.Content)
                print('Reply message info:\n')
                print('toUser =', toUser)
                print('fromUser = ', fromUser)
                print('content = ', content)
                return self.render.reply_text(toUser, fromUser, int(time.time()), content)
            else:
                print("Message types not supported:",recMsg.MsgType)
                return "success"
        except (Exception) as Argment:
            return Argment
```

3. Create the **receive.py** file and copy the following data:

```
# -*- coding: utf-8 -*-
# filename: receive.py
import xml.etree.ElementTree as ET

def parse_xml(web_data):
    if len(web_data) == 0:
        return None
    xmlData = ET.fromstring(web_data)
    msg_type = xmlData.find('MsgType').text
    if msg_type == 'text':
        return TextMsg(xmlData)
    elif msg_type == 'image':
        return ImageMsg(xmlData)
    elif msg_type == 'location':
        return LocationMsg(xmlData)
    elif msg_type == 'event':
        return EventMsg(xmlData)

class Event(object):
    def __init__(self, xmlData):
        self.ToUserName = xmlData.find('ToUserName').text
        self.FromUserName = xmlData.find('FromUserName').text
        self.CreateTime = xmlData.find('CreateTime').text
        self.MsgType = xmlData.find('MsgType').text
        self.Eventkey = xmlData.find('EventKey').text

class Msg(object):
    def __init__(self, xmlData):
        self.ToUserName = xmlData.find('ToUserName').text
        self.FromUserName = xmlData.find('FromUserName').text
        self.CreateTime = xmlData.find('CreateTime').text
        self.MsgType = xmlData.find('MsgType').text
        self.MsgId = xmlData.find('MsgId').text

class TextMsg(Msg):
    def __init__(self, xmlData):
        Msg.__init__(self, xmlData)
        self.Content = xmlData.find('Content').text

class ImageMsg(Msg):
    def __init__(self, xmlData):
        Msg.__init__(self, xmlData)
        self.PicUrl = xmlData.find('PicUrl').text
        self.MediaId = xmlData.find('MediaId').text

class LocationMsg(Msg):
    def __init__(self, xmlData):
        Msg.__init__(self, xmlData)
        self.Location_X = xmlData.find('Location_X').text
        self.Location_Y = xmlData.find('Location_Y').text

class EventMsg(Msg):
    def __init__(self, xmlData):
```



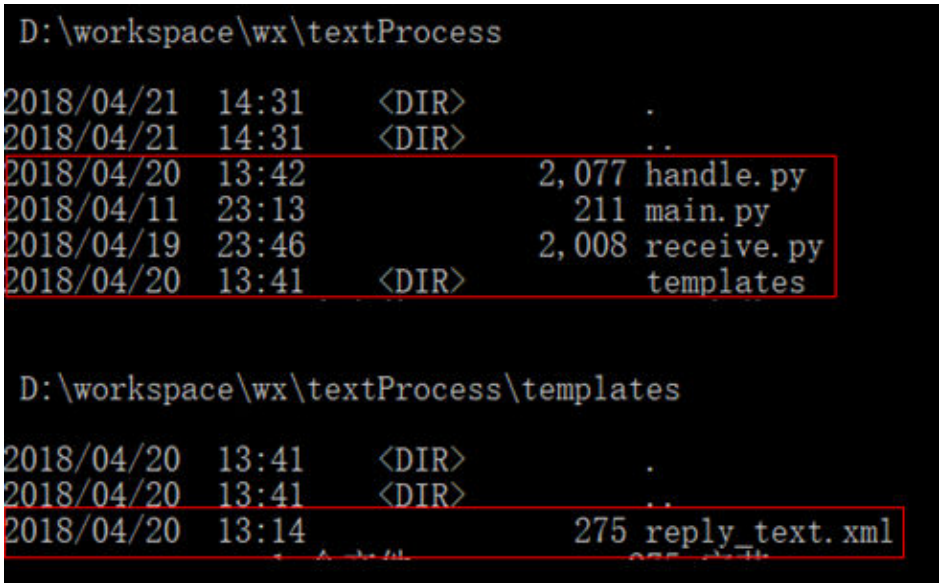
```
    Event.__init__(self, xmlData)
    self.Event = xmlData.find('Event').text
```

4. Create the **templates** folder and the **reply_text.xml** file in the folder. Then, copy the following data:

```
$def with (toUser,fromUser,createTime,content)
<xml>
<ToUserName><![CDATA[$toUser]]></ToUserName>
<FromUserName><![CDATA[$fromUser]]></FromUserName>
<CreateTime>$createTime</CreateTime>
<MsgType><![CDATA[text]]></MsgType>
<Content><![CDATA[$content]]></Content>
</xml>
```

5. Obtain the local file.

Figure 15-16 Local file



6. Use WinSCP to upload the preceding files and folder to the specified directory on the ECS.

Figure 15-17 Uploading files

Starting the Service

Run the following command to start the service:

```
python3 main.py 80
```

If the command output shown in **Figure 15-18** is displayed, the service has been started.

Figure 15-18 Successful service startup

Enabling the Developer Mode

1. Log in to official WeChat platform, choose **Develop** > **Basic Configuration**, and click **Modify Configuration**.
2. Specify the following basic configurations and click **Submit**.
   - **URL**: contains the EIP bound to the ECS, and port 80 is not required.
   - **Token**: the same as the token value in the **handle.py** file.
   - **EncodingAESKey**: generated randomly.
   - **Message encryption and decryption**: plaintext in this example.
3. Authenticate the token and click **Enable**.

   NOTE

   If authenticating the token failed, check whether the token configuration is the same as that in the code for processing GET messages in the **handle.py** file.

Verifying Service Deployment

Send a text message to the official WeChat account. If the response is properly received, the service has been successfully deployed.

16 Manually Deploying GitLab (CentOS 7.2)

Overview

The best practices for HUAWEI CLOUD ECS guide you through the manual deployment of GitLab on a Linux ECS. GitLab is an open-source version management system that uses Git as the code management tool. The CentOS 7.2 64bit OS is used as an example in this section.

Prerequisites

- The memory of the target ECS is greater than or equal to 4 GB.
- The rule listed in the following table has been added to the security group to which the target ECS belongs. For details, see **Adding a Security Group Rule**.

Table 16-1 Security group rule

Transfer Direction	Protocol/ Application	Port/Range	Source End
Inbound	HTTP (80)	80	0.0.0.0/0

Procedure

Step 1 Install the dependency package.

1. Log in to the ECS.
2. Run the following command to install the dependency package:

   sudo yum install -y curl policycoreutils-python openssh-server
3. Run the following commands to configure automatic SSH enabling upon ECS startup and start SSH:

   sudo systemctl enable sshd

   sudo systemctl start sshd

Step 2 Install Postfix to send emails.

1. Run the following command to install Postfix:

   sudo yum install postfix

2. Run the following commands to configure automatic Postfix enabling upon ECS startup and start Postfix:

   sudo systemctl enable postfix

   sudo systemctl start postfix

Step 3 Add the GitLab repository and install the software package.

1. Run the following command to add the GitLab repository:

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

2. Run the following command to install GitLab:

   sudo EXTERNAL_URL="http://*gitlab.example.com***" yum install -y gitlab-ee**

   Set **EXTERNAL_URL** to the IP address of the GitLab server, which can be the public IP address of the server or the domain name.

   NOTE

   – After the command is executed, you can view the software download speed and the estimated download completion time in the command output.

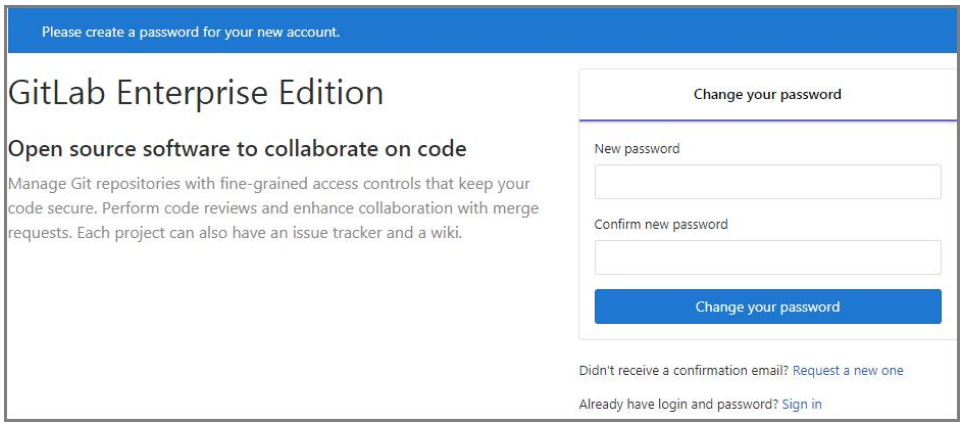
   – If the download speed is slow, obtain the response IP addresses of github.com at **http://tool.chinaz.com/dns** and select the IP address with a smaller TTL value. Then add the local DNS resolution to the **hosts** file on the target ECS.

   If information similar to the following is displayed, GitLab has been installed:

```
Running handlers:
Running handlers complete
Chef Client finished, 452/672 resources updated in 01 minutes 38 seconds
gitlab Reconfigured!

       *.                  *.
      ***                 ***
     *****               *****
    .******             *******
    ********            ********
   ,,,,,,,,,***********,,,,,,,,,
  ,,,,,,,,,,,*********,,,,,,,,,,,
  .,,,,,,,,,,,*******,,,,,,,,,,,,
      ,,,,,,,,,*****,,,,,,,,,.
         ,,,,,,,****,,,,,,
            .,,,***,,,,
                ,*,.



     _______ __  __          __
    / ____(_) /_/ /   ____ _/ /_
   / / __/ / __/ /   / __ `/ __ \
  / /_/ / / /_/ /___/ /_/ / /_/ /
  \____/_/\__/_____/\__,_/_.___/


Thank you for installing GitLab!
```

Step 4 Test the GitLab deployment.

1. Enter http://*Server IP address* in the address bar. If the following page is displayed, GitLab has been set up.



2. Change the password upon your first login. Then, enter the new password to log in.

----End

17 Manually Deploying RabbitMQ (CentOS 7.4)

Overview

The best practices for HUAWEI CLOUD ECS guide you through the manual deployment of RabbitMQ on a Linux ECS. RabbitMQ is a message middleware that uses the Erlang programming language for the Advanced Message Queuing Protocol (AMQP). It originates from the financial system and is used to store and forward messages in the distributed system. Featuring high reliability, scalability, availability, and rich functions, RabbitMQ is widely used.

Prerequisites

The rule listed in the following table has been added to the security group to which the target ECS belongs. For details, see **Adding a Security Group Rule**.

Table 17-1 Security group rule

Transfer Direction	Type	Protocol	Port/Range	Source
Inbound	IPv4	TCP	5672	0.0.0.0/0
Inbound	IPv4	TCP	15672	0.0.0.0/0

Procedure

Step 1 Install the dependency package and perl.

1. Log in to the target ECS.
2. Run the following command to install the dependency package:

   yum -y install make gcc gcc-c++ m4 ncurses-devel openssl-devel unixODBC-devel
3. Run the following command to install perl:

   yum install perl

Step 2 Install Erlang.

1. Run the following command to download the Erlang installation package:

   wget http://erlang.org/download/otp_src_19.3.tar.gz
2. Run the following command to decompress the package:

   tar xzf otp_src_19.3.tar.gz

   After the decompression, the folder **otp_src_19.3** is obtained.
3. Run the following command to create the **erlang** folder:

   mkdir /usr/local/erlang
4. Run the following command to switch to the **otp_src_19.3** folder:

   cd otp_src_19.3
5. Run the following command to check whether the system configuration meets installation requirements:

   ./configure --prefix=/usr/local/erlang --without-javac
6. Run the following command to compile and install Erlang:

   make && make install
7. Configure Erlang environment variables.
   a. Run the following command to open the **profile** configuration file:

      vi /etc/profile
   b. Press **i** to enter editing mode.
   c. Add the following content to the end of the **profile** file:

      ```
      export PATH=$PATH:/usr/local/erlang/bin
      ```
   d. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the configuration file.
   e. Run the following command for the environment variables to take effect:

      source /etc/profile
8. Run the following command to check the installation result:

   erl -version

   If information similar to the following is displayed, Erlang has been installed:

   ```
   [root@ecs-rabbitmq ~]# erl -version
   Erlang (ASYNC_THREADS,HIPE) (BEAM) emulator version 8.3
   ```

Step 3 Install RabbitMQ.

1. Run the following command to switch to the home directory:

   cd
2. Run the following commands to download the RabbitMQ installation package:

   wget https://www.rabbitmq.com/releases/rabbitmq-server/v3.6.9/rabbitmq-server-generic-unix-3.6.9.tar.xz
3. Run the following command to decompress the package:

   tar xvJf rabbitmq-server-generic-unix-3.6.9.tar.xz
4. Run the following command to move the decompressed directory to **/usr/local/rabbitmq**:

   mv rabbitmq_server-3.6.9 /usr/local/rabbitmq

5. Configure RabbitMQ environment variables.
   a. Run the following command to open the **profile** configuration file:

      vi /etc/profile
   b. Press **i** to enter editing mode.
   c. Add the following content to the end of the **profile** file:

      ```
      export PATH=$PATH:/usr/local/rabbitmq/sbin
      ```
   d. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the configuration file.
   e. Run the following command for the environment variables to take effect:

      source /etc/profile

Step 4 Run the following command to enable the RabbitMQ management web page:

rabbitmq-plugins enable rabbitmq_management

Information similar to the following is displayed:

```
[root@ecs-rabbitmq ~]# rabbitmq-plugins enable rabbitmq_management
The following plugins have been enabled:
  amqp_client
  cowlib
  cowboy
  rabbitmq_web_dispatch
  rabbitmq_management_agent
  rabbitmq_management

Applying plugin configuration to rabbit@ecs-rabbitmq... started 6 plugins.
```

Step 5 Run the following command to create a user:

rabbitmqctl add_user *Username password*

For example, run the following command:

rabbitmqctl add_user root 123456

Step 6 Run the following command to set the user as the administrator:

rabbitmqctl set_user_tags *Username* **administrator**

For example, run the following command:

rabbitmqctl set_user_tags root administrator

Step 7 Run the following command to assign all permissions to the user:

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

For example, run the following command:

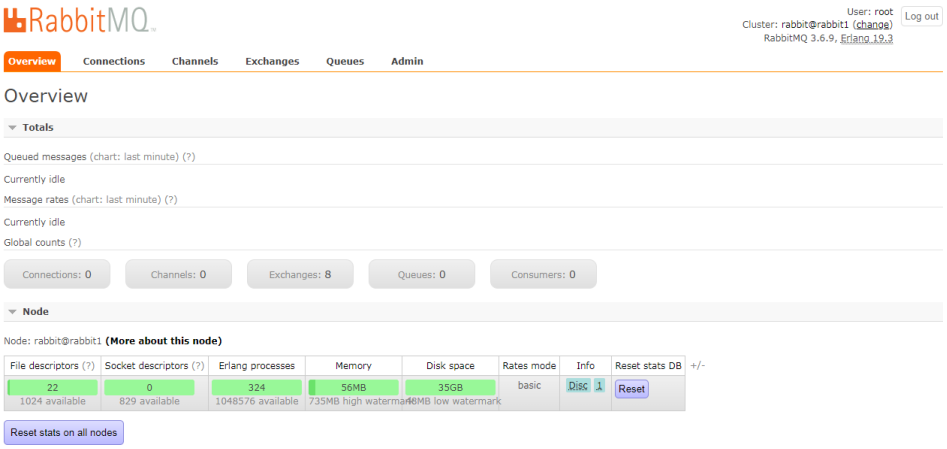
rabbitmqctl set_permissions -p / root '.*' '.*' '.*'

Step 8 Run the following command to start RabbitMQ on the backend:

rabbitmq-server -detached

Step 9 Enter http://*EIP:15672* in the address bar to visit RabbitMQ. If the following page is displayed, RabbitMQ has been installed.

Step 10 Enter the username and password of the account created in **Step 5** to switch to the RabbitMQ management page.



----End

18 Manually Building a Ghost Blog

Ghost is an open source blog platform based on Node.js and makes writing and release more convenient. This section walks you through the deployment of a Ghost blog on an ECS running Ubuntu 16.04.

Installing GCC and g++

1. Run the following command to install the common development and compilation tool package:

   sudo apt-get install build-essential

2. Run the following command to install the GNU Compiler Collection (GCC):

   apt-get install gcc

3. Run the following command to query the GCC version:

   gcc --version

   The following information is displayed:

   ```
   root@ecs-c47c:~# gcc --version
   gcc (Ubuntu 5.4.0-6ubuntu1~16.04.10) 5.4.0 20160609
   Copyright (C) 2015 Free Software Foundation, Inc.
   ```

4. Run the following command to install g++:

   sudo apt-get install g++

5. Run the following command to query the g++ version:

   g++ --version

   The following information is displayed:

   ```
   root@ecs-c47c:~# g++ --version
   g++ (Ubuntu 5.4.0-6ubuntu1~16.04.10) 5.4.0 20160609
   Copyright (C) 2015 Free Software Foundation, Inc.
   ```

Installing Node.js

1. Run the following commands to install Node.js:

   sudo curl -sL https://deb.nodesource.com/setup_10.x | sudo -E bash -

   sudo apt-get install -y nodejs

2. Run the following commands to query the version of Node.js and Node Package Manager (npm), respectively:

   node -v

npm -v

The following information is displayed:

```
root@ecs-c47c:~# node -v
v9.11.2
root@ecs-c47c:~# npm -v
5.6.0
```

Installing Nginx

Before deploying the Ghost blog, you need to install Nginx on the ECS so that the ECS can work as an HTTP server. The following operations use Nginx 1.10.0 as an example.

1. Run the following commands to install Nginx:

   sudo apt-get update

   sudo apt-get install nginx

2. (Optional) Configure the firewall.

   Uncomplicated Firewall (UFW) is an iptables interface that simplifies the firewall configuration. By default, UFW is installed in Ubuntu. Run the following command to check the firewall status:

   sudo ufw status

   If you do not want to enable the firewall, skip this step. If you want to enable the firewall, run the following command:

   sudo ufw enable

   Verify that the firewall is enabled.

   Before testing Nginx, you need to reconfigure the firewall to allow access to Nginx. Run the following command to automatically register Nginx with UFW:

   sudo ufw app list

   The following information is displayed:

   ```
   Available applications:
     Nginx Full
     Nginx HTTP
     Nginx HTTPS
     ...
   ```

   - **Nginx Full**: Port 80 is enabled to distribute normal and unencrypted web traffic, and port 443 to handle encrypted TLS/SSL traffic.
   - **Nginx HTTP**: Only port 80 is enabled to distribute normal and unencrypted web traffic.
   - **Nginx HTTPS**: Only port 443 is enabled to distribute encrypted TLS/SSL traffic.

   Run the following command to ensure that the firewall allows HTTP and HTTPS connections:

   sudo ufw allow 'Nginx Full'

3. Verify that Nginx can work properly.

   Use the domain name or IP address to access Nginx. The **Welcome to nginx** page is displayed if Nginx is started normally.

   Enter **http://***Nginx IP address* in a browser address bar to visit Nginx. If the following page is displayed, Nginx has been installed.

4. Configure Nginx.
   a. Create a configuration file.

      vim /etc/nginx/sites-available/ghost.conf

   b. Add the following content to the configuration file:

```
server {
    listen 80;
    server_name 119.3.xx.xxx.com; #Domain name or IP address
    location / {
        proxy_set_header   X-Real-IP $remote_addr;
        proxy_set_header   Host      $http_host;
        proxy_pass         http://127.0.0.1:2368;
    }
}
```

      The reverse proxy has been written. You only need to set the value of **server_name** to your own top-level domain name.

   c. Run the following command to create a soft link between the configuration file to the **sites-enabled** directory:

      sudo ln -s /etc/nginx/sites-available/ghost.conf /etc/nginx/sites-enabled/ghost.conf

   d. Restart Nginx.

      sudo service nginx restart

Creating a User

Performing operations as user **root** is not recommended by Ghost. Therefore, you need to create a new user and grant permissions to it.

1. Run the following commands to create a user:

   adduser <user>

   The following information is displayed:

```
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

2. Run the following command to add the newly created user to the user group:

   usermod -aG sudo <user>

   The following information is displayed:

```
Changing the user information for sxm
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
```



```
Other []:
Is the information correct? [Y/n]
```

3. Run the following command to switch to the created user:

   su - <user>

Installing MySQL

MySQL is an open-source database management system, which is usually installed as a part of the popular LAMP (Linux, Apache, MySQL, and PHP/Python/Perl) stack. MySQL uses relational databases and the structured query language (SQL) to manage data.

1. Install MySQL.
   - Run the following command to update the software package:

     sudo apt-get update
   - Run the following command to install the **mysql-server** software package (during the installation, you will be asked to set the password of user **root**):

     sudo apt-get install mysql-server
2. Configure MySQL.

   Run the following command and perform operations as prompted to harden MySQL:

   mysql_secure_installation

```
Securing the MySQL server deployment.

Enter password for user root:    #Enter the obtained password of user root.
The existing password for the user account root has expired. Please set a new password.

New password:  #Enter the new password.

Re-enter new password:   #Enter the new password again.
The 'validate_password' plugin is installed on the server.
The subsequent steps will run with the existing configuration of the plugin.
Using existing password for root.

Estimated strength of the password: 100
Change the password for root ? ((Press y|Y for Yes, any other key for No) : N   #Asks you whether to change the password of user root. Press n.

 ... skipping.
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y   #Asks you whether to remove anonymous users. Press 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   #Asks you whether to forbid remote login of user root. Press y.
Success.

By default, MySQL comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment.
```



```
Remove test database and access to it? (Press y|Y for Yes, any other key for No) : Y   #Asks you whether to delete the test database and cancel access permissions to it. Press y.
 - Dropping test database...
Success.

 - Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : Y   #Asks you whether to reload privilege tables. Press y.
Success.

All done!
```

3. Test MySQL.

   Run the following command to check the MySQL status:

   systemctl status mysql.service

   If MySQL is in normal status, the following information is displayed:

   ```
   ● mysql.service - MySQL Community Server
     Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2019-01-07 10:57:27 CST; 2min 42s ago
   Main PID: 26065 (mysqld)
     CGroup: /system.slice/mysql.service
             └─26065 /usr/sbin/mysqld
   ```

4. To avoid garbled characters in the database, run the following command to set the MySQL code:

   sudo vi /etc/my.cnf

   Copy and paste the following content:

   ```
   [client]
   default-character-set=utf8
   [mysql]
   default-character-set=utf8
   [mysqld]
   character-set-server=utf8
   collation-server=utf8_general_ci
   ```

   Save the modification and exit. Then, run the following command to restart MySQL:

   sudo /usr/sbin/service mysql restart

5. Create a Ghost database.

   Log in to MySQL as user **root**, create a database named **ghost**, and verify that the database is successfully created.

   mysql -u root -p;

   mysql> create database ghost;

   mysql> show databases;

   mysql> exit

Installing and Configuring Ghost

Ghost-CLI has been added to Ghost v1.0.0 and later versions. You can directly install and configure Ghost-CLI.

1. Run the following command to install Ghost-CLI:

sudo npm i -g ghost-cli

2. Create a folder named **ghost** under **/var/www/**.

   sudo mkdir -p /var/www/ghost

   NOTICE

   If **ghost** is created under **/root**, Ghost cannot work properly.

3. Run the following command to grant the user permissions on **ghost**:

   sudo chown [user]:[user] /var/www/ghost

   NOTE

   [user] is the newly created user.

4. Run the following command to switch to the created folder:

   cd /var/www/ghost/

5. Run the following command to install Ghost using Ghost-CLI: **ghost install**

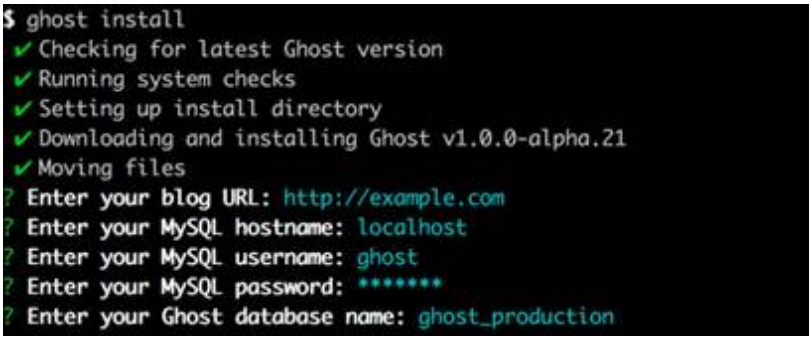
   NOTE

   If a message is displayed indicating that the node version does not match, obtain the required version on the official website of Node.js and reinstall Ghost.

   https://nodejs.org/en/download/

6. Configure Ghost.

   If **ghost install** is successfully executed in the **/var/www/ghost/** directory, you need to configure some items.

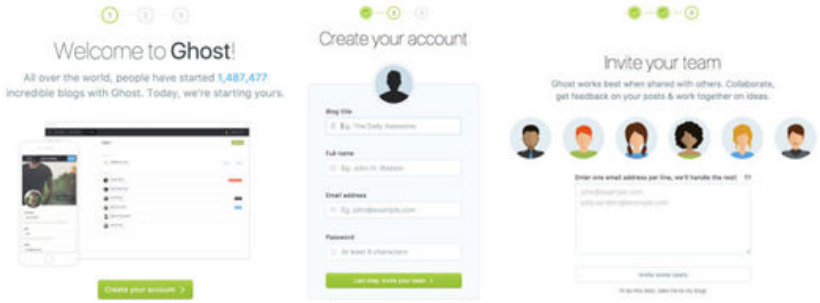
   Configuration the items as required. If you need to modify the configuration later, run the following command to modify the configuration file:

   vi config.production.json

   After the modification, the configuration is the same as that in the production environment. The following figure is for reference only.

Verifying Blog Access

If Ghost is successfully installed, you can access the Ghost blog using the domain name.



19 Manually Deploying Node.js (CentOS 7.2)

Overview

The best practices for HUAWEI CLOUD ECS guide you through the manual deployment of Node.js on a Linux ECS.

Node.js is a JavaScript running environment based on the Google Chrome V8 engine. It enables simple deployment of network applications that feature fast response and easy-to-expand. Based on the event-driven and non-blocking I/O model, Node.js is lightweight and efficient. It is ideal for running data-intensive real-time applications on distributed devices.

For more information about Node.js, see **https://nodejs.org**.

This section uses CentOS 7.2 64bit (40 GB) and Node.js installation packages **node-v10.14.1-linux-x64.tar** and **node-v10.14.2-linux-x64.tar** as an example to describe how to deploy Node.js.

Prerequisites

- A Linux ECS is available. For details, see **Purchasing an ECS**.
- The target ECS has an EIP bound. For instructions about how to bind an EIP to an ECS, see **Assigning an EIP and Binding It to an ECS**.
- A tool (for example, **PuTTY**) for accessing the Linux ECS has been installed on the local computer.

Procedure

Step 1 Install the Node.js software packages.

- Using the binary file
  a. Log in to the ECS.
  b. Run the following command to download a Node.js installation package:
     wget https://nodejs.org/dist/v10.14.1/node-v10.14.1-linux-x64.tar.xz
  c. Run the following command to decompress the file:
     tar xvJf node-v10.14.1-linux-x64.tar.xz

d. Run the following commands in any directory to set up a soft connection for node and NPM, respectively:

ln -s /root/node-v10.14.1-linux-x64/bin/node /usr/local/bin/node

ln -s /root/node-v10.14.1-linux-x64/bin/npm /usr/local/bin/npm

e. Run the following commands to check the node and NPM versions:

node -v

npm -v

- Using the NVM version manager

a. Log in to the ECS.

b. Run the following command to install git:

yum install git

c. Run the following command to copy the source code to the local **~/.nvm** directory using git and check the version:

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

d. Run the following command to activate NVM and add it to the **profile** file:

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

e. Run the following command for the environment variables to take effect:

source /etc/profile

f. Run the following command to list available Node.js versions:

nvm ls-remote

g. Run the following command to install multiple Node.js versions:

nvm install v10.14.1

nvm install v10.14.2

h. Run the following command to view the installed versions:

nvm ls

i. Run the following command to switch the Node.js version to V10.14.2:

nvm use v10.14.2

NOTE

- Run the **nvm alias default v10.14.2** command to set the default version to **10.14.2**.
- Run the **nvm help** command to obtain more information about NVM.

Step 2 Verify the deployment.

1. Run the following command to switch to the home directory:

cd

2. Run the following command to create a **test.js** project file:

touch test.js

3. Use VIM to edit the **test.js** file.

a. Run the following command to install the VIM editor:

yum install vim

b. Run the following command to open the **test.js** file:

vim test.js

c. Press **i** to enter editing mode.

Modify the file as follows:

```
const http = require('http');
const hostname = '0.0.0.0';
const port = 3000;
const server = http.createServer((req, res) => {
   res.statusCode = 200;
   res.setHeader('Content-Type', 'text/plain');
   res.end('Hello World\n');
});
server.listen(port, hostname, () => {
   console.log(`Server running at http://${hostname}:${port}/`);
});
```

The port number can be customized.

d. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the file.

4. Run the following command to view enabled port:

netstat -lntp

If the port is unavailable, log in to the ECS console and change the security group rule. For details, see **Adding a Security Group Rule**.

5. Add exception ports in the firewall configuration.

a. For example, to add port 3000, run the following command:

firewall-cmd --zone=public --add-port=3000/tcp --permanent

If the following information is displayed, the firewall is disabled. Then, go to step **Step 2.6**.

```
[root@ecs-centos7 ~]# firewall-cmd --zone=public --add-port=3000/tcp --permanent
FirewallD is not running
```

If the following information is displayed, the firewall is enabled, and the exception port has been added:

```
[root@ecs-centos7 ~]# firewall-cmd --zone=public --add-port=3000/tcp --permanent
success
```

b. Reload the policy configuration for the new configuration to take effect.

firewall-cmd --reload

c. Run the following command to view all enabled ports:

firewall-cmd --list-ports

```
[root@ecs-centos7 ~]# firewall-cmd --list-ports
300/tcp
```

6. Run the following command to run the project:

node ~/test.js

7. Enter http://*EIP:3000* in the address bar to visit Node.js. If the following page is displayed, Node.js has been deployed.

Figure 19-1 Deployment and testing

----End

20 Setting Up Master-Slave Replication on PostgreSQL

What Is PostgreSQL?

PostgreSQL is an open source object relational DBMS (ORDBMS) with an emphasis on extensibility and standards compliance. It applies to business-oriented online transaction processing (OLTP) scenarios as well as supports NoSQL (JSON, XML, or hstore) and geographic information system (GIS) data types. It has won a good reputation in reliability and data integrity, and applies widely to Internet websites, location-based applications, and complex data object processing.

This section helps you use HUAWEI CLOUD ECSs to set up PostgreSQL.

Preparations

- Create two ECSs.
- Configure a security group rule for the ECSs to allow port 5432.

  NOTE

  The ECS in this section uses CentOS 7.6 64bit as OS.

  The version of the PostgreSQL in this section is PostgreSQL 11.2.

Configuring the Master Node

1. Run the following commands in sequence to install PostgreSQL on the master node:

   # yum update -y

   # yum install https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm

   # yum install postgresql11-server

   # yum install postgresql11

   # /usr/pgsql-11/bin/postgresql-11-setup initdb

   # systemctl enable postgresql-11

   # systemctl start postgresql-11

2. Run the following command to switch to the default user **postgres**:

   # su - postgres

3. Run the following command to enter the database:

   # psql

4. Run the following command to create an account and assign permissions to it:

   create role *Username* **login replication encrypted password** '*Password*'

   NOTE

   The password in the preceding command must be enclosed in single quotation marks.

   Assume the username is **dbar** and the password is **dbar_password**, run the following command:

   create role dbar login replication encrypted password 'dbar_password'

5. Run the following command to open configuration file **/var/lib/pgsql/11/data/pg_hba.conf**:

   # vim /var/lib/pgsql/11/data/pg_hba.conf

   Add the following content to the file:

   ```
   host all all 192.168.1.0/24 md5 #Allows MD5 password authentication in the VPC network segment.
   host replication dbar IP address of the slave database/24 md5 #Enables data from the master database to be replicated to the slave database.
   ```

6. Run the following command to open file **/var/lib/pgsql/11/data/postgresql.conf**:

   # vim postgresql.conf

   Add the following content to the file:

   ```
   wal_level = hot_standby
   max_wal_senders= 6
   wal_sender_timeout = 60s
   max_connections = 512 #The max_connections value of the slave database must be greater than that of the master database.
   archive_command= 'cp %p /var/lib/pgsql/11/data/archivelog/%f'
   wal_keep_segments=10240
   archive_mode = on
   listen_addresses= xxx.xx.xx.xx #Listens to the actual local IP address.
   ```

7. Run the following command to restart PostgreSQL:

   # systemctl restart postgresql-11

Configuring the Slave Node

1. Run the following commands in sequence to install PostgreSQL on the slave node:

   # yum update -y

   # yum install https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm

   # yum install postgresql11-server

   # yum install postgresql11

2. Run the following commands to copy the configuration file from the master node:

   # pg_basebackup -h *IP address of the master node* **-U *dbar* -D /var/lib/pgsql/11/data -X stream -P**

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

```
[root@ecs-22f5-0002 ~]# pg_basebackup -D /var/lib/pgsql/11/data -h [redacted] -p 5432 -U test  -X s
tream -P
Password:
24508/24508 kB (100%), 1/1 tablespace
[root@ecs-22f5-0002 ~]#
```

3. Run the following command to modify the **recovery.conf** file:

   # vim recovery.conf

   ```
   standby_mode = on  # This node is used as the slave database.
   primary_conninfo = 'host=IP address of the master node port=5432 user=dbar
   password=dbar_password    #Do not enclose the password in single quotation marks.
   trigger_file = '/var/lib/pgsql/11/data/trigger.kenyon'    #Trigger file for master/slave switchover
   recovery_target_timeline = 'latest'
   restore_command = 'cp /var/lib/pgsql/11/data/archivelog/%f %p'
   archive_cleanup_command = 'pg_archivecleanup /var/lib/pgsql/11/data/archivelog %r' #Clear
   outdated archives.
   ```

4. Run the following command to modify the **postgresql.conf** file:

   # chown -R postgres.postgres /var/lib/pgsql/11/data

5. Add the following content to the **/var/lib/pgsql/11/data/postgresql.conf** file.

   listen_addresses= *xxx.xx.xx.xx*

   max_connections = 600

6. Run the following commands to start PostgreSQL and enable PostgreSQL to automatically start upon ECS startup:

   #systemctl enable postgresql-11

   #systemctl start postgresql-11

Verifying Master-Slave Replication

1. Run the following command to check whether process **sender** runs on the master node:

   # ps aux |grep sender

   ```
   [root@ecs-22f5-0001 ~]# ps aux |grep sender
   postgres 14406  0.0  0.3 397240  3620 ?        Ss   20:19   0:00 postgres: walsender test [redacted] (53052) streaming 0/3000140
   ```

2. Run the following command to check whether process **receiver** runs on the slave node:

   # ps aux | grep receiver

   ```
   [root@ecs-22f5-0002 ~]# ps aux |grep receiver
   postgres  4390  0.0  0.3 403500  3632 ?        Ss   20:19   0:00 postgres: walreceiver   streaming 0/3000140
   ```

3. Run the following commands to check whether the status of the slave database can be viewed from the master database:

   # su - postgres

   -bash-4.2# psql

   replication=# select * from pg_stat_replication;

   ```
   postgres=#  select * from pg_stat_replication;
     pid  | usesysid | usename | application_name | client_addr  | client_hostname | client_port |         backend_start         | backend_xmin |   state   | se
   nt_lsn   | write_lsn | flush_lsn | replay_lsn | write_lag | flush_lag | replay_lag | sync_priority | sync_state
   -------+----------+---------+------------------+--------------+-----------------+-------------+-------------------------------+--------------+-----------+---
   -----------+-----------+-----------+------------+-----------+-----------+------------+---------------+------------
    14406 |    16384 | test    | walreceiver      | [redacted] |                 |       53052 | 2019-03-26 20:19:18.693053+08 |              | streaming | 0/
   3000140 | 0/3000140 | 0/3000140 | 0/3000140  |           |           |            |             0 | async
   (1 row)
   ```

4. Create a database from the master database and check whether the newly created database is synchronized to the slave database.

a. Run the following commands to create a database from the master database:

   postgres=# create database testdb;

   postgres=# \l

b. Run the following command to check whether the newly created database is synchronized to the slave database.

   postgres=# \l

21 Manually Installing a BT Panel (CentOS 7.2)

Overview

The best practices for HUAWEI CLOUD ECS guide you through the manual installation of a BT panel on Linux ECSs. BT panel is easy-to-use, powerful, and free-of-charge server management software that supports Linux and Windows. It allows you to configure LAMP, LNMP, websites, databases, FTP, and SSL with few clicks and easily manage ECSs through a web client. This section uses CentOS 7.2 64bit as an example to describe how to install BT panel 6.9.

To manually install a BT panel on the Linux ECS, perform the following steps:

1. **Install the BT panel.**
2. **Log in to the BT panel.**

Prerequisites

- ECS OS and specifications:
  - A minimum of 512 MB memory is required, but 768 MB or above is recommended. A BT panel occupies about 60 MB of the total.
  - A minimum of 100 MB disk space is required. A BT panel occupies about 20 MB of the total.
  - BT panel Linux 6.0 was developed based on CentOS 7, so CentOS 7.x is strongly recommended.
  - The OS has no Apache, Nginx, PHP, or MySQL installed.
- The rule listed in the following table has been added to the security group to which the target ECS belongs. For details, see **Adding a Security Group Rule**.

Table 21-1 Security group rule

Direction	Protocol/ Application	Port/Range	Source
Inbound	TCP	8888	0.0.0.0/0

Procedure

Step 1 Install the BT panel.

1. Log in to the target ECS.
2. Run the following command to download and install the BT panel:

   yum install -y wget && wget -O install.sh http://download.bt.cn/install/install_6.0.sh && sh install.sh

   When information similar to the following is displayed, enter **y**:

   ```
   ...
   Do you want to install Bt-Panel to the /www directory now?(y/n): y
   ...
   ```

   After the installation is displayed, information similar to the following is displayed:

   ```
   ...
   ==================================================================
   Congratulations! Installed successfully!
   ==================================================================
   Bt-Panel: http://114.115.xxx.xx:8888/46722528
   username: ut22gsvp
   password: ********
   Warning:
   If you cannot access the panel,
   release the following port (8888|888|80|443|20|21) in the security group
   ==================================================================
   Time consumed: 2 Minute!
   ```

   NOTE

   Record the values of **Bt-Panel**, **username**, and **password** in the command output.

Step 2 Log in to the BT panel.

1. In the address bar of your browser, enter the address following parameter **Bt-Panel**, for example, **http://114.115.xxx.xx:8888/46722528**.
2. Enter the username and password you recorded.
3. Install desired suites and deploy websites using the BT panel based on service requirements.

----End

22 Accessing OBS over Intranet

22.1 Overview

Scenario Introduction

An enterprise runs basic services on Elastic Cloud Servers (ECSs), but storage capacity of hard disks becomes insufficient for storing a large number of images and videos. After learning that HUAWEI CLOUD provides OBS, an elastic cloud storage service for massive amounts of data, the enterprise determined to use OBS as the data storage resource pool to reduce the burden on local servers.

From ECSs, you can access OBS over the internet or HUAWEI CLOUD intranet. However, for access over the internet, the network response speed is subject to the network conditions, and you need to pay for data access over the internet. To maximize performance and reduce costs, enterprise administrators want to access OBS over the intranet.

NOTE

When accessing OBS over the intranet, ensure that the OBS resources to be accessed are in the region where the ECS resides. If the OBS resources reside in a different region, access is supported only over the Internet.

Solution

Configure intranet DNS on the established ECS. The intranet DNS resolves the OBS domain name so that the ECS can access OBS through the intranet. **Figure 22-1** shows the access process.

Figure 22-1 Accessing OBS through the intranet

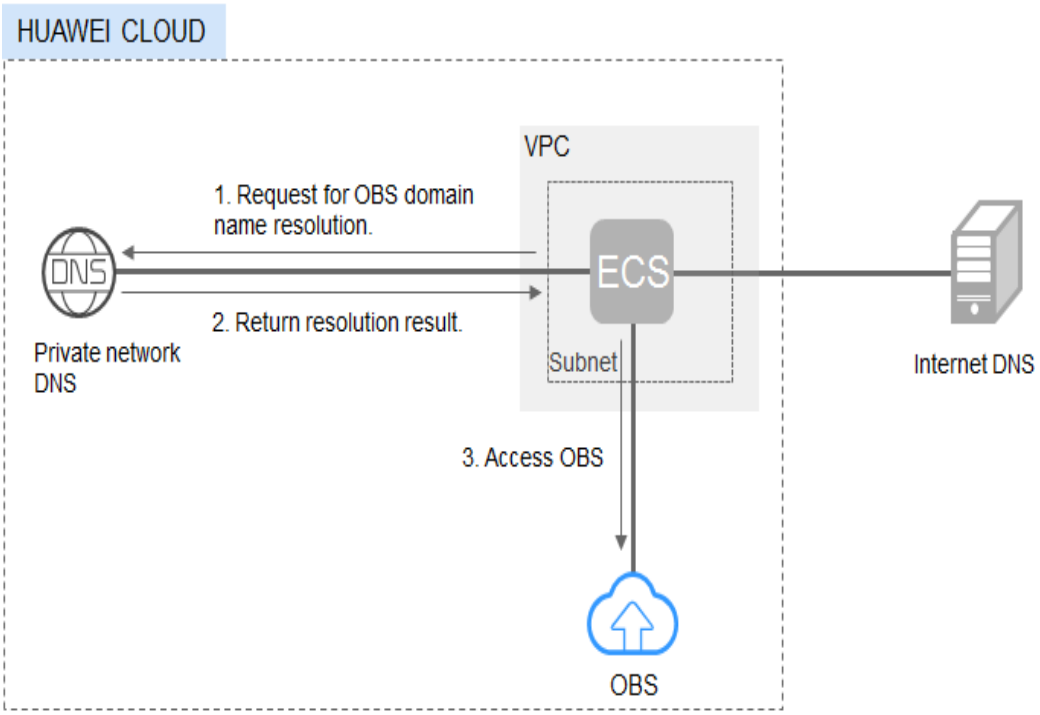


Table 22-1 describes the services in the figure.

Table 22-1 Service description

Service	Description
Virtual Private Cloud (VPC)	VPC enables users to create an isolated virtual network environment defined and managed by themselves, improving security of resources in the cloud and simplifying network deployment. A subnet is a network that provides IP address management and DNS services for the ECS in a VPC. IP addresses of an ECS must be in the same subnet of the ECS.
Domain Name Service (DNS)	Intranet DNS is provided for resolving intranet domain names and OBS domain names. This simplifies the domain name resolution process and reduces costs on data transfer over the internet.

- For Windows ECSs, you are advised to use OBS Browser+ to access OBS over intranet. For details, see:

  Accessing OBS over Intranet by Using OBS Browser+ on a Windows ECS
- For Linux ECSs, you are advised to use obsutil to access OBS over intranet. For details, see:

  Accessing OBS over Intranet by Using obsutil on a Linux ECS

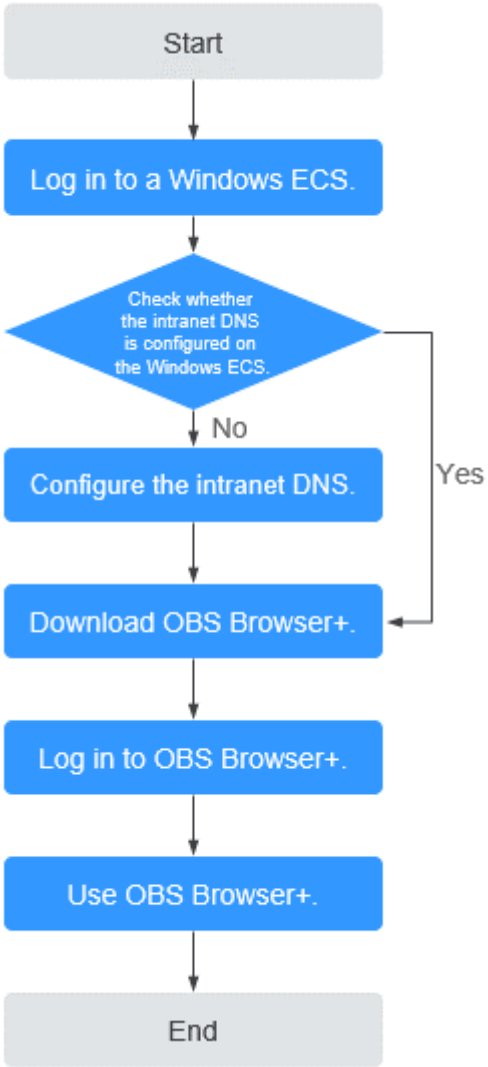
When accessing OBS through the intranet from your ECSs, you can read, back up, and archive data without affecting the internet bandwidth.

22.2 Accessing OBS over Intranet by Using OBS Browser + on a Windows ECS

OBS Browser+ is a graphical interface tool applicable to object-based storage services. You can configure the intranet DNS server address to access OBS over intranet on a HUAWEI CLOUD Windows ECS. The process and procedure are described as follows.

Process

Figure 22-2 The process of accessing OBS over intranet by using OBS Browser+ on a Windows ECS



Procedure

Step 1 Log In to the Windows ECS.

1. Log in to **HUAWEI CLOUD** and click **Console**.
2. On the home page of the console, choose **Computing** > **Elastic Cloud Server**.
3. Select an ECS and log in to it.

   A Windows ECS can be logged in using either VNC or MSTSC. For details, see **Logging In to an ECS**.

Step 2 Check whether the intranet DNS is configured on the Windows ECS.

On the Windows ECS, you can view the current DNS configuration by using the graphical user interface (GUI) or command line interface (CLI). This section uses the CLI as an example to describe how to view the DNS configuration.

1. After logging in to the ECS, open the CLI.
2. Run the **ipconfig /all** command to check whether DNS server is at the intranet DNS address of the region where the current ECS resides.

   NOTE

   HUAWEI CLOUD provides different private DNS server addresses for different regions. For details, see **What Are the Private DNS Server Addresses Provided by the DNS Service?**

   - If no, go to **Step 3**.
   - If yes, go to **Step 4**.

Step 3 Configure the Intranet DNS.

Change the DNS server address of the ECS to the intranet DNS provided by HUAWEI CLOUD. You can change the DNS address of the VPC subnet or modify the local DNS configuration to achieve this.

- **Methods 1: Changing the DNS server address of the VPC subnet**

  Locate the VPC where the ECS resides and change the DNS server address of the VPC subnet the intranet DNS address. In this manner, ECSs in the VPC can use the intranet DNS for resolution and thereby you can access OBS on HUAWEI CLOUD intranet. For details, see **Modifying a Subnet**.

  NOTE

  The intranet DNS server address must be selected based on the region where the ECS resides. For details, see **What Are the Private DNS Server Addresses Provided by the DNS Service?**

- **Method 2: Modifying the local DNS configuration**

  The intranet DNS configured in this method becomes invalid once the ECS is restarted. Therefore, you need to reconfigure the intranet DNS after each restart of the ECS. This section uses configuration through CLI as an example to describe how to modify the DNS configuration locally.

1. Open the CLI.
2. Run the following command to configure the IP address of the primary DNS server:

   netsh interface ip set dns name="*Local connection*" **source**=**static addr**= *Intranet DNS server address* **register**=**primary**

NOTE

- **Local connection**: NIC name. You need to modify the name according to the actual NIC.
- **Intranet DNS server address**: Select the intranet DNS server address based on the region where the ECS resides. For details, see **What Are the Private DNS Server Addresses Provided by the DNS Service?**

3. (Optional) Run the following command to configure the IP address of the backup DNS server:
netsh interface ip add dns name="*Local connection*" **addr**= *Alternative DNS server address* **index**=2

NOTE

- **Local connection**: NIC name. Use the actual NIC name when configuring the local DNS.
- **Alternative DNS server address**: The DNS server is used when the primary DNS server is faulty, unavailable, or cannot resolve the requested domain name. Therefore, you can set this parameter to the IP address of the HUAWEI CLOUD intranet DNS server. (You need to select the intranet DNS server address based on the region where the ECS resides. For details, see **What Are the Private DNS Server Addresses Provided by the DNS Service?**) You can also set this parameter to the IP address of a public DNS server.

Step 4 Download OBS Browser+.

For details, see **Downloading OBS Browser+**.

Step 5 Log in to OBS Browser+.

OBS Browser+ uses the public network to access OBS by default. Therefore, when you log in to OBS Browser+ to add an account, set **Service** and **Server Address** as follows:

- **Service**: Select **Other object storage services**.
- **Server Address**: Enter the OBS domain name in the region where your ECS resides and the port number. The HTTPS port number is **443** and the HTTP port number is **80**. The HTTPS server is used by default. If you want to use the HTTP server, click  in the upper right corner of OBS Browser+ and click **System Configuration**. In the **System Configuration** dialog box that is displayed, deselect **Enable HTTPS**.

  Example: obs.cn-south-1.myhuaweicloud.com:443

  Example: obs.ap-southeast-1.myhuaweicloud.com:443

  NOTE

  For details about OBS regions and endpoints, see **Regions and Endpoints**.

Step 6 Start to use OBS Browser+.

After logging in to OBS Browser+, you can access OBS over HUAWEI CLOUD intranet on the Windows ECS to perform basic data access operations and other advanced settings.

For details, see the following topics:

- **Uploading a File or Folder**
- **Downloading a File or Folder**

For details, see **OBS Browser+ Tools Guide**.

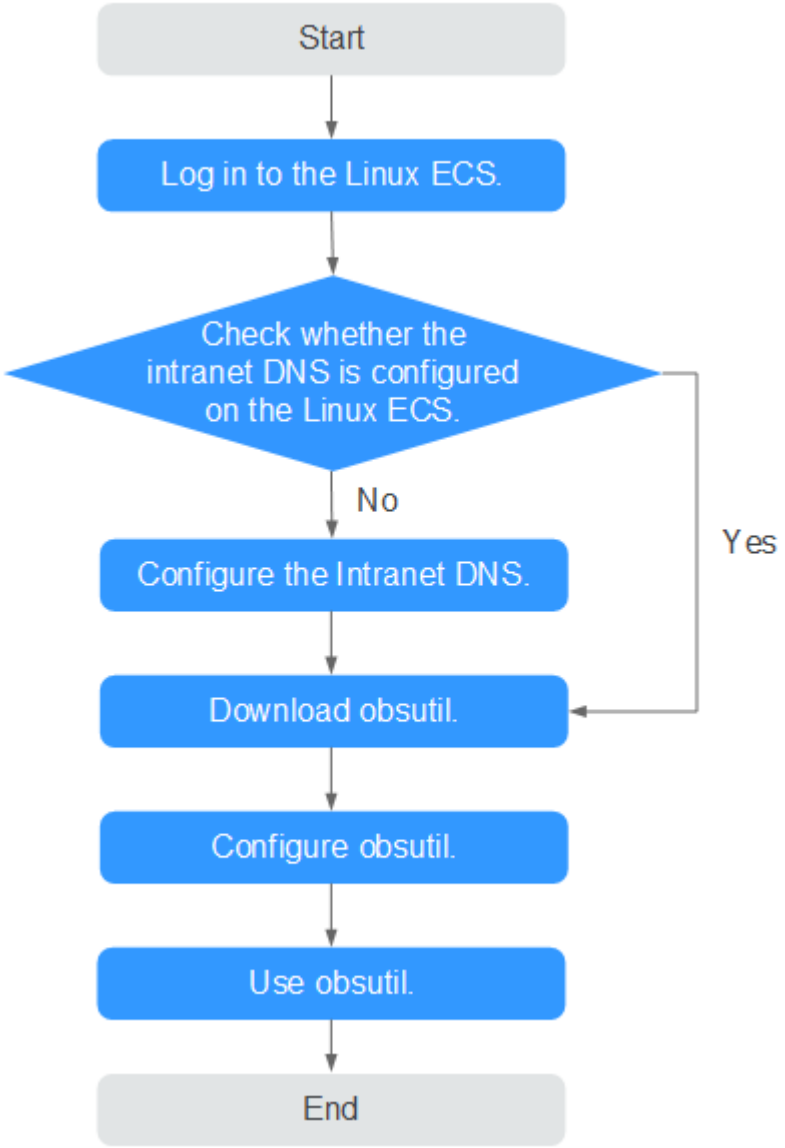
----End

22.3 Accessing OBS over Intranet by Using obsutil on a Linux ECS

obsutil is a command line tool applicable to Windows and Mac operating systems. You can configure the intranet DNS server address to access OBS over intranet on a HUAWEI CLOUD Linux ECS. The process and procedure are described as follows.

Process

Figure 22-3 The process of accessing OBS over intranet by using OBS Browser on a Linux ECS



Procedure

Step 1 Log In to the Linux ECS.

1. Log in to **HUAWEI CLOUD** and click **Console**.
2. On the home page of the console, choose **Computing** > **Elastic Cloud Server**.
3. Select an ECS and log in to the ECS.

   The login mode is set during the Linux EC creation.

   For details about how to log in to the ECS, see **Logging In to an ECS**.

Step 2 Check whether the intranet DNS is configured on the Linux ECS.

1. Log in to the Linux ECS and open the CLI.
2. Run the **cat /etc/resolv.conf** command to check whether the IP address after **nameserver** in the first line is the intranet DNS address of the region where the current ECS resides.

   NOTE

   HUAWEI CLOUD provides different private DNS server addresses for different regions. For details, see **What Are the Private DNS Server Addresses Provided by the DNS Service?**

   - If no, go to **Step 3**.
   - If yes, go to **Step 4**.

Step 3 Configure the Intranet DNS.

Change the DNS server address of the ECS to the intranet DNS provided by HUAWEI CLOUD. You can change the DNS address of the VPC subnet or modify the local DNS configuration to achieve this.

- **Methods 1: Changing the DNS server address of the VPC subnet**

  Locate the VPC where the ECS resides and change the DNS server address of the VPC subnet the intranet DNS address. In this manner, ECSs in the VPC can use the intranet DNS for resolution and thereby you can access OBS on HUAWEI CLOUD intranet. For details, see **Modifying a Subnet**.

  NOTE

  The intranet DNS server address must be selected based on the region where the ECS resides. For details, see **What Are the Private DNS Server Addresses Provided by the DNS Service?**

- **Method 2: Modifying the local DNS configuration**

  The following uses an ECS running 64-bit CentOS 6.x as an example to describe how to modify the local DNS configuration.

  a. Open the CLI.

  b. Run the following command to open the **/etc/resolv.conf** file:

  ```
  vi /etc/resolv.conf
  ```

  c. Press **i** to enter the editing mode. In the **/etc/resolv.conf** file, add the intranet DNS server address before the existing DNS server address in the following format:

  nameserver *Intranet DNS server address*

NOTE

- The intranet DNS server address must be selected based on the region where the ECS resides. For details, see **What Are the Private DNS Server Addresses Provided by the DNS Service?**
- The IP address of the new DNS server must come before all existing DNS IP addresses.
- DNS servers are selected in the sequence of **nameserver**. A new DNS server is selected only when the previous DNS server is faulty, unavailable, or cannot resolve the requested domain name. Therefore, if you want to switch to the public network access mode, you need to change the first line of the DNS address to a public DNS server address or add a public DNS server address before the existing DNS server address.

d. Press **ESC** and enter **:wq!** to save the settings and close the file.

NOTE

The modified DNS server address takes effect immediately after you save the modification to the **/etc/resolv.conf** file.

Step 4 Download obsutil.

For details about the latest version of obsutil and download link, see **Downloading obsutil**.

Step 5 Configure obsutil.

Before using obsutil, you need to configure the interconnection between obsutil and OBS. Parameters include OBS endpoints and access keys (AK and SK).

For details, see **Performing Initial Configuration** in the tool guide of obsutil.

NOTE

The OBS endpoint needs to be entered according to the region where the ECS resides.

For details about OBS regions and endpoints, see **Regions and Endpoints**.

Step 6 Use obsutil.

After obsutil is successfully configured, you can access OBS over HUAWEI CLOUD intranet on the Linux ECS to perform basic data access operations and other advanced settings.

For details, see the following topics:

- **Uploading an Object**
- **Downloading an Object**

For details, see **OBS Tools Guide (obsutil)**.

----End

