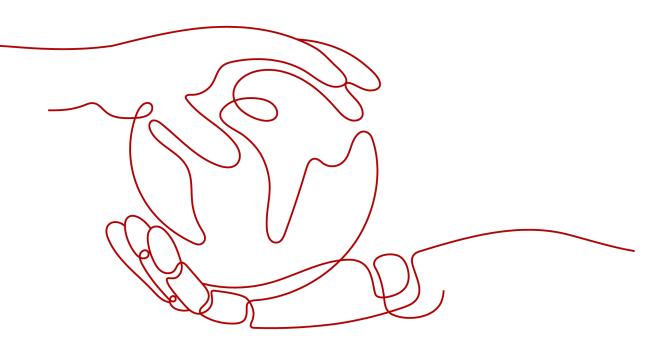
Elastic Cloud Server

Best Practices

 Issue
 01

 Date
 2024-11-04





HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

NUAWEI 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:

https://www.huawei.com/en/psirt/vul-response-process

For vulnerability information, enterprise customers can visit the following web page: <u>https://securitybulletin.huawei.com/enterprise/en/security-advisory</u>

Contents

1 Best Practices Summary	1
2 Setting Up Websites on ECSs	6
3 Configuring an ECS	11
4 Setting Up an Environment	
4.1 Setting Up an LNMP Environment	14
4.1.1 Manually Deploying LNMP (CentOS 7.2)	14
4.1.2 Manually Deploying LNMP (CentOS 8.0)	
4.1.3 Manually Deploying LNMP (Ubuntu 20.04)	
4.1.4 Manually Deploying LNMP (Huawei Cloud EulerOS 2.0)	
4.2 Setting Up an LAMP Environment	
4.2.1 Manually Deploying LAMP (CentOS 7.8 PHP 7.0)	41
4.3 Setting Up a Java Web Environment	47
4.3.1 Setting Up Tomcat-based Java Web Environment (CentOS 7.4)	
4.3.2 Setting Up Tomcat-based Java Web Environment (Huawei Cloud EulerOS 2.0)	54
4.4 Manually Deploying Node.js (CentOS 7.2)	56
5 Setting Up a Website	60
5 Setting Up a Website	
	60
5.1 Setting Up a WordPress Website	60 60
5.1 Setting Up a WordPress Website5.1.1 Setting Up a WordPress Website (Linux)	60 60 65
5.1 Setting Up a WordPress Website5.1.1 Setting Up a WordPress Website (Linux)5.2 Setting Up a Discuz Forum	
 5.1 Setting Up a WordPress Website	
 5.1 Setting Up a WordPress Website	
 5.1 Setting Up a WordPress Website	
 5.1 Setting Up a WordPress Website	
 5.1 Setting Up a WordPress Website	
 5.1 Setting Up a WordPress Website	
 5.1 Setting Up a WordPress Website	
 5.1 Setting Up a WordPress Website	
 5.1 Setting Up a WordPress Website	

6.1.3 Setting Up an FTP Site (Linux)	140
6.1.4 Setting Up an FTP Site (Huawei Cloud EulerOS 2.0)	
6.2 Building Microsoft SharePoint Server 2016	147
6.2.1 Purchasing and Logging In to an ECS	147
6.2.2 Adding AD, DHCP, DNS, and IIS Services	
6.2.3 Installing SQL Server	155
6.2.4 Installing Microsoft SharePoint Server 2016	
6.2.5 Configuring Microsoft SharePoint Server 2016	
6.2.6 Verifying Microsoft SharePoint Server 2016	171
6.3 Deploying Docker	174
6.3.1 Manually Deploying Docker (CentOS 7.5)	174
6.4 Deploying an ECS for Handling Text Messages from an Official WeChat Account	178
6.5 Manually Deploying GitLab (CentOS 7.2)	
6.6 Manually Deploying RabbitMQ (CentOS 7.4)	189
6.7 Setting Up Master-Slave Replication on PostgreSQL	193
6.8 Manually Installing a BT Panel (CentOS 7.2)	196
6.9 Installing and Deploying Jenkins on an ECS	
6.10 Using auditd to Record File Changes (Linux)	204
6.11 Restoring Accidentally Deleted Data Using Extundelete (Linux)	
6.12 Setting Up a ThinkPHP Framework	
7 Securing an ECS	
7.1 Enhancing Security for SSH Logins to Linux ECSs	212
7.2 Using a Virtual IP Address and Keepalived to Set Up a High-Availability Web Cluster	
8 Migrating an ECS	234
8.1 Migrating Servers to the Cloud	234
8.2 Migrating ECSs Across Accounts and Regions Through Image Replication	236
9 Accessing OBS from an ECS over the Intranet	
9.1 Overview	248
9.2 Accessing OBS over Intranet by Using OBS Browser+ on a Windows ECS	250
9.3 Accessing OBS over Intranet by Using obsutil on a Linux ECS	253
10 Using VNC Viewer to Access a Linux ECS	257



This section describes common application scenarios of Elastic Cloud Server (ECS) and provides solution details and an operation guide for each scenario, so you can easily deploy services using ECS.

Best Practices for Using ECSs

Category	Scenario	Reference	Description
Environmen t setup	Setting up an LNMP environme nt	Manually Deploying LNMP (CentOS 7.2)	An ECS running CentOS 7.2 64-bit is used as an example to describe how to set up an LNMP environment.
		Manually Deploying LNMP (CentOS 8.0)	An ECS running CentOS 8.0 64-bit is used as an example to describe how to set up an LNMP environment.
		Manually Deploying LNMP (Ubuntu 20.04)	An ECS running Ubuntu 20.04 64-bit is used as an example to describe how to set up an LNMP environment.
		Manually Deploying LNMP (Huawei Cloud EulerOS 2.0)	An ECS running Huawei Cloud EulerOS 2.0 64-bit is used as an example to describe how to set up an LNMP environment.

Category	Scenario	Reference	Description
	Setting up an LAMP environme nt	Manually Deploying LAMP (CentOS 7.8 PHP 7.0)	An ECS running CentOS 7.8 64-bit is used as an example to describe how to set up an LAMP environment.
	Setting up a Java web environme nt	Setting Up Tomcat- based Java Web Environment (CentOS 7.4)	An ECS running CentOS 7.4 64-bit is used as an example to describe how to set up a Java Web environment.
		Setting Up Tomcat- based Java Web Environment (Huawei Cloud EulerOS 2.0)	An ECS running Huawei Cloud EulerOS 2.0 64-bit is used as an example to describe how to set up a Java Web environment.
	Setting up a Node.js environme nt	Manually Deploying Node.js	An ECS running CentOS 7.2 64-bit is used as an example to describe how to set up a Node.js environment.
Website setup	Setting up a WordPress website	Setting Up a WordPress Website (Linux)	An ECS running CentOS 7.2 64-bit is used as an example to describe how to set up a WordPress website.
	Setting up a Discuz forum	Setting Up a Discuz Forum	An ECS running CentOS is used as an example to describe how to set up a Discuz forum.
	Setting up a Magento e- commerce website	Manually Setting Up a Magento E-Commerce Website (Linux)	An ECS running CentOS 7.2 64-bit is used as an example to describe how to set up a Magento e- commerce website.
	Deploying a Ghost blog	Manually Deploying a Ghost Blog (Ubuntu 20.04)	An ECS running Ubuntu 20.04 64-bit is used as an example to describe how to deploy a Ghost blog.
Application setup	Setting up an FTP site	Setting Up an FTP Site (Windows 2012)	An ECS running Windows Server 2012 Datacenter 64-bit is used as an example to describe how to set up an FTP site.

Category	Scenario	Reference	Description
		Setting Up an FTP Site (Windows 2019)	An ECS running Windows Server 2019 Datacenter 64-bit is used as an example to describe how to set up an FTP site.
		Setting Up an FTP Site (Linux)	An ECS running CentOS 7.2 64-bit is used as an example to describe how to set up an FTP website.
	Building Microsoft SharePoint Server	Building Microsoft SharePoint Server 2016	An ECS running Windows Server 2012 Datacenter 64-bit is used as an example to describe how to build Microsoft SharePoint Server 2016.
	Deploying Docker	Manually Deploying Docker (CentOS 7.5)	An ECS running CentOS 7.5 64-bit is used as an example to describe how to deploy Docker.
	Deploying an ECS as an official WeChat account server	Deploying an ECS for Handling Text Messages from an Official WeChat Account	An ECS running CentOS 7.4 64-bit is used as an example to describe how to deploy an ECS as an official WeChat account server.
	Installing the BT panel	Manually Installing a BT Panel (CentOS 7.2)	An ECS running CentOS 7.2 64-bit is used as an example to describe how to install the BT panel.
	Deploying GitLab	Manually Deploying GitLab (CentOS 7.2)	An ECS running CentOS 7.2 64-bit is used as an example to describe how to deploy GitLab.
	Deploying RabbitMQ	Manually Deploying RabbitMQ (CentOS 7.4)	An ECS running CentOS 7.4 64-bit is used as an example to describe how to deploy RabbitMQ.
	Setting up a ThinkPHP framework	Setting Up a ThinkPHP Framework	An ECS running CentOS 7.2 64-bit is used as an example to describe how to set up a ThinkPHP framework.

Category	Scenario	Reference	Description
	Setting up master- slave replication on PostgreSQ L	Setting Up Master- Slave Replication on PostgreSQL	An ECS running CentOS 7.6 64-bit is used as an example to describe how to set up master-slave replication on PostgreSQL.
	Deploying Jenkins	Installing and Deploying Jenkins on an ECS	An ECS running CentOS 7.6 64-bit is used as an example to describe how to deploy Jenkins.
	Configurin g auditd	Using auditd to Record File Changes (Linux)	An ECS running CentOS 7.4 64-bit is used as an example to describe how to install and configure auditd.
	Restoring data using Extundelet e quickly	Restoring Accidentally Deleted Data Using Extundelete (Linux)	An ECS running CentOS 7.5 64-bit is used as an example to describe how to use the open-source tool Extundelete to quickly restore accidentally deleted data.
ECS security	Enhancing security for SSH logins to Linux ECSs	Enhancing Security for SSH Logins to Linux ECSs	An ECS running CentOS 7.6 64-bit is used as an example to describe how to enhance security for SSH logins.
	Setting up a high- availability web cluster	Using a Virtual IP Address and Keepalived to Set Up a High-Availability Web Cluster	An ECS running CentOS 7.8 64-bit is used as an example to describe how to use a virtual IP address and Keepalived to set up a high-availability web cluster.
Cloud server migration	Migrating servers to the cloud	Migrating Servers to the Cloud	It describes how to use Server Migration Service (SMS) and image import to migrate applications and data from your existing servers to Huawei Cloud.

Category	Scenario	Reference	Description
	Migrating ECSs across accounts and regions through image replication	Migrating ECSs Across Accounts and Regions Through Image Replication	It describes how to migrate ECSs between Huawei Cloud accounts in different regions.
Other	Accessing OBS from an ECS over an	Accessing OBS over Intranet by Using OBS Browser+ on a Windows ECS	It describes how to use OBS Browser+ to access OBS over intranet on a Windows ECS.
	intranet	Accessing OBS over Intranet by Using obsutil on a Linux ECS	It describes how to use obsutil to access OBS over intranet on a Linux ECS.
	Using VNC Viewer to access a Linux ECS	Using VNC Viewer to Access a Linux ECS	Ubuntu 20.04 OS is used as an example to describe how to install VNC Server on a Linux ECS and how to use VNC Viewer to access the ECS.

2 Setting Up Websites on ECSs

Overview

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

Summary

 Table 2-1
 Summary on website setups

Website Setup Solution	How to Set Up	OS	Image and Resources	Description
Setting Up a Discuz Forum	Manual setup	Linux	Public image	Discuz! is a common community forum software system. Its basic architecture is based on the popular web programming combination of PHP +MySQL.
Setting Up an FTP Site (Windows 2012)	Manual setup	Windo ws	Public image	Use FTP delivered with Windows to set up an FTP site.
Setting Up an FTP Site (Linux)	Manual setup	Linux	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.

Website Setup Solution	How to Set Up	OS	Image and Resources	Description
Setting Up Tomcat- based Java Web Environme nt	Manual setup	Linux	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.
Manually Setting Up a Magento E- Commerce Website (Linux)	Manual setup	Linux	Public imageMySQL 5.7PHP 7.0Magento 2.1	Magento is an open source e-commerce system that features flexible design, modular architecture, and rich functions. It is suitable for building medium- and large- sized sites.
Building Microsoft SharePoint Server 2016	Manual setup	Windo ws	 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.
Manually Deploying LNMP (CentOS 7.2)	Manual setup	Linux	Public imageNginx 1.14.0MySQL 5.7PHP 7.0.31	LNMP indicates the Nginx+MySQL+PHP website server architecture in Linux. Nginx is compact, efficient web server software in Linux.
Setting Up a WordPress Website (Linux)	Manual setup	Linux	 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 free CMS or website setup system.

Website Setup Solution	How to Set Up	OS	Image and Resources	Description
Manually Deploying Docker (CentOS 7.5)	Manual setup	Linux	Public image	Docker is deployed on a Linux ECS. Additionally, common Docker operations and the process of creating a Docker image are provided.
Deploying an ECS for Handling Text Messages from an Official WeChat Account	Manual setup	Linux	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.
Manually Deploying GitLab (CentOS 7.2)	Manual setup	Linux	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.

Website Setup Solution	How to Set Up	OS	Image and Resources	Description
Manually Deploying RabbitMQ (CentOS 7.4)	Manual setup	Linux	Public imageErlang 8.3RabbitMQ 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.
Manually Deploying a Ghost Blog (Ubuntu 20.04)	Manual setup	Linux	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 20.04.

Website Setup Solution	How to Set Up	OS	Image and Resources	Description
Manually Deploying Node.js (CentOS 7.2)	Manual setup	Linux	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.

3 Configuring an ECS

To use ECSs more securely, reliably, flexibly, and efficiently, follow the best practices for ECS.

Access and Connection

We recommend that you use the Virtual Network Computing (VNC) when logging in to your ECS for the first time and check that the ECS is running properly.

For details, see:

- Login Using VNC
- Login Using VNC

The next time you log in, you can choose a proper login method based on your local environment and whether your ECS has an EIP bound. For details, see **How Do I Log In to My ECS?**.

System Updates

• Linux image source updates

To obtain the latest system updates and software installation dependencies, update the image source before using an ECS.

Huawei Cloud image sources are stable and can be updated without accessing the Internet. For ECSs running EulerOS, CentOS, Debian, or Ubuntu, replace their image sources with Huawei Cloud images sources by referring to How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)?

• Windows patches and drivers updates

To improve the fault rectification capability and performance of ECSs, periodically update Windows patches and drivers.

You can enable Windows automatic updates to detect the latest patches and driver versions.

Data Storage

• Storage security

To ensure data storage security, use the system disk to store OS data and use data disks to store application data. This ensures data security and prevents

data loss caused by system faults. As service demand changes, you can expand storage capacity by:

- Expanding disk capacity: You can expand both system disks and data disks. For details, see Expanding Capacity for an In-use EVS Disk.
- Adding data disks: You can add only data disks. After adding disks, you need to attach and initialize them before they can be used.
- Data encryption

To further protect data security, both the system and data disks can be encrypted. For details, see **Managing Encrypted EVS Disks**.

Security Management

• Identity authentication

To securely control access to resources and centrally manage permissions, use IAM users and Enterprise Management for identity authentication, permissions management, and resource group management. For details, see Assigning Permissions to O&M Personnel and Multi-project Management Cases.

• Login authentication

To ensure that the password can be reset successfully, **install one-click password reset plug-ins** or **update one-click password reset plug-ins** after purchasing an ECS.

Access control

To control inbound and outbound access to ECSs and improve security, set access control policies based on:

- ECSs: Configure security group rules to control access to ECSs.
- Subnets: Configure network ACLs to control access to all ECSs in a given subnet.
- Server security

In addition to the basic edition of Host Security Service (HSS), use advanced editions to enhance the security of your ECSs. For details about HSS editions, see **Edition details** and **HSS Getting Started**.

Network security

To protect an ECS with an EIP bound from online attacks, purchase **Selecting DDoS Mitigation Editions**.

• Critical operation protection

To ensure account and operation security, enable operation protection. This will require identity authentication for critical operations like stopping, restarting, or deleting resources. Operation protection takes effect for your account and IAM users created using your account.

For details, see **Protection for Mission-Critical Operations**.

Backup and Restore

• Data backup and restore

To quickly restore data in case of virus intrusion, mis-deletion, and hardware or software faults, back up data periodically. For details, see **Cloud Backup** and **Recovery (CBR)**.

After the backup is successful, you can **restore data using a cloud server backup** or **use a backup to create an image**.

• Service disaster recovery (DR)

For high service DR capabilities, deploy ECSs in the same region in different AZs. For details about AZs, see **Region and AZ** and **Purchasing a Custom ECS**.

• Service high availability (HA)

To achieve HA through active/standby ECS switchovers, **build highly** available web server clusters with Keepalived.

Resource Management

• Monitoring

Use **Cloud Eye** to keep informed of ECS performance metrics and statuses in real time, and receive alarms if any exceptions occur.

• Tracing

Use **Cloud Trace Service (CTS)** to record operations on your ECSs for later query, auditing, and backtracking.

• Logging

Use **Log Tank Service (LTS)** to collect ECS logs for centralized management. With LTS, you can analyze large volumes of logs efficiently, securely, and in real time and gain insights into improving availability and performance of applications.

4 Setting Up an Environment

4.1 Setting Up an LNMP Environment

4.1.1 Manually Deploying LNMP (CentOS 7.2)

Overview

LNMP (Linux, Nginx, MySQL, and PHP) is one of the mainstream website server architectures. It is used for running large-sized and high-concurrency website applications, such as e-commerce websites, social networks, and content management systems. This section describes how to use a CentOS 7.2 64bit Linux ECS to set up an LNMP environment on Huawei Cloud.

The process is as follows:

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

Prerequisites

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

Table 4-1	Security	group rule
-----------	----------	------------

Directi on	Priori ty	Action	Туре	Protocol & Port	Source Address
Inboun d	1	Allow	IPv4	TCP: 80	0.0.0.0/0

3. To obtain and update the system and software, you are advised to update the image source to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)?

Resource Planning

Table 4-2 lists the resource configuration and software versions used in this practice. The commands and parameters may vary according to the hardware specifications or software versions you would use.

Resource	Description	Cost
ECS	 Billing mode: pay-per-use AZ: AZ1 Flavor: s6.large.4 Image: CentOS 7.2 64bit System disk: 40 GiB EIP: Auto assign EIP type: Dynamic BGP Billed by: Traffic Bandwidth: 5 Mbit/s 	The following resources generate costs: • ECSs • EVS disks • EIPs For billing details, see Billing Modes .
Nginx	A high-performance HTTP and reverse proxy server. Download URL: http://nginx.org/packages/ centos/7/noarch/RPMS/ nginx-release- centos-7-0.el7.ngx.noarch.rp m	Free
MySQL	An open-source relational database software. Download URL: https://dev.mysql.com/get/ mysql80-community- release-el7-11.noarch.rpm	Free
РНР	An open-source software used for web development. Download URL: https:// mirrors.huaweicloud.com/ remi/enterprise/remi- release-7.rpm	Free

Table 4-2 R	lesources a	and costs
-------------	-------------	-----------

Procedure

Step 1 Install Nginx.

- 1. Log in to the ECS.
- Run the following command to download the Nginx package: wget http://nginx.org/packages/centos/7/noarch/RPMS/nginx-releasecentos-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 command to check the Nginx version:

nginx -v

Information similar to the following is displayed: nginx version: nginx/1.26.1

6. Run the following commands to start Nginx and enable it to start automatically upon ECS startup:

systemctl start nginx

systemctl enable nginx

7. Check the startup status.

systemctl status nginx.service

8. 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 4-1 Accessing Nginx

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to <u>nginx.org</u>. Commercial support is available at <u>nginx.com</u>.

Thank you for using nginx.

Step 2 Install MySQL.

1. Run the following commands in sequence to install MySQL:

rpm -Uvh https://dev.mysql.com/get/mysql80-community-releaseel7-11.noarch.rpm

yum -y install mysql-community-server

 Run the following command to check the MySQL version: mysql -V

Information similar to the following is displayed: mysql Ver 8.0.39 for Linux on x86_64 (MySQL Community Server - GPL) 3. Run the following commands in sequence to start MySQL and enable it to start automatically upon ECS startup:

systemctl start mysqld

systemctl enable mysqld

4. Run the following command to check the MySQL status:

systemctl status mysqld.service

Information similar to the following is displayed.

[root@
■ mysqld.service - MySQL Server
Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; vendor preset: disabled)
Active: active (running) since Wed 2024-08-14 17:01:17 CST; 19s ago
Docs: man:mysqld(8)
http://dev.mysql.com/doc/refman/en/using-systemd.html
Main PID: 8482 (mysqld)
Status: "Server is operational"
CGroup: /system.slice/mysqld.service
└─8482 /usr/sbin/mysqld
Aug 14 17:01:11 systemd[1]: Starting MySQL Server
Aug 14 17:01:17 systemd[1]: Started MySQL Server.

5. Run the following command to obtain the **root** user's password 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

6. Run the following command and follow the prompts 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 a new 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) : N #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 #Press Y to remove anonymous users. 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 #Press Y to disallow remote logins of user **root**. 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 #Press Y to

delete the test database and remove access to it. - 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 #Press Y to reload privilege tables. Success.

All done!

Step 3 Install PHP.

1. Run the following commands to install the EPEL and REMI repositories:

yum install -y epel-release

rpm -Uvh https://mirrors.huaweicloud.com/remi/enterprise/remirelease-7.rpm

- 2. Run the following command to install the Yum repository management tool: **yum -y install yum-utils**
- 3. Run the following command to enable the PHP 8.0 repository:

yum-config-manager --enable remi-php80

4. Run the following commands to install PHP:

yum install -y php php-cli php-fpm php-mysqlnd php-zip php-devel phpgd php-mcrypt php-mbstring php-curl php-xml php-pear php-bcmath php-json

5. Run the following command to check the version of the installed PHP:

php -v

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

[rootQ. ~]# php -v PHP 8.0.30 (cli) (built: Jun 4 2024 15:19:49) (NTS gcc x86_64) Copyright (c) The PHP Group Zend Engine v4.0.30, Copyright (c) Zend Technologies

6. Run the following commands to start PHP and enable it to start automatically upon ECS startup:

systemctl start php-fpm systemctl enable php-fpm

- 7. 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**

Figure 4-2 nginx.conf

iser nginx; worker_processes auto;	
error_log /var/log/nginx/error.log notice; pid /var/run/nginx.pid;	
events { worker_connections 1024; }	
<pre>http { include /etc/nginx/mime.types; default_type application/octet-stream; log_format main '\$remote_addr - \$remote_user [\$time_local] "\$request" ' '\$status \$body_bytes_sent "\$http_referer" ' '"\$http user agent" "Shttp x forwarded for"'; } }</pre>	
access_log /var/log/nginx/access.log main; sendfile on; #tcp_nopush on;	
keepalive_timeout 65; #gzip on;	
include /etc/nginx/conf.d/*.conf;	

According to the nginx.conf, the configuration file is directed to **/etc/nginx/conf.d/*.conf**.

- b. Enter :quit to exit nginx.conf.
- c. Run the following command to open the **/etc/nginx/conf.d/default.conf** file:

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

- d. Press **i** to enter insert mode.
- e. Modify the **default.conf** file.

Find the **server** paragraph and configure it as follows:

```
server {
   listen
             80:
   server_name localhost;
   #access_log /var/log/nginx/host.access.log main;
 location / {
    root /usr/share/nginx/html;
   index index.html index.htm index.php;
 }
 location ~ \.php$ {
   root
              /usr/share/nginx/html;
    fastcgi_pass 127.0.0.1:9000;
   fastcgi_index index.php;
   fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    include
               fastcgi_params;
 }
}
```

Figure 4-3 shows the configuration after modification.



```
listen
             80;
             localhost;
server_name
#access_log /var/log/nginx/host.access.log main;
location ∕ {
    root /usr/share/nginx/html;
    index index.html index.htm
                                  index.php
}
location ~
           N.php$ {
    root
                   /usr/share/nginx/html;
   fastcgi_pass
fastcgi_index
                   127.0.0.1:9000;
                   index.php;
    fastcgi_param_SCRIPT_FILENAME_$document_root$fastcgi_script_name;
    include
                   fastcgi_params;
}
#error_page 404
                               /404.html;
# redirect server error pages to the static page /50x.html
#
             500 502 503 504 /50x.html;
error_page
location = /50 \times .html {
          /usr/share/nginx/html;
    root
```

- f. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the file.
- 8. 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 file 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 insert mode.

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

PHP Version 8.0.30	Php
System	Linux 💻 페 3.10.0-1160.53.1.el7.x86_64 #1 SMP Fri Jan 14 13:59:45 UTC 2022 x86_64
Build Date	Jun 4 2024 15:19:49
Build System	Red Hat Enterprise Linux Server release 7.9 (Maipo)
Build Provider	Remi's RPM repository <https: rpms.remirepo.net=""></https:> #StandWithUkraine
Compiler	gcc (GCC) 8.3.1 20190311 (Red Hat 8.3.1-3)
Architecture	x86_64
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/20-bcmath.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-trinii, /etc/php.d/20-dom.ini, /etc/php.d/20-extif.ni, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-trip.ini, /etc/php.d/20-sinii, /etc/php.d/20-gettext.ini, /etc/php.d/20-icnov.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-simpsqind.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-sintini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sodium.ini, /etc/php.d/20-solite3.ini, /etc/php.d/20-symmsgi.ini, /etc/php.d/20-syssem.ini, /etc/php.d/20-sodium.ini, /etc/php.d/20-solite3.ini, /etc/php.d/20-symmsgi.ini, /etc/php.d/20-syssem.ini, /etc/php.d/20-syssem.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-syssem.jii, /etc/php.d/20-syssem.ini, /etc/php.d/20-system.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-syssem.jii, /etc/php.d/20-syssem.ini, /etc/php.d/20-system.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-syssem.jii, /etc/php.d/20-syssem.ini, /etc/php.d/30-mcrypt.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_gsqlites.ini, /etc/php.d/30-sip.simi
РНР АРІ	20200930
PHP Extension	20200930
Zend Extension	420200930
Zend Extension Build	API420200930,NTS
PHP Extension Build	API20200930,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*, mcrypt.*, mdecrypt.*

----End

4.1.2 Manually Deploying LNMP (CentOS 8.0)

Overview

LNMP (Linux, Nginx, MySQL, and PHP) is one of the mainstream website server architectures. It is used for running large-sized and high-concurrency website applications, such as e-commerce websites, social networks, and content management systems. This section describes how to use a CentOS 8.0 64bit Linux ECS to set up the LNMP environment on Huaei Cloud.

The process is as follows:

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

Prerequisites

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

Table 4-3	Security	group	rules
-----------	----------	-------	-------

Directi on	Priori ty	Action	Туре	Protocol & Port	Source Address
Inboun d	1	Allow	IPv4	TCP: 80	0.0.0.0/0

3. To obtain and update the system and software, you are advised to update the image source to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)?

Resource Planning

Table 4-4 lists the resource configuration and software versions used in this practice. The commands and parameters may vary according to the hardware specifications or software versions you would use.

Resource	Description	Cost
ECS	 Billing mode: pay-per-use AZ: AZ1 Flavor: s6.large.4 Image: CentOS 8.0 64bit System disk: 40 GiB EIP: Auto assign EIP type: Dynamic BGP Billed by: Traffic Bandwidth: 5 Mbit/s 	 The following resources generate costs: ECSs EVS disks EIPs For billing details, see Billing Modes.
Nginx	A high-performance HTTP and reverse proxy server. Example: Nginx 1.20.1	Free
MySQL	An open-source relational database software Example: MySQL 8.0.26	Free
РНР	An open-source software used for web development Example: PHP 7.4.19	Free

Table 4-4 Resources and c	costs
---------------------------	-------

Procedure

Step 1 Install Nginx.

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

sudo dnf -y install https://nginx.org/packages/centos/8/x86_64/RPMS/ nginx-1.20.1-1.el8.ngx.x86_64.rpm

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

nginx -v

Information similar to the following is displayed: nginx version: nginx/1.20.1

4. Run the following commands to start Nginx and enable it to start automatically upon ECS startup:

systemctl start nginx

systemctl enable nginx

5. Run the following command to check the startup status:

systemctl status nginx.service

Information similar to the following is displayed.

[root@
Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
Active: active (running) since Wed 2024-00-14 10:47:48 CST; 25s ago
Docs: http://nginx.org/en/docs/
Main PID: 1793 (nginx)
Tasks: 3 (limit: 49517)
Memory: 3.0M
CGroup: /system.slice/nginx.service
−1793 nginx: master process /usr/sbin/nginx -c /etc/nginx/nginx.conf
-1794 nginx: worker process
└─1795 nginx: worker process
Aug 14 10:47:48
Aug 14 10:47:48

6. 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 4-4 Accessing Nginx

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to <u>nginx.org</u>. Commercial support is available at <u>nginx.com</u>.

Thank you for using nginx.

Step 2 Install MySQL.

1. Run the following command to install MySQL:

sudo dnf -y install @mysql

 Run the following command to check the MySQL version: mysql -V

Information similar to the following is displayed: mysql Ver 8.0.26 for Linux on x86_64 (Source distribution) 3. Run the following commands in sequence to start MySQL and enable it to start automatically upon ECS startup:

systemctl start mysqld

systemctl enable mysqld

4. Check the MySQL status.

systemctl status mysqld.service

Information similar to the following is displayed.

[root@
• mysqld.service - MySQL 8.0 database server
Loaded: loaded (/usr/lib/systemd/system/mysgld.service; enabled; vendor preset: disabled)
Active: active (running) since Wed 2024-08-14 10:55:34 CST; 21s ago
Main PID: 2008 (mysqld)
Status: "Server is operational"
Tasks: 38 (limit: 49517)
Memory: 527.8M
CGroup: /system.slice/mysqld.service
└-2088 /usr/libexec/musgldbasedir=/usr
Aug 14 10:55:28 sustemd[1]: Starting MuSQL 8.0 database server
Aug 14 10:55:28 👘 👘 👘 🧰 mysql-prepare-db-dir[2004]: Initializing MySQL database
Aug 14 10:55:34 systemd[1]: Started MySQL 8.0 database server.

5. Run the following command and follow the prompts to harden MySQL:

mysql_secure_installation

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

VALIDATE PASSWORD COMPONENT can be used to test passwords and improve security. It checks the strength of password and allows the users to set only those passwords which are secure enough. Would you like to setup VALIDATE PASSWORD component? Press y|Y for Yes, any other key for No: Y #Press Y to set the password validation policy. There are three levels of password validation policy: LOW Length >= 8 MEDIUM Length >= 8, numeric, mixed case, and special characters STRONG Length >= 8, numeric, mixed case, special characters and dictionary file Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2 #Enter 2 to select the password validation policy. Please set the password for root here. New password: #Enter a new password of user root. 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 to confirm the new password. 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 #Press Y to remove anonymous users. 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 #Press Y to disallow remote logins of user **root**. 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 #Press Y to delete the **test** database and remove access to it. - 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 #Press Y to reload privilege tables. Success.

All done!

- Step 3 Install PHP.
 - 1. Run the following commands to add and update the EPEL repository:

```
sudo dnf -y install epel-release
```

sudo dnf -y update epel-release

2. Run the following commands to delete unnecessary software packages from the cache and update the software repository:

sudo dnf clean all

sudo dnf makecache

3. Run the following command to start the PHP 7.4 module:

dnf module enable php:7.4

4. Run the following command to install the required PHP module:

sudo dnf -y install php php-curl php-dom php-exif php-fileinfo php-fpm php-gd php-hash php-json php-mbstring php-mysqli php-openssl phppcre php-xml libsodium

5. Run the following command to check the version of the installed PHP:

php -v

Information similar to the following is displayed.

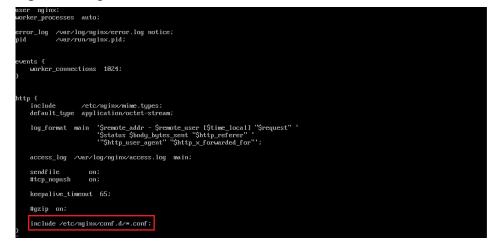
```
[root0
PHP 7.4.19 (cli) (built: May 4 2021 11:06:37) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
with Zend OPcache v7.4.19, Copyright (c), by Zend Technologies
```

6. Run the following commands to start PHP and enable it to start automatically upon ECS startup:

systemctl start php-fpm systemctl enable php-fpm

- 7. Modify the Nginx configuration file to support PHP.
 - Run the following command to open the /etc/nginx/nginx.conf file:
 vim /etc/nginx/nginx.conf

Figure 4-5 nginx.conf



According to the nginx.conf, the configuration file is directed to **/etc/nginx/conf.d/*.conf**.

- b. Enter :quit to exit nginx.conf.
- c. Run the following command to open the **/etc/nginx/conf.d/default.conf** file:

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

- d. Press **i** to enter the editing mode.
- e. Modify the **default.conf** file.

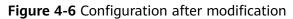
Find the **server** paragraph and configure it as follows:

```
server {
listen 80;
server_name localhost;
```

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

```
location / {
    root /usr/share/nginx/html;
    index index.html index.htm index.php;
}
location ~ \.php$ {
    root /usr/share/nginx/html;
    fastcgi_pass unix:/run/php-fpm/www.sock;
    fastcgi_index index.php;
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    include fastcgi_params;
}
```

Figure 4-6 shows the configuration after modification.



```
listen
              80;
              localhost;
server_name
#access_log /var/log/nginx/host.access.log main;
location / {
    root /usr/share/nginx/html;
index index.html index.htm
                                    index.php
location ~ \.php$ {
    root
                      /usr/share/nginx/html;
    fastcgi_pass
                    unix:/run/php-fpm/www.sock;
    fastcgi_index index.php; fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
                     fastcgi_params;
    include
#error_page 404
                                 /404.html;
# redirect server error pages to the static page /50x.html
Ħ
              500 502 503 504 /50x.html;
error_page
location = /50x.html {
          /usr/share/nginx/html;
    \mathbf{root}
3
# proxy the PHP scripts to Apache listening on 127.0.0.1:80
#
#location ~ \.php$ {
#
     proxy_pass http://127.0.0.1;
#}
```

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

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

06:37 Decache.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, url.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-forwini, sonini, /etc/php.d/20-dom.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-iconvini, sonini, /etc/php.d/20-isimplexml.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-solini, har.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-solini, sonini, /etc/php.d/20-solini, /etc/php.d/20-sockets.ini, /etc/php.d/20-solini, mysqli.ini, /etc/php.d/20-solini, /etc/php.d/20-solini, /etc/php.d/20-solini, mysqli.ini, /etc/php.d/20-solini, /etc/php.d/20-solini, /etc/php.d/20-solini, mysqli.ini, /etc/php.d/20-solini, /etc/php.d/30-pdo_sqlite.ini, /etc/php.d/30-
opcache.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, url.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-exit.ini, /etc/php.d/20-fileinfo.ini, tp.ini, /etc/php.d/20-gal.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-orourini, son.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-solini, ihar.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sokets.ini, /etc/php.d/20-solini
urlini, /etc/php.d/20-dom.ini, /etc/php.d/20-exitini, /etc/php.d/20-fileinfo.ini, tp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, son.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, ohenizer.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-suklini, /etc/php.d/20-suklini, soenizer.ini, /etc/php.d/20-unilini, /etc/php.d/20-suklini, /etc/php.d/20-suklini
urlini, /etc/php.d/20-dom.ini, /etc/php.d/20-exifini, /etc/php.d/20-fileinfo.ini, tp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, son.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, ohenizer.ini, /etc/php.d/20-simplesml.ini, /etc/php.d/20-sukl.ini, /etc/php.d/20-sukl.ini, soenizer.ini, /etc/php.d/20-unil.ini, /etc/php.d/20-sukl.ini, /etc/php.d/20-sukl.ini
urlini, /etc/php.d/20-dom.ini, /etc/php.d/20-exifini, /etc/php.d/20-fileinfo.ini, tp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconvini, sonini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-gdo.ini, ohenizerini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sckets.ini, /etc/php.d/20-sclini, ohenizerini, /etc/php.d/20-sclini, ini, /etc/php.d/20-sckets.ini, /etc/php.d/20-sclini
urlini, /etc/php.d/20-dom.ini, /etc/php.d/20-exifini, /etc/php.d/20-fileinfo.ini, tp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconvini, sonini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-gdo.ini, ohenizerini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sckets.ini, /etc/php.d/20-sclini, ohenizerini, /etc/php.d/20-sclini, ini, /etc/php.d/20-sckets.ini, /etc/php.d/20-sclini
urlini, /etc/php.d/20-dom.ini, /etc/php.d/20-exifini, /etc/php.d/20-fileinfo.ini, tp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconvini, son.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-gdo.ini, ohar.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sql.ini, soenizer.ini, /etc/php.d/20-unlini, /etc/php.d/20-swl.ini, /etc/php.d/20-skl.ini
urlini, /etc/php.d/20-dom.ini, /etc/php.d/20-exifini, /etc/php.d/20-fileinfo.ini, tp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconvini, son.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-gdo.ini, ohar.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sql.ini, soenizer.ini, /etc/php.d/20-unlini, /etc/php.d/20-swl.ini, /etc/php.d/20-skl.ini
NTS
TS
string
ed
press.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar
ıdg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, bzip2:

----End

4.1.3 Manually Deploying LNMP (Ubuntu 20.04)

Overview

The best practices for Huawei Cloud ECS guide you through the deployment of LNMP on a Linux ECS. This section uses the Ubuntu 20.04 64bit as an example.

The process is as follows:

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

Prerequisites

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

Directi on	Priori ty	Action	Туре	Protocol & Port	Source Address		
Inboun d	1	Allow	IPv4	TCP: 80	0.0.0/0		

 Table 4-5
 Security group rule

 The image source has been updated to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)? This facilitates obtaining and updating the system and software.

Resource Planning

Table 4-6 lists the resource configuration and software versions used in this practice. The commands and parameters may vary according to the hardware specifications or software versions you would use.

Resource	Description	Cost	
ECS	 Billing mode: pay-per-use AZ: AZ1 Flavor: s6.large.2 Image: Ubuntu 20.04 64bit System disk: 40 GiB EIP: Auto assign EIP type: Dynamic BGP Billed by: Traffic Bandwidth: 5 Mbit/s 	The following resources generate costs: • ECSs • EVS disks • EIPs For billing details, see Billing Modes.	
Nginx	A high-performance HTTP and reverse proxy server.	Free	
MySQL	An open-source relational database software.	Free	
РНР	An open-source software used for web development.	Free	

Table 4-6	Resources	and	costs
-----------	-----------	-----	-------

Procedure

Step 1 Install Nginx.

- 1. Log in to the ECS.
- Run the following commands to install Nginx: sudo apt-get update

sudo apt-get install nginx

If **Do you want to continue? [Y/n]** is displayed, enter **y** or **Y** to continue the installation.

3. (Optional) Configure the firewall.

Uncomplicated Firewall (UFW) is an iptables interface that simplifies the firewall configuration. By default, Ubuntu has UFW installed. 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

Information similar to the following 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 distribute TLS/SSL-encrypted traffic.
- Nginx HTTP: Port 80 is enabled to distribute normal and unencrypted web traffic.
- Nginx HTTPS: Port 443 is enabled to distribute TLS/SSL-encrypted traffic.

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

sudo ufw allow 'Nginx Full'

4. 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://***IP* address of the Nginx server in the address bar to access Nginx. If the following page is displayed, Nginx has been installed.

Figure 4-7 Accessing Nginx

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to <u>nginx.org</u>. Commercial support is available at <u>nginx.com</u>.

Thank you for using nginx.

Step 2 Install MySQL.

1. Run the following command to install MySQL:

sudo apt -y install mysql-server

2. Check the MySQL status.

sudo systemctl status mysql

```
    mysql.service - MySQL Community Server
Loaded: loaded (/lib/system//system/mysql.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2023-07-26 15:57:29 CST; 22min ago
Main PID: 10770 (mysqld)
Status: "Server is operational"
Tasks: 37 (limit: 4217)
Memory: 364.9M
CGroup: /system.slice/mysqld.service
10770 /usr/sbin/mysqld
```

Jul 26 15:57:29 ecs-ubuntu systemd[1]: Starting MySQL Community Server... Jul 26 15:57:29 ecs-ubuntu systemd[1]: Started MySQL Community Server.

3. Run the following command to access MySQL:

sudo mysql

4. Run the following command to set the password for user **root**:

ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password by 'xxxxx';

In the preceding command, *xxxxx* indicates the password you set for user **root**.

5. Run the following command to exit MySQL:

exit;

6. Run the following command and follow the prompts to harden MySQL:

mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root: #Enter the password of user **root** set in step 4.

VALIDATE PASSWORD COMPONENT can be used to test passwords and improve security. It checks the strength of password and allows the users to set only those passwords which are secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: Y #Press Y to set the password validation policy.

There are three levels of password validation policy:

LOW Length >= 8 MEDIUM Length >= 8, numeric, mixed case, and special characters STRONG Length >= 8, numeric, mixed case, special characters and dictionary file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2 #Enter **2** to select the password validation policy.

Using existing password for root.

Estimated strength of the password: 25 Change the password for root ? ((Press y|Y for Yes, any other key for No) : Y #Press Y to change the password of user **root**.

New password: #Enter a new password of user root.

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 to confirm the new password. 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 #Press Y to remove anonymous users. 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 #Press Y to disallow remote logins of user root. 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 #Press \mathbf{Y} to delete the test database and remove access to it. - 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 #Press Y to reload privilege tables. Success. All done!

Step 3 Install PHP.

1. Run the following commands to install PHP:

sudo apt update

sudo apt install php-fpm

2. Run the following command to check the version of the installed PHP:

php -v

Information similar to the following is displayed:

PHP 7.4.3-4ubuntu2.19 (cli) (built: Jun 27 2023 15:49:59) (NTS)
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
with Zend OPcache v7.4.3-4ubuntu2.19, Copyright (c), by Zend Technologies

3. Run the following command to check the runtime status of PHP:

systemctl status php7.4-fpm

Information similar to the following is displayed:

 php7.4-fpm.service - The PHP 7.4 FastCGI Process Manager Loaded: loaded (/lib/system/system/php7.4-fpm.service; enabled; vendor preset: enabled) Active: active (running) since Mon 2023-07-31 17:33:35 CST; 3min 50s ago Docs: man:php-fpm7.4(8)

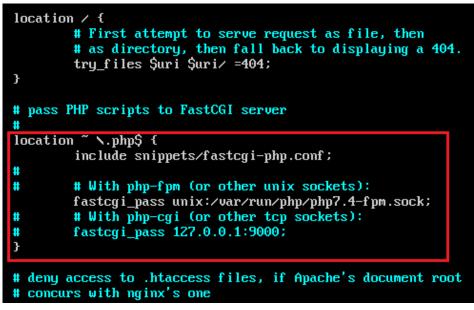
D NOTE

If lines 1-16/16 (end) is displayed in the command output, press q to exit.

- 4. Modify the Nginx configuration file to support PHP.
 - a. Run the following command to open the default Nginx configuration file: sudo vim /etc/nginx/sites-enabled/default
 - b. Press i to enter insert mode.
 - c. Modify the opened Nginx configuration file.
 - In **server{}**, find the line starting with **index** and add **index.php** to this line.

```
# Default server configuration
server {
        listen 80 default_server;
        listen [::]:80 default_server;
       # SSL configuration
        #
       # listen 443 ssl default_server;
       # listen [::]:443 ssl default_server;
       #
       # Note: You should disable gzip for SSL traffic.
       # See: https://bugs.debian.org/773332
       #
       # Read up on ssl_ciphers to ensure a secure configuration.
       # See: https://bugs.debian.org/765782
       #
       # Self signed certs generated by the ssl-cert package
       # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;
        root /var/www/html;
        # Add index.php to the list if you are using PHP
        index index.php index.html index.htm index.nginx-debian.html;
        server_name _;
        location / {
               # First attempt to serve request as file, then
```

Find **location** ~ \.**php\$ {}** in **server{}** and delete the comments from the lines in the following red box:



- d. Press **Esc** to exit insert mode. Then, enter **:wq** to save the settings and exit.
- 5. Run the following command to reload the Nginx configuration file: **sudo systemctl restart nginx**
- **Step 4** Test the LNMP deployment.
 - In the root directory of the Nginx website, create the phpinfo.php file.
 sudo vim /var/www/html/phpinfo.php
 - 2. Press **i** to enter insert mode.
 - 3. Modify the **phpinfo.php** file and add the following to the file: <?php echo phpinfo(); ?>
 - 4. Press **Esc** to exit insert mode. Then, enter :wq to save the settings and exit.
 - 5. Enter **http://***IP* address of the Nginx server/**phpinfo.php** in the address bar. If the following page is displayed, the LNMP environment has been deployed.

PHP Version 7.4.3-4ubuntu2.19	php
System	Linux ecs-Inmp 5.4.0-153-generic #170-Ubuntu SMP Fri Jun 16 13:43:31 UTC 2023 x86_64
Build Date	Jun 27 2023 15:49:59
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/fpm
Loaded Configuration File	/etc/php/7.4/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/fpm/conf.d
Additional .ini files parsed	/etc/php/7.4/fpm/conf.d/10-opcache.ini, /etc/php/7.4/fpm/conf.d/10-pdo.ini, /etc/php/7.4/fpm/conf.d/20-ackini, /etc/php/7.4/fpm/conf.d/20-ctype.ini, /etc/php/7.4/fpm/conf.d/20-exitini, /etc/php/7.4/fpm/conf.d/20-fple.ini, /etc/php/7.4/fpm/conf.d/20- fileinfo.ini, /etc/php/7.4/fpm/conf.d/20-ftp.ini, /etc/php/7.4/fpm/conf.d/20-gettext.ini, /etc/php/7.4/fpm/conf.d/20-iconx.ini, /etc/php/7.4/fpm/conf.d/20-joon.ini, /etc/php/7.4/fpm/conf.d/20- phar.ini, /etc/php/7.4/fpm/conf.d/20-sockini, /etc/php/7.4/fpm/conf.d/20-sockets.ini, /etc/php/7.4/fpm/conf.d/20-syswini, /etc/php/7.4/fpm/conf.d/20-sockets.ini, /etc/php/7.4/fpm/conf.d/20-syswsm.ini, /etc/php/7.4/fpm/conf.d/20-sockets.ini, /etc/php/7.4/fpm/conf.d/20-syswsm.ini, /etc/php/7.4/fpm/conf.d/20-sockets.ini,
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

----End

4.1.4 Manually Deploying LNMP (Huawei Cloud EulerOS 2.0)

Overview

The best practices for Huawei Cloud ECS guide you through the deployment of LNMP on a Linux ECS. This section uses the Huawei Cloud EulerOS 2.0 64bit as an example.

The process is as follows:

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

Prerequisites

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

		5 1			
Directi on	Priori ty	Action	Туре	Protocol & Port	Source Address
Inboun d	1	Allow	IPv4	TCP: 80	0.0.0.0/0

 Table 4-7 Security group rule

Resource Planning

Table 4-8 lists the resource configuration and software versions used in this practice. The commands and parameters may vary according to the hardware specifications or software versions you would use.

 Table 4-8 Resources and costs

Resource	Description	Cost
ECS	 Billing mode: pay-per-use AZ: AZ1 Flavor: s6.large.2 Image: Huawei Cloud EulerOS 2.0 64bit System disk: 40 GiB EIP: Auto assign EIP type: Dynamic BGP Billed by: Traffic Bandwidth: 5 Mbit/s 	The following resources generate costs: • ECSs • EVS disks • EIPs For billing details, see Billing Modes .
Nginx	A high-performance HTTP and reverse proxy server.	Free
MySQL	An open-source relational database software.	Free
РНР	An open-source software used for web development.	Free

Procedure

Step 1 Install Nginx.

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

sudo yum -y install nginx

3. Run the following command to check the version of the installed Nginx: **nginx -v**

Information similar to the following is displayed:

nginx version: nginx/1.21.5

4. Run the following commands to start Nginx and enable it to start automatically upon ECS startup:

systemctl start nginx

systemctl enable nginx

5. Run the following command to check the startup status:

systemctl status nginx.service

Information similar to the following is displayed:

<pre>Iroot@ecs-hce ~1# systemct1 status nginx.service • nginx.service - The nginx HTTP and reverse proxy server Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled) Active: active (running) since Fri 2023-08-11 14:59:59 CST; 18s ago Main PID: 4634 (nginx) Tasks: 3 (limit: 47418) Memory: 7.2M CGroup: /system.slice/nginx.service</pre>
– 4635 "nginx: worker process" – 4636 "nginx: worker process"
Aug 11 14:59:58 ecs-hce systemd[1]: Starting The nginx HTTP and reverse proxy server
Aug 11 14:59:58 ecs-hce nginx[4631]: nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
Aug 11 14:59:58 ecs-hce nginx[4631]: nginx: configuration file /etc/nginx/nginx.conf test is successful
Aug 11 14:59:59 ecs-hce systemd[1]: Started The nginx HTTP and reverse proxy server.

6. 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 4-8 Accessing Nginx

Welcome to nginx on openEuler!		
This page is used to test the proper operation of the nginx HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working property.		
Website Administrator		
This is the default inter that page that is distributed with nginx on openEuler. It is located in /wr/harv/hgint/hal. You should now put your content in a location of your choice and edit the rwis configuration directive in the nginx configuration file /win/hginx.wwf.		

NGINX

Step 2 Install MySQL.

1. Run the following commands in sequence to install MySQL:

mkdir mysql-server

cd mysql-server

wget https://repo.huaweicloud.com/hce/2.0/os/x86_64/Packages/ mysql-8.0.28-1.hce2.x86_64.rpm

yum install mysql-server

2. Run the following commands in sequence to start MySQL and enable it to start automatically upon ECS startup:

systemctl start mysqld

systemctl enable mysqld

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

systemctl status mysqld.service

Information similar to the following is displayed:

[root@ecs-hce mysql-server]# systemctl status mysqld.service
• mysgld.service - MySQL 8.0 database server
Loaded: loaded (/usr/lib/systemd/system/mysgld.service; enabled; vendor preset: disabled)
Active: active (running) since Fri 2023-08-11 11:17:57 CST; 20s ago
Main PID: 5390 (mysqld)
Status: "Server is operational"
Tasks: 38 (limit: 21654)
Memory: 465.7M
CGroup: /system.slice/mysqld.service
└──5390 /usr/libexec/musgldbasedir=/usr
Aug 11 11:17:51 ecs-hce systemd[1]: Starting MuSQL 8.0 database server
Aug 11 11:17:51 ecs-hce mysgl-prepare-db-dir[5312]: Initializing MuSQL database
Aug 11 11:17:57 ecs-hce sustemd[1]: Started MuSQL 8.0 database server.

4. Run the following command and follow the prompts to harden MySQL:

mysql_secure_installation

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

VALIDATE PASSWORD COMPONENT can be used to test passwords and improve security. It checks the strength of password and allows the users to set only those passwords which are secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No : Y

There are three levels of password validation policy:

LOW Length >= 8 MEDIUM Length >= 8, numeric, mixed case, and special characters SERONG Length >= 8, numeric, mixed case, special characters and dictionary file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2 Please set the password for root here.

New password: #Enter a new password of user root.

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 to confirm the new password. 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 #Press Y to remove anonymous users. 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 #Press Y to disallow remote logins of user **root**.

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 #Press Y to delete the test database and remove access to it. - 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 #Press Y to reload privilege tables. Success.

All done!

5. Run the following command to exit the current folder:

cd ~

Step 3 Install PHP.

1. Run the following commands in sequence to install PHP 8:

wget https://repo.huaweicloud.com/hce/2.0/os/x86_64/Packages/ php-8.0.0-10.hce2.x86_64.rpm

yum install php-8.0.0-10.hce2.x86_64.rpm

2. Run the following command to check the version of the installed PHP:

php -v

Information similar to the following is displayed:

```
[root@ecs-hce ~]# php -v
PHP 8.0.0 (cli) (built: Nov 24 2020 17:04:03) ( NTS )
Copyright (c) The PHP Group
Zend Engine v4.0.0-dev, Copyright (c) Zend Technologies
```

3. Run the following commands to start PHP and enable it to start automatically 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 Nginx configuration file:

vim /etc/nginx/nginx.conf

- b. Press i to enter insert mode.
- c. Modify the **nginx.conf** file.

Find the server paragraph and configure it as follows:

```
server {
  listen
            80:
  listen
            [::]:80;
  server_name _;
            /usr/share/nginx/html;
  root
  # Load configuration files for the default server block.
  include /etc/nginx/default.d/*.conf;
  location / {
    index index.php index.html index.htm; }
  location ~ .php$ {
     root /usr/share/nginx/html;
     fastcgi_pass 127.0.0.1:9000;
     fastcgi_index index.php;
     fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
     include fastcgi_params;
```

Figure 4-9 shows the configuration after modification.

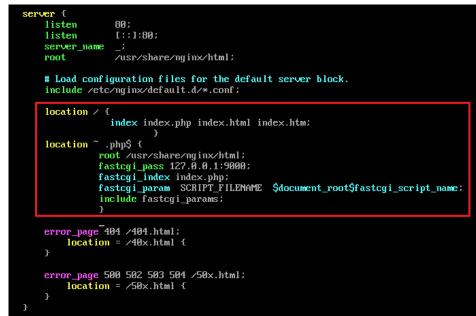


Figure 4-9 Configuration after modification

- d. Press **Esc** to exit insert mode. Then, enter **:wq** to save the settings and exit.
- 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 file 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 insert mode.
 - c. Modify the **info.php** file and add the following to the file: <?php phpinfo();
 - d. Press **Esc** to exit insert mode. Then, enter **:wq** to save the settings and exit.
- 2. Enter **http://***Server IP address***/info.php** in the address bar. If the following page is displayed, the LNMP environment has been set up.

zendengine

PHP Version 8.0.0	php
System	Linux ecs-hce 5.10.0-60.18.0.50.r865_35.hce2.x86_64 #1 SMP Sun Mar 26 18:01:01 UTC 2023 x86_64
Build Date	Nov 24 2020 17:04:03
Build System	Linux szxrtosci10000 4.19.90-2003.4.0.0036.oe1.x86_64 #1 SMP Mon Mar 23 19:10:41 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
Server API	FPM/FastCGI
/irtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
oaded Configuration File	/etc/php.ini
can this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-tokenizer.ini
PHP API	20200930
HP Extension	20200930
end Extension	420200930
end Extension Build	API420200930,NTS
PHP Extension Build	API20200930,NTS
Debug Build	no
hread Safety	disabled
end Signal Handling	enabled
end Memory Manager	enabled
end Multibyte Support	disabled
Pv6 Support	enabled
OTrace Support	available, disabled
egistered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*

This program makes use of the Zend Scripting Language Engine: Zend Engine v4.0.0-dev, Copyright (c) Zend Technologies

----End

4.2 Setting Up an LAMP Environment

4.2.1 Manually Deploying LAMP (CentOS 7.8 PHP 7.0)

Overview

LAMP is a web application platform consisting of Linux, Apache, MySQL, and PHP.

The best practices for Huawei Cloud ECS guide you through the deployment of LAMP on a Linux ECS. The CentOS 7.8 64bit OS is used as an example in this section.

Prerequisites

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

Table 4-9 Security group rule	
-------------------------------	--

Directi on	Priori ty	Action	Туре	Protocol & Port	Source Address
Inboun d	1	Allow	IPv4	TCP: 80	0.0.0.0/0

 The image source has been updated to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)? This facilitates obtaining and updating the system and software.

Resource Planning

Table 4-10 lists the resource configuration and software versions used in this practice. The commands and parameters may vary according to the hardware specifications or software versions you would use.

Resource	Description	Cost
ECS	 Billing mode: pay-per-use AZ: AZ1 Flavor: c7.large.2 Image: CentOS 7.8 64bit System disk: 40 GiB EIP: Auto assign EIP type: Dynamic BGP Billed by: Traffic Bandwidth: 5 Mbit/s 	The following resources generate costs: • ECSs • EVS disks • EIPs For billing details, see Billing Modes.
Apache	An open-source web server	Free
MySQL	An open-source relational database software Download URL: http://dev.mysql.com/get/ mysql57-community- release-el7-10.noarch.rpm	Free

Table 4-10 Resources and costs

Resource	Description	Cost
РНР	An open-source software used for web development	Free
	Download URL:	
	https:// mirror.webtatic.com/yum/el 7/epel-release.rpm	
	https:// mirror.webtatic.com/yum/el 7/webtatic-release.rpm	

Procedure

Step 1 Install Apache.

- 1. Log in to the ECS.
- 2. Run the following commands as user **root** to update the software package and install Apache:

yum -y update

yum -y install httpd

3. Run the following command to check the version of the installed Apache:

httpd -v

Information similar to the following is displayed: Server version: Apache/2.4.6 (CentOS) Server built: May 30 2023 14:01:11

4. Run the following commands in sequence to start Apache and enable it to start automatically upon ECS startup:

systemctl start httpd

systemctl enable httpd

5. Enter **http://***Server IP address* in the address bar of the browser to access Apache. If the following page is displayed, Apache has been installed.

Testing 123..

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

Just visiting?

Important note:

website run

domain should reach the appropriate person.

The website you just visited is either experiencing problems or is undergoing routine maintenance. If you would like to let the administrators of this website know that you've seen

Are you the Administrator?

You should add your website content to the directory /var/www/html/. To prevent this page from ever being used, follow the instructions in the file /etc/httpd/conf. d/welcome. conf.

this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's Promoting Apache and CentOS

You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOSI

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

The CentOS Project has nothing to do with this website or

its content, it just provides the software that makes the

The CentOS Project

The CentOS Linux distribution is a stable, predictable, manageable and reproduceable platform derived from the sources of Red Hat Enterprise Linux (RHEL).

Step 2 Install MySQL.

 Run the following commands in sequence to install MySQL: wget -i -c http://dev.mysql.com/get/mysql57-community-releaseel7-10.noarch.rpm

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

 Run the following command to check the version of the installed MySQL: mysql -V

Information similar to the following is displayed:

mysql Ver 14.14 Distrib 5.7.44, for Linux (x86_64) using EditLine wrapper

3. Run the following commands in sequence to start MySQL and enable it to start automatically upon ECS startup:

systemctl start mysqld

systemctl enable mysqld

4. Run the following command to check the MySQL status:

systemctl status mysqld.service

[root@ecs-adc3 ~]# systemctl status mysqld.service

- mysqld.service MySQL Server
 - Loaded: loaded (/usr/lib/system/system/mysqld.service; enabled; vendor preset: disabled) Active: active (running) since Tue 2023-10-31 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.

5. Run the following commands to obtain the **root** user's password that is automatically set during MySQL installation:

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

Information similar to the following is displayed: 2023-10-31T11:53:08.691748Z 1 [Note] A temporary password is generated for root@localhost: 2YY? 3uHUA?Ys

6. Run the following command and follow the prompts 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 a new 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) : N #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 #Press Y to remove anonymous users. 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 #Press Y to disallow remote logins of user **root**. 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 #Press Y to delete the **test** database and remove access to it. - 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 #Press Y to reload privilege tables. Success.

All done!

Step 3 Install PHP.

 Run the following commands to install PHP 7 and required PHP extensions: 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-devel php70w.x86_64 php70w-cli.x86_64 php70wcommon.x86_64 php70w-gd.x86_64 php70w-ldap.x86_64 php70wmbstring.x86_64 php70w-mcrypt.x86_64 php70w-pdo.x86_64 php70wmysqlnd php70w-fpm php70w-opcache php70w-pecl-redis php70w-peclmongodb

2. Run the following command to check the version of the installed PHP:

php -v

Information similar to the following is displayed: 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 enable it to start automatically upon ECS startup:

systemctl start php-fpm

systemctl enable php-fpm

- **Step 4** Test the LAMP deployment.
 - 1. Create the **info.php** test file in /var/www/html/.
 - a. Run the following command to create and open the **info.php** test file: **vim /var/www/html/info.php**
 - b. Press **i** to enter insert mode.

 - d. Press **Esc** to exit insert mode. Then, enter **:wq** to save the settings and exit.
 - 2. Run the following command to restart Apache:

systemctl restart httpd

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

PHP Version 7.0.33	php
System	Linux ecs-maxiaorui-wx1058652-20231103 3.10.0-1160.92.1.el7.x86_64 #1 SMP Tue Jun 20 11:48:01 UT 2023 x86_64
Build Date	Dec 6 2018 22:31:47
Server API	Apache 2.0 Handler
/irtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
oaded Configuration File	/etc/php.ini
can 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/gd.ini, /etc/php.d/stif.ini, /etc/php.d/fileinfo.ini, /etc/php.d/fiplini, /etc/php.d/gd.ini, /etc/php.d/gdetatx.ini, /etc/php.d/mstring.ini, /etc/php.d/iconvini, /etc/php.d/igbinary.ini, /etc/php.d/gd.ini, /etc/php.d/gd.ini, /etc/php.d/mstring.ini, /etc/php.d/iconvript.ini, /etc/php.d/posito.ini, /etc/php.d/gd.ini, /etc/php.d/msqlnd, mysqlinini, /etc/php.d/opcache.ini, /etc/php.d/pod.ini, /etc/php.d/pd.gd.ini, /etc/php.d/msqlnd, mysqlinini, /etc/php.d/opcache.ini, /etc/php.d/pod.ini, /etc/php.d/gd.ini, /etc/php.d/shlmop.ini, /etc/php.d/spiniexml.ini, /etc/php.d/sockets.ini, /etc/php.d/redis.ini, /etc/php.d/sslmoj.ini, /etc/php.d/sysvesm.ini, /etc/php.d/sockets.ini, /etc/php.d/sklme3.ini, /etc/php.d/sklmi, /etc/php.d/xslmi, /etc/php.d/sysvesm.ini, /etc/php.d/sklme3.ini, /etc/php.d/sklmi, /etc/php.d/xslmi, /etc/php.d/xmlreader.ini, /etc/php.d/xmlwriter.ini, /etc/php.d/sklmi, /etc/php.d/zip.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
hread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
Pv6 Support	enabled
OTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.", string.rot13, string.toupper, string.tolower, string.strip_tags, convert.", consumed, dechunk, bzip2. convert.iconv.", mcrypt.", mdecrypt."

----End

4.3 Setting Up a Java Web Environment

4.3.1 Setting Up Tomcat-based Java Web Environment (CentOS 7.4)

Application Scenarios

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

The ECS in this chapter uses CentOS 7.4 64bit as OS.

Architecture

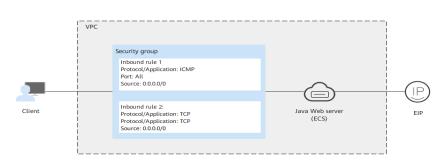


Figure 4-10 Setting up Tomcat-based Java web environment

Resource and Cost Planning

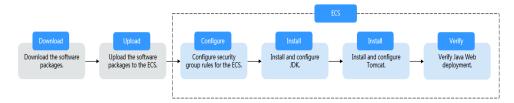
Resource	Description	Cost
VPC	VPC CIDR block: 192.168.0.0/16	Free
Subnet	AZ: AZ1CIDR block: 192.168.0.0/24	Free
Security group	 Inbound rule 1: Priority: Set it to 1. Action: Select Allow. Type: Select IPv4. Protocol & Port: Set it to ICMP: All. Source: Set it to 0.0.0.0/0. Inbound rule 2: Priority: Set it to 1. Action: Select Allow. Type: Select IPv4. Protocol & Port: Set it to TCP: 8080. Source: Set it to 0.0.0.0/0. 	Free

Resource	Description	Cost
ECS	 Billing mode: Yearly/ Monthly AZ: AZ1 Flavor: c7.large.2 Image: CentOS 7.4 64bit System disk: 40 GiB EIP: Auto assign EIP type: Dynamic BGP Billed by: Traffic Bandwidth: 5 Mbit/s 	The following resources generate costs: • ECSs • EVS disks • EIPs For billing details, see Billing Modes .
jdk	A Java development tool software. You can download it from: http://www.oracle.com/ technetwork/java/javase/ downloads	Free
tomcat	An open-source web application server. You can download it from: http://tomcat.apache.org/ download-80.cgi	Free
PuTTY	A cross-platform remote access tool, which is used to access various nodes from a Windows OS during software installation. You can download it from: https:// www.chiark.greenend.org.u k/~sgtatham/putty/ latest.html	Free
WinSCP	A file transfer across platform, which is used for transferring files between Windows and Linux systems. You can download it from: http://winscp.net/	Free

Table 4-11 lists the official paths to download JDK and Tomcat installation packages. You can also obtain the packages from open-source image paths.

Process

Figure 4-11 Deployment Process



Procedure

Preparations

- An ECS is created and has an EIP bound.
- The image source has been updated to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)? This facilitates obtaining and updating the system and software.
- The **jdk** and **tomcat** directories have been created on the ECS using the following commands:
 - cd /home/

mkdir webDemo

cd webDemo/

mkdir jdk

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 go to the **jdk** directory:

cd /home/webDemo/jdk

ii. Run 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 4-11** or from other open-source image paths.

For example, to check the available versions of the **jdk17** software package (**jdk-17_linux-x64_bin.tar.gz** used as an example), run the following command:

wget https://download.oracle.com/java/17/latest/jdk-17_linuxx64_bin.tar.gz

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

cd /home/webDemo/tomcat

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

Download the Tomcat installation package from the path listed in **Table 4-11** or from other open-source image paths.

wget http://mirrors.tuna.tsinghua.edu.cn/apache/tomcat/tomcatx/vx.x.xx/bin/apache-tomcat-x.x.xx.tar.gz

Find the required version from **the open-source image path**. The Tomcat installation package of version 8.5.xx is used as an example. Run the following commands to download the package:

wget https://mirrors.tuna.tsinghua.edu.cn/apache/tomcat/ tomcat-8/v8.5.xx/bin/apache-tomcat-8.5.xx.tar.gz --no-checkcertificate

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**.
- 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 traffic to an ECS is disabled by default, pinging the ECS EIP will time out. Add a rule to allow ICMP traffic to the ECS first.

Figure 4-12 Adding a rule to allow ICMP traffic

Add Inboun	dd Inbound Rule Learn more about security group configuration.								
1 Inbound n	1 Inbound rules allow incoming traffic to instances associated with the security group.								
Security Group d	lefault Jultiple rules in a bat	trh.							
Priority ⑦	Action	Protocol & Port ⑦	Туре	Source ?	Description	Operation			
1	Allow •	ICMP -	IPv4 v	IP address 0.0.0.0/0	• 	Operation 👻			
			🕀 Add Rule						
			ОК	Cancel					

b. Set an appropriate port. Port 8080 is used as an example here.

Figure 4-13 Adding port 8080

Add Inbound	d Rule Learn	more about security group	configuration.			
1 Inbound ru	ules allow incoming	traffic to instances associated v	vith the security gro	up.		
Security Group d	efault ultiple rules in a bat	sch.				
Priority 🕐	Action	Protocol & Port ?	Туре	Source ⑦	Description	Operation
1	Allow v	. TCP •	IPv4 v	IP address 0.0.0.0/0	•	Operation 👻
			🕀 Add Rule			
			ОК	Cancel		

Installing JDK

- Run the following command to go to the jdk directory: cd /home/webDemo/jdk
- 2. Run the following command to decompress the JDK installation package to the **jdk** directory:

tar -xvf jdk-17_linux-x64_bin.tar.gz -C /home/webDemo/jdk/

3. Run the following command to configure environment variables:

vim /etc/profile

```
4. Add the following content to the end of the file:

#set java environment

JAVA_HOME=/home/webDemo/jdk/jdk-17.0.x

JRE_HOME=$JAVA_HOME

PATH=$JAVA_HOME/bin:$PATH

CLASSPATH=::$JAVA_HOME/lib/dt.jar:$JRE_HOME/lib/tools.jar

export JAVA_HOME JRE_HOME PATH CLASSPATH
```

NOTE

In the preceding command, jdk-17.0.x indicates the version of the JDK installation package that is obtained from the command output in **2**.

Example value: jdk-17.0.9

5. Run the following command to save the settings and exit:

:wq

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

source /etc/profile

7. Run the following command to verify the installation.

java -version

If the following information is displayed, JDK is installed.

[root@ecs-c525-web ~]# java -version java version "17.0.9" 2023-10-17 LTS Java(TM) SE Runtime Environment (build 17.0.9+11-LTS-201) Java HotSpot(TM) 64-Bit Server VM (build 17.0.9+11-LTS-201, mixed mode, sharing)

Installing Tomcat

1. Run the following command to go to the **tomcat** directory:

cd /home/webDemo/tomcat

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

tar -xvf apache-tomcat-x.x.xx.tar.gz -C /home/webDemo/tomcat/

For example, to decompress the Tomcat installation package of version 8.5.*xx*, run the following commands:

tar -xvf apache-tomcat-8.5.xx.tar.gz -C /home/webDemo/tomcat/

3. Run the following commands to install Tomcat:

cd /home/webDemo/tomcat/apache-tomcat-x.x.xx/

cd bin/

For example, to install the Tomcat installation package of version 8.5.*xx*, run the following commands:

cd /home/webDemo/tomcat/apache-tomcat-8.5.xx/

cd bin/

4. Run the following command to edit the **setclasspath.sh** script:

vi setclasspath.sh

Add the following content to the end of the **setclasspath.sh** script:

```
Use the java version in Resource and Cost Planning to replace the JDK version in the following script:
export JAVA_HOME=/home/webDemo/jdk/jdk-17.0.9
export JRE_HOME=$JAVA_HOME
```

5. Run the following command to save the settings and exit:

:wq

6. Run the following command to start Tomcat:

./startup.sh

7. Run the following command to check the Tomcat process:

ps -ef | grep tomcat

If the following information is displayed, Tomcat is started successfully.

Figure 4-14 Checking the Tomcat process

[root@ccs]
root 8671 1 16 14:33 tty1 00:00:02 /home/webDemo/jdk/jdk-17.0.9/bin/java -Djava.util.logging.config.file=/home/webD
emo/tomcat/apache-tomcat-8.5.95/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djdk.
tls.ephemeralDHKeySize=2048 -Djava.protocol.handler.pkgs=org.apache.catalina.webresources -Dorg.apache.catalina.security.Securit
yListener.UMASK=0027 -Dignore.endorsed.dirs= -classpath /home/webDemo/tomcat/apache-tomcat-8.5.95/bin/bootstrap.jar:/home/webDem
o/tomeat/apache-tomeat-8.5.95/bin/tomeat-juli.jar -Deatalina.base=/home/webDemo/tomeat/apache-tomeat-8.5.95 -Deatalina.home=/hom
e/webDemo/tomcat/apache-tomcat-8.5.95 -Djava.io.tmpdir=/home/webDemo/tomcat/apache-tomcat-8.5.95/temp org.apache.catalina.startu
p.Bootstrap start
root 8710 7902 0 14:33 tty1 00:00:00 grepcolor=auto <mark>tomcat</mark>
[root@ccsbin]#

Verifying Java Web Deployment

Enter the following URL in the address bar of the browser:

http://EIP bound to the ECS:8080

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

Figure 4-15 Accessing port 8080

Home Documentat	ion Configuration	Examples Wik	i Mailing Lists			Find Help
Apache Tomcat/8.5.95						
	If you're seeing thi		essfully install	led Tomcat	. Congratulations!	Conver Status
Recommended Reading: Server Status Security Considerations How-To Manager Application How-To Clustering/Session Replication How-To Host Manager						
Developer Quick St Tomcat Setup First Web Application	tart <u>Realms & A</u> JDBC Datas		<u>Examples</u>		<u>Servlet Specifica</u> Tomcat Versions	
Managing Tomcal For security, access to the restricted. Users are defined \$CATALINA_HOME/conf/conear In Tomcat 8.5 access to 1 application is split between Read more Release Notes Changelog Migration Guide Security Notices	ne <u>manager webapp</u> is ned in: .t=users.xml the manager	Documenta Tomcat 8.5 Co Tomcat 8.5 Co Tomcat 8.5 Co Tomcat Wiki Find additional in information in: scataling_home/su Developers may Tomcat 8.5 Bug Dr Tomcat 8.5 JavaDr Tomcat 8.5 Git Res	Documentation ponfiguration mportant configuration MNILNG, txt be interested in: atabase Docs	'n	Getting Help FAQ and Mailing List The following mailing lists Important announce Important announcements vulnerability notifications. Important announcement Interset announceme	s are available: , releases, security (Low volume). 1 for <u>Apache Taplibs</u>
Other Downloads Tomcat Connectors Tomcat Native Taglibs Deplover	Other Documentati Tomcat Connectors mod .k Documentatior Tomcat Native Deployer	Overview	<u>/</u> Repositories	Miscellane <u>Contact Legal</u> <u>Sponsorship</u> <u>Thanks</u>	Found Who W	le Are le a Home

Copyright ©1999-2023 Apache Software Foundation. All Rights Reserved

4.3.2 Setting Up Tomcat-based Java Web Environment (Huawei Cloud EulerOS 2.0)

Introduction

Apache Tomcat (or simply Tomcat) is an open source web server and servlet container developed by the Apache Software Foundation. This tutorial describes how you can deploy Tomcat in HCE 2.0.

Preparations

- Prepare an ECS and assign a public IP address or EIP to the ECS.
- Ensure that inbound security group rules allow traffic to flow to the ECS over port 8080.

Procedure

Step 1 Install Tomcat.

- 1. Run the following command to install Java: dnf install java-1.8.0-openjdk
- 2. Run the following command to check whether the installation is successful: java -version

3. Run the following command to install Tomcat: dnf install tomcat

The Tomcat is installed in the **/usr/share/tomcat** directory.

Step 2 Configure Tomcat.

- 1. Add the following content to the **/etc/profile** file: JAVA_HOME=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.342.b07-0.hce2.x86_64/jre PATH=\$PATH:\$JAVA_HOME/bin CLASSPATH=::\$JAVA_HOME/lib/dt.jar:\$JAVA_HOME/lib/tools.jar export JAVA_HOME CLASSPATH PATH
- 2. Run the following command to activate the preceding environment variables: source /etc/profile
- 3. Clear the **/usr/share/tomcat/conf/server.xml** file and paste the following content:

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

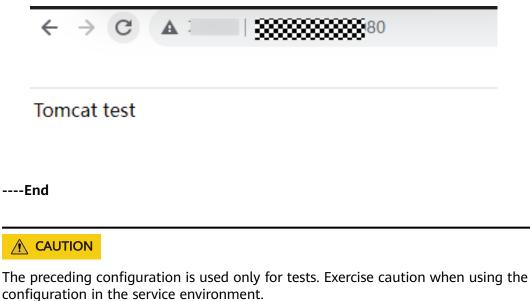
Save the settings and exit. You can customize the preceding configuration as required.

- Run the following command to create the directories specified by appbase and docbase in the preceding configuration: mkdir -p /data/wwwroot/default
- Run the following command to set tomcat as the owner of the preceding directory: chown -R tomcat.tomcat /data/wwwroot/
- 6. Create the **/usr/share/tomcat/bin/setenv.sh** file and enter the following information to set JVM memory parameters: JAVA_OPTS='-Djava.security.egd=file:/dev/./urandom -server -Xms256m -Xmx496m - Dfile.encoding=UTF-8'
- 7. Run the following command to start Tomcat: systemctl start tomcat
- 8. Run the following command to check the Tomcat status: systemctl status tomcat

If active (running) is displayed, Tomcat is started.

Step 3 Check whether Tomcat is installed.

1. Run the following command to create a test page: echo Tomcat test > /data/wwwroot/default/index.jsp Enter http://<Public IP address of the Tomcat service>:8080 in the address box of the browser. If the following page is displayed, the installation is successful.



4.4 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 runtime environment based on the Google Chrome V8 engine for building fast and scalable network applications. Based on the eventdriven 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

- An ECS has been created. For details, see Purchasing a Custom ECS.
- The target ECS has an EIP bound. For instructions about how to bind an EIP to an ECS, see Assigning an EIP.
- The image source has been updated to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)? This facilitates obtaining and updating the system and software.
- 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 the **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
- Run the following command to check 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**

D 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 go 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 open the **test.js** file: **vim test.js**
 - b. Press **i** to enter insert 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.
- c. Press **Esc** to exit insert mode. Then, enter **:wq** to save the settings and exit.
- 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 3000/tcp

6. Run the following command to run the project:

node ~/test.js

7. Enter **http://***EIP***.3000** in the address bar to access Node.js. If the following page is displayed, Node.js has been deployed.

Figure 4-16 Deployment and testing



----End

5 Setting Up a Website

5.1 Setting Up a WordPress Website

5.1.1 Setting Up a WordPress Website (Linux)

Application Scenarios

WordPress (WP for short) is initially a blog system and gradually evolved to a free CMS or website setup system. The best practices for ECS guide you through the setup of LNMP on a Linux ECS running the CentOS 7.2 64bit OS and deploy WordPress on the website.

Architecture

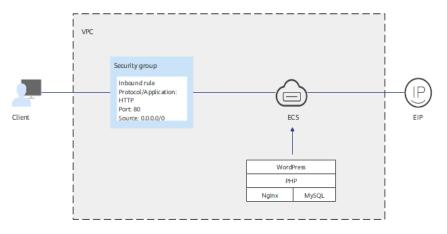


Figure 5-1 Setting up a WordPress website (Linux)

Advantages

- A website with a simple networking architecture can be quickly set up.
- The website is secure and easy to use.

Resources and Costs

Table 5-1	Resources	and	costs
-----------	-----------	-----	-------

Resource	Description	Cost
VPC	VPC CIDR block: 192.168.0.0/16	Free
VPC subnet	AZ: AZ1CIDR block: 192.168.0.0/24	Free
Security group	 Inbound rule: Priority: Set it to 1. Action: Select Allow. Type: Select IPv4. Protocol & Port: Set it to TCP: 80. Source: Set it to 0.0.0/0. 	Free
ECS	 Billing mode: Yearly/ Monthly AZ: AZ1 Flavor: s6.large.4 Image: CentOS 7.2 64bit System disk: 40 GiB EIP: Auto assign EIP type: Dynamic BGP Billed by: Traffic Bandwidth: 5 Mbit/s 	The following resources generate costs: • ECSs • EVS disks • EIPs For billing details, see Billing Modes .
Nginx	A high-performance HTTP and reverse proxy server. Download URL: http://nginx.org/packages/ centos/7/noarch/RPMS/ nginx-release- centos-7-0.el7.ngx.noarch.rp m	Free
MySQL	An open-source relational database software Download URL: https://dev.mysql.com/get/ mysql80-community- release-el7-11.noarch.rpm	Free

Resource	Description	Cost
РНР	An open-source software used for web development Download URL: https:// mirrors.huaweicloud.com/ remi/enterprise/remi- release-7.rpm	Free
WordPress	An open-source blogging software. Download URL: https://wordpress.org/ download/releases/	Free
Domain name	Used to access the created website.	The price of a domain name is subject to that provided by the domain name registrar. For details, see the help document of the domain name registrar.

Process

The process of manually setting up a WordPress website on a Linux ECS is as follows:

- 1. Set up the LNMP environment.
- 2. Create a database.
- 3. Install WordPress.
- 4. Purchase a domain name.
- 5. Configure DNS records.

Procedure

Preparations

- 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 **Table 5-2** has been added to the security group which the target ECS belongs to. For details, see **Configuring Security Group Rules**.

Table	5-2	Security	group	rules
-------	-----	----------	-------	-------

Directi on	Priori ty	Action	Туре	Protocol & Port	Source Address
Inboun d	1	Allow	IPv4	TCP: 80	0.0.0.0/0

 To obtain and update the system and software, you are advised to update the image source to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)?

Procedure

- **Step 1** Log in to the ECS.
- Step 2 Set up the LNMP environment. For details, see Manually Deploying LNMP (CentOS 7.2).

Step 3 Create a database.

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

mysql -u root -p

2. Run the following command to create a database:

CREATE DATABASE wordpress,

In the preceding command, *wordpress* is the database name, which can be customized.

3. Run the following command to create a user:

CREATE USER 'user'@'localhost' IDENTIFIED BY 'xxxxx';

In the preceding command, *user* is the name of the database user, and *xxxxx* is the configurable user password.

4. Run the following command to grant all permissions on the WordPress database to the user:

GRANT ALL PRIVILEGES ON wordpress.* TO 'user'@'localhost';

- Run the following command to make all configurations take effect: FLUSH PRIVILEGES;
- Run the following command to exit the MySQL CLI:
 exit

exit

7. (Optional) Run the following commands to verify the creation of the database and user and then exit the MySQL CLI:

mysql -u user -p

SHOW DATABASES;

exit

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

Step 4 Install WordPress.

1. Run the following commands to go to the root directory of the Nginx website and download the WordPress package:

cd /usr/share/nginx/html

wget https://cn.wordpress.org/wordpress-6.6.1-zh_CN.tar.gz

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

tar zxvf wordpress-6.6.1-zh_CN.tar.gz

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

3. Run the following commands to go to the WordPress installation directory, copy the **wp-config-sample.php** file to the **wp-config.php** file, and retain the original sample configuration file as a backup:

cd /usr/share/nginx/html/wordpress

cp wp-config-sample.php wp-config.php

- 4. Run the following command to open and edit the created configuration file: **vim wp-config.php**
- 5. Press **i** to enter insert mode. Find MySQL configurations in the file and modify them to information in **Step 3**.

Figure 5-2 Modifying MySQL configurations



- 6. Press **Esc** to exit the editing mode. Then, enter **:wq** to save the settings and exit the file.
- 7. Enter **http://***Server IP address***/wordpress** in the address bar of the browser to access the installation wizard.
- 8. Set the site title, administrator username, password, and email address. Then, click **Install WordPress**.

Table 5-3	Configuration	parameters
-----------	---------------	------------

Parameter	Description
Site title	Name of the WordPress website.

Parameter	Description	
Username	Name of the WordPress administrator.	
Password	Default or user-defined password. Do not reuse an existing password and keep you password secure.	
Email address	Email address for receiving notifications.	

- 9. Check that the installation is successful.
- 10. Click **Log In**. Alternatively, enter **http://***Server IP address***/wordpress/wp-login.php** in the address bar of the browser, enter the username or email address and password, and click **Log In**.
- **Step 5** Purchase a domain name.

Configure a unique domain name for website access. You need to obtain an authorized domain name from the domain name registrar first.

Step 6 Configure DNS records.

Your website can be visited using the registered domain name only after DNS records are configured. For details, see **Routing Internet Traffic to 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

5.2 Setting Up a Discuz Forum

5.2.1 Overview

Application Scenarios

This guide describes how you can build a website using HUAWEI CLOUD.

Small websites are often deployed on a single server, which handles requests from users, stores static and dynamic content, and processes data. As the number of website users increase, database access drastically increases, and a single server fails to meet the service requirements. In this case, two or more servers are required to run the website, and a load balancing service is also required to balance their loads.

To build a website (a forum is used as an example in this guide), the following requirements must be met:

- Database nodes and service nodes are deployed on different servers.
- The number of servers is dynamically adjusted as incoming traffic changes over time.
- Traffic is automatically distributed across multiple servers.

• The website must be licensed.

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

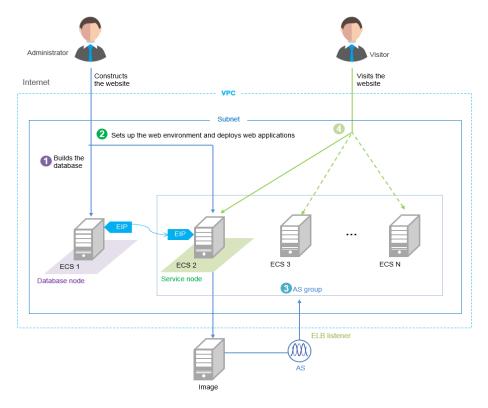
Solution

You can use the following solution to build a website.

Table 5-4 Solution de	etails
-----------------------	--------

Requirement	Solution	Service
Database nodes and service nodes are deployed on different servers.	 Building the website Buy two Elastic Cloud Servers (ECSs) to replace the physical server. One ECS works as the database node, and the other as the service node. Create a Virtual Private Cloud (VPC) to provide network resources for the two ECSs. Buy an Elastic Volume Service (EVS) disk for each ECS and attach it to each ECS as the data disk if required. 	ECS VPC (Optional) EVS
The number of servers is dynamically adjusted as incoming traffic changes over time.	Configuring features : Configure Auto Scaling (AS) policies 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
Traffic is automatically distributed across multiple servers.	Configuring features : Configure Elastic Load Balance (ELB) to automatically distribute the traffic across multiple servers, achieving better fault tolerance and expanding service capabilities for applications.	ELB

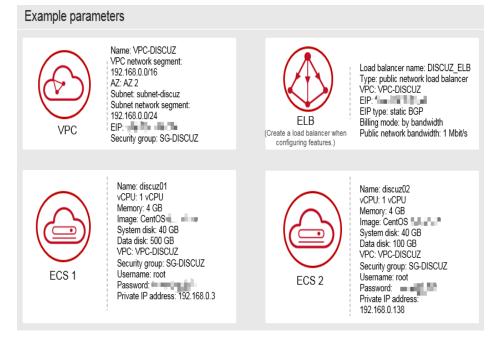
Logical Architecture



- 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 the traffic increases, AS adds ECSs created from the image of ECS 2 to the AS group.
- 4. Visitors access the website using the EIP of the load balancer, which automatically distributes traffic across multiple ECSs.

5.2.2 Requesting Cloud Resources

Required Cloud Resources



NOTE

Retain default settings for parameters not highlighted in the figures when creating or purchasing cloud resources and configuring features.

Applying for a VPC

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

Figure 5-3 Applying for a VPC

	👋 HUAWEI 💿	Console Ser	vice List ▼ Favorites
	Hello Account Balan \$5113.25		View Quota
	Computing ~ Elastic Cloud Server Auto Scaling Image Management Service	Volume Backup	Network Virtual Private Cloud Service Elastic Load Balance Service WPN
3	A Virtual Private Cloud (VPC) is a + Apply for VPC	a secure, isolated, log	ical network environment.

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

Figure 5-4 Configuring parameters

Basic Inform	ation
Regio 4	To change the region, use the region selector in the upper left corner of this page.
Name:	VPC-DISCUZ Enter the VPC name.
CIDR Block:	192.168.0 . / 16
Tag:	To comply with best practices, it is recommended that you use the predefined tag function provided by TMS to add tags to your resources. View Predefined Tag
	Enter a tag key. Enter a tag value
	You can add 9 more tags.
Subnet Setti	ngs
AZ: Subnet Name	Subnet-discuz
CIDR:	192.168.0.1 / [24]
Gateway:	192.168.0 .1
DNS Server A	Address 1: 100.125.1 .250
DNS Server /	Address 2: 114.114.114
	6
	I have read and agreed to the Huawei Virtual Private Cloud Service Agreement
	Create Now

Buying an EIP

	Elastic IP Address	0			2	Buy EIP
Network Console	You can create 5 mor	e EIPs.	All ~	EIP -	Q	Search by Tag 🛛 🔿
Dashboard Virtual Private Cloud	EIP/ID Status	Bound Private Type	Bandwidth Sh	Bandwidth Siz B	illing Mode Opera	tion
Security Group						
Network ACL						
Elastic IP						
Bandwidth VPC Peering						
VPN						
Direct Connect						
Apply for EIP @						
Specify E)etails		Confirm Order			Pay
1	,		2			3
Basic Information	on					
Region:	To char	ige the region, use the re	egion selector in the	e upper left corner o	of this page.	
Type:	3 Dynamic BG	P Static BGP	(?) Select	the billing mode:		
Billing Mode:	Yearly/Month	ly On-demand	Mont	thly/Yearly lemand		
Tag:		est practices, it is recom view Predefined Tag	mended that you u	se the predefined ta	ag function provided	by TMS to add tags to
	Enter a tag key	Enter a tag	g value.			
	You can add 9 m	ore tags.				

Bandwidth Settings	5
Select Bandwidth:	Allocate new Use existing
Bandwidth Name:	discuz_ip
Sharing Type:	Exclusive Shared
	The sharing type cannot be changed after being specified.
Charged By:	Traffic
	After specified, this parameter value cannot be changed.
Bandwidth Size (Mbit/s):	1Mbit/s
(4)	1 100 200 300
Quantity	
Quantity:	- 1 + You can create 2 more EIPs.To apply for a higher EIP quota, click Apply for Higher Quota
EIP Price \$0.01/hou	ur (5)
Public Network Traffic Pric	
The estimated price is for i	reference only and may vary from the final price in your bill Price Details
	01/hour Public Network Traffic Price \$0.15/GB
	for reference only and may vary from the final price in your bill. Price Details
	6
	■ I have read and agreed to the Huawei VPC Service Announcement
	Back Submit Order

Creating a Security Group and Adding Rules

\bigcirc	Security Group @		(2) + Create	e Security Group
Network Console	You can create 97 more security groups a	nd 4984 more security group	rules. N 🔻	QC
Virtual Private Cloud	Security Groups Name/ID	Description	Operation	
Security Group Network ACL Elastic IP Address Bandwidth VPC Peering		Create Sec * Name: 3	sg-discuz	×
VPN Direct Connect		٩	OK Cancel	/64_

Ø	Security Group	urity Group
Network Console	You can create 97 more security groups and 4984 more security group rules.	QC
Dashboard		
Virtual Private Cloud	Security Groups Name/ID Description Operation	
Security Group	SG-DISCUZ 233e23a0-07a3-4539-9b4d-92850 Fast Add Rule Add Rule More +	
Network ACL	×	
Elastic IP Address	Add Rule	
Bandwidth	* Transfer Direction: Inbound Outbound	
VPC Peering	* Protocol:	
VPN	* Protocol: CP After an access rule i security group, ECSs	
Direct Connect	* Port Range: 80 group are protected b	y the rule.
Select TCP f Range to 80.	for Protocol and set Port IP Address Security Group	
	SG-DISCUZ(233e 🔻	
	Cancel	

NOTE

Default security group rules 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**.

🧏 HUAWEI 💿	Console Ser	vice List 🔻 Favorites
Hello Account Balar \$5113.25		View Quota
Computing ~	Storage ~	Network ~
Elastic Cloud Server	Elastic Volume S	ervice 🖄 Virtual Private Cloud
Auto Scaling	Volume Backup	Service 📣 Elastic Load Balance
Image Management Servic	e 💮 Object Storage S	Service VPN
An Elastic Cloud Server (ECS) isolated environment.) is a virtual server th	hat runs in a secure and

2. Configure the parameters and submit your request.

Image:	Public Image Private Image	Shared Image	Select	t an image for the ECS.
	CentOS CentOS	bit(40GB) - C	;	
Disk:			ich an EVS disk f	or the ECS as a data disk.
	System Disk Common I/O - @ - 40 + GB 100-1,000 IOPS	Common I/O - 500 + GB 10	• 0 10-1,000 IOPS	Data Disk You can attach 22 more disks
)		51	ed VPC and secu	urity group.
VPC 🕜 :	VPC-DISCUZ *	View VPC C		
Security Group	SG-DISCUZ (Inbound:TCP/ × -	C Manage Security Grou	D Learn more abo	ut how to configure a security group

Figure 5-5 Basic configuration

Figure 5-6 Network configuration

Disk:			for the ECS as a data disk.
	System Disk Common I/O	Data Disk Common I/O • • • - 500 + GB 100-1,000 IOPS	Data Disk You can attach 22 more disks
VPC @ :	VPC-DISCUZ - M	Select the created VPC and sec	surity group.

	EIP 🛛 :	If you need to access the Internet from your ECSs, make a plan for the elastic IP addresses you need. Click here to view Elastic IP Addresses. Specify EIP Do Not Use Select the EIP you have obtained.			
		ECSs cannot be created in batches if an elastic IP address is specified.			
	C Current EIP Specifications: Static BGP Bandwidth: 1Mbit/s Charging Mode: By bandwidth				
	Login Mode: Password Key pair To reset the ECS password, you must install a plug-in on the ECS after it is created Learn more about how to install the plug-in. Item (install the plug-in)				
(11	Username: Password:	root Security Level: Low Keep your password secure. The system cannot detect your password.			
	Confirm Password:				
	ECS Name:	discuz01			
(12)		If you buy ECSs in batches, the system automatically adds a suffix to the ECS names, for example, my_ECS-0001.			
	Purchase Quantity:	- 1 + You can only create one ECS at a time if an EIP or a static NIC IP address is specified.			

Figure 5-7 Advanced settings

Figure 5-8 Confirming the configurations

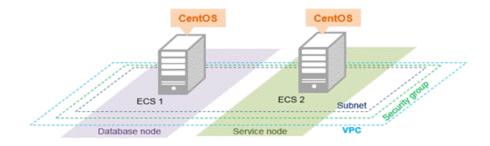
Price \$0.03/Hour	13 Buy Now
The estimated price is for reference only and may vary from the final price in your bill Price	ce Details
I have read and agreed to the Huawei	Elastic Cloud Server Agreement and Huawei Image Management Service Agreement Previous 15

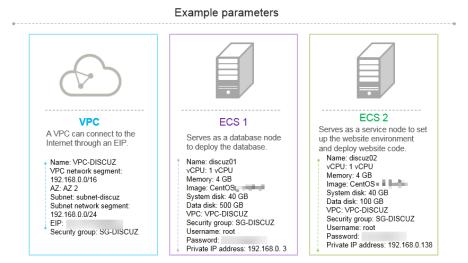
NOTE

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

5.2.3 Building the Website

Requested Cloud Resources





Building Process



Obtaining the Software

1. WinSCP

WinSCP is a free and open-source SFTP, FTP, WebDAV and SCP client for Microsoft Windows. It is mainly used to transfer files between a local and a remote computer in a secure manner. **Download the required version of WinSCP**.

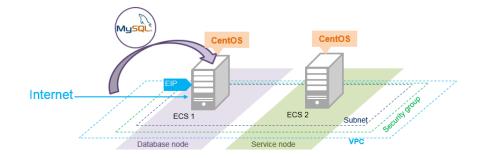
2. Discuz X3.5 (UTF-8)

Discuz X3.5 (UTF-8) is used to deploy website applications. Download the software package of the required version from the official website.

NOTE

- The recommended English version of Discuz X3.5 (UTF-8) is not free of charge. 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.

Building the Database



Install MySQL.

CentOS 7.2 is used as an example to describe how to install MySQL.

- 1. Log in to ECS **discuz01** remotely and enter the username and password.
- 2. Install MySQL.

wget -i -c http://dev.mysql.com/get/mysql57-community-releaseel7-10.noarch.rpm

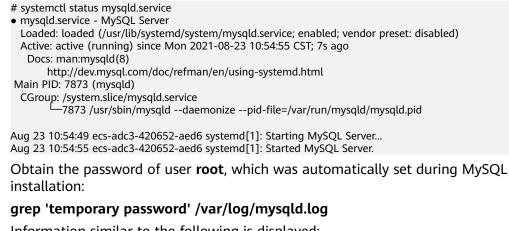
yum -y install mysql57-community-release-el7-10.noarch.rpm yum -y install mysql-community-server --nogpgcheck

Configure MySQL.

- 1. Start and enable MySQL.
 - systemctl start mysqld
 - systemctl enable mysqld
- 2. Query the running status of MySQL.

systemctl status mysqld.service

Information similar to the following is displayed:



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

4. Harden MySQL.

3.

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!

5. Enter the password of user **root** to log in to the database.

mysql -u root -p

6. Set the MySQL database as the default database.

use mysql;

7. Query the user list.

select host, user from user;

NOTE

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

- 8. Refresh the user list and allow all IP addresses to access the database. update user set host='%' where user='root' LIMIT 1;
- 9. Forcibly update the permissions to allow ECSs in the same subnet to access the MySQL database using private IP addresses.

flush privileges;

- 10. Exit the database. quit
- 11. Restart MySQL.

systemctl restart mysqld

12. Enable MySQL to automatically start upon system boot.

systemctl enable mysqld

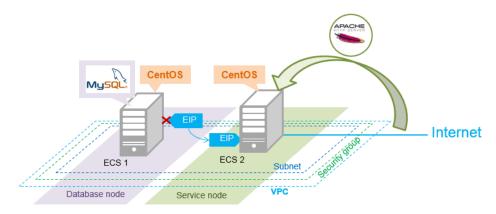
13. Disable the firewall.

systemctl stop firewalld.service

14. Check the firewall status.

systemctl status firewalld

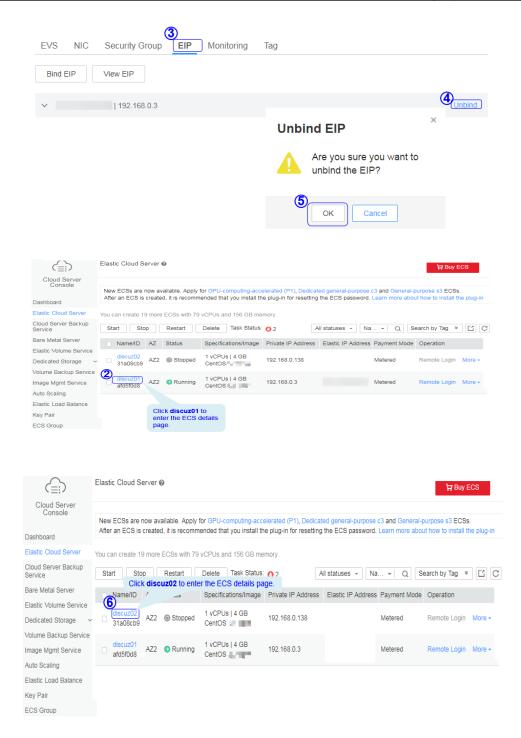
Setting Up the Web Environment



Install the web environment.

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

Start Stop	Restart	Delete	All statuses 👻	Name 👻	Q Search by Tag *
Task Status: 🚺 🤉					
Name/ID AZ	Status	Specifications/Image	Private IP Address	Elastic IP Address	Payment Mode Operation
discuz01 afd5f0d8 AZ2	Running	1 vCPUs 4 GB CentOS	192.168.0.3	-	Metered Remote Login More -
		Enter the username root , press Enter , an enter the password.	CENTUS	release (Fi 2.6.32-279.e16.	inal) x86_64 on an x86_64
			discuzØ)1 login: _	



- 2. Log in to ECS discuz02 remotely and enter the username and password.
- 3. Install MySQL.

wget -i -c http://dev.mysql.com/get/mysql57-community-releaseel7-10.noarch.rpm

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

4. Install the Apache HTTP Server (httpd), PHP FastCGI Process Manager (phpfpm), MySQL client (mysql), and MySQL server (mysql-server).

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

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

5. Reinstall the Apache HTTP Server (httpd), PHP FastCGI Process Manager (php-fpm), MySQL client (mysql), and MySQL server (mysql-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. Start httpd. service httpd start
- 2. Enable httpd to automatically start upon system boot. chkconfig httpd on
- 3. Start php-fpm.

service php-fpm start

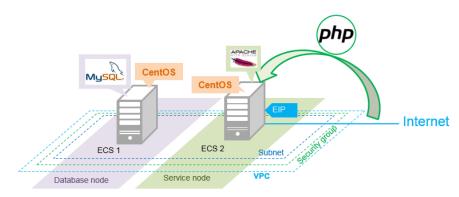
- Enable php-fpm to automatically start upon system boot.
 chkconfig php-fpm on
- Disable the firewall.
 systemctl stop firewalld.service
- Check the firewall status again.
 systemctl status firewalld
- 7. Start MySQL.

systemctl start mysqld

- 8. Enable MySQL to automatically start upon system boot. systemctl enable mysqld.service
- 9. Enter **http://***EIP* in a browser to query the default page of the ECS.



Deploying the Website Code



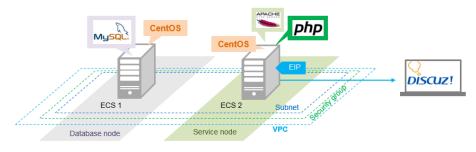
- 1. Decompress the Discuz_X3.5_SC_UTF8_20231001.zip package to the Discuz_X3.5_SC_UTF8_20231001 folder.
- Use WinSCP to upload the upload file in the Discuz_X3.5_SC_UTF8_20231001 folder to the /var/www/html directory on ECS discuz02. For details, see WinSCP documents.
- 3. Log in to **discuz02** and run the following command to grant the write permission to other users:

chmod -R 777 /var/www/html

- 4. Enter **http://***Elastic IP address* in the address bar of a browser. Follow the installation wizard to install Discuz.
 - The database address if the private IP address of **discuz01**.
 - The database password is the password of the database administrator's root account configured on **discuz01**.

Verifying the Website

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



5.2.4 Configuring Features

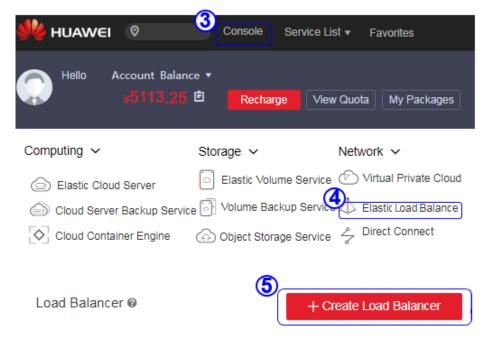
Unbinding the EIP

By default, you can use only one EIP. You can apply for more as needed. 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.

\bigcirc	Elastic IP Addre	SS 🛛					Apply for EIP	þ
Network Console Dashboard	You can create 18 r	nore EIPs.			All + EIP	Ŧ	Q	C
Virtual Private Cloud Security Group	EIP/ID	Status	Bound Private IP Address	Туре	Bandwidth Size (Mbi	t/s) Billing Mode	Operation	
Network ACL Elastic IP Address	9488617f-6a28-4	Bound	192.168.0.138	Static BGP		1 On-demand	Bind Unbind Re	elease
Bandwidth VPC Peering								
VPN Direct Connect								

Creating a Load Balancer

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



2. Specify the parameters and submit the application.

Create Load Balancer ⊚	
Specify Details	Confirm Specifications Finish
Basic Information Region: Asia Pacific-HongKong Name: DISCUZ_ELB	To change the region, use the region selector in the upper left corner of this page.
VPC: VPC-DISCUZ If no desired VPC is available	Select the VPC to which the load balancer belongs.
8	View Subnet C ual sting EIP View EIP C Use an existing EIP.
The estimated price is for reference only and may vary f	rom the final price in your bill. Price Details: I have read and agreed to the Huawel Elastic Load Balance Agreement Back Submit

Configuring the Load Balancer

		Load Balancer 🖲	9					+ Create Load E	Balancer
	Cloud Server Console	Load Balancer			balancer nam	e DISCUZ_E	LB to view t	he	
	Dashboard Elastic Cloud Server	You can create 9 mo		tails.			N •		QC
	Elastic Volume Service	Name/ID	Statue Public	: IP Address	Service IP Ad	dress ervice	Subnet	Operation	
	Volume Backup Service	DISCUZ_ELB 826fa0df8a92	Running				subnet-discu:	z Delete	
1	Auto Scaling 3	Add Listener Yo	u can add 10 more li:	steners.					
2		Name/ID	Status	LB Protoco	ol/Port	ECS Protoco	l/Port		

Add Listener		LB Protocol/Port: ELB provides two types of load balancing services (layer 4 (TCP) and layer 7 (HTTP) load balancing). Select TCP for Protocol, and set the port number to 80.						
Name:	discuz-listener	ECS Protoc	ECS Protocol/Port: specifies the protocol and port that ECSs use to provide					
LB Protocol/Port:	tocol/Port: TCP 80 The value ranges from 1 to 655		P is selected for Protoco	I, and port 80	is used.			
ECS Protocol/Port:	TCP - 80							
	The value ranges from 1 to 65	535.	Health Check Configurat	tion				
LB Mode 🔞 :	Round robin 👻		Check Mode:	TCP 👻	80			
Sticky Session:	\bigcirc	G	y	The value ra	nges from 1 to 65535.			
Stickiness Duration (min):	1 The value range	s from 1 to 60.	Interval (s) 🔞 :	2	The value ranges from 1 to 5.			
Description:			Timeout (s) 👩 :	5	The value ranges from 1 to 50.			
		0/128	Healthy Threshold @:	3	The value ranges from 1 to 10.			
 Interval (s): specifies the interval or value is 2. Timeout (s): specifies the maximum recommended value is 5. Healthy Threshold: specifies the r 	n timeout duration for one health	check. The	Linhealthy Threshold @:	3	The value ranges from 1 to 10.			
 Heating Intesticit, specifies the f checks necessary for an ECS to be is 3. Unhealthy Threshold: specifies th necessary for an ECS to be consid Success response time: 15 second Failure Response Time: 11 second 	e considered healthy. The recomme e number of consecutive failed he red unhealthy. The recommende (2 × 3 = 6)	ealth checks	6	ок с	ancel			

Creating Images

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

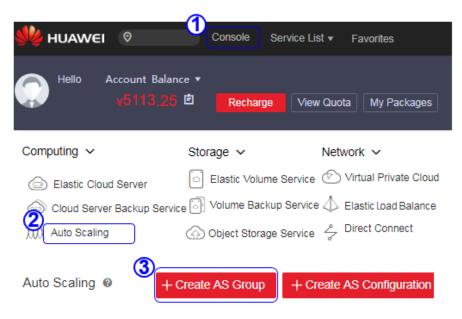
👋 HUAWEI 🛛 🔍	Console Se	ervice List 🔻 Favorites
Hello Account Bal		View Quota My Packages
Computing ~	Storage 🗸	Network 🗸
Elastic Cloud Server	Elastic Volume	Service 🕑 Virtual Private Cloud
Cloud Server Backup Se	ervice 🔄 Volume Backup	Service 📣 Elastic Load Balance
Cloud Container Engine	Object Storage	Service 🥜 Direct Connect
	Stop the ECS bef	ore creating an image.
Start Stop Rest	art Delete Task	: Status: 🙆 2
Name/ID AZ S	tatus Payment M	ode Operation
3 discuz02 AZ2 € 31a08cb9	Running Metered	Remote Login More -
afd5f0d8 AZ2	Stopped Metered	Remote Login More -

2. Configure the parameters and submit your request.

		Name/ID	AZ	Status	Specifications/Image	Private IP Address	Payment Mode	Operation	
		ivame/ID	AZ	Status	opecinications/image	Filvate in Address	Fayment Mode	5	
		discuz02 31a08cb9	AZ1	Stopped	1 vCPUs 4 GB CentOS	192.168.0.138	Metered	Remote Login More -)
		31400009			Centos				Modify Specifications
		discuz01	AZ1	Stopped	1 vCPUs 4 GB	192.168.0.3	Metered	Remote Login More -	Make Image 6
		afd5f0d8			CentOS				Reset Password
									Reinstall OS
_	Sou	rce:	ECS	Image Fi	le				Change OS
7		_]			Start
1	+ ECS	5. (discuz02			Select			Stop
									Restart
			ECS De	tails:					Delete
				discuz02					
				Disk: 40 GB					
			oystem	Disk. 40 00					
	-				(0			
_	Enci	ryption: U	nencrypte	ed 🕜		🛃 I have read and agr	eed to the Huawei Elasti	c Cloud Server Agreement	and System Image Disclaime
	Nam	ne:	discuz_c	entOS				Previous	Submit Application
8							1	(1)	
						Apply Now		-	
					(

Configuring AS

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



AS Group Name:	as-group-discuz	Specify Min. Instances, Expected Instances, and Max. Instances
(5) Min. Instances	0	J for the AS group. An AS group can have 0 to 50 ECSs. Expected Instances can be set to 2.
* Expected Instances	2	Select the VPC, subnet, and security group. Choose whether to
* Max. Instances	10	use ELB for health check and then select the load balancer if ELB is used for health check. Specify Health Check Method, Health Check Interval, and Instance Removal Policy.
Cooling Duration (s):	900	 ELB checks the health of ECSs in the selected security group every five minutes. The health check configuration has been set when the listener is
* AZ:	AZ2 × •	added for the selected load balancer. C © • Instances created and configured earlier are removed first.
OVPC:	VPC-DISCUZ(192.168.0.0/16) -	View VPC
* Subnet:	subnet-discuz(192.168.0.0/ × •	CO
* Security Group:	SG-DISCUZ (Inbound: - Outboun • Inbound: - Outbound: -	C Manage Security Group Learn more about how to configure a security group
* Load Balancing:	O Do not use O Use ULB View ULB (C 10
	Load Balancer: DISCUZ_E +	Listener: discuz-liste 👻
* Health Check Method:	ELB health check	- Ø
* Health Check Interval:	5 minutes	Y
* Instance Removal Policy:	Oldest instance created based on th	•
* Release EIP on Instance Removal:	C @ 8	
O Use Existing AS C		
You can select an exis Basic Informa		s c ^o nfiguration. You can also change the AS configuration of an existing AS group.
* Configuration Name:	as-config-discuz	
* Configuration Template:	Create a new specifications tem	plate Use specifications of an existing ECS
Specifications		
* ECS Type:	General-purpose Memory	optimized Disk-intensive GPU-acceleration
	First generation Second g	eneration Third generation
*vCPU:	1vCPUs 2vCPUs 4	CPUs 8vCPUs 16vCPUs 32vCPUs
* Memory:	1GB 2GB 4GB	
	Selected Specifications: s1.medium 1	I vCPUs 4 GB
Image Public Image		ect the private image I have created.
*Image:	discuz_centOS (40G) - C	

Elastic IP Address:	Do Not Use	Automatically Ass	sign 🕜		
	Automatically assigns insufficient, apply for a		hat exclusively uses bandwid	th. If you select this option,	check the EIP quota. If the quota is
Specifications:	Dynamic BGP	Static BGP	BGP(Discontinued)		
Charging Mode:	By bandwidth	By traffic			
1	Mbit/s				
Bandwidth:	· · · · ·				1 Mbit/s
	1		50	100	
.ogin	(12)				
Login Mode:	Key Pair	Account Password			
Username:	root				
Account Password:		Security Level	Keep your p	assword secure. The system	n cannot retrieve your password. 🥥
Confirm Password:			14_		
	13			I have read and agreed i	to the Huawei Autoscaling Service Agre
	Next A	pply Now	_		

2. Configure AS policies.

Name	Status	AS Configuration	Current Insta	Expected Instan	Min. Instances	Max. Instances Operation	
as-group-discuz	Enabled	as-config-discuz	0	1	1	10 View AS Po	Disable More -
Monitoring Ins	2 tance AS Pol	icy Notification	Tag Lifecycle Ho	юk			
Add AS Policy	You can add 1	0 more policies.					

	Add Policy	×
	* Policy Name:	as-policy-discuz-cpu
	* Policy Type:	Alarm Scheduled Periodic CPU alarm policy: When the CPU usage exceeds 70% for three
	* Alarm:	Create Alarm Rule
	* Alarm Name:	as-alarm-cpu
6	* Trigger Condition:	CPU Us ▼ Max. ▼ > ▼ 70 %
	* Monitoring Interval:	5 minutes 👻
	* Consecutive Occurrences:	3
	Scaling Action:	Add 👻 1 instan 👻
	Cooling Duration (s):	900
		OK Cancel

Add Policy

Policy Type	Alarm	Sch	eduled		Perio	dic	
Alarm	Create Alarm	Rule	٠				
Alarm Name	as-alarm-cpu-	02					
Trigger Condition	ODUUT	-		-			10
 Trigger Condition 	CPU Usage To check wheth Outcoming Rate different OSs, se	e, or Inba	and Inco	oming	Rate ar	e sup	portec
Monitoring Interval	To check wheth Outcoming Rate	e, or Inba	toring n and Inco	oming	Memo Rate ar	e sup	age, In portec
	To check wheth Outcoming Rate different OSs, se	e, or Inba	toring n and Inco astic C	oming	Memo Rate ar	e sup	age, In portec
Monitoring Interval	To check wheth Outcoming Rate different OSs, so 5 minutes	e, or Inba	toring n and Inco astic C	oming I loud Se	Memo Rate ar	e sup	age, In porte

3. Add AS instances.

				Start ECS			0	
				Are you sur	e you want to star	t the fo	llowing ECSs?	
	Cloud Server Console			Name	Status	Expire	At	
	Dashboard			discuz02	Stopped			
0	Elastic Cloud Server	ECSs before ad	ding them to the	4	OK Cance	əl	Dashboard	
3	AS group		Tanlı Olaharı 🙆 a				Elastic Cloud Server	
	Start Stop Restart	Delete 1	fask Status: 🙆 2				Cloud Server Backup	Service
	Name/ID	AZ	Status				Bare Metal Server	
2	discuz02 31a08cb9-f2fc-4727-8a5	AZ2	Stopped				Elastic Volume Servi Dedicated Storage	ce ~
	discuz01 afd5f0d8-d933-4395-a27	AZ2	Stopped			G	Volume Backup Serv Image Mgmt Service	
						G	Auto Scaling	

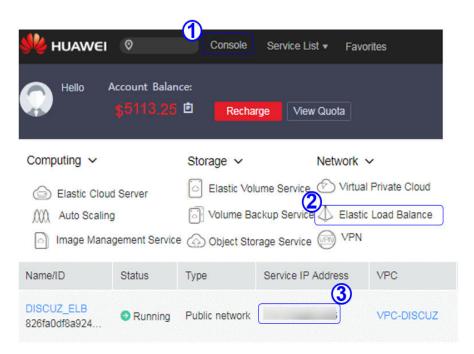
Name	Status	AS Configuration	Current Insta	Expected Instan	Min. Instances	Max. Instances	Operation	
as-group-discuz	Enabled	as-config-discuz	0	1	1	6	View AS Policy Disable	More •
Monitoring Ins 8 Add Remo	AS P AS P Remo		Tag Lifecy More∙ Ø	cle Hook				
Add						×		
Max. Instanc	es in a Batch: 10							
Available Inst	tances: En	ter a name.	Q C Selec	ted Instances:				
9 Nan	ne	ID	Nar	ne	ID	Opera		
disc	uz02	31a08cb9-f2fc-472	7-8a5 disc	uz02	31a08cb9-f2fc-472	Delete		
		10						
		Ĭ	OK Can	cel				

4. Modify AS policies.

¥5113.2	5 🖻 Rechar	ge View Quota	My Packages			
mputing 🗸	Storage 🗸	Network				
Elastic Cloud Server		ime Service 🕐 Virtu				
Cloud Server Backup Ser		ckup Service 📣 Elas				
() Auto Scaling	Object Stora	age Service 🥜 Direc	ct Connect			
e Status	AS Configuration	Current Instances	Expected Instances	Min. Instances	Max. Instances	Operation
oup-discuz 🕑 Enabled	as-config-discuz	0	2	1	10	View AS Policy Disable
					(4)	Change AS Configuration
Modify AS Grove * AS Group Name: * Min. Instances: * Expected Instances: * Max. Instances:	a					footify few Details Delete
* AS Group Name: * Min. Instances: * Expected Instances:	1	2			nces to 1 to en	footify few Details Delete
* AS Group Name: * Min. Instances: * Expected Instances: * Max. Instances:	a 1 2 1 9	0			nces to 1 to en	footify few Details Delete
* AS Group Name: * Min. Instances: * Expected Instances: * Max. Instances: Cooling Duration (s):	1 2 1 9 ¢. E	0			nces to 1 to en	footify few Details Delete
* AS Group Name: * Min. Instances: * Expected Instances: * Max. Instances: Cooling Duration (s): * Health Check Method	1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	0 0 ELB health check			nces to 1 to en	footify few Details Delete
* AS Group Name: * Min. Instances: * Expected Instances: * Max. Instances: Cooling Duration (s): * Health Check Interva	a 1 2 1 9 4: E 1: 5 1: 5 1: 5	0 00 ELB health check i minutes			nces to 1 to en	footify few Details Delete

Verifying the Configuration

Obtain the EIP of the load balancer. 1.



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**.

5.2.5 Visiting the Website

Filing the Website

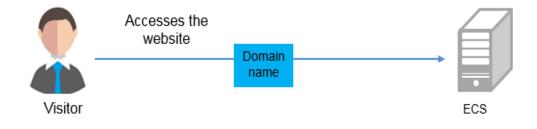
According to national regulations, if the servers used to deploy the website are located in the Chinese mainland, Internet Content Provider (ICP) licensing is required. The domain name that is not licensed cannot be used to access the website.

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.



5.3 Setting Up a Magento E-Commerce Website

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

Overview

The section guides you through the manual 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 is suitable for building medium- and large-sized sites. Magento is written in PHP and employs the MySQL database management system for data storage.

Prerequisites

- You have purchased an ECS and bound an EIP to it.
- The rules listed in the following table have been added to the security group which the target ECS belongs to. For details, see Adding a Security Group Rule.

Directi on	Priori ty	Action	Туре	Protocol & Port	Source Address
Inboun d	1	Allow	IPv4	TCP: 22	IP address of the client that is allowed to remotely connect to Linux ECSs using SSH. If the source IP is set to 0.0.0.0/0 , access from all IP addresses is allowed. For security purposes, 0.0.0.0/0 is not recommended.
Inboun d	1	Allow	IPv4	TCP: 80	IP address of the client that is allowed to access Magento. If the source IP is set to 0.0.0/0 , access from all IP addresses is allowed.

Table 5-5 Security group rules

Directi on	Priori ty	Action	Туре	Protocol & Port	Source Address
Inboun d	1	Allow	IPv4	TCP : 3306	IP address of the client that is allowed to remotely access MySQL databases. If the source IP is set to 0.0.0.0/0 , access from all IP addresses is allowed. For security purposes, 0.0.0.0/0 is not recommended.

Resource Planning

Table 5-6 lists the resource configuration and software versions used in this practice. The commands and parameters may vary according to the hardware specifications or software versions you would use.

Table 5-6	Resource	plannin	g

Resource	Туре	Specification/Version
ECS configuration	Flavor	c6s.large.2
	vCPUs	2 vCPUs
	Memory	4 GiB
	OS	CentOS 7.2
Software resources	Apache	2.4.6
	MySQL	5.7 Download URL: http:// dev.mysql.com/get/ mysql57-community- release- el7-8.noarch.rpm
	PHP	7.0.33 Download URL: https:// mirror.webtatic.com/yu m/el7/webtatic- release.rpm

Resource	Туре	Specification/Version
	Composer	1.10.19
		Download URL:
		https:// getcomposer.org/ installer
	Magento	2.1.0
		Download URL:
		https://github.com/ magento/magento2.git

To make sure that the website works properly, use an ECS whose memory is 2 GiB or higher.

Step 1: Install and Configure Apache

- Step 1 Remotely log in to the ECS by referring to Logging In to a Linux ECS.
- Step 2 The image source has been updated to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)? This facilitates obtaining and updating the system and software.
- **Step 3** Run the following commands as user **root** to update the software package and install Apache:

yum -y update yum -y install httpd

If an error message is displayed, indicating that the domain name cannot be resolved, add a DNS server to the **/etc/resolv.conf** file.

Step 4 Open the Apache configuration file.

vim /etc/httpd/conf/httpd.conf

NOTE

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

- **Step 5** Press **i** to enter insert mode and modify the file as follows:
 - Change AllowOverride None to AllowOverride all.

0)	ptions Indexes FollowSymLinks
	AllowOverride controls what directives may be placed in .htaccess files. It can be "All", "None", or any combination of the keywords: Options FileInfo AuthConfig Limit
Ĥ	llowOverride None

• Add the following parameters to the end of the configuration file: LoadModule rewrite_module modules/mod_rewrite.so # Load config files in the "/etc/httpd/conf.d" directory, if any. IncludeOptional conf.d/*.conf

LoadModule rewrite_module modules/mod_rewrite.so

- Step 6 Press Esc to exit insert mode. Then, enter :wq to save the settings and exit.
- Step 7 Run the following commands in sequence to start Apache and enable it to start automatically upon ECS startup: systemctl start httpd systemctl enable httpd

```
----End
```

Step 2: Install and Configure MySQL

- **Step 1** Run the following command as the **root** user to add a yum repository: rpm -Uvh http://dev.mysql.com/get/mysql57-community-release-el7-8.noarch.rpm
- **Step 2** Run the following command to Install MySQL: yum -y install mysql-community-server --nogpgcheck
- **Step 3** Run the following commands in sequence to start MySQL and enable it to start automatically upon ECS startup: systemctl start mysqld systemctl enable mysqld
- **Step 4** Run the following command to obtain the **root** user's password that is automatically set during MySQL installation: grep 'temporary password' /var/log/mysgld.log

Information similar to the following is displayed, in which **(n?K7jP#cirM** is the temporary password. 2019-05-09T11:29:42.365419Z 1 [Note] A temporary password is generated for root@localhost: **(n? K7jP#cirM**

Step 5 Run the following command to harden MySQL:

mysql_secure_installation

Perform operations as prompted.

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 a new password for 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 #Press Y to change the password of user **root**.

New password: #Enter a new password that consists of 8 to 30 characters, including letters, digits, and special characters (`~!@#\$%^&*-+=|(){[]:;'<>,.?/). 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 #Press Y to remove anonymous users. 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 #Press Y to disallow remote logins of user **root**. 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 #Press Y to delete the **test** database and remove access to it. - 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 #Press Y to reload privilege tables. Success.

All done!

Step 6 Log in to the MySQL database as the **root** user.

mysql -u root -p

- **Step 7** Run the following command to create a database named **magento**. CREATE DATABASE *magento*;
- **Step 8** Run the following command to create a user for the database and assign full permissions to the user:

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

In this command, **magento** is the name of the database created in the previous step, **magentouser** is the name of the database user, and **xxxxx** is the password of the database user.

- **Step 9** Run the following command to exit the MySQL CLI: exit
- **Step 10** (Optional) Perform the following operations to check whether the database and account have been created and then exit the MySQL CLI:
 - Run the following command to log in to the MySQL CLI as user magentouser: mysql -u magentouser -p
 - 2. Run the following command to view the created database: SHOW DATABASES;

In the displayed information, magento is the newly created database.

++
Database
++
information_schema
magento
++
2 rows in set (0.00 sec)

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

----End

Step 3: Install and Configure PHP

Step 1 Run the following command to add the IUS and EPEL repositories:

yum install \ https://repo.ius.io/ius-release-el7.rpm \ https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm

- **Step 2** Run the following command to add a webtatic repository: rpm -Uvh https://mirror.webtatic.com/yum/el7/webtatic-release.rpm
- **Step 3** Run the following command to install PHP7 and required PHP extensions for Magento:

yum -y install php70w php70w-pdo php70w-mysqlnd php70w-opcache php70w-xml php70w-gd php70wmcrypt php70w-devel php70w-intl php70w-mbstring php70w-bcmath php70w-json php70w-iconv

Step 4 Run the following command to check the version of the installed PHP: php -v

Information similar to the following is displayed:

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

- **Step 5** Run the following command to open the PHP configuration file **php.ini**: vim /etc/php.ini
- Step 6 Press i to enter insert mode and modify the file as follows:
 - Set memory_limit to a proper value.

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

• Uncomment and set **date.timezone**.



- Step 7 Press Esc to exit insert mode. Then, enter :wq to save the settings and exit.
- **Step 8** Run the following command to restart the web service process: systemctl restart httpd

----End

Step 4: Install Composer

Composer is a package manager for the PHP programming language that provides a standard format for managing dependencies of PHP software and required libraries. **Step 1** Install composer 1.*x* for the dependency of Magento 2.

Run the following commands to install the Composer of the specified version and set the installation path to **/usr/bin/** for global use: php -r "copy('https://getcomposer.org/installer', 'composer-setup.php');" php composer-setup.php --install-dir=**/usr/bin/** --filename=composer --**version=1.10.19**

The command output is as follows:

All settings correct for using Composer Downloading...

Composer (version 1.10.19) successfully installed to: /usr/bin/composer Use it: php /usr/bin/composer

Step 2 Run the following command to check whether the Composer is successfully installed:

composer -v

The command output is as follows:

`_V_V_V_/_V /_/ /_/ /_/ .___/___/___/__/_/ 11

Composer version 1.10.19 2020-12-04 09:14:16

----End

Step 5: Install Magento

When installing Magento, you can determine whether to install sample data. If Magento is only used for testing, it is optional for you to install sample data. If Magento is used in production environments, you are advised to perform initial configuration instead of installing sample data.

- **Step 1** Run the following command to install git: yum -y install git
- **Step 2** Run the following commands to go to the default root directory **/var/www/html/** of the web server and use git to download Magento: cd /var/www/html/

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

Step 3 Switch Magento to a stable version.

By default, Magento of the latest version is installed. In the production environment, you are advised to switch to a stable version.

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

The command output is as follows:

Switched to a new branch '2.1.0'

Step 4 Run the following command to move the installation file to the root directory /var/www/html/ of the web server. /var/www/html/magento2/ is the directory where Magento is installed.
Short is detailed nulleigh %% my /uar/www/html/magento2/* /uar/www/html/ %% sd

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

Then, you can access the Magento site from **http://magento server IP address**. If you do not move the installation file to the root directory, you can access the Magento site only from **http://magento server IP address/magento2**.

Step 5 Run the following commands to set file permissions for Magento:

chown -R apache: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

- **Step 6** Run the following command to install unzip and zip. yum install -y unzip zip
- Step 7 Run the following commands to go to the default root directory /var/www/html/ of the web server and use Composer to install Magento: cd /var/www/html/ composer install
- **Step 8** After the installation is complete, enter **http://magento server IP address** in the address bar of a browser to visit Magento. If the following page is displayed, Magento is installed successfully.



Version 2.1.0

Welcome to Magento Admin, your online store headquarters. Click 'Agree and Set Up Magento' or read Getting Started to learn more.

Terms & Agreement

Agree and Setup Magento

----End

Step 6: Configure Magento

- **Step 1** Visit **http://magento server IP address** and click **Agree and Setup Magento** to start the configuration.
- **Step 2** Click **Start Readiness Check** to check the environment. After the check is passed, click **Next**.

Û							
O Readiness Check	2 Add a Database	3 Web Configuration	4 Customize Your Store	5 Create Admin Account	6 Install	Back	
Step 1: Readiness Check							
Let's check your environment for the correct PHP version, PHP extensions, file permissions and compatibility.							

|--|

Step 3 Enter the MySQL database user magentouser, the password of the database user, and the database magento created in Step 2: Install and Configure MySQL, and click Next.

Step 2: Add a Database

Database Server Host 🖈	localhost
Database Server Username 🔺	magentouser
Database Server Password	•••••
Database Name 🔸	magento
Table prefix	(optional)

Step 4 Set the website access address and background management address, and click **Next**.

Step 3: Web Configuratio	n	
Your Store Address	http://124.	
Magento Admin Address ★	http://124.	admin_1pj83g

NOTE

The background management address can be customized.

Step 5 Set the time zone and language, and click **Next**.

Step 4: Customize Your Store

Store Default Time Zone *	GMT (UTC)	•
Store Default Currency 🔸	Chinese Yuan (CNY)	•
Store Default Language *	Chinese (China)	•

Step 6 Set the admin account and click **Next**.

Step 5: Create Admin Account

Create a new Admin account to manage your store.

New Username 🔸	admin
New Email 🔸	endedes op gestime
New Password 🔸	•••••
Confirm Password	•••••

Step 7 Click **Install Now** and wait until the installation is complete.

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



Please keep this information for your records:

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

Encryption Key:

here a substance of a particular property of the

Database Info:

Database Name:	magento
Username:	magentouser

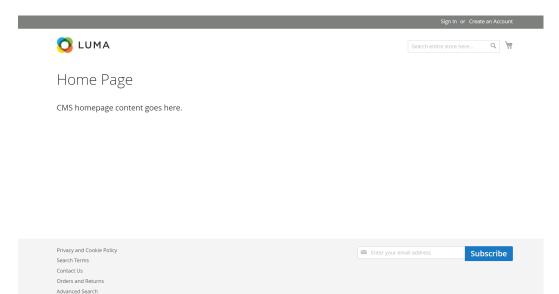
- **Step 8** Log in to the Magento server and set up cron jobs. crontab -u apache -e
- **Step 9** Press **i** to enter insert mode and add the following content:

*/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

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

For more information about running Magento cron jobs, see **Magento Documentation**.

Step 10 Enter **http://magento server IP address** in the address bar of a browser. The following page is displayed by default.



Step 11 Enter **http://magento background management address** in the address bar of a browser and use the admin account to log in. After the login is successful, the following page is displayed.

Ŵ	Dashboard			Q	🌲 上 admir	n 🔻
dashboard	Store View: All Store Views -				Reload Data	
SALES PRODUCTS	Lifetime Sales Chart is disabled. To enable the chart, click here. CN¥0.00 Revenue Tax Shipping Quantity					
CUSTOMERS	Average Order CN¥0.00	CN¥0.00		CN¥0.00	0	
	Last Orders We couldn't find any records.	Bestsellers	Most Viewed Products	New Customers	Customers	
CONTENT REPORTS	Last Search Terms We couldn't find any records.	We couldn't find	any records.			

NOTE

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

For more information about Magento configuration, see **Magento Documentation**.

----End

Step 7: Other Operations

Step 1 Purchase a domain name.

Configure a unique domain name for website access. You need to obtain an authorized domain name from the domain name registrar first.

Step 2 Configure DNS records.

Your website can be visited using the registered domain name only after DNS records are configured. For details, see **Routing Internet Traffic to 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

5.4 Manually Deploying a Ghost Blog (Ubuntu 20.04)

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 20.04.

Creating a User

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

1. Run the following command to create a user: The following uses **user** as an example.

adduser user

The following information is displayed:

```
Adding user `user' ...
Adding new group `user' (1000) ...
Adding new user 'user' (1000) with group 'user' ...
Creating home directory `/home/user' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user
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] Y
```

- a. In the **New password:** and **Retype new password:** lines, enter and confirm the user password (not displayed by default) as prompted, and press **Enter**.
- b. In the **Enter the new value, or press ENTER for the default** line, press **Enter** to retain the default settings. You can also specify the information as needed.
- c. In the **Is the information correct? [Y/n]** line, press **Y** to confirm the information and press **Enter** to complete the settings.
- 2. Run the following command to add the newly created user to the user group: **usermod -aG sudo user**
- 3. Run the following command to switch to user:

su - user

Installing Nginx

Before deploying the Ghost blog, you need to install Nginx and use it as an HTTP server. The following uses Nginx 1.18.0 as an example.

1. Run the following commands to update the Linux OS and software package:

sudo apt-get update

sudo apt-get upgrade -y

2. Run the following command to install Nginx:

sudo apt-get install -y nginx

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

nginx -v

The following information is displayed: nginx version: nginx/1.18.0 (Ubuntu)

4. (Optional) Configure the firewall.

Uncomplicated Firewall (UFW) is an iptables interface that simplifies the firewall configuration. By default, Ubuntu has UFW installed. 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 distribute TLS/SSL-encrypted traffic.
- **Nginx HTTP**: Port 80 is enabled to distribute normal and unencrypted web traffic.
- **Nginx HTTPS**: Port 443 is enabled to distribute TLS/SSL-encrypted traffic.

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

sudo ufw allow 'Nginx Full'

5. 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://***IP* address of the Nginx server in the address bar to access Nginx. If the following page is displayed, Nginx has been installed.

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to <u>nginx.org</u>. Commercial support is available at <u>nginx.com</u>.

Thank you for using nginx.

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. Run the following command to install MySQL:

sudo apt-get install -y mysql-server

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

mysql -V

The following information is displayed: mysql Ver 8.0.37-0ubuntu0.20.04.3 for Linux on x86_64 ((Ubuntu))

3. Run the following command to access MySQL:

sudo mysql

- Create a database for Ghost. The following uses ghost_data as an example.
 CREATE DATABASE ghost_data;
- 5. Run the following commands to set the password for user **root**:

ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'xxxxx';

In the preceding command, *xxxxx* indicates the password you set for user **root**.

6. Run the following command to reload the privilege tables of MySQL to check that the change takes effect:

FLUSH PRIVILEGES;

 Run the following command to exit MySQL: exit

Installing Node.js

- Run the following commands to install Node.js: sudo curl -sL https://deb.nodesource.com/setup_18.x | sudo -E bash sudo apt-get install -y nodejs
- 2. Run the following commands to view the versions of Node.js and Node Package Manager (npm), respectively:

node -v

npm -v

The following information is displayed: root@ecs-c47c:~# node -v v18.20.3 root@ecs-c47c:~# npm -v 10.7.0

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 install ghost-cli@latest -g

 Create a folder named ghost under /var/www/. sudo mkdir -p /var/www/ghost

NOTE

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

 Run the following command to grant user permissions to ghost: sudo chown user:user /var/www/ghost sudo chmod 775 /var/www/ghost

NOTE

user is created in step **1**.

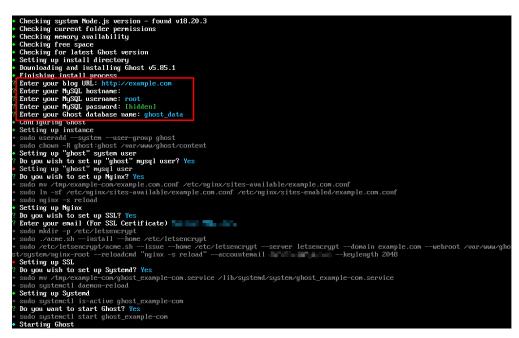
- Run the following command to switch to the created folder: cd /var/www/ghost
- 5. Run the following command to install Ghost using Ghost-CLI: **ghost install**

D 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 **/var/www/ghost/**, follow the prompts to configure related parameters.



- Enter your blog URL: Enter a resolved domain name, for example, http:// example.com.
- Enter your MySQL hostname: Enter the database connection address. In this example, the MySQL database and Ghost are deployed on the same ECS. Press Enter to retain the default settings.
- **Enter your MySQL username**: Enter the database username **root** and press **Enter**.
- Enter your MySQL password: Enter the database password set in step 5 and press Enter.
- **Enter your Ghost database name**: Enter the name of the database used by Ghost. Enter **ghost_data** and press **Enter**.

To modify the configuration, run the following command:

vi config.production.json

The following example is for your reference.



Verifying Blog Access

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

6 Setting Up an Application

6.1 Setting Up an FTP Site

6.1.1 Setting Up an FTP Site (Windows 2012)

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.

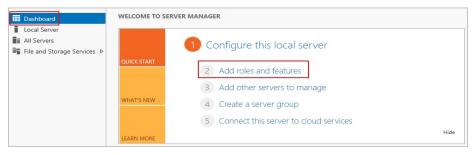
The process is as follows:

- 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**.

B	Add Roles and Features Wizard				
Select installatio	n type destination server ecs-7306				
Before You Begin	Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).				
Installation Type Server Selection	Role-based or feature-based installation Configure a single server by adding roles, role services, and features.				
Server Roles Features Confirmation Results	 Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment. 				
	< Previous Next > Install Cancel				

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

Add Roles and Features Wizard					
Select destination	on server			DESTINATION SERVER ecs-7306	
Before You Begin Installation Type Server Selection		from the server pool	n to install roles and features.		
Server Roles	Server Pool				
Features]	
Confirmation	Filter:				
Results	Name	IP Address	Operating System		
	ecs-7306		Microsoft Windows Server 201	12 R2 Standard	
	Add Servers comr	ervers that are running Wi	ndows Server 2012, and that have ffline servers and newly-added ser		
		< Pr	evious Next >	Install Cancel	

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

P	Add Roles and Features Wizard	_ _ ×
Select server roles Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	Select one or more roles to install on the selected server. Roles Application Server DHCP Server SAX Server Fax Server Fax Server Fat Server File and Storage Services (1 of 12 installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Access Remote Desktop Services Volume Activation Services Windows Deployment Services Windows Server Essentials Experience	DESTINATION SERVER ecs-7306 Description Meb Server (IIS) provides a reliable, mangeable, and scalable Web application infrastructure.
Add	Windows Server Update Services Previous Roles and Features Wizard	Vext > Install Cancel
The following tools at have to be installed of Web Server (IIS) A Management		

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

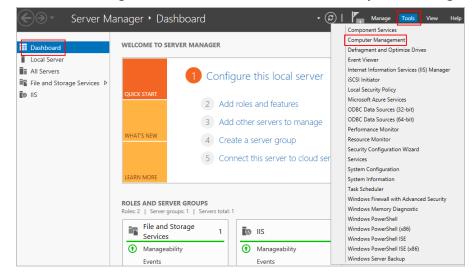
Select role servi	ces	DESTINATION SERVER ecs-7300
Before You Begin Installation Type	Select the role services to install for Web Server (IIS)	Description
Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	Digest Authentication Digest Authentication IIS Client Certificate Mapping Authenticatio IP and Domain Restrictions URL Authorization Windows Authentication Application Development FTP Server FTP Server FTP Service FTP Service FTP Service FTP Service IIS 6 Management Console IIS 6 Management Scripts and Tools Management Service Kanagement Service Kanagement Service Kanagement Service	FTP Extensibility enables support fo FTP extensibility features such as custom providers, ASP.NET users or IIS Manager users.

- 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 Management.



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.

£			Com	nputer Management
File Action View Help				
🗢 🔿 🙍 🖬 🖉				
Computer Management (Local	Name	Full Name		Description
⊿	Mathematical Administrator			Built-in account for administering
Task Scheduler	💭 cloudbase-init	cloudbase-init		
Event Viewer	👧 Guest			Built-in account for guest access t
Shared Folders				
Local Users and Groups Users	Ne	ew User		
Groups	Re	fresh		
Performance Bevice Manager	Exp	port List	_	
⊿ 📇 Storage	Vie	ew 🕨		
Windows Server Backup Disk Management	Ar	range lcons 🔹 🕨		
Services and Applications	Lir	ne up Icons		
	He	elp		

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

	New User	? X
User name:	ftpadmin	
Full name:		
Description:		
Password:	•••••	
Confirm password	•••••	
User must cha	nge password at next logon	
User cannot d	hange password	
 Password nev 	er expires	
Account is dis	abled	
Help	Create	Close

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 and it contains the **test.txt** file to be shared.

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

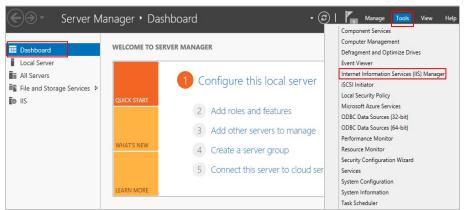
If **Everyone** is unavailable, add it. For details, see **FAQs**.

👃 work01 Properties 🗙
General Sharing Security Previous Versions Customize
Object name: C:\work01
Group or user names:
Everyone
CREATOR OWNER
SYSTEM
<
To change permissions, click Edit.
Permissions for Everyone Allow Deny
Full control
Modify
Read & execute 🗸 🗉
List folder contents 🗸
Read 🗸
Write
For special permissions or advanced settings, Advanced click Advanced.
OK Cancel Apply

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

Permissions	for work01	X
Security		
Object name: C:\work01		
Group or user names:		
Everyone CREATOR OWNER		
SYSTEM .		
Administrators (ECS-7306\Ad & Users (ECS-7306\Users)	ministrators)	
	Add	Remove
Permissions for Everyone	Allow	Deny
Full control		
Modify Read & execute		
List folder contents		
Read	✓	
	_	
ОК	Cancel	Apply

- 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.

File View Help	p					
Connections		Sit	tes			
Start Page ECS-7306 (ECS-7306\Adminis		Filter:		- 1	ኛ Go 🕞 😽 Show A	.II 📮
		Name 📩		ID	Status	Bind
D Sites		😌 Default \	Web Site	1	Started (ht	*:80
Image: Add Website Image: Add Website Image: Refresh						
e	Add FTP Site					
	Switch to Conte	nt View				

3. In the displayed dialog box, 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.

Add FTP Site	?	x
Site Information		
FTP site name: FTPSERVER Content Directory Physical path: C:\work01 		
Previous Next Finish C	ancel	

- 4. Enter the private IP address and port number of the ECS, set SSL, and click **Next**.
 - Port 21 is used by default. You can set it as required.
 - You can also set SSL as required.
 - **No SSL**: SSL encryption is not required.
 - Allow SSL: Non-SSL and SSL connections between the FTP server and the client are allowed.
 - Require 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 **3**.

	Add FTP Site	? X
Binding and SSL Settings		
Binding IP Address:	Port:	
Enable Virtual Host Names: Virtual Host (example: ftp.contoso.com):	21	
 Start FTP site automatically SSL 		
No SSL Allow SSL		
O Require SSL		
SSL Certificate:	V Select View	
	Previous Next Finish C	Cancel

- 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. 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 groups 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.

Add FTP Site	? ×
Authentication and Authorization Information	
Authentication Anonymous Basic	
Authorization Allow access to: Not Selected	
Permissions Read Write	
Previous Next	Finish Cancel

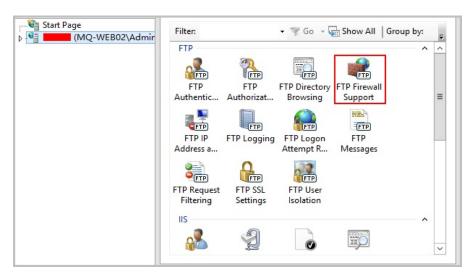
6. Add the private IP address of the ECS to the FTP site.

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 and click **OK**.

	Application Pools	Name Default Web Site FTPSERVER	ID 1 2	Status Started (ht Started (ftp)	Binding *:80 (http)	Path %SystemDrive C:\work01		Add FTP Site Set FTP Site Def Edit Site Bindings
		:	Site B	indings		? X		Basic Settings
	Type Host Name ftp	Port IP Addres 21 139.159.1 Add Site Bind	47.143	Binding Info	rma	Add Edit	×	Explore Edit Permission Remove
	Type: IP ad	dress:	ing	Port:	1	Remove	ŀ	Rename View Applicatio View Virtual Dire
< Ready	Host name:	n or marketing.contoso.c	om		4		M	anage FTP Site Restart Start Stop
				ОК	Cancel	Close		

Step 5 (Optional) Configure the FTP firewall.

- To enable the passive mode on the FTP server, the FTP firewall must be configured.
- 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: specifies the public IP address of the ECS.

	Alerts
FTP Firewall Support The settings on this page let you configure your FTP server to accept passive connections from an external firewall. Data Channel Port Range: 5000-6000 Example: 5000-6000 External IP Address of Firewall: External IP Address of Firewall: Example: 10.0.0.1	Alerts ▲ To accept passive connections when you are using FTP over SSL (FTPS) or when your firewall does not filter packets, configure the external IPv4 address of your firewall. Actions Actions Cancel ② Help
The Features View 📴 Content View	

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**. For details about which ports are allowed, see **Table 6-1**.

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.

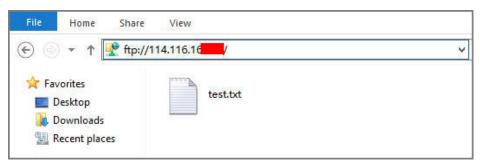
Dir ecti on	Priori ty	Acti on	Туре	Protocol & Port	Source Address
Inb oun d	1	Allo w	IPv4	Protocols/TCP (Custom): 20-21	0.0.0.0/0
Inb oun d	1	Allo w	IPv4	Protocols/TCP (Custom): 1024-65535 (for example, 5000-6000)	0.0.0.0/0

 Table 6-1 Security group rules

Step 7 Verify the configuration on the client.

On the computer with the client installed, enter **ftp://***IP* address of the FTP server.FTP port number in the Internet Explorer address bar. If you do not specify the port number, port 21 is used by default. 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.

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



----End

FAQs

- 1. For more information about setting up an FTP site on a Windows ECS, see Microsoft official documents.
- 2. 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**.

👃 work01 Properties 💌
General Sharing Security Previous Versions Customize
Object name: C:\work01
Group or user names:
& CREATOR OWNER
SYSTEM .
Administrators (ECS-7306\Administrators)
& Users (ECS-7306\Users)
To change permissions, click Edit.
Permissions for CREATOR
OWNER Allow Deny
Full control
Modify
Read & execute
List folder contents
Read
Write 🗸
For special permissions or advanced settings, Advanced click Advanced.
OK Cancel Apply

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

Permissions	for work01	X
Security		
Object name: C:\work01		
Group or user names:		
CREATOR OWNER		
Administrators (ECS-7306\Administrators)	dministrators)	
Permissions for CREATOR OWNER	Add Allow	Remove Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		

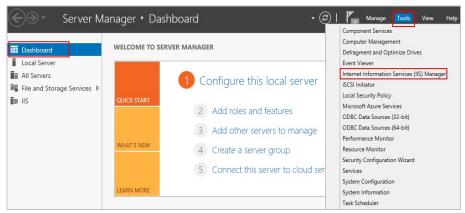
c. In the displayed dialog box, click **Advanced**.

Select Users or Groups	X
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
ECS-7306	Locations
Enter the object names to select (<u>examples</u>):	
	Check Names
Advanced OK	Cancel

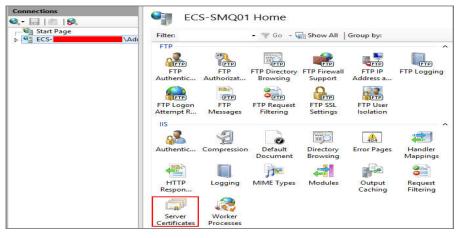
d. In the displayed dialog box, click **Find Now**, select **Everyone** in search results, and click **OK**.

Se	lect Users or Groups		x
Select this object type:			
Users, Groups, or Built-in security princip	als	Object	Types
From this location:			
ECS-7306		Loca	tions
Common Queries			
Name: Starts with V			Columns
Description: Starts with V			Find Now
Disabled accounts			Stop
Non expiring password			
Days since last logon: 🔍 🗸			,
Search results:		ОК	Cancel
Name In Folder			^
Distributed C ECS-7306			
Event Log Re ECS-7306	1		
S ftpadmin ECS-7306			_
ECS-7306			=
Guests ECS-7306			
Hyper-V Admi ECS-7306			
KIIS_IUSRS ECS-7306			
			~

- e. Click **OK** to return to the permissions page.
- f. Click OK.
- 3. Create a server certificate.
 - a. In Server Manager, choose Dashboard > Tools > Internet Information Services (IIS) Manager.



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



c. Click Create Self-Signed Certificate.

V j	Inter	net Information Services	(IIS) Manager		×
ECS-SMQ01	•				📴 🔤 🟠 🔞 •
File View Help					W.
Connections		- Cartification		Ac	tions
😪 • 🔚 🖄 🥵	Serve	er Certificates		Import	
Start Page		o request and manage certifica s configured for SSL.		Create Certificate Request Complete Certificate Request	
Application Pools ⊳ Sites	Filter:	🝷 🛒 Go 👒 🙀 She	ow All Group by:		Create Domain Certificate
	Name 🔺	Issued To	Issued By		Create Self-Signed Certificate
					Enable Automatic Rebind of Renewed Certificate
				0	Help

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

Create Self-Signed Certificate	?	x
Specify Friendly Name		
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:		
Specify a friendly name for the certificate: SSL-FTP		
Select a certificate store for the new certificate: Personal V		
ОК	Cancel	

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

Connections		C	
🔍 • 🔚 🖄 🕵	Serve	r Certificates	
Start Page		request and manage certifi configured for SSL.	cates that the Web server can
→ 💣 Application Pools	Filter:	🕶 🛒 Go 👒 🕁 S	Show All Group by: 💡
	Name 📤	Issued To	Issued By
	SSL-FTP		

6.1.2 Setting Up an FTP Site (Windows 2019)

Overview

The best practices for ECS guide you through the setup of an FTP site on a Windows ECS. The Windows Server 2019 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.

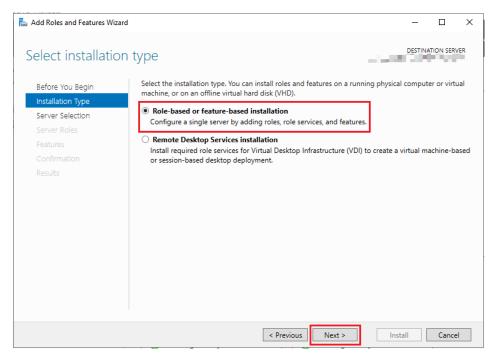
Procedure

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.

🚡 Server Manager						- 0	×
Server M	anager • Dashl	poard	• @ 🏲	Manage	Tools	View	Help
🔛 Dashboard	WELCOME TO SERVI	ER MANAGER					^
Local Server All Servers File and Storage Services		1 Configure this local serv	ver				
	QUICK START	2 Add roles and features					
		3 Add other servers to mana	age				
	WHAT'S NEW	4 Create a server group					
		5 Connect this server to clou	ud services				
	LEARN MORE					Hide	

- 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.

Select destinati	ion server			DESTINA	TION SERVE
Before You Begin Installation Type Server Selection		from the server pool	n to install roles and features.		
Server Roles	Server Pool				
Features	Filter:				
	Name	IP Address	Operating System		
	2, 10 March 10	64. CUILD	Microsoft Windows Server	2019 Standard	
	1 Computer(s) fou	ind			
	and that have bee	n added by using the Add	ndows Server 2012 or a newer Servers command in Server Ma ion is still incomplete are not s	anager. Offline se	

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

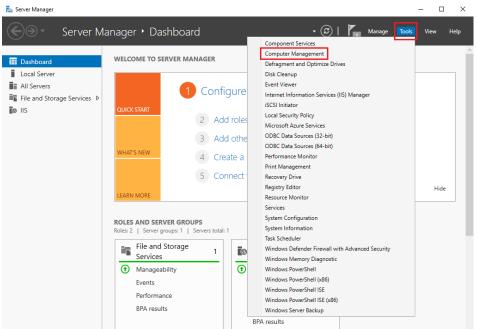
	Select one or more roles to install on the selected server.	
	Roles Descript	ion
Server Selection Server Roles Peatures Confirmation Results	Active Directory Certifica Active Directory Domain Active Directory Event Directory Rights Active Directory Lightwe Active Directory Lightwe A	

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

📥 Add Roles and Features Wizard		- 🗆 X
Select role service Before You Begin Installation Type Server Selection Server Roles Features	S Select the role services to install for Web Server (IIS) Role services Security Request Filtering Basic Authentication Centralized SSL Certificate Support	DESTINATION SERVER Description FTP Extensibility enables support for FTP extensibility features such as custom providers, ASP.NET users or IIS Manager users.
Web Server Role (IIS) Role Services Confirmation Results	Client Certificate Mapping Authentication Digest Authentication IIS Client Certificate Mapping Authenticatic IP and Domain Restrictions URL Authorization VRL Authorization Restriction FP Server FTP Server FTP Server FTP Service FTP Extensibility Management Tools	
	IIS Management Console IIS 6 Management Compatibility IIS Management Scripts and Tools Management Service	
	< Previous Next >	Install Cancel

- 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 Management.

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.

😓 Computer Management File Action View Help				-		×
Computer Management (Local System Tools Computer Meanagement (Local System Tools Computer Meanagement Computer Viewer Computer Viewer C	Name F Administrator Cloudbase-init o DefaultAcco Guest WDAGUtility	Full Name cloudbase-init cloudbase-init Refresh Export List View Arrange Ico Line up Icor Help	> ns >	Actions Users More Act	ions	-

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

New User					?	×
User name:	ftpadmin					
Full name:						
Description:						
Password:	•••	••••				
Confirm password:	•••	••••				
User must cha	nge passwo	ord at n	ext logo	n		
User cannot ch	nange pass	word				
Password neve	er expires					
Account is disa	abled					
Help				Create	0	Close

4. Click Create.

Step 3 Assign permissions to shared files.

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

 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 and it contains the **test.txt** file to be shared.

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

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

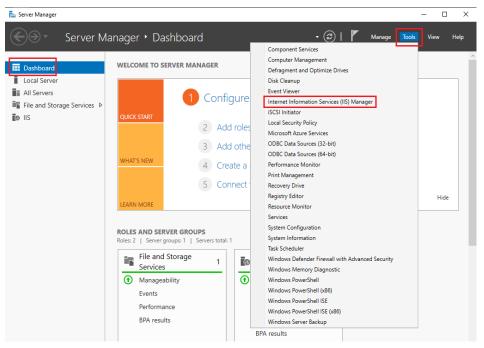
work01 Properties	×
General Sharing Security Previous Versions Customize	
Object name: C:\work01	
Group or user names:	
Severyone	•
SYSTEM	
Administratore (ECS.MAXIAORI II.W/\ Administratore)	1
< >	
To change permissions, click Edit. Edit	
Permissions for Everyone Allow Deny	
Full control	1 1
Modify	
Read & execute 🗸	
List folder contents	
Read 🗸	
Write	/
For special permissions or advanced settings, Advanced click Advanced.	
OK Cancel Apply	

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

Permissions for work01			×	<
Security				
Object name: C:\work01				
Group or user names:				
Everyone				
🧟 Administrators (Administra	ators)	
🤽 Users (Users)			
	Ad	d	Remove	
Permissions for Everyone		Allow	Deny	
Full control			□ ^	
Modify				
Read & execute List folder contents				
Read				
	-			
ОК		Cancel	Apply	

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.

Internet Information Services (IIS) M	anager	- 🗆 X
← →	ir 🕨	📴 🖂 🕼 🗸
File View Help		
Connections		Actions
Contraction of the second seco	Filter:	Manage Server Restart Start Stop View Application Pools
Refresh	TP FTP FTP Directory entic Authorizat Browsing	View Sites Get New Web Platform Components
Add Website	FTP FTP irewall FTP IP FTP Logging port Address a	Help
Stop		
G Add FTP Site	FTP FTP CFTP	
Rename	npt R Messages Filtering	
Switch to Content View		
< >> Ready	📰 Features View 💦 Content View	•1.:

3. In the displayed dialog box, 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.

Add FTP Site	?	Х
Site Information		
FTP site name: FTPSERVER		
Content Directory		
Physical path: C:\work01		
Previous Next Finish	Cancel	

- 4. Enter the private IP address and port number of the ECS, set SSL, and click **Next**.
 - Port 21 is used by default. You can set it as required.
 - You can also set SSL as required.

- **No SSL**: SSL encryption is not required.
- Allow SSL: Non-SSL and SSL connections between the FTP server and the client are allowed.
- **Require SSL**: SSL encryption is required for the communication between the FTP server and the client.

NOTE

When **Allow SSL** and **Require SSL** are selected, you can select an existing SSL certificate or create one. For details, see **3**.

dd FTP Site	? >
Binding and SSL Settings	
Binding	
IP Address: Port:	
Enable Virtual Host Names: Virtual Host (example: ftp.contoso.com):	
☑ Start FTP site automatically	
SSL O No SSL	
Allow SSL	
C Allow 35L	
Allow SSL Require SSL	

- 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. 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 groups 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.

Add FTP Site	?	×
Authentication and Authorization Information		
Authentication		
Anonymous		
Basic		
Authorization		
Allow access to:		
Not Selected V		
Permissions		
Read Write		
vince		
Previous Next Finish	Cancel	

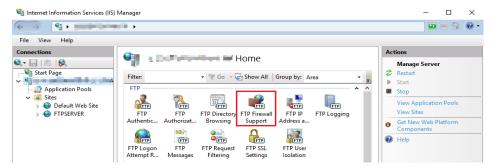
6. Add the private IP address of the ECS to the FTP site.

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 and click **OK**.

🝓 Internet Information Services	: (IIS) Manager	- 🗆 ×
\leftrightarrow \rightarrow \bullet	Sites >	🔯 🖂 🏠 🔞 🗸
File View Help		
Connections	Citer	Actions
🔍 • 🔒 🖄 🕼	Sites	💣 Add Website
Start Page	Filter: • 🐨 Go - 🕁 Show All Group by: No Grouping •	Set Website Defaults
Application Pools	Name ID Status Binding F	G Add FTP Site
🗸 - 🚺 Sites	Default Web Site 1 Started (ht *:80 (http)	Set FTP Site Defaults
> 😻 Default Web Site	FTPSERVER 2 Started (ftp)	Edit Site Bindings.
	Bindings	2 × ettings
Site	- unungs	
1	Type Host Name Port IP Address Binding Informa A	dd rmissions
f	tp 21	e dit
	Add Site Binding ? ×	move pplications
	т р. н. р. н. Ви	rowse P Site
	Type: IP address: Port: ftp v 21	r Site
	Host name:	
		ced Settings
	Example: www.contoso.com or marketing.contoso.com	
	c	Close
< Ready		61
Reduy		¶.:

Step 5 (Optional) Configure the FTP firewall.

- To enable the passive mode on the FTP server, the FTP firewall must be configured.
- 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: specifies 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**. For details about which ports are allowed, see **Table 6-2**.

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.

Priori ty	Acti on	Туре	Protocol & Port	Source Address
1	Allo w	IPv4	Protocols/TCP (Custom): 20-21	0.0.0.0/0
1	Allo w	IPv4	Protocols/TCP (Custom): 1024-65535 (for example, 5000-6000)	0.0.0.0/0

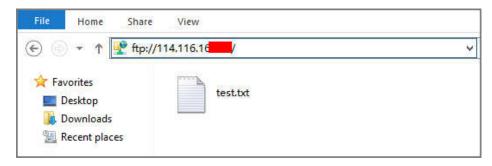
Table 6-2 Security group rules

Step 7 Verify the configuration on the client.

On the computer with the client installed, enter **ftp://***Public IP address of the FTP server.FTP port number* in the Internet Explorer address bar. If you do not specify the port number, port 21 is used by default. 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 cannot be accessed. To configure the Internet Explorer browser, choose **Tools** > **Internet Options** > **Advanced**, select **Enable FTP folder view**, and deselect **Use Passive FTP**.





FAQs

- 1. For more information about setting up an FTP site on a Windows ECS, see Microsoft official documents.
- 2. 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**.

work01 Properties ×
General Sharing Security Previous Versions Customize
Object name: C:\work01
Group or user names:
CREATOR OWNER
SYSTEM Statisticators (
St Users (
To change permissions, click Edit.
Permissions for CREATOR
OWNER Allow Deny
Full control
Full control ^
Full Control
Modify
Modify Read & execute
Modify Read & execute List folder contents
Modify Read & execute List folder contents Read
Modify Read & execute List folder contents Read Write
Modify Read & execute List folder contents Read Write

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

Permissions for work01		×
Security		
Object name: C:\work01		
Group or user names:		
SCREATOR OWNER		
SYSTEM Administrators (2) St Users (2)	VAdministrat Users)	ors)
Permissions for CREATOR	Add	Remove
Permissions for CREATOR OWNER	Add Allow	Remove Deny
OWNER		Deny
OWNER Full control		Deny
OWNER Full control Modify Read & execute List folder contents		Deny
OWNER Full control Modify Read & execute		Deny
OWNER Full control Modify Read & execute List folder contents		Deny

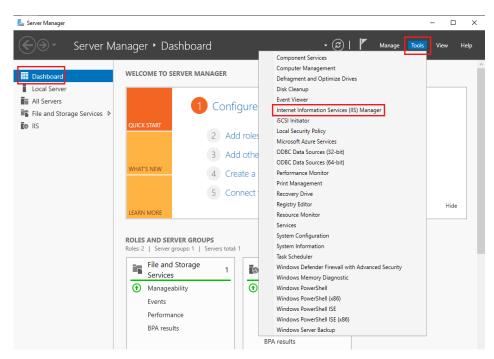
c. In the displayed dialog box, click **Advanced**.

Select Users or Groups	×
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
die der der der der der der der der der de	Locations
Enter the object names to select (<u>examples</u>):	
1	Check Names
Advanced OK	Cancel

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

Select Users or Gr	oups					×
Select this object to Users, Groups, or		principals		Object 1	Types	
From this location:				,	.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
				Locati	ons	
Common Queries	•					
Name: (Starts with $~{\sim}~$				Columns	
Description:	Starts with $~\vee~$				Find Now	
Disabled ac	counts				Stop	
Non expiring	g password					
Days since last	logon:	\sim			?	
Search results:			Oł	<	Cancel	
Name	In Folder					^
Default Account		1.				
Contraction Contract						
Distributed C	a deserve a					
Event Log Re	ALC: N					T
Everyone						
🐁 ftpadmin 🕁 Guest						
Guest Guests	in the second					
Hyper-V Admi	100					¥

- e. Click **OK** to return to the permissions page.
- f. Click **OK**.
- 3. Create a server certificate.
 - a. In Server Manager, choose Dashboard > Tools > Internet Information Services (IIS) Manager.



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

💐 Internet Information Services (IIS	Manager	- 🗆 ×
	all a	😰 🐼 🚱 🕶
File View Help		
Connections		Actions
🔍 - 🔜 🖄 🥵	Home	Open Feature
Start Page	Filter: • 🐨 Go - 🥁 Show All Group by: Area •	Manage Server
	FTP A A	Restart Start
		Stop
	FTP FTP FTP Directory FTP Firewall FTP IP FTP Logging	View Application Pools
	Authentic Authorizat Browsing Support Address a	View Sites
		Get New Web Platform Components
	FTP Logon FTP FTP Request FTP SSL FTP User Attempt R Messages Filtering Settings Isolation	😧 Help
	IIS •	
	🔏 🔮 🝺 🛋 🛋	
	Authentic Compression Default Directory Error Pages Handler Document Browsing Mappings	
	👚 💵 🏂 📫	
	HTTP Logging MIME Types Modules Output Request Respon Caching Filtering	
	Server Worker Certificates Processes	
	Management 💦 🗸 🗸	
< >	Features View 💦 Content View	
Ready		€ <u>1</u> .:

c. Click Create Self-Signed Certificate.

💐 Internet Information Services (IIS) N	Manager			- 🗆 ×
← →	₩ +			🔯 🛛 🟠 🔞 -
File View Help				
Connections	Server Certificates		Actions	
Q				Import
Start Page	Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.			Create Certificate Request
Application Pools				Complete Certificate Request
> - 🙆 Sites	Filter: • 🐨	Go 👻 🙀 Show All Group by:	No Grouping •	Create Domain Certificate
	Name	Issued To	Issued By	Create Self-Signed Certificate.
				Enable Automatic Rebind of Renewed Certificate
				Help

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

Create Self-Signed Certificate	?	Х
Specify Friendly Name		
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing: Specify a friendly name for the certificate: SSL-FTP	Dr	
Select a certificate store for the new certificate: Personal Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate: Image: Select a certificate store for the new certificate:		
ОК	Cancel	

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

Internet Information Services (IIS)	Manager				- 🗆 ×
	<i>↓ ↓</i>				😰 🖂 🟠 🔞 ·
File View Help					
Connections		Certificates		Ac	tions
🔍 - 🔚 🖄 🤧	Server C	ertificates			Import
 Start Page Application Pools 	Use this feature to rec websites configured t	quest and manage certificates that the W for SSL.	/eb server can use with		Create Certificate Request Complete Certificate Request.
> Sites	Filter: • 🐨 Go	🝷 🐨 Go 👒 🥁 Show All 🛛 Grou	🕫 Go 🖂 🖏 Show All Group by: No Grouping 🔹		Create Domain Certificate
	Name	Issued To	Issued By		Create Self-Signed Certificate.
	SSL-FTP	website and a state of the	it. Statements in the		View
					Export
				\sim	Remove
					Enable Automatic Rebind of Renewed Certificate
					Help

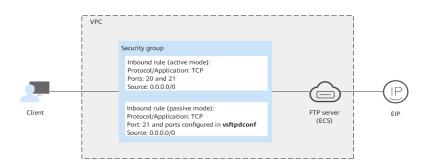
6.1.3 Setting Up an FTP Site (Linux)

Application Scenarios

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 an FTP server software that is widely used in Linux releases. The CentOS 7.2 64bit OS is used as an example in this section.

Architecture

Figure 6-1 Setting up an FTP site (Linux)



Advantages

- A website with a simple networking architecture can be quickly set up.
- The website is secure and easy to use.

Resource and Cost Planning

Table 6-3 Resources and costs

Resource	Description	Cost
VPC	VPC CIDR block: 192.168.0.0/16	Free
Subnet	 AZ: AZ1 CIDR block: 192.168.0.0/24 	Free

Resource	Description	Cost
Security group	 Inbound rule (active mode): Priority: Set it to 1. Action: Select Allow. Type: Select IPv4. Protocol & Port: Set it to TCP: 20-21. Source: Set it to 0.0.0/0. Inbound rule (passive mode): Priority: Set it to 1. Action: Select Allow. Type: Select IPv4. Protocol & Port: Set it to TCP: 21 and ports configured in vsftpdconf Source: Set it to 0.0.0/0. 	Free
ECS	 Billing mode: Yearly/ Monthly AZ: AZ1 Flavor: s6.large.2 Image: CentOS 7.2 64bit System disk: 40 GiB EIP: Auto assign EIP type: Dynamic BGP Billed by: Traffic Bandwidth: 5 Mbit/s 	The following resources generate costs: • ECSs • EVS disks • EIPs For billing details, see Billing Modes .
vsftpd	A free, open-source FTP software.	Free

Process

The process of manually setting up an FTP website on a Linux ECS 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.
- The image source has been updated to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)? This facilitates obtaining and updating the system and software.
- 3. Run the following command to install vsftpd:

yum install -y vsftpd

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

Package	Arch	Version	Repository	Size
Installing: vsftpd	×86_64	3.0.2-22.e17	base	169 k
Transaction Summar	ŋ			
Install 1 Package				
fotal download siz				
Installed size: 34 Downloading packag				
sftpd-3.0.2-22.el	7.×86_64.rpm		i 169 kB	00:00:00
Running transactio				
Running transactio Transaction test s				
Running transactio				
	tpd-3.0.2-22.e17.x86_64			1/1
Verifying : vsf	tpd-3.0.2-22.e17.x86_64			1/1
Installed:				
vsftpd.x86_64 0:	3.0.Z-ZZ.e17			

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

systemctl enable vsftpd.service

5. Run the following command to start FTP:

systemctl start vsftpd.service

6. 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/vs ftp d
------	---	---------	------	--------	-----------------------

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**
- 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 insert mode.
- c. Modify the **vsftpd.conf** file.

Set FTP to active or passive 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 FTP to passive 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_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

 Apart from the parameters configured in active FTP mode, the following parameters are also required for passive 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 #Public IP address of the FTP server

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

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

Priori ty	Acti on	Туре	Protocol & Port	Source Address
1	Allo w	IPv4	Protocols/TCP (Custom): 20-21	0.0.0.0/0
1	Allo w	IPv4	Protocols/TCP (Custom): 1024-65535 (for example, 5000-6000)	0.0.0/0

Step 4 Verify the configuration on the client.

On the computer with the client installed, enter **ftp://***IP* address of the FTP server.FTP port number in the Internet Explorer address bar. If you do not specify the port number, port 21 is used by default. 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 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, clear the browser caches and try again.

----End

6.1.4 Setting Up an FTP Site (Huawei Cloud EulerOS 2.0)

Introduction

vsftpd (very secure FTP daemon), is an FTP server for Unix-like systems, including Linux. This tutorial describes how you can deploy vsftpd in HCE 2.0.

Preparations

- Prepare an ECS and assign a public IP address or EIP to the ECS.
- Ensure that inbound security group rules allow traffic to flow to the ECS over port 21.

Procedure

Step 1 Install vsftpd and start it.

- 1. Run the following command to install vsftpd: dnf install vsftpd
- 2. Run the following command to start vsftpd: systemctl start vsftpd
- 3. Run the following command to check the vsftpd status: systemctl status vsftpd

If **active (running)** is displayed, vsftpd is started.

]# systemctl status vsftpd vice - Vsftpd ftp daemon
	loaded (/usr/lib/systemd/system/vsftpd.service; disabled; vendor preset: disabled)
	active (running) since Tue 2023-10-10 15:55:11 CST; 1s ago
	21033 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
Main PID:	21034 (vsftpd)
Tasks:	1 (limit: 198730)
Memory:	408.0K
CGroup:	/system.slice/vsftpd.service
	21034 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

NOTE

To set vsftpd to automatically enable upon system boot, run the following command: **systemctl enable vsftpd**

- **Step 2** Add a user for the FTP service.
 - 1. Run the following command to create a user for the FTP service: adduser ftp
 - 2. Run the following command to set a password of the created user: passwd ftp

Step 3 Configure vsftpd.

- Run the following commands to create directories and files for the FTP service (you can change the directories as required): mkdir -p /data/ftp/ touch /data/ftp/test.txt
- 2. Run the following command to set the created user as the owner of the directories:

chown -R ftp:ftp /data/ftp/

3. Open the **/etc/vsftpd/vsftpd.conf** file and set the following parameters: # Listen to IPv4 sockets. listen=YES

Determine whether to configure IPv6 listening. listen_ipv6=YES

Add the following parameters to the end of the configuration file: # Set the directory where the local user resides after login. local_root=/data/ftp/hce # Restrict all users to the home directory. chroot_local_user=YES # Enable the passive mode. pasv_enable=YES pasv_address=<Public IP address of the FTP server> chroot list enable=NO # Determine whether to allow users to access other directories. # If chroot_list_enable is set to YES, you need to set chroot_list_file to a file that contains the users who can access other directories. # chroot_list_file=/etc/vsftpd/chroot_list # Set the port range that can be used in passive mode. Set a large port range to improve the security of accessing the FTP server. # Minimum port in the available port range pasv_min_port=<port number>

Maximum port in the available port range pasv_max_port=<port number>

D NOTE

Retain the default values for other parameters.

The **/etc/vsftpd/chroot_list** file must be created regardless of whether **chroot_list_enable** is configured.

4. Run the following command to restart vsftpd: systemctl restart vsftpd

Step 4 Verify vsftpd.

1. Run the following command to check the port used by vsftpd: netstat -natp | grep vsftpd

By default, port 21 is used.

- 2. Configure inbound security group rules to enable port 21 and ports 5000 to 5010.
- In the Windows file manager, enter ftp://<Public IP address of the FTP server>:21 to access the FTP service. Enter the password, as shown in the following figure.

2 > Internet > 200000000000000000000000000000000000	~ C
test.txt	
de la	
*	
*	

If the following error occurs, add **allow_writeable_chroot=YES** to the end of the **/etc/vsftpd/vsftpd.conf** file and restart vsftpd:

500 OOPS: vsftpd: refusing to run with writable root inside chroot()

```
----End
```

6.2 Building Microsoft SharePoint Server 2016

6.2.1 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 \bigcirc in the upper left corner and select the desired region and project.
- 3. Under **Compute**, click **Elastic Cloud Server**.
- 4. Click **Buy ECS**. The **Buy ECS** page is displayed.
- 5. Configure ECS parameters. For details, see **Purchasing a Custom ECS**.

Figure 6-2 Setting ECS specifications

Instance Selection	By Type By Scenario						
CPU Architecture	x86 Kunpeng	D					
Specifications	Latest generation 👻	vCPUs -Select vCPUs-	Memory -Select Memory	ny	e	Q Hide sold-out specification	ons
	General computing-plus	General computing Memory-	optimized Large-memor	y Disk-intensive	Ultra-high I/O GPU-	accelerated Al-accelerated	General computing-basic
	Select All \$7 Collapse Help ^	s6 s3					
	General computing ECSs provide a b	valance of compute, memory, and network	resources with a baseline level of	vCPU performance and the ability t	o deliver occasional bursts of extra	a compute above this baseline.	
	ECS Type	Flavor Name	vCPUs 💠	Memory \$	CPU \$	Assured / Maximum ⑦ Bandwidth	Packets Per Second 🔅
	General computing s6	s6.small.1	1 vCPU	1 GIB	Intel Cascade Lake 2.6GHz	0.1 / 0.8 Gbit/s	100,000 PPS
	General computing s6	s6.medium.2	1 vCPU	2 GIB	Intel Cascade Lake 2.6GHz	0.1 / 0.8 Gbit/s	100,000 PPS
	General computing s6	s6.medium.4	1 vCPU	4 GiB	Intel Cascade Lake 2.6GHz	0.1 / 0.8 Gbit/s	100,000 PPS
	 General computing s6 	s6.large.2	2 vCPUs	4 GiB	Intel Cascade Lake 2.6GHz	0.2 / 1.5 Gbit/s	150,000 PPS
	General computing s6	s6.large.4	2 vCPUs	8 GiB	Intel Cascade Lake 2.6GHz	0.2 / 1.5 Gbit/s	150,000 PPS
	General computing s6	s6.xlarge.2	4 vCPUs	8 GIB	Intel Cascade Lake 2.6GHz	0.35 / 2 Gbit/s	250,000 PPS
	 General computing s6 	s6.xlarge.4	4 vCPUs	16 GIB	Intel Cascade Lake 2.6GHz	0.35 / 2 Gbit/s	250,000 PPS

Selected specifications General computing | s6.large.2 | 2 vCPUs | 4 GiB

Figure 6-3 Setting the network

Network	vpc-f00373897(192.168.0.0/16)	- C subnet-	100373897-01(192.168.0.0/24)	C Automatically assign IP a	ddress v Available	e private IP addresses: 249
	Create VPC					
Extension NIC	Add NIC NICs you can still add: 1					
Source/Destination Check	• •					
				-		
Security Group	Sys-WebServer(13e7c1f8-959c-464e-875			iroup (?)		
	Similar to a firewall, a security group logically Ensure that the selected security group allow	controls network acc s access to port 22 (S	ess. ISH-based Linux login), 3389 (Wi	ndows login), and ICMP (ping operation). Configure Security Group Rul	es
	Security Group Rules 🔨					
	Inbound Rules Outbound Rules					
	Security Group Name	Priority	Action	Protocol & Port (?)	Туре	Source (?)
		1	Permit	TCP: 111	IPv4	0.0.0/0
		1	Permit	UDP: 111	IPv4	0.0.0.0/0
		1	Permit	TCP: 2049	IPv4	0.0.0.0/0
		1	Permit	TCP: 2052	IPv4	0.0.0.0/0
	Suc WebServer	1	Permit	TCP: 2051	IPv4	0.0.0.0/0
EIP	Auto assign Use existing	Not required ⑦				
EIP Type	Dynamic BGP	Static BGP				
	⊘ Greater than or equal to 99.95% service and the service of t	availability rate				
Billed By	Bandwidth For heavy/stable traffic Billed based on usage duration and bandwid	Traffic For light/sharply fluct		I bandwidth gered peak hours		

ECS Name	ecs-3fbc Allow duplicate name
	If you are creating multiple ECSs at the same time, automatic naming and customizable naming are available for you to select.
Description	
	0/85
Login Mode	Password Key pair
Username	Administrator
Password	Keep the password secure. If you forget the password, you can log in to the ECS console and change it.
	······· @
Confirm Password	······· @
Cloud Backup and	To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.
Recovery	Create new Use existing Not required ?
	CBR backups can help you restore data in case anything happens to your ECS. To ensure data security, you are advised to use CBR
FOO Oroup (Optional)	
ECS Group (Optional)	Anti-affinity ?
	-Select ECS group- C
	Create ECS Group

Figure 6-4 Setting the login mode and ECS name

- 6. Confirm the ECS configuration, and read and agree to the agreement.
- 7. Click **Submit** and wait for the ECS creation to complete.
- 8. In the ECS list, locate the ECS you created and click **Remote Login** in the **Operation** column.
- 9. Enter the password of the ECS to log in.
- 10. To obtain and update the system and software, update the image source to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)?

6.2.2 Adding AD, DHCP, DNS, and IIS Services

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

🔏 In	ternet Explorer Enhanced Security Configuration
expos Intern	et Explorer Enhanced Security Configuration (IE ESC) reduces the ure of your server to potential attacks from Web-based content. et Explorer Enhanced Security Configuration is enabled by It for Administrators and Users groups.
Admin	istrators:
۲	○ On (Recommended)
۲	● off
Users:	
۲	○ On (Recommended)
8	● off
More a	about Internet Explorer Enhanced Security Configuration
	OK Cancel

Figure 6-5 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 6-6 Add roles and features

<u>à</u>		Server Manager		_ 🖬 🗙
Server Ma	anager • Dashboard	· @ ۱	Manage Tools	View Help
Dashboard Local Server All Servers File and Storage Services	QUICK START	Configure this local server 2 Add roles and features		
	WHAT'S NEW	 Add other servers to manage Create a server group Connect this server to cloud service 	s	
	LEARN MORE			Hide
	ROLES AND SERVER GROUP Roles: 1 Server groups: 1 S File and Storage Services			
	 Manageability 	Manageability		
	Events Performance	Events 3 Services		
	BPA results	Performance		
		BPA results		
		6/28/2018 9:08		
				9:15
	1		• (b)	6/28/2018

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

Figure 6-7 Server role 1

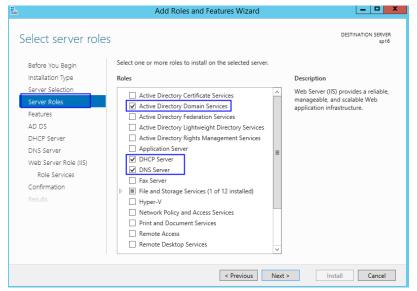
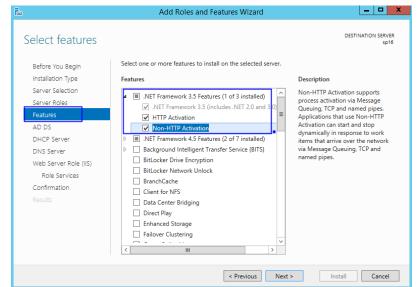


Figure 6-8 Server role 2

a	Add Roles and Features Wizard	- - X
Select server role	S	DESTINATION SERVER sp16
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection Server Roles Features AD DS DHCP Server DNS Server Web Server Role (IIS) Role Services Confirmation Results	Application Server DHCP Server DHCP Server DNS Server Fax Server Fax Server Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Access Volume Activation Services Volume Activation Services Windows Deployment Services Windows Server Update Services	Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
	< Previous Next :	> Install Cancel

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

Figure 6-9 Features



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

Figure 6-10 Confirm installation selections

2	Add Roles and Features Wizard	X
Confirm installatio		DESTINATION SERVER sp16
Before You Begin	To install the following roles, role services, or features on selected server, click	Install.
Installation Type	Restart the destination server automatically if required	
Server Selection Server Roles Features	Optional features (such as administration tools) might be displayed on this pay been selected automatically. If you do not want to install these optional featur their check boxes.	
AD DS	.NET Framework 3.5 Features	^
DHCP Server	HTTP Activation Non-HTTP Activation	=
DNS Server Web Server Role (IIS)	.NET Framework 4.5 Features ASP.NET 4.5	
Role Services Confirmation	Active Directory Domain Services DHCP Server	
Results	DNS Server	
	Group Policy Management Remote Server Administration Tools	~
	Export configuration settings Specify an alternate source path	
	< Previous Next >	Install Cancel

- 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 6-11 AD configuration

	View installation progress	
	 Feature installation 	
	Configuration required. Installation succeeded on ecs-sharepoint.	
	Active Directory Domain Services	^
	Additional steps are required to make this machine a domain controller.	=
	Promote this server to a domain controller	
	DHCP Server Launch the DHCP post-install wizard	
	Complete DHCP configuration	
	.NET Framework 3.5 Features	
	HTTP Activation	
	Non-HTTP Activation	
Results	.NET Framework 4.5 Features	

Choose Add a new forest.
 Set Root domain name to sp160.com.cn.

Figure 6-12 Add a new forest

b	Active Directory Domain Services Configuration Wizard	_ D X
Deployment Configuration Domain Controller Options Additional Options Paths Review Options Prerequisites Check Installation Results		TARGET SERVER
	More about deployment configurations	Cancel

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

Figure 6-13 Password setting

i 🖻 🖌 🖌	Active Directory Domain Services (Configuration Wizard	_ _ ×
Domain Controller	r Options		TARGET SERVER
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select functional level of the new forest Forest functional level: Domain functional level: Specify domain controller capabilities Ormain Name System (DNS) server Global Catalog (GC) Read only domain controller (RODC)	Windows Server 2012 R2 Windows Server 2012 R2	_
	Type the Directory Services Restore Mod Password: Confirm password: More about domain controller options	•••••••	
	< Pr	evious Next > Install	Cancel

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

Figure 6-14 DHCP configuration 1

à.		Server Manager	_ 0 ×
Server M	lanager • Dashboard	🗸 😨 🍢 Manage Tools	View Help
Image: Server Image: Local Server Image: Local Servers Image: Local Servers	WELCOME TO SERVER MANAGE	Configuration required for DHCP Server at ECS- SHAREPOINT Complete DHCP configuration Task Details Add Tolles and TeatUres	
	3	Connect this server to cloud services	

16. Retain the default settings and click Next.

Figure 6-15 DHCP configuration 2

2	DHCP Post-Install configuration wizard	×
Authorization		
Description	Specify the credentials to be used to authorize this DHCP server in AD DS.	
Authorization Summary	 Use the following user's credentials User Name: 	
	O Use alternate credentials UserName: Specify	
	○ Skip AD authorization	
	< Previous Next > Commit	Cancel

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

6.2.3 Installing SQL Server

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

Figure 6-16 SQL Server installation center

1	SQL Server Installation Center	x
Planning	Hardware and Software Requirements	^
Installation	View the hardware and software requirements.	
Maintenance	E Security Documentation	
Tools	View the security documentation.	
Resources	Online Release Notes	=
Advanced	View the latest information about the release.	
Options	How to Get SQL Server Data Tools	
	SQL Server Data Tools provides an integrated environment for database developers to carry out all their database design work for any SQL Server platform.	
	ast System Configuration Checker	
	Launch a tool to check for conditions that prevent a successful SQL Server installation.	
	Install Upgrade Advisor	
	Upgrade Advisor analyzes any SQL Server 2012, SQL Server 2008 RZ, SQL Server 2008 or SQL Server 2005 components that are installed and identifies issues to fix either before or after you upgrade to SQL Server 2014.	
	Online Installation Help	
	Launch the online installation documentation.	
	How to Get Started with SQL Server 2014 Failover Clustering	
	Read instructions on how to get started with SQL Server 2014 failover clustering.	
	How to Get Started with a PowerPivot for SharePoint Standalone Server Installation	
Microsoft SQL Server 2014	Read instructions on how to install PowerPivot for SharePoint in the fewest possible steps on a new SharePoint 2010 server.	
		Y

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

3	SQL Server Installation Center
Planning Installation Maintenance Tools	New SQL Server stand-alone installation or add features to an existing installation Launch a wizard to install SQL Server 2014 in a non-clustered environment or to add features to an existing SQL Server 2014 instance. New SQL Server failover cluster installation Launch a wizard to install a single-node SQL Server 2014 failover cluster.
Resources Advanced Options	Ladinth a wizard to instant a single-flobe Sup Jerver 2014 failover cluster. Add node to a SQL Server failover cluster Launch a wizard to add a node to an existing SQL Server 2014 failover cluster. Upgrade from SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012 Launch a wizard to upgrade SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012 to SQL Server 2014.
Microsoft SQL Server 2014	

Figure 6-17 SQL Server installation options

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

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

Figure 6-18 SQL Server free edition

1	SQL Server 2014 Setup	x
Product Key Specify the edition of SQL Se	erver 2014 to install.	
Product Key License Terms Global Rules Microsoft Update Product Updates Install Stutp Files Install Rules Setup Role Feature Selection Feature Configuration Rules Ready to Install Installation Progress Complete	Validate this instance of SQL Server 2014 by entering the 25-character key from the Microsoft certificate of authenticity or product packaging. You can also specify a free edition of SQL Server, suc as Evaluation or Express. Evaluation has the largest set of SQL Server features, as documented in SQL Server Books Online, and is activated with a 180-day expiration. To upgrade from one edition to another, run the Edition Upgrade Wizard. © Specify a free edition: <u>Evaluation</u> C Enter the product key: <u>NQG3R-63HC8-XCRQH-MYVCH-333QR</u>	
	< Back Next > Cano	el

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

Figure 6-19 SQL Server license option

15	SQL Server 2014 Setup	
License Terms To install SQL Server 2014, yo	u must accept the Microsoft Software License Terms.	
Product Key License Terms Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Setup Role Feature Selection	MICROSOFT EVALUATION SOFTWARE LICENSE TERMS MICROSOFT SQL SERVER 2014 EVALUATION These license terms are an agreement between Microsoft Corporation live, one of its affiliates) and you. Please read them. They apply to the named above, which includes the media on which you received it, if an any Microsoft • updates,	evaluation software
Feature Rules Feature Configuration Rules Ready to Install Installation Progress Complete	Complement I accept the license terms. Turn on Customer Experience Improvement Program ("CEIP") and Error R quality, reliability and performance of Microsoft SQL Server 2014. See the Microsoft SQL Server 2014 Privacy Statement for more information. * Microsoft SQL Server 2014 also includes a Visual Studio component that w off by default. If Visual Studio is installed, this component will use the CEIP s	ill have CEIP settings turned
	< Back	Next > Cancel

- 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 6-20 SQL Server Feature Selection

5	SQL Server 2014 Setup	
Feature Selection	p install.	
Product Key License Terms Global Rules Microsoft Updates Install Setup Files Install Rules Setup Role Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration	Features: Instance Features Database Engine Services SQL Server Replication Full-Text and Semantic Extractions for: Data Quality Services Reporting Services - Native Shared Features Reporting Services - SharePointt Reporting Services - SharePointt Data Quality Client Other Tools Connectivity Integration Services Select All Unselect All Instance root directory: CC\Program Fill	Prerequisites for selected features: Already installed: Windows PowerShell 2.0 Microsoft_NET_Eramework 3.5 V
Distributed Replay Client Feature Configuration Rules Ready to Install	, <u> </u>	es\Microsoft SQL Server\ es (x86)\Microsoft SQL Server\
Ready to Install	< Ba	

7. Select **Default instance**.

Figure 6-21 SQL Server instance

1	SQL Se	erver 2014 S	etup		_ D X
Instance Configuration Specify the name and instance	ID for the instance of SQL Serv	er. Instance ID	pecomes part of	the installation path.	
Product Key License Terms Global Rules	Default instance Named instance:	MSSQLSERVE	R		
Microsoft Update Product Updates Install Setup Files Install Rules	Instance ID:	MSSQLSERVE	R		
Setup Role Feature Selection	SQL Server directory: Analysis Services directory:	C:\Program F	iles\Microsoft S	QL Server\MSSQL12.MS QL Server\MSAS12.MSS(QLSERVER
Feature Rules Instance Configuration Server Configuration	Reporting Services directory: Installed instances:				
Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Distributed Replay Controller Distributed Replay Client Feature Configuration Rules Ready to Install	Instance Name Instan	nce ID	Features	Edition	Version
			< Back	Next > Can	cel Help

- 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 6-22 SQL Server service accounts

3	SQL Server 201	4 Setup			
Server Configuration					
Specify the service accounts and	collation configuration.				
Product Key	Service Accounts Collation				
License Terms Global Rules	Microsoft recommends that you use	a separate account for each	SQL Server servic	e.	
Microsoft Update	Service	Account Name	Password	Startup Type	
Product Updates	SQL Server Agent	NT Service\SQLSERVERA		Manual	~
Install Setup Files	SQL Server Database Engine	NT AUTHORITY\NETW		Automatic	~
Install Rules	SQL Server Analysis Services	sp160\Administrator	•••••	Automatic	~
Setup Role	SQL Server Reporting Services	NT Service\ReportServer		Automatic	~
Feature Selection	SQL Server Integration Services 12.0	NT Service\MsDtsServer		Automatic	~
Feature Rules	SQL Server Distributed Replay Client	NT Service\SQL Server D		Manual	~
Instance Configuration	SQL Server Distributed Replay Con	NT Service\SQL Server D		Manual	~
Server Configuration	SQL Full-text Filter Daemon Launc	NT Service\MSSQLFDLa		Manual	
Database Engine Configuration	SQL Server Browser	NT AUTHORITY\LOCAL		Disabled	~
Analysis Services Configuration					
Reporting Services Configuration					
Distributed Replay Controller					
Distributed Replay Client					
Feature Configuration Rules					

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

Figure 6-23 SQL	Server administrator account 1	
*	SOL Server 2014 Setup	

1	SQL Server 2014 Setup			
Product Key	Server Configuration Data Directories FILESTREAM			
License Terms Global Rules	Specify the authentication mode and administrators for the Database Engine.			
Microsoft Update	Authentication Mode			
	Windows authentication mode			
License Terms Global Rules Microsoft Update Product Updates Install Scup Files Install Scup Files Install Rules Secify the authentication mode Install Rules Secify the authentication mode Micro Mode (SQL Server authentication and Windows authentication) Setup Role Feature Selection Feature Selection Feature Rules Instance Configuration Database Engine Configuration Analysis Services Configuration Distributed Replay Client Feature Gonfiguration Rules Ready to Install				
	uct Updates • Windows authentication mode • Mixed Mode (SQL Server authentication and Windows authentication) • Role • Specify the password for the SQL Server system administrator (sa) account. • re Selection • Enter password: • Enter password: • Confirm password: • Conf			
Specify Database Engine authentication security mode, administrators and data directories. Product Key License Terms Global Rules Microsoft Update Product Updates Install Rcup Files Install Rcup Files Install Rules Seture Selection Feature Selection Feature Rules Instance Configuration Database Engine Configuration Database Engine Configuration Distributed Replay Controller Distributed Replay Client Feature Configuration Reporting Services Configuration Distributed Replay Client Feature Configuration Distributed Replay Client Feature Configuration Secify SQL Server administrators Specify SQL Server administrators<				
Feature Rules	boduct Key server Configuration ball Rules crosoft Updates aduct Updates tall Setup Files tall Setup Files tall Rules tature Rules tature Rules tature Rules tature Configuration tabase Engine Configuration paysis Services Configuration paysis Services Configuration paysing Services Configuration paysing Services Configuration tarbueta Replay Client ature Configuration Rules			
-				
-	Specify SQL Server administrators			
	SP160\Administrator (Administrator) SQL Server	administrators		
Analysis Services Configuration	ver Configuration Data Directories FILESTREAM becify the authentication mode and administrators for the Database Engine. uthentication Mode Windows authentication mode Windows authentication mode Windows authentication mode Windows authentication) becify the password for the SQL Server authentication (sa) account. her password: becify SQL Server administrators P160VAdministrator (Administrator) SQL Server administrators have unrestricted access to the Database Engine.			
Specify Database Engine authentication security mode, administrators and data directories. Product Key License Terms Global Rules Global Rules Microsoft Updates Install Setup Files Install Rules Status Expire Configuration Reature Roling Services Configuration Distributed Replay Controller Distributed Replay Client Feature Configuration Rules Ready to Install				
Database Engine Configuration Specify Database Engine authentication security mode, administrators and data directories. Product Key License Terms Global Rules Microsoft Update Install Setup Files Install Setup Files Install Rules Seture Rules Instance Configuration Server Configuration Server Configuration Seture Rules Instance Configuration Database Engine Configuration Services Configuration Distributed Replay Clent Distributed Replay Controller Distributed Replay Controller Add Current User Add Remove				
Specify Database Engine authentication security mode, administrators and data directories. Product Key License Terms Global Rules Microsoft Update Product Updates Install Scup Files Install Stup Files Install Setup Files Install Rules Setup Role Feature Selection Feature Selection Feature Selection Sever Configuration Database Engine Configuration Database Engine Configuration Analysis Services Configuration Distributed Replay Cirent Feature Ray Configuration Reporting Services Configuration Reparting Services Configuration Distributed Replay Cirent Feature Rules Install Rules Specify SQL Server administrators Add Current User Add Remove				
Database Engine Configuration Specify Database Engine authentication security mode, administrators and data directories. Product Key License Terms Global Rules Microsoft Updates Install Setup Files Install Rules Seture Sole Feature Engine Configuration Server Configuration Server Configuration Setury Role Feature Rules Install Rules Server Configuration Database Engine Configuration Reporting Services Configuration Reporting Services Configuration Distributed Replay Client Feature Configuration Rules Ready to Install				
Database Engine Configuration Specify Database Engine authentication security mode, administrators and data directories. Product Key License Terms Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Seture Rules Feature Rules Install Rules Server Configuration Specify the password for the SQL Server system administrator (sa) account. Enter Configuration Patabase Engine Configuration Analysis Services Configuration Reporting Services Configuration Distributed Replay Client Feature Rules Reporting Services Configuration Reporting Services Configuration Distributed Replay Client Feature Configuration Rules Ready to Install				
	< Back Next > Cancel	Help		

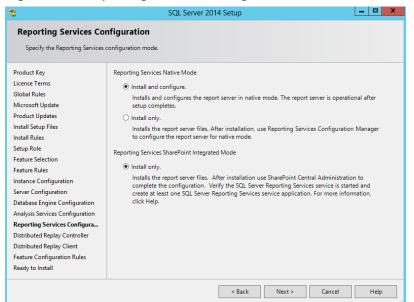
10. Click **Add Current User** to grant Analysis Services administrator permissions to the current account, and click **Next**.

Figure 6-24 SQL Server administrator account 2

	SQL Server 2014 Setup	
Analysis Services Confi	guration	
Specify Analysis Services server	modes, administrators, and data directories.	
Product Key	Server Configuration Data Directories	
License Terms	Server Mode:	
Global Rules	Multidimensional and Data Mining Mode	
Microsoft Update	Multidimensional and Data Mining Mode Tabular Mode	
Product Updates		
Install Setup Files	Specify which users have administrative permissions for Analysis Services.	
Install Rules	SP160\Administrator (Administrator)	Analysis Services
Setup Role		administrators have unrestricted access to
Feature Selection		Analysis Services.
Feature Rules		
Instance Configuration		
Server Configuration		
Database Engine Configuration		
Analysis Services Configuration		
Reporting Services Configuration		
Distributed Replay Controller		
Distributed Replay Client		
Feature Configuration Rules	Add Current User Add Remove	

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

Figure 6-25 Reporting Services Configuration



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

Figure 6-26 Distribution Replay Controller service

5	SQL Server 2014 Setup	
Distributed Replay Co	ntroller	
Specify Distributed Replay Con	troller service access permissions.	
Product Key	Specify which users have permissions for the Distributed Replay Controller se	ervice.
License Terms	SP160\Administrator (Administrator)	Users that have been
Global Rules		granted permission will have
Microsoft Update		unlimited access to the
Product Updates		Distributed Replay Controller service.
Install Setup Files		
Install Rules		
Setup Role		
Feature Selection		
Feature Rules		
Instance Configuration		
Server Configuration		
Database Engine Configuration		
Analysis Services Configuration		
Reporting Services Configuration		
Distributed Replay Controller		
Distributed Replay Client		
Feature Configuration Rules		
Ready to Install	Add Current User Add Remove	
	< Back Next >	Cancel Help

13. Confirm SQL Server configurations and click Install.

5	SQL Server 2014 Setup	
Ready to Install		
Verify the SQL Server 2014 fea	tures to be installed.	
Product Key	Ready to install SQL Server 2014:	
License Terms	- Summary	
Global Rules	- Edition: Evaluation	1
Microsoft Update	Action: Install (Product Update)	
Product Updates	Prerequisites	- 1
Install Setup Files	Already installed: Windows PowerShell 2.0	
Install Rules		
Setup Role	Microsoft .NET Framework 4.0	
Feature Selection	□ To be installed from media:	
Feature Bules	Microsoft Visual Studio 2010 Redistributables	
Instance Configuration	Microsoft Visual Studio 2010 Shell	
-	Microsoft Visual Studio Tools for Applications 3.0	
Server Configuration	General Configuration	
Database Engine Configuration	Database Engine Services	
Analysis Services Configuration		
Reporting Services Configuration	Full-Text and Semantic Extractions for Search	-
Distributed Replay Controller	C Data Quality Servicer	>
Distributed Replay Client	Configuration file path:	
Feature Configuration Rules		
	C:\Program Files\Microsoft SQL Server\120\Setup Bootstrap\Log\20180703_202844\ConfigurationFile	ini

Figure 6-27 SQL Server installation

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

Figure 6-28 Finish SQL Server installation

6	SQL Server 2014 Setu	p 📃 🗖 🗴
Complete Your SOL Server 2014 installati	ion completed successfully with product updates.	
	, ,	
Product Key	Information about the Setup operation or possil	ple next steps:
License Terms	Feature	Status
Global Rules	Management Tools - Complete	Succeeded
Microsoft Update	Client Tools Connectivity	Succeeded –
Product Updates	Client Tools SDK	Succeeded
Install Setup Files	Client Tools Backwards Compatibility	Succeeded
Install Rules	Management Tools - Basic	Succeeded
Setup Role	Reporting Services - Native	Succeeded
Feature Selection		
Feature Rules	Details:	
	Details:	
Instance Configuration	Viewing Product Documentation for SQ	Server ^
Server Configuration	Only the components that you use to view of	and manage the documentation for SQL Server have
Database Engine Configuration		component uses the online library. After installing
Analysis Services Configuration	SQL Server, you can use the Help Library N	lanager component to download documentation to
Reporting Services Configuration		see Use Microsoft Books Online for SQL Server
Distributed Replay Controller	(<http: ?linkid="29</td" fwlink="" go.microsoft.com=""><td><u>9578></u>).</td></http:>	<u>9578></u>).
Distributed Replay Client	Summary log file has been saved to the followin	g location:
Feature Configuration Rules	C:\Program Files\Microsoft SQL Server\120\Setu	- un Bootstran) og\ 20180703_202844
Ready to Install	Summary sp16 20180703 202844.txt	19 0003009/20100103 202044
incody to instan		
		Close Help

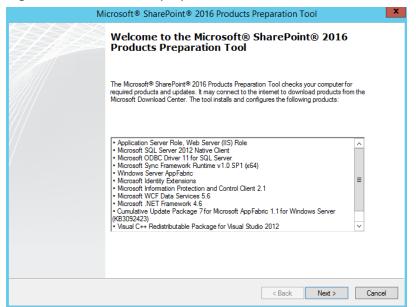
6.2.4 Installing Microsoft SharePoint Server 2016

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

inguit 0 25	ShareFoint prepar				
🖾 l 💽 🔝 = l	Application Tools	DVD Drive (D:) 16.	0.4351.1000	_ _ ×	
File Home Share	View Manage			^	?
Copy Paste X Cut Copy Paste Paste sho	Move Conv Delete Rename	New item *	Properties	Select all Select none	1
Clipboard	Organize	New	Open	Select	
🔄 💿 🝷 🕇 🔛 🕨 Tł	nis PC + DVD Drive (D:) 16.0.4351.1000	~	C Search DVD Drive	e (D:) 16.0.435 🔎	
🛠 Favorites	Name	Date modified	Туре	Size	^
Desktop	🗟 api-ms-win-crt-locale-l1-1-0.dll	7/30/2015 5:30	Application extens	19 KB	
Downloads	🗟 api-ms-win-crt-math-I1-1-0.dll	7/30/2015 5:30	Application extens	28 KB	
Recent places	🗟 api-ms-win-crt-runtime-I1-1-0.dll	7/30/2015 5:30	Application extens	23 KB	
	🗟 api-ms-win-crt-stdio-l1-1-0.dll	7/30/2015 5:30	Application extens	25 KB	
🌉 This PC	🚳 api-ms-win-crt-string-l1-1-0.dll	7/30/2015 5:30	Application extens	25 KB	
膧 Desktop	🖾 autorun	5/29/2015 3:05	ICO File	2 KB	L
Documents	autorun	5/29/2015 3:05	Setup Information	1 KB	
🐌 Downloads	🖻 default	11/24/2015 17:22	HTA File	14 KB	
🜗 Music	prerequisiteinstaller	2/11/2016 2:13	Application	973 KB	
📔 Pictures	🖃 readme	9/24/2015 5:28	HTM File	1 KB	
Videos	🚳 setup	5/29/2015 3:05	Windows Comma	1 KB	=
🊢 Local Disk (C:)	🚳 setup.dll	11/26/2015 0:29	Application extens	763 KB	
💹 DVD Drive (D:) 16.0.4		7/31/2015 22:05	Application	257 KB	
	splash	7/30/2015 14:27	HTA File	3 KB	
👊 Network	🚳 svrsetup.dll	2/11/2016 2:13	Application extens	12,959 KB	
	🚳 ucrtbase.dll	7/30/2015 5:30	Application extens	960 KB	
	🚳 vcruntime140.dll	7/30/2015 5:30	Application extens	87 KB	~
27 items 1 item selected	972 KB			8== 8	-

Figure 6-29 SharePoint preparation tool

- 2. Open the installation wizard of the SharePoint preparation tool and click **Next**.
 - Figure 6-30 SharePoint preparation tool installation wizard

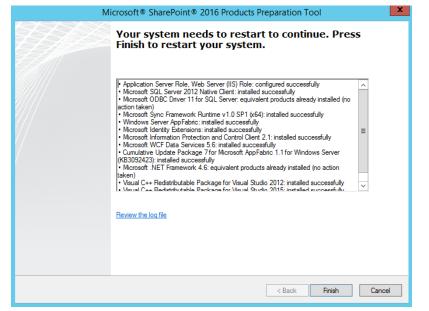


3. Select I accept the terms of the License Agreement(s) and click Next.

Microsoft® SharePoir	nt® 2016 Products Preparation Tool
cense Terms for software products. This solution requires that you install each of the follo review the license terms.	owing software modules and agree to their license terms. Please
MICROSOFT SOFTWARE LICENSE TERM	MS
Below are two sets of Licen	se Terms that cover twelve different
Microsoft products. The products	ducts covered by these license terms
are:	
LICENSE 1	
Microsoft Windows Management Fr	ramework 3.0
LICENSE 2	
	<u> </u>
Be sure to carefully read and understand all of the rigit the EULA before the products can be downloaded ar	hts and restrictions described in the EULA. You must accept the terms of nd installed on your computer.
I have used surdensheed and save discharge of a	الم
I have read, understood, and agreed to the terms of t terms of the License Agreement(s)" and using these p	the End User License Agreement(s) and so signify by clicking "I accept the products.
▼ I accept the terms of the License Agreement(s)	1
I accept the terms of the License Agreement(s)	

- CULUR HUNLY CONTOUR
- 4. After the preparation tool is installed, click **Finish** to restart the system.

Figure 6-32 Successful preparation tool installation



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

Figure 6-33 Installing SharePoint

a I 🕞 🐘 = I		Application Tools		DVD Drive (D:) 16.	0.4351.1000	_ □	x
File Home Sha	are View	Manage					^ (
Copy Paste	Mov		Rename	New item * New folder	Properties	Select all Select none	-
Clipboard		Organize		New	Open	Select	
• 🖻 🔹 🕈 💽	This PC + DV	D Drive (D:) 16.0.435	1.1000	Ý	C Search DVD Driv	re (D:) 16.0.435	P,
☆ Favorites	Name	•		Date modified	Туре	Size	[
Desktop	🚳 api-ms	-win-crt-locale-I1-1	-0.dll	7/30/2015 5:30	Application extens	19 KB	
Downloads	🚳 api-ms	-win-crt-math-I1-1	-0.dll	7/30/2015 5:30	Application extens	28 KB	
📃 Recent places	🚳 api-ms	-win-crt-runtime-I1	-1-0.dll	7/30/2015 5:30	Application extens	23 KB	
	🚳 api-ms	-win-crt-stdio-I1-1-	0.dll	7/30/2015 5:30	Application extens	25 KB	
🖳 This PC	🚳 api-ms	-win-crt-string-I1-1	-0.dll	7/30/2015 5:30	Application extens	25 KB	
📔 Desktop 🗉	autorui 🔝	n		5/29/2015 3:05	ICO File	2 KB	
Documents	autorui	n		5/29/2015 3:05	Setup Information	1 KB	
Downloads	📄 default			11/24/2015 17:22	HTA File	14 KB	
Music	🚡 prerequ	usiteinstaller		2/11/2016 2:13	Application	973 KB	
📔 Pictures	readme	:		9/24/2015 5:28	HTM File	1 KB	
Videos	🚳 setup			5/29/2015 3:05	Windows Comma	1 KB	
🚢 Local Disk (C:)	setup.c			11/26/2015 0:29	Application extens	763 KB	
DVD Drive (D:) 1	🚺 setup			7/31/2015 22:05	Application	257 KB	
퉬 catalog	🖻 splash			7/30/2015 14:27	HTA File	3 KB	
퉬 files	🚳 svrsetu	p.dll		2/11/2016 2:13	Application extens	12,959 KB	
퉬 global	🚳 ucrtbas	e.dll		7/30/2015 5:30	Application extens	960 KB	
퉬 prerequisitein 🗸	🗸 🚳 vcrunti	me140.dll		7/30/2015 5:30	Application extens	87 KB	
27 items 1 item select	ted 256 KB					8	

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

Figure 6-34 SharePoint product key

5	Microsoft SharePoint Server 2016 Trial	x
P	Enter your Product Key	Ø
	Need to find your Product Key? Your Product Key is 25 characters and is typically found in your product packaging. If you cannot find your Product Key, click the "Learn more about Product Keys and see examples" link. Learn more about Product Keys and see examples	
	NQGJR-63HC8-XCRQH-MYVCH-3J3QR	

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

Microsoft SharePoint Server 2016 Trial Read the Microsoft Software License Terms To continue you must accept the terms of this agreement. If you do not want to accept the Microsoft Software License Terms, close this window to cancel the installation. This installation contains the following software, the license terms of each of which are included below, respectively: 1. Microsoft Project Server 2016 2. Microsoft Project Server 2016 Scroll down to read these license terms. #1 MICROSOFT EVALUATION SOFTWARE LICENSE TERMS MICROSOFT SHAREPOINT SERVER 2016 Below are two separate sets of terms for Microsoft SharePoint Server 2016. Only one set of the Microsoft SharePoint Server 2016 terms applies to you. Your product key will determine which terms apply to you. If you have	
To continue you must accept the terms of this agreement. If you do not want to accept the Microsoft Software License Terms, close this window to cancel the installation. This installation contains the following software, the license terms of each of which are included below, respectively: 1. Microsoft SharePoint Server 2016 Scroll down to read these license terms. #1 MICROSOFT EVALUATION SOFTWARE LICENSE TERMS MICROSOFT SHAREPOINT SERVER 2016 Below are two separate sets of terms for Microsoft SharePoint Server 2016. Only one set of the Microsoft SharePoint Server 2016 terms applies to	
the Microsoft Software License Terms, close this window to cancel the installation. This installation contains the following software, the license terms of each of which are included below, respectively: 1. Microsoft SharePoint Server 2016 2. Microsoft Project Server 2016 Scroll down to read these license terms. #1 MICROSOFT EVALUATION SOFTWARE LICENSE TERMS MICROSOFT SHAREPOINT SERVER 2016 Below are two separate sets of terms for Microsoft SharePoint Server 2016. Only one set of the Microsoft SharePoint Server 2016 terms applies to	0
of which are included below, respectively: 1. Microsoft SharePoint Server 2016 2. Microsoft Project Server 2016 Scroll down to read these license terms. #1 MICROSOFT EVALUATION SOFTWARE LICENSE TERMS MICROSOFT SHAREPOINT SERVER 2016 Below are two separate sets of terms for Microsoft SharePoint Server 2016. Only one set of the Microsoft SharePoint Server 2016 terms applies to	
 Microsoft Project Server 2016 Scroll down to read these license terms. #1 MICROSOFT EVALUATION SOFTWARE LICENSE TERMS MICROSOFT SHAREPOINT SERVER 2016 Below are two separate sets of terms for Microsoft SharePoint Server 2016. Only one set of the Microsoft SharePoint Server 2016 terms applies to 	
#1 MICROSOFT EVALUATION SOFTWARE LICENSE TERMS MICROSOFT SHAREPOINT SERVER 2016 Below are two separate sets of terms for Microsoft SharePoint Server 2016. Only one set of the Microsoft SharePoint Server 2016 terms applies to	
MICROSOFT SHAREPOINT SERVER 2016 Below are two separate sets of terms for Microsoft SharePoint Server 2016. Only one set of the Microsoft SharePoint Server 2016 terms applies to	
Below are two separate sets of terms for Microsoft SharePoint Server 2016. Only one set of the Microsoft SharePoint Server 2016 terms applies to	
you. Your product key will determine which terms apply to you. If you have	
a Trial product key, then the Trial Terms below apply to you. If you do not have a Trial Product key, then the following Notice applies to you:	
NOTICE Your use of this software is subject to the terms and conditions of the license agreement by which you acquire this software. For instance, if you	
are:	
a volume license customer, use of this software is subject to your volume license agreement.	
A SDN customer use of this software is subject to the MSDN	

Figure 6-35 SharePoint license terms

8. Retain the default installation paths.

Figure 6-3	36 SharePoint	installation paths
------------	---------------	--------------------

5		Microsoft SharePoint Server 2016 Trial	X
	<u>F</u> ile Locatio	n	
		Choose a file location	0
		Microsoft SharePoint Server 2016 will be installed on your computer. To install this product in a different location, click Browse, and then select the location.	
		C:\Program Files\Microsoft Office Servers <u>B</u> rowse	
		If you intend to use this computer as a search server, the search index files will be stored on the local hard drive. These files can be very large, so ensure that there is sufficient free space on the selected drive. To change where Microsoft SharePoint Server 2016 will store its search index files, click Browse, and then select the location.	
		C:\Program Files\Microsoft Office Servers\16.0\Data	
		insta	I Now

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

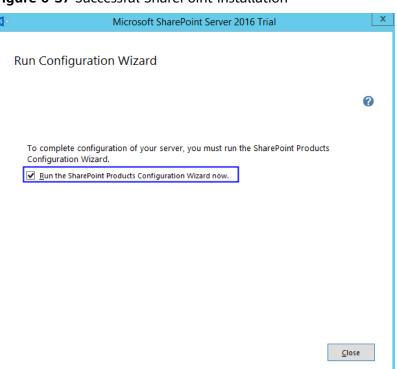
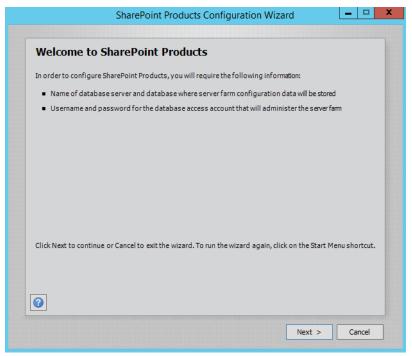


Figure 6-37 Successful SharePoint installation

6.2.5 Configuring Microsoft SharePoint Server 2016

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

Figure 6-38 SharePoint Products	Configuration Wizard
---------------------------------	-----------------------------



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

	e to SharePoint Products	
	database server and database where server farm configuration data will be stored	
 Upperson 	SharePoint Products Configuration Wizard	
d Click N	The following services may have to be started or reset during configuration: Internet Information Services SharePoint Administration Service SharePoint Timer Service Choose yes to restart the services if required and continue with the configuration wizard or no to exit the configuration wizard.	tcut.
0	Yes No	

Figure 6-39 Service restart prompt

3. Select Create a new server farm.

Figure 6-40 Creating a new server farm

		farm			
A server fa connect to	m is a collection of tw an existing server far	vo or more computers tha m?	t share configuration	data. Do you wa	intto
0	Connect to an existing	g server farm			
۲	Create a new server f	farm			
0					

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

SharePoint	Products Configuration Wizard
Specify Configuration Da	ntabase Settings
name. If the database does not exist, it v	configuration database. Type the database server and database will be created. To reuse an existing database, the database must be ding database server security configuration and network access
Database server:	
Database name:	SharePoint_Config
Specify Database Access Acco	unt
Select an existing Windows account that	this machine will always use to connect to the configuration
database. If your configuration databas	e is hosted on another server, you must specify a domain account.
· · ·	e is hosted on another server, you must specify a domain account.
Type the username in the form DOMAIN	e is hosted on another server, you must specify a domain account. User_Name and password for the account.
Type the username in the form DOMAIN Username:	e is hosted on another server, you must specify a domain account. User_Name and password for the account.
Type the username in the form DOMAIN Username:	e is hosted on another server, you must specify a domain account. User_Name and password for the account.
Type the username in the form DOMAIN	e is hosted on another server, you must specify a domain account. User_Name and password for the account.
Type the username in the form DOMAIN	e is hosted on another server, you must specify a domain account. User_Name and password for the account.
Type the username in the form DOMAIN Username: Password:	e is hosted on another server, you must specify a domain account. User_Name and password for the account.

Figure 6-41 Configuring the SharePoint database

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

Figure 6-42 Setting the password for the SharePoint server farm

	arePoint Products farm. This passphrase is used to secure farm Ich server that joins the farm. The passphrase can be changed af
the farm is configured.	
Passphrase:	•••••
Confirm passphrase:	•••••

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

Specify Server Role	
Select the role for this server in the s nore about server farm topology.	erver farm. The role determines which services run on this server. <u>Lea</u>
Multiple-Server Farm	Server Role Description
Front-end	Service applications, services, and components that serve user requests belong on front-end web servers. These
O Application	servers are optimized for fast performance.
 Distributed Cade 	
○ Search	
○ Custom	
- Single-Server Farm	
O Single-Server Farm	

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

Figure 6-44 Port number of SharePoint Central Administration Web Application

	SharePoint Produ	cts Configuration W	'izard	
Configure Sh	arePoint Centra	Administration	Web Applic	ation
farm. The first server web application host	Administration Web Applic added to a server farm mus ed on this machine, check t port number, a random one	t host this web application he box below and type a m	n. To specify a port	numberforthe
Specify po	ort number: 10000			
Configure Secur	ity Settings			
requires special conf	mended security configura guration by the domain ad unt and the default domain	ministrator. NTLM authenti	cation will work with	
Choose an authentica	tion provider for this Web	Application.		
NTLM				
O Negotiate	(Kerberos)			
0				
		< Back	Next >	Cancel

8. Check and confirm the SharePoint configurations.

SharePoint Products Conf	iguration Wiza	rd	
Completing the SharePoint Products	s Configurat	ion Wizar	d
The following configuration settings will be applied:			
Configuration Database Server	SP 16		
Configuration Database Name	SharePoi	nt_Config	=
Host the Central Administration Web Application	yes		
Central Administration URL	http://sp	16:10000/	
Authentication provider	NTLM		
Local Server Role	Front-en	ł	
ick Next to apply configuration settings.			
Advanced Settings			
]			
	< Back	Next >	Cance

Figure 6-45 SharePoint configurations

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

Figure 6-46 Configuration progress

SharePoint Products Configuration Wizard	ا <u>بنا با</u>
Configuring SharePoint Products	
Please wait while SharePoint Products are configured.	
Performing configuration task 3 of 10	
Creating the configuration database	
0	

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

	tion Wizard 🛛 🗖 🗖
Configuration Successful	
he following configuration settings were successfully applied:	
Configuration Database Server	SP 16
 Configuration Database Name 	SharePoint_Config
 Host the Central Administration Web Application 	yes
Central Administration URL	http://sp16:10000/
Authentication provider	NTLM
Local Server Role	Front-end
lick Finish to close this wizard and launch the SharePoint Central Ac onfiguring your SharePoint installation. The users may be prompted the form DOMAIN(User_Name and password to access the site. A ou used to logon to this computer. Add this site to the list of truste	ed by their web browser for the usernam At that prompt, enter the credentials tha
٥	

<u>م</u> ، ، c٠ Fi C I CI . •

6.2.6 Verifying Microsoft SharePoint Server 2016

1. Open the SharePoint central administration.

<	http://sp16:10000/_admin/admin 🍳 🕆 🖒 🚺 Initial	Farm Configuration ×	h ★ Ø
Central Adi Applica Monito Backup Security Upgrad General Setting Apps	Help Make SharePoint Better Do you want to help make SharePoint better? You can help make SharePoint better by signing up for the Customer Experince Improvement Program and automatically sending error reports to Microsoft.	Sign up for the Customer Experience Improvement Program and automatically upload error reports to Microsoft O Yes, I am willing to participate (Recommended). O No, I don't wish to participate.	icount SHARE (C) Wizard
Office 36	5 ation Wizards		

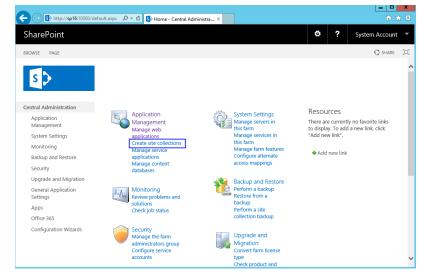
Figure 6-48 SharePoint central administration

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

Figure 6-49 SharePoint farm configuration 10 × 😔 🚯 http://sp16:10000/_admin/admin 🔎 🕈 🖒 🚯 Initial Farm Configuration ... 🗴 SharePoint ₿? System Account 🗘 SHARE [[]] s 🗦 Welcome 🛛 Central Administration How do you want to configure your SharePoint farm? Application Management Yes, walk me through the configuration of my farm using this wizard. Start the Wizard This wizard will help with the initial configuration of your SharePoint farm. You can select the services to use in this farm and create your first site. System Settings Monitoring Backup and Restore You can launch this wizard again from the Configuration Wizards page in the Central Administration site. No, I will configure everything myself. Security Cancel Upgrade and Migration General Application Settings Apps Office 365 Configuration Wizards

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

Figure 6-50 Creating a SharePoint site



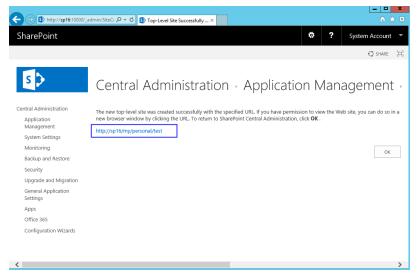
4. Set SharePoint site parameters.

narePoint		🛱 ? Svs	tem Accou
		••••••••••••••••••••••••••••••••••••••	
			🗘 shar
Management	Web Application		
System Settings	Select a web application.	Web Application: http://sp16/ -	
Monitoring			
Backup and Restore	To create a new web application go to New Web Application page.		
Security			
Upgrade and Migration	Title and Description	1974)	
General Application	Type a title and description for your	Title:	
Settings	new site. The title will be displayed on each page in the site.	Description:	
Apps		example	
Office 365		example	
Configuration Wizards			
	Web Site Address		
	Specify the URL name and URL path	URL: http://sp16 /my/personal/	
	to create a new site, or choose to create a site at a specific path.	http://spie/my/personal/	
	To add a new URL Path go to the Define Managed Paths page.		
	Denne manageo Patris page.		
	Template Selection		

Figure 6-51 Setting SharePoint site parameters

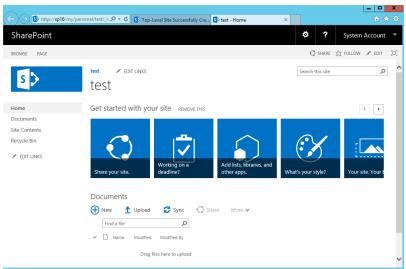
5. The SharePoint top-level site is created successfully. Click the link to open the page.

Figure 6-52 SharePoint top-level site created successfully



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

Figure 6-53 SharePoint verification



6.3 Deploying Docker

6.3.1 Manually Deploying Docker (CentOS 7.5)

Overview

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

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	Images become containers at runtime, that is, containers are created from images. A container can be created, started, stopped, deleted, and suspended.

Table	6-5	Docker	termino	loaies
	•••	Docker		i gies

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 64bit (40 GiB) 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**.
- The rule listed in the following table has been added to the security group which the target ECS belongs to. For details, see Adding a Security Group Rule.

Directi on	Priori ty	Action	Туре	Protocol & Port	Source Address
Inboun d	1	Allow	IPv4	TCP: 80	0.0.0.0/0

Table 6-6 Security group rule

Deploying Docker

- 1. Log in to the ECS.
- 2. To obtain and update the system and software, update the image source to a Huawei Cloud image source. For details, see How Can I Use an EPEL Image Source (x86_64 or Arm) Provided by Huawei Cloud?
- 3. Add a yum repository.

yum install epel-release -y

yum clean all

4. Install yum-utils.

yum install -y yum-utils device-mapper-persistent-data lvm2

5. Configure the yum repository for Docker.

yum-config-manager --add-repo https://download.docker.com/linux/ centos/docker-ce.repo

6. Install and run Docker.

yum -y install docker-ce

systemctl enable docker

systemctl start docker

7. Check the installation.

docker --version

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

Docker version 26.1.4, build 5650f9b

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

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".

D 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:

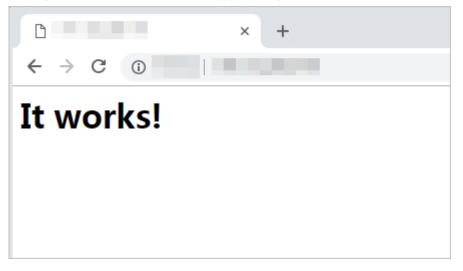
[[]root@ecs-b67a-docker ~]# docker run -it -d -p 80:80 --name datahttpd -v /data/:/var/www/httpd/ httpd 6a514dea52a9465c1f6863c0f17ff41debda231ccff8bf66e3c0dbcc5f33cb20 [root@ecs-b67a-docker ~]#

b. Check whether the container has been started.

docker ps -a

NAMES	PORTS	STATUS	CREATED	COMMAND	ocker ~]# docker ps · IMAGE	CONTAINER ID
INFIGUE D	FORID	JINIUJ	CREATED	COPIEIMIND	THROE	CONTRINER ID
p datahttp	0.0.0.0:80->80/tcp	Up 4 minutes	4 minutes ago	"httpd-foreground"	httpd	6a514dea52a9
p:	0.0.0.0:80->80/tcp	Up 4 minutes	4 minutes ago	"httpd-foreground"		6a514dea52a9 [root@ecs-b67a-d

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 customize 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://docs.docker.com**):

- FROM statement (mandatory): 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 with the message "Hello, Docker!" 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

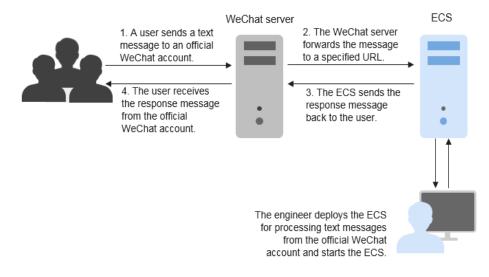
REPOSITORY TAG nginx v3 IMAGE ID CREATED 09422e465d96 10 seconds ago SIZE 109 MB

6.4 Deploying an ECS for Handling 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 6-54 shows the service flow.

Figure 6-54 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 do not have an account, **sign up for a HUAWEI ID and enable Huawei Cloud services**.

This section uses an ECS running CentOS 7.4 as an example.

Figure 6-55 Public images



• Purchase an EIP.

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

Figure 6-56 EIP

Public Network Access		
EIP 💿		
Auto assign Use existing Not required		
EIP Type ⑦		
Dynamic BGP Static BGP		
Greater than or equal to 99.95% service availability rate		
Billed By ③		
Bandwidth 📫 For heavy/stable traffic	For light/sharply fluctuating traffic	Shared bandwidth For staggered peak hours
Billed based on usage duration and bandwidth size.		
Bandwidth Size		
1 2 5 10 1	00 200 Custom	
Anti-DDoS protection ⑦ Free		

 The image source has been updated to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)? This facilitates obtaining and updating the system and software.

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 old to use. You are advised to upgrade it to Python 3.

1. Run the following command to view the Python version:

python --version

Figure 6-57 Viewing the Python version



- Download the Python installation package, for example, Python 3.6.0.
 wget https://www.python.org/ftp/python/3.6.0/Python-3.6.0a1.tar.xz
 - Figure 6-58 Downloading the Python installation package



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

cd Python-3.6.0a1

./configure

 If information similar to the following is displayed, the command has been successfully executed.

Figure 6-59 Successful execution

```
configure: creating ./config.status
config.status: creating Makefile.pre
config.status: creating Modules/Setup.config
config.status: creating Misc/python.pc
config.status: creating Misc/python-config.sh
config.status: creating Modules/ld_so_aix
config.status: creating pyconfig.h
creating Modules/Setup
creating Modules/Setup.local
creating Makefile
```

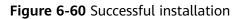
- If the message "configure: error: no acceptable C compiler found in \$PATH" is displayed, no proper compiler has been installed.

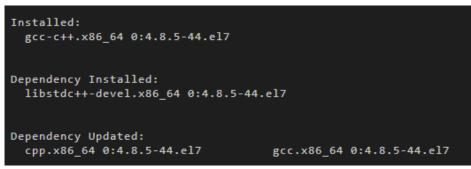
Solution:

Run the following command to install or upgrade GCC and its dependent packages:

sudo yum install gcc-c++

Enter **y** and press **Enter** as prompted. If information shown in **Figure 6-60** is displayed, the dependency packages have been installed.





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 openssldevel package is unavailable. Ignore the error.

Figure 6-61 Successful execution



Run the following command to view the Python 3 version:
 python3 --version

Figure 6-62 Viewing the Python 3 version



7. Run the following command to verify the Python 3 installation:

python3

If information shown in the following figure is displayed, Python 3 has been installed.

Figure 6-63 Successful installation

```
[root@ecs- Python-3.6.0a1]# python3
Python 3.6.0a1 (default, Dec 18 2020, 15:45:57)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-44)] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

NOTE

Before performing subsequent operations, exit the Python CLI by running any of the following commands and press **Enter**:

- Ctrl+Z
- exit()
- quit()

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 Python 3, but the version is too old to use. Upgrade pip to the latest version. During Python 3 installation, the error message "Ignoring ensurepip failure: pip 8.1.1 requires SSL/TLS" indicates a pip installation failure, so pip must be reinstalled.

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

yum install openssl-devel -y

Figure 6-64 Installing the openssl-devel package

2. Run the following command to install pip:

make && make install

If information shown in the following figure is displayed, pip has been installed.

Figure 6-65 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 6-66 Successful upgrade

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 6-67 Installing Web.py

<pre>[root@ecs-c438 Python-3.6.0a1]# pip3 install web.py==0.40.dev0</pre>
Collecting web.py==0.40.dev0
Downloading web.py-0.40.dev0.tar.gz (116 kB)
116 kB 76 kB/s
Using legacy 'setup.py install' for web.py, since package 'wheel'
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.

Download WinSCP from https://winscp.net/eng/index.php.

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 Create the **templates** folder and the **reply_text.xml** file in the folder. Then, 4. 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.

	100 1001	100000000000000000000000000000000000000		
2018/04/21	14:31	<dir></dir>		
2018/04/21	14:31	<dir></dir>		
2018/04/20	13:42		2,077	handle.py
2018/04/11	23:13		211	main.py
2018/04/19	23:46		2,008	receive.py
2018/04/20	13:41	<dir></dir>		templates
				compreteoo
D:\workspa 2018/04/20	13:41	xtProcess <dir></dir>	\templa	
D:\workspa		xtProcess	\templa	

Figure 6-68 Local file

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

Figure 6-69 Uploading files

[root@ecs-t	te	st1-0	001 w	x]# 1	s -11	R		
total 16								
-rw-rr	1	root	root	2077	Apr	20	13:42	handle.py
-rw-rr	1	root	root	211	Apr	11	23:13	main.py
-rw-rr	1	root	root	2008	Apr	19	23:46	receive.py
drwxr-xr-x	2	root	root	4096	May	7	22:40	
./templates	3:							
total 4								
-rw-rr	1	root	root	275	Apr	20	13:14	reply_text.xml

Starting the Service

Run the following command to start the service:

python3 main.py 80

If the command output shown in **Figure 6-70** is displayed, the service has been started.

Figure 6-70 Successful service startup

```
[root@ecs-test1-0001 wx] # python3 main.py 80
http://0.0.0.0:80/
```

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: https://*EIP bound to the ECS*/wx. 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.

6.5 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 which the target ECS belongs to. For details, see Adding a Security Group Rule.

Directi on	Priori ty	Action	Туре	Protocol & Port	Source Address
Inboun d	1	Allow	IPv4	TCP: 80	0.0.0.0/0

 Table 6-7
 Security group rule

Procedure

Step 1 Install the dependency package.

- 1. Log in to the ECS.
- The image source has been updated to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)? This facilitates obtaining and updating the system and software.
- 3. Run the following command to install the dependency packages: sudo yum install -y curl policycoreutils-python openssh-server

4. 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

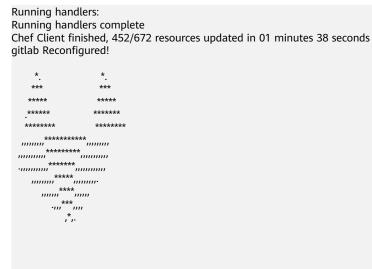
2. Run the following command to install GitLab:

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





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.

Please create a password for your new account.			
GitLab Enterprise Edition	Change your password		
Open source software to collaborate on code	New password		
Manage Git repositories with fine-grained access controls that keep your code secure. Perform code reviews and enhance collaboration with merge requests. Each project can also have an issue tracker and a wiki.	Confirm new password		
	Change your password		
	Didn't receive a confirmation email? Request a new one		
	Already have login and password? Sign in		

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

----End

6.6 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 which the target ECS belongs to. For details, see **Adding a Security Group Rule**.

Directio n	Priori ty	Action	Туре	Protocol & Port	Source Address
Inbound	1	Allow	IPv4	TCP: 5672	0.0.0/0
Inbound	1	Allow	IPv4	TCP: 15672	0.0.0/0

 Table 6-8 Security group rule

Procedure

Step 1 Install the dependency package and perl.

- 1. Log in to the target ECS.
- The image source has been updated to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)? This facilitates obtaining and updating the system and software.
- Run the following command to install the dependency packages: yum -y install make gcc gcc-c++ m4 ncurses-devel openssl-devel unixODBC-devel
- 4. Run the following command to install perl:

yum install perl

Step 2 Install Erlang.

For details, see Erlang Packages Download.

1. Run the following commands to add **Erlang Solutions repository** to your system:

wget https://packages.erlang-solutions.com/erlangsolutions-2.0-1.noarch.rpm

rpm -Uvh erlang-solutions-2.0-1.noarch.rpm

Alternatively, add the repository entry manually.

rpm --import https://packages.erlang-solutions.com/rpm/ erlang_solutions.asc

2. In the **/etc/yum.repos.d/** directory, create a file named **rabbitmq-erlang.repo**, and add the following to the file:

cd /etc/yum.repos.d/

vi rabbitmq-erlang.repo

```
[erlang-solutions]
name=CentOS $releasever - $basearch - Erlang Solutions
baseurl=https://packages.erlang-solutions.com/rpm/centos/$releasever/$basearch
gpgcheck=1
gpgkey=https://packages.erlang-solutions.com/rpm/erlang_solutions.asc
enabled=1
```

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

3. Run the following command to install Erlang:

sudo yum install erlang

Run the following command to install esl-erlang:

sudo yum install esl-erlang

4. 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-rabbitmg ~]# erl -version

```
Erlang (SMP,ASYNC_THREADS,HIPE) (BEAM) emulator version 11.1.7
```

Step 3 Install RabbitMQ.

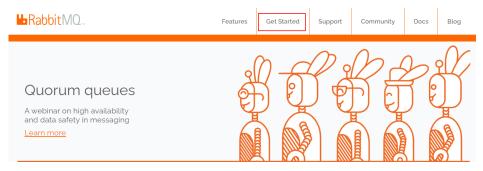
1. Run the following command to go to the home directory:

cd

2. Perform the following steps to download the RabbitMQ installation package:

- a. Open RabbitMQ.
- b. Click Get Started.

Figure 6-71 Get Started



c. Click **Download+Installation**.

Figure 6-72 Download+Installation

	Get Started	
Download + Installation Servers and clients for popular operating systems and languages		RabbitMQ Tutorials Hands-on examples to get you started with RabbitMQ

d. Select a download address based on the ECS OS. Here, the CentOS 7.x is used as an example.

Figure 6-73 Selecting a download address

Downloads on GitHub

- <u>Windows installer</u>
- <u>Debian, Ubuntu</u>
- RHEL/CentOS 8.x | RHEL/CentOS 7.x | RHEL/CentOS 6.x | OpenSUSE | SLES 11.x | Erlang RPM
- Generic UNIX binary
- Windows binary
- e. Run the following command to download the RabbitMQ installation package.

For example, the download address in **Step 3.2.d** is as follows:

https://github.com/rabbitmq/rabbitmq-server/releases/download/ v3.8.12/rabbitmq-server-3.8.12-1.el7.noarch.rpm

Run the following command:

wget https://github.com/rabbitmq/rabbitmq-server/releases/ download/v3.8.12/rabbitmq-server-3.8.12-1.el7.noarch.rpm

If the message **Unable to establish SSL connection.** is displayed during the download,

you can add **--no-check-certificate** to the end of the wget command and repeat it for several times for download.

For example:

wget https://github.com/rabbitmq/rabbitmq-server/releases/ download/v3.8.12/rabbitmq-server-3.8.12-1.el7.noarch.rpm --nocheck-certificate

- f. Run the following command to install the RabbitMQ installation package: yum install rabbitmq-server-3.8.12-1.el7.noarch.rpm
- 3. Start the RabbitMQ after it is installed. service rabbitmq-server start
- 4. Check the RabbitMQ status.

service rabbitmq-server status

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 Enabling plugins on node rabbit@ecs-rabbitmq: rabbitmq_management The following plugins have been configured: rabbitmq_management rabbitmq_management_agent rabbitmq_web_dispatch Applying plugin configuration to rabbit@ecs-2b36... The following plugins have been enabled: rabbitmq_management rabbitmq_management rabbitmq_management_agent rabbitmq_web_dispatch

started 3 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 access RabbitMQ. If the following page is displayed, RabbitMQ has been installed.

	Login failed				
Username:		*			
Password:		*			
	Login				

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

➡Rab	bitMQ								User: root Cluster: rabbit@rabbit1 (<u>change</u>) RabbitMQ 3.6.9, <u>Erlang 19.3</u>	
Overview	Connections	Channels	Exchanges	Queues	Admin					
Overview										
▼ Totals										
Queued messag	Queued messages (chart: last minute) (?)									
Currently idle										
Message rates	chart: last minute)	(?)								
Currently idle										
Global counts ()									
Connection	: 0 Ch	annels: 0	Exchang	es: 8	Queues: 0	Consumers	s: 0			
▼ Node										
Node: rabbit@r	Node: rabbit@rabbit! (More about this node)									
File descriptor	s (?) Socket descr	iptors (?) Er	ang processes	Memory	Disk space	Rates mode	Info	Reset stats DB	+/-	
22 1024 availa	ole 829 avail	able 104	324 18576 available	56MB 735MB high wate	35GB rmarl8MB low watermark	basic	Disc 1	Reset		
Reset stats on	all nodes									

----End

6.7 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 businessoriented online transaction processing (OLTP) scenarios and 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 CentOS 7.6 64bit is used as an example.

The PostgreSQL 11.2 version is used as an example.

 To obtain and update the system and software, update the image source to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)?

Configuring the Master Node

- 1. Run the following commands 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 *xxxxx*. Run the following command:

create role dbar login replication encrypted password 'xxxxx';

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 for MD5 password authentication connection in the VPC network segment. host replication *dbar IP address of the slave database*/24 md5 #Allows for data replication from the master database 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
```

7. Run the following command to restart PostgreSQL:

systemctl restart postgresql-11

Configuring the Slave Node

1. Run the following commands 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 /P 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

<pre>[root@ecs-22f5-0002 ~]# pg_basebackup -D /var/1 tream -P</pre>	b/pgsql/11/data -h -p 5432 -U test -X s
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=/P address of the master node port=5432 user=dbar password=xxxxx (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 it to start automatically 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

 [root0ecs-22/5-0001 ~]# ps aux |grep sender

 postgres 14406 0.0 0.3 397240 3620 ?
 Ss 20:19 0:00 postgres: walsender test
 (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;



- 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

6.8 Manually Installing a BT Panel (CentOS 7.2)

Application Scenarios

The best practices for Huawei Cloud ECS guide you through the manual installation of a BT panel on Linux ECSs. BT panel is an 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.

Advantages

- A management project can be quickly created.
- You can view your server resource usage.
- The software installation and source code deployment is easy.

Constraints

- 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 recommended.
 - The OS has no Apache, Nginx, PHP, or MySQL installed.
- The rule listed in **Table 6-9** has been added to the security group which the target ECS belongs to. For details, see **Adding a Security Group Rule**.

D NOTE

The BT panel usually uses port 8888, but it may vary according to the installation environment, so the port used by the panel installed in **Step 1.3** or the port set in the system is recommended.

 Table 6-9 Security group rule

Directi on	Priori ty	Action	Туре	Protocol & Port	Source Address
Inboun d	1	Allow	IPv4	TCP: 8888	0.0.0.0/0

Process of Installing a BP Panel

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.

Procedure

Step 1 Install the BT panel.

- 1. Log in to the target ECS.
- The image source has been updated to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)? This facilitates obtaining and updating the system and software.
- 3. 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 complete, information similar to the following is displayed:



NOTE

Record the address information in the red box as well as the **username** and **password** in the command output.

- **Step 2** Log in to the BT panel.
 - 1. In the address bar of the browser, enter the recorded address, for example, https://1.92.xxx.xx:27832/0677640c. In this example, port 27832 is used, and you need to add it to the security group, or the message "The webpage cannot be found" is displayed.
 - 2. Enter the username and password you recorded.
 - 3. Select I have read and agreed to *Service Agreement* and click Enter Panel.
 - 4. Bind the BT panel account.
 - 5. Install desired suites and deploy websites using the BT panel based on service requirements.

----End

6.9 Installing and Deploying Jenkins on an ECS

Preparations

- Before installing Jenkins, purchase an ECS (recommended configuration: 4 GB + memory and 40 GB+ disk size) running CentOS 7.6. Bind an EIP to the ECS.
- After the ECS is purchased, add the inbound rule listed in the following table to the security group which the ECS belongs to. For details, see Adding a Security Group Rule.

Direction	Priorit y	Action	Туре	Protocol & Port	Source Address
Inbound	1	Allow	IPv4	TCP: 8080	0.0.0/0

Procedure

Step 1 Install JDK.

To ensure compatibility with Jenkins, install OpenJDK 11 (view supported Java versions).

- 1. Remotely log in to the purchased ECS.
- 2. Run the following command to view the current JDK version: **java -version**

If JDK exists and its version is earlier than 11, uninstall the JDK.

- rpm -qa | grep java | xargs rpm -e --nodeps
- 3. Install JDK 11.
 - yum install -y java-11-openjdk
- 4. Restart the ECS.
- 5. Check whether the installation is successful.

```
java -version
```

[root@ecs-jenkins ~]# java -version
openjdk version "11.0.16" 2022-07-19 LTS
<pre>DpenJDK Runtime Environment (Red_Hat-11.0.16.0.8-1.el7_9) (build 11.0.16+8-LTS)</pre>
)penJDK 64-Bit Server VM (Red_Hat-11.0.16.0.8-1.el7_9) (build 11.0.16+8-LTS, mixed mode, sharing)

Step 2 Install Jenkins.

1. Run the following commands one at a time:

sudo wget -O /etc/yum.repos.d/jenkins.repo https://pkg.jenkins.io/redhatstable/jenkins.repo

sudo rpm --import https://pkg.jenkins.io/redhat-stable/jenkins.io.key yum install -y jenkins --nogpgcheck

2. Edit the **Jenkins** file.

vim /etc/sysconfig/Jenkins

#Port
JENKINS_PORT="8080"
#Modify the user
\$JENKINS_USER="root"
#Modify directory permissions
chown -R root:root /var/lib/jenkins
chown -R root:root /var/cache/jenkins
chown -R root:root /var/log/Jenkins

3. Start Jenkins and check its status.

systemctl start jenkins

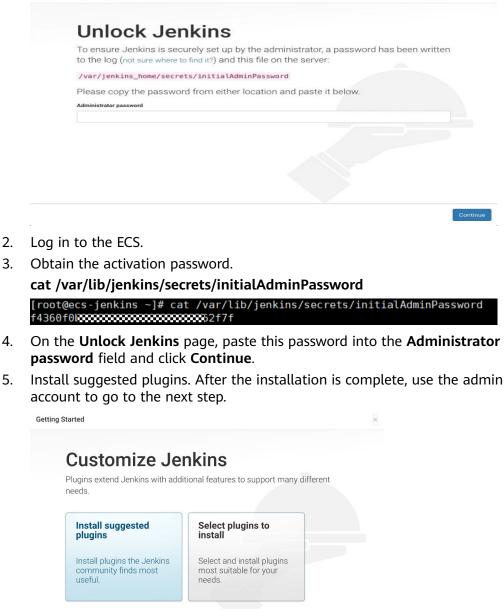
systemctl status jenkins



Step 3 Unlock Jenkins.

1. In the address bar of your local browser, enter **http:***EIP bound to the ECS hosting Jenkins*.8080. The unlocking page is displayed.

Getting Started



6. Save the settings and complete the installation. The Jenkins page is displayed.

Q Search (CTRL+K)	0
/Item	
ople	
Welcome to Jenkins!	
ild History This page is where your Jenkins jobs will be displayed. To get started, you can anage Jenkins distributed builds or start building a software project.	n set up
y Views Start building your software project	
ue V Create a job	\rightarrow
e queue.	
utor Status V Set up a distributed build	
Set up an agent	\rightarrow
C. Course days	
Configure a cloud	\rightarrow
Learn more about distributed builds	Θ

----End

Verification

Single Job

- 1. Choose New item, select Freestyle Project, click OK.
- 2. In **Build Steps**, select **Execute shell**, enter **echo hello world; exit**, and click **OK**.

Build Steps	
= Execute shell ?	
Command See the list of available environment variables	
echo hello world exit	
Advanced	

- 3. Click **Build Now**.
- 4. Wait until the execution of build task in the lower left corner is complete. Click Console Output, you can see the job is finished and **hello world** is displayed.

Console Output
Started by user 001
Running as SYSTEM
[EnvInject] - Loading node environment variables.
Building in workspace /var/lib/jenkins/workspace/Demo
[Demo] \$ /bin/sh -xe /tmp/jenkins14186913887102109696.sh
+ echo hello world
hello world
+ exit
Finished: SUCCESS

Multiple Jobs

1. On the plug-in management page, search for the MultiJob plug-in and install it.

NOTE

• After the plug-in is installed, you need to restart Jenkins for the plug-in to take effect. Select **Download now and install after restart**.

Updates	Plug	ins	
어 Available plugins			
Installed plugins	QM	/	
Advanced settings			
	Instal	I Name ↓	Released
Download progress		Multijob 623.v03401733c9a_9	
	-	Miscellaneous	
		Enabling full hierarchy of Jenkins jobs	2 0 1
		This plugin is deprecated. In general, this means that it is either obsolete, no longer being developed, or may no longer work. Learn more.	3 mo 8 days ag

• After Jenkins is restarted, check whether the MultiJob plug-in takes effect on the installed plug-ins page.

Dashboard > Manage Jenkins > Plugin Mar	lager	
년 Updates 연 Available plugins	Plugins	
気 Installed plugins	Q MultiJob 7	
Advanced settings	Name 1	Enabled
	Multijob plugin 623x03401733:9a_9 Enabling full hierarchy of Jenkins jobs Report an issue with this plugin This plugin is deprecated, in general, this means that it is either obsolete, no longer being developed, or may no longer work. Lear more.	

2. Click New item, select MultiJob Project, and click OK.



NOTE

Before creating a MultiJob project, you need to create three jobs.

3. In Build Steps, select MultiJob Phase.

Build Steps

Add build step 🔺
Filter
▲
Execute shell
Inject environment variables
Invoke Ant
Invoke Gradle script
Invoke top-level Maven targets
MultiJob Phase

4. Add three jobs as follows:

Build Steps

■ MultiJob Phase	×
Phase name (?	
excuteJobSequentialy	
Phase jobs	
Job Job name 🕃	×
Demo1	
Advanced	
≡ Job	×
Job name ?	
Demo2	
Advanced	
≡ Job	×
Job name ?	
Demo3	

Job execution	type	?
---------------	------	---

Running phase jobs sequentially

- 5. Save the settings. The jobs are added.
- 6. Click **Build Now**. The three jobs are successfully built in sequence.

MultiJob Project multijobDemo

					🖉 Add description
					Disable Project
S W Job	Last Success	Last Failure	Last Duration	Console	Built On
⊘ XQX multijobDemo	28 sec #2	N/A	7.5 sec	Console output	Display="block-state="block-sta
⊘ :Q̂: Demo1	28 sec #2	N/A	8 ms	Console output	Jenkins
⊘ XỘX Demo2	25 sec #5	N/A	9 ms	Console output	Jenkins
⊘ :Ç̂; Demo3	23 sec #4	N/A	9 ms	Console output	Jenkins
con: S M L			Icon legend	Atom feed for all 💦 Atom feed for failures	Atom feed for just latest builds
-					
Workspace					
Recent Changes					
Downstream Projects					
 Demo1 Demo2 Demo3 					

6.10 Using auditd to Record File Changes (Linux)

The auditd is a user-space component of the Linux audit system. It records operation logs, including file read/write and invoking records, in the OS, which can be used for audit if a fault occurs. This section uses CentOS 7.4 64bit as an example to describe how to install and configure auditd.

auditd-related Tool Commands and Configuration Files

Tool commands:

- **auditctl**: controls the audit daemon in real time, such as adding rules.
- **aureport**: checks and generates audit reports.
- **ausearch**: searches for audit events.
- **auditspd**: forwards event notifications to other applications instead of writing them to audit logs.
- **autrace**: traces processes.

Configuration files:

- /etc/audit/auditd.conf: specifies configuration file of auditd.
- /etc/audit/rules.d/audit.rules: contains audit rules.
- /etc/audit/audit.rules: records audit rules.

Procedure

Installing auditd

 Run the following command to install auditd: yum install -y auditd*

NOTE

After auditd is installed for the first time, there are no audit rules by default. You can run the **sudo auditctl -l** command to query the audit rules.

2. Run the following command to check the runtime status of auditd:

service auditd status

Figure 6-74 Runtime status

<pre>Iroot@ecs</pre>
Aug 28 10:46:20 localhost.localdomain augenrules[404]: lost 0 Aug 28 10:46:20 localhost.localdomain augenrules[404]: backlog 0
Aug 28 19:46:29 local host. local domain augenruites [494]: enabled 1
Aug 28 10:46:20 localhost.localdomain augenrules[404]: failure 1
Aug 28 10:46:20 localhost.localdomain augenrules[404]: pid 400
Aug 28 10:46:20 localhost.localdomain augenrules[404]: rate limit 0
Aug 28 10:46:20 localhost.localdomain augenrules[404]: backlog_limit 8192
Aug 28 10:46:20 localhost.localdomain augenrules[404]: lost 0
Aug 28 10:46:20 localhost.localdomain augenrules[404]: backlog 0
Aug 28 10:46:20 localhost.localdomain systemd[1]: Started Security Auditing Service.

Configuring audit rules

1. Run the following command to configure the monitoring file and change the directory:

auditctl -w /etc/passwd -p rwxa

where:

- -w: specifies the file path to be monitored. The preceding command specifies the monitored file path /etc/passwd.
- **-p**: specifies the access permission of the file or directory that triggers the audit.
- rwxa: specifies trigger conditions. r indicates the read permission, w the write permission, x the execution permission, and a the attribute.
- 2. Run the following commands to audit all accesses to /production:

mkdir production

auditctl -w /production/

3. Run the following command to check configured rules:

auditctl -l

-w /etc/passwd -p rwxa -w /production -p rwxa

4. After rules are added, run the following command to check the audit log:

ausearch -f /etc/passwd

Figure 6-75 Checking the audit log

time->Mon Aug 28 14:57:10 2023
type=PR0CTITLE msg=audit(1693205830.281:154): proctitle=7375646F006175736561726368002D66002F6574632F706173737764
type=PATH msg=audit(1693205830.281:154): item=0 name="/etc/passwd" inode=1314178 dev=fd:01 mode=0100644 ouid=0 ogid=0 rdev=00:00
objtype=NORMAL cap_fp=0000000000000000 cap_fi=00000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1693205830.281:154):
type=SYSCALL msg=audit(1693205830.281:154): arch=c000003e syscall=2 success=yes exit=4 a0=7f9205d96552 a1=80000 a2=1b6 a3=24 ite
ms=1 ppid=7919 pid=18923 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 fsgid=0 fsgid=0 tty=tty1 ses=1 comm="sudo" exe="/usr/bin
(sudo [®] keu=(sull)

Figure 6-75 shows that the file is not modified. The parameters are described as follows:

- time: audit time
- **name**: audit object

- cwd: current path
- syscall: related system calls
- **auid**: ID of the audited user
- uid and gid: user ID and user group ID for accessing a file
- comm: command for a user to access a file
- **exe**: file path where the preceding command can be executed
- 5. Run the following command to add a user **test** to the monitoring file: **useradd test**
- 6. Run the following command to check the audit log again:

ausearch -f /etc/passwd

Figure 6-76 Checking the audit log again

```
time->Mon Aug 28 15:35:52 2823

type=PROCTITLE msg=audit(1693280152.845:283): proctitle=7375646F006175736561726368002D66002F6574632F706173737764

type=PROT msg=audit(1693280152.845:283): item=0 name=""ctc/passwd" inode=1315998 dev=Fd:81 mode=0100644 ouid=0 ogid=0 rdev=00:80

objtype=NORMAL cap_fp=800000000000000000 cap_f=0 cap_fver=0

type=CAU msg=audit(1693280152.845:283): cud="/root"

type=SYSCALL msg=audit(1693280152.845:283): arch=200000000 syscall=2 success=yes exit=4 a0=7fdc42775552 a1=80000 a2=1b6 a3=24 item

ms=1 ppid=7219 pid=19034 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty1 ses=1 comm="sudo" exe="/subsciences.ses")
```

Figure 6-76 shows that **/etc/passwd** is modified by user **root** (uid=0, gid=0) in the **/root** directory at a specified time. The **/etc/passwd** file is accessed from **/usr/bin/sudo**.

7. Run the following command to check whether the audit log contains any content:



8. Run the following commands to change the directory permissions as user **root** and check the audit log again:

chmod -R 777 /test/

ausearch -f /test/

9. Run the following command to view the audit report:

aureport

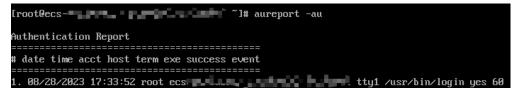
Figure 6-77 Viewing the audit report

[root@ecs	l# aurenort
Summary Report	
=======================================	
Range of time in logs: 01/01/1970 08:00:0	0.000 - 08/28/2023 18:11:02.564
Selected time for report: 01/01/1970 08:0	0:00 - 08/28/2023 18:11:02.564
Number of changes in configuration: 4	
Number of changes to accounts, groups, or	roles: 1
Number of logins: 4	
Number of failed logins: 0	
Number of authentications: 1	
Number of failed authentications: 0	
Number of users: 2	
Number of terminals: 4	
Number of host names: 3	
Number of executables: 7	
Number of commands: 3	
Number of files: 0	
Number of AVC's: 0	
Number of MAC events: 0	
Number of failed syscalls: 0	
Number of anomaly events: 0	
Number of responses to anomaly events: 0	
Number of crypto events: 12	
Number of integrity events: 0	
Number of virt events: 0	
Number of keys: 0	
Number of process IDs: 15 Number of events: 140	
number of evenus, 140	

10. Run the following command to view the authorization failure details:

aureport -au

Figure 6-78 Viewing authorization failure details



11. Run the following command to view all events related to account modifications:

aureport -m

Figure 6-79 Viewing account modification events



12. (Optional) Run the following commands to clear the defined rules: auditctl -D

auditctl -l

Figure 6-80 Clearing defined rules

[root@ecs-	~]#	auditctl	-D
No rules [root@ecs-	~1#	auditctl	-1
No rules			-

6.11 Restoring Accidentally Deleted Data Using Extundelete (Linux)

Application Scenarios

You can use Extundelete to restore accidentally deleted files. Extundelete is a utility that can restore deleted files from an ext3 or ext4 partition.

NOTICE

Whether deleted files can be restored are determined by the following factors:

- Whether data in the files is overwritten after being deleted
- Whether metadata is stored in journal

If the accidentally deleted files were stored in the system disk and data was continuously written into the files after deletion, the files cannot be restored using Extundelete.

To improve data security, you are advised to periodically back up data. For details, see **Creating a Snapshot**, **Creating a Private Image**, and **Creating a Cloud Disk Backup**.

The following uses an ECS running CentOS 7.5 as an example to describe how to use the open-source tool Extundelete to quickly restore accidentally deleted data.

Prerequisites

Before restoring data, complete the following preparations:

- Back up data by referring to Creating a Snapshot and Creating a Private Image to ensure that data can be restored to its original state if an error occurs during data restoration.
- Stop writing data to the file system. If you want to restore a data disk, unmount it first.

Procedure

Step 1 Install Extundelete.

- 1. Log in to the ECS.
- 2. Run the following commands in sequence to install Extundelete dependencies and libraries:

yum install libcom_err e2fsprogs-devel

yum install gcc gcc-c++

- 3. Type **y** when the following information is displayed: Installed size: 25 M Is this OK [y/d/N]: **y**
- Run the following command to download the Extundelete source code: wget https://github.com/curu/extundelete/archive/refs/tags/v1.0.tar.gz
- 5. Run the following command to decompress **v1.0.tar.gz**:

tar xf v1.0.tar.gz

Run the following commands in sequence to compile and install Extundelete:
 cd extundelete-1.0

./configure

make

7. Run the following command to go to the **src** directory and view the compiled Extundelete file:

cd ./src

Step 2 Run the following command to restore data:

```
./extundelete --restore-all /dev/partition
```

The data is restored in **RECOVERED_FILES** in the same directory.

----End

6.12 Setting Up a ThinkPHP Framework

Overview

ThinkPHP, a free, open-source, fast, and simple object-oriented lightweight PHP development framework, is released under the Apache2 open source protocol and is designed for developing agile web applications and simple enterprise applications. The section guides you through the setup of ThinkPHP using an ECS running CentOS 7.2 on Huawei Cloud.

Prerequisites

- You have purchased an ECS and bound an EIP to it.
- The rule listed in the following table has been added to the security group which the target ECS belongs to. For details, see Adding a Security Group Rule.

Directio n	Priority	Acti on	Туре	Protocol & Port	Source Address
Inbound	1	Allo w	IPv4	TCP: 22	0.0.0.0/0

Table	6-10	Security	group	rules
-------	------	----------	-------	-------

Directio n	Priority	Acti on	Туре	Protocol & Port	Source Address
Inbound	1	Allo w	IPv4	TCP: 443	0.0.0.0/0
Inbound	1	Allo w	IPv4	TCP: 8000	0.0.0.0/0

 To obtain and update the system and software, you are advised to update the image source to a Huawei Cloud image source. For details, see How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)?

Procedure

- 1. Install PHP.
 - a. Run the following commands to install the EPEL and REMI repositories: sudo yum install -y epel-release sudo yum install -y https://rpms.remirepo.net/enterprise/remirelease-7.rpm
 - b. Run the following commands to enable the PHP 8.0 repository: sudo yum -y install yum-utils

sudo yum-config-manager --enable remi-php80

c. Run the following commands to install PHP:

sudo yum install -y php php-cli php-fpm php-mysqlnd php-zip phpdevel php-gd php-mcrypt php-mbstring php-curl php-xml php-pear php-bcmath php-json

d. Run the following command to check the version of the installed PHP:

php -v

Information similar to the following is displayed: PHP 8.0.30 (cli) (built: Jun 4 2024 15:19:49) (NTS gcc x86_64) Copyright (c) The PHP Group Zend Engine v4.0.30, Copyright (c) Zend Technologies

2. Install Composer.

Composer is a package manager for the PHP programming language that provides a standard format for managing dependencies of PHP software and required libraries.

a. Run the following command to install the dependencies required by Composer:

sudo yum install -y unzip git

b. Run the following commands to install Composer:

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

sudo mv composer.phar /usr/local/bin/composer

c. Run the following command to check the version of the installed Composer:

composer --version

Information similar to the following is displayed: Composer version 2.7.7 2024-06-10 22:11:12 PHP version 8.0.30 (/usr/bin/php)

- 3. Install ThinkPHP.
 - a. Use Composer to create a new ThinkPHP application.

Run the following command to create **my-thinkphp-app** in the current directory and download the core files and dependencies of ThinkPHP:

composer create-project topthink/think my-thinkphp-app

b. Run the following commands to switch to the created directory and start the ThinkPHP built-in server for development:

cd my-thinkphp-app

php think run

If information similar to the following is displayed, ThinkPHP has been started:

[root0
ThinkPHP Development server is started On http://0.0.88000/>
You can exit with `CTRL-C`
Document root is: /root/my-thinkphp-app/public
[Thu Jul 4 16:07:47 2024] PHP 8.0.30 Development Server (http://0.0.0.0:8000) started

c. After the installation is complete, enter **http://***ECS EIP***:8000** in the address bar of the browser. If the following page is displayed, ThinkPHP has been installed.

7 Securing an ECS

7.1 Enhancing 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 enhance security for SSH logins.

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

 Table 7-1 ECS configurations

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

Figure 7-1 Before the change

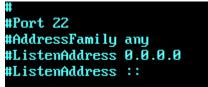


Figure 7-2 After the change



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

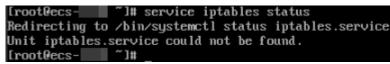
Adding a Firewall Rule to Open a Specified Port

CentOS 7 series use the **fireware** firewall rather than **iptables** by default. Perform the operations described in this section only if Iptables has been installed on your ECS to open 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.

Redirecting to /bin/syst iptables.service - IP Loaded: loaded (/usr/ Active: active (exit Process: 23744 Execta	<pre>[root@ccs]</pre>				
Main PID: 23744 (code=exited, status=0/SUCCESS)					
Apr 16 10:42:53 ecs-	systemd[1]: Starting IPv4 firewall with iptables				
Apr 16 10:42:53 ecs- iptables.init[23744]: iptables: Applying firewall rules: [OK]					
Apr 16 10:42:53 ecs					

2. Run the following command to add an Iptables rule to open 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

Chain INP	UT (po	licy	ACCEPT)	Value Neuro				
target	prot	opt	source	destination				
ACCEPT	tcp		0.0.0.0/0	0.0.0.0/0	state	NEW	tcp	dpt:5000
ACCEPT	tcp		0.0.0.0/0	0.0.0.0/0	state	NEW	tcp	dpt:5000

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 **Compute**, click **Elastic Cloud Server**. The ECS console is displayed.

- 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 \cong 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 7-3**.

Figure 7-3 Security group rules

Add Rule Fast-Add Rule Delete Allow Common Ports Intound Rules: 3 View Security Group Configuration Examples (2						
 Select a property or enter 	r a keyword.					
Priority	Action	Туре	Protocol & Port	Source	Description	
01	Allow	IPv4	TCP : 5000	0.0.0.0/0 ⑦	-	
1	Allow	IPv4	TCP : 22	0.0.0.0/0 ⑦	Used to remotely connect t	
□ 1	Allow	IPv4	TCP : 443	0.0.0.0/0 ③	Used to access websites o	

Changing Password Authentication to Key-Pair Authentication

Create a key pair on the management console, bind the key pair to your ECS to change the ECS login mode.

- 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 keep the private key file secure.
- 4. Choose Service List > Security & Compliance > Data Encryption Workshop. In the left navigation pane, click Key Pair Service.
- Click the ECS List tab, locate the row containing ecs-f5a2, and click Bind in the Operation column. Set parameters according to Figure 7-5, and click OK.
 To disable password authentication, select Disable the password login mode on the Bind Key Pair page, or edit the sshd_config configuration file.

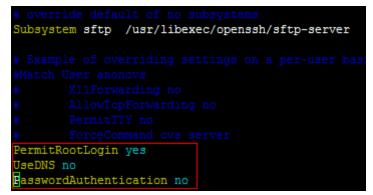
Figure 7-4 Bind Key Pair

key to log in t	vill configure the key pair for the server. After this operation, you can use the to the server. To ensure security, it is recommended that you disable the jin mode of the server and use only the key to log in to the server.
ECS Name	ecs-a51c-
IP Address	
Status	8 Running
New Key Pair	KeyPair-
Boot Password	

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

vim /etc/ssh/sshd_config

Press **i** to enter insert mode, and configure the data in last several lines according to 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". 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 7-5**, the configuration is successful.

SSH User Authent	tication		?	x
Remote Host: Login Name: Server Type:	119.3. :5000 root SSH2, OpenSSH_7.4	4	2	
	r user authenticatio vide necessary infor			thods
© <u>P</u> assword				
Pass <u>w</u> ord;				
O Public Key				
User Key:		•	Browse	•
Passp <u>h</u> rase:				
C Keyboard Int	eractive			
Use keyboard	d input for user authent	ication,		
Remember Pass	sword	OK	Cano	el

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 from certain IP addresses or IP address ranges to a process running on the Linux ECS.

For example, if SSH is available only to the administrator, you can only allow access from the IP address ranges used by the administrator.

The ECS may be logged in anywhere. You are advised to allow accesses from 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 from these IP addresses.

7.2 Using a Virtual IP Address and Keepalived to Set Up a High-Availability Web Cluster

Scenarios

A virtual IP address is a private IP address assigned from a VPC subnet. You can use a virtual IP address and Keepalived to set up a high-availability active/standby web cluster. In such a cluster, if the active ECS goes down, the virtual IP address is bound to the standby ECS to provide services. This section describes how to use a virtual IP address and Keepalived to set up a high-availability web cluster.

Architecture

Figure 7-6 shows a high-availability web cluster using Keepalived. In this architecture, virtual IP address **192.168.0.177** is bound to **ECS-HA1** and **ECS-HA2**. To allow **ECS-HA1** and **ECS-HA2** to access and be accessed from the Internet, an EIP (**EIP-A**) is bound to the virtual IP address. They work as follows:

- 1. **ECS-HA1** works as the active ECS and provides services accessible from the Internet using **EIP-A**. **ECS-HA2** works as the standby ECS, with no services deployed on it.
- 2. If **ECS-HA1** goes down, **ECS-HA2** takes over services, ensuring service continuity.

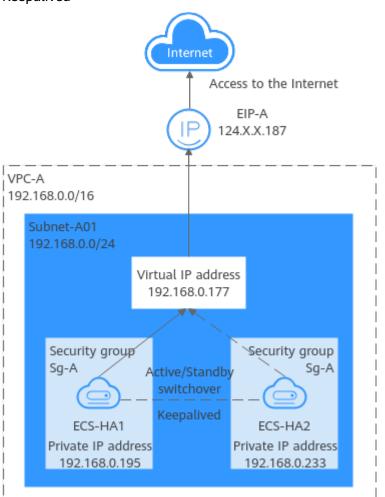


Figure 7-6 A high-availability web cluster using a virtual IP address and Keepalived

Advantages

A high-availability cluster can have one active ECS and one standby ECS or one active ECS and multiple standby ECSs. You can bind a virtual IP address to these ECSs. If the active ECS goes down, the standby ECS becomes the active ECS and continues to provide services.

Notes and Constraints

All servers of the HA cluster must be in the same subnet.

Resource Planning

In this example, the VPC, subnet, virtual IP address, EIP, and ECSs must be in the same region but can be in different AZs.

NOTE

The following resource details are only for your reference. You can modify them if needed.

Table 7-2 Resource planning

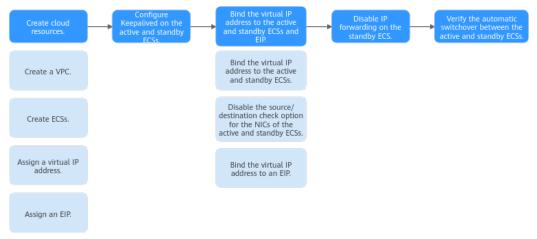
Resource Type	Quan tity	Description		
VPC and subnet	1	 VPC name: Set it as needed. In this example, VPC-A is used. VPC IPv4 CIDR block: Set it as needed. In this example, 192.168.0.0/16 is used. Subnet name: Set it as needed. In this example, Subnet-A01 is used. Subnet IPv4 CIDR block: Set it as needed. In this example, 192.168.0.0/24 is used. 		
ECS	2	 In this example, two ECSs are required for active/standby switchover. Configure the two ECSs as follows: Name: Set this parameter as needed. In this example, the two ECSs are named ECS-HA1 and ECS-HA2. Image: Select an image as needed. In this example, a public image (CentOS 7.8 64bit) is used. System Disk: General Purpose SSD 40 GiB Data Disk: In this example, no data disk is required. You can attach data disks based on service requirements and ensure data consistency between the two ECSs. Network parameters VPC: Select a VPC. In this example, VPC-A is used. Subnet: Select a subnet. In this example, Subnet-A01 is used. Security Group: Select a security group as needed. In this example, ECS-HA1 and ECS-HA2 are associated with the same security group (Sg-A). Private IP address: Specify 192.168.0.195 for ECS-HA1 and 192.168.0.233 for ECS-HA2. 		
Virtual IP address	1	 Assign a virtual IP address from Subnet-A01. Assignment Mode: Set it as needed. In this example, Automatic is selected. Virtual IP address: 192.168.0.177 is used in this example. Instances: Bind 192.168.0.177 to ECS-HA1 and ECS- HA2. EIP: Bind 192.168.0.177 to EIP-A. 		

Resource Type	Quan tity	Description
EIP	1	• Billing Mode: Select a billing mode as needed. In this example, Pay-per-use is used.
		• EIP Name : Set it as needed. In this example, EIP-A is used.
		• EIP : The IP address is randomly assigned. In this example, 124.X.X.187 is used.

Procedure

You can follow the process in **Figure 7-7** to set up a high-availability web cluster using a virtual IP address and Keepalived

Figure 7-7 Process for setting up a high-availability web cluster



Step 1: Create Cloud Resources

- 1. Create a VPC and subnet.
 - For details, see Creating a VPC and Subnet.
- Create two ECSs, one as the active ECS and the other as the standby ECS.
 For details, see Purchasing a Custom ECS.

Configure the ECSs as follows:

- Network: Select VPC-A and Subnet-A01 you have created.
- Security Group: Create security group Sg-A and add inbound and outbound rules to it. Each security group comes with preset rules. You need to check and modify the rules as required.

Add rules in **Table 7-3** to **Sg-A** and associate **Sg-A** with **ECS-HA1** and **ECS-HA2**.

Table 7-3 Sg-A rules

Direc tion	Act ion	Туре	Protoc ol & Port	Source/ Destination	Description
Inbou nd	Allo w	IPv4	TCP: 22	Source: 0.0.0.0/0	Allows remote logins to Linux ECSs over SSH port 22.
Inbou nd	Allo w	IPv4	TCP: 3389	Source: 0.0.0.0/0	Allows remote logins to Windows ECSs over RDP port 3389.
Inbou nd	Allo w	IPv4	TCP: 80	Source: 0.0.0.0/0	Allows external access to the website deployed on the ECSs over HTTP port 80.
Inbou nd	Allo w	IPv4	All	Source: current security group (Sg-A)	Allows the ECSs in Sg-A to communicate with each other using IPv4 addresses.
Inbou nd	Allo w	IPv6	All	Source: current security group (Sg-A)	Allows the ECSs in sg-A to communicate with each other using IPv6 addresses.
Outb ound	Allo w	IPv4	All	Destination: 0.0.0.0/0	Allows ECSs in Sg-A to access the Internet using IPv4 addresses.
Outb ound	Allo w	IPv6	All	Destination: : :/0	Allows ECSs in Sg-A to access the Internet using IPv6 addresses.

NOTICE

In this example, **Source** is set to **0.0.0.0/0**, which allows any external IP address to remotely log in to ECSs in **Sg-A**. To ensure security, you are advised to set **Source** to a specific IP address, for example, the IP address of your local PC.

If your ECSs are associated with different security groups, you need to add rules in **Table 7-4** to allow the ECSs in the two security groups to communicate with each other.

Se cur ity Gr ou p	Dire ction	A ct io n	Ту pe	Prot ocol & Port	Source/ Destinati on	Description
Sg- A	Inbo und	Al lo w	IP v4	All	Source: Sg-B	Allows ECSs in Sg-B to access those in Sg-A over any IPv4 protocol and port.
Sg- B	Inbo und	Al lo w	IP v4	All	Source: Sg-A	Allows ECSs in Sg-A to access those in Sg-B over any IPv4 protocol and port.

Table 7-4 Rules of security groups Sg-A and Sg-B

- **EIP**: Select **Not required**.
- Assign a virtual IP address from Subnet-A01.
 For details, see Assigning a Virtual IP Address.
- Assign an EIP.
 For details, see Assigning an EIP.

Step 2: Configure Keepalived on ECS-HA1 and ECS-HA2.

- 1. Configure Keepalived on ECS-HA1.
 - a. Bind EIP-A (124.X.X.187) to ECS-HA1.

For details, see **Binding an EIP to an ECS**.

b. Remotely log in to **ECS-HA1**.

For details, see How Do I Log In to My ECS?.

c. Run the following command to install the Nginx and Keepalived packages and related dependency packages:

yum install nginx keepalived -y

If information similar to the following is displayed, the installation is complete:

```
[root@ecs-ha1 ~]# yum install nginx keepalived -y
Loaded plugins: fastestmirror
Determining fastest mirrors
base
                 | 3.6 kB 00:00:00
epel
                 | 4.3 kB 00:00:00
extras
                 | 2.9 kB 00:00:00
updates
                  2.9 kB 00:00:00
(1/7): epel/x86_64/
group
    .
399 kB 00:00:00
(2/7): epel/x86_64/
updateinfo
      | 1.0 MB 00:00:00
(3/7): base/7/x86_64/
primary_db
```

```
| 6.1 MB 00:00:00
(4/7): base/7/x86_64/
group_gz
| 153 kB 00:00:00
(5/7): epel/x86_64/
primary_db
| 8.7 MB 00:00:00
(6/7): extras/7/x86_64/
primary_db
| 253 kB 00:00:00
(7/7): updates/7/x86_64/primary_db
```

Dependency Installed:

```
centos-indexhtml.noarch 0:7-9.el7.centos gperftools-libs.x86_64
0:2.6.1-1.el7 lm_sensors-libs.x86_64 0:3.4.0-8.20160601gitf9185e5.el7_9.1
net-snmp-agent-libs.x86_64 1:5.7.2-49.el7_9.4 net-snmp-libs.x86_64
1:5.7.2-49.el7_9.4 nginx-filesystem.noarch 1:1.20.1-10.el7
openssl11-libs.x86_64 1:1.1.1k-7.el7
```

Complete!

- d. Modify the Nginx configuration file.
 - Run the following command to open the /etc/nginx/nginx.conf file:
 vim /etc/nginx/nginx.conf
 - ii. Press i to enter the editing mode.
 - iii. Replace the original content with the following:

```
user root;
worker_processes 1;
#error_log logs/error.log;
#error_log logs/error.log notice;
#error_log logs/error.log info;
#pid logs/nginx.pid;
events {
    worker_connections 1024;
    }
http {
   include mime.types;
   default_type application/octet-stream;
   #log_format main '$remote_addr - $remote_user [$time_local] "$request" '
   # '$status $body_bytes_sent "$http_referer"
   # ""$http_user_agent" "$http_x_forwarded_for"";
   #access_log logs/access.log main;
   sendfile on;
   #tcp_nopush on;
   #keepalive_timeout 0;
   keepalive_timeout 65;
   #gzip on;
   server {
       listen 80;
       server_name localhost;
       #charset koi8-r;
       #access_log logs/host.access.log main;
       location / {
              root html;
             index index.html index.htm;
             }
       #error_page 404 /404.html;
       # redirect server error pages to the static page /50x.html
       error_page 500 502 503 504 /50x.html;
       location = /50x.html {
                    root html;
                    }
       }
```

iv. Press **ESC** to exit and enter :wq! to save the configuration.

- e. Modify the **index.html** file to verify whether the website is successfully accessed.
 - i. Run the following command to open the **/usr/share/nginx/html/ index.html** file:

vim /usr/share/nginx/html/index.html

- ii. Press i to enter the editing mode.
- iii. Replace the original content with the following: Welcome to ECS-HA1
- iv. Press **ESC** to exit and enter :wq! to save the configuration.
- f. Run the following commands to set the automatic startup of Nginx upon ECS startup:

systemctl enable nginx

systemctl start nginx.service

Information similar to the following is displayed: [root@ecs-ha1 ~]# systemctl enable nginx Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service to /usr/lib/ systemd/system/nginx.service. [root@ecs-ha1 ~]# systemctl start nginx.service

g. Open a browser, enter the EIP address (**124.X.X.187**), and press **Enter** to verify the access to a single Nginx node.

If the web page shown in the following figure is displayed, Nginx is successfully configured for **ECS-HA1**.

Figure 7-8 ECS-HA1 accessed



Welcome to ECS-HA1

- h. Modify the Keepalived configuration file.
 - i. Run the following command to open the **/etc/keepalived/ keepalived.conf** file:

vim /etc/keepalived/keepalived.conf

- ii. Press i to enter the editing mode.
- iii. Replace the IP parameters in the configuration file as follows:
 - mcast_src_ip and unicast_src_ip: Change their values to the private IP address of an ECS. In this example, private IP address 192.168.0.195 of ECS-HA1 is used.
 - **virtual_ipaddress**: Change the value to a virtual IP address. In this example, **192.168.0.177** is used.

```
! Configuration File for keepalived
global_defs {
router_id master-node
}
vrrp_script chk_http_port {
    script "/etc/keepalived/chk_nginx.sh"
    interval 2
    weight -5
    fall 2
```

```
rise 1
     }
vrrp_instance VI_1 {
   state BACKUP
   interface eth0
   mcast_src_ip 192.168.0.195
   virtual_router_id 51
   priority 100
   advert_int 1
   authentication {
          auth_type PASS
          auth_pass 1111
          }
   unicast_src_ip 192.168.0.195
   virtual_ipaddress {
             192.168.0.177
             }
track script {
   chk_http_port
   }
}
```

iv. Press **ESC** to exit and enter :wq! to save the configuration.

- i. Configure the Nginx monitoring script.
 - i. Run the following command to open the **/etc/keepalived/ chk_nginx.sh** file:

vim /etc/keepalived/chk_nginx.sh

- ii. Press i to enter the editing mode.
- iii. Replace the original content with the following: #!/bin/bash

```
counter=$(ps -C nginx --no-heading|wc -l)
if [ "${counter}" = "0" ]; then
   systemctl start nginx.service
   sleep 2
   counter=$(ps -C nginx --no-heading|wc -l)
   if [ "${counter}" = "0" ]; then
      systemctl stop keepalived.service
   fi
```

- iv. Press **ESC** to exit and enter :wq! to save the configuration.
- j. Run the following command to assign execute permissions to the **chk_nginx.sh** file:

chmod +x /etc/keepalived/chk_nginx.sh

k. Run the following commands to set the automatic startup of Keepalived upon ECS startup:

systemctl enable keepalived

systemctl start keepalived.service

- l. Unbind EIP-A from ECS-HA1. For details, see Unbinding an EIP.
- 2. Configure Keepalived on ECS-HA2.
 - a. Bind EIP-A (124.X.X.187) to ECS-HA2. For details, see Binding an EIP to an ECS.
 - Remotely log in to ECS-HA2.
 For details, see How Do I Log In to My ECS?.
 - c. Run the following command to install the Nginx and Keepalived packages and related dependency packages:

yum install nginx keepalived -y

If information similar to the following is displayed, the installation is complete: [root@ecs-ha2 ~]# yum install nginx keepalived -y Loaded plugins: fastestmirror Determining fastest mirrors base | 3.6 kB 00:00:00 epel | 4.3 kB 00:00:00 extras | 2.9 kB 00:00:00 updates | 2.9 kB 00:00:00 (1/7): epel/x86_64/ group | 399 kB 00:00:00 (2/7): epel/x86_64/ updateinfo | 1.0 MB 00:00:00 (3/7): base/7/x86_64/ primary_db 6.1 MB 00:00:00 (4/7): base/7/x86_64/ group_gz | 153 kB 00:00:00 (5/7): epel/x86_64/ primary_db | 8.7 MB 00:00:00 (6/7): extras/7/x86_64/ primary_db | 253 kB 00:00:00 (7/7): updates/7/x86_64/primary_db Dependency Installed: centos-indexhtml.noarch 0:7-9.el7.centos gperftools-libs.x86_64 lm sensors-libs.x86 64 0:3.4.0-8.20160601gitf9185e5.el7 9.1 0:2.6.1-1.el7 net-snmp-agent-libs.x86_64 1:5.7.2-49.el7_9.4 net-snmp-libs.x86_64 1:5.7.2-49.el7 9.4 nginx-filesystem.noarch 1:1.20.1-10.el7 openssl11-libs.x86_64 1:1.1.1k-7.el7 Complete! Modify the Nginx configuration file.

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

vim /etc/nginx/nginx.conf

d.

- ii. Press i to enter the editing mode.
- Replace the original content with the following: iii. user root; worker_processes 1; #error_log logs/error.log; #error_log logs/error.log notice; #error_log logs/error.log info; #pid logs/nginx.pid; events { worker_connections 1024; } http { include mime.types; default_type application/octet-stream; #log_format main '\$remote_addr - \$remote_user [\$time_local] "\$request" ' # '\$status \$body_bytes_sent "\$http_referer" # '"\$http_user_agent" "\$http_x_forwarded_for"'; #access_log logs/access.log main; sendfile on;

```
#tcp_nopush on;
#keepalive_timeout 0;
keepalive_timeout 65;
#gzip on;
server {
   listen 80;
   server_name localhost;
   #charset koi8-r;
   #access_log logs/host.access.log main;
   location / {
          root html:
          index index.html index.htm;
          }
   #error_page 404 /404.html;
   # redirect server error pages to the static page /50x.html
   error_page 500 502 503 504 /50x.html;
   location = /50x.html {
                root html;
   }
```

- iv. Press **ESC** to exit and enter :wq! to save the configuration.
- e. Modify the **index.html** file to verify whether the website is successfully accessed.
 - i. Run the following command to open the **/usr/share/nginx/html/ index.html** file:

vim /usr/share/nginx/html/index.html

- ii. Press i to enter the editing mode.
- iii. Replace the original content with the following: Welcome to ECS-HA2
- iv. Press **ESC** to exit and enter :wq! to save the configuration.
- f. Run the following commands to set the automatic startup of Nginx upon ECS startup:

systemctl enable nginx

systemctl start nginx.service

Information similar to the following is displayed: [root@ecs-ha2 ~]# systemctl enable nginx Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service to /usr/lib/ systemd/system/nginx.service. [root@ecs-ha2 ~]# systemctl start nginx.service

g. Open a browser, enter the EIP address (**124.X.X.187**), and press **Enter** to verify the access to a single Nginx node.

If the web page shown in the following figure is displayed, Nginx is successfully configured for **ECS-HA2**.

Figure 7-9 ECS-HA2 accessed



Welcome to ECS-HA2

- h. Modify the Keepalived configuration file.
 - i. Run the following command to open the **/etc/keepalived/ keepalived.conf** file:

vim /etc/keepalived/keepalived.conf

- ii. Press i to enter the editing mode.
- iii. Replace the IP parameters in the configuration file as follows:
 - mcast_src_ip and unicast_src_ip: Change their values to the private IP address of an ECS. In this example, private IP address of ECS-HA2 (192.168.0.233) is used.
 - **virtual_ipaddress**: Change the value to a virtual IP address. In this example, **192.168.0.177** is used.

```
! Configuration File for keepalived
global_defs {
router_id master-node
vrrp_script chk_http_port {
       script "/etc/keepalived/chk_nginx.sh"
       interval 2
       weight -5
       fall 2
       rise 1
     }
vrrp_instance VI_1 {
   state BACKUP
   interface eth0
   mcast_src_ip 192.168.0.233
   virtual_router_id 51
   priority 100
   advert_int 1
   authentication {
          auth_type PASS
          auth_pass 1111
          }
   unicast_src_ip 192.168.0.233
   virtual_ipaddress {
              192.168.0.177
              }
track_script {
   chk_http_port
   }
}
```

- iv. Press **ESC** to exit and enter **:wq!** to save the configuration.
- i. Configure the Nginx monitoring script.
 - i. Run the following command to open the **/etc/keepalived/ chk_nginx.sh** file:

vim /etc/keepalived/chk_nginx.sh

- ii. Press i to enter the editing mode.
- iii. Replace the original content with the following: #!/bin/bash

```
counter=$(ps -C nginx --no-heading|wc -l)
if [ "${counter}" = "0" ]; then
   systemctl start nginx.service
   sleep 2
   counter=$(ps -C nginx --no-heading|wc -l)
   if [ "${counter}" = "0" ]; then
      systemctl stop keepalived.service
   fi
```

- iv. Press **ESC** to exit and enter :wq! to save the configuration.
- j. Run the following command to assign execute permissions to the **chk_nginx.sh** file:

chmod +x /etc/keepalived/chk_nginx.sh

k. Run the following commands to set the automatic startup of Keepalived upon ECS startup:

systemctl enable keepalived

systemctl start keepalived.service

l. Unbind EIP-A from ECS-HA2. For details, see Unbinding an EIP.

Step 3: Bind the Virtual IP Address to the Active and Standby ECSs and EIP

- Bind virtual IP address 192.168.0.177 to ECS-HA1 and ECS-HA2.
 For details, see Binding a Virtual IP Address to an Instance or EIP.
- 2. Disable **Source/Destination Check** for the network interfaces of the active and standby ECSs.

When you bind a virtual IP address to an ECS, **Source/Destination Check** is disabled by default. You can perform the following operations to check whether the function is disabled. If the function is not disabled, disable it.

a. In the ECS list, click the name of the target ECS.

The ECS details page is displayed.

b. On the **Network Interfaces** tab, click \checkmark to expand the details area and check whether **Source/Destination Check** is disabled.

If the information shown in **Figure 7-10** is displayed, **Source/Destination Check** is disabled.

Figure 7-10 Disabling Source/Destination Check

ecs-						
imary Disks	Network Interfaces	Security Groups	EIPs	Monitoring	Tags	Cloud Backup and Recover
After you add an extension	NIC, configure policy-base	ed routing on the ECS to er	nable networi	communication bet	ween the EC	'S and NIC.
After you attach or detach a	a network interface or char	ige a VPC, enable NIC mu	lti-queue to ir	nprove network perfo	ormance.	
Attach Network Interfac	You can attach 1 m	ore network interfaces.				
∧ 192.168.0.195						
Name						
NIC ID	Obca4a90-	d45907ea35	5a			
Status	🥝 Activated					
EIP	-					
Security Group	Sg-A					
Source/Destination Che	ck 🔵 🧿					
IPv4 Subnet ID	2b0b04ca	9d13b4d651	1			
IPv6 Subnet ID	-					

3. Bind virtual IP address **192.168.0.177** to **EIP-A**. For details, see **Binding a Virtual IP Address to an Instance or EIP**.

Step 4: Disable IP Forwarding on the Standby ECS

If a virtual IP address is bound to active/standby ECSs, you need to disable IP forwarding on the standby ECS. If an active/standby ECS switchover happens, ensure that IP forwarding of the new standby ECS is also disabled.

To make sure you do not miss any settings, it is better to disable IP forwarding on both of active and standby ECSs.

1. Open a browser, enter the EIP address (**124.X.X.187**), and press **Enter** to access the active ECS.

If the following page is displayed, the **ECS-HA1** is used as the active ECS.

Figure 7-11 The active ECS accessed



Welcome to ECS-HA1

- 2. Remotely log in to the standby ECS (**ECS-HA2** in this example). For details, see **How Do I Log In to My ECS**?.
- 3. Disable IP forwarding by following the operations in **Table 7-5**. In this example, the ECS runs the Linux OS.

os	Operations
Linux	1. Run the following command to switch to user root : su root
	 Run the following command to check whether IP forwarding is enabled: cat /proc/sys/net/ipv4/ip_forward
	In the command output, 1 indicates that IP forwarding is enabled, and 0 indicates that IP forwarding is disabled. The default value is 0 .
	• If 0 is displayed, no further action is required.
	• If 1 is displayed, go to the next step.
	 Use either of the following methods to modify the configuration file: Method 1
	 a. Run the following command to open the /etc/ sysctl.conf file: vim /etc/sysctl.conf
	b. Press i to enter the editing mode.
	c. Set net.ipv4.ip_forward to 0 .
	d. Press ESC to exit and enter :wq! to save the configuration.
	Method 2
	Run the sed command. An example command is as follows
	sed -i '/net.ipv4.ip_forward/s/1/0/g' /etc/sysctl.conf
	 Run the following command to apply the modification: sysctl -p /etc/sysctl.conf
Windows	1. In the search box, enter cmd to open the command prompt window, and run the following command: ipconfig/all
	 In the command output, if the value of IP Routing Enabled is No, IP forwarding is disabled.
	 If IP Routing Enabled is Yes, IP forwarding is not disabled. Go to the next step.
	2. Enter regedit in the search box to open the registry editor.
	3. Set the value of IPEnableRouter under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Services\Tcpip\Parameters to 0.
	 If the value is set to 0, IP forwarding will be disabled.
	 If the value is set to 1, IP forwarding will be enabled.

Table 7-5 Disabling IP forwarding

Step 5: Verify the Automatic Switchover Between the Active and Standby ECSs

- 1. Restart the active and standby ECSs.
 - a. Remotely log in to ECS-HA1.For details, see How Do I Log In to My ECS?.
 - b. Run the following command to restart **ECS-HA1**: **reboot**
 - c. Repeat **1.a** to **1.b** to restart **ECS-HA2**.
- 2. Check whether the website on the active ECS can be accessed.
 - a. Open a browser, enter the EIP address (124.X.X.187), and press Enter.

If the following page is displayed, **ECS-HA1** is used as the active ECS and the website can be accessed.

Figure 7-12 ECS-HA1 accessed



Welcome to ECS-HA1

b. Remotely log in to **ECS-HA1** and run the following command to check whether the virtual IP address is bound to the eth0 NIC of **ECS-HA1**:

ip addr show

If information similar to the following is displayed, the virtual IP address (**192.168.0.177**) has been bound to the eth0 NIC of **ECS-HA1**, and this ECS is the active one.

[root@ecs-ha1 ~]# ip addr show

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default glen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid lft forever preferred lft forever

inet6 ::1/128 scope host

valid_lft forever preferred_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000

link/ether fa:16:3e:fe:56:19 brd ff:ff:ff:ff:ff:ff

inet 192.168.0.195/24 brd 192.168.0.255 scope global noprefixroute dynamic eth0 valid_lft 107898685sec preferred_lft 107898685sec

inet 192.168.0.177/32 scope global eth0

valid_lft forever preferred_lft forever inet6 fe80::f816:3eff:fefe:5619/64 scope link

valid_lft forever preferred_lft forever

c. Run the following command to disable Keepalived on **ECS-HA1**:

systemctl stop keepalived.service

- 3. Check whether ECS-HA2 becomes the active ECS.
 - a. Remotely log in to **ECS-HA2** and run the following command to check whether the virtual IP address is bound to the eth0 NIC of **ECS-HA2**:

ip addr show

If information similar to the following is displayed, the virtual IP address (**192.168.0.177**) has been bound to the eth0 NIC of **ECS-HA2**, and this ECS becomes the active one.

[root@ecs-ha2 ~]# ip addr show

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid_lft forever preferred_lft forever

inet6 ::1/128 scope host

valid_lft forever preferred_lft forever 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000

link/ether fa:16:3e:fe:56:3f brd ff:ff:ff:ff:ff
link/ether fa:16:3e:fe:56:3f brd ff:ff:ff:ff:ff
inet 192.168.0.233/24 brd 192.168.0.255 scope global noprefixroute dynamic eth0
valid_lft 107898091sec preferred_lft 107898091sec
inet 192.168.0.177/32 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::f816:3eff:fefe:563f/64 scope link
valid_lft forever preferred_lft forever

b. Open a browser, enter the EIP address (**124.X.X.187**), and press **Enter** to check whether the website on the active ECS (**ECS-HA2**) can be accessed.

If the following page is displayed, **ECS-HA2** is used as the active ECS and the website can be accessed.

Figure 7-13 ECS-HA2 accessed



Welcome to ECS-HA2

8 Migrating an ECS

8.1 Migrating Servers to the Cloud

Background

As the public cloud is agile, flexible, reliable, easy to use, and cost-effective, more and more enterprises choose to migrate their IT applications and loads to the public cloud. An easy and quick migration method is of great significance for the enterprises. Huawei Cloud allows you to quickly and easily migrate workloads from 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 OSs**.

Before using SMS, you need to know constraints on source servers.

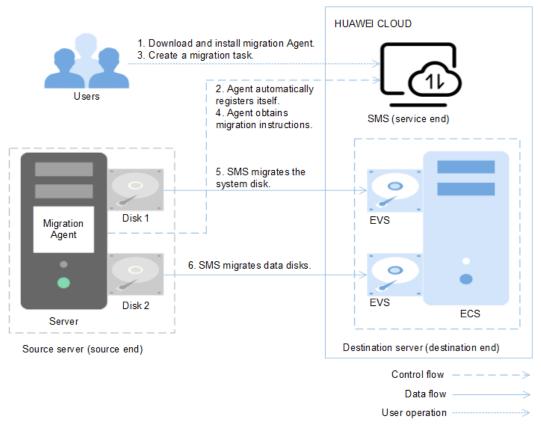


Figure 8-1 SMS working principle

SMS automatically performs the migration, and you only need to perform steps 1 and 3.

- 1. Install the migration Agent on the source server. For details, see **How Do I** Install 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 a 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. For details about how to create an ECS using a private image, see **Purchasing** a **Custom ECS**.

8.2 Migrating ECSs Across Accounts and Regions Through Image Replication

Scenarios

If you want to migrate ECSs between Huawei Cloud accounts in different regions, you are advised to use IMS to implement the migration.

For details about common scenarios and methods of server migration, see **Migration Knowledge**.

For details about migrating ECSs across accounts and regions, see **Cross-Account**, **Cross-Region ECS Migration**.

Migration Knowledge

Common server migration scenarios include migration from physical servers to cloud servers, from virtualization platforms, such as VMware, to Huawei Cloud ECSs, between Huawei Cloud ECSs across accounts or regions, from cloud servers on a third-party cloud platform to Huawei Cloud ECSs, and installation disk imaging. For details about the recommended migration methods, see **Table 8-1**.

Scenario	Condition	Recommended Solution	Remarks
From x86 physical servers to Huawei Cloud ECSs	The servers can access the Internet.	Server Migration Service See Migrating	-
For example, P2V		Servers to the Cloud.	
From virtualization	The VMs can access the	Server Migration Service	-
platforms, such as VMware, to Huawei Cloud ECSs	Internet.	See Migrating Servers to the Cloud.	

Table 8-1	Common	server	migration	scenarios
-----------	--------	--------	-----------	-----------

Scenario	Condition	Recommended Solution	Remarks
	The VMs cannot access the Internet.	 Export the VM image files from the VMware virtualization platform. Import the image files by referring to Uploading an External Image File. 	If the image file format is not vhd, vmdk, qcow2, raw, vhdx, qcow, vdi, qed, zvhd, or zvhd2, convert the file format.
Between Huawei Cloud ECSs across accounts or regions For example, the ECSs of account A in the CN North- Beijing4 region are to be migrated to account B in the CN East- Shanghai1 region.	The ECSs can access the Internet.	Server Migration Service See Migrating Servers to the Cloud.	-

Scenario	Condition	Recommended Solution	Remarks
	The ECSs cannot access the Internet.	 Recommended Migration across accounts: See Sharing Images. Use the system disk of the source ECS to create a system disk image and the data disk to create a data disk image, or use the source ECS to create a full-ECS image. Then, share the images with other accounts. Migration across regions: See Replicating Images Across Regions. Use the system disk of the source ECS to create a system disk image and the data disk to create a data disk image, or use the source ECS to create a full-ECS image. Then, replicate the data disk to create a data disk image, or use the source ECS to create a full-ECS image. Then, replicate the images to other regions. Migration across accounts and regions: See Sharing Images and Replicating Images Across Regions. 	Only the full-ECS images created using CBR can be shared. The size of images to be replicated across regions cannot be greater than 128 GB.

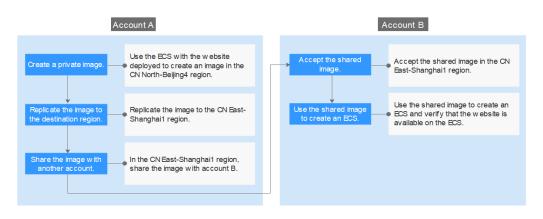
Scenario	Condition	Recommended Solution	Remarks
From a third-party cloud platform to Huawei Cloud For example, from Alibaba Cloud or	The cloud servers can access the Internet.	Server Migration Service See Migrating Servers to the Cloud.	-
Tencent Cloud to Huawei Cloud	The cloud servers cannot access the Internet.	 Export the image from the source cloud platform. Import the image files by referring to Uploading an External Image File. 	If the image file format is not vhd, vmdk, qcow2, raw, vhdx, qcow, vdi, qed, zvhd, or zvhd2, convert the file format.
Installation disk imaging For example, create an image file offline and import it to Huawei Cloud.	The ISO installation disk image of the required OS is available.	Creating a Windows Image Using VirtualBox and an ISO File Introduction or Creating a Windows System Disk Image from an ISO File	-

Cross-Account, Cross-Region ECS Migration

To migrate an ECS to a different account in another region, use the ECS to create an image, replicate the image to the destination region under the same account, and then share the image with the desired account.

For example, if a website is set up on an ECS in the **CN North-Beijing4** region and you want to migrate the ECS to another account in the **CN East-Shanghai1** region, the process is as follows.

Figure 8-2 Migration process



- 1. Create a private image
- 2. Replicate the image to the destination region
- 3. Share the image with the desired account
- 4. Accept the shared image
- 5. Use the shared image to create an ECS

Step 1: Create a Private Image

Use the ECS with the website deployed to create an image in the **CN North-Beijing4** region. Assume that the website access address is **http://121.36**.*xxx.xxx/* **index.html**.



Locate the row that contains the ECS with the website deployed (for example, ecs-fe9e), and choose More > Manage Image/Disk/Backup > Create Image in the Operation column.

The Create Image page is displayed.

4. Set parameters.

-			-				
Image Type ar	nd Source						
* Type	System disk image	Full-ECS Image	Data disk image	ISO image			
* Source	ECS CSBS Bac	kup Cloud Server Back	up				
	ECS runs Windows.	image, configure and optimize th rver backup will be generated wh			uns Linux and Cloud	ibase-Init is Installed i	If the
			All statuse	× ×	ID 💌	6b5bc85f-0 ×	QC
	Name	OS	St	atus Pri	vate IP Address	Created	
	∧ ● ecs-fe9e	CentOS 7.2	54bit 😑	Running 192	2.168.1.183	Feb 25, 2022 15:	29:58 G
	Disk Information						
	Name	Capacity (C	GB) Disk Type	Function		Encrypted	
	ecs-fe9e-volume-000	1	100 High I/O	Data disk		No	
	ecs-fe9e		40 High I/O	System Di	isk	No	
	Selected: ecs-fe9e System	Disk: High I/O 40 GB Data dis	k: High I/O 100 GB				
	* Server Backup Vault	vault-e19d 8/80 (GB)	C Create Server	Backup Vault 🕐			
		The vault is associated with the s	elected ECS. To change	the vault, go to the Clou	id Backup and Reco	very Console.	
	Buy ECS						

Figure 8-3 Creating a private image

- **Type**: Full-ECS image

Data disks contain service data. You can use an ECS with data disks attached to it to create a full-ECS image.

- Source: Select ECS and select ecs-fe9e from the list.
- Specify Server Backup Vault to store backups. If the ECS has been associated with a vault, the system selects the associated vault by default.

The created full-ECS image and backup are stored in the server backup vault.

If no server backup vault is available, click **Create Server Backup Vault** to create one. Ensure that you select **Backup** for **Protection Type**.

- **Name**: Enter a name for the image, for example, **migrate_test**.
- Enterprise Project: Select default.
- 5. Click **Next**.
- 6. Confirm the settings, read and agree to the agreement, and click **Submit**.
- 7. The system redirects to the private image list. Wait for several minutes and check whether the private image is successfully created.

Figure 8-4 Viewing private images

Name ↓≡	Status	OS Type	OS	Image Type
migrate_test	🕑 Normal	Linux	CentOS 7.2 64bit	Full-ECS image(x86)

Step 2: Replicate the Image to the Destination Region

Replicate the private image created in **Step 1: Create a Private Image** to the **CN East-Shanghai1** region. Before performing the replication, create an IAM agency.

- 1. Create an IAM agency.
 - a. In the upper right corner of the page, click the username and select **Identity and Access Management**.

- b. In the navigation pane, choose Agencies.
- c. Click Create Agency.
- d. On the **Create Agency** page, set the following parameters:
 - Agency Name: Enter an agency name, for example, ims_administrator_agency.

Figure	8-5	Creating	an	agency

* Agency Name	ims_administrator_agency
★ Agency Type	 Account Delegate another HUAWEI CLOUD account to perform operations on your resources. Cloud service Delegate a cloud service to access your resources in other cloud services.
* Cloud Service	Image Management Service (IMS)
* Validity Period	Unlimited •
Description	Enter a brief description.
	0/255

- Agency Type: Select Cloud service.
- Cloud Service: This parameter is available if you select Cloud service for Agency Type. Click Select. In the displayed Select Cloud Service dialog box, select Image Management Service (IMS) and click OK.
- Validity Period: Select Unlimited.
- Description: This parameter is optional. You can enter Agency with IMS Administrator privileges.
- e. Click **Next** and select a policy for the agency.
- f. Select IMS Administrator.

Figure 8-6 Selecting a policy

Assign :	selecti	d permissions to ims_administrator_agency.		Create Policy
0	Select	d permissions: 1, which include the dependency permissions of IMS Administrator. Click View Selected or expand the details area to view the dependency permission	ns.	
Vie	v Sele	586 (1) Copy Permissions from Another Project		All policies/toles
		Policy/Role Name	Туре	
	×	IMS ReadOnlyAccess The read-only permissions to all IMS resources, which can be used for statistics and survey.	System-	Seffred policy
	~	IMS Administrator IMS Administrator	System-	defined role
	×	INS FullAccess All permissions of Image Management Service	System-	Mined policy

- g. Click **Next** and select an authorized region.
- h. In the **Project [Region]** column, select **cn-north-4 [CN North-Beijing4]** and **cn-east-3 [CN East-Shanghai1]**, and click **OK**.

Figure 8-7 Selecting a region

Stelect PolicyRole Belect Scope Finish		Ge to Old Er
The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization	n.	×
Scope		
All resources		
Region specific projects The selected permissions will be applied to resources in the region-specific projects you select.		
Total projects: 13. Select the desired projects.		Enter a project name or description.
Project [Region] ↓ ■	Description	
on-north-4 (CN North-Beijinp4)	-	
Cn-east-3 (CN East-Shanghai1)	-	
cn-east-2 [CN East-Shanghal2]		
cn-south-1 [CN South-Guangzhou]	-	

Do not select **All projects** in the **Project [Region]** column. Otherwise, the created agency will be invalid.

i. Click **Finish**. You can view the created agency on the **Basic Information** tab.

Figure 8-8 Viewing agencies

- Agency Namelito J.E.
 Delegated Party J.E.
 Validity Period J.E.
 Created J.F.
 Description J.E.
 Operation

 Ims_schemistratur_appency
 Cloud service Image Management Service (MS)
 Unlimed
 Feb 25, 2022 15 59.34 GMT-98.00
 Authorize Modely Delete
- Under Service List, choose Compute > Image Management Service. Then, click the Private Images tab.

The **Private Images** page is displayed.

Locate the row that contains the migrate_test image, and choose More > Replicate in the Operation.

The **Replicate Image** dialog box is displayed.

4. Set parameters.

Figure 8-9 Replicating an image

Replication Mode	Within Region Across Re	gions
★ Name	copy_cn-north-4_migrate_test	
★ Destination Region	CN East-Shanghai1	•
* Destination Project	cn-east-3	•
★ Target Server Backup Vault	vault-9d01 0/100(GB)	C Create Server Backup Vault
	You can only select a server backup vault	whose type is Replication.
★ IAM Agency	ims_administrator_agency	C View Agency ⑦
Description		
		0/1,024
	ок	Cancel

- **Name**: Retain the default value **copy_cn-north-4_migrate_test**.
- Destination Region: Select CN East-Shanghai1.
- **Destination Project**: Select **cn-east-3**.
- Target Server Backup Vault: Select **vault-2398**.
- IAM Agency: Select ims_administrator_agency created in 1.
- 5. Click OK.
- 6. Switch to the **CN East-Shanghai1** region. Wait for several minutes and check whether the image is successfully replicated.

Figure 8-10 Viewing private images

Name J≡	Status	OS Type	OS	Image Type
migrate_test	🕑 Normal	Linux	CentOS 7.2 64bit	Full-ECS image(x86)

Step 3: Share the Image with the Target Account

In the **CN East-Shanghai1** region, share the image with account B. On the **API Credentials** page, obtain the project ID of account B in the **CN East-Shanghai1** region.

Figure 8-11 Obtaining the project ID

•	5 1 5					
API Credentials	API Credentials ③					
Access Keys	Learn more about HUAWEI CLOUD accounts, IAM users, and projects.					×
	IAM Doe Name all all all and a second and all all all all all all all all all al		Account Name			
	Projects				Enter a project name.	Q
	Project ID 4	Project Name JE		Region 4		
	07c101c34a001005200c01ea335a567	cn-north-4		CN North-Beijing4		
	07c301f2d1800f0c2f19c01ecd58cd39	cn-east-3		CN East-Shanghai1		
	07c302003400108288c01edd823c8b1	cn-east-2		CN East-Shanghai2		
	06457686930009929tcc01ec7625134	cn-south-1		CN South-Guangzhou		
	Def17b437880f5062ftcc01e268564ac	cn-southwest-2		CN Southwest-Gulyang1		
	078c5ftb688010fc2tbcc01ea20fc22a	ap-southeast-1		CN-Hong Kong		
	0645766e758025c02f9ec01e6592a4b5	ap-southeast-2		AP-Bangkok		
	0b4576df7380f5aa2f0bc01e90be994a	ap-southeast-3		AP-Singapore		
	054570/10/0001642164c01ee7855e37	af-south-1		AF-Johannesburg		
	Data25859538013412958c01e388a1e51	na-mexico-1		LA-Mexico City1		
	Auto According 1000170-001-contradication	is worth 9		LA MALLA PRO		

- In the CN East-Shanghai1 region, choose Service List > Compute > Image Management Service and click the Private Images tab.
 The Private Images page is displayed.
- Locate the row that contains the copy_cn-north-4_migrate_test private image. Choose More > Share in the Operation column. The Share Image dialog box is displayed.
- 3. Click the **Shared Images** tab, enter the project ID of account B, and click **OK**.

Figure 8-12 Sharing an image

Share Imag	ge
i An image	e can be shared only inside its region.
Image Deta	ails
Image Name	copy_cn-north-4_migrate_test
OS Type	Linux
OS	CentOS 7.2 64bit
Shared Image	s Stop Sharing
Enter one or mor	re project IDs of the recipients. Separate multiple IDs with commas (,).Learn how to obtain the project ID.
* Project ID	and the second sec
	OK

4. Click OK.

Step 4: Accept the Shared Image

Accept the shared image in the CN East-Shanghai1 region.

- 1. Log in to the management console using the account the image is shared with (account B) and switch to the **CN East-Shanghai1** region.
- 2. Under Service List, choose Compute > Image Management Service. Then, click the Images Shared with Me tab.

3. In the displayed dialog box, select **copy_cn-north-4_migrate_test** and click **Accept**.

	Figure	8-13 Acce	pting a	shared	image
--	--------	-----------	---------	--------	-------

 Tenant manual has shared 1 images with you. Accept 	pt All C			
Accept Reject				
Name	ID	OS Type	OS	Disk Capacity (GB) Source Tenant
copy_on-north-4_migrate_test	4d719f7e-6762-45d4-8122-6b2c0b290c9a	Linux	CentOS 7.2 64bit	40 Account

After the image is accepted, it is displayed in the shared image list.

Figure 8-14 Viewing shared images

Public Images Private Images	Shared Images		
Reject Rejected Image			
Name J≡	ОЅ Туре	OS	Image Type
✓ copy_cn-north-4_migrate_test	Linux	CentOS 7.2 64bit	Full-ECS image(x86)

Step 5: Use the Shared Image to Create an ECS

Use the shared image to create an ECS and verify that the website is available on the ECS.

- Locate the row that contains the shared image copy_cnnorth-4_migrate_test, and click Apply for Server in the Operation column. The page for purchasing ECSs is displayed.
- 2. Set the billing mode, AZ, specifications, and network as needed to create an ECS. Retain the default value for **Image**.

Figure 8-15 Selecting an image

nage	Public image	Privale image	Shared image	Marketplace image	
	copy_cn-north-4_mig	rate_test Full-ECS Image	e)(40GB)		٣
	You have selected a ful ECS is created.	I-ECS image, which does	not allow you to use other	r data disk images to create data	disks. If

- 3. Wait for several minutes and check whether the new ECS is displayed in the ECS list.
- 4. Access the website to check whether the website is available on the new ECS. In the address bar of the browser, enter http://ECS EIP/index.html, for example, http://124.70.xxx.xxx/index.html. If the website can be normally accessed, the migration is successful. No further action is required.

Figure 8-16 Verifying the website

124.70. /index.html

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to <u>nginx.org</u>. Commercial support is available at <u>nginx.com</u>.

Thank you for using nginx.

9 Accessing OBS from an ECS over the Intranet

9.1 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 9-1 shows the access process.

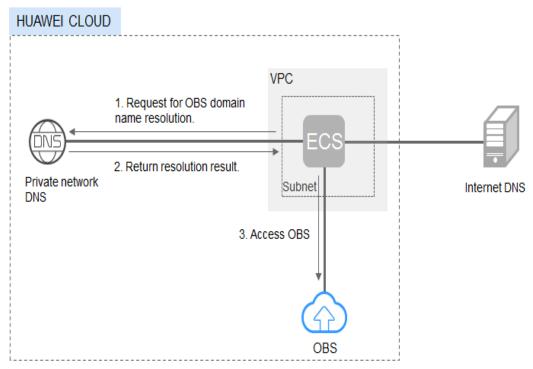


Figure 9-1 Accessing OBS through the intranet

Table 9-1 describes the services in the figure.

Table 9-1	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 saves costs.

• 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.

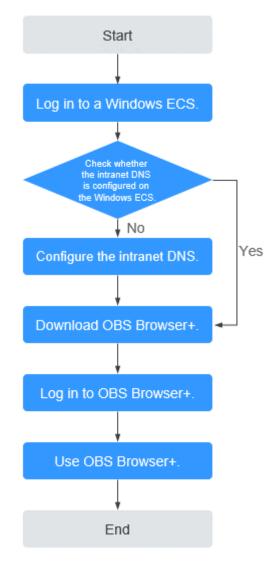
9.2 Accessing OBS over Intranet by Using OBS Browser+ on a Windows ECS

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.

You need to download OBS Browser+ over the Internet. Alternatively, you can download OBS Browser+ from a cloud server that can access the Internet and then transfer the downloaded OBS Browser+ to the current cloud server for installation.

Process

Figure 9-2 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 the Huawei Cloud official website and click Console.
- 2. On the home page of the console, choose **Compute** > **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 **How Do I Log In to My 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 Huawei Cloud?

- If no, go to Step 3.
- If yes, go to Step 5.

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 to 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 Huawei Cloud?**

• Method 2: Modifying the local DNS configuration

The intranet DNS configured in this method becomes invalid once the ECS is restarted. 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 Huawei Cloud?
- (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*: a 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. 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 Huawei Cloud?) You can also set this parameter to the IP address of a public DNS server.
- **Step 4** Check whether OBS is accessed over the intranet.

For details, see **How Do I Determine Whether OBS Is Being Accessed from an Intranet Connection**?

The global domain name of an OBS bucket is in the *Bucket name*.obs.mykualalumpur-1.alphaedge.tmone.com.my format.

Step 5 Download OBS Browser+.

For details, see **Downloading OBS Browser+**.

Step 6 Log in to OBS Browser+.

OBS Browser+ accesses OBS over a public network by default. When you log in to OBS Browser+ and add an account, set **Service** and **Server Address** as follows:

• 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.ap-southeast-1.myhuaweicloud.com:443

NOTE

For details about OBS regions and endpoints, see Regions and Endpoints.

Step 7 Start to use OBS Browser+.

After logging in to OBS Browser+, you can access OBS over the intranet from the Windows ECS to perform basic data access operations and other advanced settings.

For details, see **OBS Browser+ Tool Guide**.

----End

9.3 Accessing OBS over Intranet by Using obsutil on a Linux ECS

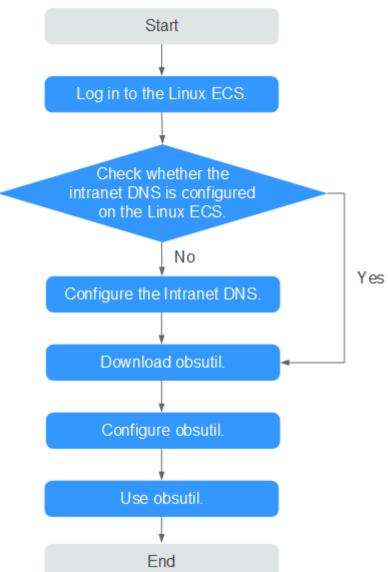
obsutil is a command line tool that can run Windows, macOS, and Linux operating systems. This section describes how to configure an intranet DNS server for a Huawei Cloud Linux ECS to access OBS over the intranet.

NOTE

You need to download obsutil over the Internet. Alternatively, you can download obsutil from a cloud server that can access the Internet and then transfer the downloaded obsutil to the current cloud server for installation.

Process

Figure 9-3 The process of accessing OBS over intranet by using obsutil on a Linux ECS



Procedure

Step 1 Log In to the Linux ECS.

- 1. Log in to the Huawei Cloud official website and click Console.
- 2. On the home page of the console, choose **Compute** > **Elastic Cloud Server**.

3. Select an ECS and log in to it.

The login mode is set during the Linux ECS creation.

For details about how to log in to the ECS, see How Do I Log In to My 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 Huawei Cloud?

- If no, go to Step 3.
- If yes, go to Step 5.
- **Step 3** Configure the Intranet DNS.

Change the DNS server address of the ECS to the intranet DNS provided by Huawei CloudDNS. To do this, you can change the DNS address of the VPC subnet or change the local DNS configuration.

• 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 to 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 Huawei Cloud?**

• Method 2: Modifying the local DNS configuration

The following uses an ECS running CentOS 6.x 64bit 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 insert 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

D 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 Huawei Cloud?
- The IP address of the new DNS server must be placed 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. 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 Check whether OBS is accessed over the intranet.

For details, see **How Do I Determine Whether OBS Is Being Accessed from an Intranet Connection**?

Step 5 Download obsutil.

For details about the latest version of obsutil and download link, see **Downloading obsutil**.

Step 6 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 Initializing Configurations 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 7 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

10 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 20.04 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

• An ECS running Ubuntu 20.04 has been created, and an EIP has been bound to it for internet access.

For details, see **Purchasing a Custom ECS** and **Assigning an EIP**.

• The VNC Viewer client has been installed on a local PC.

NOTE

Log in at https://www.realvnc.com/en/connect/download/viewer/ to download VNC Viewer.

Installing VNC Server

Ubuntu 20.04 has no GUI or VNC Server installed by default. In this example, Xfce, a compact lightweight desktop is used. Xfce is more compact and user-friendly than Gnome and KDE. It applies to remote ECS access.

1. Remotely log in to the ECS.

The username is **root**, and the password is the one you set during ECS creation.

- 2. Run the following command to update the software package list:
 - 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.

rootlecs-9240- : # Uncserver
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 (8), 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 prod	cess	ID 2738	
root@ecs-9240-	:~#		

2. Modify the **xstartup** file.

vim ~/.vnc/xstartup

Press i to enter insert mode and add the following 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
xrab Shundz Aresources xsetroot -solid grey
<pre>#x-terminal-emulator -geometry 80x24+10+10 -ls -title "\$VNCDESKTOP Desktop" &</pre>
#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.

root@ecs-9240-	:~# vncserver	
New 'X' desktop is ecs	-9240- :1	
Starting applications s Log file is /root/.vnc/		-
root@ecs-9240-	:~#	

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.

Configuring the ECS on the Management Console

Summany Inhound Dules Outhound Dules Associated In

- 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.

Figure 10-1 Modifying security group rules

ld Rule F	ast-Add Rule Delete	Allow Common Ports Inbour	td Rules: 6 Learn more about security grou	p configuration.			
Specity filter criter	ia.						
Priority ⑦	Action ③	Туре	Protocol & Port (2)	Source 💮	Description	Last Modified	Operation
] 1	Allow	IPv4	TCP : 5901		-	Apr 17, 2024 15:14:17 GMT+08:00	Modify Replicate Delet
) 1	Allow	IPv6	All	· 0	And the second s	Jun 27, 2023 14:54:20 GMT+08:00	Modify Replicate Delet
	Allow	IPv6 IPv4	AII ICMP : AII		special and a second se		Modify Replicate Delet
1 1 1							

Using VNC Viewer to Access an ECS

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

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 **1**.

🔁 ubuntu - Properties — 🗆	\times
General Options Expert	
	·
VNC Server:	
Name: ubuntu	
Labels	
To nest labels, separate names with a forward slash (/)	
Enter a label name, or press Down to apply existing labels	
Security	
Encryption: Let VNC Server choose \checkmark	
Authenticate using single sign-on (SSO) if possible	
Authenticate using a smartcard or certificate store if possible	
Privacy	,
OK Cance	1

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

V2 Encryption
Unencrypted connection
The connection to this VNC Server will not be encrypted.
VNC Server: (TCP)
Your authentication credentials will be transmitted securely, but all subsequent data exchanged while the connection is in progress may be susceptible to interception by third parties.
Don't warn me about this again on this computer.
Continue Cancel

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

R Authentication			×	
Authenticate to VNC Server				
Enter VNC Server credentials (Hint: NOT your RealVNC account details)				
Username:				
Password:	•••••		Ø	
Remember password Forgot password?				
		ОК	Cancel	

4. Verify the GUI of the Ubuntu 20.04 OS.

