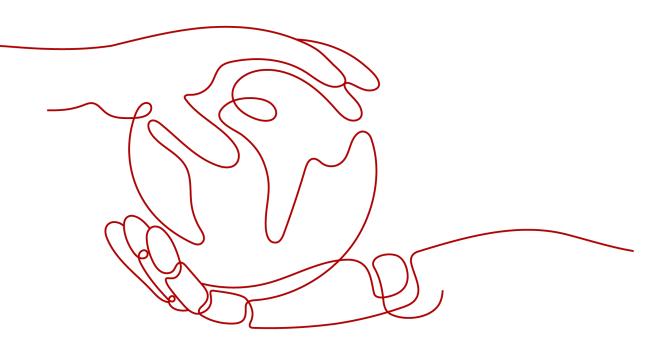
Elastic Cloud Server

Best Practices

 Issue
 02

 Date
 2024-03-06





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 for ECS	1
2 Migrating Servers to the Cloud	4
3 Enhancing Security for SSH Logins to Linux ECSs	7
4 Using VNC Viewer to Access a Linux ECS	13
5 Building Highly Available Web Server Clusters with Keepalived	19
6 Setting Up Websites	30
7 Setting Up a Discuz Forum	35
7.1 Overview	
7.2 Requesting Cloud Resources	
7.3 Building the Website	44
7.4 Configuring Features	
7.5 Visiting the Website	59
8 Setting Up a WordPress Website (Linux)	61
9 Setting Up an FTP Site (Windows)	74
10 Setting Up an FTP Site (Linux)	91
11 Setting Up Tomcat-based Java Web Environment (CentOS 7.4)	96
12 Manually Setting Up a Magento E-Commerce Website (Linux)	103
13 Building Microsoft SharePoint Server 2016	116
13.1 Purchasing and Logging In to an ECS	116
13.2 Adding AD, DHCP, DNS, and IIS Services	
13.3 Installing SQL Server	
13.4 Installing Microsoft SharePoint Server 2016	
13.5 Configuring Microsoft SharePoint Server 2016	
13.6 Verifying Microsoft SharePoint Server 2016	140
14 Manually Deploying LNMP (CentOS 7.2, PHP 7.0)	144
15 Manually Deploying Docker (CentOS 7.5)	151

16 Deploying an ECS for Handling Text Messages from an Official WeChat Acco	
17 Manually Deploying GitLab (CentOS 7.2)	1 <mark>64</mark>
18 Manually Deploying RabbitMQ (CentOS 7.4)	167
19 Manually Deploying a Ghost Blog (on an ECS Running Ubuntu 20.04)	172
20 Manually Deploying Node.js (CentOS 7.2)	179
21 Setting Up Master-Slave Replication on PostgreSQL	183
22 Manually Installing a BT Panel (CentOS 7.2)	187
23 Accessing OBS from an ECS over the Intranet	189
23.1 Overview	189
23.2 Accessing OBS over Intranet by Using OBS Browser+ on a Windows ECS	191
23.3 Accessing OBS over Intranet by Using obsutil on a Linux ECS	195
24 Restoring Accidentally Deleted Data on a Linux ECS Using Extundelete	199
25 Installing and Deploying Jenkins on an ECS	201

Best Practices for ECS

To use ECSs more securely, reliably, flexibly, and efficiently, you are advised to follow the following best practices.

Access

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

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 **Logging In to an 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.

• 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.

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**.

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 **Step 1: Configure Basic Settings**.

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.

2 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.

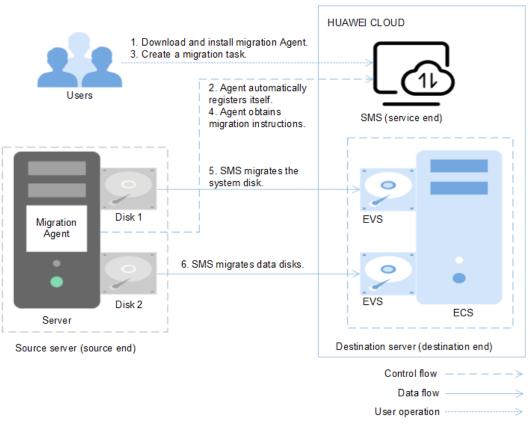


Figure 2-1 SMS working principle

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

- 1. Install the migration Agent on the source server. For details, see **How Do I Download and 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 the migration task.
- Service end: indicates the SMS service.

Service entry

SMS procedure: Creating a Migration Task.

SMS introduction: Server Migration Service.

Image Import

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

3 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 3-1 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 3-1 Before the change

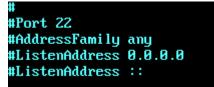


Figure 3-2 After the change



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

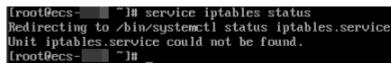
Adding a Firewall Rule to Open a Specified Port

CentOS 7 series use Fireware firewalls, but not 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 - IPv Loaded: loaded (/usr/ Active: active (exite Process: 23744 ExeCta	ce iptables status emctl status iptables.service A firewall with iptables 'lib/systemd/system/iptables.service; disabled; vendor preset: disabled) d) since Tue 2019-04-16 10:42:53 CST: 3s ago rt=/usr/libexec/iptables/iptables.init start (code=exited, status=0/SUCCESS) :xited, 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-	systemd[1]: Started IPv4 firewall with iptables.

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 3-3**.

Figure 3-3 Security group rules

Type 🗘	Protocol \$	Port/Range 🗘	Source \$	Description
IPv4	All	All	sg-9341 🕐	-
IPv4	TCP	22	0.0.0.0/0 ②	Permit default Linux SSH port.
IPv4	TCP	3389	0.0.0.0/0 ②	Permit default Windows remote desktop port.
IPv4	TCP	5000	0.0.0.0/0 ⑦	

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 navigation pane on the left, 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 3-5, 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.

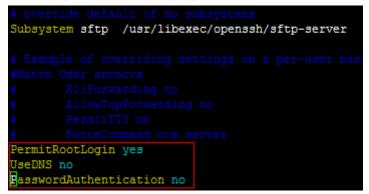
Figure 3-4 Bind Key Pair

key to log in	will 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 gin mode of the server and use only the key to log in to the server.
ECS Name	ecs-a51c-
IP Address	
Status	8 Bunning
New Key Pair	KeyPair-
Root 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". Therefore, the **PasswordAuthentication** value should be **no**. You only need to verify it.

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

7. Run the following command to restart sshd:

systemctl restart sshd

8. Attempt to log in to the ECS using Xshell or an SSH client. If password input is unavailable, as shown in **Figure 3-5**, the configuration is successful.

SSH User Authen	tication			?	x
Remote Host: Login Name: Server Type:	119.3. :500 root SSH2, OpenSSH	-		Z	5
	er user authentica vide necessary in			e meth	ods
© <u>P</u> assword	·				
Pass <u>w</u> ord:					
Public Key					
User <u>K</u> ey:			- B	rowse	•
Passp <u>h</u> rase:					_
C Keyboard <u>I</u> nt	eractive				
Use keyboar	d input for user auth	entication,			
Remember Pass	sword	OK		Cancel	

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 allow accesses only from the IP address ranges that may be used by the administrator.

The ECS may be logged in anywhere. Therefore, 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 of these IP addresses.

4 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 **Creating an ECS** and **Assigning an EIP and Binding It to an ECS**.

• The VNC Viewer client has been installed on a local PC.

D 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.

root@ecs-9240- :~# vncserver
You will require a password to access your desktops.
Password:
Verify:
Would you like to enter a view-only password (y/n)? n xauth: file /root/.Xauthority does not exist
New 'X' desktop is ecs-9240- :1
Creating default startup script /root/.vnc/xstartup
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/ecs-9240- :1.log
root@ecs-9240- :~#

- Password: consists of 6 to 8 characters. When the number of characters reaches the upper limit (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 proc	ess	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
xsetroot -solid grey
#x-terminal-emulator -geometry 80x24+10+10 -ls -title "\$UNCDESKTOP Desktop" &
#x-window-manager &
Fix to make GNOME work
export XKL_XMODMAP_DISABLE=1
/etc/X11/Xsession
startxfce4 &

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

sudo chmod +x ~/.vnc/xstartup

4. Restart VNC Server.

vncserver

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

root@ecs-9240-	:~# uncserver					
New 'X' desktop is ecs	-9240-	:1				
Starting applications specified in /root/.vnc/xstartup Log file is /root/.vnc/ecs-9240- :1.log						
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. The VNC port number is "5900+virtual desktop number", which is used by the VNC Viewer agent to access your ECS.

Configuring the ECS on the Management Console

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

Summary Inbound Rules Associated Instances							
Add Rule Fast-Add Rule Delete	Allow Common P	orts Inbound Rules: 7 Learn more abo	ut security group configuration.	С			
Protocol & Port 7 (?)	Туре	Source ⑦	Description	Operation			
	IPv4	sg-DISCUZ ⑦	-	Modify Replicate Delete			
ICMP : All	IPv4	0.0.0.0/0 ⑦	-	Modify Replicate Delete			
TCP : 22	IPv4	0.0.0.0/0 ⑦	-	Modify Replicate Delete			
TCP: 3389	IPv4	0.0.0.0/0 ⑦	-	Modify Replicate Delete			
C TCP : 5901	IPv4	0.0.0/0 ③		Modify Replicate Delete			

D NOTE

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

Using VNC Viewer to Access the ECS

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

NOTE

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

M	🖉 ubuntu18 - Properties 📃 💷 🔳	x
	General Options Expert	
		•
	VNC Server: :5901	
	Name: ubuntu18	
	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	
	Authenticate using single sign-on (SSO) if possible	
	Authenticate using a smartcard or certificate store if possible	
	Privacy	+
	OK Cance	el

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

V2 Encryption
(1) 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**.

V2 Authentica	tion	X
Ģ	Authentic	ate to VNC Server (TCP)
Username:		
Password:		Ø
🔲 Remembe	er password	Forgot password?
		OK Cancel

4. Verify the GUI of the Ubuntu 20.04 OS.



5 Building Highly Available Web Server Clusters with Keepalived

Scenarios

Virtual IP addresses are used for active and standby switchover of ECSs to achieve high availability. This way if one ECS goes down for some reason, the other one can take over and services continue uninterrupted.

This document uses CentOS 7.4 (64-bit) ECSs as an example to describe how to set up highly available web server clusters using Keepalived and Nginx.

Background

A web cluster consists of multiple web servers and a load balancer. Access requests will first be received by the load balancer, which then distributes the requests to backend web servers based on the load balancing policy.

In this document, Nginx is used to implement load balancing.

Network Topology

The data planning is as follows:

No.	ltem	Quant ity	Specification
1	VPC	1	192.168.0.0/16
	Subnet	1 192.168.0.0/24	
2	ECS	2	1 vCPU, 1 GB, CentOS 7.4 64bit
	IP address	2	ecs-HA1: 192.168.0.10 ecs-HA2: 192.168.0.20
3	EIP	1	122.xx.xx.189

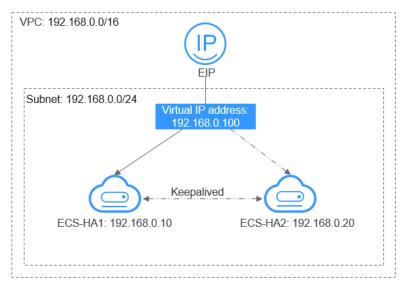
Table 5-1	Data	planning
-----------	------	----------

No.	Item	Quant ity	Specification
	Virtual IP address	1	192.168.0.100

Implementation methods:

- Configure the two ECSs in the same subnet to work in the active/standby mode using Keepalived.
- Bind a single virtual IP address to the two ECSs.
- Bind the virtual IP address to an EIP, then you can access the active and standby ECSs bound with the virtual IP address from the Internet.

Figure 5-1 Network topology



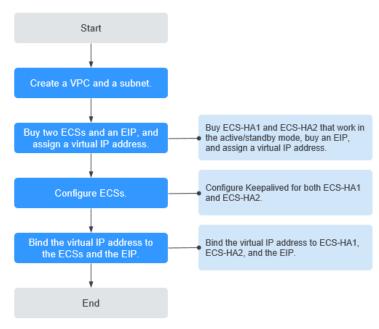
NOTE

- Select a region based on your service requirements.
- All cloud resources must be in the same region.

Procedure

The overall operation process is as follows:

Figure 5-2 Operation process



Step 1 Create a VPC and a subnet.

- 1. Log in to the management console.
- 2. Click Service List. Under Networking, click Virtual Private Cloud.
- 3. Click Create VPC.

Set required parameters as prompted based on Table 5-2.

Table 5-2 Paramete	r configurations
--------------------	------------------

Parameter	Example Value
Name (of the VPC)	vpc-НА
CIDR Block (of the VPC)	192.168.0.0/16
Name (of the subnet)	subnet-HA
CIDR Block (of the subnet)	192.168.0.0/24

4. Click Create Now.

Step 2 Apply for required cloud resources.

- 1. Buy ECSs.
 - a. Log in to the management console.
 - b. Click Service List. Under Compute, click Elastic Cloud Server.
 - c. Click **Buy ECS**.
 - d. On the **Buy ECS** page, set parameters as prompted. For details, see **Table 5-1**.

e. Set the ECS name to ecs-HA1 and ecs-HA2.

D NOTE

In this example, no data disk is purchased. You can buy data disks based on service requirements and ensure their service data consistency.

f. (Optional) Configure security group rules to ensure that the two ECSs can communicate with each other.

In this example, the two ECSs are in the same security group and can communicate with each other through the internal network by default. In this case, you do not need to configure rules.

Figure 5-3 Add Inbound Rule

Add Inbound	Add Inbound Rule Learn more about security group configuration.							
1 Inbound ru	Inbound rules allow incoming traffic to instances associated with the security group.							
	Security Group sg-fqy You can import multiple rules in a batch.							
Priority 🕐	Action	Protocol & Port (?)	Туре	Source ⑦	Description	Operation		
1	Allow v	TCP Example: 22 or 22-30 	IPv4 v	Security group (03fd]	Operation 👻		
			ОК	Cancel				

- 2. Buy an EIP.
 - a. Log in to the management console.
 - b. Click Service List. Under Networking, click Elastic IP.
 - c. Click **Buy EIP** and set parameters as prompted. For details, see **Table 5-1**.
- 3. Assign a virtual IP address.
 - a. Log in to the management console.
 - b. Click Service List. Under Networking, click Virtual Private Cloud.
 - c. In the navigation pane on the left, click **Subnets**.
 - d. In the subnet list, locate the target subnet and click its name.
 - e. On the **IP Addresses** tab page, click **Assign Virtual IP Address** and set parameters as prompted.

Step 3 Configure the ECSs.

- 1. Configure the ecs-HA1.
 - a. Bind EIP (122.xx.xx.189) to ecs-HA1.
 - i. Log in to the management console.
 - ii. Click Service List. Under Compute, click Elastic Cloud Server.
 - iii. In the ECS list, click the name of ecs-HA1.
 - iv. Click the EIPs tab and then Bind EIP.
 - v. On the **Bind EIP** page, select a NIC and an EIP, and click **OK**.

b. Connect to ecs-HA1 using SSH and run the following command to install the Nginx and Keepalived packages and related dependency packages:

```
yum install nginx keepalived -y
```

c. Run the following command to edit the **nginx** configuration file and save it:

vim /etc/nginx/nginx.conf

An example is provided as follows:

```
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.html;
               }
               #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;
                              }
      }
 }
```

d. Run the following command to edit the **index.html** file and save the file: **vim /usr/share/nginx/html/index.html**

```
An example is provided as follows:
Welcome to ECS-HA1
```

e. Run the following commands to set the automatic startup of Nginx upon ECS startup:

systemctl enable nginx

systemctl start nginx.service

f. Verify the access to a single Nginx node.

Figure 5-4 ECS-HA1 access verification



Welcome to ECS-HA1

g. Run the following command to edit the **keepalived** configuration file and save it:

vim /etc/keepalived/keepalived.conf

An example is provided as follows:

```
! 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 MASTER
           interface eth0
          mcast_src_ip 192.168.0.10
          virtual_router_id 51
           priority 101
           advert_int 1
           authentication {
                    auth_type PASS
                    auth_pass 1111
                   }
           unicast_src_ip 192.168.0.10
          virtual_ipaddress {
                    192.168.0.100
                    }
track_script {
       chk_http_port
        }
}
```

h. Run the following command to edit the **nginx** monitoring script and save it:

vim /etc/keepalived/chk_nginx.sh

An example is provided as follows:

```
#!/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
fi
```

chmod +x /etc/keepalived/chk_nginx.sh

i. Run the following commands to set the automatic startup of Keepalived upon ECS startup:

systemctl enable keepalived

systemctl start keepalived.service

- 2. Configure the ecs-HA2.
 - a. Unbind EIP (122.xx.xx.189) from ecs-HA1.
 - i. Log in to the management console.
 - ii. Click Service List. Under Compute, click Elastic Cloud Server.
 - iii. In the ECS list, click the name of ecs-HA1.
 - iv. Click the **EIPs** tab.
 - v. Locate the row that contains the EIP (122.xx.xx.189), and click **Unbind**.
 - b. Bind EIP (122.xx.xx.189) to ecs-HA2.
 - i. Log in to the management console.
 - ii. Click Service List. Under Compute, click Elastic Cloud Server.
 - iii. In the ECS list, click the name of ecs-HA2.
 - iv. Click the **EIPs** tab.
 - v. Click Bind EIP.
 - vi. Select a NIC and an EIP and click OK.
 - c. Connect to ecs-HA2 using SSH and run the following command to install the Nginx and Keepalived packages and related dependency packages:

```
yum install nginx keepalived -y
```

d. Run the following command to edit the **nginx.conf** configuration file: vim /etc/nginx/nginx.conf

An example is provided as follows:

```
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;
}
}
```

e. Run the following command to edit the **index.html** file:

```
vim /usr/share/nginx/html/index.html
```

An example is provided as follows:

Welcome to ECS-HA2

f. Run the following commands to set the automatic startup of Nginx upon ECS startup:

systemctl enable nginx systemctl start nginx.service

g. Test the access to a single Nginx node.

Figure 5-5 ECS-HA2 verification result



Welcome to ECS-HA2

h. Run the following command to edit the Keepalived configuration file:

vim /etc/keepalived/keepalived.conf

An example is provided as follows:

```
! 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 192.168.0.20
   virtual_router_id 51
   priority 100
   advert_int 1
   authentication {
          auth_type PASS
          auth_pass 1111
   unicast_src_ip 192.168.0.20
   virtual_ipaddress {
             192.168.0.100
             }
track_script {
   chk_http_port
   }
}
```

i. Run the following command to edit the **nginx** monitoring script and add execute permissions:

vim /etc/keepalived/chk_nginx.sh

```
An example is provided as follows:
```

```
#!/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
fi
```

chmod +x /etc/keepalived/chk_nginx.sh

j. Run the following commands to set the automatic startup of Keepalived upon ECS startup:

systemctl enable keepalived systemctl start keepalived

Step 4 Bind a virtual IP address to an ECS.

- 1. Unbind EIP (122.xx.xx.189) from ecs-HA2.
- 2. Bind the virtual IP address to ecs-HA1.
 - a. Log in to the management console.
 - b. Click Service List. Under Networking, click Virtual Private Cloud.
 - c. In the navigation pane on the left, click **Subnets**.
 - d. In the subnet list, locate the target subnet and click its name.
 - e. Click the **IP Addresses** tab, locate the row that contains the target virtual IP address, and click **Bind to Server** in the **Operation** column.
 - f. On the page that is displayed, select ecs HA1.
- 3. Bind the virtual IP address to ecs-HA2 by referring to 2.
- 4. Bind the virtual IP address to the EIP 122.xx.xx.189.
 - a. Log in to the management console.
 - b. Click Service List. Under Networking, click Virtual Private Cloud.
 - c. In the navigation pane on the left, click **Subnets**.
 - d. In the subnet list, locate the target subnet and click its name.
 - e. Click the **IP Addresses** tab, locate the row that contains the target virtual IP address, and click **Bind to EIP** in the **Operation** column.
 - f. On the page that is displayed, select the EIP (122.xx.xx.189).
 - g. Click OK.

----End

Verification

- 1. Run the **reboot** command to restart ecs-HA1 and ecs-HA2.
- 2. Remotely log in to ecs-HA1 through the management console.
- 3. Run the following command to check whether the virtual IP address is bound to the eth0 NIC of ecs-HA1:

ip addr show

As shown in **Figure 5-6**, the virtual IP address has been bound to the eth0 NIC of ecs-HA1.

Figure 5-6 Virtual IP address of ecs-HA1

[root@ecs-ha1 ~]# ip addr show					
1: lo: <loopback,up,lower_up> mtu 65536 qdisc noqueue state UNKNOWN qlen 1</loopback,up,lower_up>					
link/loopback 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 pfifo_fast state UP qlen 1000</broadcast,multicast,up,lower_up>					
link/ether fa:16:3e:a2:c5:72 brd ff:ff:ff:ff:ff:ff					
inet 192.168.0.10/24 brd 192.168.0.255 scope global dynamic eth0					
valid_lft 86066sec preferred_lft 86066sec					
inet 192.168.0.100/32 scope global eth0					
valid_lft forever preferred_lft forever					
inet6 fe80::f816:3eff:fea2:c572/64 scope link					
valid_lft forever preferred_lft forever					

4. Use a browser to access the EIP and check whether the web page on ecs-HA1 can be accessed.

If the information shown in Figure 5-7 is displayed, the access is normal.

Figure 5-7 ecs-HA1 access verification



Welcome to ECS-HA1

5. Run the following command to disable Keepalived on ecs-HA1:

systemctl stop keepalived.service

6. Run the following command to check whether ecs-HA2 has taken over the virtual IP address:

ip addr show

Figure 5-8 Virtual IP address of ecs-HA2

[root@ecs-ha2]]# ip addr show	
1: Io: <loopback,up,lower_up> mtu 65536 qdisc noqueue state UNKNOWN qlen 1</loopback,up,lower_up>	
link/loopback 08:08:08:08:00:00 brd 08:09:08:08:00:08	
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: <brdadcast,multicast,up,lower_up> mtu 1500 qdisc pfifo_fast state UP qlen 1000</brdadcast,multicast,up,lower_up>	
link/ether fa:16:3e:79:03:21 brd ff:ff:ff:ff:ff:ff	
inet 192.168.0.28/24 brd 192.168.0.255 scope global dynamic eth0	
valid_lft_04950sec_preferred_lft_04950sec	
inet 192.160.0.100/32 scope global eth0	
valid_lft forever preferred_lft forever	
inet6 fe80::f816:3eff:fe79:321/64 scope link	
valid_lft forever preferred_lft forever	
Unactive_ha2 11t	

7. Use a browser to access the EIP and check whether the web page on ecs-HA2 can be accessed.

If the information shown in Figure 5-9 is displayed, the access is normal.

Figure 5-9 ecs-HA2 access verification

← → C ① 122.1 2 189

Welcome to ECS-HA2

6 Setting Up Websites

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 6-1
 Summary on website setups

Website Setup Solution	How to Setup	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)	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 Setup	OS	Image and Resources	Description
Setting Up Tomcat- based Java Web Environme nt	Manual setup	Linux	Public imageTomcat 8.5.31JDK 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 provides solutions for 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, PHP 7.0)	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 CMS or website setup system that is free of charge.

Website Setup Solution	How to Setup	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 Setup	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 (on an ECS Running Ubuntu 20.04)	Manual setup	Linux	Public imageNginx 1.14.0MySQL 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 Setup	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.

7 Setting Up a Discuz Forum

7.1 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.

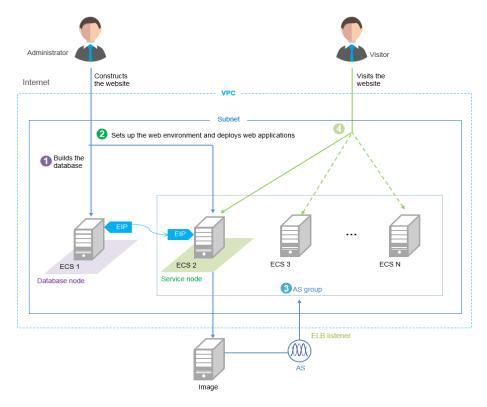
Solution

You can use the following solution to build a website.

Table 7-1	Solution	details
-----------	----------	---------

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

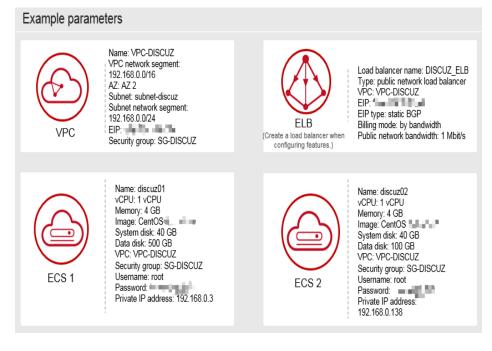
Logical Architecture



- 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.

7.2 Requesting Cloud Resources

Required Cloud Resources



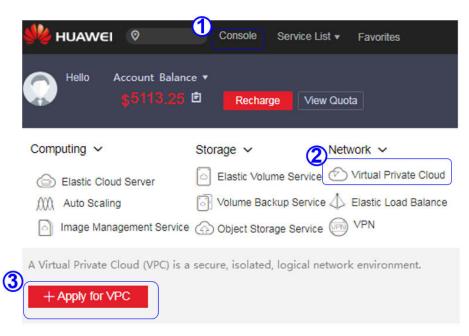
NOTE

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 7-1 Applying for a VPC



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

Figure 7-2 Configuring parameters

ply for VPC 🔞	
Basic Inform	ation
Regio	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 Settin AZ: Subnet Name	5 AZ2 AZ1 Enter the subnet name.
CIDR:	192.168.0.1 / 24
Gateway:	192.168.0 .1
DNS Server A	ddress 1: 100.125.1 .250
DNS Server A	ddress 2: 114.114.114
	6
	I have read and agreed to the Huawei Virtual Private Cloud Service Agr
	Create N

Buying an EIP

Ð	Elastic IP Address @	2	Buy EIP
Network Console	You can create 5 more EIPs. All	Q	search by Tag ⊭ C
Dashboard /irtual Private Cloud	EIP/ID Status Bound Private Type Bandwidth Sh Bandwidth Siz Billing Mode	Operation	1
Security Group			
3andwidth /PC Peering			
/PN Direct Connect			
Apply for EIP @			
Specify [Details Confirm Order		Pay
1	2		3
Basic Information	n		
Region:	To change the region, use the region selector in the upper left corner of this page	÷.	
Type:	Dynamic BGP Static BGP 💿		
	3 Select the billing mode:		
Billing Mode:	Yearly/Monthly On-demand • Monthly/Yearly • On-demand		
Tag:	To comply with best practices, it is recommended that you use the predefined tag function your resources. View Predefined Tag	provided by	r TMS to add tags to
	Enter a tag key. Enter a tag value.		
	You can add 9 more tags.		
Select Bandwidth:	Allocate new Use existing discuz_ip		
Sharing Type:	Exclusive Shared		
snanng type.	The sharing type cannot be changed after being specified.		
Charged By:	Traffic		
sharged by.	After specified, this parameter value cannot be changed.		
Bandwidth Size (Mbit/s):	IMbit/s		
	O	1	
4	1 100 200 3	300	
Quantity			
Quantity:	- 1 + You can create 2 more EIPs. To apply for a higher EIP quota, click Apply for Higher Qui	ota	
IP Price \$0.01/hour		G	5
ublic Network Traffic Price	\$0.15 _{/GB}		Apply Now
he estimated price is for re	ference only and may vary from the final price in your bill Price Details		
EIP Price $\$0.0$	1/hour Public Network Traffic Price \$0.15/GB		
The estimated price is f	or reference only and may vary from the final price in your bill. Price Details		
	6 I have read and agreed to the Huaw	ei VPC Ser	vice Announcement
	Back		ubmit Order
		1	

Creating a Security Group and Adding Rules

Ø	Security Group @		2 + Create Se	curity Group
Network Console	You can create 97 more security grou	ps and 4984 more security grou	ip rules.	QC
Virtual Private Cloud	Security Groups Name/ID	Description	Operation	
Security Group				
Network ACL				×
Elastic IP Address		Create Se	ecurity Group	
Bandwidth		* Name:	SG-DISCUZ	
VPC Peering		* Name.	SG-DISCOZ	
VPN		Description:		
Direct Connect				
			0/64	
		4	OK Cancel	
\bigcirc	Security Group @		+ Create Secu	rity Group
Network Console	You can create 97 more security groups	and 4984 more security group	rules. V 🔻	QC
Dashboard				
Virtual Private Cloud	Security Groups Name/ID	Description	Operation 5	
Security Group	SG-DISCUZ 233e23a0-07a3-4539-9b4d-92850	-	Fast Add Rule Add Rule More -	
Network ACL	Add Rule		×	
Elastic IP Address	6			
Bandwidth	* Transfer Direction:	Inbound Outbound		
VPC Peering	* Protocol:	CP -	After an access rule is	added to a
VPN	* Port Range: 8	0	security group, ECSs i group are protected by	in the security
	Protocol and set Port			
Range to 80.		IP Address Security G	Group	
	S	G-DISCUZ(233e 👻		
	8			
		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 Service	e 💮 Object Storage S	
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.

Figure 7-3 Basic configuration

Image:	Public Image Private Image	Shared Image	Select an image for the ECS.
	CentOS CentOS	bit(40GB) - C	
Disk:			VS disk for the ECS as a data disk.
	System Disk Common I/O - @ - 40 + GB 100-1,000 IOPS	Data Disk Common I/O	
)		Select the created VPC	and security group.
VPC 🕜 :	VPC-DISCUZ *	View VPC C	
Security Group	SG-DISCUZ (Inbound:TCP/ × -	C Manage Security Group Learn	more about how to configure a security group

			ect an image for the ECS.
	CentOS - CentOS 6.3 64	lbit(40GB) - C	
Disk:			t for the ECS as a data disk.
	System Disk Common I/O - @ - 40 + GB 100-1,000 IOPS	Data Disk Common I/O GB 100–1,000 IOPS	Data Disk You can attach 22 more disks.
		Select the created VPC and se	curity group.

Figure 7-4 Network configuration

Figure 7-5 Advanced settings

	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.
	\smile	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.
(11	Username:	root
	Password:	Security Level: Low Keep your password secure. The system cannot detect your password.
	Confirm	
	Password:	
(12)	ECS Name:	discuz01
C		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.

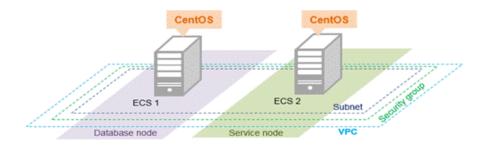
Figure 7-6 Confirming the configurations

Price \$0.03/Hour The estimated price is for reference only and may vary from the final price in your bill Price D	ıy Now
I have read and agreed to the Huawei Ela	ement and Huawei Image ment Service Agreement Submit Order

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

7.3 Building the Website

Requested Cloud Resources



Example parameters ECS 2 VPC ECS 1 Serves as a service node to set A VPC can connect to the Serves as a database node up the website environment and deploy website code. Internet through an EIP to deploy the database Name: discuz02 vCPU: 1 vCPU Name: VPC-DISCUZ Name: discuz01 vCPU: 1 vCPU VPC network segment: 192.168.0.0/16 Memory: 4 GB Image: CentOS System disk: 40 GB AZ: AZ 2 Subnet: subnet-discuz Subnet network segment: Data disk: 500 GB VPC: VPC-DISCUZ VPC: VPC-DISCUZ Security group: SG-DISCUZ 192.168.0.0/24 Security group: SG-DISCUZ EIP Security group: SG-DISCUZ Username: root Username: root Password: Private IP address: 192.168.0.138 Password: Private IP address: 192.168.0. 3

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**.

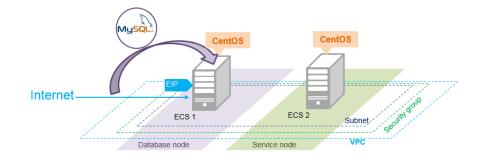
2. Discuz X3.3 (UTF-8)

Discuz X3.3 (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 X3.3 (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 --noqpgcheck

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:

```
# systemctl status mysqld.service

mysqld.service - MySQL Server
Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2021-08-23 10:54:55 CST; 7s ago
Docs: man:mysqld(8)
http://dev.mysql.com/doc/refman/en/using-systemd.html

Main PID: 7873 (mysqld)
CGroup: /system.slice/mysqld.service

7873 /usr/sbin/mysqld --daemonize --pid-file=/var/run/mysqld/mysqld.pid

Aug 23 10:54:49 ecs-adc3-420652-aed6 systemd[1]: Starting MySQL Server...
Aug 23 10:54:55 ecs-adc3-420652-aed6 systemd[1]: Started MySQL Server.
```

3. Obtain the password of user **root**, which was automatically set during MySQL installation:

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

Information similar to the following is displayed: 2021-08-16T11:33:37.790533Z 1 [Note] A temporary password is generated for root@localhost: ;8nPd29lhs,k

4. Harden MySQL.

mysql_secure_installation

Securing the MySQL server deployment.

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

New password: #Enter the new password.

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

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

... skipping.

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

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

Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network.

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

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

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

- Removing privileges on test database... Success.

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

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

All done!

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 (;).

- Refresh the user list and allow all IP addresses to access the database.
 update user set host='%' where user='root' LIMIT 1;
- 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.

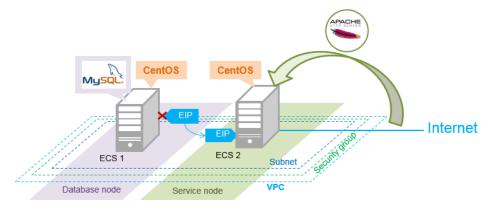
quit

- 11. Restart MySQL.
 - systemctl restart mysqld
- 12. Enable MySQL to automatically start upon system boot.

systemctl enable mysqld

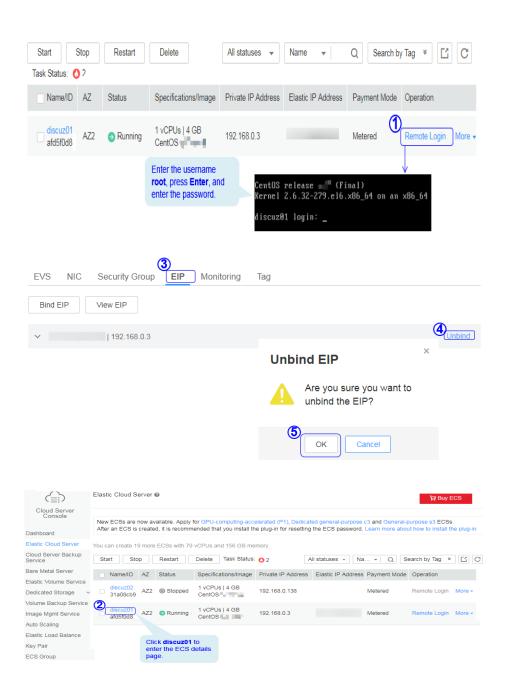
- 13. Disable the firewall. systemctl stop firewalld.service
- 14. Check the firewall status. systemctl status firewalld

Setting Up the Web Environment



Install the web environment.

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



	Elastic Cloud Server 🖗 🙀 Buy ECS
Cloud Server Console Dashboard	New ECSs are now available. Apply for GPU-computing-accelerated (P1), Dedicated general-purpose c3 and General-purpose s3 ECSs. After an ECS is created, it is recommended that you install the plug-in for resetting the ECS password. Learn more about how to install the plug-in
Elastic Cloud Server	You can create 19 more ECSs with 79 vCPUs and 156 GB memory.
Cloud Server Backup Service	Start Stop Restart Delete Task Status: O 2 All statuses - Na + Q Search by Tag * C
Bare Metal Server	Name/ID / Specifications/Image Private IP Address Flastic IP Address Payment Mode Operation
Elastic Volume Service Dedicated Storage ~	Image: State of the s
Volume Backup Service Image Mgmt Service	Giscuz01 AZ2 O Running 1 vCPUs 4 GB CentOS 192.168.0.3 Metered Remote Login More -
Auto Scaling	
Elastic Load Balance	
Key Pair	
ECS Group	

- 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 (php-fpm), 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

- Enable httpd to automatically start upon system boot.
 chkconfig httpd on
- Start php-fpm.
 service php-fpm start
- 4. Enable php-fpm to automatically start upon system boot. chkconfig php-fpm on
- 5. Disable the firewall.

systemctl stop firewalld.service

6. Check the firewall status again.

systemctl status firewalld

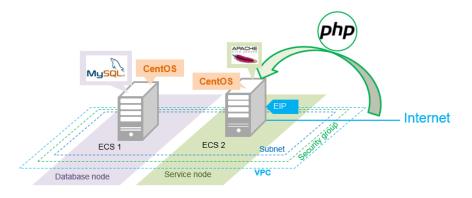
- Start MySQL.
 systemctl start mysqld
- 8. Enable MySQL to automatically start upon system boot.

systemctl enable mysqld.service

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

u can read this page it means that the Apache HTTP server installed at this site is
ou are the website administrator:
may now add content to the directory /vac/ww/btsl/. Note that until you do so, ple visiting your velosite will see this page and not your content. To prevent this page ever being used, follow the instructions in the
/etc/httpd/conf.d/welcome.conf.
are free to use the images below on Apache and CentOS Linux powered HTTP vers. Thanks for using Apache and CentOS!
Istribution derived from sources freely provided to the public by Red Hat. As such, organization that builds CentOS. We mainly change packages to remove upstream

Deploying the Website Code



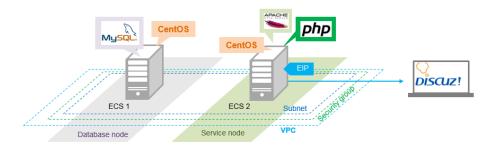
- 1. Decompress the **Discuz_X3.3_SC_UTF8.zip** package to the **Discuz_X3.3_SC_UTF8** folder.
- Use WinSCP to upload the update file in the Discuz_X3.3_SC_UTF8 folder to the /var/www/html directory on ECS discuz02. For details, see WinSCP documents.
- 3. Log in to **discuz02** and run the following 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.



7.4 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	ess Ø					Apply for EIP
Network Console Dashboard	You can create 18	more EIPs.			All 👻 EIP	•	QC
Virtual Private Cloud Security Group	EIP/ID	Status	Bound Private IP Address	Туре	Bandwidth Size (Mbit/s)	Billing Mode	Operation
Network ACL	9488617f-6a28-4	8 Bound	192.168.0.138	Static BGP	1	On-demand	Bind Unbind Release
Bandwidth							
VPC Peering							
VPN							
Direct Connect							

Creating a Load Balancer

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

ال HUAWEI 🛛	Console Sen	vice List 🔻 Favorites
Hello Account Balan x5113.25		View Quota My Packages
Computing ~	Storage 🗸	Network ~
Elastic Cloud Server	Elastic Volume S	ervice 🕑 Virtual Private Cloud
Cloud Server Backup Service	e 🕞 Volume Backup S	Servier Elastic Load Balance
Cloud Container Engine	Object Storage Se	ervice 🥜 Direct Connect
Load Balancer @	5	+ Create Load Balancer

2. Specify the parameters and submit the application.

Spec	ify Details	Confirm Specifications	Finis
	1	2	3
Basic Informatic	on		
Region:	Asia Pacific-HongKo	To change the region, use the region selector in the upper left	t corner of this page.
Name:	DISCUZ_ELB	Enter a name for your load balancer.	
/PC:	VPC-DISCUZ	Select the VPC to which the load balancer below ble, apply for a new one. View VPC	ngs.
Subnet	subnet-discuz(19	View Subnet C	
_B Virtual IP Address	: Automatic M	anual	
EIP @:	Do Not Use	xisting EIP	
Elastic IP Address:		View EIP C Use an existing EIP.	
		9	
he estimated price is	for reference only and may var	y from the final price in your bill. Price Details	Create Now
		I have read and agreed to the Huawei Elastic Load Balance	e Agreement

Configuring the Load Balancer

		Load Balancer	0					+	Create Load Balan	icer
	Cloud Server Console	Load Balancer	Certificate	Click		balancer name	e DISCUZ_I	ELB to view the		
	Dashboard	You can create 9 m	nore load balan		-			N	(C
	Elastic Cloud Server									
	Elastic Volume Service	Name/ID	Statur	Public IP	Address	Service IP Add	dress ervice	Subnet	Operation	
	Volume Backup Service	DISCUZ ELB 826fa0df8a92	Running					subnet-discuz	Delete	
	Image Mgmt Service									
~	Auto Scaling									
U	Elastic Load Balance	Add Listener	fou can add 10	more listen	iers.					
	Key Pair	Name/ID	Status	6	LB Protoco	l/Port	ECS Protoco	ol/Port		
	ECS Group									
	200 01000									
	Add Listener	discuz-listener		(TCP) a port nu • ECS P	and layer imber to 8 rotocol/F	7 (HTTP) load 0. ort: specifies t	l balancing). the protocol	Select TCP for and port that EC	ng services (layer 4 Protocol, and set t CSs use to provide	
	LB Protocol/Port:	TCP 👻 8	30	service	ICP IS	selected for P	rotocol, and	d port 80 is used		
		The value range	es from 1 to 655	35.						
	ECS Protocol/Port:	TCP 👻 8	30							
		The value range	es from 1 to 655	35.	Н	ealth Check Co	onfiguration			
	LB Mode 👩 :	Round robin	•			neck Mode:	то	P 👻 80		
	Sticky Session:	\bigcirc			5		Th	e value ranges fror	m 1 to 65535.	
	Stickiness Duration (min):	1 TI	he value ranges	from 1 to 6	0.	terval (s) 👩 :	2		lue ranges from 1 to 5.	
	Description:				Ti	meout (s) 🔞 :	5	The val	lue ranges from 1 to 50).
				0/128		ealthy Threshold	@ : 3	The val	lue ranges from 1 to 10	D.
	Interval (s): specifies the interva value is 2. Timeout (s): specifies the maxin					bealthy Thresho	old 🔞 : 🛛 3	The val	lue ranges from 1 to 10	D.
	recommended value is 5. Healthy Threshold: specifies th checks necessary for an ECS to	e number of consecu	tive successful h	health			ОК	Cancel		
•	is 3. Unhealthy Threshold: specifies necessary for an ECS to be cons Success response time: 6 secon Failure Response Time: 11 seco	sidered unhealthy. Th ds (2 x 3 = 6)					6	Cantel		

Creating Images

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

		HUAWEI	0	1 c	onsole Ser	vice List 🔻 Favoril	tes
		Hello A		Balance ▼ 3.25 ট	Recharge	View Quota My	/ Packages
	Com	puting 🗸		Storag	je 🗸	Network 🗸	
	2	Elastic Cloud	d Server) [] EI	astic Volume S	ervice 🕐 Virtual F	Private Cloud
	6			Service 🔄 Vo	olume Backup	Service 📣 Elastic L	oad Balance
	\	Cloud Conta	iner Engi	ine 💮 Ot	oject Storage S	ervice 🥜 Direct C	onnect
			4	Stop t	he ECS befo	re creating an ima	ige.
	Sta	rt Stop	R	estart De	elete Task	Status: 🙆 2	
		Name/ID	AZ	Status	Payment Mo	de Operation	
3		discuz02 31a08cb9	AZ2	Running	Metered	Remote Logi	n More -
		discuz01 afd5f0d8	AZ2	Stopped	Metered	Remote Logi	n More -

2. Configure the parameters and submit your request.

		Name/ID	AZ	Status	Specifications/Image	Private IP Address	Payment Mode	Operation	
		discuz02 31a08cb9	AZ1	Stopped	1 vCPUs 4 GB CentOS	192.168.0.138	Metered	Remote Login More	Modify Specifications
		discuz01 afd5f0d8	AZ1	Stopped	1 vCPUs 4 GB CentOS	192.168.0.3	Metered	Remote Login More	Make Image 6
(7)	* Sou	rce:	ECS	Image Fi	le				Reinstall OS Change OS Start
1	* ECS		discuz02			Select			Stop Restart
			OS: Cer	etails: discuz02 ntOS Disk: 40 GB					Delete
	Enci	ryption: U	nencrypte	ed 😡	ji I	10	reed to the Huawei Ela	astic Cloud Server Agreement	and System Image Disclaimer
	* Nam	ne:	discuz_c	entOS]		Previous	Submit Application
8						Apply Now		(1)	

Configuring AS

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

👋 HUAWEI	• 1 ₀	onsol	e Sen	vice List 🔻 🛛 Fa	avorites
Hello A	ccount Balance ▼ ×5113.25 ট	Rec	harge	View Quota	My Packages
Computing 🗸	Stora	ge 🗸		Networ	k ~
 Elastic Cloud Cloud Server Auto Scaling Auto Scaling 	Backup Service 🕞 V	olume bject S	Backup S	Service 📣 Ela ervice 🥏 Dir	tual Private Cloud Istic Load Balance ect Connect Configuration
AS Group Name:	as-group-discuz		for the AS gro An AS group o	up.	stances, and Max. Instances Expected Instances can be
Cooling Duration (s): AZ:	0 2 10 900 AZ2 ×		use ELB for is used for h Check Inter ELB check every five i The health added for t	health check and then s ealth check. Specify He val, and Instance Rem is the health of ECSs in minutes.	the selected security group s been set when the listener is er.
VPC: * Subnet: * Security Group:	VPC-DISCUZ(192.168.0.0/16) subnet-discuz(192.168.0.0/ × SG-DISCUZ (Inbound: - Outboun	View▼ C ③	VPC		iow to configure a security group @
	Inbound: - Outbound: - Do not use O Use ULB View ULE Load Balancer: DISCUZ_E •				on a configure a coordiny group 🥁
* Health Check Method:	ELB health check	•	0		
★ Health Check Interval:	5 minutes	•			
* Instance Removal Policy: * Release EIP on Instance Removal:	Oldest instance created based on the second of the second	h ext			

		ing AS confi guration or create a new AS c onfiguration. You can also change the AS configuration of an existing AS gr
	Basic Informatio	ion
*	Configuration Name:	as-config-discuz
*	Configuration Template:	Create a new specifications template Use specifications of an existing ECS
5	Specifications	
*	ECS Type:	General-purpose Memory-optimized Disk-intensive GPU-acceleration
		First generation Second generation Third generation
*	vCPU:	1vCPUs 2vCPUs 4vCPUs 8vCPUs 16vCPUs 32vCPUs
*	Memory:	1GB 2GB 4GB
		Selected Specifications: s1.medium 1 vCPUs 4 GB
	mage 10 Public Image F	Private Image Shared Image you have created.
	Image:	
	inage.	discuz_centOS
Elastic IP Addr Elastic IP Address		Automatically Assign
	Do Not Use	Automatically Assign
	Do Not Use	ssigns to each ECS an EIP that exclusively uses bandwidth. If you select this option, check the EIP quota. If the quota is y for a higher quota.
Elastic IP Address	C Do Not Use Automatically ass insufficient, apply	ssigns to each ECS an EIP that exclusively uses bandwidth. If you select this option, check the EIP quota. If the quota is by for a higher quota.
Elastic IP Address • Specifications: • Charging Mode:	Do Not Use Automatically ass insufficient, apply Dynamic BC	ssigns to each ECS an EIP that exclusively uses bandwidth. If you select this option, check the EIP quota. If the quota is y for a higher quota. GP Static BGP BGP(Discontinued) dth By traffic
Elastic IP Address • Specifications: • Charging Mode:	Do Not Use Automatically ass insufficient, apply Dynamic B0 By bandwid 1Mbit/s	ssigns to each ECS an EIP that exclusively uses bandwidth. If you select this option, check the EIP quota. If the quota is y for a higher quota. GP Static BGP BGP(Discontinued) dth By traffic 1 Mbit/s
Elastic IP Address • Specifications: • Charging Mode: • Bandwidth:	Do Not Use Automatically assist insufficient, apply Dynamic BC By bandwid 1Mblt/s 1	ssigns to each ECS an EIP that exclusively uses bandwidth. If you select this option, check the EIP quota. If the quota is ty for a higher quota. I Mbit/s 50 100
Elastic IP Address • Specifications: • Charging Mode:	Do Not Use Automatically ass insufficient, apply Dynamic B0 By bandwid 1Mbit/s	ssigns to each ECS an EIP that exclusively uses bandwidth. If you select this option, check the EIP quota. If the quota is ty for a higher quota. I Mbit/s 50 100
Elastic IP Address + Specifications: + Charging Mode: Bandwidth: Login	Do Not Use Automatically ass insufficient, apply Dynamic BC By bandwid Mblt/s 1 2 1 2 1 2 1 2 2 1 2 2 1 2 2	signs to each ECS an EIP that exclusively uses bandwidth. If you select this option, check the EIP quota. If the quota is y for a higher quota. GP Static BGP BGP(Discontinued) dth By traffic 50 100
Elastic IP Address * Specifications: Charging Mode: Bandwidth: Login * Login Mode:	C Do Not Use Automatically as insufficient, apply Dynamic BC By bandwid 1Mbit/s 1 1 Key Pair	signs to each ECS an EIP that exclusively uses bandwidth. If you select this option, check the EIP quota. If the quota is y for a higher quota. GP Static BGP BGP(Discontinued) dth By traffic 50 100
Elastic IP Address	C Do Not Use Automatically as insufficient, apply Dynamic BC By bandwid 1Mbit/s 1 1 Key Pair	ssigns to each ECS an EIP that exclusively uses bandwidth. If you select this option, check the EIP quota. If the quota is y for a higher quota. GP Static BGP BGP(Discontinued) dth By traffic 1 Mbit/s 50 100 Account Password
Elastic IP Address	C Do Not Use Automatically as insufficient, apply Dynamic BC By bandwid 1Mbit/s 1 1 Key Pair	ssigns to each ECS an EIP that exclusively uses bandwidth. If you select this option, check the EIP quota. If the quota is y for a higher quota. GP Static BGP BGP(Discontinued) dth By traffic 1 Mbit/s 50 100 Account Password Security Level: Keep your password secure. The system cannot retrieve your password.

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		View AS Policy Disabl	e More •
	2							
-	2 ance AS Po	Notification	Tag Lifecycle Ho	ook				
Monitoring Inst	ance AS Po	Notification	Tag Lifecycle Ho	pok				

Add Policy	×
* Policy Name:	is-policy-discuz-cpu
* Policy Type:	Alarm Scheduled Periodic CPU alarm policy: When the CPU
* Alarm:	usage exceeds 70% for three consecutive times, an ECS will b added.
* Alarm Name: a	is-alarm-cpu
6 * Trigger Condition: C	2PU Us ▼ Max. ▼ > ▼ 70 %
* Monitoring Interval: 5	minutes -
* Consecutive Occurrences: 3	
Scaling Action: A	dd ▼ 1 instan ▼
Cooling Duration (s): 9	00
(7	OK Cancel
	Calicel
Add Deliev	
Add Policy	
* Policy Name	as-policy-cpu-02
* Policy Type	Alarm Scheduled Periodic
* Alarm	Create Alarm Rule
* Alarm Name	as-alarm-cpu-02
* Trigger Condition	CPU Usage 💌 Min. 💌 < 💌 30
	To check whether monitoring metrics Memory Usage, Inba
	Outcoming Rate, or Inband Incoming Rate are supported b
	different OSs, see the Elastic Cloud Server User Guide.
* Monitoring Interval	5 minutes 👻
* Consecutive Occurrence	es 3 ⑦
Scaling Action	Reduce - 1 instances -
contraining metropy stational	
Cooling Duration (s)	900 ⑦
	OK Cancel

3. Add AS instances.

			Start ECS	1		×	
			Are ye	ou sure you wa	nt to start	the following ECSs?	
Cloud Server Console			Name	Statu	IS	Expire At	
			discuz02	@ S	topped		
Start Stop Res Name/ID discuz02 discuz01 discu201 discu201 discu201	AZ AZ AZ	dding them to the Task Status: • 2 Status • Stopped • Stopped		. Ок	Cancel		up Service vice
Name Status	AS Configuration	Current Insta Expe	ected Instan	Min. Instances	Max. Instan	Ces Operation	
as-group-discuz 🕑 Enabled	as-config-discuz	0	1	1		View AS Policy Disable	e More -
Monitoring Instance AS Por Add Remove Remove Add		Tag Lifecycle Ho ore • @	ok		c	×	
Max. Instances in a Batch: 10							
Available Instances: En	ter a name. C	C Selected Ins	tances:				
9 Name	ID	Name	ID		Opera		
discuz02	31a08cb9-f2fc-4727	-8a5 discuz02	31aD	8cb9-f2fc-472	Delete		
	10	OK Cancel					

4. Modify AS policies.

2	•						
👐 HUAWE	≣I ⊘	Console	Service List 🔻 Fa	avorites			
Hello Hello	Account Bala x5113,2		View Quota	My Packages			
Computing 🗸		Storage 🗸	Network	< ~			
🙆 Elastic Cle	oud Server	Elastic Volu	me Service 🕐 Virt	ual Private Cloud			
2 Cloud Ser	ver Backup Ser	vice 🕞 Volume Bac	kup Service 📣 Elas	stic Load Balance			
Auto Scali			ige Service 🥜 Dire				
Name	Status	AS Configuration	Current Instances	Expected Instances	Min. Instances	Max. Instances	Operation
as-group-discuz	Enabled	as-config-discuz	0	2	1	10	View AS Policy Disable More -
						₩ M	hange AS Configuration odify ew Details
						D	elete

Min. Instances:	1	Set Min. Instances to 1 to ensure that ECS discuz02 to not be removed from the AS group.
Expected Instances:	2	
Max. Instances:	10	
Cooling Duration (s):	900	
Health Check Method:	ELB health check	•
Health Check Interval:	5 minutes	•
Instance Removal Policy:	Oldest instance created ba	•
lotification Mode:	By email 🕜	
Release EIP on Instance Remov	al: 💽	
	security group, and load balancing configu S instances, and does not have any ongo	ation only when the AS group has not been ing scaling actions.

Verifying the Configuration

1. Obtain the EIP of the load balancer.

👋 HUAWEI	0	Console	Service List ▼ Favo	prites
Hello A	ccount Balan \$5113.25		rge View Quota	
Computing 🗸		Storage 🗸	Network	~
 Elastic Cloud Auto Scaling Image Manage 		Volume Ba	ackup Service Lasti	I Private Cloud
Name/ID	Status	Туре	Service IP Address	VPC
DISCUZ_ELB 826fa0df8a924	🖯 Running	Public network		VPC-DISCUZ

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**.

7.5 Visiting the Website

Filing the Website

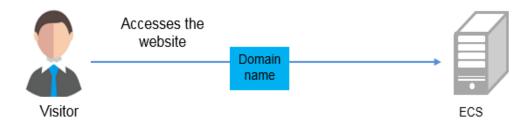
According to national regulations, if the servers used to deploy the website are located in the Chinese mainland, Internet Content Provider (ICP) licensing is required. The domain name that is not licensed cannot be used to access the website.

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.



8 Setting Up a WordPress Website (Linux)

Application Scenarios

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

Architecture

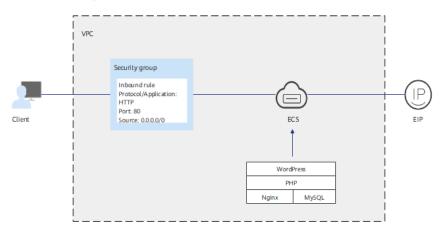


Figure 8-1 Setting up a WordPress website on a Linux ECS

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 8-1 Resources and costs

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: • Protocol/Application: HTTP • Port: 80 • Source: 0.0.0.0/0	Free
ECS	 Billing mode: Yearly/ Monthly AZ: AZ1 Flavor: s6.large.2 Image: CentOS 7.2 64bit System disk: 40 GB EIP: Auto assign EIP type: Dynamic BGP Billed by: Traffic Bandwidth: 5 Mbit/s 	 The following resources incur costs: ECSs EVS disks EIPs For billing details, see Billing.
Nginx	A high-performance HTTP and reverse proxy server. You can download it from: 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. You can download it from: http://dev.mysql.com/get/ mysql57-community- release-el7-10.noarch.rpm	Free

Resource	Description	Cost
РНР	An open-source software used for web development.	Free
	You can download it from:	
	http://rpms.remirepo.net/ enterprise/remi- release-7.rpm	
WordPress	An open-source blogging software.	Free
	You can download it from:	
	https://wordpress.org/ download/releases/	
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. Install Nginx.
- 2. Install MySQL.
- 3. Install PHP.
- 4. Test the LNMP environment.
- 5. Create a database.
- 6. Install WordPress.
- 7. Purchase a domain name.
- 8. 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 8-2** has been added to the security group to which the target ECS belongs. For details, see **Configuring Security Group Rules**.

Table 8-2 Security group rule

Direction	Protocol	Port	Source
Inbound	HTTP(80)	80	0.0.0/0

Procedure

- **Step 1** Install Nginx.
 - 1. Log in to the target 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 commands to start Nginx and configure automatic Nginx start upon ECS startup:

systemctl start nginx

systemctl enable nginx

6. Check the startup status.

systemctl status nginx.service

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

Figure 8-2 Accessing Nginx



Step 2 Install MySQL.

1. 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

2. Start MySQL and enable MySQL to start automatically upon ECS startup: systemctl start mysqld

systemctl enable mysqld

3. Query the running status of MySQL.

systemctl status mysqld.service

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

- mysqld.service MySQL Server
 - Loaded: loaded (/usr/lib/system//system/mysqld.service; enabled; vendor preset: disabled) Active: active (running) since Mon 2021-08-16 19:33:40 CST; 36s ago
 - Docs: man:mysqld(8)

http://dev.mysql.com/doc/refman/en/using-systemd.html

- Main PID: 7916 (mysqld)
- CGroup: /system.slice/mysqld.service

-7916 /usr/sbin/mysqld --daemonize --pid-file=/var/run/mysqld/mysqld.pid

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

Obtain the password of user **root** that is automatically set during MySQL installation:

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

Information similar to the following is displayed: 2021-08-16T11:33:37.790533Z 1 [Note] A temporary password is generated for root@localhost: ;8nPd29lhs,k

5. Harden MySQL:

mysql_secure_installation

Securing the MySQL server deployment.

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

New password: #Enter the new password.

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

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

... skipping.

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

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

Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network.

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

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

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

- Dropping test database... Success.

- Removing privileges on test database... Success.

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

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

All done!

Step 3 Install PHP.

1. Run the following command to install the EPEL repository:

yum install epel-release

- Run the following command to install the REMI repository: yum install http://rpms.remirepo.net/enterprise/remi-release-7.rpm
- 3. Run the following command to install the Yum repository management tool: **yum install yum-utils**
- 4. Run the following command to install PHP 7.4:

```
yum -y install php74-php-gd php74-php-pdo php74-php-mbstring php74-
php-cli php74-php-fpm php74-php-mysqlnd
```

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

php74 -v

If information similar to the following is displayed, PHP has been installed: PHP 7.4.33 (cli) (built: Jun 6 2023 15:55:08) (NTS) Copyright (c) The PHP Group Zend Engine v3.4.0, Copyright (c) Zend Technologies

6. Start PHP and configure PHP automatic start upon ECS startup:

systemctl start php74-php-fpm systemctl enable php74-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 8-3 nginx.conf

user nginx; worker_processes auto;
error_log /var/log/nginx/error.log notice; pid /var/run/nginx.pid;
events { worker_connections 1024; }
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" "\$http_x_forwarded_for"';
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.php index.html index.htm; }
location ~ \.php$ {
   root
             html;
   fastcgi_pass 127.0.0.1:9000;
  fastcgi_index index.php;
  fastcgi_param SCRIPT_FILENAME /usr/share/nginx/html$fastcgi_script_name;
              fastcgi_params;
  include
}
```

Figure 8-4 shows the configuration after modification.

Figure 8-4 Configuration after modification

- server {
 isten 80;
 server_name localhost;
 #access_log /var/log/ngimx/host.access.log main;
 location / {
 root /var/log/ngimx/host.access.log main;
 location / {
 root /var/share/ngimx/host.access.log main;
 location ~ \.php\$ {
 root /var/share/ngimx/host.access.log main;
 }
 location ~ N.php\$ {
 root /var/share/ngimx/host.access.log main;
 }
 location ~ N.php\$ {
 root /var/share/ngimx/host.access.log main;
 }
 #
 redirect server error pages to the static page /50%.html
 root /var/share/ngimx/html;
 root /var/share/ngimx/html;
 location = /500 502 503 504 /50%.html;
 location = /sphp\$ {
 root /var/share/ngimx/html;
 }
 root /var/share/ngimx/html;
 }
 # proxg the PHP scripts to Apache listening on 127.0.0.1:80
 #
 location ~ \.php\$ {
 root / html;
 root / html;
 root //sr/share/ngimx/html;
 }
 # pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000
 #
 location ~ \.php\$ {
 root //sr /127.0.0.1:9000;
 root //sr /127.0.0.1:9000;
- f. Press **Esc** to exit insert mode. Then, enter **:wq** to save the settings and exit.
- 8. Run the following command to reload the Nginx configuration file: service nginx reload
- **Step 4** Test the LNMP environment.
 - 1. Create the **info.php** test page in /usr/share/nginx/html.
 - a. Run the following command to create and open the **info.php** test file: **vim /usr/share/nginx/html/info.php**
 - b. Press **i** to enter insert mode.

 - 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 website has been set up.

PHP Version 7.4.33	php
System	Linux ecs-wordpress 3.10.0-1160.53.1.el7.x86_64 #1 SMP Fri Jan 14 13:59:45 UTC 2022 x86_64
Build Date	Jun 6 2023 15:55:08
Build System	Red Hat Enterprise Linux Server release 7.9 (Maipo)
Build Provider	Remi's RPM repository <https: rpms.remirepo.net=""></https:> #StandWithUkraine
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/opt/remi/php74
Loaded Configuration File	/etc/opt/remi/php74/php.ini
Scan this dir for additional .ini files	/etc/opt/remi/php74/php.d
Additional .ini files parsed	/etc/opt/remi/php74/php.d/20-bz2.ini, /etc/opt/remi/php74/php.d/20-calendar.ini, /etc/opt/remi/php74/php.d/20-ctype.ini, /etc/opt/remi/php74/php.d/20-curl.ini, /etc/opt/remi/php74/php.d/20-ftp.ini, /etc/opt/remi/php74/php.d/20-fileinfo.ini, /etc/opt/remi/php74/php.d/20-ftp.ini, /etc/opt/remi/php74/php.d/20-di. /etc/opt/remi/php74/php.d/20-gottext.ini, /etc/opt/remi/php74/php.d/20-icanv.ini, /etc/opt/remi/php74/php.d/20-isan.ini, /etc/opt/remi/php74/php.d/20-mbstring.ini, /etc/opt/remi/php74/php.d/20-isan.ini, /etc/opt/remi/php74/php.d/20-mbstring.ini, /etc/opt/remi/php74/php.d/20-isan.ini, /etc/opt/remi/php74/php.d/20-coket.ini, /etc/opt/remi/php74/php.d/20-sini, /etc/opt/remi/php74/php.d/20-coket.ini, /etc/opt/remi/php74/php.d/20-sqlite3.ini, /etc/opt/remi/php74/php.d/20-tokenizer.ini, /etc/opt/remi/php74/php.d/20-sqlite3.ini, /etc/opt/remi/php74/php.d/20-tokenizer.ini, /etc/opt/remi/php74/php.d/20-gotlite3.ini, /etc/opt/remi/php74/php.d/20-tokenizer.ini, /etc/opt/remi/php74/php.d/30-mysqli.ini, /etc/opt/remi/php74/php.d/30-pdo_mysqli.ini, /etc/opt/remi/php74/php.d/30-got_sqlite3.ini
РНР АРІ	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	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
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.*

Step 5 Create a database.

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

mysql -u root -p

2. Run the following command to create a database:

CREATE DATABASE *wordpress*,

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

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

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

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

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

mysql -u wordpressuser -p

SHOW DATABASES

exit

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

Step 6 Install WordPress.

1. Obtain the WordPress software package and upload it to the /usr/share/ nginx/html directory. For details, see How Can I Use WinSCP to Transfer Files from a Local Windows Computer to a Linux ECS?

The WordPress software package **wordpress-6.2.2.tar.gz** is used as an example.

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

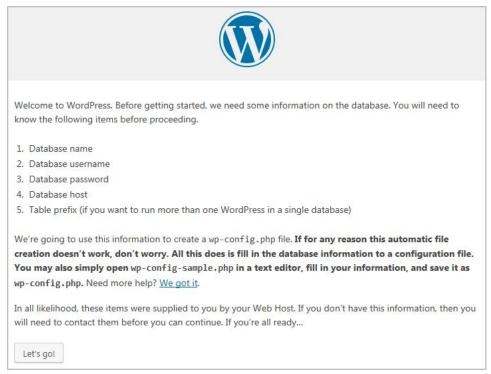
tar -zxvf /usr/share/nginx/html/wordpress-6.2.2.tar.gz

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

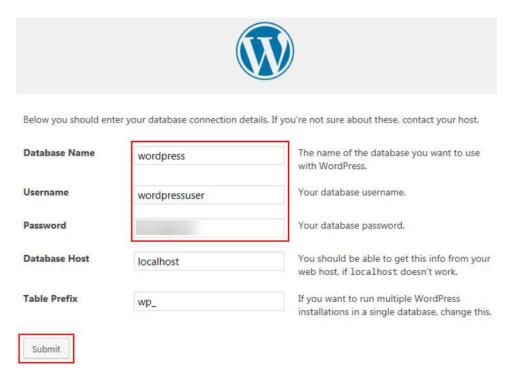
3. Run the following command to assign permissions to the **wordpress** folder:

chmod -R 777 wordpress

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



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



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

All right, sparky! You've made it through this part of the installation. WordPress can now communicate with your database. If you are ready, time now to Run the installation

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

Welcome to the fai	mous five-minute WordPress installa	ion process! Just fill in the information below a	and you'
be on your way to	using the most extendable and pow	rful personal publishing platform in the world.	1
Information	n needed		
Please provide the	following information. Don't worry, y	ou can always change these settings later.	
		63 6288 Film C	
Site Title	Cloud		
Username	admin		
	Usernames can have only alphanume	ic characters, spaces, underscores, hyphens, periods, and th	ne @
	symbol.		
	And the second second second second	🔊 Hide	
Password		The	
Password	Channel		
Password	Strong		
Password		word to log in. Please store it in a secure location.	
	Important: You will need this pas	word to log in. Please store it in a secure location.	
Password Your Email	Important: You will need this pas		
	Important: You will need this pas		
Your Email	Important: You will need this pas	ore continuing.	
	Important: You will need this pas	ore continuing.	

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

Success!	
WordPress has be	en installed. Thank you, and enjoy!
Username	admin
Password	Your chosen password.
Log In	

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

	Email Address		
Password			
Remember	Me + New	Log In	Howdy, adm
Dashboard D	ashboard		Screen Options 🔻 Help
ne Jates	A new, modern publishing	g experience is coming soon.	🕄 Dismiss
	Take your words media and lavo	ut in new directions with Gutenberg, the W	ordPress editor we're currently building.
Media		Test the new editor today.	Not quite ready?
Media Pages Comments Appearance			Not quite ready? The new editor will be enabled by default in the next major release of WordPress. If you're not sure how compatible your current themes and plugins are, we've got you covered. Install the <u>classic Editor plugin</u> to keep
Media Pages Comments Appearance Plugins Users Tools		Test the new editor today. You can take Gutenberg for a spin (and share your feedback, if you'd like) before we officially release it, by installing it as a plugin. You can help by <u>testing, filing bugs</u> or contributing	Not quite ready? The new editor will be enabled by default in the next major release of WordPress. If you're not sure how compatible your current themes and plugins are, we've got you covered.
Posts Media Pages Comments Appearance Plugins Users Users Tools Settings Collapse menu		Test the new editor today. You can take Gutenberg for a spin (and share your feedback, if your di like) before we officially release it, by installing it as a plugin. You can help by testing, filing bugs, or contributing on the <u>GitHub repository</u> .	Not quite ready? The new editor will be enabled by default in the next major release of WordPress. If you're not sure how compatible your current themes and plugins are, we've got you covered. Install the <u>Classic Editor plugin</u> to keep using the current editor until you're

Step 7 Purchase a domain name.

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

Step 8 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

9 Setting Up an FTP Site (Windows)

Overview

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

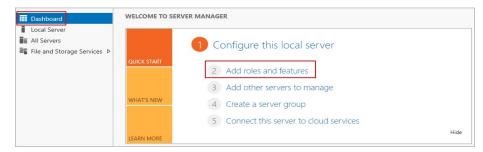
The process is as follows:

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

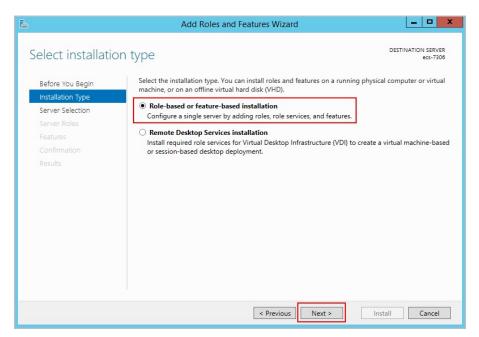
Procedure

Step 1 Add IIS and FTP service roles.

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



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



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

	Add Roles and Features Wizard	
Select destinat	ON SERVER DESTINATI	ON SERV ecs-73
Before You Begin	Select a server or a virtual hard disk on which to install roles and features.	
Installation Type	Select a server from the server pool	
Server Selection	Select a virtual hard disk	
Server Roles	Server Pool	
Features		
	Filter:	
	Name IP Address Operating System	
	ecs-7306 Microsoft Windows Server 2012 R2 Standard	
	1 Computer(s) found This page shows servers that are running Windows Server 2012, and that have been added by	v using
	Add Servers command in Server Manager. Offline servers and newly-added servers from white collection is still incomplete are not shown.	

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

a	Add Roles and Features Wizard	_ D X
Select server roles		DESTINATION SERVER ecs-7306
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	Application Server DHCP Server DNS Server Fax Server Fax Server Fax Server File and Storage Services (1 of 12 installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Volume Activation Services Windows Deployment Services Windows Server Update Services Windows Server Update Services Volume Activation	Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
	< Previous Next	> Install Cancel
Add features that The following tools are have to be installed of Web Server (IIS) Management [Tools] IIS		lot

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

B	Add Roles and Features Wizard	_ _ ×
Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results		DESTINATION SERVER ecs-7306 Description FTP Extensibility enables support for FTP extensibility features such as custom providers, ASP.NET users or IIS Manager users.
	✓ 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 Manager.

Server M	anager • Dashboard	- 3	Manage Tools View Help
Dashboard	WELCOME TO SERVER MANAGER		Component Services Computer Management Defragment and Optimize Drives
Local Server All Servers File and Storage Services ▷		ure this local server	Event Viewer Internet Information Services (IIS) Manager iSCSI Initiator Local Security Policy
To IIS	QUICK START	roles and features	Microsoft Azure Services ODBC Data Sources (32-bit)
	WHAT'S NEW	other servers to manage	ODBC Data Sources (64-bit) Performance Monitor Resource Monitor
		ect this server to cloud ser	Security Configuration Wizard Services
	LEARN MORE		System Configuration System Information Task Scheduler
	ROLES AND SERVER GROUPS Roles: 2 Server groups: 1 Servers total: 1		Windows Firewall with Advanced Security Windows Memory Diagnostic
	File and Storage Services 1	IIS	Windows PowerShell Windows PowerShell (x86) Windows PowerShell ISE
	Manageability Events	Manageability Events	Windows PowerShell ISE (x86) Windows Server Backup

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.

<u>#</u>			Computer Management
Computer Management (Local Computer Management (Local System Tools Task Scheduler Event Viewer Shared Folders Courses Groups No Performance Device Manager Corage Storage Storage Disk Management	Administrator Cloudbase-init Guest Nu Re Vi Ar		Description Built-in account for administering Built-in account for guest access t
Services and Applications	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	inge password at next logon	
User cannot o	hange password	
Password new	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.

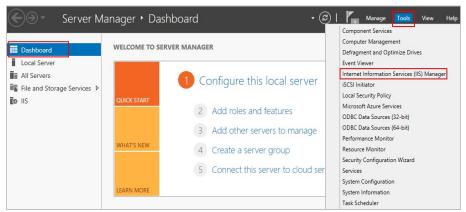
2. On the **Security** tab, select **Everyone** and click **Edit**. If **Everyone** is unavailable, add it. For details, see **FAQs**.

🐌 work01 Properties 🗙
General Sharing Security Previous Versions Customize
Object name: C:\work01
Group or user names:
Everyone
CREATOR OWNER
SYSTEM V
SQ Administratore (ECS-7306) Administratore)
To change permissions, click Edit. 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				
Connections	Sites			
Start Page	Filter:	- 1	🌹 Go 🕞 😽 Show A	.II 👳
Application Pools	Name 📩	ID	Status	Bind
⊳ 🐻 Sites	Sefault Web Site	e 1	Started (ht	*:80
of Add Website				
🚱 Refresh				
dd FTP Site				
Switch to Cont	ent View			

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

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

	Add FTP Site	? X
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**.
 - The default port number is 21. You can set the port number as required.
 - Set SSL as required.
 - **No SSL**: SSL encryption is not required.
 - Allow SSL: allows non-SSL and SSL connections between the FTP server and the client.
 - Required SSL: SSL encryption is required for the communication between the FTP server and the client.

NOTE

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

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

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

Add FTP S	Site ? X
Authentication and Authorization Informat	ation
Authentication Anonymous Basic Authorization Allow access to: Not Selected Permissions Read Wite	
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 add click **OK**.

Þ	Application Pools	Name ID Status Binding Default Web Site 1 Started (ht *:80 (http) FTPSERVER 2 Started (ft.p)	Path %SystemDrive C:\work01
		Site Bindings	? X Bindings Basic Settings
	Type Host Name ftp	Port IP Address Binding Informa 21 139.159.147.143 Add Site Binding ? ×	Add Edit Edit Edit
	Type: IP	address: Port:	Remove View Applicatio Browse View Virtual Dire
< Ready	Host name: Example: www.contoso.co	om or marketing.contoso.com	Manage FTP Site Restart Start Stop
		OK Cancel	Close

Step 5 (Optional) Configure the FTP firewall.

- To enable the passive mode on the FTP server, configure the FTP firewall.
- If Huawei Cloud servers use public IP addresses to access the FTP site that is set up on a Huawei Cloud ECS, the passive mode must be enabled on the FTP server.
- 1. Double-click FTP Firewall Support.

Start Page ▶ 😋 🗾 (MQ-WEB02\Admir	Filter:		• 🛒 Go 🕞 🖣	Show All	Group by:	Ŧ
	FTP FTP FTP		FTP Directory		^	^
	Authentic		Browsing	Support		≡
	FTP IP Address a	FTP Logging	FTP Logon Attempt R	FTP Messages		
	FTP	FTP	FTP			
	FTP Request Filtering	FTP SSL Settings	FTP User Isolation			
	lis				^	
	0	A				
			V			\sim

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

	Alerts
FTP Firewall Support	⚠ To accept passive
The settings on this page let you configure your FTP server to accept	connections when you are using FTP over SSL (FTPS) or
passive connections from an external firewall.	when your firewall does not filter packets, configure the
Data Channel Port Range:	external IPv4 address of your firewall.
5000-6000 Example: 5000-6000	Actions
External IP Address of Firewall:	Apply
	🖹 Cancel
Example: 10.0.0.1	Help
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 the ports on which to allow packets, see **Table 9-1**.

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.

Tab	le	9-1	Security	aroup	rules
Tub		5	Jecunty	group	ruics

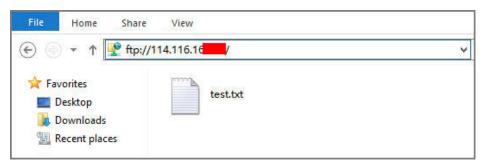
FTP Mode	Dire ctio n	Pr ot oc ol	Port	Source
Active	Inbo und	TC P	Ports 20 and 21	0.0.0.0/0
Passive	Inbo und	TC P	Port 21, and port range from 1024 to 65535 (such as 5000-6000)	0.0.0.0/0

Step 7 Verify the configuration on the client.

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

D NOTE

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



----End

FAQs

- 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 Advanced.
OK Cancel Apply

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

Permissions	for work01)	x
Security			_
Object name: C:\work01			
Group or user names:			
CREATOR OWNER			
& SYSTEM & Administrators (ECS-7306\Ad & Users (ECS-7306\Users)	lministrators)		
	Add	Remove	
Permissions for CREATOR OWNER	Allow	Deny	
Full control			
Modify			
Read & execute			
List folder contents			
Read			
ОК	Cancel	Apply	5

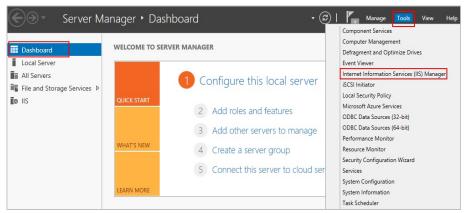
c. In the dialog box that is displayed, click **Advanced**.

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

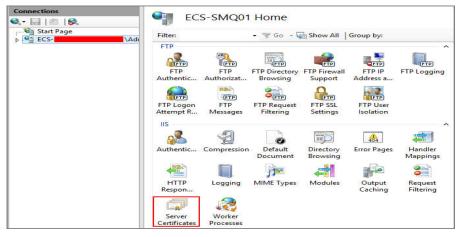
d. In the dialog box that is displayed, click **Find Now**, select **Everyone** in search results, and click **OK**.

		Select Users or Groups		x
Select this object ty				
Users, Groups, or	Built-in security pri	incipals	Obj	ect Types
From this location:				
ECS-7306			L	ocations
Common Queries				
Name:	Starts with \vee			Columns
Description:	Starts with \vee			Find Now
Disabled ac	counts			Stop
Non expiring	password			
Days since last	logon:	~		
Days since last		×		P
Search results:		l	OK	Cancel
Name	In Folder			^
A Distributed C	ECS-7306			
Event Log Re	ECS-7306			
Everyone tpadmin	ECS-7306			
Guest	ECS-7306			=
Auguests	ECS-7306			
🕂 Hyper-V Admi	ECS-7306			
Realis_IUSRS	ECS-7306			
A IUSR				~
A Local account				

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



c. Click Create Self-Signed Certificate.

V j	Inter	net Information Services		×	
ECS-SMQ01	•				📴 🔤 🟠 🔞 •
File View Help					W.
Connections		Server Certificates Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.			tions
😪 • 🔚 🖄 🥵	Serve				Import
Start Page					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		Cartificator	
🔍 - 🔚 🛯 🖄 🔛	Server Certificates		
Start Page ECS- Application Pools b- Sites	Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.		
	Filter:	👻 🐺 Go 👒 🕁 Sh	ow All Group by: 💡
	Name	Issued To	Issued By
	SSL-FTP		

10 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.

Solution Architecture

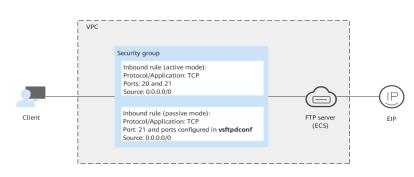


Figure 10-1 Setting up an FTP site (Linux)

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 10-1 Resources and costs

Resource	Description	Cost
VPC	VPC CIDR block: 192.168.0.0/16	Free

Resource	Description	Cost
Subnet	 AZ: AZ1 CIDR block: 192.168.0.0/24 	Free
Security group	 Inbound rule (active mode): Protocol/Application: TCP Ports: 20 and 21 Source: 0.0.0.0/0 Inbound rule (passive mode): Protocol/Application: TCP Port: 21 and ports configured in vsftpdconf Source: 0.0.0.0/0 	Free
ECS	 Billing mode: Yearly/ Monthly AZ: AZ1 Flavor: s6.large.2 Image: CentOS 7.2 64bit System disk: 40 GB EIP: Auto assign EIP type: Dynamic BGP Billed by: Traffic Bandwidth: 5 Mbit/s 	 The following resources incur costs: ECSs EVS disks EIPs For billing details, see Billing.
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.
- 2. Run the following command to install vsftpd:

yum install -y vsftpd

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

Dependencies Resolv	ved			
Package	Arch	Version	Repository	Size
Installing: vsftpd	x86_64	3.0.2-22.e17	base	169 k
Transaction Summary				
Install 1 Package Total download size Installed size: 348 Downloading package vsftpd-3.0.2-22.e17 Running transaction Transaction test su Running transaction	} k s: .x86_64.rpm a check 1 test ucceeded		† 169 kI	8 00:00:00
Installing : vsft Verifying : vsft	pd-3.0.2-22.e17.x86_64 pd-3.0.2-22.e17.x86_64			1/1 1/1
Installed: vsftpd.x86_64 0:3	3.0.2-22.e17			

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

systemctl enable vsftpd.service

4. Run the following command to start FTP:

systemctl start vsftpd.service

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

netstat -antup | grep ftp

Information similar to the following is displayed.

	000040				
tcp6	0	0 :::21	:::*	LISTEN	11836/vs <mark>ftp</mark> 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**
- 3. Run the following command to create a file directory for the FTP server, **/var/ftp/work01** is used as an example:

mkdir /var/ftp/work01

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

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

- 5. Modify the vsftpd.conf configuration file.
 - a. Run the following command to open the file:

vi /etc/vsftpd/vsftpd.conf

- b. Press **i** to enter 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.

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

#Maximum port number in passive FTP mode

pasv_address=*xx.xx.xx* #Public IP address of the FTP server pasv_min_port=*3000* #Minimum 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/**.

pasv_max_port=**3100**

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.

Table 10-2 Security group rules

FTP Mode	Dire ctio n	Pr ot oc ol	Port	Source
Active	Inbo und	TC P	Ports 20 and 21	0.0.0/0
Passive	Inbo und	TC P	Port 21 and all ports between the value of pasv_min_port and that of pasv_max_port in the /etc/vsftpd/vsftpd.conf file	0.0.0/0

Step 4 Verify the configuration on the client.

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

NOTE

- If 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

11 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 11-1 Setting up Tomcat-based Java web environment

Resource and Cost Planning

Table 11-1 Resources and costs

Resource	Description	Cost
VPC	VPC CIDR block: 192.168.0.0/16	Free

Resource	Description	Cost
Subnet	 AZ: AZ1 CIDR block: 192.168.0.0/24 	Free
Security group	Inbound rule 1: Protocol/Application: ICMP Port: All Source: 0.0.0.0/0 Inbound rule 2: Protocol/Application: TCP Port: 8080 Source: 0.0.0.0/0	Free
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 details about billing, 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

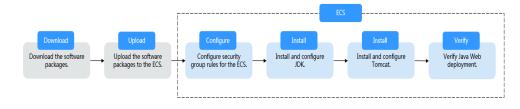
Resource	Description	Cost
PuTTY	A cross-platform remote access tool, which is used to access various nodes from a Windows OS during software installation.	Free
	You can obtain it from: https:// www.chiark.greenend.org.u k/~sgtatham/putty/ latest.html	
WinSCP	A file transfer across platform, which is used for transferring files between Windows and Linux systems. You can obtain it from:	Free
	http://winscp.net/	

NOTE

Table 11-1 lists the official paths to download JDK and Tomcat installation packages. You can also obtain the packages from open-source image paths.

Process

Figure 11-2 Deployment Process



Procedure

Preparations

- An ECS is created and has an EIP bound.
- 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 switch to the **jdk** directory:

cd /home/webDemo/jdk

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

wget JDK package download address

Download the JDK installation package from the path listed in **Table 11-1** or from other open-source image paths.

Check the available **jdk17** software package versions. The JDK installation package **jdk-17_linux-x64_bin.tar.gz** is used as an example. Run the following command to download the package:

wget https://download.oracle.com/java/17/latest/jdk-17_linux-x64_bin.tar.gz

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

cd /home/webDemo/tomcat

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

Download the Tomcat installation package from the path listed in **Table 11-1** 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 v8.5.*xx* is used as an example. Run the following command 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**.
- 4. In the Add Inbound Rule dialog box, add a security group rule as prompted.

To set up Java Web environment, 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. Therefore, add a rule to allow ICMP traffic to the ECS.

Figure 11-3 Adding the security group rule

Add Inboun	d Rule Learn	more about security g	roup configuration.			
1 Inbound r	ules allow incoming	traffic to instances associa	ited with the security gr	oup.		
Security Group	lefault Jultiple rules in a bat	rch				
Priority ②	Action	Protocol & Port ②	Туре	Source 🕐	Description	Operation
1	Allow •	ICMP All	▼ IPv4 ▼	IP address •		Operation 👻
			🕀 Add Rule			
			ОК	Cancel		

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

Figure 11-4 Adding port 8080

Add Inbound Rule Learn more about security group configuration.								
1 Inbound ru	Inbound rules allow incoming traffic to instances associated with the security group.							
Security Group d	efault ultiple rules in a bate	ch.						
Priority 🕐	Action	Protocol & Port ②	Туре	Source ③	Description	Operation		
1	Allow •	TCP •	IPv4 💌	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

 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 configuration 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

JDK is successfully installed if the following information is displayed:

```
[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 command:

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/

4.

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/

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 11-5 Checking the Tomcat process

[root@ecsbin]# ps -ef grep tomcat	
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	
emo/tomcat/apache-tomcat-8.5.95/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -	
tls.ephemeralDHKeySize=2048 -Djava.protocol.handler.pkgs=org.apache.catalina.webresources -Dorg.apache.catalina.security.Se	
yListener.UMASK=0027 -Dignore.endorsed.dirs= -classpath /home/webDemo/tomcat/apache-tomcat-8.5.95/bin/bootstrap.jar:/home/w	
o/tomcat/apache-tomcat-8.5.95/bin/tomcat-juli.jar -Dcatalina.base=/home/webDemo/tomcat/apache-tomcat-8.5.95 -Dcatalina.home	
e/webDemo/tomcat/apache-tomcat-8.5.95 -Djava.io.tmpdir=/home/webDemo/tomcat/apache-tomcat-8.5.95/temp org.apache.catalina.s	tartu
p.Bootstrap start	
root 8710 7902 0 14:33 tty1 00:00:00 grep –-color=auto tomcat	
[root@ecs bin]#	

Verifying Java Web Deployment

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

http://EIP bound to the ECS:8080

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

Figure 11-6 Accessing port 8080

Home	Documentatio	n Configuration	Examples	Wiki	Mailing Lists			Find Help
\pach	e Tomcat/	8.5.95					APACHE	SOFTWARE FOUNDATIO
	lf y	you're seeing th	is, you've	succes	ssfully installe	d Tomcat	. Congratulations!	
Recommended Reading: Security Considerations How-To Manager Application How-To Clustering/Session Replication How-To								Server Status Manager App Host Manager
omcat Se	Der Quick Star <u>etup</u> Application	t <u>Realms & P</u> <u>JDBC Data</u>			<u>Examples</u>		<u>Servlet Specificatio</u> <u>Tomcat Versions</u>	ons
Managing Tomcat For security, access to the <u>manager webapp</u> is restricted. Users are defined in: \$CATALINA_HOME/consf/towcat-users. xal In Tomcat 8.5 access to the manager application is split between different users. Read more Release Notes Changelog Migration Guide Security Notices		Documentation <u>Tomcat 8.5 Documentation</u> <u>Tomcat 8.5 Configuration</u> <u>Tomcat Wiki</u> Find additional important configuration information in: <u>SCATALINA_HOME/RUNGLING_text</u> Developers may be interested in: <u>Tomcat 8.5 Bug Databases</u> <u>Tomcat 8.5 Git Repository at GitHub</u>			Cetting Help EAQ and Mailing Lists The following mailing lists are available: Moratant announcoments, releases, security unerability notifications. (Low volume). Moratuser Moratuser Ber support and discussion for <u>Apache Taglibs</u> Moratuser Development mailing list, including commit messages			
Other Dow <u>Tomcat Con</u> Tomcat Nati Taglibs Deployer	inectors	Other Documental Tomcal Connectors mod Jk Documentatio Tomcat Native Deployer	on <u>s</u>	Get Involt <u>Overview</u> <u>Source Rep</u> <u>Aailing List</u> <u>Viki</u>	positories	Miscellane <u>Contact</u> Legal Sponsorship Thanks	Foundati Who We A	ion vre ome

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

12 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.
- You have configured the security group rules listed in the following table for the target ECS. For details, see **Adding a Security Group Rule**.

Transfer Directio n	Protocol /Port	Port/ Range	Mandat ory	Source IP Address
Inbound	TCP(22)	22	Yes	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 , access from all IP addresses is allowed. For security purposes, 0.0.0.0/0 is not recommended.
Inbound	HTTP (80)	80	Yes	IP address of the client that is allowed to access Magento. If the source IP is set to 0.0.0.0/0 , access from all IP addresses is allowed.

Table 12-1	Security	group	rules
------------	----------	-------	-------

Transfer Directio n	Protocol /Port	Port/ Range	Mandat ory	Source IP Address
Inbound	MySQL(3 306)	3306	No	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 12-2 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	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
	РНР	7.0.33
		Download URL:
		https:// mirror.webtatic.com/yu m/el7/webtatic- release.rpm

 Table 12-2 Resource planning

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** Run the following commands as the **root** user to update the software package and install Apache:

yum -y update yum -y install httpd

NOTE

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 3 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 4 Press i to enter insert mode and modify the file as follows:
 - Change AllowOverride None to AllowOverride all.

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

• 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 5** Press **Esc** to exit insert mode. Then, enter **:wq** to save the settings and exit.
- Step 6
 Run the following commands to start Apache and configure automatic start 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 command to start MySQL and enable MySQL to start automatically upon ECS startup: systemctl start mysqld systemctl enable mysqld
- **Step 4** Run the following command to obtain the **root** password that is automatically set during MySQL installation:

grep 'temporary password' /var/log/mysqld.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 of user root 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.**

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.** 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.** 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.** - 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.** 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 the full-access permission to the user:

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

magento is the name of the database created in the previous step, **magentouser** is the username of the created database, and **BLOck@123** is the user password.

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 sources: yum install https://repo.ius.io/ius-release-el7.rpm https://dl.fedoraproject.org/pub/epel/epel-releaselatest-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:

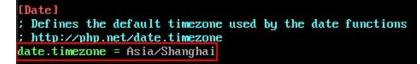
yum -y install php70w php70w-pdo php70w-mysqlnd php70w-opcache php70w-xml php70w-gd php70wmcrypt php70w-devel php70w-intl php70w-mbstring php70w-bcmath php70w-json php70w-iconv

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:



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
 - git clone https://github.com/magento/magentoz.g
- **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.

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**.

0	2	3	4	5	6	Back	Next
Readiness Check	Add a Database	Web Configuration	Customize Your Store	Create Admin Account	Install	Buck	NCAL .

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

Step 2: Add a Database

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

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

Step 3: Web Configuration					
Your Store Address	http://124.				
Magento Admin Address ★	http://124. http:/ /adu	min_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 🔸	endedealop-pealmes
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:

Magento Admin Info:	
Username:	admin
Email:	873/040 stdr
Password:	*****
Your Store Address:	http://124.
Magento Admin Address:	http://124.

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

Encryption Key:

proprint partners with propriots of

Database Info:

Database Name:	magento
Username:	magentouser

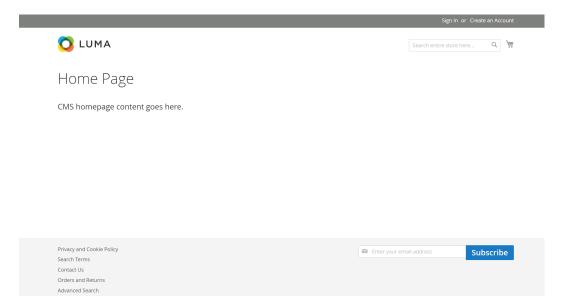
- **Step 8** Log in to the Magento server and set up cron jobs. crontab -u apache -e
- **Step 9** Press **i** to enter insert mode and add the following content:

*/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.

Û	Dashboard			Q	🌲 💄 admin 🗸
dashboard \$	Store View: All Store Views •)			Reload Data
PRODUCTS	Lifetime Sales CN¥0.00	Chart is disable Revenue	d. To enable the chart, click Tax	here. Shipping	Quantity
CUSTOMERS	Average Order CN¥0.00	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.

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

Step 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.

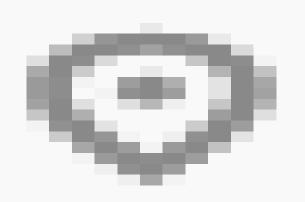
----End

13 Building Microsoft SharePoint Server 2016

13.1 Purchasing and Logging In to an ECS

Purchase an ECS on Huawei Cloud with specified specifications and OS.

- 1. Log in to the management console.
- 2. Click



in the upper left corner and select the desired region and project.

- 3. Under **Compute**, click **Elastic Cloud Server**.
- 4. Click **Buy ECS**. The **Buy ECS** page is displayed.
- Configure ECS parameters.
 For details, see Creating an ECS.

Instance Selection	By Type By Scenario						
CPU Architecture	x86 Kunpeng (?)					
Specifications	Latest generation 💌	vCPUs -Select vCPUs-	Memory -Select Memor	y- • Flavor Name	2	Q Hide sold-out specificatio	ns
	General computing-plus	General computing Memory-C	ptimized Large-memory	Disk-intensive	Ultra-high I/O GPU-a	accelerated Al-accelerated	General computing-basic
	Select All \$7	s6 s3					
	Collapse Help ^						
	General computing ECSs provide a b	alance of compute, memory, and network	resources with a baseline level of v	CPU performance and the ability to	o deliver occasional bursts of extra	compute above this baseline.	
	EC\$ Type	Flavor Name	vCPUs \$	Memory ¢	CPU \$	Assured / Maximum 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

Figure 13-1 Setting ECS specifications

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

Figure 13-2 Setting the network

Network	vpc-f00373897(192.168.0.0/16)	▼ C subnet-f00373	897-01(192.168.0.0/24)	C Automatically assign IP ad	Idress	private IP addresses: 249
Extension NIC	Create VPC Add NIC NICs you can still add: 1					
Source/Destination Che	ick 💽 🕐					
Security Group	Sys-WebServer(13e7c1f8-959c-464e-87 Similar to a freveal), a security group logical Ensure that the selected security group allo Security Group Rules A Inbound Rules Outbound Rules	ly controls network access. ws access to port 22 (SSH-ba			. Configure Security Group Rule	S
	Security Group Name	Priority	Action	Protocol & Port (?)	Туре	Source ⑦
		1	Permit	TCP: 111	IPv4	0.0.0/0
		1	Permit	UDP: 111	IPv4	0.0.0/0
		1	Permit	TCP: 2049	IPv4	0.0.0/0
		1	Permit	TCP: 2052	IPv4	0.0.0.0/0
	Sue MichQonver	1	Permit	TCP: 2051	IPv4	0.0.0/0
EIP	Auto assign Use existing	Not required 🕐				
EIP Type	Dynamic BGP	Static BGP				
Billed By	 Greater than or equal to 99.95% service Bandwidth For heavy/stable traffic Billed based on usage duration and bandwidth 	Traffic For light/sharply fluctuating f	shared ba	ndwidth d 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
ECS Group (Optional)	Anti-affinity 🕜
	-Select ECS group-
	Create ECS Group

Figure 13-3 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.

13.2 Adding AD, DHCP, DNS, and IIS Services

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

- 8 Y

igure re i internet Exptorer Enhanced Security Configuration				
Internet Explorer Enhanced Security Configuration				
Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content. Internet Explorer Enhanced Security Configuration is enabled by				
default for Administrators and Users groups.				
Administrators:				
🧭 🔿 On (Recommended)				
😵 💿 off				
Users:				
On (Recommended)				
🔇 💿 off				
More about Internet Explorer Enhanced Security Configuration				
OK Cancel				

Figure 13-4 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 13-5 Add roles and features

had	5	erver manager	
Server Mar	nager • Dashboard	• 🕲 🚩 м	anage Tools View Help
Dashboard Local Server All Servers	QUICK START	figure this local server	
File and Storage Services	3 A	dd roles and features dd other servers to manage reate a server group	
	5 C	onnect this server to cloud services	Hide
	ROLES AND SERVER GROUPS Roles: 1 Server groups: 1 Servers tot File and Storage Services 1	al: 1	
	 Manageability Events 	Manageability Events	
	Performance BPA results	3 Services Performance BPA results	
		6/28/2018 9:08	
			▲ 👍 🔁 😼 9:15 6/28/2018

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

Figure 13-6 Server role 1

È.	Add Roles and Features Wizard	
Select server roles	;	DESTINATION SERVER sp16
Before You Begin Installation Type Server Selection Server Roles AD DS DHCP Server DNS Server Web Server Role (IIS) Role Services Confirmation Results	Select one or more roles to install on the selected server. Roles Active Directory Certificate Services Active Directory Federation Services Active Directory Federation Services Active Directory Rights Management Services Fax Server Fax Server Fax Server Fint and Storage Services (1 of 12 installed) Hyper-V Network Policy and Access Services Frint and Document Services Remote Access Remote Desktop Services V	Description Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
	< Previous Next	t > Install Cancel

Figure 13-7 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 13-8 Features

a	Add Roles and Features Wizard	
Select features	Select one or more features to install on the selected server.	DESTINATION SERVER sp16
Installation Type Server Selection Server Roles Peatures AD DS DHCP Server DNS Server Web Server Role (IIS) Role Services Confirmation Results	Features Image: Installed install installed instale	Description Non-HTTP Activation supports process activation via Message Queuing, TCP and named pipes. Applications that use Non-HTTP Activation can start and stop dynamically in response to work items that arrive over the network via Message Queuing, TCP and named pipes.
	< Previous Next	> Install Cancel

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

Figure 13-9 Confirm installation selections

a	Add Roles and Features Wizard	= - X
Confirm installat	To install the following roles, role services, or features on selected server, clic	DESTINATION SERVER sp16 k Install.
Installation Type	Restart the destination server automatically if required	
Server Selection Server Roles	Optional features (such as administration tools) might be displayed on this p been selected automatically. If you do not want to install these optional feature their check boxes.	
Features AD DS DHCP Server DNS Server Web Server Role (IIS)	.NET Framework 3.5 Features HTTP Activation Non-HTTP Activation .NET Framework 4.5 Features ASP.NET 4.5	E
Role Services Confirmation Results	Active Directory Domain Services DHCP Server DNS Server Group Policy Management Remote Server Administration Tools	
	Export configuration settings Specify an alternate source path < Previous	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 13-10 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	
Results	Non-HTTP Activation	
		~
Results	Non-HTTP Activation .NET Framework 4.5 Features ASPNET 4.5 Vou can close this wizard without interrupting running tasks. View task progress	or open this

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

Figure 13-11 Add a new forest

a	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 < Previous	Cancel

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

Figure 13-12 Password setting

🛓 📃 Active Directory Domain Services Configuration Wizard				
Domain Controller Options				
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation	Select functional level of the new forest Forest functional level: Domain functional level: Specify domain controller capabilities Omain Name System (DNS) server Global Catalog (GC) Read only domain controller (RODC)	Windows Server 2012 R2 ▼ Windows Server 2012 R2 ▼		
Results	Type the Directory Services Restore Moc Password: Confirm password: More about domain controller options	Je (DSRM) password		
< Previous Next > Install Cancel				

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

Figure 13-13 DHCP configuration 1

2		Server Manager	- 0	x
Server M	anager • Dashboard	• 🕄 🍢 Manage Tools	View Help	
Dashboard Local Server All Servers	WELCOME TO SERVER MANAG	Post-deployment Configura TASS V X Configuration required for DHCP Server at ECS- SHAREPOINT Complete DHCP configuration		^
間 AD DS 恒 DHCP 畠 DNS	QUICK START	Task Details Add roles and teatures		=
■ File and Storage Services ▷	3 WHAT'S NEW 4	Add other servers to manage Create a server group		
	5	Connect this server to cloud services		

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

Figure 13-14 DHCP configuration 2

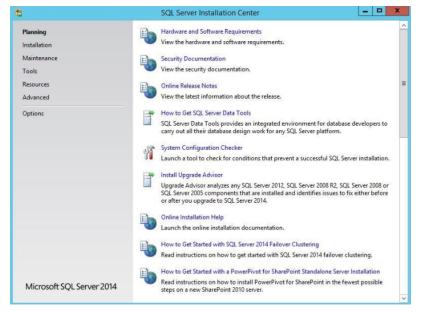
a	DHCP Post-Install configuration wizard	×
Authorization		
Description Authorization Summary	Specify the credentials to be used to authorize this DHCP server in AD DS. Use the following user's credentials User Name:	
	O Use alternate credentials UserName: Specify	
	 Skip AD authorization 	
	Coming News	Canad
	< Previous Next > Commit	t Cancel

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

13.3 Installing SQL Server

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

Figure 13-15 SQL Server installation center



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

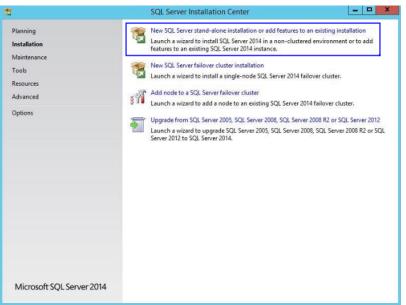


Figure 13-16 SQL Server installation options

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 13-17 SC	L 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 Setup 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: Evaluation C Enter the product key: NQGJR-63HC8-XCRQH-MYVCH-333QR	
	< Back Next > Can	cel

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

Figure 13-18 SQL Server license option

12	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 (or based on where you live, one of its affiliates) and you. Please read them. They apply to the evaluation software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft • updates,
Feature Rules Feature Configuration Rules Ready to Install Installation Progress Complete	Copy Print C
	< 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 13-19 SQL Server features

3	SQL Serve	r 2014 Setup	
Feature Selection Select the Evaluation features to	o install.		
Product Key License Terms	Features:		Feature description:
Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Setup Role Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration	Instance Features Database Engine Services SQL Server Replication Full-Text and Semantin Analysis Services Analysis Services Analysis Services - Nativ Shared Features Reporting Services - Nativ Shared Features Reporting Services - Share Control Control Control Data Quality Client Control Contro	Extractions for Sea ≡ Point	The configuration and operation of each instance feature of a SQL Server instances. SqL
Analysis Services Configuration Reporting Services Configuration Distributed Replay Controller Distributed Replay Controller Evature Configuration Rules Ready to Install	Select All Unselect All Instance root directory: Shared feature directory: Shared feature directory (x86):	C:\Program Files\Mic C:\Program Files\Mic C:\Program Files (x86	
		< Back	Next > Cancel Help

7. Select **Default instance**.

Figure 13-20 SQL Server instance

1	SQL Se	erver 2014 Setup				
Instance Configuration Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.						
Product Key License Terms Global Rules	Default instance Named instance:	MSSQLSERVER				
Microsoft Update Product Updates Install Setup Files	Instance ID:	MSSQLSERVER				
Install Rules Setup Role Feature Selection	SQL Server directory: Analysis Services directory:	C:\Program Files\Microsoft C:\Program Files\Microsoft				
Feature Rules Instance Configuration Server Configuration	Reporting Services directory: Installed instances:	C:\Program Files\Microsoft	SQL Server\MSRS12.MSSC	QLSERVER		
Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Distributed Replay Controller Distributed Replay Client Feature Configuration Rules Ready to Install	Instance Name Instan	ce ID Features	Edition	Version		
		< Back	Next > Cane	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 13-21 SQL Server service accounts

2	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					
Ready to Install					
nearly to mature					
		< Back Next	> Cance	el He	In
		Next Next	Cance	ne ne	Ψ

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

Figure 13-22 SQL Server administrator account 1

1	SQL Server 2014 Setup	X
Database Engine Confi Specify Database Engine auther	guration	
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	
Product Updates Install Setup Files	Windows authentication mode	
Install Rules	Mixed Mode (SQL Server authentication and Windows authentication)	
Setup Role Feature Selection	Specify the password for the SQL Server system administrator (sa) account.	
Feature Rules	Enter password:	
Instance Configuration	Confirm password:	
Server Configuration	Specify SQL Server administrators	
Database Engine Configuration		administrators
Analysis Services Configuration		tricted access base Engine.
Reporting Services Configuration	to the bata	Jase Engine.
Distributed Replay Controller		
Distributed Replay Client		
Feature Configuration Rules	Add Current User Add Remove	
Ready to Install		
	< Back Next > Cancel	Help

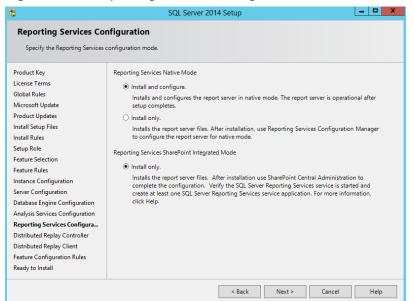
10. Click **Add Current User** to grant Analysis Services administrator permissions to the current account, and click **Next**.

Figure 13-23 SQL Server administrator account 2

Specify Analysis Services server	modes, administrators, and data directories.	
Product Key License Terms	Server Configuration Data Directories	
Global Rules Microsoft Update Product Updates	Multidimensional and Data Mining Mode Tabular Mode	
Install Setup Files Install Rules	Specify which users have administrative permissions for Analysis Services. SP160\Administrator (Administrator)	Analysis Services
Setup Role Feature Selection Feature Rules		administrators have unrestricted access to Analysis Services.
reature 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	

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

Figure 13-24 Reporting Services Configuration



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

1	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 ser	rvice.
License Terms	SP160\Administrator (Administrator)	Users that have been
Global Rules		granted permission will have
Microsoft Update		unlimited access to the Distributed Replay
Product Updates		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.

	SQL Server 2014 Setup	
Ready to Install Verify the SQL Server 2014 featu Product Key	res to be installed. Ready to install SQL Server 2014:	
Induct Rey Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Setup Role Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Analysis Services Configuration Analysis Services Configuration Distributed Replay Controller Distributed Replay Client Feature Configuration Rules Ready to Install	Summary Edition: Evaluation Action: Install (Product Update) Prerequisites Arready installed: Windows PowerShell 2.0 Microsoft. NET Framework 4.0 To be installed from media: Microsoft Visual Studio 2010 Redistributables Microsoft Visual Studio 2010 Relativation Microsoft Visual Studio 2010 Shell Microsoft Visual Studio 2010 Shell Microsoft Visual Studio 2010 Shell Features SQL Server Replication Full-Text and Semantic Extractions for Search Data Outsing Sensing	i

Figure 13-26 SQL Server installation

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

1	SQL Server 2014 Setup	
Complete Your SQL Server 2014 installation	on completed successfully with product updates.	
Product Key License Terms	Information about the Setup operation or possib	le next steps:
Global Rules	Feature Management Tools - Complete	Status ^
Microsoft Update	Client Tools Connectivity	Succeeded
Product Updates Install Setup Files	 Client Tools SDK Client Tools Backwards Compatibility 	Succeeded Succeeded
Install Rules	Management Tools - Basic Reporting Services - Native	Succeeded Succeeded Y
Setup Role Feature Selection		
Feature Rules	Details:	
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	been installed. By default, the Help Viewer c SQL Server, you can use the Help Library M	nd manage the documentation for SQL Server have omponent uses the online library. After installing anager component to download documentation to ee Use Microsoft Books Online for SQL Server (5782).
		Close Help

13.4 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.

			_ 0 X
	Application Tools	DVD Drive (D:) 16.0.4351.1000	
File Home Share	View Manage		^ (?
Copy Paste Paste Paste shore	Move Conv Delete Pename	New Easy access - Reporties	Select all Select none Invert selection
Clipboard	Organize	New Open	Select
🔄 💿 🔹 🕇 🔛 🕨 Thi	is PC + DVD Drive (D:) 16.0.4351.1000	✓ ♂ Search DVD Drive (D	:) 16.0.435 🔎
☆ Favorites	Name	Date modified Type Si	ze
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-I1-1-0.dll	7/30/2015 5:30 Application extens	25 KB
📔 Desktop	💹 autorun	5/29/2015 3:05 ICO File	2 KB
Documents	autorun 🗿	5/29/2015 3:05 Setup Information	1 KB
\rm Downloads	🖻 default	11/24/2015 17:22 HTA File	14 KB
🚺 Music	n 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	🚺 setup	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		100

Figure 13-28 SharePoint preparation tool

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

Figure 13-29 SharePoint preparation tool installation wizard



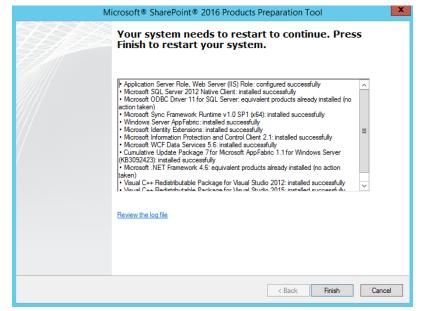
3. Select I accept the terms of the License Agreement(s) and click Next.

	Microsoft® SharePo	pint® 2016 Produ	ucts Preparation Tool	
ense Terms for so This solution require review the license to	s that you install each of the fo	vllowing software module	es and agree to their license terms. Please	
MICROSOFT S)FTWARE LICENSE TE	RMS		^
			at cover twelve differ	
Microsoft are:	products. The pr	oducts cover	ed by these license te	rms
LICENSE 1 Microsoft W:	indows Management	Framework 3.0		
LICENSE 2				~
	ead and understand all of the products can be downloaded		escribed in the EULA. You must accept the computer.	e terms of
	ood, and agreed to the terms of Agreement(s)'' and using thes		e Agreement(s) and so signify by clicking "I	accept the
I accept the term	s of the License Agreement(s)			

Figure 13-30 SharePoint preparation tool license

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

Figure 13-31 Successful preparation tool installation



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

Figure 13-32 Installing SharePoint

A 🕞 🖟 = I	Application Tools	DVD Drive (D:) 16.0.4351.1000	- 🗆 X
File Home Share	e View Manage		^ (?
Copy Paste Sh Cibboard	Move Conv Delete Rename	New ten * Folder New Upen *	Select all Select none
	-		
(e) (e) < ↑ [□ • 1]	his PC > DVD Drive (D:) 16.0.4351.1000	✓ C Search DVD Driv	re (D:) 16.0.435 🔎
👉 Eavorites	Name	Date modified Type	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 🛛 ≡	💹 autorun	5/29/2015 3:05 ICO File	2 KB
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:) 1	🚺 setup	7/31/2015 22:05 Application	257 KB
퉬 catalog	🖻 splash	7/30/2015 14:27 HTA File	3 KB
鷆 files	🚳 svrsetup.dll	2/11/2016 2:13 Application extens	12,959 KB
鷆 global	🚳 ucrtbase.dll	7/30/2015 5:30 Application extens	960 KB
퉬 prerequisitein 🗸	🚳 vcruntime140.dll	7/30/2015 5:30 Application extens	87 KB
27 items 1 item selected	d 256 KB		800 🖬

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

Figure 13-33 SharePoint product key

Microsoft SharePoint Server 2016 Trial	x
Enter your Product Key	0
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	
	Enter your Product Key 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

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

5	Microsoft SharePoint Server 2016 Trial	X
	Read the Microsoft Software License Terms	0
	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 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 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 MCDNL suctomer, use of this coftware is cubicet to the MACDNL V I accept the terms of this agreement	

Figure 13-34 SharePoint license terms

8. Retain the default installation paths.

Figure	13-35 Shar	rePoint installation path	ns
--------	------------	---------------------------	----

	Choose a file location	?
	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	
	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	

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

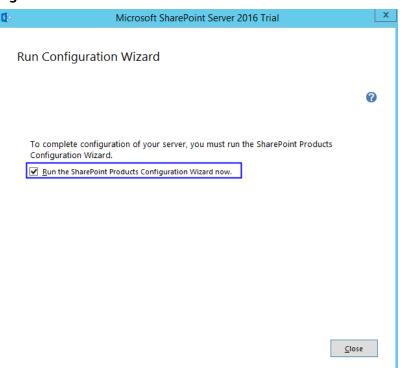


Figure 13-36 Successful SharePoint installation

13.5 Configuring Microsoft SharePoint Server 2016

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

Figure 13-37 SharePoint Products Configuration Wizard



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

_ 🗆 X

 SharePoint Products Configuration Wizard	
Welcome to SharePoint Products	
In order to configure SharePoint Products, you will require the following information:	
Name of database server and database where server farm configuration data will be stored	ł
SharePoint Products Configuration Wizard	

Figure 13-38 Service restart prompt

	SharePoint Products Configuration Wizard
	The following services may have to be started or reset during configuration:
	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.
Click N	Yes No
2	

3. Select Create a new server farm.

Figure 13-39 Create a new server farm

A server farm is	a collection of two or i	'M more computers that sha	are configuration	data. Do you wa	ntto
connect to an e	xisting server farm? nect to an existing serv		-		
• Cre	ate a new server farm				

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

Specify Configuration Database Settings All servers in a server farm must share a configuration database. Type the database server and database name. If the database does not exist, it will be created. To reuse an existing database, the database must empty. For additional information regarding database server security configuration and network access please see help. Database server:		
name. If the database does not exist, it will be created. To reuse an existing database, the database must empty. For additional information regarding database server security configuration and network access pleasesee help. Database server: Database name: SharePoint_Config Specify Database Access Account Select an existing Windows account that this machine will always use to connect to the configuration database. If your configuration database is hosted on another server, you must specify a domain account Type the username in the form DOMAIN\User_Name and password for the account. Username: Specify Database Access Ac	Specify Configuration D	atabase Settings
Database name: . Database name: SharePoint_Config Specify Database Access Account Select an existing Windows account that this machine will always use to connect to the configuration database. If your configuration database is hosted on another server, you must specify a domain account Type the username in the form DOMAIN\User_Name and password for the account. Username: Descendence	name. If the database does not exist, i empty. For additional information reg	t will be created. To reuse an existing database, the database must be
Specify Database Access Account Select an existing Windows account that this machine will always use to connect to the configuration database. If your configuration database is hosted on another server, you must specify a domain account Type the username in the form DOMAIN\User_Name and password for the account. Username: sp160\/Administrator Descended sp160\/Administrator	Database server:	
Select an existing Windows account that this machine will always use to connect to the configuration database. If your configuration database is hosted on another server, you must specify a domain account Type the username in the form DOMAIN\User_Name and password for the account. Username: provide the server of the server	Database name:	SharePoint_Config
database. If your configuration database is hosted on another server, you must specify a domain account Type the username in the form DOMAIN\User_Name and password for the account. Username: sp160\Administrator		
Username: sp 160\Administrator	Specify Database Access Acc	ount
Spico (kuninistrato)	Select an existing Windows account the	at this machine will always use to connect to the configuration
Password:	Select an existing Windows account the database. If your configuration database	at this machine will always use to connect to the configuration ase is hosted on another server, you must specify a domain account.
	Select an existing Windows account the database. If your configuration databa Type the username in the form DOMAIN	at this machine will always use to connect to the configuration ase is hosted on another server, you must specify a domain account. \\User_Name and password for the account.
	Select an existing Windows account th database. If your configuration datab Type the username in the form DOMAII Username:	at this machine will always use to connect to the configuration ase is hosted on another server, you must specify a domain account. V\User_Name and password for the account.
	Select an existing Windows account th database. If your configuration datab Type the username in the form DOMAII Username:	at this machine will always use to connect to the configuration ase is hosted on another server, you must specify a domain account. V\User_Name and password for the account.
	Select an existing Windows account th database. If your configuration datab Type the username in the form DOMAII Username:	at this machine will always use to connect to the configuration ase is hosted on another server, you must specify a domain account. V\User_Name and password for the account.
0	Select an existing Windows account th database. If your configuration datab Type the username in the form DOMAII Username:	at this machine will always use to connect to the configuration ase is hosted on another server, you must specify a domain account. V\User_Name and password for the account.
	Select an existing Windows account th database. If your configuration datab Type the username in the form DOMAII Username:	at this machine will always use to connect to the configuration ase is hosted on another server, you must specify a domain accoun v\User_Name and password for the account.
	Select an existing Windows account th database. If your configuration datab Type the username in the form DOMAII Username:	at this machine will always use to connect to the configuration see is hosted on another server, you must specify a domain account. VUser_Name and password for the account.

Figure 13-40 Configuring the SharePoint database

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

Figure 13-41 Setting the password for the SharePoint server farm

Please enter a new passphrase for th configuration data and is required for the farm is configured.	e SharePoint Produc or each server that jo	ts farm. This passp ins the farm. The pa	hrase is used to se ssphrase can be cl	cure farm hanged after
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.	server 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
Application	servers are optimized for fast performance.
 Distributed Cadhe 	
○ Search	
○ Custom	
- Single-Server Farm	
 Single-Server Farm 	

Figure 13-42 Setting the SharePoint server role

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

Figure 13-43 Port number of SharePoint Central Administration Web Application

SharePoint Products Configuration Wizard			x
Configure SharePoint Central Administration Web Appli	cation	1]
A SharePoint Central Administration Web Application allows you to manage configuration se farm. The first server added to a server farm must host this web application. To specify a po web application hosted on this machine, check the box below and type a number between 1 you do not specify a port number, a random one will be chosen.	rt number	forthe	
Specify port number: 10000			
Configure Security Settings			
Kerberos is the recommended security configuration to use with Integrated Windows auther requires special configuration by the domain administrator. NTLM authentication will work w application pool account and the default domain configuration. <u>Show memore information</u> .		erberos	
Choose an authentication provider for this Web Application.			
● NTLM			
🔿 Negotiate (Kerberos)			
< Back Next >	Ca	ncel	7
			7

8. Check and confirm the SharePoint configurations.



Figure 13-44 SharePoint configurations

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

Figure 13-45 Configuration progress

	SharePoint Products	
Please wait while Sl	narePointProducts are configured.	
Performing configu	irationtask3of10	
Creating the config	uration database	
0		

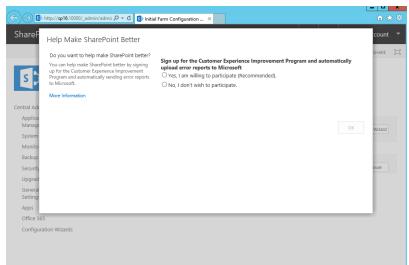
10. After SharePoint is configured successfully, click **Finish**.

SharePoint Products Conf	iguration Wizard 📃 💻 🗖
Configuration Successful	
The following configuration settings were successfully applie	:d:
 Configuration Database Server 	SP16
 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
Jick Finish to close this wizard and launch the SharePoint Co onfiguring your SharePoint installation. The users may be p the form DOMAIN(User_Name and password to access th ou used to logon to this computer. Add this site to the list o	rompted by their web browser for the username e site. At that prompt, enter the credentials that
9	

Figure 13-46 Successful SharePoint configuration

13.6 Verifying Microsoft SharePoint Server 2016

1. Open the SharePoint central administration.



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

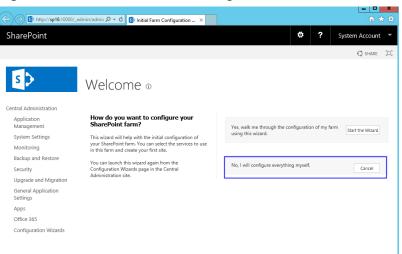


Figure 13-48 SharePoint farm configuration

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

Figure 13-49 Creating a SharePoint site

http://sp16:10000/de	efault.aspx 🔎 🗸 🖒 🚺 Home - Central Adm	inistra ×	• - - - - - - - - - -
SharePoint			System Account
BROWSE PAGE			🗘 SHARE
s >			
Central Administration Application Management	Application Management Manage web	System Settings Manage servers in this farm	Resources There are currently no favorite links to display. To add a new link, click
System Settings	applications	Manage services in	"Add new link".
Monitoring	Create site collections Manage service	this farm Manage farm features	
Backup and Restore	applications	Configure alternate	🕈 Add new link
Security	Manage content databases	access mappings	
Upgrade and Migration		Backup and Restore	
General Application Settings	Monitoring Review problems and	Perform a backup Restore from a backup	
Apps	solutions Check job status	Perform a site	
Office 365		collection backup	
Configuration Wizards	Security Manage the farm administrators group Configure service accounts	Upgrade and Migration Convert farm license type Check product and	

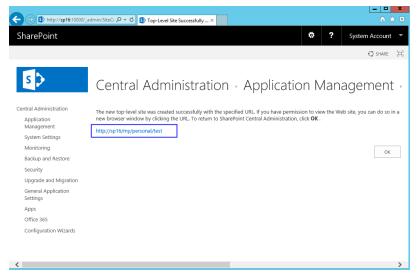
4. Set SharePoint site parameters.

narePoint			۵	?	System Accour
					🖓 SHARE
Management					
System Settings	Web Application	Web Application: http://sp16/ -			
Monitoring	Select a web application.				
Backup and Restore	To create a new web application go to New Web Application page.				
Security					
Upgrade and Migration	Title and Description				
General Application Settings	Type a title and description for your new site. The title will be displayed on each page in the site.	Title: test			
Apps		Description:			
Office 365		example			
Configuration Wizards					
	Web Site Address Specify the URL name and URL path to create a new site, or choose to create a site at a specific path.	URL: http://sp16 /my/personal/			
	To add a new URL Path go to the Define Managed Paths page.				

Figure 13-50 Setting SharePoint site parameters

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

Figure 13-51 SharePoint top-level site created successfully



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

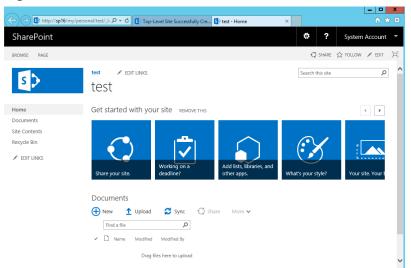


Figure 13-52 SharePoint verification

14 Manually Deploying LNMP (CentOS 7.2, PHP 7.0)

Overview

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

The process is as follows:

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

Prerequisites

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

 Table 14-1
 Security group rule

Transfer Direction	Protocol/ Application	Port/Range	Source End
Inbound	HTTP (80)	80	0.0.0/0

Resource Planning

Table 14-2 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.2 Image: CentOS 7.2 64bit System disk: 40 GB 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.
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: http://dev.mysql.com/get/ mysql57-community- release-el7-10.noarch.rpm	Free
РНР	An open-source software used for web development. Download URL: https:// mirror.webtatic.com/yum/el 7/epel-release.rpm https:// mirror.webtatic.com/yum/el 7/webtatic-release.rpm	Free

 Table 14-2 Resources and costs

Procedure

Step 1 Install Nginx.

- 1. Log in to the ECS.
- 2. Run the following command to download the Nginx package: wget http://nginx.org/packages/centos/7/noarch/RPMS/nginx-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 commands to start Nginx and configure automatic Nginx enabling upon ECS startup:

systemctl start nginx

systemctl enable nginx

6. Check the startup status.

systemctl status nginx.service

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

Figure 14-1 Accessing Nginx



Step 2 Install MySQL.

1. Run the following commands 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

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

systemctl start mysqld

systemctl enable mysqld

3. Run the following command to query the running status of MySQL:

systemctl status mysqld.service

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

mysqld.service - MySQL Server
Loaded: loaded (/usr/lib/system//system/mysqld.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2021-08-16 19:33:40 CST; 36s ago
Docs: man:mysqld(8)
http://dev.mysql.com/doc/refman/en/using-systemd.html

Main PID: 7916 (mysqld)

CGroup: /system.slice/mysqld.service
—7916 /usr/sbin/mysqld --daemonize --pid-file=/var/run/mysqld/mysqld.pid

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

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

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

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

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

mysql_secure_installation

Securing the MySQL server deployment.

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

New password: #Enter the new password.

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

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

... skipping.

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

Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y #Asks you whether to remove anonymous users. Press **y**. Success.

Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network.

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

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

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

- Removing privileges on test database...

Success.

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

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

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-tidy php70w-common php70w-devel php70w-pdo php70w-mysql php70w-gd php70w-ldap php70w-mbstring php70wmcrypt php70w-fpm

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

php -v

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

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

3. Start PHP and configure PHP automatic start upon ECS startup:

systemctl start php-fpm

systemctl enable php-fpm

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

Figure 14-2 nginx.conf

iser nginx; iorker_processes auto;
error_log /var/log/nginx/error.log notice; rid /var/run/nginx.pid;
wents { worker_connections 1024;
nttp { 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" "\$http_x_forwarded_for"';
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.

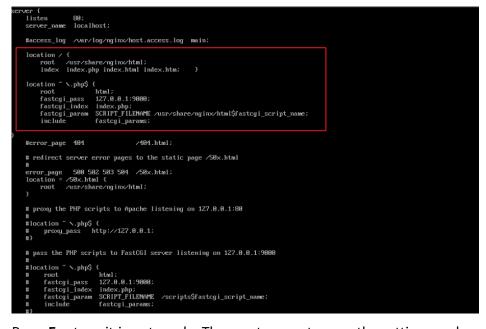
e. Modify the **default.conf** file.

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

Figure 14-3 shows the configuration after modification.

Figure	14-3	Configuration	after	modification
--------	------	---------------	-------	--------------



- f. 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 page in /usr/share/nginx/html/.
 - a. Run the following command to create and open the **info.php** test file: **vim /usr/share/nginx/html/info.php**
 - b. Press **i** to enter insert mode.
 - c. Modify the **info.php** file and add the following data 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 deployment.

PHP Version 7.0.31	php
System	Linux ecs-5d3f.novalocal 3.10.0-693.11.1.el7.x86_64 #1 SMP Mon Dec 4 23:52:40 UTC 2017 x86_64
Build Date	Jul 20 2018 08:57:28
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/bz2_ini, /etc/php.d/calendar.ini, /etc/php.d/ctype ini, /etc/php.d/curi ini, /etc/php.d/scim,
PHP API	20151012
PHP Extension	20151012

----End

15 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.

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

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

Prerequisites

• The target ECS has an EIP bound. For instructions about how to bind an EIP to an ECS, see **Assigning an EIP and Binding It to an ECS**.

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

Transfer Direction	Туре	Protocol	Port/Range	Remote End
Inbound	IPv4	ТСР	80	0.0.0.0/0

Deploying Docker

- 1. Log in to the ECS.
- Add a yum repository.
 yum install epel-release -y
 yum clean all
- 3. Install yum-utils. sudo yum install -y yum-utils device-mapper-persistent-data lvm2
- Configure the yum repository for Docker.
 sudo yum-config-manager --add-repo https://download.docker.com/linux/ centos/docker-ce.repo
- 5. Install and run Docker.

sudo yum install docker-ce

systemctl enable docker

systemctl start docker

6. Check the installation.

docker --version

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

Client: Docker Engine - Community Version: 19.03.13

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	latest	75835a67d134	5 weeks ago	200 MB
[root@ecs-b67a-doc		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	o neeno ago	2001

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".

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

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

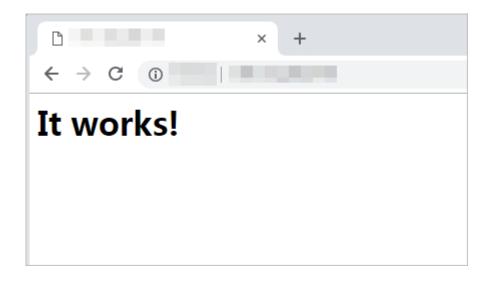
[root@ecs-b67a-docker ~]# docker run -it -d -p 80:80 --name datahttpd -v /data/:/var/www/httpd/ httpd 6a514dea52a9465c1f6863c0f17ff41debda231ccff8bf66e3c0dbcc5f33cb20 [root@ecs-b67a-docker ~]#

b. Check whether the container has been started.

docker ps -a

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

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 and must be the first instruction in Dockerfile, indicating that the Nginx image is used as a basic image.
- **RUN** statement: indicates that the echo command is executed 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

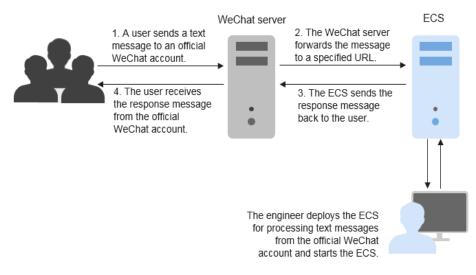
REPOSITORY	TAG	IMAGE ID	CREATED	SIZE	
nginx	v3	09422e465d96	10 seconds ago	109 MB	

16 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 16-1 shows the service flow.

Figure 16-1 Flowchart for processing text messages



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

Preparations

Apply for an official WeChat account.
 URL: https://mp.weixin.qq.com/

This section uses the Service Infographics WeChat account as an example.

• Purchase an ECS.

If you don't have an account, **register a HUAWEI ID and enable Huawei Cloud services**.

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

Figure 16-2 Public image

Image	Public image	Private	e image	Shared image	Marketplace imag	le
	CentOS	•	CentOS 7.4	4 64bit(40GB)	•	C

• Purchase an EIP.

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

Figure 16-3 EIP

EIP 💿	To enable Internet access from your	ECSs, create a plan for th	e EIPs you require. View B	EIP
	Automatically assign	Use existing	Not required	

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 16-4 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 16-5 Downloading the Python installation package

.0/Python-3.6.0a1.tar.xz 6.0/Python-3.6.0a1.tar.xz
2a04:4e42:1a::223 :443 connected.
]:445 connected.
ed [15328032/15328032]

- 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 16-6 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 16-7** is displayed, the dependency packages have been installed.

Figure 16-7 Successful installation

```
Installed:
  gcc-c++.x86_64 0:4.8.5-44.el7
Dependency Installed:
  libstdc++-devel.x86_64 0:4.8.5-44.el7
Dependency Updated:
  cpp.x86_64 0:4.8.5-44.el7 gcc.x86_64 0:4.8.5-44.el7
```

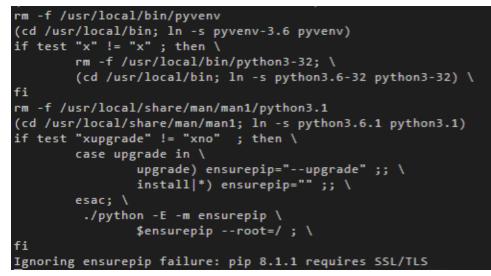
Run the ./configure command again.

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 16-8 Successful execution



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

Figure 16-9 Viewing the Python 3 version

[root@ecs-	Python-3.6.0a1]#	python3	version
Python 3.6.0a1			

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 16-10 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. Therefore, pip must be reinstalled.

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

Figure 16-11 Installing the openssl-devel package

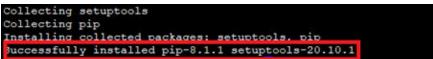


2. Run the following command to install pip:

make && make install

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

Figure 16-12 Successful installation



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 16-13 Successful upgrade

<pre>[root@ecs- Python-3.6.0a1]# pip3 installupgrade pip</pre>
Collecting pip
Downloading https://files.pythonhosted.org/packages/54/eb/4a36
100%
Installing collected packages: pip
Found existing installation: pip 8.1.1
Uninstalling pip-8.1.1:
Successfully uninstalled pip-8.1.1
Successfully installed pip-20.3.3

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 16-14 Installing Web.py
```

```
[root@ecs-c438 Python-3.6.0a1]# pip3 install web.py==0.40.dev0
Collecting web.py==0.40.dev0
  Downloading web.py-0.40.dev0.tar.gz (116 kB)
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()
     Create the handle.py file and copy the following data:
2.
     # -*- 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 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

3.

```
class TextMsg(Msg):
  def __init__(self, xmlData):
     Msg.__init__(self, xmlData)
     self.Content = xmlData.find('Content').text
class ImageMsg(Msg):
  def __init__(self, xmlData):
     Msg.__init__(self, xmlData)
     self.PicUrl = xmlData.find('PicUrl').text
     self.MediaId = xmlData.find('MediaId').text
class LocationMsg(Msg):
  def __init__(self, xmlData):
     Msg.__init__(self, xmlData)
     self.Location_X = xmlData.find('Location_X').text
     self.Location_Y = xmlData.find('Location_Y').text
class EventMsg(Msg):
  def __init__(self, xmlData):
     Event.__init__(self, xmlData)
     self.Event = xmlData.find('Event').text
```

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

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

5. Obtain the local file.

Figure	16-15	Local file
--------	-------	------------

018/04/21	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
D:\workspa 2018/04/20	ace\wx\te 13:41	xtProcess	\templa	tes
			\templa	tes

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

Figure 16-16 Uploading files

.:								
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	5:							
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 16-17** is displayed, the service has been started.

Figure 16-17 Successful service startup



Enabling the Developer Mode

- 1. Log in to official WeChat platform, choose **Develop** > **Basic Configuration**, and click **Modify Configuration**.
- 2. Specify the following basic configurations and click **Submit**.
 - **URL**: 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.

17 Manually Deploying GitLab (CentOS 7.2)

Overview

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

Prerequisites

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

Table 17-1 Security group rule

Transfer Direction	Protocol/ Application	Port/Range	Source End
Inbound	HTTP (80)	80	0.0.0/0

Procedure

Step 1 Install the dependency package.

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

sudo yum install -y curl policycoreutils-python openssh-server

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

sudo systemctl enable sshd

sudo systemctl start sshd

Step 2 Install Postfix to send emails.

- 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.

D NOTE

- After the command is executed, you can view the software download speed and the estimated download completion time in the command output.
- If the download speed is slow, obtain the response IP addresses of github.com at http://tool.chinaz.com/dns and select the IP address with a smaller TTL value. Then add the local DNS resolution to the hosts file on the target ECS.

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

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

*	*		
***	***		
*****	*****		
*****	******		
******	******		

,,,,,,,,,,,	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
****	****		
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
****	-ladada		
••••••			

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

	,,,,,		
	*		
	<i>, ,</i> .		

11 1 Λ./. $I \cap I$

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	
Aanage Git repositories with fine-grained access controls that keep your ode secure. Perform code reviews and enhance collaboration with merge equests. 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

18 Manually Deploying RabbitMQ (CentOS 7.4)

Overview

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

Prerequisites

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

Transfer Direction	Туре	Protocol	Port/Range	Source
Inbound	IPv4	тср	5672	0.0.0/0
Inbound	IPv4	ТСР	15672	0.0.0/0

Table 18-1 Security group rule

Procedure

Step 1 Install the dependency package and perl.

- 1. Log in to the target ECS.
- Run the following command to install the dependency packages: yum -y install make gcc gcc-c++ m4 ncurses-devel openssl-devel unixODBC-devel
- 3. Run the following command to install perl: yum install perl

Step 2 Install Erlang.

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-rabbitmq ~]# erl -version Erlang (SMP,ASYNC_THREADS,HIPE) (BEAM) emulator version 11.1.7

Step 3 Install RabbitMQ.

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

cd

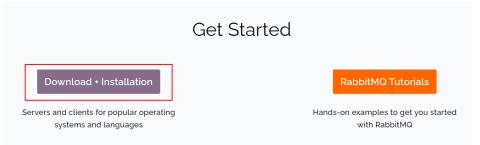
- 2. Perform the following steps to download the RabbitMQ installation package:
 - a. Open **RabbitMQ**.
 - b. Click Get Started.

Figure 18-1 Get Started



c. Click **Download+Installation**.

Figure 18-2 Download+Installation



d. Select a download address based on the ECS OS. Here, the CentOS 7.x is used as an example.

Figure 18-3 Selecting a download address

Downloads on GitHub

- <u>Windows installer</u>
- Debian, Ubuntu
- 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 visit 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 switch to the RabbitMQ management page.

⊌ RabbitMQ.	User: root Cluster: rabbit@rabbit1 (<u>change</u>) RabbitMQ 3.6.9, <u>Erlang 19.3</u>	Log out				
Overview Connections Channels Exchanges Queues Admin						
Overview						
▼ Totals						
Queued messages (chart: last minute) (?)						
Currently idle						
Message rates (chart: last minute) (?)						
Currently idle						
Global counts (?)						
Connections: 0 Channels: 0 Exchanges: 8 Queues: 0 Consumers: 0						
▼ Node						
Node: rabbit@rabbit1 (More about this node)						
File descriptors (?) Socket descriptors (?) Erlang processes Memory Disk space Rates mode Info Reset stats DB +/-						
22 0 324 56MB 35GB basic Diss I Reset 1024 available 829 available 1048376 available 735MB high watermark8MB low watermark Diss 1 Reset						
Reset stats on all nodes						

----End

19 Manually Deploying a Ghost Blog (on an ECS Running 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.

Installing GCC and g++

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

sudo apt-get install build-essential

- 2. Run the following command to install the GNU Compiler Collection (GCC): **apt-get install gcc**
- 3. Run the following command to query the GCC version:

gcc --version

The following information is displayed:

root@ecs-c47c:~# gcc --version gcc (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0 Copyright (C) 2019 Free Software Foundation, Inc.

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

sudo apt-get install g++

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

g++ --version

The following information is displayed: root@ecs-c47c:~# g++ --version g++ (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0 Copyright (C) 2019 Free Software Foundation, Inc.

Installing Node.js

1. 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 query the version of Node.js and Node Package Manager (npm), respectively:

node -v

npm -v

```
The following information is displayed:
root@ecs-c47c:~# node -v
v18.16.1
root@ecs-c47c:~# npm -v
9.5.1
```

Installing Nginx

Before deploying the Ghost blog, you need to install Nginx and use it as an HTTP server. The following operations use Nginx 1.10.0 as an example.

1. Run the following commands to install Nginx:

sudo apt-get update

sudo apt-get install nginx

2. (Optional) Configure the firewall.

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

sudo ufw status

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

sudo ufw enable

Verify that the firewall is enabled.

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

sudo ufw app list

The following information is displayed:

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

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

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

sudo ufw allow 'Nginx Full'

3. Verify that Nginx can work properly.

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

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

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.

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

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

b. Add the following content to the configuration file:

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

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

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

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

d. Restart Nginx.

sudo service nginx restart

Creating a User

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

1. Run the following command to create a user:

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

- 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 the created user:

su - <user>

Installing MySQL

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

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

sudo apt-get update

 Run the following command to install the mysql-server software package (During the installation, you will be asked to set the password of user root):

sudo apt-get install mysql-server

2. Configure MySQL.

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

mysql_secure_installation

Securing the MySQL server deployment.

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

New password: #Enter the new password.

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

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

... skipping.

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

Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y #Asks you whether to remove anonymous users. Press **y**. Success.

Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : Y #Asks you whether to forbid remote login of user **root**. Press **y**.

Success.

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

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

- Removing privileges on test database... Success.

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

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

All done!

3. Test MySQL.

Run the following command to check the MySQL status:

systemctl status mysql.service

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

- mysql.service MySQL Community Server Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled) Active: active (running) since Mon 2019-01-07 10:57:27 CST; 2min 42s ago Main PID: 26065 (mysqld) CGroup: /system.slice/mysql.service _____26065 /usr/sbin/mysqld
- 4. To avoid garbled characters in the database, run the following command to set the MySQL code:

sudo vi /etc/my.cnf

Copy and paste the following content:

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

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

sudo /usr/sbin/service mysql restart

5. Create a Ghost database.

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

mysql -u root -p;

mysql> create database ghost;

mysql> show databases;

mysql> exit

Installing and Configuring Ghost

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

- 1. Run the following command to install Ghost-CLI: sudo npm i -g ghost-cli
- 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

NOTE

[user] is the newly created user.

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

cd /var/www/ghost/

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

ghost install

NOTE

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

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

6. Configure Ghost.

If **ghost install** is successfully executed in the **/var/www/ghost/** directory, configure some items as prompted.

You can run the following command to modify the configuration:

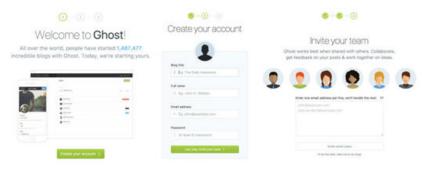
vi config.production.json

The following is a sample for your reference.



Verifying Blog Access

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



20 Manually Deploying Node.js (CentOS 7.2)

Overview

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

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

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

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

Prerequisites

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

Procedure

Step 1 Install the Node.js software packages.

- Using the binary file
 - a. Log in to the ECS.
 - b. Run the following command to download 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

- h. Run the following command to view the installed versions: **nvm ls**
- i. Run the following command to switch the Node.js version to V10.14.2: **nvm use v10.14.2**

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.

- Run the following command to switch to the home directory: cd
- Run the following command to create a test.js project file: touch test.js
- 3. Use VIM to edit the **test.js** file.

- a. Run the following command to install the VIM editor: yum install vim
- b. Run the following command to open the **test.js** file: **vim test.js**
- c. Press i to enter insert mode.

```
Modify the file as follows:
const http = require('http');
const hostname = '0.0.0';
const port = 3000;
const server = http.createServer((req, res) => {
    res.statusCode = 200;
    res.setHeader('Content-Type', 'text/plain');
    res.end('Hello World\n');
});
server.listen(port, hostname, () => {
    console.log(`Server running at http://${hostname}:${port}/`);
});
```

- The port number can be customized.
- d. Press **Esc** to exit 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 visit Node.js. If the following page is displayed, Node.js has been deployed.

Figure 20-1 Deployment and testing



----End

21 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.

The following describes how to use Huawei Cloud ECSs to set up PostgreSQL.

Preparations

- Create two ECSs.
- Configure a security group rule for the ECSs to allow port 5432.

D NOTE

The CentOS 7.6 64bit is used as an example. The PostgreSQL 11.2 version is used as an example.

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'

D NOTE

The password in the preceding command must be enclosed in single quotation marks.

Assume the username is **dbar** and the password is **dbar_password**, run the following command:

create role dbar login replication encrypted password 'dbar_password'

5. Run the following command to open configuration file /var/lib/pgsql/11/ data/pg_hba.conf:

vim /var/lib/pgsql/11/data/pg_hba.conf

Add the following content to the file: host all all 192.168.1.0/24 md5 #Allows 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.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 tream -P</pre>	-D /var/lib/pgsql/ll/data -h and and and	-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=*IP address of the master node* port=5432 user=*dbar* password=*dbar_password* #Do not enclose the password in single quotation marks. trigger_file = '/var/lib/pgsql/11/data/trigger.kenyon' #Trigger file for master/slave switchover recovery_target_timeline = 'latest' restore_command = 'cp /var/lib/pgsql/11/data/archivelog/%f %p' archive_cleanup_command = 'pg_archivecleanup /var/lib/pgsql/11/data/archivelog %r' #Clear outdated archives.

4. Run the following command to modify the **postgresql.conf** file:

chown -R postgres.postgres /var/lib/pgsql/11/data

5. Add the following content to the **/var/lib/pgsql/11/data/postgresql.conf** file.

listen_addresses= xxx.xx.xx.xx

max_connections = 600

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

#systemctl enable postgresql-11

#systemctl start postgresql-11

Verifying Master-Slave Replication

1. Run the following command to check whether process **sender** runs on the master node:

ps aux |grep sender [root@ecs-22f5-0001 -]# ps aux |grep sender postgres 14466 0.0 0.3 397240 3520 7 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: wal<mark>receiver</mark> 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

22 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 strongly recommended.
 - The OS has no Apache, Nginx, PHP, or MySQL installed.
- The rule listed in the following table has been added to the security group to which the target ECS belongs. For details, see Adding a Security Group Rule.

Direction	Protocol/ Application	Port/Range	Source	
Inbound	ТСР	8888	0.0.0/0	

Table 22-1 Security group rule

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.
- 2. Run the following command to download and install the BT panel:

yum install -y wget && wget -O install.sh http://download.bt.cn/install/ install_6.0.sh && sh install.sh

When information similar to the following is displayed, enter **y**:

Do you want to install Bt-Panel to the /www directory now?(y/n): y

After the installation is complete, information similar to the following is displayed:

Congratulations! Installed successfully!
Bt-Panel: http://114.115.xxx.xx:8888/46722528 username: ut22gsvp password: ******* Warning: If you cannot access the panel, release the following port (8888/888/80/443/20/21) in the security group
Time consumed: 2 Minute!

NOTE

Record the values of **Bt-Panel**, **username**, and **password** in the command output.

Step 2 Log in to the BT panel.

- 1. In the address bar of your browser, enter the address following parameter **Bt-Panel**, for example, http://114.115.xxx.xx:8888/46722528.
- 2. Enter the username and password you recorded.
- 3. Install desired suites and deploy websites using the BT panel based on service requirements.
- ----End

23 Accessing OBS from an ECS over the Intranet

23.1 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.

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 23-1 shows the access process.

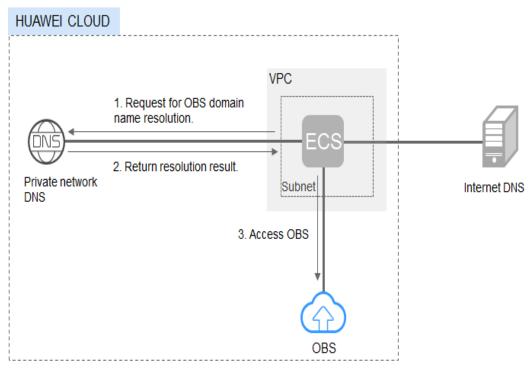


Figure 23-1 Accessing OBS through the intranet

Table 23-1 describes the services in the figure.

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.

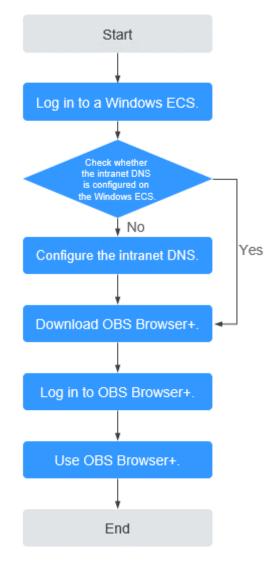
23.2 Accessing OBS over Intranet by Using OBS Browser + on a Windows ECS

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 23-2 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 **Logging In to an ECS**.

Step 2 Check whether the intranet DNS is configured on the Windows ECS.

On the Windows ECS, you can view the current DNS configuration by using the graphical user interface (GUI) or command line interface (CLI). This section uses the CLI as an example to describe how to view the DNS configuration.

- 1. After logging in to the ECS, open the CLI.
- 2. Run the **ipconfig /all** command to check whether DNS server is at the intranet DNS address of the region where the current ECS resides.

NOTE

Huawei Cloud provides different private DNS server addresses for different regions. For details, see What Are the Private DNS Server Addresses Provided by 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. Therefore, you need to reconfigure the intranet DNS after each restart of the ECS. This section uses configuration through CLI as an example to describe how to modify the DNS configuration locally.

- 1. Open the CLI.
- 2. Run the following command to configure the IP address of the primary DNS server:

netsh interface ip set dns name="Local connection" source=static addr=Intranet DNS server address register=primary

NOTE

- Local connection: NIC name. You need to modify the name according to the actual NIC.
- Intranet DNS server address: Select the intranet DNS server address based on the region where the ECS resides. For details, see What Are the Private DNS Server Addresses Provided by 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

D 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. Therefore, you can set this parameter to the IP address of the Huawei Cloud intranet DNS server. (You need to select the intranet DNS server address based on the region where the ECS resides. For details, see What Are the Private DNS Server Addresses Provided by 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+ uses a public network to access OBS by default. Therefore, when you log in to OBS Browser+ to add an account, set **Service** and **Server Address** as follows:

• Server Address: Enter the OBS domain name in the region where your ECS resides and the port number. The HTTPS port number is 443 and the HTTP port number is 80. The HTTPS server is used by default. If you want to use the

HTTP server, click in the upper right corner of OBS Browser+ and click **System Configuration**. In the **System Configuration** dialog box that is displayed, deselect **Enable HTTPS**.

Example: obs.cn-south-1.myhuaweicloud.com:443

Example: obs.ap-southeast-1.myhuaweicloud.com:443

Example: obs.eu-west-101.myhuaweicloud.eu:443

NOTE

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

23.3 Accessing OBS over Intranet by Using obsutil on a Linux ECS

obsutil is a command line tool applicable to Windows and macOS. You can configure the intranet DNS server address to access OBS over intranet on a Huawei Cloud Linux ECS. The process and procedure are described as follows.

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

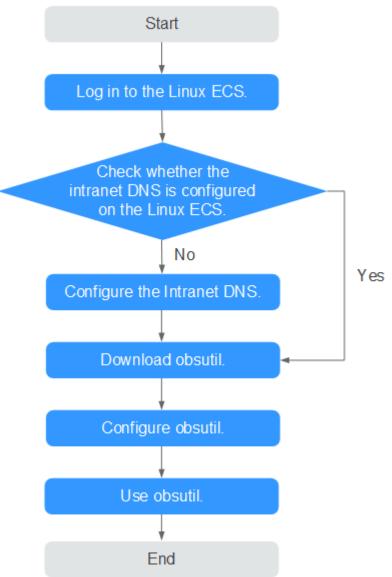


Figure 23-3 The process of accessing OBS over intranet by using obsutil on a Linux ECS

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**.
- Select an ECS and log in to the ECS.
 The login mode is set during the Linux ECS creation.
 For details about how to log in to the ECS, see Logging In to an ECS.
- **Step 2** Check whether the intranet DNS is configured on the Linux ECS.
 - 1. Log in to the Linux ECS and open the CLI.

2. Run the **cat /etc/resolv.conf** command to check whether the IP address after **nameserver** in the first line is the intranet DNS address of the region where the current ECS resides.

NOTE

Huawei Cloud provides different private DNS server addresses for different regions. For details, see What Are the Private DNS Server Addresses Provided by 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 64-bit CentOS 6.x as an example to describe how to modify the local DNS configuration.

- a. Open the CLI.
- b. Run the following command to open the **/etc/resolv.conf** file: vi /etc/resolv.conf
- c. Press i to enter 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

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. Therefore, if you want to switch to the public network access mode, you need to change the first line of the DNS address to a public DNS server address or add a public DNS server address before the existing DNS server address.

d. Press **ESC** and enter :wq! to save the settings and close the file.

D 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.

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

24 Restoring Accidentally Deleted Data on a Linux ECS Using Extundelete

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**
- 4. 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

6. 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

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

Direction	Туре	Protocol/ Application	Port/Range	Source
Inbound	IPv4	ТСР	8080	0.0.0/0

Procedure

Step 1 Install JDK.

NOTE

To ensure compatibility with Jenkins, install JDK 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.

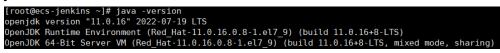
rpm -qa | grep java | xargs rpm -e --nodeps

3. Install JDK 11.

yum install -y java-11-openjdk

- 4. Restart the ECS.
- 5. Check whether the installation is successful.

java -version



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

froot@ecs-jenkins ~]# systemctl start jenkins
[root@ecs-jenkins ~]# systemctl status jenkins
🛛 jenkins.service – Jenkins Continuous Integration Server
Loaded: loaded (/usr/lib/systemd/system/jenkins.service; disabled; vendor preset: disabled)
Active: active (running) since Thu 2022-12-22 10:30:57 CST; 1min 34s ago
Main PID: 8236 (java)
CGroup: /system.slice/jenkins.service
–8236 /usr/bin/java -Djava.awt.headless=true -jar /usr/share/java/jenkins.warwebroot=%C/jenkins/war

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

Unlock Jenkins

To ensure Jenkins is securely set up by the administrator, a password has been written to the log (not sure where to find it?) and this file on the server:

/var/jenkins_home/secrets/initialAdminPassword

Please copy the password from either location and paste it below.

Continue

- 2. Log in to the ECS.
- 3. Obtain the activation password.

cat /var/lib/jenkins/secrets/initialAdminPassword

[root@ecs-jenkins ~]# cat /var/lib/jenkins/secrets/initialAdminPassword
f4360f0textent f436

4. On the **Unlock Jenkins** page, paste this password into the **Administrator password** field and click **Continue**.

5. Install suggested plugins. After the installation is complete, use the admin account to go to the next step.

g Started		
Customize Je	enkins	
Plugins extend Jenkins with add	ditional features to support many different	
needs		
needs.		
needs. Install suggested plugins	Select plugins to install	

6. Save the settings and complete the installation. The Jenkins page is displayed.

Jenkins		Q. Search (CTRL+K)	0
nboard >			
+ New Item			
2 People		Welcome to Jenkins!	
Build History			
Manage Jenkins		This page is where your Jenkins jobs will be displayed. To get started, you can set up distributed builds or start building a software project.	
My Views		Start building your software project	
d Queue	~	Create a job	\rightarrow
ds in the queue.			
Executor Status	~	Set up a distributed build	
		Set up an agent	\rightarrow
le		Configure a cloud	\rightarrow
		Learn more about distributed builds	Θ



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.



```
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**.

상 Updates 어 Available plugins	Plugii	15	
Installed plugins	Q Mu	ttiJob 🛛	
Advanced settings Download progress	Install	Name i	Released
E Download progress		Multijob 623.v03401733:9a_9 Miscellaneous	
		Enabling full hierarchy of Jenkins jobs 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 ago

• After Jenkins is restarted, check whether the MultiJob plug-in takes effect on the installed plug-ins page.

Dashboard	>	Manage Jenkins	>	Plugin Manager	

Dashboard > Manage Jenkins > Plugin Manager

먼 Updates 먼 Available plugins	Plugins	
۲ کار Installed plugins	Q MultiJob 📝	
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. Learn more.	,

2. Click New item, select MultiJob Project, and click OK.



MultiJob Project

MultiJob Project, suitable for running other jobs

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 va	ariables
Invoke Ant	
Invoke Gradle script	
Invoke top-level Mav	en targets
MultiJob Phase	

4. Add three jobs as follows.

Build Steps

MultiJob Phase	×
Phase name ?	
excuteJobSequentialy	
Phase jobs	
Job Job name 🔋	×
Demo1	
Advanced	
≡ doL	×
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

					Disable Project
S W Job	Last Success	Last Failure	Last Duration	Console	Built On
⊘ ¹ Q ¹ multijobDemo	28 sec #2	N/A	7.5 sec	Console output	D Jenkins
XQ X excute/obSequentialy					
⊘ IộI Demo1	28 sec #2	N/A	8 ms	Console output	Jenkins
⊘ XộX Demo2	25 sec #5	N/A	9 ms	Console output	Jenkins
⊘ :ộ: Demo3	23 sec #4	N/A	9 ms	Console output	Jenkins
Vor 5 M L Workspace Recent Changes			Keen legend 👘	, Atom feed for all 🦙 Atom feed for failures	s 🔊 Atom feed for just latest build

/ Add descrie