

弹性云服务器

# 最佳实践

文档版本 01  
发布日期 2024-11-04



版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 安全声明

## 漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

---

# 目录

---

<b>1 ECS 最佳实践汇总</b> .....	<b>1</b>
<b>2 ECS 自助建站汇总</b> .....	<b>5</b>
<b>3 弹性云服务器配置最佳实践</b> .....	<b>8</b>
<b>4 搭建环境</b> .....	<b>11</b>
4.1 搭建 LNMP 环境.....	11
4.1.1 手工搭建 LNMP 环境（CentOS 7.2）.....	11
4.1.2 手工搭建 LNMP 环境（CentOS 8.0）.....	18
4.1.3 手工搭建 LNMP 环境（Ubuntu 20.04）.....	25
4.1.4 手工搭建 LNMP 环境（Huawei Cloud EulerOS 2.0）.....	31
4.2 搭建 LAMP 环境.....	37
4.2.1 手工搭建 LAMP 环境（CentOS 7.8 PHP7.0）.....	37
4.3 搭建 Java Web 环境.....	42
4.3.1 基于 Tomcat 构建 Java web 环境（CentOS 7.4）.....	42
4.3.2 基于 Tomcat 构建 Java web 环境（Huawei Cloud EulerOS 2.0）.....	49
4.4 手工搭建 Hadoop 环境（Linux）.....	51
4.5 手工部署 Node.js（CentOS 7.2）.....	56
<b>5 搭建网站</b> .....	<b>60</b>
5.1 搭建 WordPress 网站.....	60
5.1.1 基于 WordPress 搭建个人网站（Linux）.....	60
5.2 搭建 Discuz 论坛网站.....	65
5.2.1 方案概述.....	65
5.2.2 购买服务.....	67
5.2.3 搭建网站.....	75
5.2.4 配置特性.....	84
5.2.5 访问网站.....	95
5.3 搭建 Magento 电子商务网站.....	97
5.3.1 手工搭建 Magento 电子商务网站（Linux）.....	97
5.4 手工搭建 Ghost 博客（Ubuntu 20.04）.....	108
<b>6 搭建应用</b> .....	<b>114</b>
6.1 构建 FTP 站点.....	114
6.1.1 快速构建 FTP 站点（Windows 2012）.....	114



6.1.2 快速构建 FTP 站点（Windows 2019）	130
6.1.3 快速构建 FTP 站点（Linux）	148
6.1.4 搭建 FTP 站点（Huawei Cloud EulerOS 2.0）	153
6.2 搭建 Microsoft SharePoint Server 2016	155
6.2.1 购买并登录弹性云服务器	155
6.2.2 添加 AD、DHCP、DNS、IIS 服务	157
6.2.3 安装 SQL Server	163
6.2.4 安装 Sharepoint 2016	169
6.2.5 配置 Sharepoint 2016	174
6.2.6 验证 Sharepoint 2016	179
6.3 部署 Docker	182
6.3.1 手工部署 Docker（CentOS 7.5）	182
6.4 搭建微信公众号后台——收发文本消息	186
6.5 手工部署 GitLab（CentOS7.2）	194
6.6 手工部署 RabbitMQ（CentOS 7.4）	199
6.7 PostgreSQL 本地 Slave 搭建步骤	203
6.8 手工安装宝塔面板（CentOS 7.2）	205
6.9 基于弹性云服务器安装及部署 Jenkins	207
6.10 如何使用 auditd 记录 Linux 系统文件改动	213
6.11 通过 Extundelete 恢复弹性云服务器误删除数据（Linux）	217
6.12 搭建 ThinkPHP 框架	218
<b>7 云服务器安全</b>	<b>221</b>
7.1 Linux 云服务器 SSH 登录的安全加固	221
7.2 使用虚拟 IP 和 Keepalived 搭建高可用 Web 集群	225
<b>8 云服务器迁移</b>	<b>241</b>
8.1 最佳实践-主机迁移	241
8.2 跨账号跨区域迁移云服务器	243
<b>9 在 ECS 上通过内网访问 OBS</b>	<b>252</b>
9.1 概述	252
9.2 在 Windows ECS 上使用 OBS Browser+通过内网访问 OBS	254
9.3 在 Linux ECS 上使用 obsutil 通过内网访问 OBS	256
<b>10 使用 VNC Viewer 连接 Linux 云服务器</b>	<b>260</b>

# 1 ECS 最佳实践汇总

本文汇总了弹性云服务器（ECS）服务的常见应用场景，并为每个场景提供详细的方案描述和操作指南，以帮助您在ECS服务器中轻松搭建业务。

## ECS 最佳实践

表 1-1 ECS 最佳实践

分类	场景	相关文档	说明
环境搭建	搭建LNMP环境	<a href="#">手工搭建LNMP环境（CentOS 7.2）</a>	以CentOS 7.2 64bit操作系统云服务器为例，介绍如何搭建LNMP环境。
		<a href="#">手工搭建LNMP环境（CentOS 8.0）</a>	以CentOS 8.0 64bit操作系统云服务器为例，介绍如何搭建LNMP环境。
		<a href="#">手工搭建LNMP环境（Ubuntu 20.04）</a>	以Ubuntu 20.04 64bit操作系统云服务器为例，介绍如何搭建LNMP环境。
		<a href="#">手工搭建LNMP环境（Huawei Cloud EulerOS 2.0）</a>	以Huawei Cloud EulerOS 2.0 64bit操作系统云服务器为例，介绍如何搭建LNMP环境。
	搭建LAMP环境	<a href="#">手工搭建LAMP环境（CentOS 7.8 PHP7.0）</a>	以CentOS 7.8 64bit操作系统云服务器为例，介绍如何搭建LAMP环境。
	搭建Java Web环境	<a href="#">基于Tomcat构建Java web环境（CentOS 7.4）</a>	以CentOS 7.4 64bit操作系统云服务器为例，介绍如何搭建Java Web环境。
<a href="#">基于Tomcat构建Java web环境（Huawei Cloud EulerOS 2.0）</a>		以Huawei Cloud EulerOS 2.0 64bit操作系统云服务器为例，介绍如何搭建Java Web环境。	

分类	场景	相关文档	说明
	搭建Node.js环境	<a href="#">手工部署Node.js环境</a>	以CentOS 7.2 64bit操作系统云服务器为例，介绍如何搭建Node.js环境。
网站搭建	搭建WordPress网站	<a href="#">手工搭建WordPress网站</a>	以CentOS 7.2 64bit操作系统云服务器为例，介绍如何搭建WordPress网站。
	搭建Discuz论坛网站	<a href="#">手工搭建Discuz论坛网站</a>	以CentOS操作系统云服务器为例，介绍如何搭建Discuz论坛网站。
	搭建Magento电子商务网站	<a href="#">手工搭建Magento电子商务网站</a>	以CentOS 7.2 64bit操作系统云服务器为例，介绍如何搭建Magento电子商务网站。
	搭建Ghost博客	<a href="#">手工搭建Ghost博客 (Ubuntu 20.04)</a>	以Ubuntu 20.04 64bit操作系统云服务器为例。介绍如何部署Ghost博客。
应用搭建	构建FTP站点	<a href="#">快速构建FTP站点 (Windows 2012)</a>	以Windows 2012数据中心版 64bit操作系统云服务器为例，介绍如何搭建FTP站点。
		<a href="#">快速构建FTP站点 (Windows 2019)</a>	以Windows 2019数据中心版 64bit操作系统云服务器为例，介绍如何搭建FTP站点。
		<a href="#">快速构建FTP站点 (Linux)</a>	以CentOS 7.2 64bit操作系统云服务器为例，介绍如何搭建FTP站点。
	搭建Microsoft SharePoint Server	<a href="#">搭建Microsoft SharePoint Server 2016</a>	以Windows 2012数据中心版 64bit操作系统云服务器为例，介绍如何搭建Microsoft SharePoint Server 2016。
	部署Docker	<a href="#">手工部署Docker (CentOS 7.5)</a>	以CentOS 7.5 64bit操作系统云服务器为例，介绍如何搭建Docker。
	搭建微信公众号	<a href="#">手工搭建微信公众号后台</a>	以CentOS 7.4 64bit操作系统云服务器为例，介绍如何搭建微信公众号后台
	安装宝塔面板	<a href="#">手工安装宝塔面板 (CentOS 7.2)</a>	以CentOS 7.2 64bit操作系统云服务器为例，介绍如何安装宝塔面板。

分类	场景	相关文档	说明
	部署GitLab	<a href="#">手工部署GitLab (CentOS7.2)</a>	以CentOS 7.2 64bit操作系统云服务器为例，介绍如何搭建GitLab
	部署RabbitMQ	<a href="#">手工部署RabbitMQ (CentOS 7.4)</a>	以CentOS 7.4 64bit操作系统云服务器为例，介绍如何搭建RabbitMQ
	搭建ThinkPHP框架	<a href="#">搭建ThinkPHP框架</a>	以CentOS 7.2 64bit操作系统云服务器为例，介绍如何搭建ThinkPHP框架。
	搭建PostgreSQL本地Slave	<a href="#">PostgreSQL本地Slave搭建步骤</a>	以CentOS 7.6 64bit操作系统云服务器为例，介绍如何搭建PostgreSQL本地Slave。
	部署Jenkins	<a href="#">基于弹性云服务器安装及部署Jenkins</a>	以CentOS 7.6 64bit操作系统云服务器为例，介绍如何部署Jenkins。
	配置auditd工具	<a href="#">如何使用auditd记录Linux系统文件改动</a>	以CentOS 7.4 64bit操作系统云服务器为例，介绍auditd工具的安装和配置。
	Extundelete快速恢复数据	<a href="#">通过Extundelete恢复弹性云服务器误删除数据 (Linux)</a>	以CentOS 7.5 64bit操作系统云服务器为例，介绍如何使用开源工具Extundelete快速恢复被误删除的数据。
云服务器安全	Linux云服务器SSH登录的安全加固	<a href="#">Linux云服务器SSH登录的安全加固</a>	以CentOS 7.6 64bit操作系统云服务器为例，介绍如何对SSH登录进行安全加固。
	搭建高可用Web集群	<a href="#">使用虚拟IP和Keepalived搭建高可用Web集群</a>	以CentOS 7.8 64bit操作系统云服务器为例，介绍使用虚拟IP和Keepalived搭建高可用Web集群的方法。
云服务器迁移	主机迁移	<a href="#">最佳实践-主机迁移</a>	介绍如何使用主机迁移服务和镜像导入方式把服务器上的应用和数据迁移到华为云。
	跨账号跨区域迁移云服务器	<a href="#">跨账号跨区域迁移云服务器</a>	介绍如何将华为云上的云服务器进行跨账号跨区域迁移。
其他	在ECS上通过内网访问OBS	<a href="#">在Windows ECS上使用OBS Browser+通过内网访问OBS</a>	介绍Windows ECS如何使用OBS Browser+工具，实现内网访问OBS。

分类	场景	相关文档	说明
		<a href="#">在Linux ECS上使用obsutil通过内网访问OBS</a>	介绍Linux ECS如何使用obsutil工具，实现内网访问OBS。
	VNC View 连接云服务器	<a href="#">使用VNC Viewer连接Linux云服务器</a>	以Ubuntu 20.04操作系统为例，介绍如何为云服务器安装VNC Server及如何使用VNC Viewer连接云服务器。

# 2 ECS 自助建站汇总

## 简介

为了方便用户搭建网站，本文汇总了华为云常用的网站搭建指导。并提供了指导文档和相关镜像的链接，您可以根据介绍选择需要搭建的网站，并通过链接获取指导文档和镜像，轻松搭建您的网站。

## 汇总表

表 2-1 网站搭建汇总表

网站搭建方案	搭建方式	操作系统	镜像及所含资源	说明
<a href="#">搭建Discuz论坛网站</a>	手动部署	Linux	公共镜像	Discuz是通用的社区论坛软件系统，基础架构采用流行的web编程组合PHP+MySQL实现。
<a href="#">搭建FTP站点 (Windows)</a>	手动部署	Windows	公共镜像	使用Windows自带的FTP服务搭建FTP站点。
<a href="#">快速构建FTP站点 (Linux)</a>	手动部署	Linux	公共镜像	使用vsftpd软件搭建FTP站点。vsftpd全称是“very secure FTP daemon”，是一款在Linux发行版中使用较多的FTP服务器软件。
<a href="#">基于Tomcat构建Java web环境</a>	手动部署	Linux	公共镜像 <ul style="list-style-type: none"><li>Tomcat 8.5.31</li><li>JDK 8u171</li></ul>	Tomcat是一个免费的开放源代码的Web应用，是目前比较常用的Web应用程序。可以用来托管常用的Java Web应用程序。

网站搭建方案	搭建方式	操作系统	镜像及所含资源	说明
<a href="#">手工搭建Magento电子商务网站 (Linux)</a>	手动部署	Linux	公共镜像 <ul style="list-style-type: none"><li>MySQL 5.7</li><li>PHP 7.0</li><li>Magento 2.1</li></ul>	Magento是一款开源电子商务系统，设计灵活，具有模块化架构体系和丰富的功能，可为大中型站点提供解决方案。
<a href="#">搭建Microsoft SharePoint Server 2016</a>	手动部署	Windows	公共镜像 <ul style="list-style-type: none"><li>Microsoft SQL Server 2014</li><li>SharePoint Server 2016</li></ul>	Microsoft SharePoint Server是一个门户站点，使得企业能够开发出智能的门户站点。这个站点能够无缝连接到用户、团队和知识。
<a href="#">手工搭建LNMP环境</a>	手动部署	Linux	公共镜像 <ul style="list-style-type: none"><li>Nginx 1.14.0</li><li>MySQL 5.7</li><li>PHP 7.0.31</li></ul>	LNMP代表Linux系统下Nginx+MySQL+PHP这种网站服务器架构，Nginx是一个小巧而高效的Linux下的Web服务器软件。
<a href="#">基于WordPress搭建个人网站 (Linux)</a>	手动部署	Linux	公共镜像 <ul style="list-style-type: none"><li>Nginx 1.14.0</li><li>MySQL 5.7</li><li>PHP 7.0.31</li><li>WordPress 4.9.8</li></ul>	使用弹性云服务器的Linux实例手工搭建LNMP平台，并部署WordPress环境。WordPress简称WP，最初是一款博客系统，后逐步演化成一款免费的CMS（内容管理系统/建站系统）。
<a href="#">手工部署Docker (CentOS 7.5)</a>	手动部署	Linux	公共镜像	使用弹性云服务器的Linux实例部署Docker，并提供了Docker常用操作及简单的镜像制作过程。
<a href="#">搭建微信公众号后台——收发文本消息</a>	手动部署	Linux	公共镜像	使用弹性云服务器搭建微信公众号处理后台，使用Python语言编写对应的微信消息处理逻辑代码，接收从微信服务端转发过来的消息，并返回处理结果给最终用户。

网站搭建方案	搭建方式	操作系统	镜像及所含资源	说明
<a href="#">手工部署 GitLab (CentOS 7.2)</a>	手动部署	Linux	公共镜像	使用弹性云服务器的Linux实例手工部署GitLab。GitLab是一个开源的版本管理系统，使用Git作为代码管理工具。
<a href="#">手工部署 RabbitMQ (CentOS 7.4)</a>	手动部署	Linux	公共镜像 <ul style="list-style-type: none"><li>Erlang 8.3</li><li>RabbitMQ 3.6.9</li></ul>	使用弹性云服务器的Linux实例部署RabbitMQ。RabbitMQ是采用Erlang语言实现AMQP (Advanced Message Queuing Protocol, 高级消息队列协议) 的消息中间件，它最初起源于金融系统，用于在分布式系统中存储转发消息。RabbitMQ凭借其高可靠、易扩展、高可用及丰富的功能特性成为目前非常热门的一款消息中间件。
<a href="#">手工搭建 Ghost博客 (Ubuntu 20.04)</a>	手动部署	Linux	公共镜像 <ul style="list-style-type: none"><li>Nginx 1.14.0</li><li>MySQL 5.7</li></ul>	Ghost是基于Node.js的开源博客平台，可以为用户提供更加便捷的写作与发布平台，本文指导用户基于华为云弹性云服务器（以Ubuntu 20.04操作系统云服务器为例）部署Ghost博客。
<a href="#">手工部署 Node.js (CentOS 7.2)</a>	手动部署	Linux	公共镜像	使用弹性云服务器的Linux实例部署Node.js。Node.js是一个基于Chrome V8引擎的JavaScript运行环境，用于方便地搭建响应速度快、易于扩展的网络应用。Node.js使用事件驱动，非阻塞I/O模型而得以轻量和高效，非常适合在分布式设备上运行数据密集型的实时应用。



# 3 弹性云服务器配置最佳实践

为了能够更加安全、可靠、灵活、高效的使用弹性云服务器，建议您购买弹性云服务器后执行以下最佳实践。

## 访问与连接

为了确保弹性云服务器创建成功且状态正常，建议您第一次通过VNC方式远程登录弹性云服务器，若登录成功则表明弹性云服务器资源状态正常。

详细操作，请参见：

- [Windows弹性云服务器管理控制台远程登录（VNC方式）](#)
- [Linux弹性云服务器远程登录（VNC方式）](#)

之后，您就可以根据本地环境以及弹性云服务器是否绑定弹性公网IP，选择合适的登录方式，详细内容请参见[如何登录弹性云服务器？](#)。

## 系统更新

- 更新镜像源（Linux）  
为了及时获取最新的系统更新和软件安装依赖，建议您在使用弹性云服务器之前更新镜像源。  
华为云内网源无需连接Internet、且服务稳定，对于使用EulerOS、CentOS、Debian、Ubuntu操作系统的弹性云服务器，建议您更新为华为云内网源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)
- 更新Windows补丁和驱动（Windows）  
为了提高弹性云服务器的问题修复能力和性能，建议您定时更新Windows的补丁和驱动程序。  
您可以通过设置Windows自动更新，及时发现最新的补丁和驱动版本，提醒您进行更新。

## 数据存储

- 存储安全  
为了实现数据的存储安全性，建议您将操作系统和应用数据分别存储在系统盘和数据盘，一方面保证数据的安全，避免因系统故障导致用户数据丢失；另一方面可根据业务需要扩容或新增磁盘扩展存储容量。

- 扩容磁盘：支持扩容系统盘和数据盘，建议您参考[扩容“正在使用”状态的云硬盘容量](#)扩容磁盘容量。
- 新增磁盘：支持新增数据盘，建议您[新增磁盘](#)，并完成[挂载磁盘](#)和[初始化数据盘](#)后，才可以正常使用。
- 数据加密  
为了进一步保护数据的安全性，建议您使用加密的系统盘和数据盘。详细内容，请参见[管理加密云硬盘](#)。

## 安全管理

- 身份认证  
为了实现对资源的安全访问和权限控制，建议您创建IAM用户，并结合企业项目实现对资源的身份认证、权限管理和资源分组管理，详细内容请参见[多运维人员权限设置案例](#)和[多项目管理实践案例](#)。
- 登录鉴权方式  
为了保证在丢失密码或密码失效的情况下，可以成功重置密码，建议您在弹性云服务器的购买完成后，优先执行[安装一键式重置密码插件（可选）](#)或[更新一键式重置密码插件（单台操作）](#)操作。
- 访问控制  
为了实现对弹性云服务器入方向和出方向的访问进行控制，提高安全性，建议您根据控制的范围设置相应的访问控制策略：
  - 基于ECS实例：建议您使用安全组功能，通过安全组规则实现对ECS的访问控制。详细内容，请参见[安全组配置示例](#)。
  - 基于ECS所在子网：建议您使用网络ACL功能，通过网络ACL规则实现对子网内所有ECS实例的访问控制。详细内容，请参见[网络ACL配置示例](#)。
- 安全防护  
为了实现对弹性云服务器的高阶安全防护，除了免费开启的主机安全基础防护外，建议您根据防护需求购买高阶的主机安全防护版本，详细的版本功能、版本差异及购买方式，请参见[版本功能差异](#)和[主机安全快速入门](#)。
- 网络防护  
为了防止弹性云服务器绑定的弹性公网IP被攻击，建议您购买华为云的[DDoS防护](#)服务。
- 敏感操作保护  
为了保证账号及操作的安全性，建议您开启敏感操作保护功能，在控制台执行关机、重启、删除等敏感操作时，进行身份验证。该功能对账号以及账号下的用户都生效。  
详细内容，请参见[敏感操作保护](#)。

## 备份与恢复

- 数据备份与恢复  
为了在发生病毒入侵、人为误删除、软硬件故障等事件时，能够快速恢复数据，建议您定期进行数据备份，备份的具体方案和适用场景，请参见[云备份概述](#)。  
备份成功后，可以[使用云服务器备份恢复数据](#)或[使用备份创建镜像](#)的方式恢复数据。
- 高可用容灾业务部署

为了实现较高的业务容灾能力，建议您将云服务器资源部署在同一区域的不同可用区内。可用区的具体内容，请参见[区域和可用区](#)和[自定义购买ECS](#)。

- 主备应用HA业务部署

为了实现弹性云服务器的主备切换、达到高可用HA的目的，建议您参考[搭建Keepalived Nginx高可用Web集群](#)方案进行部署。

## 操作维护管理

- 监控管理

为了使用户能够及时获取弹性云服务器的各项性能指标及运行状态，建议您使用云监控服务，执行自动实时监控、告警和通知操作。

详细内容，请参见[云监控服务](#)。

- 关键操作管理

为了能够对弹性云服务器的操作进行查询、审计和回溯，建议您开启云审计服务记录与之相关的操作事件。

更多内容，请参见[云审计服务](#)。

- 日志管理

为了提高弹性云服务器和应用程序的可用性和性能，建议您通过云日志服务收集日志数据，通过对海量日志数据的分析和处理，实现实时决策分析、设备运维管理、用户业务趋势分析等能力。

详细内容，请参见[云日志服务](#)。

# 4 搭建环境

## 4.1 搭建 LNMP 环境

### 4.1.1 手工搭建 LNMP 环境 (CentOS 7.2)

#### 简介

LNMP分别代表Linux、Nginx、MySQL和PHP，是目前主流的网站服务器架构之一，适合运行大型和高并发的网站应用，例如电子商务网站、社交网络、内容管理系统等。本文主要介绍了在华为云上如何使用CentOS 7.2 64位操作系统的Linux实例搭建LNMP环境。

Linux实例手工部署LNMP环境具体操作步骤如下：

1. [安装Nginx。](#)
2. [安装MySQL。](#)
3. [安装PHP。](#)
4. [浏览器访问测试。](#)

#### 前提条件

1. 弹性云服务器已绑定弹性公网IP。
2. 弹性云服务器所在安全组添加了如下表所示的安全组规则，具体步骤参见[为安全组添加安全组规则](#)。

表 4-1 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 80	0.0.0.0/0

3. 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。

## 资源规划

本次实践所用的资源配置及软件版本如表4-2中所示。当您使用不同的硬件规格或软件版本时，本指导中的命令及参数可能会发生改变，需要根据实际情况进行调整。

表 4-2 资源和成本规划

资源	资源说明	成本说明
弹性云服务器	<ul style="list-style-type: none"><li>计费模式：按需计费</li><li>可用区：可用区1</li><li>规格：s6.large.4</li><li>镜像：CentOS 7.2 64bit</li><li>系统盘：40G</li><li>弹性公网IP：现在购买</li><li>线路：全动态BGP</li><li>公网带宽：按流量计费</li><li>带宽大小：5 Mbit/s</li></ul>	ECS涉及以下几项费用： <ul style="list-style-type: none"><li>云服务器</li><li>云硬盘</li><li>弹性公网IP</li></ul> 具体的计费方式及标准请参考 <a href="#">计费模式概述</a> 。
Nginx	是一个高性能的HTTP和反向代理web服务器。 获取方式： <a href="http://nginx.org/packages/centos/7/noarch/RPMS/nginx-release-centos-7-0.el7ngx.noarch.rpm">http://nginx.org/packages/centos/7/noarch/RPMS/nginx-release-centos-7-0.el7ngx.noarch.rpm</a>	免费
MySQL	是一款开源的关系数据库软件。 获取方式： <a href="https://dev.mysql.com/get/mysql80-community-release-el7-11.noarch.rpm">https://dev.mysql.com/get/mysql80-community-release-el7-11.noarch.rpm</a>	免费
PHP	是一款开源软件，用于Web开发。 获取方式： <a href="https://mirrors.huaweicloud.com/remi/enterprise/remi-release-7.rpm">https://mirrors.huaweicloud.com/remi/enterprise/remi-release-7.rpm</a>	免费

## 操作步骤

### 步骤1 安装Nginx。

1. 登录弹性云服务器。

2. 执行以下命令，下载对应当前系统版本的Nginx包。  
**wget http://nginx.org/packages/centos/7/noarch/RPMS/nginx-release-centos-7-0.el7ngx.noarch.rpm**
3. 执行以下命令，建立Nginx的yum仓库。  
**rpm -ivh nginx-release-centos-7-0.el7ngx.noarch.rpm**
4. 执行以下命令，安装Nginx。  
**yum -y install nginx**
5. 执行以下命令，查看Nginx版本。  
**nginx -v**  
回显如下类似信息。  
nginx version: nginx/1.26.1
6. 执行以下命令，启动Nginx并设置开机启动。  
**systemctl start nginx**  
**systemctl enable nginx**
7. 查看启动状态。  
**systemctl status nginx.service**
8. 使用浏览器访问“<http://服务器IP地址>”，显示如下页面，说明Nginx安装成功。

图 4-1 测试访问 Nginx

## Welcome to nginx!

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

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

### 步骤2 安装MySQL。

1. 依次执行以下命令，安装MySQL。  
**rpm -Uvh https://dev.mysql.com/get/mysql80-community-release-el7-11.noarch.rpm**  
**yum -y install mysql-community-server**
2. 执行以下命令，查看MySQL版本。  
**mysql -V**  
回显如下类似信息。  
mysql Ver 8.0.39 for Linux on x86\_64 (MySQL Community Server - GPL)
3. 依次执行以下命令，启动MySQL服务并设置开机自启动。  
**systemctl start mysqld**  
**systemctl enable mysqld**
4. 查看MySQL运行状态。  
**systemctl status mysqld.service**

回显如下类似信息。

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

Aug 14 17:01:11 systemd[1]: Starting MySQL Server...
Aug 14 17:01:17 systemd[1]: Started MySQL Server.
```

5. 执行以下命令，获取安装MySQL时自动设置的root用户密码。

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

回显如下类似信息。

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

6. 执行以下命令，并按照回显提示信息进行操作，加固MySQL。

```
mysql_secure_installation
```

Securing the MySQL server deployment.

Enter password for user root: #输入上一步骤中获取的安装MySQL时自动设置的root用户密码  
The existing password for the user account root has expired. Please set a new password.

New password: #设置新的root用户密码

Re-enter new password: #再次输入密码

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 #是否更改root用户密码，输入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 #是否删除匿名用户，输入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 #禁止root远程登录，输入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 #是否删除test库和对它的访问权限，输入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 #是否重新加载授权表，输入Y

```
Success.  
All done!
```

### 步骤3 安装PHP。

1. 执行以下命令，安装EPEL源和Remi仓库。

```
yum install -y epel-release
```

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

2. 执行以下命令，安装Yum源管理工具。

```
yum -y install yum-utils
```

3. 执行以下命令，启用PHP 8.0仓库。

```
yum-config-manager --enable remi-php80
```

4. 执行以下命令，安装PHP。

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

5. 执行以下命令，验证PHP的安装版本。

```
php -v
```

回显如下类似信息：

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

6. 执行以下命令，启动PHP服务并设置开机自启动。

```
systemctl start php-fpm
```

```
systemctl enable php-fpm
```

7. 修改Nginx配置文件以支持PHP。

- a. 执行以下命令打开配置文件/etc/nginx/nginx.conf。

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



图 4-2 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;
}
```

从nginx.conf可以看出，配置文件定向至/etc/nginx/conf.d/\*.conf。

- b. 输入:**quit**退出nginx.conf。
- c. 执行以下命令打开配置文件/etc/nginx/conf.d/default.conf。  
**vim /etc/nginx/conf.d/default.conf**
- d. 按i键进入编辑模式。
- e. 修改打开的“default.conf”文件。

找到server段落，修改或添加下列配置信息。

```
server {
    listen 80;
    server_name localhost;

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

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

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

如图4-3所示：

图 4-3 修改后截图

```
server {
    listen      80;
    server_name localhost;

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

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

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

    #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    /usr/share/nginx/html;
    }
}
```

- f. 按Esc键退出编辑模式，并输入:wq保存后退出。
- 8. 执行以下命令，重新载入Nginx的配置文件。

**service nginx reload**

**步骤4** 浏览器访问测试。

- 1. 在/usr/share/nginx/html/目录下创建“info.php”的测试页面。
  - a. 执行以下命令创建并打开“info.php”的测试文件。  
**vim /usr/share/nginx/html/info.php**
  - b. 按i键进入编辑模式。
  - c. 修改打开的“info.php”文件，将如下内容写入文件。  

```
<?php
phpinfo();
?>
```
  - d. 按Esc键退出编辑模式，并输入:wq保存后退出。
- 2. 使用浏览器访问“http://服务器IP地址/info.php”，显示如下页面，说明环境搭建成功。

PHP Version 8.0.30	
System	Linux 3.10.0-1160.53.1.el7.x86_64 #1 SMP Fri Jan 14 13:59:45 UTC 2022 x86_64
Build Date	Jun 4 2024 15:19:49
Build System	Red Hat Enterprise Linux Server release 7.9 (Maipo)
Build Provider	Remi's RPM repository <https://rpms.remirepo.net/> #StandWithUkraine
Compiler	gcc (GCC) 8.3.1 20190311 (Red Hat 8.3.1-3)
Architecture	x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bcmath.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-posix.ini, /etc/php.d/20-shmop.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sodium.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-sysvmsg.ini, /etc/php.d/20-sysvsem.ini, /etc/php.d/20-sysvshm.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-xml.ini, /etc/php.d/20-xmlwriter.ini, /etc/php.d/20-xsl.ini, /etc/php.d/30-mcrypt.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini, /etc/php.d/30-xmlreader.ini, /etc/php.d/30-zip.ini
PHP API	20200930
PHP Extension	20200930
Zend Extension	420200930
Zend Extension Build	API420200930,NTS
PHP Extension Build	API20200930,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*, mcrypt.*, mdecrypt.*

----结束

## 4.1.2 手工搭建 LNMP 环境 (CentOS 8.0)

### 简介

LNMP分别代表Linux、Nginx、MySQL和PHP，是目前主流的网站服务器架构之一，适合运行大型和高并发的网站应用，例如电子商务网站、社交网络、内容管理系统等。本文主要介绍了在华为云上如何使用CentOS 8.0 64位操作系统的Linux实例搭建LNMP环境。

Linux实例手工部署LNMP环境具体操作步骤如下：

1. [安装Nginx。](#)
2. [安装MySQL。](#)
3. [安装PHP。](#)
4. [浏览器访问测试。](#)

### 前提条件

1. 弹性云服务器已绑定弹性公网IP。
2. 弹性云服务器所在安全组添加了如下表所示的安全组规则，具体步骤参见[安全组添加安全组规则](#)。

表 4-3 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 80	0.0.0.0/0

- 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。

## 资源规划

本次实践所用的资源配置及软件版本如表4-4中所示。当您使用不同的硬件规格或软件版本时，本指导中的命令及参数可能会发生改变，需要您根据实际情况进行调整。

表 4-4 资源和成本规划

资源	资源说明	成本说明
弹性云服务器	<ul style="list-style-type: none"><li>计费模式：按需计费</li><li>可用区：可用区1</li><li>规格：s6.large.4</li><li>镜像：CentOS 8.0 64bit</li><li>系统盘：40G</li><li>弹性公网IP：现在购买</li><li>线路：全动态BGP</li><li>公网带宽：按流量计费</li><li>带宽大小：5 Mbit/s</li></ul>	ECS涉及以下几项费用： <ul style="list-style-type: none"><li>云服务器</li><li>云硬盘</li><li>弹性公网IP</li></ul> 具体的计费方式及标准请参考 <a href="#">计费模式概述</a> 。
Nginx	是一个高性能的HTTP和反向代理web服务器。 示例版本：Nginx 1.20.1	免费
MySQL	是一款开源的关系数据库软件。 示例版本：MySQL 8.0.26	免费
PHP	是一款开源软件，用于Web开发。 示例版本：PHP 7.4.19	免费

## 操作步骤

### 步骤1 安装Nginx。

- 登录弹性云服务器。
- 执行以下命令，安装Nginx。

```
sudo dnf -y install https://nginx.org/packages/centos/8/x86_64/RPMS/  
nginx-1.20.1-1.el8ngx.x86_64.rpm
```

3. 执行以下命令，查看Nginx版本。

```
nginx -v
```

回显如下类似信息。

```
nginx version: nginx/1.20.1
```

4. 执行以下命令，启动Nginx并设置开机启动。

```
systemctl start nginx
```

```
systemctl enable nginx
```

5. 查看启动状态。

```
systemctl status nginx.service
```

回显如下类似信息。

```
[root@ ~]# systemctl status nginx.service
● nginx.service - nginx - high performance web server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2024-08-14 10:47:48 CST; 25s ago
     Docs: http://nginx.org/en/docs/
   Main PID: 1793 (nginx)
    Tasks: 3 (limit: 49517)
   Memory: 3.0M
   CGroup: /system.slice/nginx.service
           └─1793 nginx: master process /usr/sbin/nginx -c /etc/nginx/nginx.conf
             └─1794 nginx: worker process
               └─1795 nginx: worker process

Aug 14 10:47:48 systemd[1]: Starting nginx - high performance web server...
Aug 14 10:47:48 systemd[1]: Started nginx - high performance web server.
```

6. 使用浏览器访问“<http://服务器IP地址>”，显示如下页面，说明Nginx安装成功。

图 4-4 测试访问 Nginx

## Welcome to nginx!

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

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

### 步骤2 安装MySQL。

1. 执行以下命令，安装MySQL。

```
sudo dnf -y install @mysql
```

2. 执行以下命令，查看MySQL版本。

```
mysql -V
```

回显如下类似信息。

```
mysql Ver 8.0.26 for Linux on x86_64 (Source distribution)
```

3. 依次执行以下命令，启动MySQL服务并设置开机自启动。

```
systemctl start mysqld
```

```
systemctl enable mysqld
```

## 4. 查看MySQL运行状态。

**systemctl status mysqld.service**

回显如下类似信息。

```
[root@ ~]# systemctl status mysqld.service
● mysqld.service - MySQL 8.0 database server
   Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2024-08-14 10:55:34 CST; 21s ago
     Main PID: 2088 (mysqld)
    Status: "Server is operational"
       Tasks: 38 (limit: 49517)
      Memory: 527.8M
     CGroup: /system.slice/mysqld.service
            └─2088 /usr/libexec/mysqld --basedir=/usr

Aug 14 10:55:28 systemd[1]: Starting MySQL 8.0 database server...
Aug 14 10:55:28 mysql-prepare-db-dir[2084]: Initializing MySQL database
Aug 14 10:55:34 systemd[1]: Started MySQL 8.0 database server.
```

## 5. 执行以下命令，并按照回显提示信息进行操作，加固MySQL。

**mysql\_secure\_installation**

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

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

Press y|Y for Yes, ant other key for No: Y #设置密码验证策略，输入Y

There are three levels of password validation policy:

LOW Length >= 8

MEDIUM Length >= 8, numeric, mixed case, and special characters

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

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2 #选择密码验证策略，输入2  
Please set the password for root here.

New password: #设置新的root用户密码

Re-enter new password: #再次输入密码

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 #确认使用已设置的密码，输入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 #是否删除匿名用户，输入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 #禁止root远程登录，输入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 #是否删除test库和对它的访问权限, 输入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 #是否重新加载授权表, 输入Y
Success.

All done!
```

### 步骤3 安装PHP。

1. 执行以下命令，添加并更新epel源。  
**sudo dnf -y install epel-release**  
**sudo dnf -y update epel-release**
2. 执行以下命令，删除缓存的无用软件包并更新软件源。  
**sudo dnf clean all**  
**sudo dnf makecache**
3. 执行以下命令，启动PHP 7.4模块。  
**dnf module enable php:7.4**
4. 执行以下命令，安装PHP对应模块。  
**sudo dnf -y install php php-curl php-dom php-exif php-fileinfo php-fpm php-gd php-hash php-json php-mbstring php-mysqli php-openssl php-pcre php-xml libsodium**
5. 执行以下命令，验证PHP的安装版本。

**php -v**

回显如下类似信息：

```
[root@ ~]# php -v
PHP 7.4.19 (cli) (built: May 4 2021 11:06:37) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
with Zend OPcache v7.4.19, Copyright (c), by Zend Technologies
```

6. 执行以下命令，启动PHP服务并设置开机自启动。  
**systemctl start php-fpm**  
**systemctl enable php-fpm**
7. 修改Nginx配置文件以支持PHP。
  - a. 执行以下命令打开配置文件/etc/nginx/nginx.conf。  
**vim /etc/nginx/nginx.conf**

图 4-5 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;
}
```

从nginx.conf可以看出，配置文件定向至/etc/nginx/conf.d/\*.conf。

- b. 输入:quit退出nginx.conf。
- c. 执行以下命令打开配置文件/etc/nginx/conf.d/default.conf。

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

- d. 按i键进入编辑模式。
- e. 修改打开的“default.conf”文件。

找到server段落，修改或添加下列配置信息。

```
server {
    listen 80;
    server_name localhost;

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

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

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

如图4-6所示：



图 4-6 修改后截图

```
server {
    listen      80;
    server_name localhost;

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

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

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

    #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    /usr/share/nginx/html;
    }

    # proxy the PHP scripts to Apache listening on 127.0.0.1:80
    #
    #location ~ \.php$ {
    #    proxy_pass http://127.0.0.1;
    #}
}
```

- f. 按Esc键退出编辑模式，并输入:wq保存后退出。
8. 执行以下命令，重新载入Nginx的配置文件。  
**service nginx reload**


#### 步骤4 浏览器访问测试。

1. 在/usr/share/nginx/html/目录下创建“info.php”的测试页面。
  - a. 执行以下命令创建并打开“info.php”的测试文件。  
**vim /usr/share/nginx/html/info.php**
  - b. 按i键进入编辑模式。
  - c. 修改打开的“info.php”文件，将如下内容写入文件。  

```
<?php
phpinfo();
?>
```
  - d. 按Esc键退出编辑模式，并输入:wq保存后退出。
2. 使用浏览器访问“http://服务器IP地址/info.php”，显示如下页面，说明环境搭建成功。

PHP Version 7.4.19	
System	Linux 4.18.0-348.7.1.el8_5.x86_64 #1 SMP Wed Dec 22 13:25:12 UTC 2021 x86_64
Build Date	May 4 2021 11:06:37
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/10-opcache.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-json.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-xml.ini, /etc/php.d/20-xmlwriter.ini, /etc/php.d/20-xsl.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysqli.ini, /etc/php.d/30-pdo_sqlite.ini, /etc/php.d/30-xmlreader.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	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, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:  
Zend Engine v3.4.0, Copyright (c) Zend Technologies  
with Zend OPcache v7.4.19, Copyright (c), by Zend Technologies



----结束

## 4.1.3 手工搭建 LNMP 环境 ( Ubuntu 20.04 )

### 简介

本文主要介绍了在华为云上如何使用弹性云服务器的Linux实例手工搭建LNMP平台的Web环境。本文档以Ubuntu 20.04 64位操作系统为例。

Linux实例手工部署LNMP环境具体操作步骤如下：

1. [安装Nginx](#)
2. [安装MySQL](#)
3. [安装PHP](#)
4. [浏览器访问测试](#)

### 前提条件

1. 弹性云服务器已绑定弹性公网IP。
2. 弹性云服务器所在安全组添加了如下表所示的安全组规则，具体步骤参见[安全组添加安全组规则](#)。

表 4-5 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 80	0.0.0.0/0

- 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。

## 资源规划

本次实践所用的资源配置及软件版本如表4-6中所示。当您使用不同的硬件规格或软件版本时，本指导中的命令及参数可能会发生改变，需要您根据实际情况进行调整。

表 4-6 资源和成本规划

资源	资源说明	成本说明
弹性云服务器	<ul style="list-style-type: none"><li>计费模式：按需计费</li><li>可用区：可用区1</li><li>规格：s6.large.2</li><li>镜像：Ubuntu 20.04 64bit</li><li>系统盘：40G</li><li>弹性公网IP：现在购买</li><li>线路：全动态BGP</li><li>公网带宽：按流量计费</li><li>带宽大小：5 Mbit/s</li></ul>	ECS涉及以下几项费用： <ul style="list-style-type: none"><li>云服务器</li><li>云硬盘</li><li>弹性公网IP</li></ul> 具体的计费方式及标准请参考 <a href="#">计费模式概述</a> 。
Nginx	是一个高性能的HTTP和反向代理web服务器。	免费
MySQL	是一款开源的关系数据库软件。	免费
PHP	是一款开源软件，用于Web开发。	免费

## 操作步骤

### 步骤1 安装Nginx。

- 登录弹性云服务器。
- 执行以下命令安装Nginx。

```
sudo apt-get update
```

```
sudo apt-get install nginx
```

安装过程中若出现“Do you want to continue? [Y/n]”提示信息，输入“y”或“Y”即可继续安装。

## 3. 调整防火墙（可选）。

UFW（Uncomplicated Firewall）是一个iptables的接口，可以简化配置防火墙的过程。Ubuntu默认安装了UFW，执行以下命令查看防火墙的状态。

**sudo ufw status**

如果你没有也不想开启防火墙，则可以直接跳过此步骤，如果你想要开启防火墙可以通过以下命令实现。

**sudo ufw enable**

之后再次检查防火墙状态验证是否成功开启防火墙。

在测试Nginx之前，需要重新配置防火墙软件以允许访问Nginx。执行以下命令，将Nginx自动注册在UFW。

**sudo ufw app list**

回显信息：

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

- Nginx Full: 此配置文件打开端口 80（正常，未加密的Web流量）和端口 443（TLS / SSL加密流量）
- Nginx HTTP: 此配置文件仅打开端口 80（正常，未加密的Web流量）
- Nginx HTTPS: 此配置文件仅打开端口 443（TLS / SSL加密流量）

执行以下命令确保防火墙允许HTTP和HTTPS连接。

**sudo ufw allow 'Nginx Full'**

## 4. 验证Nginx是否正常工作。

在浏览器中通过域名或者IP地址进行访问Nginx，如果Nginx正常启动则会打开Welcome to nginx的欢迎页面。

使用浏览器访问“<http://云服务器IP地址>”，显示如下页面，说明Nginx安装成功。

图 4-7 测试访问 nginx

**步骤2 安装MySQL。**

## 1. 执行以下命令安装MySQL。

```
sudo apt -y install mysql-server
```

## 2. 查看MySQL运行状态。

```
sudo systemctl status mysql
```

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

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

3. 执行以下命令，进入MySQL。

```
sudo mysql
```

4. 执行以下命令，设置root用户密码。

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

其中'xxxxx'为待设置的密码。

5. 执行以下命令，退出MySQL数据库。

```
exit;
```

6. 执行以下命令，并按照回显提示信息进行操作，加固MySQL。

```
mysql_secure_installation
```

```
Securing the MySQL server deployment.
```

```
Enter password for user root:          #输入步骤4中设置的root用户密码
```

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

```
Press y|Y for Yes, any other key for No: Y  #设置密码验证策略，输入Y
```

```
There are three levels of password validation policy:
```

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

```
Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2  #选择密码验证策略，输入2
```

```
Using existing password for root.
```

```
Estimated strength of the password: 25
```

```
Change the password for root ? ((Press y|Y for Yes, any other key for No) : Y  #是否更改root用户密码，输入Y
```

```
New password: #设置新的root用户密码
```

```
Re-enter new password: #再次输入密码
```

```
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  #确认使用已设置的密码，输入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  #是否删除匿名用户，输入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 #禁止root远程登录, 输入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 #是否删除test库
和对它的访问权限, 输入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 #是否重新加载授权表, 输入Y
Success.

All done!
```

### 步骤3 安装PHP。

1. 执行以下命令，安装PHP。

```
sudo apt update
sudo apt install php-fpm
```

2. 执行以下命令，验证PHP的安装版本。

```
php -v
```

回显如下类似信息：

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

3. 执行以下命令，查看PHP运行状态。

```
systemctl status php7.4-fpm
```

回显如下信息：

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

#### 说明

回显信息中若出现“lines 1-16/16 (end)”，可按q键退出。

4. 修改Nginx配置文件以支持PHP。
  - a. 执行以下命令，打开Nginx默认的配置文。

```
sudo vim /etc/nginx/sites-enabled/default
```

- b. 按i键进入编辑模式。
- c. 修改打开的Nginx配置文件。

在server{}内，找到index开头的配置行，在该行中添加index.php。

```
# Default server configuration
#
server {
    listen 80 default_server;
    listen [::]:80 default_server;

    # SSL configuration
    #
    # listen 443 ssl default_server;
    # listen [::]:443 ssl default_server;
    #
    # Note: You should disable gzip for SSL traffic.
    # See: https://bugs.debian.org/773332
    #
    # Read up on ssl_ciphers to ensure a secure configuration.
    # See: https://bugs.debian.org/765782
    #
    # Self signed certs generated by the ssl-cert package
    # Don't use them in a production server!
    #
    # include snippets/snakeoil.conf;

    root /var/www/html;

    # Add index.php to the list if you are using PHP
    index index.php index.html index.htm index.nginx-debian.html;

    server_name _;

    location / {
        # First attempt to serve request as file, then
```

在server{}内找到location ~ /\.php\$ {}，去除以下配置行的注释符号。

```
location / {
    # First attempt to serve request as file, then
    # as directory, then fall back to displaying a 404.
    try_files $uri $uri/ =404;
}

# pass PHP scripts to FastCGI server
#
location ~ /\.php$ {
    include snippets/fastcgi-php.conf;

    #
    # With php-fpm (or other unix sockets):
    fastcgi_pass unix:/var/run/php/php7.4-fpm.sock;
    # With php-cgi (or other tcp sockets):
    fastcgi_pass 127.0.0.1:9000;
}

# deny access to .htaccess files, if Apache's document root
# concurs with nginx's one
```

d. 按Esc键退出编辑模式，并输入:wq保存后退出。

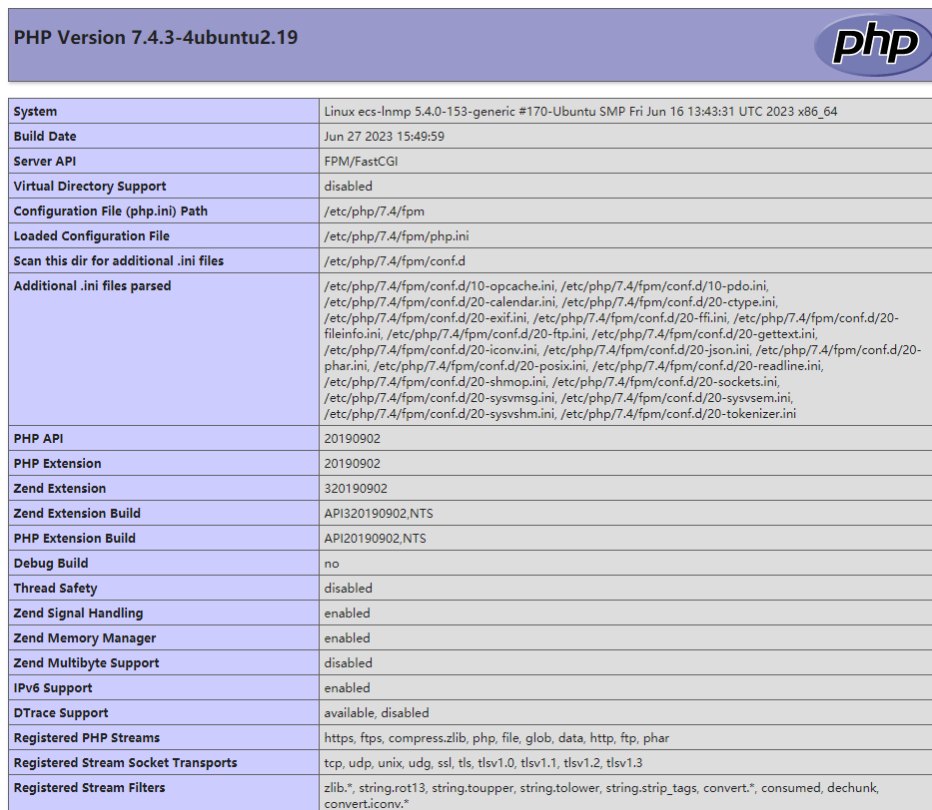
5. 执行以下命令，重新载入nginx的配置文件。

```
sudo systemctl restart nginx
```

**步骤4** 浏览器访问测试。

1. 在Nginx网站根目录中，新建phpinfo.php文件。  
**sudo vim /var/www/html/phpinfo.php**
2. 按*i*键进入编辑模式。
3. 修改打开的“phpinfo.php”文件，将如下内容写入文件。  

```
<?php echo phpinfo(); ?>
```
4. 按Esc键退出编辑模式，并输入:wq保存后退出。
5. 使用浏览器访问“http://服务器IP地址/phpinfo.php”，显示如下页面，说明环境搭建成功。



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

----结束

## 4.1.4 手工搭建 LNMP 环境 ( Huawei Cloud EulerOS 2.0 )

### 简介

本文主要介绍了在华为云上如何使用弹性云服务器的Linux实例手工搭建LNMP平台的Web环境。该指导具体操作以Huawei Cloud EulerOS 2.0 64位操作系统为例。

Linux实例手工部署LNMP环境具体操作步骤如下：

1. [安装Nginx。](#)
2. [安装MySQL。](#)
3. [安装PHP。](#)
4. [浏览器访问测试。](#)



## 前提条件

1. 弹性云服务器已绑定弹性公网IP。
2. 弹性云服务器所在安全组添加了如下表所示的安全组规则，具体步骤参见[为安全组添加安全组规则](#)。

表 4-7 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 80	0.0.0.0/0

## 资源规划

本次实践所用的资源配置及软件版本如[表4-8](#)中所示。当您使用不同的硬件规格或软件版本时，本指导中的命令及参数可能会发生改变，需要您根据实际情况进行调整。

表 4-8 资源和成本规划

资源	资源说明	成本说明
弹性云服务器	<ul style="list-style-type: none"><li>● 计费模式：按需计费</li><li>● 可用区：可用区1</li><li>● 规格：s6.large.2</li><li>● 镜像：Huawei Cloud EulerOS 2.0 64bit</li><li>● 系统盘：40G</li><li>● 弹性公网IP：现在购买</li><li>● 线路：全动态BGP</li><li>● 公网带宽：按流量计费</li><li>● 带宽大小：5 Mbit/s</li></ul>	ECS涉及以下几项费用： <ul style="list-style-type: none"><li>● 云服务器</li><li>● 云硬盘</li><li>● 弹性公网IP</li></ul> 具体的计费方式及标准请参考 <a href="#">计费模式概述</a> 。
Nginx	是一个高性能的HTTP和反向代理web服务器。	免费
MySQL	是一款开源的关系数据库软件。	免费
PHP	是一款开源软件，用于Web开发。	免费

## 操作步骤

### 步骤1 安装Nginx。

1. 登录弹性云服务器。
2. 执行以下命令，安装Nginx。

```
sudo yum -y install nginx
```

3. 执行以下命令，验证Nginx的安装版本。

```
nginx -v
```

回显如下类似信息：

```
nginx version: nginx/1.21.5
```

4. 执行以下命令，启动Nginx并设置开机启动。

```
systemctl start nginx
```

```
systemctl enable nginx
```

5. 查看启动状态。

```
systemctl status nginx.service
```

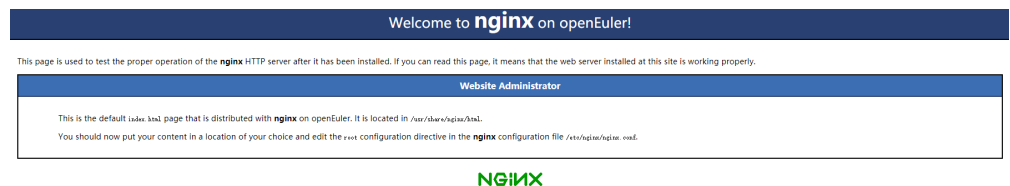
回显如下类似信息。

```
root@ecs-hce ~# systemctl status nginx.service
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2023-08-11 14:59:59 CST; 18s ago
     Main PID: 4634 (nginx)
       Tasks: 3 (limit: 47418)
      Memory: 7.2M
     CGroup: /system.slice/nginx.service
            └─ 4634 "nginx: master process /usr/sbin/nginx"
               └─ 4635 "nginx: worker process"
                  └─ 4636 "nginx: worker process"

Aug 11 14:59:58 ecs-hce systemd[1]: Starting The nginx HTTP and reverse proxy server...
Aug 11 14:59:58 ecs-hce nginx[4631]: nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
Aug 11 14:59:58 ecs-hce nginx[4631]: nginx: configuration file /etc/nginx/nginx.conf test is successful
Aug 11 14:59:59 ecs-hce systemd[1]: Started The nginx HTTP and reverse proxy server.
```

6. 使用浏览器访问“<http://服务器IP地址>”，显示如下页面，说明Nginx安装成功。

图 4-8 测试访问 Nginx



## 步骤2 安装MySQL。

1. 依次执行以下命令，安装MySQL。

```
mkdir mysql-server
```

```
cd mysql-server
```

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

```
yum install mysql-server
```

2. 依次执行以下命令，启动MySQL服务并设置开机自启动。

```
systemctl start mysqld
```

```
systemctl enable mysqld
```

3. 查看MySQL运行状态。

```
systemctl status mysqld.service
```

回显如下类似信息。

```
[root@ecs-hce mysql-server]# systemctl status mysqld.service
● mysqld.service - MySQL 8.0 database server
   Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2023-08-11 11:17:57 CST; 20s ago
     Main PID: 5390 (mysqld)
    Status: "Server is operational"
      Tasks: 38 (limit: 21654)
     Memory: 465.7M
    CGroup: /system.slice/mysqld.service
            └─ 5390 /usr/libexec/mysqld --basedir=/usr

Aug 11 11:17:51 ecs-hce systemd[1]: Starting MySQL 8.0 database server...
Aug 11 11:17:51 ecs-hce mysql-prepare-db-dir[5312]: Initializing MySQL database
Aug 11 11:17:57 ecs-hce systemd[1]: Started MySQL 8.0 database server.
```

4. 执行以下命令，并按照回显提示信息进行操作，加固MySQL。

### mysql\_secure\_installation

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

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

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

There are three levels of password validation policy:

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

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

New password: #设置新的root用户密码

Re-enter new password: #再次输入密码

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 #确认使用已设置的密码，输入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 #是否删除匿名用户，输入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 #禁止root远程登录，输入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 #是否删除test库和对它的访问权限，输入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 #是否重新加载授权表, 输入Y  
Success.
```

```
All done!
```

5. 执行以下命令，退出当前文件夹。

```
cd ~
```

### 步骤3 安装PHP。

1. 依次执行以下命令，安装PHP 8。

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

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

2. 执行以下命令，验证PHP的安装版本。

```
php -v
```

回显如下类似信息：

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

3. 执行以下命令，启动PHP服务并设置开机自启动。

```
systemctl start php-fpm
```

```
systemctl enable php-fpm
```

4. 修改Nginx配置文件以支持PHP。

- a. 执行以下命令打开Nginx配置文件。

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

- b. 按i键进入编辑模式。

- c. 修改打开的“nginx.conf”文件。

找到server段落，修改或添加下列配置信息。

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

如图4-9所示：

图 4-9 修改后截图

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

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

    location / {
        index index.php index.html index.htm;
    }

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

    error_page 404 /404.html;
    location = /40x.html {
    }

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

- d. 按Esc键退出编辑模式，并输入:wq保存后退出。
- 5. 执行以下命令，重新载入Nginx的配置文件。

**service nginx reload**


**步骤4 浏览器访问测试。**

- 1. 在/usr/share/nginx/html/目录下创建“info.php”的测试页面。
  - a. 执行以下命令创建并打开“info.php”的测试文件。  
**vim /usr/share/nginx/html/info.php**
  - b. 按i键进入编辑模式。
  - c. 修改打开的“info.php”文件，将如下内容写入文件。  

```
<?php
phpinfo();
?>
```
  - d. 按Esc键退出编辑模式，并输入:wq保存后退出。
- 2. 使用浏览器访问“http://服务器IP地址/info.php”，显示如下页面，说明环境搭建成功。

PHP Version 8.0.0	
System	Linux ecs-hce 5.10.0-60.18.0.50.r865_35.hce2.x86_64 #1 SMP Sun Mar 26 18:01:01 UTC 2023 x86_64
Build Date	Nov 24 2020 17:04:03
Build System	Linux szxrtosci10000 4.19.90-2003.4.0.0036.oe1.x86_64 #1 SMP Mon Mar 23 19:10:41 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-tokenizer.ini
PHP API	20200930
PHP Extension	20200930
Zend Extension	420200930
Zend Extension Build	API420200930,NTS
PHP Extension Build	API20200930,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
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, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*

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



----结束

## 4.2 搭建 LAMP 环境

### 4.2.1 手工搭建 LAMP 环境（CentOS 7.8 PHP7.0）

#### 简介

LAMP是由Linux、Apache、MySQL和PHP建立的web应用平台。

本文主要介绍了在华为云上如何使用弹性云服务器的Linux实例手工搭建LAMP平台的web环境。该指导具体操作以CentOS 7.8 64位操作系统为例。

#### 前提条件

1. 弹性云服务器已绑定弹性公网IP。
2. 弹性云服务器所在安全组添加了如下表所示的安全组规则，具体步骤参见[为安全组添加安全组规则](#)。

表 4-9 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 80	0.0.0.0/0

- 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。

## 资源规划

本次实践所用的资源配置及软件版本如表4-10中所示。当您使用不同的硬件规格或软件版本时，本指导中的命令及参数可能会发生改变，需要您根据实际情况进行调整。

表 4-10 资源和成本规划

资源	资源说明	成本说明
弹性云服务器	<ul style="list-style-type: none"><li>计费模式：按需计费</li><li>可用区：可用区1</li><li>规格：c7.large.2</li><li>镜像：CentOS 7.8 64bit</li><li>系统盘：40G</li><li>弹性公网IP：现在购买</li><li>线路：全动态BGP</li><li>公网带宽：按流量计费</li><li>带宽大小：5 Mbit/s</li></ul>	ECS涉及以下几项费用： <ul style="list-style-type: none"><li>云服务器</li><li>云硬盘</li><li>弹性公网IP</li></ul> 具体的计费方式及标准请参考 <a href="#">计费模式概述</a> 。
Apache	是一个开放源码的Web服务器。	免费
MySQL	是一款开源的关系数据库软件。 获取方式： <a href="http://dev.mysql.com/get/mysql57-community-release-el7-10.noarch.rpm">http://dev.mysql.com/get/mysql57-community-release-el7-10.noarch.rpm</a>	免费
PHP	是一款开源软件，用于Web开发。 获取方式： <a href="https://mirror.webtatic.com/yum/el7/epel-release.rpm">https://mirror.webtatic.com/yum/el7/epel-release.rpm</a> <a href="https://mirror.webtatic.com/yum/el7/webtatic-release.rpm">https://mirror.webtatic.com/yum/el7/webtatic-release.rpm</a>	免费

## 操作步骤

### 步骤1 安装Apache。

1. 登录弹性云服务器。
2. 使用root用户执行以下命令更新软件包，并安装Apache。

```
yum -y update  
yum -y install httpd
```

3. 执行以下命令，验证Apache的安装版本。

```
httpd -v
```

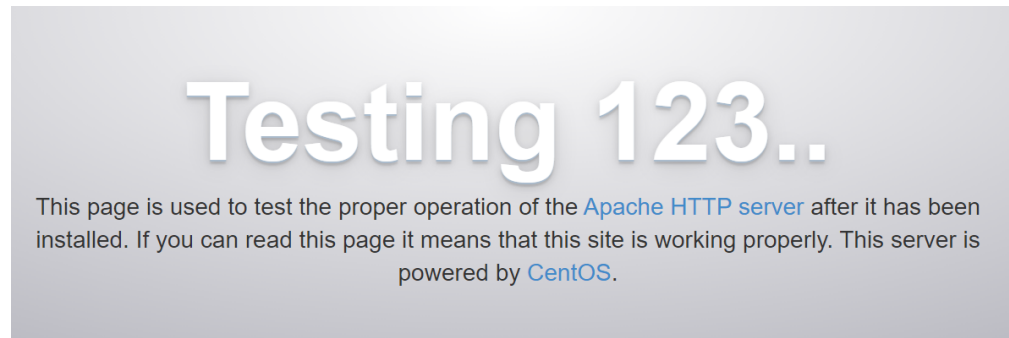
回显如下类似信息：

```
Server version: Apache/2.4.6 (CentOS)  
Server built:   May 30 2023 14:01:11
```

4. 依次执行以下命令，启动Apache服务并设置开机自启动。

```
systemctl start httpd  
systemctl enable httpd
```

5. 使用浏览器访问“http://服务器IP地址”，显示如下页面，说明Apache安装成功。



#### Just visiting?

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

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

#### Are you the Administrator?

You should add your website content to the directory /var/www/html/.

To prevent this page from ever being used, follow the instructions in the file /etc/httpd/conf.d/welcome.conf.

#### Promoting Apache and CentOS

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



#### Important note:

The CentOS Project has nothing to do with this website or its content, it just provides the software that makes the website run.

#### The CentOS Project

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

### 步骤2 安装MySQL。

1. 依次执行以下命令，安装MySQL。

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

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

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



2. 执行以下命令，验证MySQL的安装版本。

```
mysql -V
```

回显如下类似信息：

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

3. 依次执行以下命令，启动MySQL服务并设置开机自启动。

```
systemctl start mysqld
```

```
systemctl enable mysqld
```

4. 查看MySQL运行状态。

```
systemctl status mysqld.service
```

```
[root@ecs-adc3 ~]# systemctl status mysqld.service
● mysqld.service - MySQL Server
  Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; vendor preset: disabled)
  Active: active (running) since Tue 2023-10-31 19:33:40 CST; 36s ago
    Docs: man:mysqld(8)
           http://dev.mysql.com/doc/refman/en/using-systemd.html
  Main PID: 7916 (mysqld)
  CGroup: /system.slice/mysqld.service
          └─7916 /usr/sbin/mysqld --daemonize --pid-file=/var/run/mysqld/mysqld.pid
```

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

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

5. 执行以下命令，获取安装MySQL时自动设置的root用户密码。

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

回显如下类似信息。

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

6. 执行以下命令，并按照回显提示信息进行操作，加固MySQL。

```
mysql_secure_installation
```

Securing the MySQL server deployment.

Enter password for user root: #输入上一步骤中获取的安装MySQL时自动设置的root用户密码  
The existing password for the user account root has expired. Please set a new password.

New password: #设置新的root用户密码

Re-enter new password: #再次输入密码

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 #是否更改root用户密码，输入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 #是否删除匿名用户，输入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 #禁止root远程登录，输入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 #是否删除test库和对它的访问权限, 输入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 #是否重新加载授权表, 输入Y
Success.

All done!
```

### 步骤3 安装PHP。

1. 依次执行以下命令，安装PHP 7和一些所需的PHP扩展。

```
rpm -Uvh https://mirror.webtatic.com/yum/el7/epel-release.rpm
rpm -Uvh https://mirror.webtatic.com/yum/el7/webtatic-release.rpm
yum -y install php70w-devel php70w.x86_64 php70w-cli.x86_64 php70w-common.x86_64 php70w-gd.x86_64 php70w-ldap.x86_64 php70w-mbstring.x86_64 php70w-mcrypt.x86_64 php70w-pdo.x86_64 php70w-mysqldb php70w-fpm php70w-opcache php70w-pecl-redis php70w-pecl-mongodb
```

2. 执行以下命令，验证PHP的安装版本。

```
php -v
```

回显如下类似信息：

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

3. 执行以下命令，启动PHP服务并设置开机自启动。

```
systemctl start php-fpm
systemctl enable php-fpm
```

### 步骤4 浏览器访问测试。

1. 在/var/www/html/目录下创建“info.php”的测试页面。

- a. 执行以下命令创建并打开“info.php”的测试文件。

```
vim /var/www/html/info.php
```

- b. 按i键进入编辑模式。

- c. 修改打开的“info.php”文件，将如下内容写入文件。

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

- d. 按Esc键退出编辑模式，并输入:wq保存后退出。


2. 执行以下命令，重启Apache服务。

```
systemctl restart httpd
```

3. 使用浏览器访问“http://服务器IP地址/info.php”，显示如下页面，说明环境搭建成功。

PHP Version 7.0.33	
System	Linux ecs-maxiaorui-wx1058652-20231103 3.10.0-1160.92.1.el7.x86_64 #1 SMP Tue Jun 20 11:48:01 UTC 2023 x86_64
Build Date	Dec 6 2018 22:31:47
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/bz2.ini, /etc/php.d/calendar.ini, /etc/php.d/ctype.ini, /etc/php.d/curl.ini, /etc/php.d/dom.ini, /etc/php.d/exif.ini, /etc/php.d/fileinfo.ini, /etc/php.d/ftp.ini, /etc/php.d/gd.ini, /etc/php.d/gettext.ini, /etc/php.d/gmp.ini, /etc/php.d/iconv.ini, /etc/php.d/igbinary.ini, /etc/php.d/json.ini, /etc/php.d/ldap.ini, /etc/php.d/mbstring.ini, /etc/php.d/mcrypt.ini, /etc/php.d/mongodb.ini, /etc/php.d/mysqli.ini, /etc/php.d/mysqli_mysqlnd.ini, /etc/php.d/openssl.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_mysqlnd.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/posix.ini, /etc/php.d/redis.ini, /etc/php.d/shmop.ini, /etc/php.d/simplexml.ini, /etc/php.d/sockets.ini, /etc/php.d/sqlite3.ini, /etc/php.d/sybase.ini, /etc/php.d/sybase-ctlib.ini, /etc/php.d/sysvsem.ini, /etc/php.d/sysvshm.ini, /etc/php.d/tokenizer.ini, /etc/php.d/xml.ini, /etc/php.d/xml_wddx.ini, /etc/php.d/xmlreader.ini, /etc/php.d/xmlwriter.ini, /etc/php.d/xsl.ini, /etc/php.d/zip.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*, mcrypt.*, mdecrypt.*

This program makes use of the Zend Scripting Language Engine:  
Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies  
with Zend OPcache v7.0.33, Copyright (c) 1999-2017, by Zend Technologies



----结束

## 4.3 搭建 Java Web 环境

### 4.3.1 基于 Tomcat 构建 Java web 环境 (CentOS 7.4)

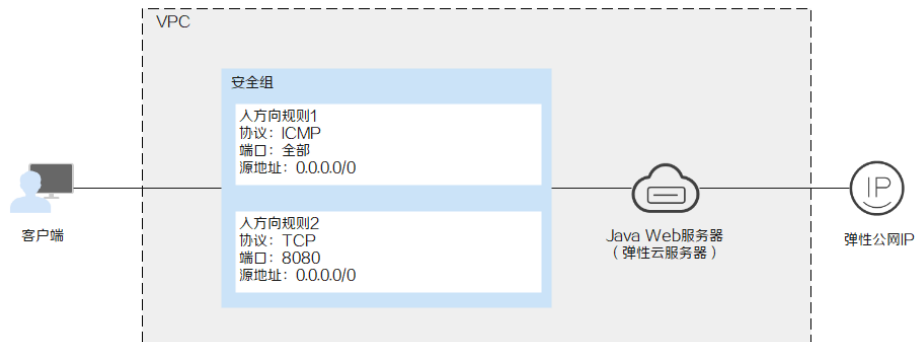
#### 应用场景

Tomcat是一个被广泛使用的Java Web应用服务器。本文介绍了在华为云弹性云服务器上部署Java Web环境的操作步骤。首先需要下载部署Java Web环境所需的安装包，并将安装包上传至云服务器，然后设置弹性云服务器安全组规则，再安装并配置相关软件，完成开发环境的配置。

本文使用的云服务器以华为云CentOS 7.4 64bit操作系统云服务器为例。

## 方案架构

图 4-10 基于 Tomcat 构建 Java web 环境示意图



## 资源和成本规划

表 4-11 资源和成本规划

资源	资源说明	成本说明
虚拟私有云VPC	VPC网段: 192.168.0.0/16	免费
虚拟私有云子网	<ul style="list-style-type: none"> <li>可用区: 可用区1</li> <li>子网网段: 192.168.0.0/24</li> </ul>	免费
安全组	入方向规则1: <ul style="list-style-type: none"> <li>优先级: 1</li> <li>策略: 允许</li> <li>类型: IPv4</li> <li>协议端口: ICMP: 全部</li> <li>源地址: 0.0.0.0/0</li> </ul> 入方向规则2: <ul style="list-style-type: none"> <li>优先级: 1</li> <li>策略: 允许</li> <li>类型: IPv4</li> <li>协议端口: TCP: 8080</li> <li>源地址: 0.0.0.0/0</li> </ul>	免费

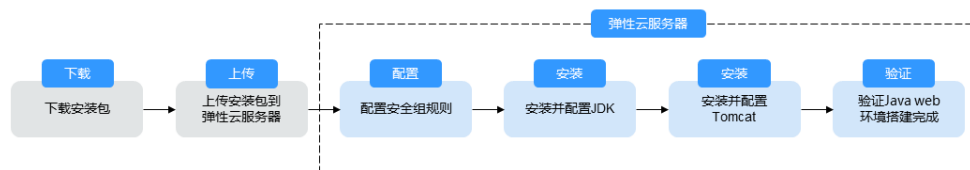
资源	资源说明	成本说明
弹性云服务器	<ul style="list-style-type: none"><li>● 计费模式：包年/包月</li><li>● 可用区：可用区1</li><li>● 规格：c7.large.2</li><li>● 镜像：CentOS 7.4 64bit</li><li>● 系统盘：40G</li><li>● 弹性公网IP：现在购买</li><li>● 线路：全动态BGP</li><li>● 公网带宽：按流量计费</li><li>● 带宽大小：5 Mbit/s</li></ul>	ECS涉及以下几项费用： <ul style="list-style-type: none"><li>● 云服务器</li><li>● 云硬盘</li><li>● 弹性公网IP</li></ul> 具体的计费方式及标准请参考 <a href="#">计费模式概述</a> 。
jdk	Java开发工具软件。 获取方式： <a href="http://www.oracle.com/technetwork/java/javase/downloads">http://www.oracle.com/technetwork/java/javase/downloads</a>	免费
tomcat	是一款开源的Web应用服务器。 获取方式： <a href="http://tomcat.apache.org/download-80.cgi">http://tomcat.apache.org/download-80.cgi</a>	免费
PuTTY	跨平台远程访问工具。用于在软件安装过程中在Windows系统上访问云服务器。 获取方式： <a href="https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html">https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html</a>	免费
WinSCP	跨平台文件传输工具。用于在Windows系统和Linux系统间传输文件。 获取方式： <a href="http://winscp.net/">http://winscp.net/</a>	免费

#### 📖 说明

[表4-11](#)中为jdk和tomcat官方获取地址，您还可以参考其他开源镜像地址获取安装包。

## 基于 Tomcat 构建 Java web 环境操作流程

图 4-11 安装流程



## 实施步骤

### 安装前准备

- 创建弹性云服务器，且弹性云服务器已绑定弹性公网IP。
- 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。
- 登录弹性云服务器，执行如下命令，新建jdk目录和tomcat目录。

```
cd /home/  
mkdir webDemo  
cd webDemo/  
mkdir jdk  
mkdir tomcat
```

- 您可以选择将安装包下载至本地后使用文件传输工具将安装包上传至云服务器。或者选择使用wget命令直接下载安装包至云服务器。

– 方法一：使用文件传输工具上传安装包至云服务器。

- 使用WinSCP工具上传jdk软件包至云服务器jdk文件夹。
- 使用WinSCP工具上传tomcat软件包至云服务器tomcat文件夹。

– 方法二：使用wget命令直接下载安装包至云服务器。

i. 执行如下命令，进入jdk目录。

```
cd /home/webDemo/jdk
```

ii. 执行如下命令，下载jdk软件包。

```
wget jdk软件包下载地址
```

请参考表4-11查询jdk下载地址，或者使用其他开源镜像地址获取安装包。

例如：以jdk17为例，在列表中查看可用的JDK软件包版本，以jdk-17\_linux-x64\_bin.tar.gz安装包为例，执行以下命令。

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

iii. 执行如下命令，进入tomcat目录。

```
cd /home/webDemo/tomcat
```

iv. 执行如下命令，下载tomcat软件包。

请参考表4-11查询tomcat下载地址，或者使用其他开源镜像地址获取安装包。

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

例如：单击[开源镜像地址](#)，查询当前可用版本，以v8.5.xx版本安装包为例，执行以下命令。

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

### 设置弹性云服务器安全组规则

1. 单击弹性云服务器名称，查看弹性云服务器详情，在弹性云服务器详情页面，选择“安全组”。
2. 在“安全组”界面，单击“更改安全组规则”，进入安全组详情界面。
3. 在安全组详情界面，单击“添加规则”，弹出添加规则窗口。
4. 根据界面提示配置安全组规则。

部署Java Web环境需为弹性云服务器添加两个安全组规则。

- a. 为云服务器添加ICMP安全组规则。

如果云服务器默认设置是禁止ICMP规则，当ping弹性服务器IP时会显示超时。因此首先为云服务器添加ICMP规则。

图 4-12 添加 ICMP 规则

添加方向规则 [教我设置](#)

安全组输入方向规则为白名单（允许），放通入方向网络流量。

安全组 default

如您要添加多条规则，建议单击导入规则以进行批量导入。

优先级	策略	协议端口	类型	源地址	描述	操作
1	允许	ICMP	IPv4	IP地址 0.0.0.0/0		复制 删除

增加1条规则

确定 取消

- b. 为云服务器添加web项目分配端口的访问规则，以8080端口为例。

图 4-13 添加 8080 端口

添加方向规则 [教我设置](#)

安全组输入方向规则为白名单（允许），放通入方向网络流量。

安全组 default

如您要添加多条规则，建议单击导入规则以进行批量导入。

优先级	策略	协议端口	类型	源地址	描述	操作
1	允许	TCP 8080	IPv4	IP地址 0.0.0.0/0		复制 删除

增加1条规则

确定 取消

## 安装jdk

1. 执行如下命令，进入jdk目录。

```
cd /home/webDemo/jdk
```

2. 解压jdk安装包到jdk目录下。

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

3. 配置环境变量。

```
vim /etc/profile
```

4. 在底部添加以下内容。

```
#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
```

### 📖 说明

“*jdk-17.0.x*”表示jdk安装包的具体版本，实际值需要从步骤2的返回值中获取。

例如：jdk-17.0.9

5. 执行以下命令保存并退出。

```
:wq
```

6. 执行以下命令使/etc/profile里的配置生效。

```
source /etc/profile
```

7. 验证安装。

```
java -version
```

回显信息如下所示验证安装jdk成功。

```
[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)
```

## 安装tomcat

1. 执行如下命令，进入tomcat目录。

```
cd /home/webDemo/tomcat
```

2. 解压tomcat安装包到tomcat目录下。

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

例如：以v8.5.xx版本安装包为例，执行以下命令。

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

3. 进入tomcat的bin目录，执行以下命令安装tomcat。

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

```
cd bin/
```

例如：以v8.5.xx版本安装包为例，执行以下命令。

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

```
cd bin/
```

4. 执行如下命令编辑setclasspath.sh脚本。

```
vi setclasspath.sh
```

并在setclasspath.sh脚本底部添加以下内容。



请根据[资源和成本规划](#)中jdk的版本号替换如下内容中的jdk版本号。

```
export JAVA_HOME=/home/webDemo/jdk/jdk-17.0.9
export JRE_HOME=$JAVA_HOME
```

5. 执行如下命令保存后退出。

```
:wq
```

6. 可输入以下命令启动tomcat。

```
./startup.sh
```

7. 执行如下命令查看tomcat进程。

```
ps -ef | grep tomcat
```

若返回如下图所示，表示tomcat启动成功。

图 4-14 查看 tomcat 进程

```
root@ecs ~# 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/webDemo/tomcat/apache-tomcat-8.5.95/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djdk.tls.ephemeralDHKeySize=2048 -Djava.protocol.handler.pkgs=org.apache.catalina.webresources -Dorg.apache.catalina.security.SecurityListener.UMSK=0027 -Dignore.endorsed.dirs=-classpath /home/webDemo/tomcat/apache-tomcat-8.5.95/bin/bootstrap.jar:/home/webDemo/tomcat/apache-tomcat-8.5.95/bin/tomcat-juli.jar -Dcatalina.base=/home/webDemo/tomcat/apache-tomcat-8.5.95 -Dcatalina.home=/home/webDemo/tomcat/apache-tomcat-8.5.95 -Djava.io.tmpdir=/home/webDemo/tomcat/apache-tomcat-8.5.95/temp org.apache.catalina.startup.Bootstrap start
root      8718      0 14:33 tty1      00:00:00 grep --color=auto tomcat
root@ecs ~#
```

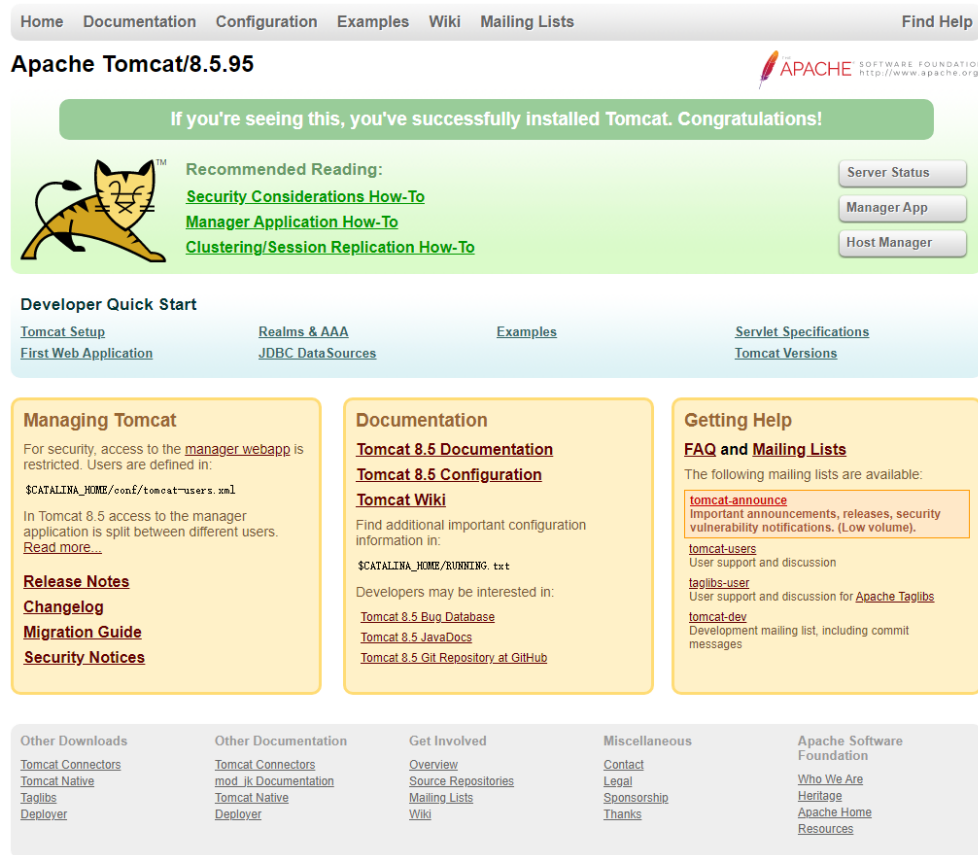
### 验证Java Web环境搭建完成

在浏览器输入以下内容。

<http://云服务器弹性公网IP:8080>

如果界面跳转至默认的Tomcat界面，证明Java Web环境搭建完成。就可以在公网访问云服务器的8080端口了。

图 4-15 访问云服务器的 8080 端口



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

## 4.3.2 基于 Tomcat 构建 Java web 环境（ Huawei Cloud EulerOS 2.0 ）

### 简介

Tomcat是一个免费的，开放源代码的Web应用服务器，是Apache软件基金会项目中的一个核心项目，是一款比较流行的web应用服务器。本教程介绍如何在HCE 2.0上安装部署Tomcat。

### 准备工作

- 准备一台ECS，并分配公网IP或者弹性公网IP（EIP）。
- 安全组入方向已放开8080端口。

### 操作步骤

#### 步骤1 软件安装。

1. 执行以下命令安装Java。  
`dnf install java-1.8.0-openjdk`
2. 执行如下命令验证是否安装成功。  
`java -version`

3. 执行如下命令安装Tomcat。

```
dnf install tomcat
```

Tomcat会被安装到“/usr/share/tomcat”目录。

## 步骤2 配置软件。

1. 编辑“/etc/profile”配置环境变量，新增如下内容。

```
JAVA_HOME=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.342.b07-0.hce2.x86_64/jre  
PATH=$PATH:$JAVA_HOME/bin  
CLASSPATH=.:$JAVA_HOME/lib/dt.jar:$JAVA_HOME/lib/tools.jar  
export JAVA_HOME CLASSPATH PATH
```

2. 执行以下命令激活上述环境变量。

```
source /etc/profile
```

3. 清空“/usr/share/tomcat/conf/server.xml”文件，粘贴以下内容。

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

保存并退出，可根据需要，自定义上述配置。

4. 执行以下命令创建上述配置中appbase和docbase填入的目录。

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

5. 然后执行以下命令将上述目录所属用户设置为tomcat。

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

6. 新建“/usr/share/tomcat/bin/setenv.sh”文件，输入以下内容配置JVM内存参数。

```
JAVA_OPTS='-Djava.security.egd=file:/dev/./urandom -server -Xms256m -Xmx496m -  
Dfile.encoding=UTF-8'
```

7. 执行以下命令启动Tomcat服务。

```
systemctl start tomcat
```

8. 执行如下命令查看Tomcat服务状态。

```
systemctl status tomcat
```

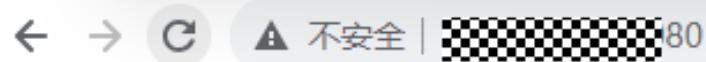
如果显示**active (running)**则表示服务启动成功。

## 步骤3 验证Tomcat安装是否成功。

1. 执行以下命令，新增测试页面。

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

2. 然后在浏览器输入http://<Tomcat服务公网IP>:8080进行访问，如果显示如下图则表示安装成功。



## Tomcat test

----结束

### ⚠ 注意

以上相关配置仅用于测试，业务环境请谨慎使用。

## 4.4 手工搭建 Hadoop 环境（Linux）

### 简介

本文介绍了如何在华为云上使用弹性云服务器的Linux实例手工搭建Hadoop环境。Hadoop是一款由Apache基金会用Java语言开发的分布式开源软件框架，用户可以在不了解分布式底层细节的情况下，开发分布式程序，充分利用集群的能力进行高速运算和存储。Hadoop的核心部件是HDFS（Hadoop Distributed File System）和MapReduce：

- HDFS：是一个分布式文件系统，可对应用程序数据进行分布式储存和读取。
- MapReduce：是一个分布式计算框架，MapReduce的核心思想是把计算任务分配给集群内的服务器执行。通过对计算任务的拆分（Map计算和Reduce计算），再根据任务调度器（JobTracker）对任务进行分布式计算。

更多信息，请参见[Hadoop官网](#)。

### 前提条件

- 已购买一台弹性云服务器，且已为其绑定弹性公网IP。
- 弹性云服务器所在安全组添加了如下表所示的安全组规则，具体步骤参见[为安全组添加安全组规则](#)。

表 4-12 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 8088	0.0.0.0/0
入方向	1	允许	IPv4	TCP: 50070	0.0.0.0/0

- 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。

## 操作流程

Linux实例手工搭建Hadoop环境的具体操作步骤如下：

1. [安装JDK](#)
2. [安装Hadoop](#)
3. [配置Hadoop](#)
4. [配置SSH免密登录](#)
5. [启动Hadoop](#)

## 实施步骤

### 步骤1 安装JDK

1. 登录弹性云服务器。
2. 执行以下命令，下载jdk软件包。  
以jdk17为例，在列表中查看可用的JDK软件包版本，以jdk-17\_linux-x64\_bin.tar.gz安装包为例，执行以下命令。

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

3. 解压jdk安装包到opt目录下。  
**tar -xvf jdk-17\_linux-x64\_bin.tar.gz -C /opt/**
4. 配置环境变量。

```
vim /etc/profile
```

5. 在底部添加以下内容。  

```
#set java environment  
export JAVA_HOME=/opt/jdk-17.0.x  
export PATH=$PATH:$JAVA_HOME/bin
```

#### 说明

“jdk-17.0.x”表示jdk安装包的具体版本，实际值需要从步骤3的返回值中获取。

例如：jdk-17.0.8

6. 按“Esc”退出编辑模式。
7. 执行以下命令保存并退出。  
**:wq**
8. 执行以下命令使/etc/profile里的配置生效。  
**source /etc/profile**
9. 验证安装。

```
java -version
```

回显信息如下表示jdk安装成功。

```
java version "17.0.8" 2023-07-18 LTS  
Java(TM) SE Runtime Environment (build 17.0.8+9-LTS-211)  
Java HotSpot(TM) 64-Bit Server VM (build 17.0.8+9-LTS-211, mixed mode, sharing)
```

### 步骤2 安装Hadoop

1. 执行以下命令，下载Hadoop软件包。此处以2.10.x版本为例。

### 📖 说明

以下命令中，需要将“2.10.x”中的“x”替换为具体的软件版本号。

```
wget https://mirrors.bfsu.edu.cn/apache/hadoop/common/hadoop-2.10.x/hadoop-2.10.x.tar.gz
```

2. 解压Hadoop安装包到opt目录下。

```
tar -xvf hadoop-2.10.x.tar.gz -C /opt/
```

3. 配置环境变量。

```
vim /etc/profile
```

4. 在底部添加以下内容。

```
#set hadoop environment
export HADOOP_HOME=/opt/hadoop-2.10.x
export PATH=$PATH:$HADOOP_HOME/bin:$HADOOP_HOME/sbin:$PATH
export HDFS_NAMENODE_USER=root
export HDFS_DATANODE_USER=root
export HDFS_SECONDARYNAMENODE_USER=root
```

5. 按“Esc”退出编辑模式。

6. 执行以下命令保存并退出。

```
:wq
```

7. 执行以下命令使/etc/profile里的配置生效。

```
source /etc/profile
```

8. 执行以下命令，修改配置文件yarn-env.sh和hadoop-env.sh中JAVA\_HOME的路径。

```
echo "export JAVA_HOME=/opt/jdk-17.0.8" >> /opt/hadoop-2.10.x/etc/hadoop/yarn-env.sh
```

```
echo "export JAVA_HOME=/opt/jdk-17.0.8" >> /opt/hadoop-2.10.x/etc/hadoop/hadoop-env.sh
```

9. 验证安装。

```
hadoop version
```

回显信息如下所示表示Hadoop安装成功。

```
Hadoop 2.10.x
Subversion https://github.com/apache/hadoop -r 1827467c9a56f133025f28557bfc2c562d78e816
Compiled by centos on 2020-09-14T13:17Z
Compiled with protoc 2.5.0
From source with checksum 3114edef868f1f3824e7d0f68be03650
This command was run using /opt/hadoop-2.10.x/share/hadoop/common/hadoop-common-2.10.x.jar
```

### 步骤3 配置Hadoop

1. 修改Hadoop配置文件core-site.xml。

- a. 执行以下命令，进入编辑页面。

```
vim /opt/hadoop-2.10.x/etc/hadoop/core-site.xml
```

- b. 输入i，进入编辑模式。

- c. 在<configuration></configuration>节点内，插入如下内容。

```
<property>
  <name>hadoop.tmp.dir</name>
  <value>file:/opt/hadoop-2.10.x/tmp</value>
  <description>location to store temporary files</description>
</property>
<property>
  <name>fs.defaultFS</name>
```

```
<value>hdfs://localhost:9000</value>
</property>
```

- d. 按“Esc”退出编辑模式。
- e. 执行以下命令保存并退出。

```
:wq
```

2. 修改Hadoop配置文件hdfs-site.xml。

- a. 执行以下命令，进入编辑页面。

```
vim /opt/hadoop-2.10.x/etc/hadoop/hdfs-site.xml
```

- b. 输入i，进入编辑模式。

- c. 在<configuration></configuration>节点内，插入如下内容。

```
<property>
  <name>dfs.replication</name>
  <value>1</value>
</property>
<property>
  <name>dfs.namenode.name.dir</name>
  <value>file:/opt/hadoop-2.10.x/tmp/dfs/name</value>
</property>
<property>
  <name>dfs.datanode.data.dir</name>
  <value>file:/opt/hadoop-2.10.x/tmp/dfs/data</value>
</property>
```

- d. 按“Esc”退出编辑模式。
- e. 执行以下命令保存并退出。

```
:wq
```

#### 步骤4 配置SSH免密登录

1. 执行以下命令，创建公钥和私钥。

```
ssh-keygen -t rsa
```

按三次回车后回显信息如下图所示，表示创建公钥和私钥成功。

```
[root@ecs-... hadoop1# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:kd/RaF80FQ+e0wHocH+3YYKQvCT9XXr1G3oF5q/1Qz4 root@ecs-...
The key's randomart image is:
+---[RSA 2048]---+
|  o . .o+ = |
| . 0 o +o* = |
| = B BoB.* |
| + * B.O+ |
| S . . B.B |
| . =o |
| ++ |
| .E. |
| o |
+---[SHA256]-----+
```

2. 执行以下命令，将公钥添加到authorized\_keys文件中。

```
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
```

```
chmod 0600 ~/.ssh/authorized_keys
```

#### 步骤5 启动Hadoop

1. 执行以下命令，初始化namenode。

## hadoop namenode -format

2. 依次执行以下命令，启动Hadoop。

a. **start-dfs.sh**

在回显信息中，依次输入yes。

```
[root@ecs ~]# start-dfs.sh
Starting namenodes on [localhost]
The authenticity of host 'localhost (:::1)' can't be established.
ECDSA key fingerprint is SHA256:UGSremAysYcu3KTSqseKti+QBDXEIPoCjefIruELM0g.
ECDSA key fingerprint is MD5:ac:49:99:62:92:8b:3f:07:91:8e:29:c1:76:54:46:78.
Are you sure you want to continue connecting (yes/no)? yes
localhost: Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
localhost: starting namenode, logging to /opt/hadoop-2.10.1/logs/hadoop-root-namenode-ecs-...out
localhost: starting datanode, logging to /opt/hadoop-2.10.1/logs/hadoop-root-datanode-ecs-...out
Starting secondary namenodes [0.0.0.0]
The authenticity of host '0.0.0.0 (0.0.0.0)' can't be established.
ECDSA key fingerprint is SHA256:UGSremAysYcu3KTSqseKti+QBDXEIPoCjefIruELM0g.
ECDSA key fingerprint is MD5:ac:49:99:62:92:8b:3f:07:91:8e:29:c1:76:54:46:78.
Are you sure you want to continue connecting (yes/no)? yes
0.0.0.0: Warning: Permanently added '0.0.0.0' (ECDSA) to the list of known hosts.
0.0.0.0: starting secondarynamenode, logging to /opt/hadoop-2.10.1/logs/hadoop-root-secondarynamenode-ecs-...out
230925.out
```

b. **start-yarn.sh**

回显信息如下图所示。

```
[root@ecs ~]# start-yarn.sh
starting yarn daemons
starting resourcemanager, logging to /opt/hadoop-2.10.1/logs/yarn-root-resourcemanager-ecs-...out
localhost: starting nodemanager, logging to /opt/hadoop-2.10.1/logs/yarn-root-nodemanager-ecs-...out
```

3. 执行以下命令，可查看成功启动的进程。

### jps

成功启动的进程如下所示。

```
9138 NameNode
9876 Jps
9275 DataNode
9455 SecondaryNameNode
```

4. 打开浏览器访问<http://服务器弹性公网IP地址:8088>和<http://服务器弹性公网IP地址:50070>。

若显示如下界面，表示Hadoop环境搭建完成。

The screenshot shows the Hadoop All Applications web interface. The top navigation bar includes the Hadoop logo and the text "All Applications". On the right, it says "Lopped in as: dr:who". The main content area is divided into several sections:

- Cluster Metrics:** A table with columns: Apps Submitted (0), Apps Pending (0), Apps Running (0), Apps Completed (0), Containers Running (0), Memory Used (8 GB), Memory Total (8 GB), Memory Reserved (0), VCores Used (8), VCores Total (8), VCores Reserved (0).
- Cluster Nodes Metrics:** A table with columns: Active Nodes (1), Decommissioning Nodes (0), Decommissioned Nodes (0), Lost Nodes (0), Unhealthy Nodes (0), Rebooted Nodes (0), Shutdown Nodes (0).
- Scheduler Metrics:** A table with columns: Scheduler Type (Capacity Scheduler), Scheduling Resource Type (MEMORY), Minimum Allocation (memory:1024, VCores:1), Maximum Allocation (memory:8192, VCores:4), Maximum Cluster Application Priority (0).
- Applications Table:** A table with columns: ID, User, Name, Application Type, Queue, Application Priority, StartTime, FinishTime, State, FinalStatus, Running Containers, Allocated CPU, Allocated Memory, Reserved CPU, Reserved Memory, % of Queue, % of Cluster, Progress, Tracking UI, Blacklisted Nodes. Below the table, it says "Showing 0 to 0 of 0 entries" and "No data available in table".



Hadoop Overview Datanodes Datanode Volume Failures Snapshot Startup Progress Utilities

### Overview 'localhost:9000' (active)

Started:	Mon Sep 25 19:08:17 +0800 2023
Version:	2.10.1, r1827467c9a56f133025f28557bfc2c562d78e816
Compiled:	Mon Sep 14 21:17:00 +0800 2020 by centos from branch-2.10.1
Cluster ID:	CID-f29c344a-652a-4e39-827c-c940d7dfc000
Block Pool ID:	BP-1451782850-127.0.0.1-1695640051105

### Summary

Security is off.  
Safemode is off.  
1 files and directories, 0 blocks = 1 total filesystem object(s).  
Heap Memory used 39.66 MB of 73 MB Heap Memory. Max Heap Memory is 1000 MB.  
Non Heap Memory used 42.32 MB of 45 MB Committed Non Heap Memory. Max Non Heap Memory is <unbounded>.

Configured Capacity:	39.25 GB
DFS Used:	24 KB (0%)
Non DFS Used:	5.53 GB
DFS Remaining:	31.7 GB (80.77%)
Block Pool Used:	24 KB (0%)
DataNodes usages% (Min/Median/Max/stdDev):	0.00% / 0.00% / 0.00% / 0.00%
Live Nodes	1 (Decommissioned: 0, In Maintenance: 0)
Dead Nodes	0 (Decommissioned: 0, In Maintenance: 0)

----结束

## 4.5 手工部署 Node.js (CentOS 7.2)

### 简介

本文介绍了如何在华为云上使用弹性云服务器的Linux实例部署Node.js。

Node.js是一个基于Chrome V8引擎的JavaScript运行环境，用于方便地搭建响应速度快、易于扩展的网络应用。Node.js使用事件驱动，非阻塞I/O模型而得以轻量和高效率，非常适合在分布式设备上运行数据密集型的实时应用。

更多关于Node.js信息，请参见<https://nodejs.org>。

该操作以“CentOS 7.2 64bit(40G)”操作系统为例，使用的Node.js软件包版本为“node-v10.14.1-linux-x64.tar”及“node-v10.14.2-linux-x64.tar”。

### 前提条件

- 已创建弹性云服务器，创建过程请参考[自定义购买ECS](#)。
- 弹性云服务器需要绑定弹性公网IP，具体步骤参见[申请弹性公网IP](#)。
- 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。
- 本地已经安装用于连接 Linux 弹性云服务器的工具（如 [PuTTY](#)）。

## 操作步骤

### 步骤1 安装Node.js安装包。

- 使用二进制文件安装。
  - a. 登录弹性云服务器。
  - b. 执行以下命令，下载**Node.js安装包**。  
**wget https://nodejs.org/dist/v10.14.1/node-v10.14.1-linux-x64.tar.xz**
  - c. 执行以下命令，解压文件。  
**tar xvJf node-v10.14.1-linux-x64.tar.xz**
  - d. 依次执行以下命令，为node及npm建立软连接，可在任意目录下执行node及npm命令。  
**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. 依次执行以下命令，查看node及npm版本。  
**node -v**  
**npm -v**
- 使用NVM版本管理器安装多版本。
  - a. 登录弹性云服务器。
  - b. 执行以下命令，安装git。  
**yum install git**
  - c. 执行以下命令，使用git将源码克隆到本地的~/.nvm目录下，并检查最新版本。  
**git clone https://github.com/cnpm/nvm.git ~/.nvm && cd ~/.nvm && git checkout `git describe --abbrev=0 --tags`**
  - d. 执行以下命令，激活NVM，并将其追加至profile文件下。  
**echo ". ~/.nvm/nvm.sh" >> /etc/profile**
  - e. 执行如下命令，使环境变量生效。  
**source /etc/profile**
  - f. 执行以下命令，列出Node.js可用版本。  
**nvm ls-remote**
  - g. 执行以下命令，安装多个Node.js版本。  
**nvm install v10.14.1**  
**nvm install v10.14.2**
  - h. 执行以下命令，查看已安装的Node.js版本。  
**nvm ls**
  - i. 执行以下命令切换Node.js版本至V10.14.2。  
**nvm use v10.14.2**

#### 说明

- 执行**nvm alias default v10.14.2**，设置默认版本为10.14.2。
- 执行**nvm help**，获取更多NVM操作信息。

## 步骤2 部署测试项目。

1. 执行以下命令，进入用户主目录。

```
cd
```

2. 执行以下命令，新建项目文件test.js。

```
touch test.js
```

3. 使用vim编辑器编辑项目文件test.js。

- a. 执行以下命令，打开项目文件test.js。

```
vim test.js
```

- b. 按i键进入编辑模式。

输入以下项目文件内容，修改打开的“test.js”文件。

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

端口号port可自定义。

- c. 按Esc键退出编辑模式，并输入:wq保存后退出。

4. 执行以下命令，查看已开启端口。

```
netstat -lntp
```

若定义端口不存在，需登录弹性云服务器控制台，更改安全组规则，具体步骤参见[添加安全组规则](#)。

5. 添加防火墙例外端口。

- a. 以本例使用的3000端口为例，执行以下命令，添加防火墙例外端口3000。

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

如果回显信息如下说明防火墙关闭，可直接执行[步骤2.6](#)

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

如果回显信息如下说明防火墙开启且添加例外端口成功。

```
[root@ecs-centos7 ~]# firewall-cmd --zone=public --add-port=3000/tcp --permanent
success
```

- b. 重新加载策略配置，使新配置生效。

```
firewall-cmd --reload
```

- c. 可以执行以下命令查看开启的所有端口。

```
firewall-cmd --list-ports
```

```
[root@ecs-centos7 ~]# firewall-cmd --list-ports
3000/tcp
```

6. 执行以下命令，运行项目。

```
node ~/test.js
```

7. 使用浏览器访问“http://弹性公网IP:3000”显示如下页面，说明Node.js测试项目部署成功。

图 4-16 部署测试



----结束

# 5 搭建网站

## 5.1 搭建 WordPress 网站

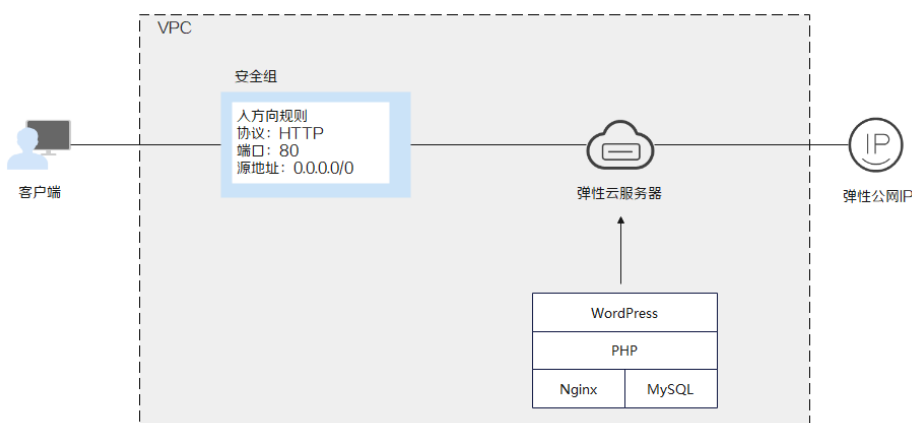
### 5.1.1 基于 WordPress 搭建个人网站（Linux）

#### 应用场景

WordPress简称WP，最初是一款博客系统，后逐步演化成一款免费的CMS（内容管理系统/建站系统）。本文主要介绍了如何使用CentOS 7.2 64位操作系统的Linux实例手工搭建LNMP平台，并部署WordPress环境。

#### 方案架构

图 5-1 基于 WordPress 搭建个人网站示意图（Linux）



#### 方案优势

- 快速构建站点，组网架构简单。
- 网站安全易用。

## 资源和成本规划

表 5-1 资源和成本规划

资源	资源说明	成本说明
虚拟私有云VPC	VPC网段：192.168.0.0/16	免费
虚拟私有云子网	<ul style="list-style-type: none"><li>可用区：可用区1</li><li>子网网段：192.168.0.0/24</li></ul>	免费
安全组	入方向规则： <ul style="list-style-type: none"><li>优先级：1</li><li>策略：允许</li><li>类型：IPv4</li><li>协议端口：TCP: 80</li><li>源地址：0.0.0.0/0</li></ul>	免费
弹性云服务器	<ul style="list-style-type: none"><li>计费模式：包年/包月</li><li>可用区：可用区1</li><li>规格：s6.large.4</li><li>镜像：CentOS 7.2 64bit</li><li>系统盘：40G</li><li>弹性公网IP：现在购买</li><li>线路：全动态BGP</li><li>公网带宽：按流量计费</li><li>带宽大小：5 Mbit/s</li></ul>	ECS涉及以下几项费用： <ul style="list-style-type: none"><li>云服务器</li><li>云硬盘</li><li>弹性公网IP</li></ul> 具体的计费方式及标准请参考 <a href="#">计费模式概述</a> 。
Nginx	是一个高性能的HTTP和反向代理web服务器。 获取方式： <a href="http://nginx.org/packages/centos/7/noarch/RPMS/nginx-release-centos-7-0.el7ngx.noarch.rpm">http://nginx.org/packages/centos/7/noarch/RPMS/nginx-release-centos-7-0.el7ngx.noarch.rpm</a>	免费
MySQL	是一款开源的关系数据库软件。 获取方式： <a href="https://dev.mysql.com/get/mysql80-community-release-el7-11.noarch.rpm">https://dev.mysql.com/get/mysql80-community-release-el7-11.noarch.rpm</a>	免费

资源	资源说明	成本说明
PHP	是一款开源软件，用于Web开发。 获取方式： <a href="https://mirrors.huaweicloud.com/remi/enterprise/remi-release-7.rpm">https://mirrors.huaweicloud.com/remi/enterprise/remi-release-7.rpm</a>	免费
WordPress	是一款开源的博客软件。 获取地址： <a href="https://wordpress.org/download/releases/">https://wordpress.org/download/releases/</a>	免费
域名	用于访问搭建的个人网站。	域名的价格以域名注册商所示为准，请参考域名注册商帮助文档。

## 基于 WordPress 搭建个人网站操作流程

Linux实例基于WordPress手动搭建个人网站的操作步骤如下：

1. [搭建LNMP环境。](#)
2. [创建数据库。](#)
3. [安装WordPress。](#)
4. [购买域名。](#)
5. [配置域名解析。](#)

## 实施步骤

### 安装前准备

- 已购买虚拟私有云和弹性公网IP。
- 如果规划为网站配置域名，需已经购买好相应的域名。
- 弹性云服务器所在安全组添加了如表5-2所示的安全组规则，具体步骤参见[为安全组添加安全组规则](#)。

表 5-2 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 80	0.0.0.0/0

- 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。

### 操作步骤

**步骤1** 登录弹性云服务器。

**步骤2** 搭建LNMP环境。具体操作请参见[手工搭建LNMP环境（CentOS 7.2）](#)。

**步骤3** 创建数据库。

1. 执行以下命令，并按照提示信息输入MySQL的root用户，登录到MySQL命令行。

```
mysql -u root -p
```

2. 执行以下命令，创建一个新的数据库。

```
CREATE DATABASE wordpress;
```

其中，“wordpress”为数据库名，可以自行设置。

3. 执行以下命令，创建一个新用户。

```
CREATE USER 'user'@'localhost' IDENTIFIED BY 'xxxx';
```

其中，“user”为用户名，'xxxx'为对应的账户密码，可以自行设置。

4. 执行以下命令，赋予用户对“wordpress”数据库的全部权限。

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

5. 执行以下命令，使所有配置生效。

```
FLUSH PRIVILEGES;
```

6. 执行以下命令，退出MySQL命令行。

```
exit
```

7. （可选）依次执行以下命令，验证数据库和用户是否已成功创建，并退出MySQL命令行。

```
mysql -u user -p
```

```
SHOW DATABASES;
```

```
exit
```

其中，“user”为刚刚创建的数据库用户名。

**步骤4** 安装WordPress。

1. 执行以下命令，进入Nginx网站根目录，下载WordPress压缩包。

```
cd /usr/share/nginx/html
```

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

2. 执行以下命令，解压缩WordPress软件包。

```
tar zxvf wordpress-6.6.1-zh_CN.tar.gz
```

解压后生成一个“wordpress”的文件夹。

3. 执行以下命令，进入WordPress安装目录，将wp-config-sample.php文件复制到wp-config.php文件中，并将原先的示例配置文件保留作为备份。

```
cd /usr/share/nginx/html/wordpress
```

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

4. 执行以下命令，打开并编辑新创建的配置文件。

```
vim wp-config.php
```

5. 按i键进入编辑模式。找到文件中MySQL的部分，并将相关配置信息修改为[步骤3](#)中的内容。





例如，配置的域名为“www.example.com”，配置成功后，可在浏览器地址栏中输入“http://www.example.com”访问部署的网站。

----结束

## 5.2 搭建 Discuz 论坛网站

### 5.2.1 方案概述

#### 应用场景

华为云可以为您提供丰富的解决方案，现以搭建网站业务为例介绍华为云的应用场景。

小型网站一般会部署在单台服务器上，用户对页面的访问，动静态内容的使用，数据库的使用和计算全部是在一台服务器上完成的。当网站业务发展到中型规模时，数据库的访问量剧增，单台服务器配置已不能满足业务要求，此时，可将数据库和网站程序分开部署在不同的服务器上分担性能压力。

本章节以搭建某论坛网站为例进行介绍，该论坛网站具体以下特点：

1. 数据节点与业务节点分开部署在不同的服务器上。
2. 可针对不同业务量动态调整服务器个数。
3. 可自动将流量分发到多台服务器。
4. 在Internet上可通过域名直接访问到该网站。

#### 方案架构

针对网站的特点，使用华为云搭建论坛网站采用表5-4所示方案。

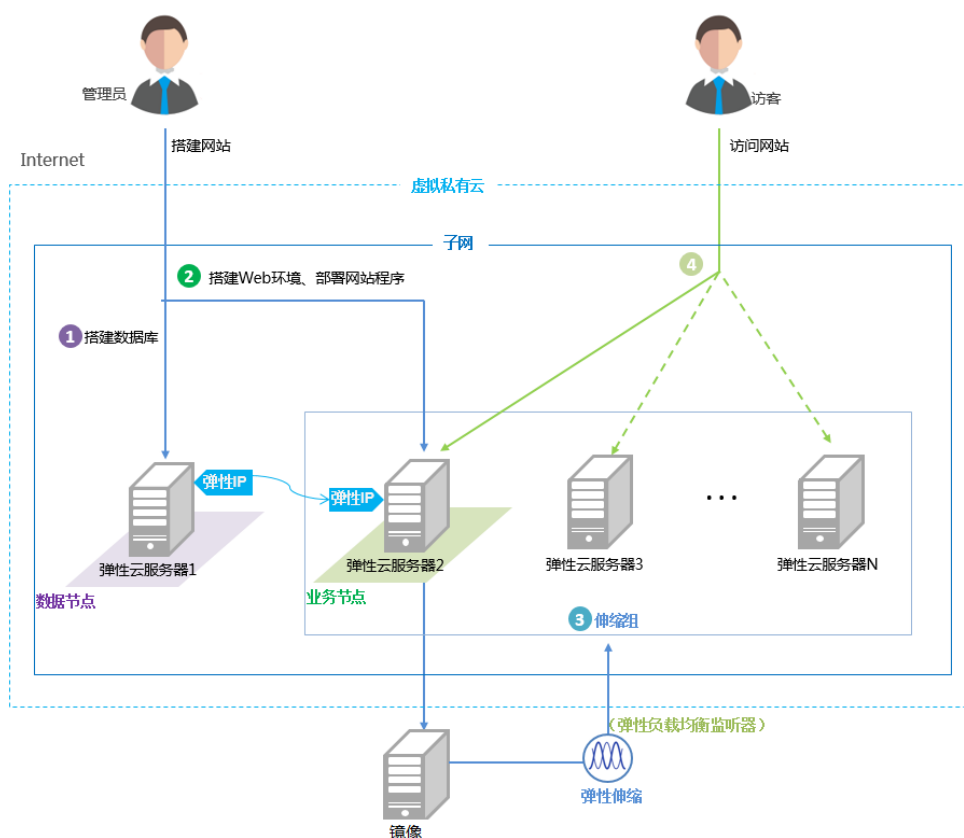
表 5-4 建站方案及所需服务

需求	华为云方案	涉及服务
数据节点与业务节点分开部署在不同的服务器上	<ol style="list-style-type: none"><li>1. 购买两台弹性云服务器代替传统服务器，分别作为网站的数据节点和基础业务节点。</li><li>2. 由虚拟私有云为弹性云服务器提供网络资源。</li><li>3. 购买服务器过程中，用户可以根据实际部署方案的要求，选择是否为云服务器挂载云硬盘作为数据盘。</li></ol>	弹性云服务器 虚拟私有云 云硬盘(可选)

需求	华为云方案	涉及服务
针对不同业务量动态调整服务器个数	根据业务需求和策略采用弹性伸缩，使用基础业务节点的镜像动态地调整作为业务节点的弹性云服务器实例个数，保证业务平稳健康运行。	弹性伸缩
自动将流量分发到多台服务器	使用负载均衡将访问流量自动分发到多台业务节点弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。	弹性负载均衡
在Internet上可通过域名直接访问到该网站	1. 通过第三方域名注册商为该网站注册域名 2. 为域名配置解析记录。	云解析服务

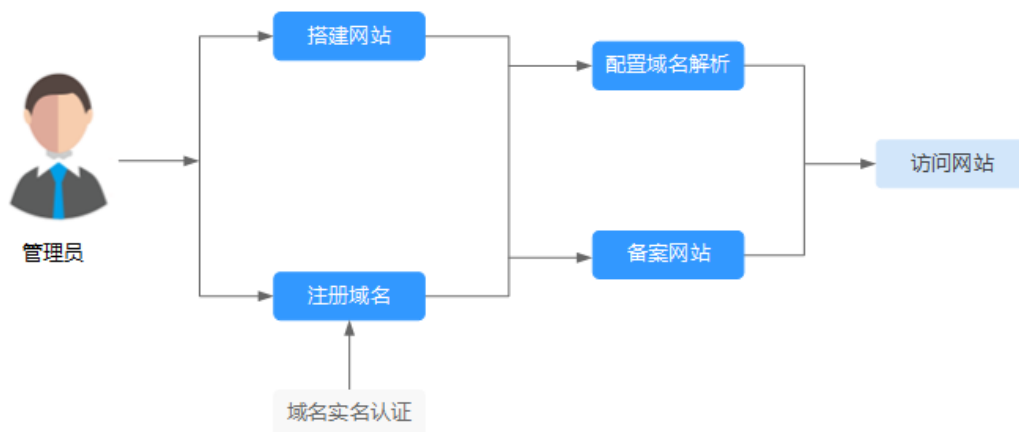
论坛网站的逻辑架构如图5-3所示。

图 5-3 论坛网站逻辑架构



1. 为弹性云服务器1绑定弹性公网IP，搭建数据库。
2. 先解绑弹性云服务器1上的弹性公网IP，再将弹性公网IP绑定至弹性云服务器2上，搭建Web环境并部署网站程序。
3. 弹性伸缩可以根据业务量的变化，通过弹性云服务器2的镜像生成弹性伸缩组中的弹性云服务器。弹性伸缩组使用弹性负载均衡监听器。
4. 可以通过弹性负载均衡服务的公网IP访问网站。弹性负载均衡服务将访问流量自动分发到多台弹性云服务器。

### 域名配置及备案

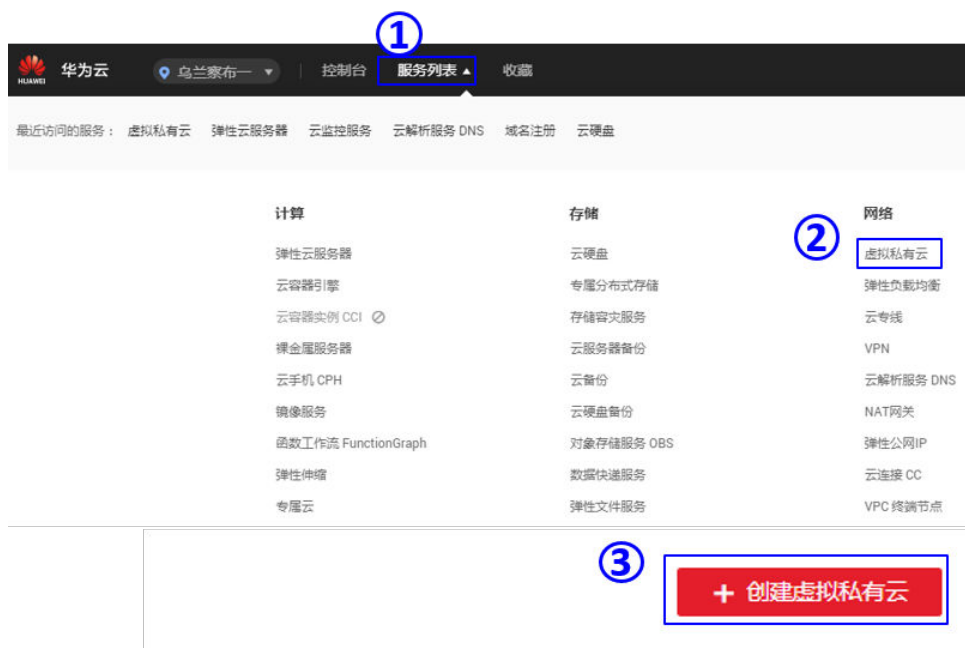


对购买的域名进行解析及备案后，网站访客可以通过域名直接访问网站。

## 5.2.2 购买服务

### 创建虚拟私有云

1. 选择“网络 > 虚拟私有云”，单击“创建虚拟私有云”。



2. 设置相关参数并完成创建。

### 创建虚拟私有云

基本信息

\* 区域: [下拉菜单]

4 \* 名称: VPC-DISCUZ 填写虚拟私有云的名称

\* 网段: 192.168.0.0 / 16

\* 企业项目: [下拉菜单] 未开通企业管理的用户页面无此参数，无需进行配置

标签: [输入框] [输入框]

子网配置

默认子网

5 \* 可用区: [可用区2] [可用区3] [可用区1] [可用区4] 选择可用区

6 \* 名称: vpc-test 填写虚拟私有云子网名称

\* 子网网段: 192.168.0.0 / 24

高级配置: [默认配置] [自定义配置]

+ 添加子网 一次最多可以添加3个子网。

7 立即创建

## 申请弹性公网 IP

### 弹性公网 IP

网络控制台

弹性公网 IP

您还可以购买44个弹性公网IP。

弹性公网IP	状态	类型	带宽	带宽计费	已绑定实例	计费模式	企业项目	操作
[图标]	绑定	全动态BGP	ecc-cloudtable-demo-bandwidth-52b7	按带宽计费 1 Mbit/s	[图标]	[图标]	[图标]	绑定 解除 更多
[图标]	绑定	全动态BGP	no_del_baseline_ansible_test-0001-b...	按流量计费 5 Mbit/s	[图标]	[图标]	[图标]	绑定 解除 更多
[图标]	绑定	全动态BGP	no_del_baseline_ansible_test-0002-b...	按流量计费 5 Mbit/s	[图标]	[图标]	[图标]	绑定 解除 更多

2 立即创建

**3** 选择计费方式：包年包月

包年包月购买华为云服务器及IP资源，可申请备案授权码，按需资源不支持备案和生成备案授权码。

**4**

未开通企业管理的用户页面无此参数，无需进行配置

**5** 立即购买

**6** 去支付

**7** 确认付款

## 创建安全组并添加规则

**1** 安全组

**2** + 创建安全组

**3** 名称 SG-DISCUZ

**4** 确定

未开通企业管理的用户页面无此参数，无需进行配置



### 说明

安全组下默认的规则不能被删除，否则将导致两个服务器彼此通信异常。

## 购买弹性云服务器

1. 选择“计算 > 弹性云服务器”，单击“购买弹性云服务器”。



2. 设置弹性云服务器参数，提交申请。

④ 计费模式  包年/包月  按需计费

⑤ 区域

⑥ 可用区  可用区3  可用区2  可用区1  可用区4

⑦ 规格

最新系列 vCPUs 1vCPUs 内存 4GB 请输入规格名称

规格名称	vCPUs   内存	CPU	基准 / 最大带宽	内网收发包
<input type="radio"/> s2.medium.4	1vCPUs   4GB	Intel E5-2680V4 2.4GHz	0.1/0.5 Gbit/s	50,000
<input checked="" type="radio"/> s3.medium.4	1vCPUs   4GB	Intel SkyLake 6161 2.2GHz	0.1/0.5 Gbit/s	50,000

当前规格 通用计算型 | s3.medium.4 | 1vCPUs | 4GB

⑧ 镜像  公共镜像  私有镜像  共享镜像  市场镜像

CentOS CentOS

⑨ 磁盘 云硬盘

系统盘 普通IO 40 GB IOPS上限580, IOPS突发上限2,200

数据盘 普通IO 500 GB IOPS上限1,500, IOPS突发上限2,200 删除

SCSI  共享盘  加密

+ 增加一块数据盘 您还可以挂载 22 块磁盘 (云硬盘)

云服务器备份  启用自动备份 推荐 购买备份套餐包, 享更多优惠。如已购买, 请在我的套餐里查看。  
数据保护已关闭。

⑩ 虚拟私有云 VPC-DISCUZ 新建虚拟私有云

网卡 主网卡 vpc-test(192.168.0.0/24) 自动分配IP地址 查看已使用IP地址

+ 增加一块网卡 您还可以增加 11 块网卡

⑪ 安全组 如何配置安全组?

SG-DISCUZ (入方向:TCP/3389, 22, 80... 新建安全组

入方向: TCP/3389, 22, 80 | 出方向: -

弹性公网IP 如有互联网访问需求, 请先规划您的弹性公网IP资源。单击[这里](#)查看弹性公网IP。

⑫ 现在购买 使用已有 暂不购买

为云服务器分配已有弹性公网IP, 不能批量创建云服务器。

当前弹性公网IP 规格: 全动态BGP 带宽: 1 Mbit/s 计费模式: 按带宽计费





### 说明

购买时请按照参数样例购买两台弹性云服务器。在购买第二台ECS时，注意参数配置有所不同：

- “计费模式”选择“包年包月”。  
包年包月购买华为云服务器及IP资源，可申请备案授权码，按需资源不支持备案和生成备案授权码。
- “弹性公网IP”选择“暂不购买”。

## 购买域名

若您已有域名可跳过此步骤。

- 选择“域名与网站 > 域名注册”，导航栏选择“信息模板”后单击“创建信息模板”。





## 2. 填写基本信息及身份认证信息。

## 3. 选择“域名列表”，并单击“注册域名”，根据页面提示完成域名购买。

**域名列表**

9 [注册域名](#)

1. 域名属于即时产品，具有唯一性，注册时请尽快结算。注册成功后不支持退款。  
 2. 根据工信部规定，2018年1月1日起，无资质批复的域名后缀，将无法实名认证和备案。例如，.org/.name后缀的域名暂无法进行网站备案，.xyz后缀的域名暂无法在北京地区进行网站备案。个人备案时如果您未满18周岁，部分管局可能会审核不通过。建议先注册域名以保护您的品牌。查看[域名备案审核规范](#)  
 3. .com/.net/.cn/.xyz/.club/.wang/.mobi/.info/.中国/.在线/.中文网等域名注册成功后必须进行实名认证，否则将无法正常解析和访问。查看[实名认证指南](#)  
 4. 注册域名中不得含有敏感词，如 av/fuck 等，否则可能被注册局保留、无法审核通过或限制注册。域名是否注册成功请以注册查询结果为准。

**域名注册** < 返回域名列表

10 单个查询 多个查询

discuztest [查询](#)

域名清单 (1) [清空](#)

discuztest.com [立即购买](#)

11 [加入清单](#)

**域名注册** < 返回域名列表

1 服务选型 2 订单确认 3 支付

**公告提醒**

1. 域名属于即时产品，具有唯一性，注册时请尽快结算。注册成功后不支持退款。  
 2. 根据工信部规定，2018年1月1日起，无资质批复的域名后缀，将无法实名认证和备案。例如，.org/.name后缀的域名暂无法进行网站备案，.xyz后缀的域名暂无法在北京地区进行网站备案。个人备案时如果您未满18周岁，部分管局可能会审核不通过。建议先注册域名以保护您的品牌。查看[域名备案审核规范](#)  
 3. .com/.net/.cn/.xyz/.club/.wang/.mobi/.info/.中国/.在线/.中文网等域名注册成功后必须进行实名认证，否则将无法正常解析和访问。查看[实名认证指南](#)  
 4. 注册域名中不得含有敏感词，如 av/fuck 等，否则可能被注册局保留、无法审核通过或限制注册。域名是否注册成功请以注册查询结果为准。  
 5. 域名产品只能使用指定域名类优惠券进行结算，华为云体验代金券不适用于本产品。

**注册域名**

设置购买年限

域名	类型	购买年限	费用	操作
discuztest.com	新购	1年 2年 3年 4年 5年 6年 7年 8年 9年 10年	¥55	删除

**域名信息**

14 以下为您使用过的域名信息模板，您可以直接使用：

域名所有者	用户类型	认证状态
个人用户	个人用户	实名认证审核中

15 [立即购买](#)

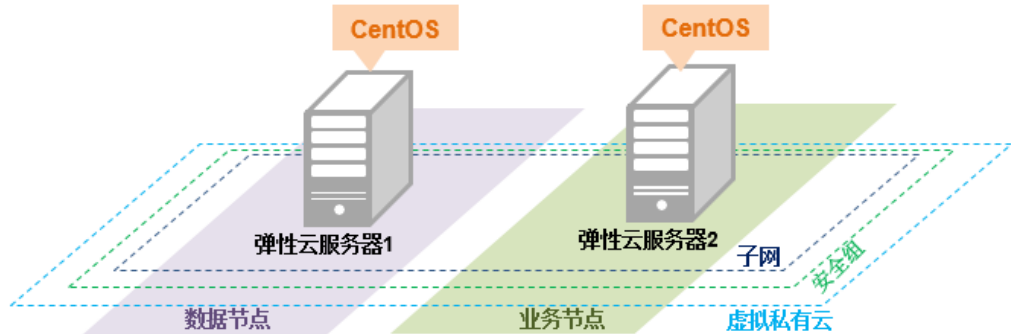
16 我已阅读并同意 [《华为云服务协议》](#)

17 [去支付](#)

18 应付金额：¥55.00  
 余额支付：¥55.00  
[确认付款](#)

## 5.2.3 搭建网站

### 已有服务



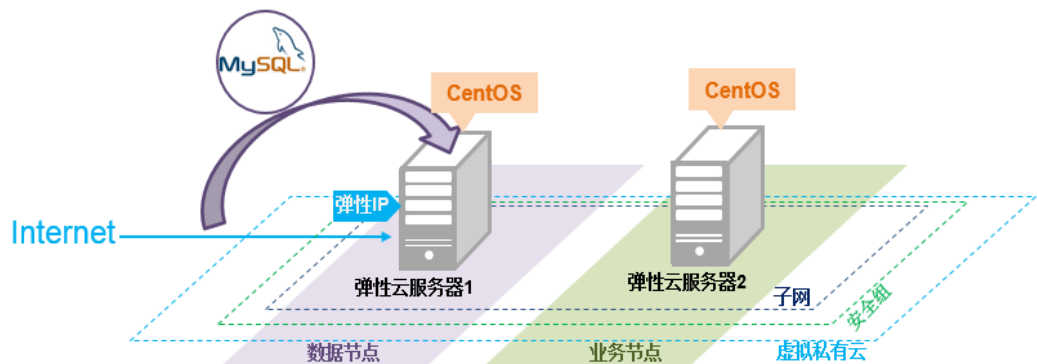
服务参数样例

服务名称	用途	配置参数
虚拟私有云	可以通过公网IP，将虚拟私有云连接到公网上。	名称：VPC_DISCUZ VPC网段：192.168.0.0/16 可用分区：可用分区1 子网名称：vpc-test 子网网段：192.168.0.0/24 弹性IP： 安全组：SG-DISCUZ
弹性云服务器1	作为数据节点，搭建数据库。	名称：discuz01 vCPU：1核 内存：4G 镜像：CentOS 系统盘：40G 数据盘：500G 虚拟私有云：VPC_DISCUZ 安全组：SG-DISCUZ 用户名： 密码： 私有IP:192.168.0.26
弹性云服务器2	作为业务节点，搭建Web环境以及部署网站代码。	名称：discuz02 vCPU：1核 内存：4G 镜像：CentOS 系统盘：40G 数据盘：100G 虚拟私有云：VPC_DISCUZ 安全组：SG-DISCUZ 用户名： 密码： 私有IP:192.168.0.146

### 搭建流程



### 搭建数据库



## 安装MySQL

本文档以CentOS 7.2操作系统为例安装MySQL。

1. 远程登录云服务器discuz01，填写用户名和密码。
2. 依次执行以下命令，安装MySQL。

```
wget -i -c https://dev.mysql.com/get/mysql80-community-release-  
el7-11.noarch.rpm  
yum -y install mysql80-community-release-el7-11.noarch.rpm  
yum -y install mysql-community-server --nogpgcheck
```

## 配置MySQL

1. 执行以下命令，启动MySQL服务。

```
systemctl start mysqld  
systemctl enable mysqld
```

2. 查看MySQL运行状态。

```
systemctl status mysqld.service
```

回显信息如下所示：

```
# 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. 执行以下命令，获取安装MySQL时自动设置的root用户密码。

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

回显如下类似信息。

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

4. 执行以下命令，并按照回显提示信息进行操作，加固MySQL。

```
mysql_secure_installation
```

Securing the MySQL server deployment.

```
Enter password for user root: #输入上一步骤中获取的安装MySQL时自动设置的root用户密码  
The existing password for the user account root has expired. Please set a new password.
```

```
New password: #设置新的root用户密码
```

```
Re-enter new password: #再次输入密码  
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 #是否更改root用户密  
码，输入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 #是否删除匿名用户, 输入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 #禁止root远程登录, 输入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 #是否删除test库
和对它的访问权限, 输入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 #是否重新加载授权表, 输入
Y
Success.

All done!
```

5. 执行以下命令，再根据提示输入数据库管理员root账号的密码进入数据库。

```
mysql -u root -p
```

6. 执行以下命令，使用MySQL数据库。

```
use mysql;
```

7. 执行以下命令，查看用户列表。

```
select host,user from user;
```

#### 说明

此命令及以下数据库语句均以分号结尾，请勿忽略。

8. 执行以下命令，刷新用户列表并允许所有IP对数据库进行访问。

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

9. 执行以下命令，强制刷新权限。允许同一子网中设置为允许访问的云服务器通过私有IP对MySQL数据库进行访问。

```
flush privileges;
```

10. 执行以下命令，退出数据库。

```
quit
```

11. 执行以下命令，重启MySQL服务。

```
systemctl restart mysqld
```

12. 执行以下命令，设置开机自动启动MySQL服务。

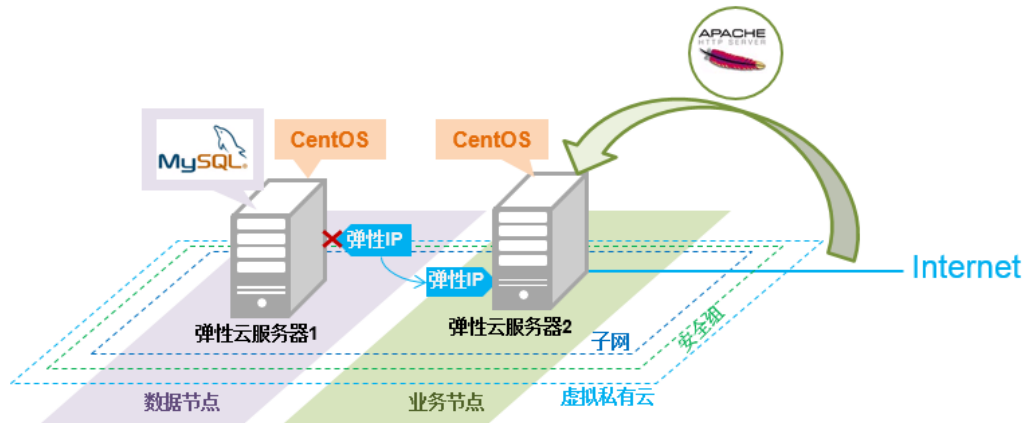
```
systemctl enable mysqld
```

13. 执行以下命令，关闭防火墙。

```
systemctl stop firewalld.service
```

- 重新查看防火墙状态是否为关闭。  
`systemctl status firewalld`

## 搭建 Web 环境



## 安装Web环境

- 将弹性公网IP从云服务器discuz01上解绑，并绑定至云服务器discuz02上。

弹性云服务器控制台

您还可以创建7,949台云服务器，使用658核vCPU和13,514GB内存。 [了解配置详情](#)

名称/ID	可用区	状态	规格/镜像	IP地址	计费模式	企业项目	操作
discuz02 aa1952d-5e3b-4e9-b38...	可用区1	运行中	1vCPU   4GB   s3 medium 4 CentOS	192.168.0.146 (私有)	包年/包月	资料	远程登录 更多
discuz01 449c87c8-fde5-4f1a-be2f...	可用区1	运行中	1vCPU   4GB   s3 medium 4 CentOS	(弹性公网) 1 Mbit/s 192.168.0.26 (私有)	按需计费	资料	远程登录 更多

单击弹性云服务器名称“discuz01”，进入服务器详细参数页面

弹性公网IP ③

绑定弹性公网IP 查看弹性公网IP

解绑 ④

解绑弹性公网IP

确定要解绑该弹性公网IP？

是 否 ⑤

单击弹性云服务器名称“discuz02”，进入服务器详细参数页面

名称/ID	可用区	状态	规格/镜像	IP地址	计费模式	企业项目	操作
discuz02 aa1952d-5e3b-4...	可用区1	远...	1vCPU   4GB   s3... CentOS	192.168.0.146 (私有)	包年/包...	资料	远程登录 更多
discuz01 449c87c8-fde5-4f...	可用区1	远...	1vCPU   4GB   s3... CentOS	(弹性公...) 1 Mbit/s 192.168.0.26 (私有)	按需计...	资料	远程登录 更多



2. 远程登录云服务器discuz02，填写用户名和密码。

3. 依次执行以下命令，安装MySQL。

```
wget -i -c https://dev.mysql.com/get/mysql80-community-release-el7-11.noarch.rpm
```

```
yum -y install mysql80-community-release-el7-11.noarch.rpm
```

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

4. 执行以下命令，安装Apache服务器。

```
yum -y install httpd httpd-manual mod_ssl mod_perl
```

5. 依次执行以下命令，安装EPEL源、Remi仓库，并启用PHP 8.0仓库。

```
yum -y install epel-release
```

```
yum -y install https://rpms.remirepo.net/enterprise/remi-release-7.rpm
```

```
yum -y install yum-utils
```

```
yum-config-manager --enable remi-php80
```

6. 执行以下命令，安装PHP。

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

7. 执行以下命令，验证PHP的安装版本。

```
php -v
```

回显如下类似信息：

```
PHP 8.0.30 (cli) (built: Jun 4 2024 15:19:49) ( NTS gcc x86_64 )  
Copyright (c) The PHP Group  
Zend Engine v4.0.30, Copyright (c) Zend Technologies
```

### 配置Web环境

1. 执行以下命令，启动httpd服务。

```
service httpd start
```

2. 执行以下命令，设置开机自动启动httpd服务。

```
chkconfig httpd on
```

3. 执行以下命令，启动php-fpm服务。

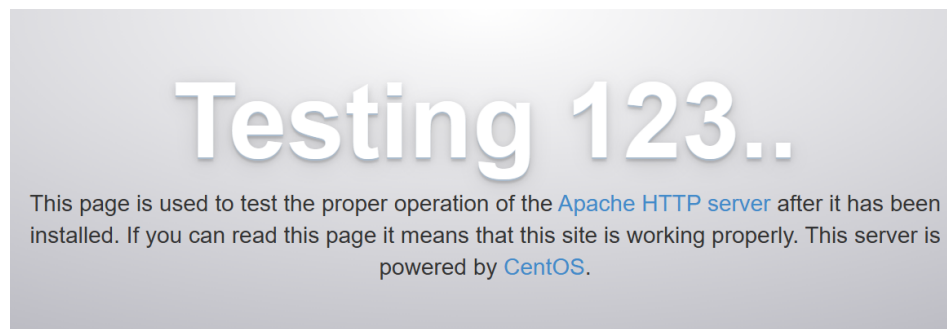
```
service php-fpm start
```

4. 执行以下命令，设置开机自动启动php-fpm服务。

```
chkconfig php-fpm on
```



5. 执行以下命令，关闭防火墙。  
**systemctl stop firewalld.service**
6. 执行以下命令，重新查看防火墙状态是否为关闭。  
**systemctl status firewalld**
7. 执行以下命令，启动MySQL服务。  
**systemctl start mysqld**
8. 执行以下命令，设置开机自动启动MySQL服务。  
**systemctl enable mysqld.service**
9. 在浏览器中输入<http://弹性公网IP地址>，即可访问服务器的默认主页。



#### Just visiting?

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting [www.example.com](http://www.example.com), you should send e-mail to "webmaster@example.com".

#### Are you the Administrator?

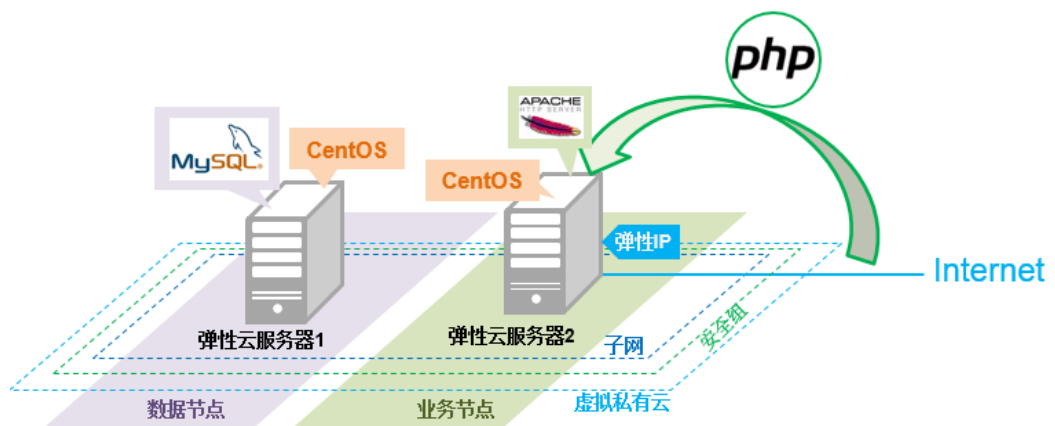
You should add your website content to the directory `/var/www/html/`. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

#### Promoting Apache and CentOS

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



## 部署网站代码



1. 远程登录云服务器discuz02，执行以下命令，安装Discuz软件。  
**wget https://gitee.com/Discuz/DiscuzX/releases/download/v3.5-20231001/Discuz\_X3.5\_SC\_UTF8\_20231001.zip**

### 📖 说明

- 以上软件来自第三方网站，仅作参考。建议自行获取需要的版本软件，以应对不同需求。
  - 上述软件仅为搭建网站指导示例，若搭建的网站做商业用途请自行准备所需软件。
2. 执行以下命令，解压Discuz安装包。  
**unzip Discuz\_X3.5\_SC\_UTF8\_20231001.zip**
  3. 执行以下命令，将解压后的“upload”文件夹下的所有文件复制到“var/www/html”路径下。  
**cp -r upload/\* /var/www/html**
  4. 执行以下命令，将写权限赋予给其他用户。  
**chmod -R 777 /var/www/html**
  5. 在浏览器里输入地址：**http://弹性公网IP地址**进入安装界面，按照Discuz安装向导进行安装。
    - a. 阅读授权协议后，单击“同意”。



- b. 开始安装后，检查安装环境并单击“下一步”。



- c. 设置运行环境，并单击“下一步”。  
本文以选择“全新安装 Discuz! X 与 UCenter Server”为例。



- d. 安装数据库，填写数据库信息，单击“下一步”完成安装。

### Discuz! 安装向导

Discuz! X3.5 简体中文 UTF8 版 Release 20231001

## 3 安装数据库

正在执行数据库安装

检查安装环境    设置运行环境    创建数据库    安装

#### 填写数据库信息

数据库服务器地址:   
一般为 127.0.0.1 或 localhost

数据库名:   
用于安装 Discuz! 的数据库

数据库用户名:   
您的数据库用户名

数据库密码:   
您的数据库密码

数据表前缀:   
同一数据库运行多个论坛时, 请修改前缀

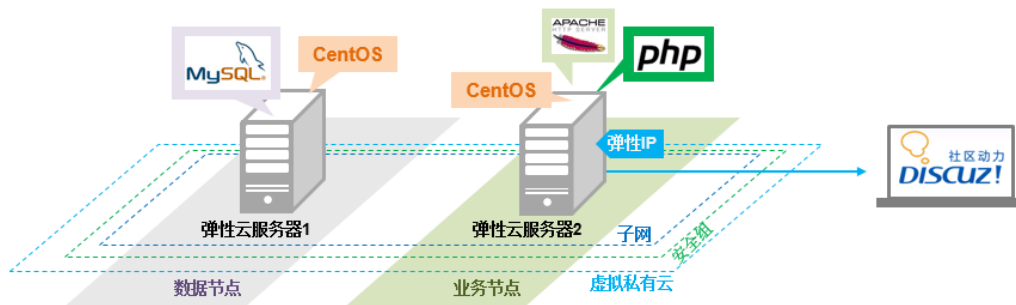
系统信箱 Email:   
用于发送程序错误报告

- 数据库服务器地址即为discuz01的私有IP地址。
  - 数据库密码是discuz01配置的数据库管理员root账号的密码。
  - 自定义管理员信息。
- e. 安装完成后, 单击“直接访问站点”, 即可访问论坛。



## 验证搭建结果

在浏览器中输入：<http://弹性公网IP地址/forum.php> 可登录论坛主页则说明网站搭建成功。



## 5.2.4 配置特性

### 释放弹性公网 IP

用户所能使用的弹性公网IP数目默认为一个，如果需要扩大弹性公网IP的配额则需要另外申请。使用负载均衡功能时，系统会自动分配一个公网IP，该公网IP属于弹性公网IP。为了避免出现弹性公网IP配额不足的情况，建议先释放弹性公网IP再申请弹性负载均衡服务。



### 说明

配置特性时，未开通企业管理的用户页面无“企业项目”参数项，无需进行配置。如需开通企业项目，请参考[如何开通企业项目/企业多账号](#)。

## 创建弹性负载均衡

1. 选择“网络 > 弹性负载均衡”，单击“创建负载均衡”。



2. 设置负载均衡器参数，提交申请。



## 配置弹性负载均衡





## 制作镜像

1. 选择“计算 > 弹性云服务器”，关闭运行中的弹性云服务器。





### 关机



确定要对以下云服务器进行关机操作吗？

1. 按需/竞价计费实例关机后，基础资源（vCPU、内存、镜像）不再计费，绑定的云硬盘（包括系统盘、数据盘）、弹性公网IP、带宽等资源按各自产品的计费方法（“包年/包月”或“按需计费”）进行收费。云服务器再次开机时，可能由于后台基础资源不足无法正常开机。请耐心等待，稍后重试。
2. 包含本地盘（如磁盘增强型、GPU加速型等）和包含FPGA卡的按需/竞价计费实例，关机后仍然计费。如需停止计费，请删除实例。

名称	状态	备注
discuz02	运行中	--

强制关机

强制关机会导致云服务器中未保存的数据丢失，请谨慎操作。

5

是 否

## 2. 制作镜像，设置镜像参数，提交申请。

名称/ID	可用区	状态	规格/镜像	IP地址	计费模式	企业项目	操作
discuz02 aea1952d-5e3b-4e8...	可用区1	关机	1vCPUs   4GB   s3.m... CentOS	192.168.0.146 (私有)	包年/包月 31天后...	资料	远程登录 更多
discuz01 449c87c8-fde5-4f1a...	可用区1	运...	1vCPUs   4GB   s3.m... CentOS	192.168.0.26 (私有)	按需计费	资料	变更规格 创建镜像 重置密码

创建私有镜像 [返回镜像列表](#)

**目前镜像服务已进入商业化阶段，私有镜像会收取一定的存储费用。详细计费标准可参考[镜像的计费标准](#)**

镜像类型和来源

\* 区域 华东-上海二  
不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。

\* 创建方式 系统盘镜像 整机镜像 数据盘镜像

\* 选择镜像源 云服务器 裸金属服务器 镜像文件

获取弹性云服务器最新状态，请手动刷新。 所有状态 名称

名称	操作系统	运行状态	私有IP地址	创建时间
<input type="checkbox"/> discuz02	CentOS	<input checked="" type="radio"/> 关机	192.168.0.146	2019/05/29 10:...

当前选择: discuz02 | 操作系统: -- | 系统盘: --  
[购买弹性云服务器](#)

配置信息

加密 未加密 8

\* 名称

\* 企业项目

标签    
您还可以添加10个标签。

描述

9

我已经阅读并同意《[镜像制作承诺书](#)》和《[华为镜像免责声明](#)》 10

## 配置弹性伸缩

1. 选择“计算 > 弹性伸缩”，创建弹性伸缩组及伸缩配置。



\*实例移除策略

弹性公网IP

若选择“释放”，在伸缩组进行缩的活动时，则会将云服务器上的弹性公网IP释放，否则仅做解绑定操作，保留弹性公网IP资源。

\*健康检查方式

\*健康检查间隔

\*健康状况检查宽限期(秒)

\*企业项目

高级配置

在高级配置中可对通知和标签进行配置。

- 先移除创建和配置时间较早的实例。
- 健康检查按照所选负载均衡服务中的负载均衡监听器配置信息完成。
- 每5分钟对云服务器进行一次弹性负载均衡健康检查。
- 未开通企业管理的用户页面无此参数，无需进行配置。

弹性伸缩本身不收取费用。但会按伸缩组内的实例收取云服务器和弹性公网IP的费用。

8

伸缩配置

\*计费模式

9

\*配置模板 您可以使用已有的弹性云服务器快速创建相同规格的伸缩配置，但需要注意此时伸缩配置中镜像、磁盘均为原始状态。

10

\*规格

规格名称	vCPUs   内存	CPU	基准 / 最大带宽	内网收发包
<input type="checkbox"/> s2.medium.4 (可用区3, 可...	1vCPUs   4GB	Intel E5...	0.1/0.5 Gbit/s	50,000
<input checked="" type="checkbox"/> s3.medium.4	1vCPUs   4GB	Intel Sky...	0.1/0.5 Gbit/s	50,000
<input type="checkbox"/> s6.medium.4 (可用区2, 可...	1vCPUs   4GB	Intel Cas...	0.1/0.8 Gbit/s	100,000
<input type="checkbox"/> sn3.medium.4 (可用区2, ...	1vCPUs   4GB	Intel Sky...	0.2/0.8 Gbit/s	100,000

已选规格: 优先使用当前选中的规格进行伸缩, 您可以点击已选规格查看规格信息。您还可以选择9个规格。

通用计算型 | s3.medium.4 | 1vCPUs | 4GB

11

\*镜像

选择使用已制作的私有镜像



## 2. 为弹性伸缩组配置策略。





### 3. 增加伸缩实例。



### 4. 修改伸缩组。



### 修改伸缩组

● 伸缩组为非启用状态、实例数为0且没有正在进行的伸缩活动时，可以修改伸缩组的可用区和子网。

\*名称

\*最大实例数(台)

⑤ 期望实例数(台)

\*最小实例数(台)

\*冷却时间(秒)

负载均衡  不使用  使用经典型  使用增强型 [新建负载均衡](#)

负载均衡器  后端云服务器组

⑥

将“最小实例数”设置为1，可以保证弹性云服务器discuz02不从伸缩组内移除。

### 验证配置结果

1. 获取负载均衡服务的弹性公网IP地址。





2. 在浏览器中输入 `http://弹性公网IP地址/forum.php` 可以访问网站则说明网站的特性配置成功。

### 说明

若无法访问网站，请在弹性伸缩组“as-group-discuz”详情页的“伸缩实例”中检查是否包含“discuz02”实例，若没有请参照3进行添加。

## 5.2.5 访问网站

### 域名解析

1. 选择“域名与网站 > 域名注册”。



2. 在域名右侧操作列单击“解析”。





## 3. 单击域名进入域名详情页后，单击“添加记录集”。



## 4. 添加记录集。



## 网站备案

根据国家规定，如果客户网站所使用的服务器是在中国大陆，就需要进行ICP备案，没有备案的域名不能访问网站。

备案受理前置条件如下：

- 有正规注册的域名。
- 确认IP地址为华为公司所属。
- 公司属于非经营性网站性质。

## 访问方法

访客可以在Internet上通过已备案的域名访问网站。



## 5.3 搭建 Magento 电子商务网站

### 5.3.1 手工搭建 Magento 电子商务网站（Linux）

#### 简介

本文主要介绍了如何使用弹性云服务器的Linux实例手工搭建Magento电子商务系统。Magento是一款开源电子商务系统，设计灵活，具有模块化架构体系和丰富的功能，可为大中型站点提供解决方案。Magento采用PHP开发，数据存储使用MySQL。

#### 前提条件

- 已购买一台弹性云服务器，且已为其绑定弹性公网IP。
- 弹性云服务器所在安全组添加了如下表所示的安全组规则，具体步骤参见[为安全组添加安全组规则](#)。

表 5-5 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 22	允许SSH远程连接Linux弹性云服务器的客户端IP地址。如允许所有IP访问，请设置为0.0.0.0/0，出于安全考虑，不建议您设置为允许所有IP访问。
入方向	1	允许	IPv4	TCP: 80	允许访问Magento网站的客户端IP地址。如允许所有IP访问，请设置为0.0.0.0/0。
入方向	1	允许	IPv4	TCP : 3306	允许远程访问MySQL数据库的客户端IP地址。如允许所有IP访问，请设置为0.0.0.0/0，出于安全考虑，不建议您设置为允许所有IP访问。

#### 资源规划

本次实践所用的资源配置及软件版本如[表5-6](#)中所示。当您使用不同的硬件规格或软件版本时，本指导中的命令及参数可能会发生改变，需要您根据实际情况进行调整。

表 5-6 资源规划

资源	类别	规格/版本
ECS配置	实例规格	c6s.large.2
	vCPUs	2vCPUs
	内存	4GiB
	操作系统	CentOS 7.2
软件资源	Apache	2.4.6
	MySQL	5.7 获取方式： <a href="http://dev.mysql.com/get/mysql57-community-release-el7-8.noarch.rpm">http://dev.mysql.com/get/mysql57-community-release-el7-8.noarch.rpm</a>
	PHP	7.0.33 获取方式： <a href="https://mirror.webtatic.com/yum/el7/webtatic-release.rpm">https://mirror.webtatic.com/yum/el7/webtatic-release.rpm</a>
	Composer	1.10.19 获取方式： <a href="https://getcomposer.org/installer">https://getcomposer.org/installer</a>
	Magento	2.1.0 获取方式： <a href="https://github.com/magento/magento2.git">https://github.com/magento/magento2.git</a>

### 📖 说明

为保证所搭建网站正常运行，所选的ECS实例规格建议为2GiB及以上。

## 步骤一：安装配置 Apache

**步骤1** 远程登录弹性云服务器，操作方法请参考[登录Linux弹性云服务器](#)。

**步骤2** 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。

**步骤3** 使用root用户执行以下命令更新软件包，并安装Apache。

```
yum -y update
yum -y install httpd
```

### 📖 说明

如果执行命令过程中报错，提示无法解析域名时，可以在“/etc/resolv.conf”配置文件中增加一个DNS服务器。

#### 步骤4 打开Apache配置文件。

```
vim /etc/httpd/conf/httpd.conf
```

### 📖 说明

如果没有安装vim，可使用`yum install -y vim*`命令进行安装。

#### 步骤5 按i键进入编辑模式，修改如下两处内容：

- 将下图所示位置的配置参数“AllowOverride None”改为“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
```

- 在配置文件末新增一行配置参数：  
`LoadModule rewrite_module modules/mod_rewrite.so`

如下图所示：

```
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
LoadModule rewrite_module modules/mod_rewrite.so
```

#### 步骤6 按Esc键退出编辑模式，并输入:wq保存后退出。

#### 步骤7 依次执行以下命令，启动Apache服务并设置开机自启动。

```
systemctl start httpd
systemctl enable httpd
```

----结束

## 步骤二：安装配置 MySQL

#### 步骤1 使用root用户执行以下命令添加yum源。

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

#### 步骤2 安装MySQL。

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

#### 步骤3 依次执行以下命令，启动MySQL服务并设置开机自启动。

```
systemctl start mysqld
systemctl enable mysqld
```

#### 步骤4 执行以下命令，获取安装MySQL时自动设置的root用户密码。

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

回显如下类似信息，其中“(n?K7jP#cirM)”即为临时密码。

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

**步骤5** 执行以下命令加固MySQL。

```
mysql_secure_installation
```

按照回显提示信息进行操作，具体操作如粗体所示：

```
Securing the MySQL server deployment.
```

```
Enter password for user root: #输入上一步骤中获取的安装MySQL时自动设置的root用户密码  
The existing password for the user account root has expired. Please set a new password.
```

```
New password: #设置root用户密码
```

```
Re-enter new password: #再次输入密码  
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 #是否更改root用户密码，输入Y
```

```
New password: #输入密码，长度为8至30个字符，须同时包含大小写英文字母、数字和特殊符号。特殊符号可以是() `~!@#$%^&*~+=|{}[]; ' <> , . ? /
```

```
Re-enter new password: #再次输入密码
```

```
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 #输入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 #是否删除匿名用户，输入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 #禁止root远程登录，输入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 #是否删除test库和对它的访问权限，输入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 #是否重新加载授权表，输入Y  
Success.
```

```
All done!
```

**步骤6** 以root用户登录MySQL数据库。

```
mysql -u root -p
```

**步骤7** 创建一个新的数据库，其中“magento”为自定义的数据库名称。

```
CREATE DATABASE magento;
```

**步骤8** 执行以下命令，为数据库创建用户并为用户分配数据库的完全访问权限。

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

其中，“magento”为上一步骤中创建的数据库名，“magentouser”为新建的数据库用户名，“xxxxx”为对应的账户密码，可以自行设置。

**步骤9** 执行以下命令，退出MySQL命令行。

```
exit
```

**步骤10** （可选）依次执行以下步骤，验证数据库和用户是否已成功创建，并退出MySQL命令行。

1. 以新建的数据库用户“magentouser”登录MySQL命令行。

```
mysql -u magentouser -p
```

2. 查看数据库。

```
SHOW DATABASES;
```

回显如下，“magento”即为新建的数据库，说明数据库已成功创建。

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

3. 执行以下命令，退出MySQL命令行。

```
exit
```

----结束

## 步骤三：安装配置 PHP

**步骤1** 添加ius源和epel源。

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

**步骤2** 添加Webtatic源。

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

**步骤3** 安装PHP7和用于Magento安装的一些必需的PHP扩展。

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

**步骤4** 执行以下命令，验证PHP的安装版本。

```
php -v
```

回显如下类似信息：

```
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
```

**步骤5** 打开PHP配置文件“php.ini”。

```
vim /etc/php.ini
```

**步骤6** 按i键进入编辑模式，修改如下两处内容：

- 根据实际情况修改参数“memory\_limit”的值，设置内存限制，如下图所示：

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



```
cd /var/www/html/  
git clone https://github.com/magento/magento2.git
```

**步骤3** 执行以下命令，将Magento切换到稳定版本。

默认情况下前一步骤的命令会安装最新开发版本的Magento。在生产环境中使用时，建议切换到稳定版本，否则将来将无法进行升级。

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

回显如下类似信息：

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

**步骤4** 执行以下命令，将安装文件移到Web服务器的根目录“/var/www/html/”下，其中“/var/www/html/magento2/”为Magento的当前安装目录。

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

迁移后可以通过“http://magento服务器的IP地址”访问Magento站点。否则，只能通过“http://magento服务器的IP地址/magento2”访问Magento站点。

**步骤5** 依次执行以下命令，设置Magento文件的权限。

```
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
```

**步骤6** 安装unzip和zip。

```
yum install -y unzip zip
```

**步骤7** 进入Web服务器的默认根目录“/var/www/html/”，然后使用composer工具安装Magento。

```
cd /var/www/html/  
composer install
```

**步骤8** 安装完成后，可通过浏览器访问“http://magento服务器IP地址”，显示如下页面，说明Magento安装成功。





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](#)

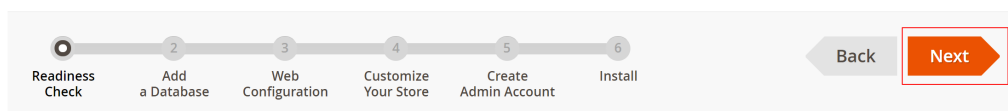
[Agree and Setup Magento](#)

----结束

## 步骤六：配置 Magento

**步骤1** 通过浏览器访问“http://magento服务器IP地址”，单击“Agree and Setup Magento”，开始配置Magento。

**步骤2** 单击“Start Readiness Check”，进行环境检测。检测通过后单击“Next”。



Step 1: Readiness Check

Let's check your environment for the correct PHP version, PHP extensions, file permissions and compatibility.

[Start Readiness Check](#)

**步骤3** 填写**步骤二：安装配置MySQL**中创建的MySQL数据库账户“magentouser”和密码，以及对应的数据库“magento”，并单击“Next”。

如下图所示：

## Step 2: Add a Database

Database Server Host *	<input type="text" value="localhost"/>
Database Server Username *	<input type="text" value="magentouser"/>
Database Server Password	<input type="password" value="....."/>
Database Name *	<input type="text" value="magento"/>
Table prefix	<input type="text" value="(optional)"/>

**步骤4** 设置网站的访问地址和后台管理地址，并单击“Next”。

如下图所示：

## Step 3: Web Configuration

Your Store Address	<input type="text" value="http://124.124.124.124"/>
Magento Admin Address *	<input type="text" value="http://124.124.124.124/admin_1pj83g"/>

### 说明

后台管理地址可自定义，请牢记设置的后台管理地址。

**步骤5** 设置语言和时区信息，并单击“Next”。

如下图所示：

## Step 4: Customize Your Store

Store Default Time Zone *	<input type="text" value="GMT (UTC)"/>
Store Default Currency *	<input type="text" value="Chinese Yuan (CNY)"/>
Store Default Language *	<input type="text" value="Chinese (China)"/>

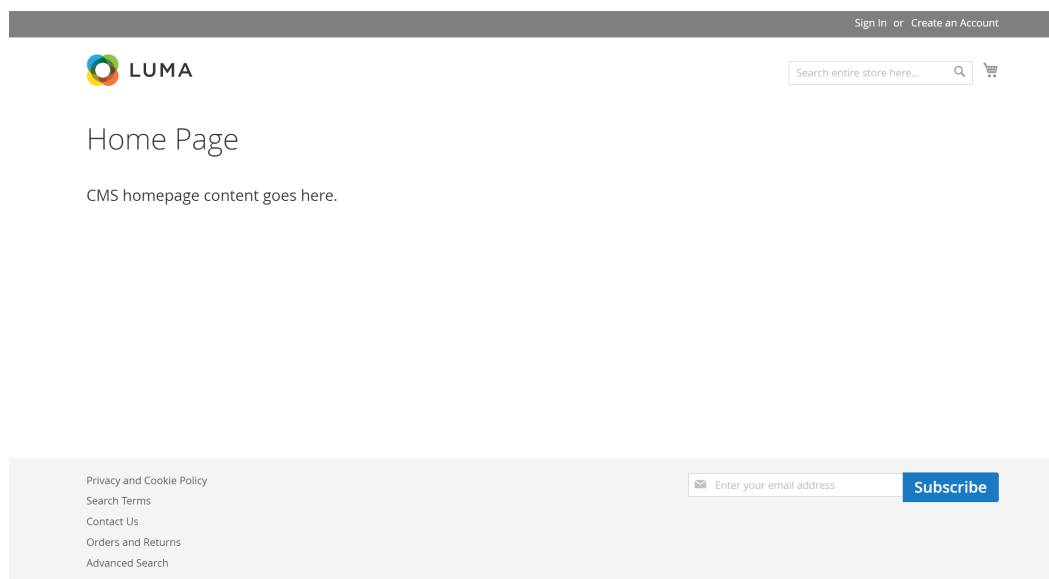
**步骤6** 设置管理账号和密码，并单击“Next”。

如下图所示：

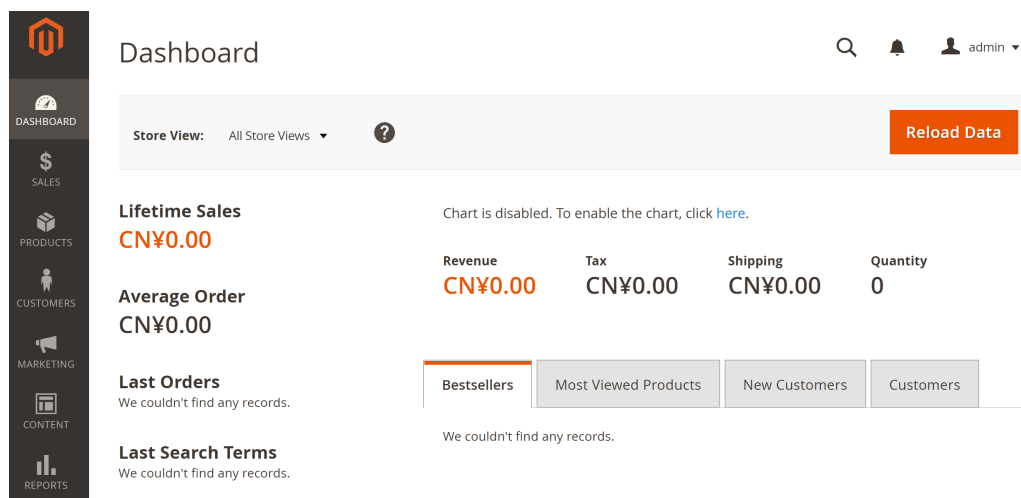


更多关于Magento使用cron作业的内容，请参见[Magento官方文档](#)。

**步骤10** 打开客户端的计算机，使用浏览器访问“http://magento服务器IP地址”，显示如下图所示的默认界面。



**步骤11** 使用浏览器访问“http://magento后台管理地址”，并使用配置Magento过程中设置的管理账号和密码登录，登录成功后显示如下图所示的界面。



### 📖 说明

如果登录后界面提示“**One or more indexers are invalid. Make sure your Magento cron job is running.**”的错误信息，可在Magento根目录“/var/www/html”执行**php bin/magento indexer:reindex**命令。

更多关于Magento配置信息，请参见[Magento官方文档](#)。

----结束

## 步骤七：其余操作

**步骤1** 购买域名。

为了便于网站的访问和使用，可以给网站设置一个单独的域名，使用域名访问网站。首先，需要在域名注册商处获得授权的域名。

#### 步骤2 配置域名解析。

配置域名解析后才能使用注册的域名访问网站。具体操作请参见[配置公网域名](#)。

例如，配置的域名为“www.example.com”，配置成功后，可在浏览器地址栏中输入“http://www.example.com”访问部署的网站。

----结束

## 5.4 手工搭建 Ghost 博客（Ubuntu 20.04）

Ghost是基于Node.js的开源博客平台，可以为用户提供更加便捷的写作与发布平台，本文指导用户基于华为云弹性云服务器（以Ubuntu 20.04操作系统云服务器为例）部署Ghost博客。

### 创建新用户

由于Ghost官方不推荐使用root用户直接操作，因此需要重新创新的用户，并为其配置权限。

1. 执行以下命令，创建新用户。本文以user为例。

```
adduser user
```

回显信息如下：

```
Adding user `user' ...
Adding new group `user' (1000) ...
Adding new user `user' (1000) with group `user' ...
Creating home directory `/home/user' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y
```

- a. 在**New password:**和**Retype new password:**提示信息中，请按照提示输入并确认用户密码，密码默认不显示，输入完成后按Enter。
  - b. 在**Enter the new value, or press ENTER for the default**提示信息中，按Enter保持默认即可，您也可以根据实际情况填写用户相关信息。
  - c. 在**Is the information correct? [Y/n]**提示信息中，输入Y确认信息，并按Enter，完成设置。
2. 执行以下命令，将新创建的用户添加到组。  

```
usermod -aG sudo user
```
  3. 执行以下命令，切换到user用户。  

```
su - user
```

## 安装 Nginx

部署Ghost博客，需要安装Nginx作为HTTP服务器，本节以安装Nginx 1.18.0 版本为例。

1. 执行以下命令，更新Linux操作系统和软件包。

```
sudo apt-get update
```

```
sudo apt-get upgrade -y
```

2. 执行以下命令，安装Nginx。

```
sudo apt-get install -y nginx
```

3. 执行以下命令查看Nginx版本。

```
nginx -v
```

回显信息如下：

```
nginx version: nginx/1.18.0 (Ubuntu)
```

4. 调整防火墙（可选）。

UFW（Uncomplicated Firewall）是一个iptables的接口，可以简化配置防火墙的过程。Ubuntu默认安装了UFW，执行以下命令查看防火墙的状态。

```
sudo ufw status
```

如果你没有也不想开启防火墙，则可以直接跳过此步骤，如果你想要开启防火墙可以通过以下命令实现。

```
sudo ufw enable
```

之后再次检查防火墙状态验证是否成功开启防火墙。

在测试Nginx之前，需要重新配置防火墙软件以允许访问Nginx。执行以下命令，将Nginx自动注册在UFW。

```
sudo ufw app list
```

回显信息：

```
Available applications:
```

```
Nginx Full  
Nginx HTTP  
Nginx HTTPS  
...
```

- Nginx Full：此配置文件打开端口 80（正常，未加密的Web流量）和端口 443（TLS / SSL加密流量）
- Nginx HTTP：此配置文件仅打开端口 80（正常，未加密的Web流量）
- Nginx HTTPS：此配置文件仅打开端口 443（TLS / SSL加密流量）

执行以下命令确保防火墙允许HTTP和HTTPS连接。

```
sudo ufw allow 'Nginx Full'
```

5. 验证Nginx是否正常工作。

在浏览器中通过域名或者IP地址进行访问Nginx，如果Nginx正常启动则会打开Welcome to nginx的欢迎页面。

使用浏览器访问“<http://云服务器IP地址>”，显示如下页面，说明Nginx安装成功。

## 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 [nginx.org](https://nginx.org).  
Commercial support is available at [nginx.com](https://nginx.com).

*Thank you for using nginx.*

## 安装 MySQL

MySQL是一种开源数据库管理系统，通常作为流行的LAMP（Linux，Apache，MySQL，PHP / Python / Perl）堆栈的一部分安装。它使用关系数据库和SQL结构化查询语言）来管理其数据。

1. 执行以下命令，安装MySQL。  
**sudo apt-get install -y mysql-server**
2. 执行以下命令查看MySQL版本。  
**mysql -V**  
回显信息如下：  
mysql Ver 8.0.37-0ubuntu0.20.04.3 for Linux on x86\_64 ((Ubuntu))
3. 执行以下命令，连接MySQL。  
**sudo mysql**
4. 执行以下命令，创建Ghost使用的数据库。本文以ghost\_data为例。  
**CREATE DATABASE ghost\_data;**
5. 执行以下命令，设置root账户密码。  
**ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql\_native\_password BY 'xxxxx';**  
其中'xxxxx'为待设置的密码。
6. 执行以下命令，重新加载MySQL的授权表，确保数据库权限的更改生效。  
**FLUSH PRIVILEGES;**
7. 执行以下命令，退出MySQL。  
**exit**

## 安装 Node.js

1. 执行以下命令，安装Node.js  
**sudo curl -sL https://deb.nodesource.com/setup\_18.x | sudo -E bash -**  
**sudo apt-get install -y nodejs**
2. 安装完成后，执行以下命令查看Node.js版本和npm版本。  
**node -v**  
**npm -v**  
回显信息：  
root@ecs-c47c:~# node -v  
v18.20.3

```
root@ecs-c47c:~# npm -v  
10.7.0
```

## Ghost 安装与配置

Ghost v1.0.0 及以上版本已加入了Ghost-CLI，因此可以直接安装配置Ghost-CLI。

1. 执行以下命令，安装Ghost-CLI。

```
sudo npm install ghost-cli@latest -g
```

2. 创建一个文件夹，之前介绍过Nginx的重要文件结构 /var/www/ 就是将要创建文件夹的地方。

```
sudo mkdir -p /var/www/ghost
```

### 📖 说明

ghost在/root文件夹中安装Ghost将无法正常工作。

3. 配置权限。

```
sudo chown user:user /var/www/ghost
```

```
sudo chmod 775 /var/www/ghost
```

### 📖 说明

user是1创建的用户。

4. 进入刚才创建的文件夹。

```
cd /var/www/ghost
```

5. 执行以下命令，用Ghost-CLI安装Ghost。

```
ghost install
```

### 📖 说明

如果Ghost安装时提示node版本不匹配，可以在nodejs官方网站查询相应的版本重新安装。

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

6. 配置Ghost。

如果上面在 /var/www/ghost/ 目录下运行**ghost install**成功的话，会要求配置相关参数：



```

+ Checking system Node.js version - found v18.20.3
+ Checking current folder permissions
+ Checking memory availability
+ Checking free space
+ Checking for latest Ghost version
+ Setting up install directory
+ Downloading and installing Ghost v5.85.1
+ Finishing install process
+ Enter your blog URL: http://example.com
+ Enter your MySQL hostname:
+ Enter your MySQL username: root
+ Enter your MySQL password: [hidden]
+ Enter your Ghost database name: ghost_data
+ Configuring Ghost
+ Setting up instance
+ sudo useradd --system --user-group ghost
+ sudo chown -R ghost:ghost /var/www/ghost/content
+ Setting up "ghost" system user
? Do you wish to set up "ghost" mysql user? Yes
+ Setting up "ghost" mysql user
? Do you wish to set up Nginx? Yes
+ sudo mv /tmp/example-con/example.com.conf /etc/nginx/sites-available/example.com.conf
+ sudo ln -sf /etc/nginx/sites-available/example.com.conf /etc/nginx/sites-enabled/example.com.conf
+ sudo nginx -s reload
+ Setting up Nginx
? Do you wish to set up SSL? Yes
? Enter your email (For SSL Certificate) [redacted]
+ sudo mkdir -p /etc/letsencrypt
+ sudo ./acme.sh --install --home /etc/letsencrypt
+ sudo /etc/letsencrypt/acme.sh --issue --home /etc/letsencrypt --server letsencrypt --domain example.com --webroot /var/www/ghost/system/nginx-root --reloadcmd "nginx -s reload" --accountemail [redacted] --keylength 2048
+ Setting up SSL
? Do you wish to set up Systemd? Yes
+ sudo mv /tmp/example-con/ghost_example-con.service /lib/systemd/system/ghost_example-con.service
+ sudo systemctl daemon-reload
+ Setting up Systemd
+ sudo systemctl is-active ghost_example-con
? Do you want to start Ghost? Yes
+ sudo systemctl start ghost_example-con
+ Starting Ghost

```

- Enter your blog URL: 输入已解析的域名，例如：http://example.com。
- Enter your MySQL hostname: 输入数据库连接地址。本示例中MySQL数据库与Ghost部署在同一台实例中，直接按Enter保持默认即可。
- Enter your MySQL username: 输入数据库用户名，输入root后按Enter。
- Enter your MySQL password: 输入数据库密码，输入5中设置的数据库密码后按Enter。
- Enter your Ghost database name: 输入Ghost使用的数据库名称。输入ghost\_data后按Enter。

如果配置后需要修改可以通过以下命令去文件中进行配置：

### vi config.production.json

打开之后就是生产环境配置内容了。参考配置见下图：

```
{
  "url": "http://www.ghost.org",
  "server": {
    "port": 2368,
    "host": "127.0.0.1"
  },
  "database": {
    "client": "mysql",
    "connection": {
      "host": "127.0.0.1",
      "user": "root",
      "password": "root",
      "database": "ghost"
    }
  },
  "mail": {
    "transport": "Direct"
  },
  "logging": {
    "transports": [
      "file",
      "stdout"
    ]
  },
  "process": "systemd",
  "paths": {
    "contentPath": "/var/www/ghost/content"
  },
  "bootstrap-socket": {
```

## 验证 Ghost 搭建完成

如果成功的安装Ghost之后，就可以通过域名访问到Ghost博客。

# 6 搭建应用

## 6.1 构建 FTP 站点

### 6.1.1 快速构建 FTP 站点（Windows 2012）

#### 简介

本文介绍了如何使用弹性云服务器的Windows实例搭建FTP站点。该指导具体操作以Windows Server 2012 R2为例。

Windows实例搭建FTP站点具体操作步骤如下：

1. [添加IIS以及FTP服务角色。](#)
2. [创建FTP用户名及密码。](#)
3. [设置共享文件的权限。](#)
4. [添加及设置FTP站点。](#)
5. [（可选）配置FTP防火墙支持。](#)
6. [设置安全组及防火墙。](#)
7. [客户端测试。](#)

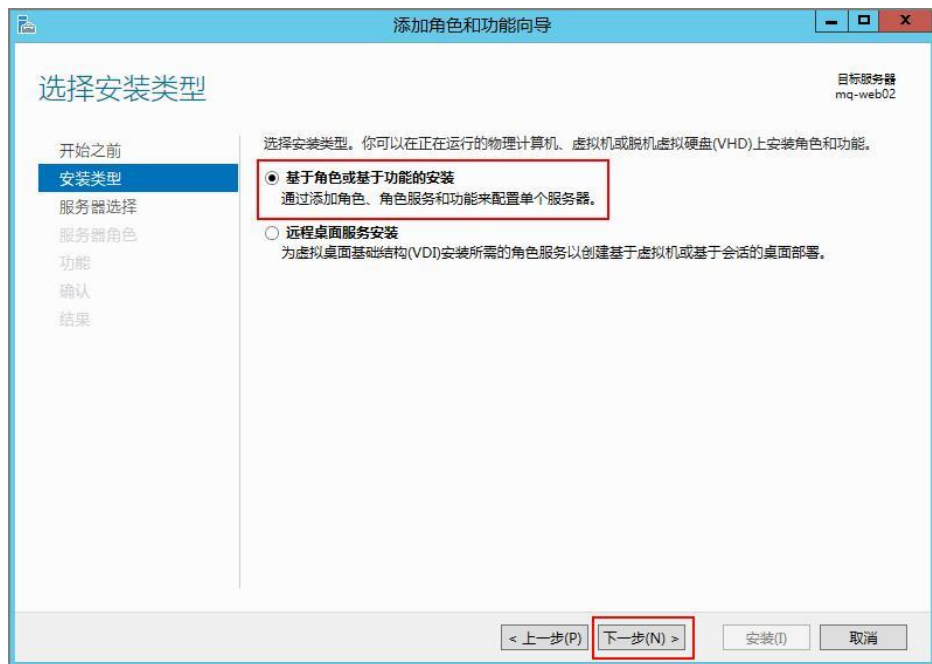
#### 操作步骤

**步骤1** 添加IIS以及FTP服务角色。

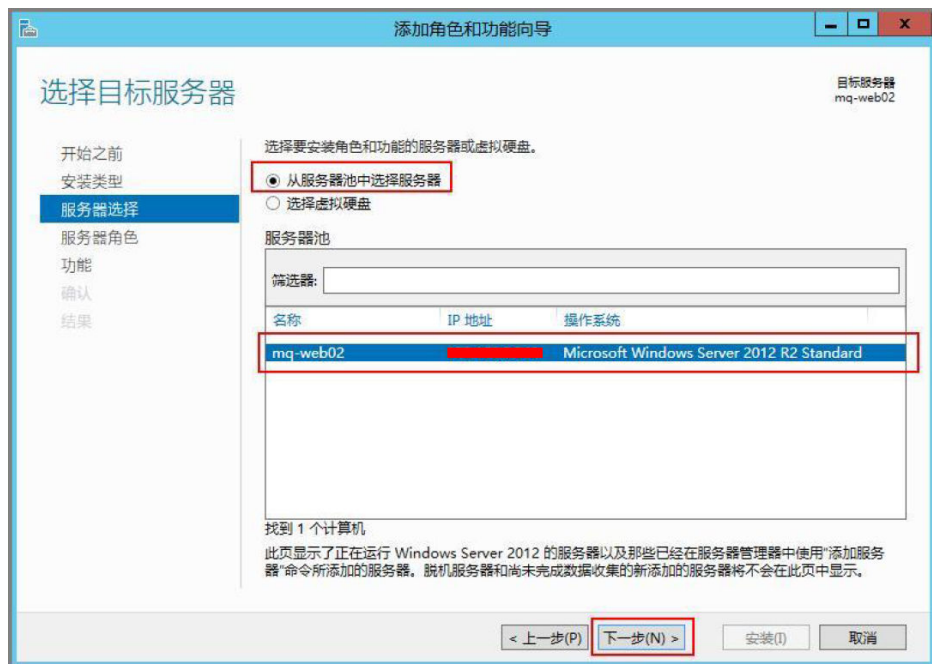
1. 登录弹性云服务器。
2. 选择“开始 > 服务器管理器”。
3. 单击“添加角色和功能”



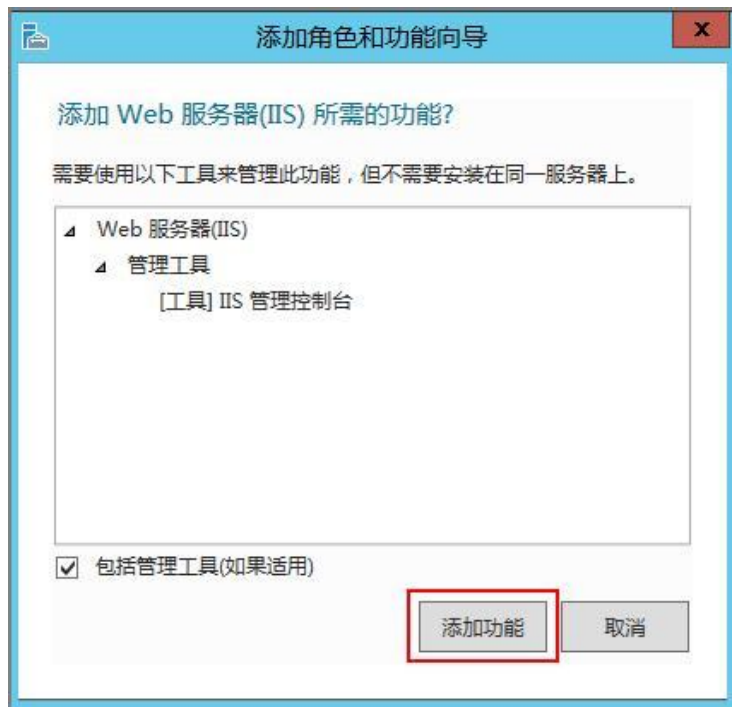
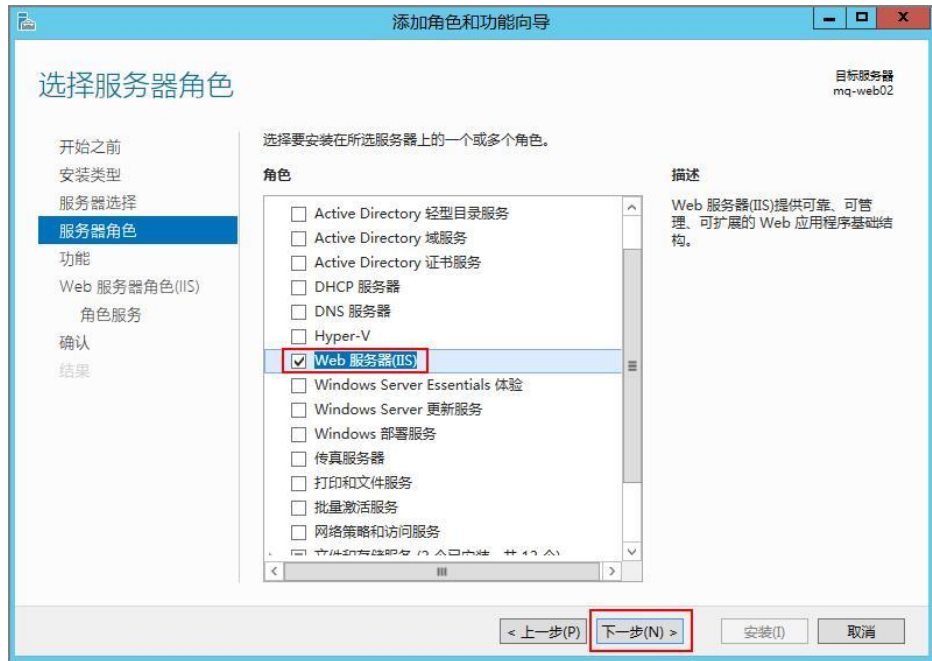
4. 在弹出的“开始之前”对话框中，单击“下一步”。
5. 选择“基于角色或基于功能的安装”，单击“下一步”。



6. 选择需要部署FTP的服务器，单击“下一步”。



7. 选择“Web服务器(IIS)”，并在弹出的对话框中单击“添加功能”，然后单击“下一步”。



8. 连续单击“下一步”，到“角色服务”页面。
9. 选择“FTP服务器”以及“IIS管理控制台”，单击“下一步”。



10. 单击“安装”，开始部署服务角色。

11. 安装完成后，单击“关闭”。

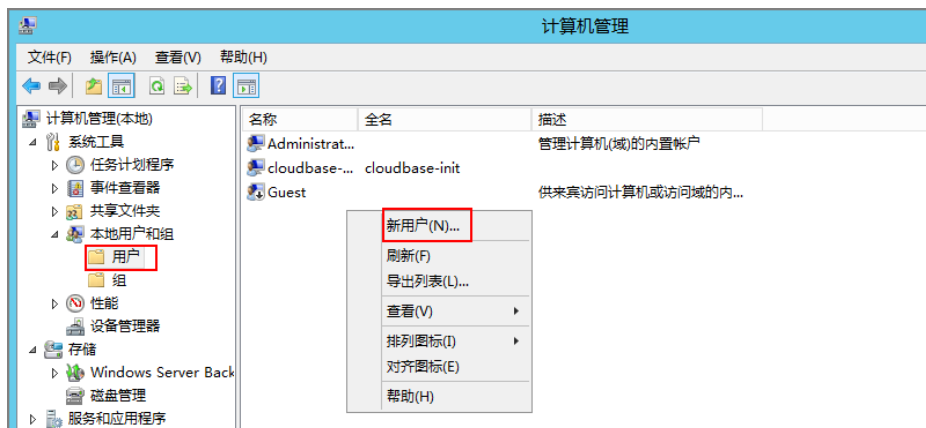
## 步骤2 创建FTP用户名及密码。

创建Windows用户名和密码，用于FTP使用。如果您希望匿名用户可以访问，可以不创建FTP用户和密码。

1. 在“服务器管理器”中，选择“仪表板 > 工具 > 计算机管理”。



2. 选择“系统工具 > 本地用户和组 > 用户”，在右侧空白处右击，并选择“新用户”。



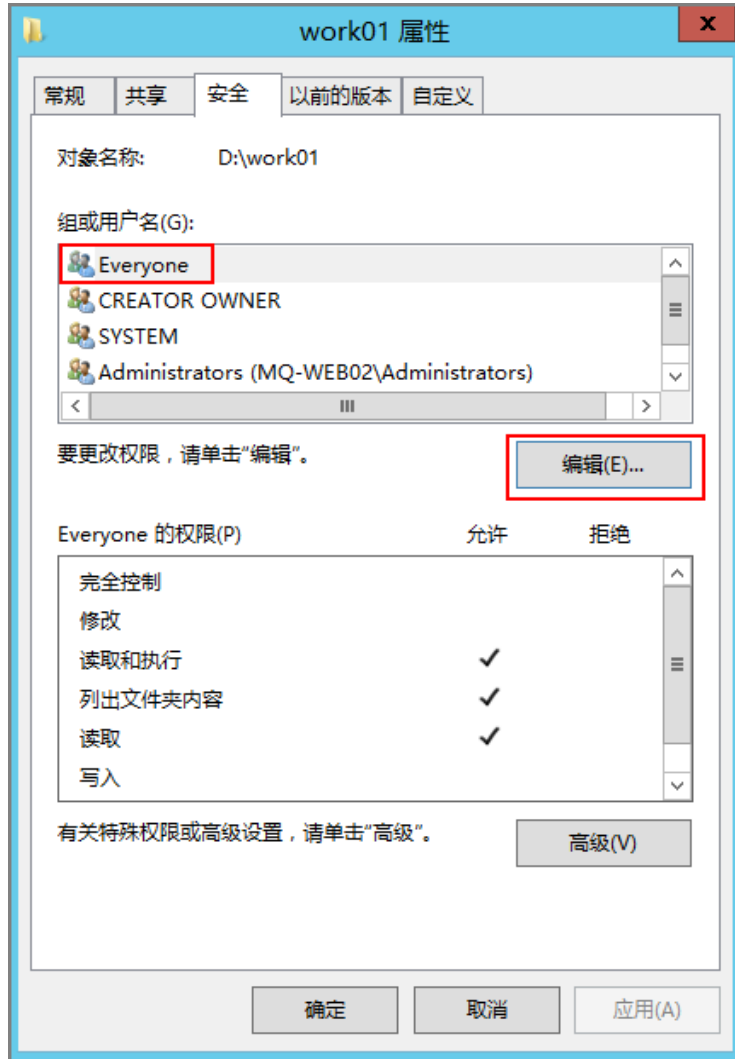
3. 设置“用户名”和“密码”，此处用户名以“ftpadmin”为例。



### 步骤3 设置共享文件的权限。

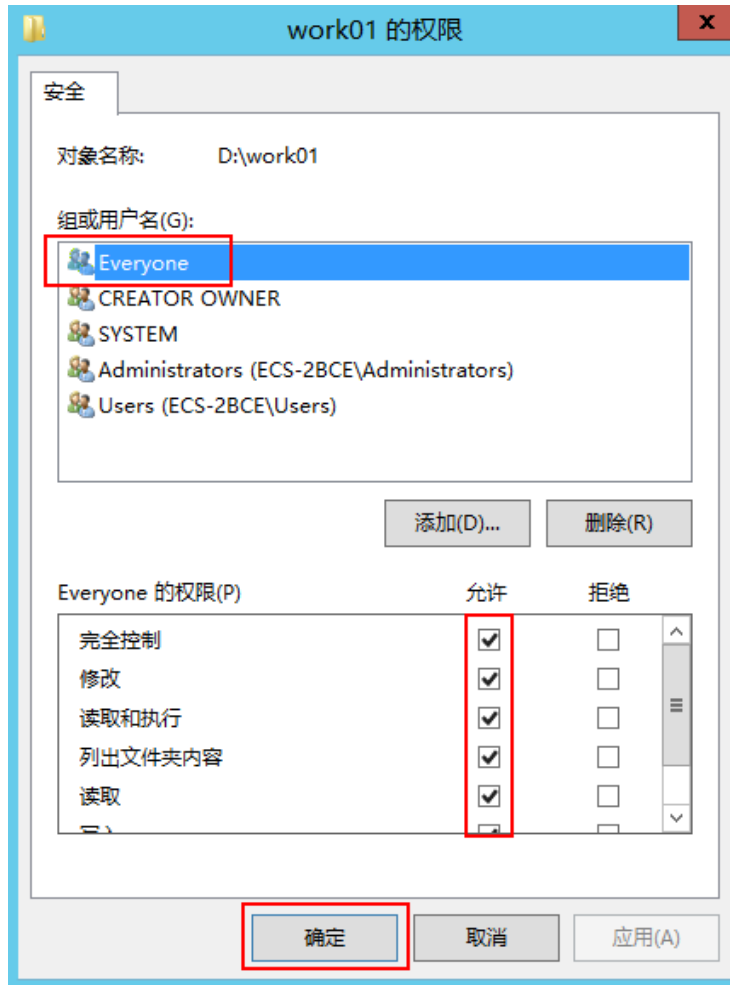
需要在FTP站点为共享给用户的文件夹设置访问及修改等权限。

1. 在服务器上创建一个供FTP使用的文件夹，选择文件夹，并单击右键选择“属性”。  
此处以“work01”文件夹为例，且文件夹包含了需共享的文件test.txt。
2. 在“安全”页签，选择“Everyone”，单击“编辑”。  
如果没有“Everyone”用户可以直接选择，需要先进行添加，添加方法请参见[FAQ](#)。



3. 选择“Everyone”，然后根据需要，选择“Everyone”的权限，并单击“确定”。  
此处以允许所有权限为例。



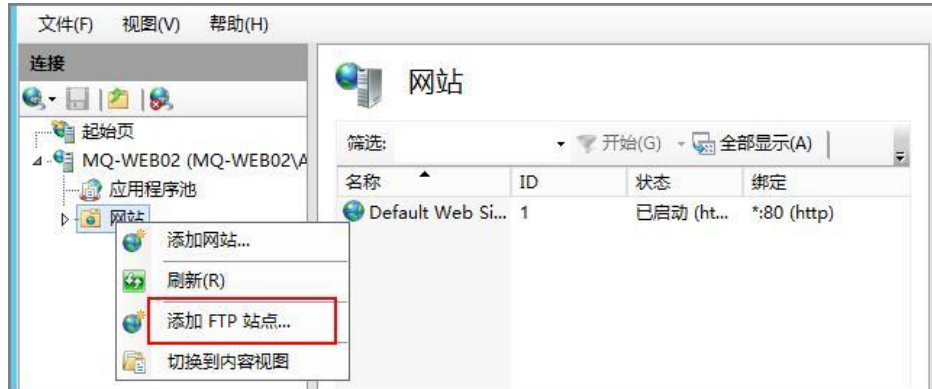


**步骤4** 添加及设置FTP站点。

1. 在“服务器管理器”中，选择“仪表板 > 工具 > Internet Information Services (IIS)管理器”。

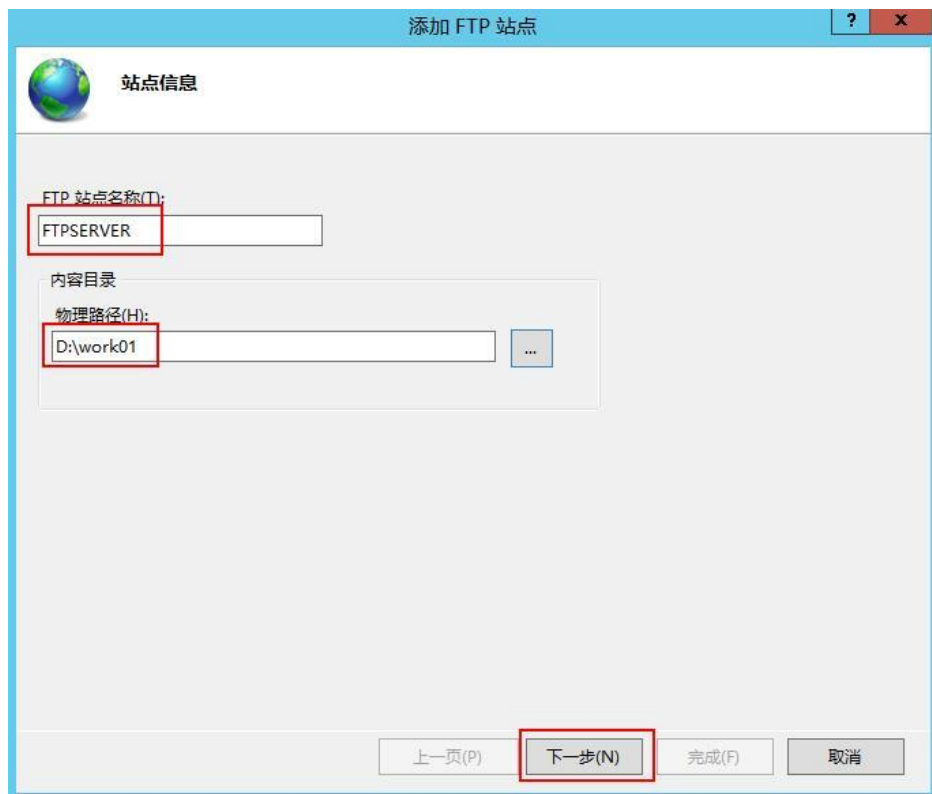


2. 选择“网站”并单击右键，然后选择“添加FTP站点”。



3. 在弹出的窗口中，填写FTP站点名称及共享文件夹的物理路径，然后单击“下一步”。

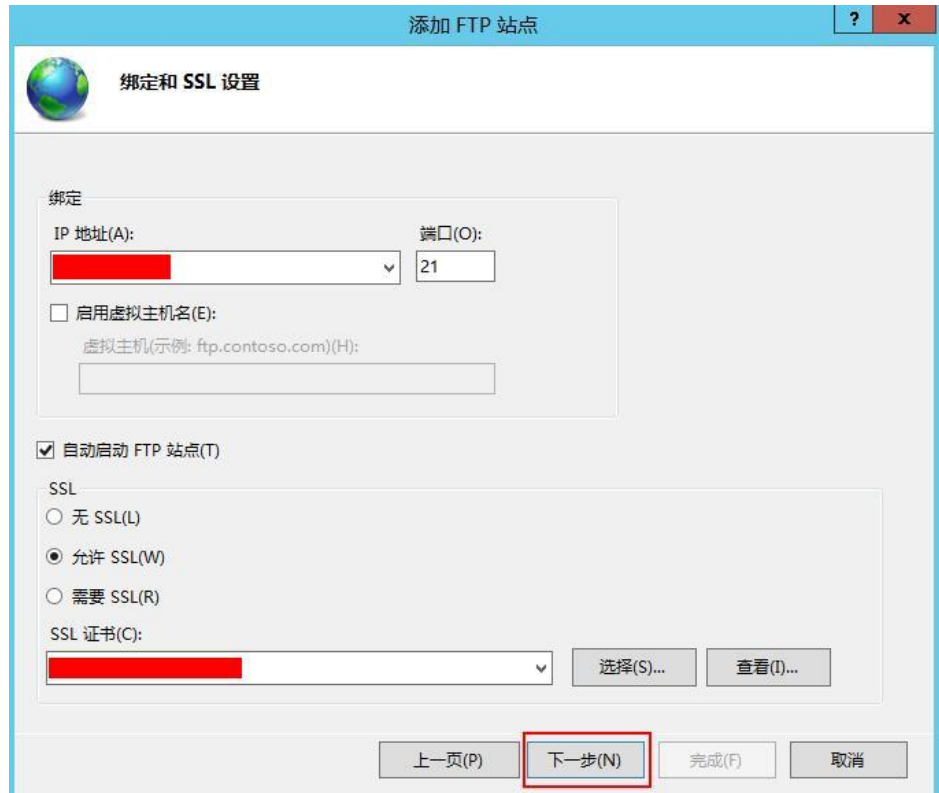
此处站点名称以“FTPSERVER”为例。



4. 输入该弹性云服务器的私有IP地址以及端口号，并设置SSL，单击“下一步”。
  - 端口号 默认为21，也可自行设置。
  - SSL根据需要进行设置。
    - **无**：不需要SSL加密。
    - **允许**：允许FTP服务器与客户端的非SSL和SSL连接。
    - **需要**：需要对FTP服务器和客户端之间的通信进行SSL加密。

#### 📖 说明

当SSL选择“允许”和“需要”时，需要选择SSL证书。可以选择已有的SSL证书，也可以制作一个SSL证书，具体制作证书的方法请参见3。



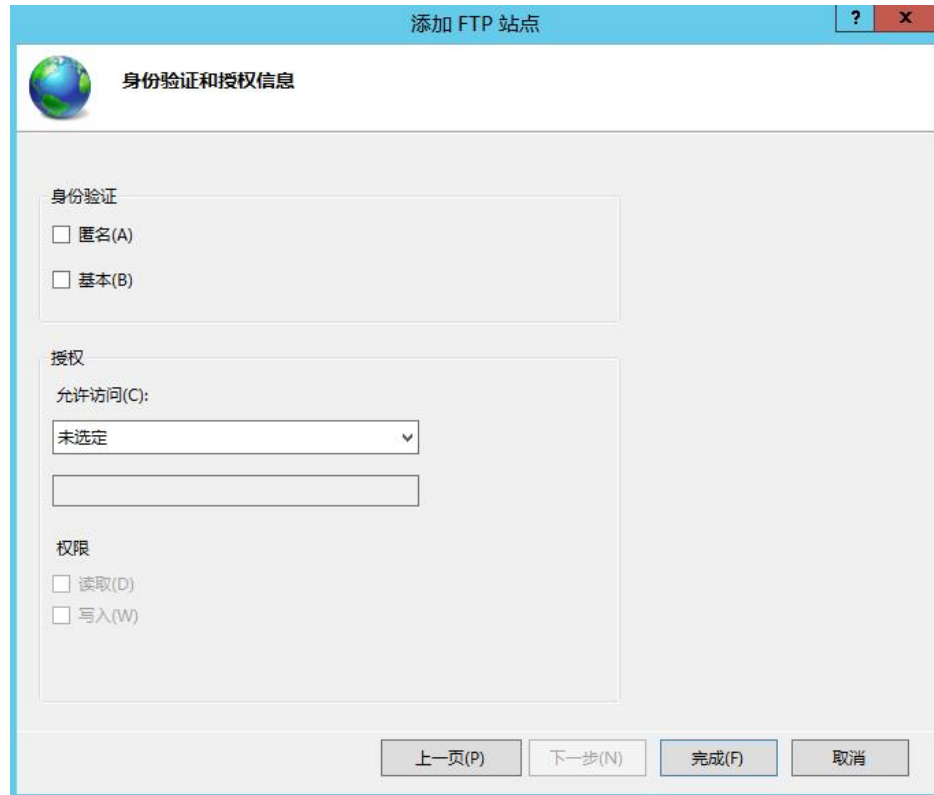
5. 设置身份认证和授权信息，并单击“完成”。

- 身份认证

- **匿名**：允许任何仅提供用户名“anonymous”或“ftp”的用户访问内容。
- **基本**：需要用户提供有效用户名和密码才能访问内容。但是基本身份验证通过网络传输密码时不加密，因此建议在确认客户端和FTP服务器之间的网络连接安全时使用此身份验证方法。

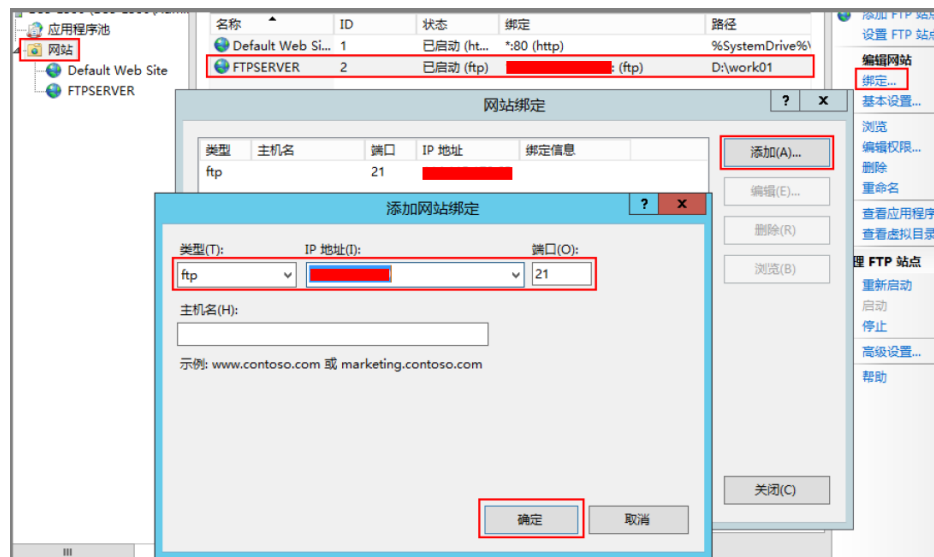
- 授权

- 允许访问
  - **所有用户**：所有用户均可访问相应内容。
  - **匿名用户**：匿名用户可访问相应内容。
  - **指定角色或用户组**：仅指定的角色或用户组的成员才能访问相应内容。如果选择此项，需要在下面输入框中输入指定的角色或用户组。
  - **指定用户**：仅指定的用户才能访问相应内容。如果选择此项，需要在下面输入框中输入指定的用户。
- 权限：选择经过授权的用户“读取”和“写入”权限。



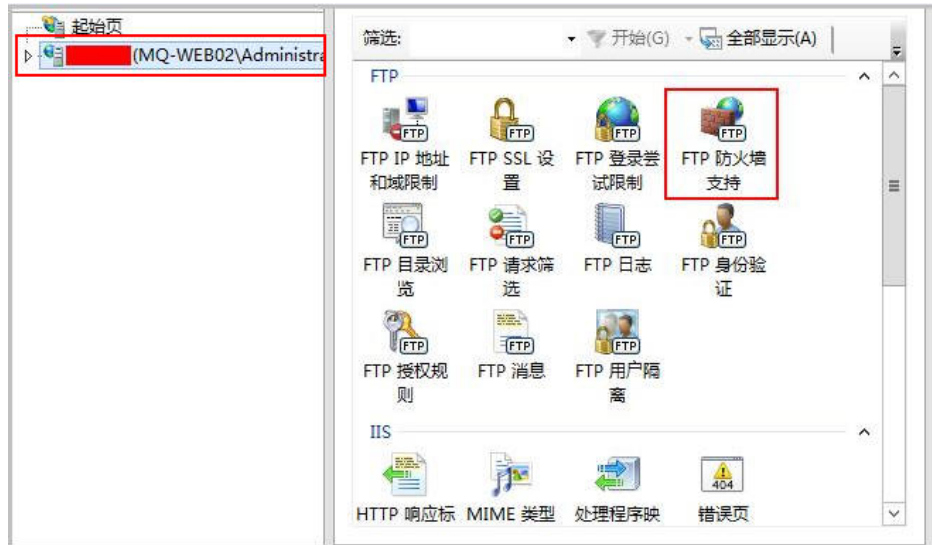
6. 绑定弹性云服务器的私网IP。

选择“网站”，选中创建的FTP站点，单击“绑定”；在弹出的“网站绑定”窗口单击“添加”，然后在弹出的窗口中添加弹性云服务器的私网IP地址，并单击“确定”。



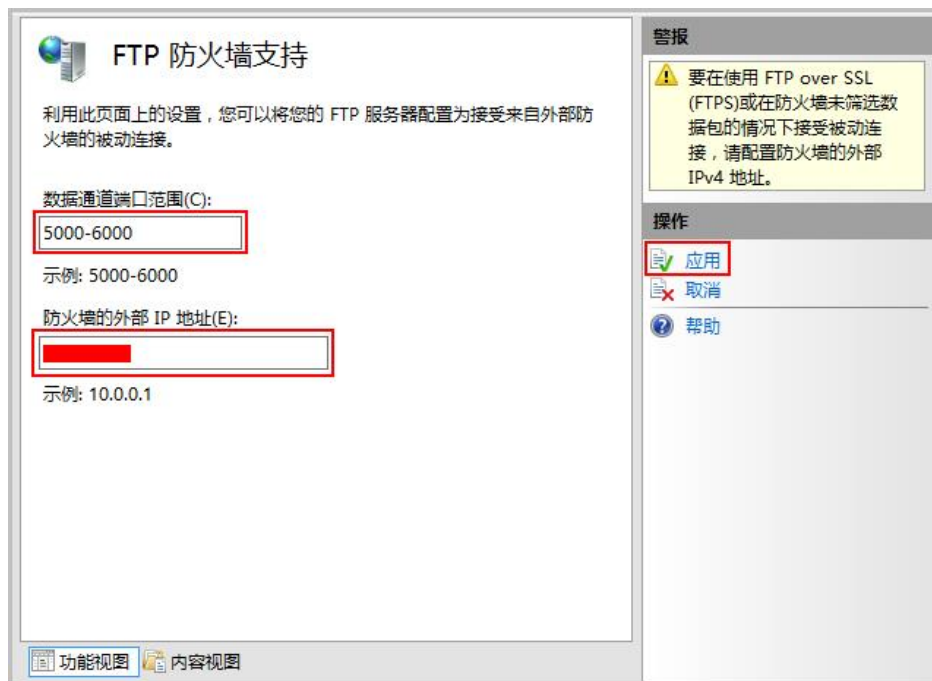
步骤5 (可选) 配置FTP防火墙支持。

- 如果需要使用FTP服务器的被动模式，则需要配置FTP防火墙支持。
  - 如果华为云上的服务器需要通过公网IP地址访问华为云上的实例搭建的FTP服务器时，需要配置FTP服务器的被动模式。
1. 双击“FTP防火墙支持”，打开FTP防火墙支持的配置界面。



2. 配置相关参数，并单击“应用”。

- 数据通道端口范围：指定用于被动连接的端口范围。可指定的有效端口范围为1025-65535。请根据实际需求进行设置。
- 防火墙的外部IP地址：输入该弹性云服务器的公网IP地址。



3. 重启云服务器使防火墙配置生效。

**步骤6** 设置安全组及防火墙。

搭建好FTP站点后，需要在弹性云服务器安全组的入方向添加一条放行FTP端口的规则，具体步骤参见[为安全组添加安全组规则](#)。放通的端口请参考[表6-1](#)。

如果配置了“FTP防火墙支持”，需要在安全组中同时放行FTP站点使用的端口和FTP防火墙使用的数据通道端口。

服务器防火墙默认放行TCP的21端口用于FTP服务。如果选用其他端口，需要在防火墙中添加一条放行此端口的入站规则。

表 6-1 设置安全组规则

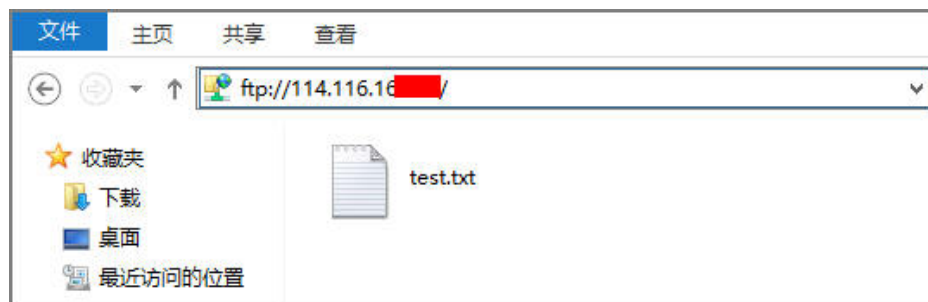
方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	基本协议/自定义TCP: 20-21端口	0.0.0.0/0
入方向	1	允许	IPv4	基本协议/自定义TCP: 1024-65535间的端口 (例如 5000-6000)	0.0.0.0/0

### 步骤7 客户端测试。

打开客户端的计算机，在路径栏输入“ftp://FTP服务器IP地址:FTP端口”（如果不填端口则默认访问21端口）。弹出输入用户名和密码的对话框表示配置成功，正确的输入用户名和密码后，即可对FTP文件进行相应权限的操作。

#### 说明

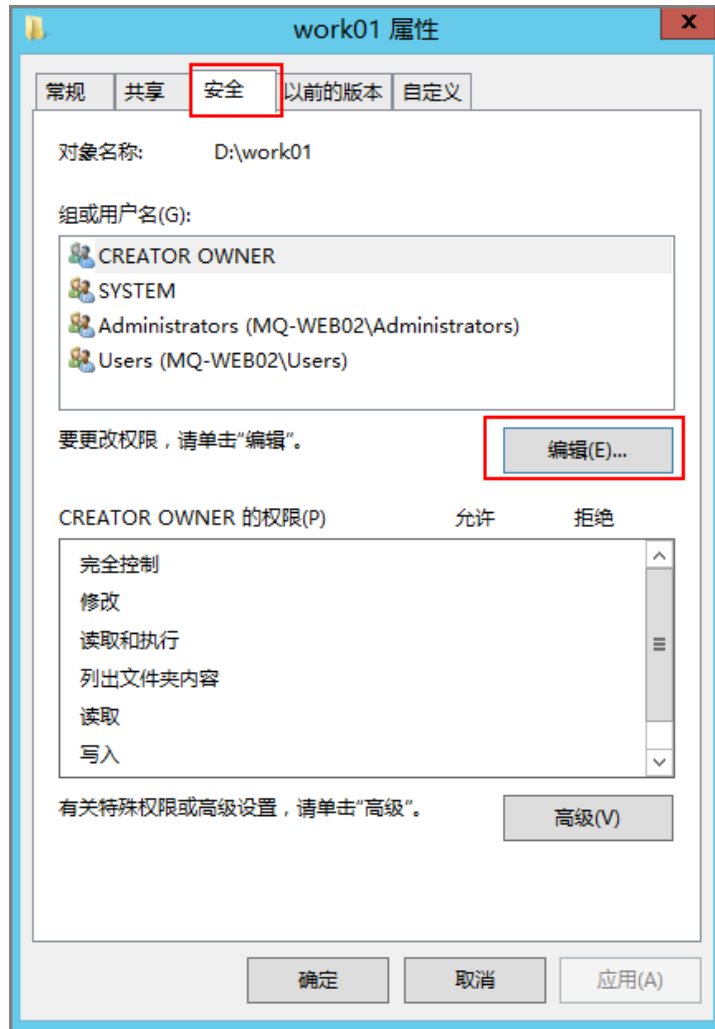
如果没有配置“FTP防火墙支持”，客户端使用此方法访问FTP站点时，需要对IE浏览器进行设置，才能打开FTP的文件夹。打开IE浏览器，选择“设置 > Internet 选项 > 高级”。勾选“启用FTP文件夹视图”，取消勾选“使用被动FTP”。



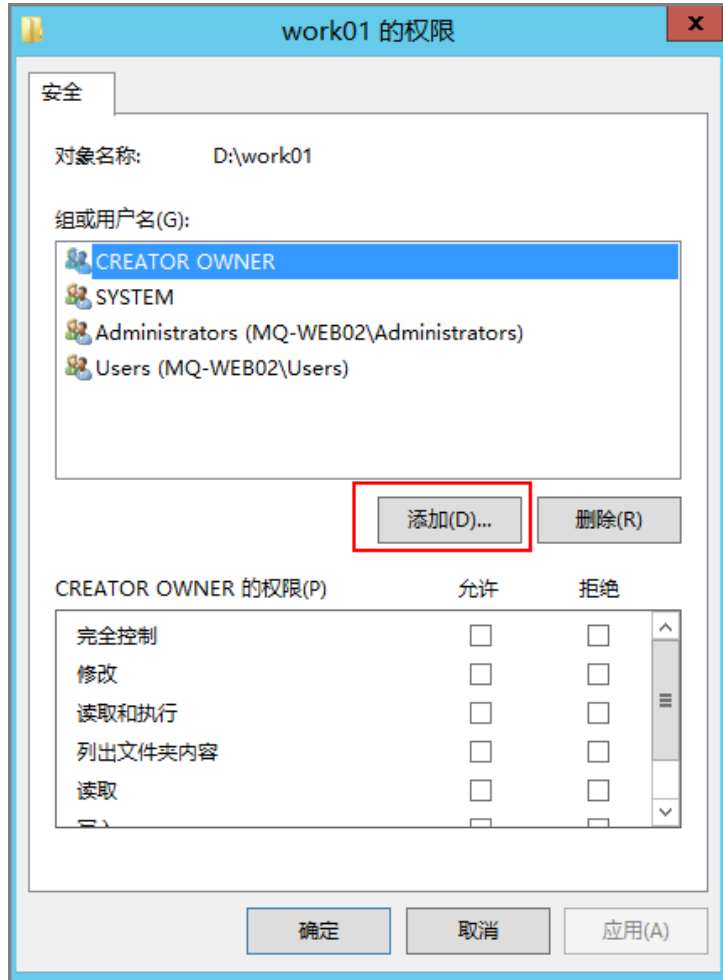
---结束

## FAQ

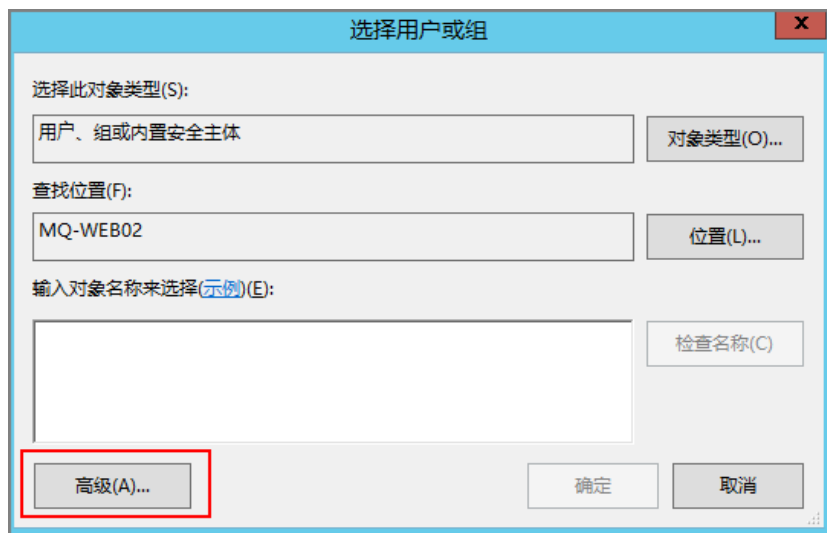
1. 使用Windows系统搭建FTP站点的更多信息请参见[微软官方文档](#)。
2. 如果设置文件夹的属性时，没有“Everyone”用户可直接选择，可按照如下步骤添加“Everyone”用户。
  - a. 在“安全”页签，单击“编辑”。



- b. 在新弹出的窗口中, 单击“添加”。

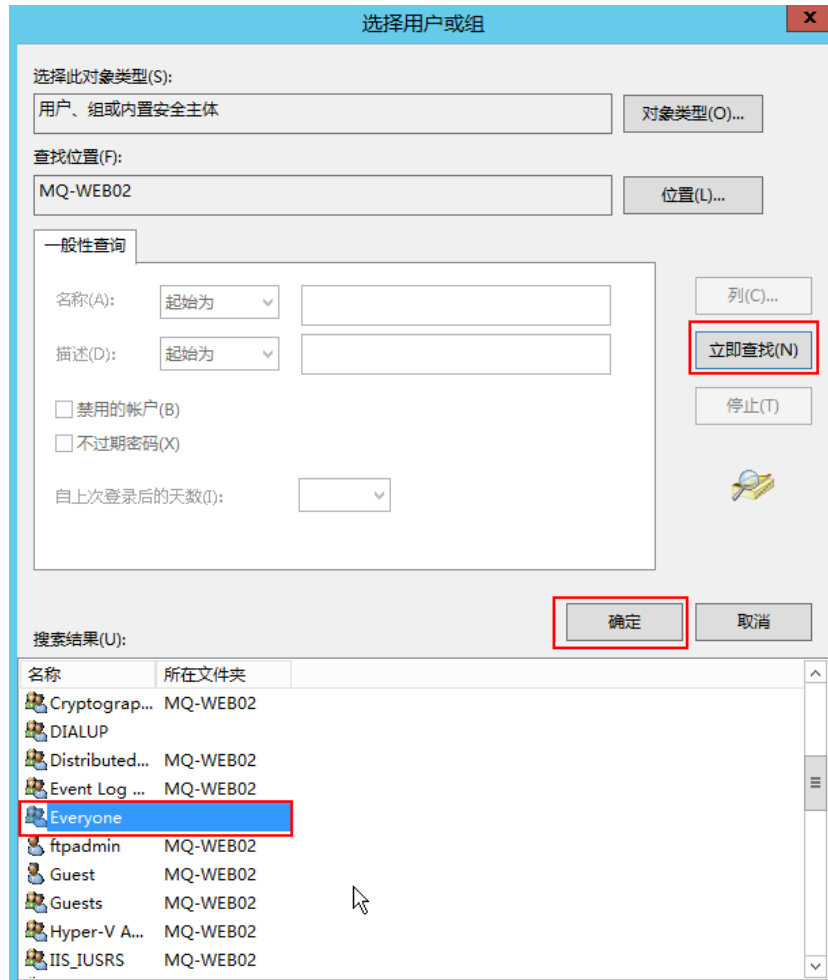


c. 在新弹出的窗口中，单击“高级”。



d. 在新弹出的窗口中，单击“立即查找(N)”，然后在搜索结果中选择“Everyone”并单击“确定”。

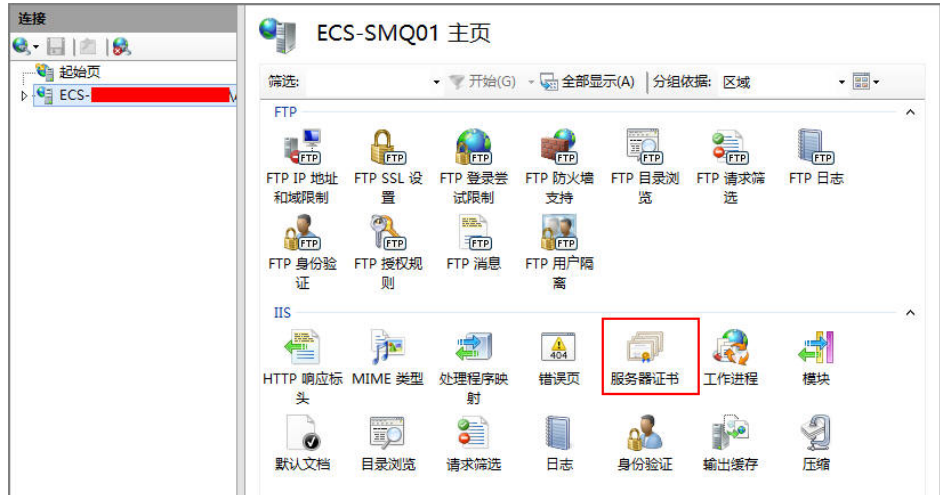




- e. 单击“确定”，返回权限窗口。
  - f. 单击“确定”，完成添加。
3. 制作服务器证书。
- a. 在“服务器管理器”中，选择“仪表板 > 工具 > Internet Information Services (IIS)管理器”。



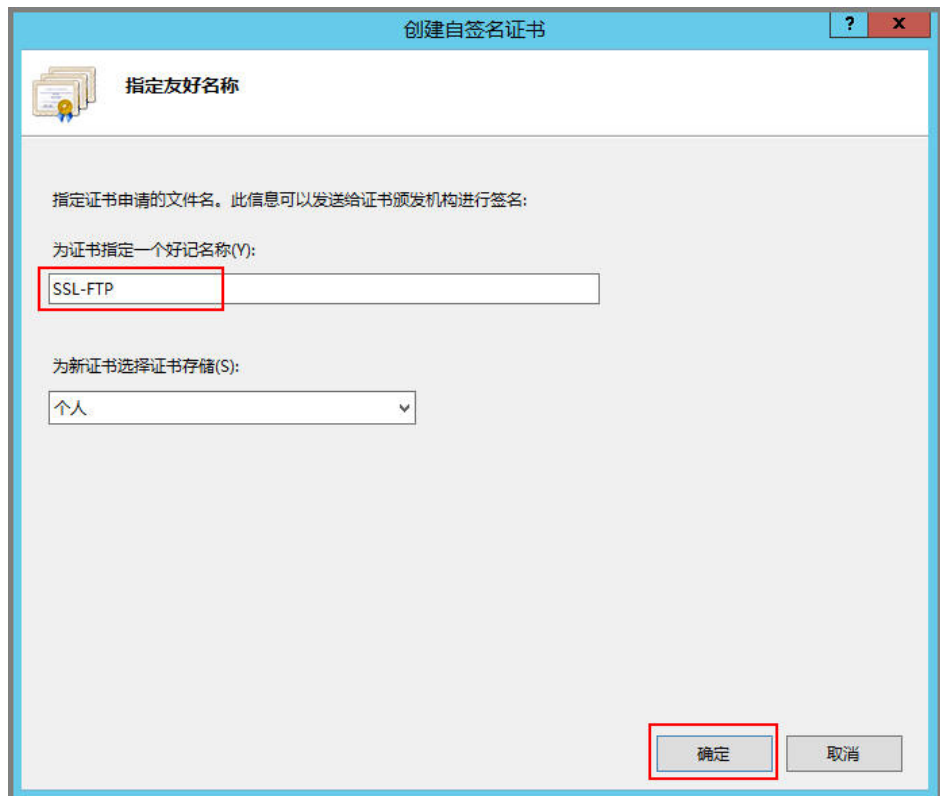
- b. 在左侧列表单击服务器，然后在服务器主页“IIS”区域，双击“服务器证书”，进入“服务器证书”页面。



c. 单击“创建自签名证书”。



d. 输入证书的名称，并选择证书存储类型，单击“确定”。



创建成功后会在服务器证书界面显示已经创建的证书。



## 6.1.2 快速构建 FTP 站点 ( Windows 2019 )

### 简介

本文介绍了如何使用弹性云服务器的Windows实例搭建FTP站点。该指导具体操作以Windows Server 2019为例。

Windows实例搭建FTP站点具体操作步骤如下：

1. 添加IIS以及FTP服务角色。
2. 创建FTP用户名及密码。
3. 设置共享文件的权限。
4. 添加及设置FTP站点。
5. (可选) 配置FTP防火墙支持。
6. 设置安全组及防火墙。
7. 客户端测试。

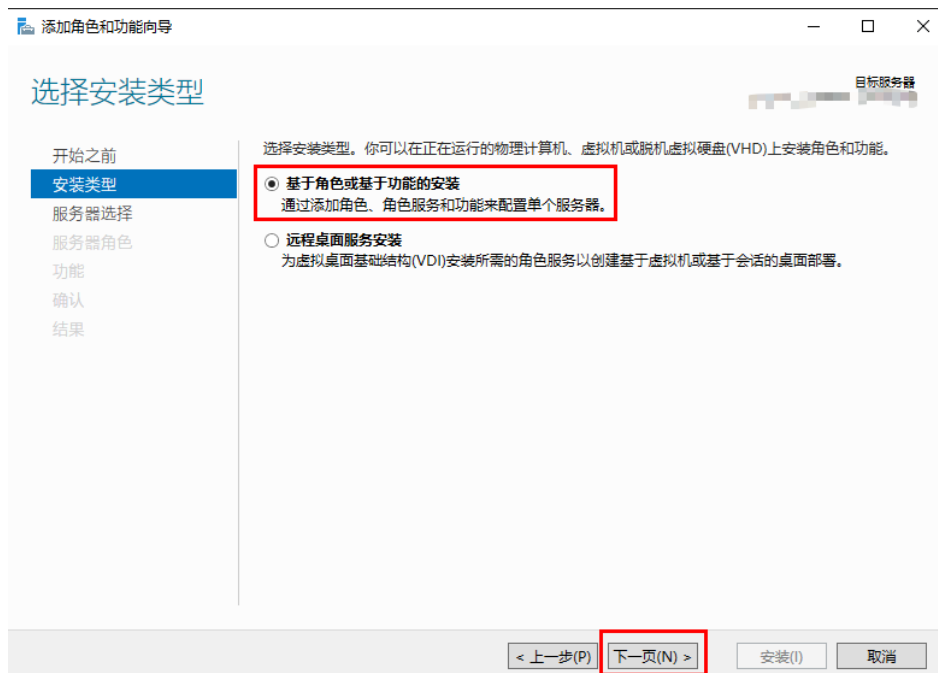
### 操作步骤

#### 步骤1 添加IIS以及FTP服务角色。

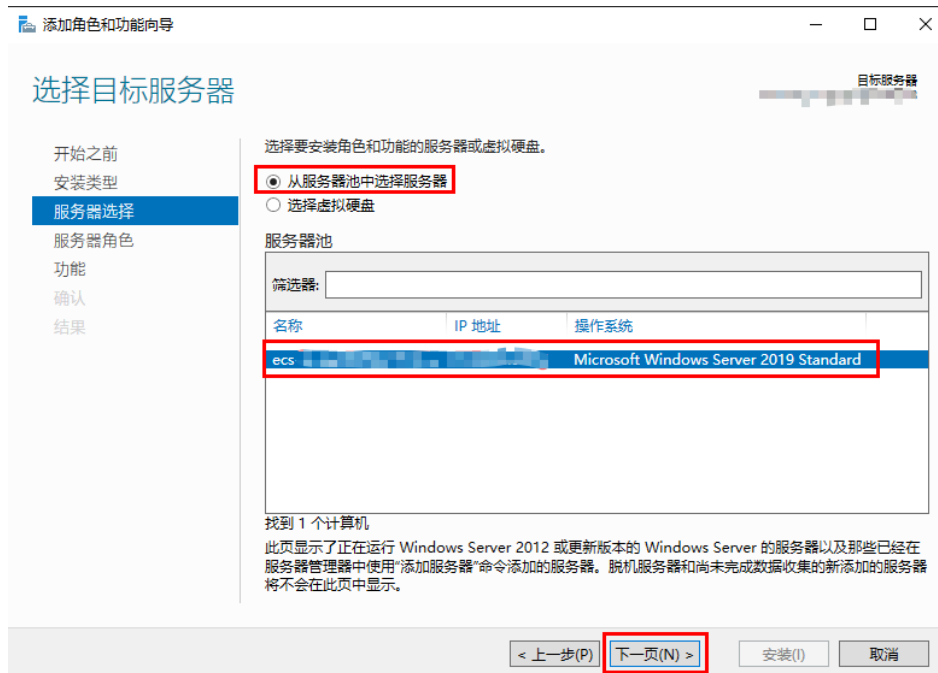
1. 登录弹性云服务器。
2. 选择“开始 > 服务器管理器”。
3. 单击“添加角色和功能”。



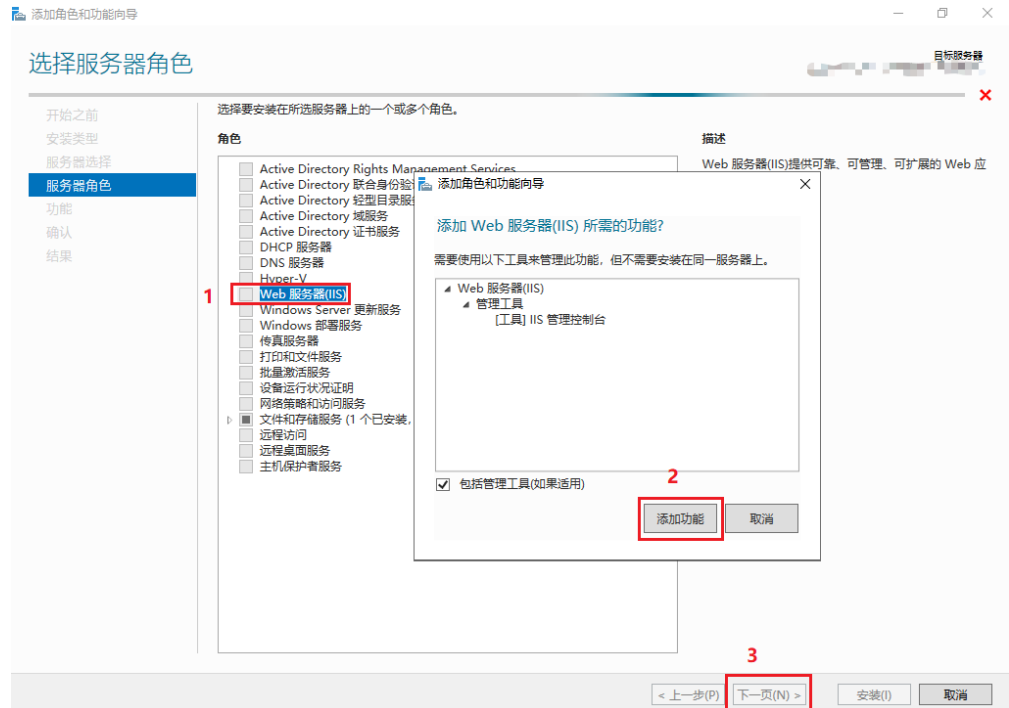
4. 在弹出的“开始之前”对话框中，单击“下一页(N)”。
5. 选择“基于角色或基于功能的安装”，单击“下一页(N)”。



6. 选择需要部署FTP的服务器，单击“下一页(N)”。



7. 选择“Web服务器 (IIS)”，并在弹出的对话框中单击“添加功能”，然后单击“下一页(N)”。



8. 连续单击“下一页(N)”，到“角色服务”页面。
9. 选择“FTP服务器”以及“IIS管理控制台”，单击“下一页(N)”。



10. 单击“安装”，开始部署服务角色。
11. 安装完成后，单击“关闭”。

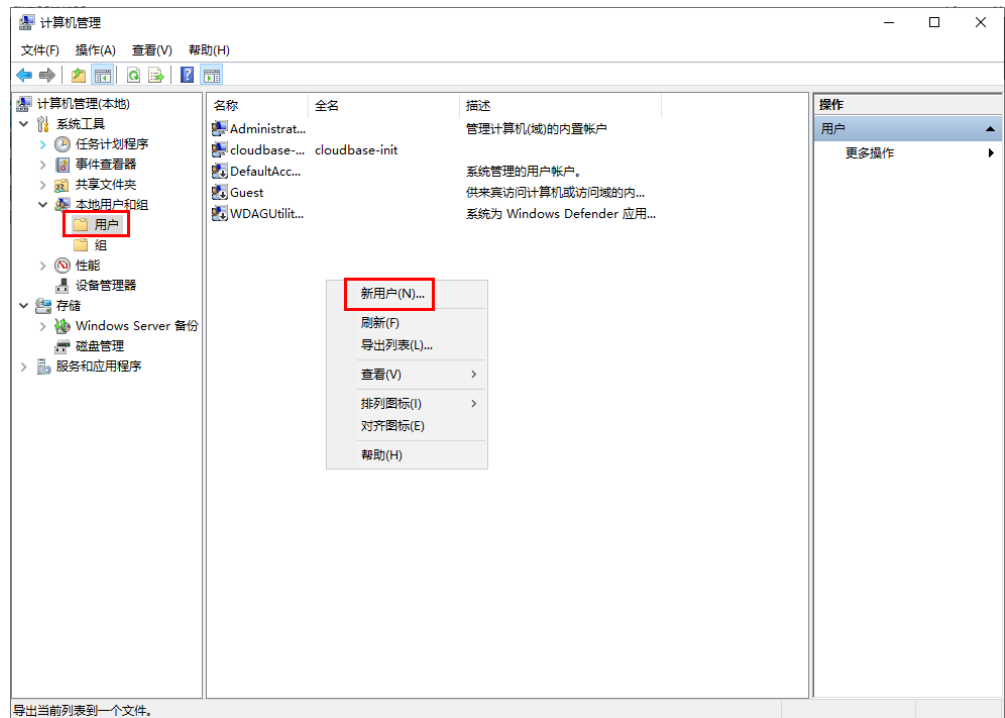
## 步骤2 创建FTP用户名及密码。

创建Windows用户名和密码，用于FTP使用。如果您希望匿名用户可以访问，可以不创建FTP用户和密码。

1. 在“服务器管理器”中，选择“仪表板 > 工具 > 计算机管理”。



2. 选择“系统工具 > 本地用户和组 > 用户”，在右侧空白处右击，并选择“新用户(N)...”。



3. 设置“用户名”和“密码”，此处用户名以“ftpadmin”为例。

The image shows a 'New User' dialog box with the following fields and options:

- 用户名(U): ftpadmin
- 全名(F):
- 描述(D):
- 密码(P):
- 确认密码(C):
- 用户下次登录时须更改密码(M)
- 用户不能更改密码(S)
- 密码永不过期(W)
- 帐户已禁用(B)
- 按钮: 帮助(H), 创建(E), 关闭(O)

4. 单击“创建”。

### 步骤3 设置共享文件的权限。

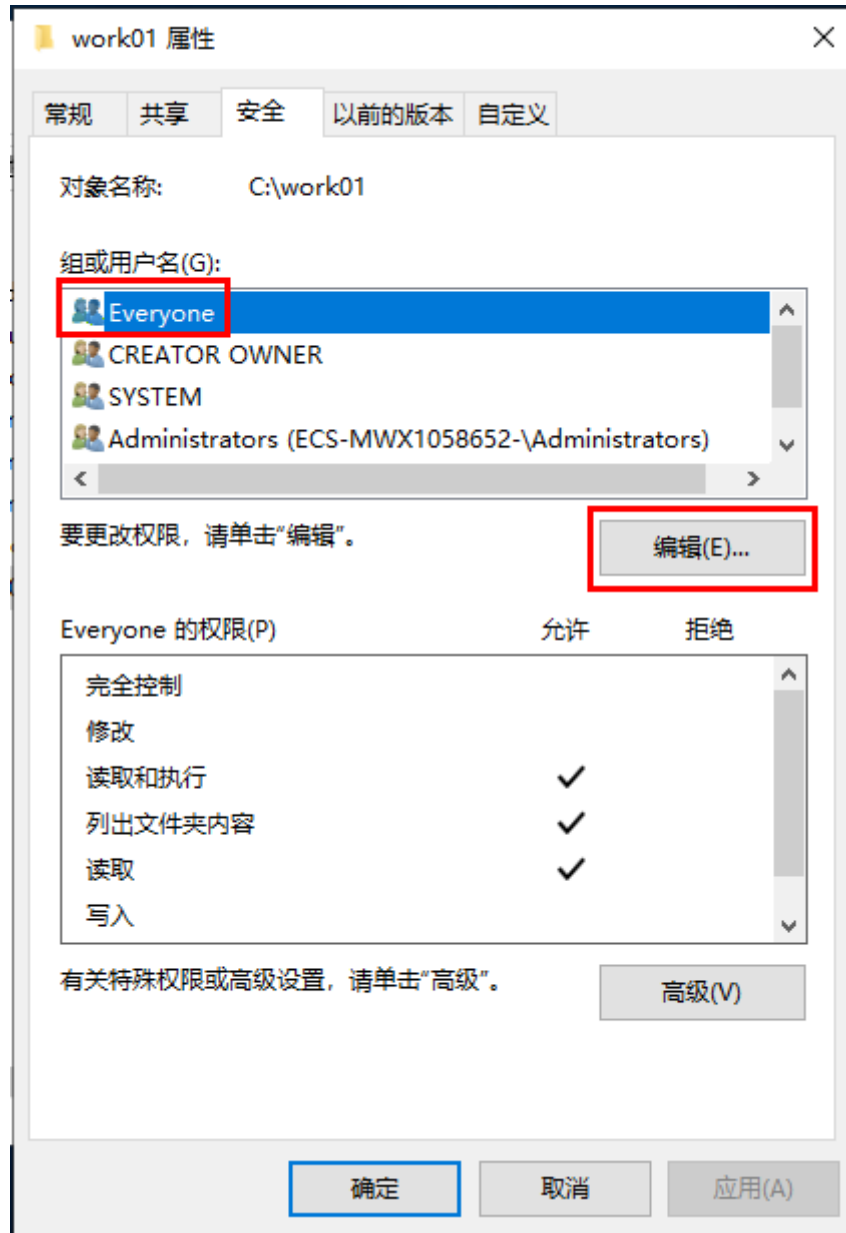
需要在FTP站点为共享给用户的文件夹设置访问及修改等权限。

1. 在服务器上创建一个供FTP使用的文件夹，选择文件夹，并单击右键选择“属性”。

此处以“work01”文件夹为例，且文件夹包含了需共享的文件test.txt。

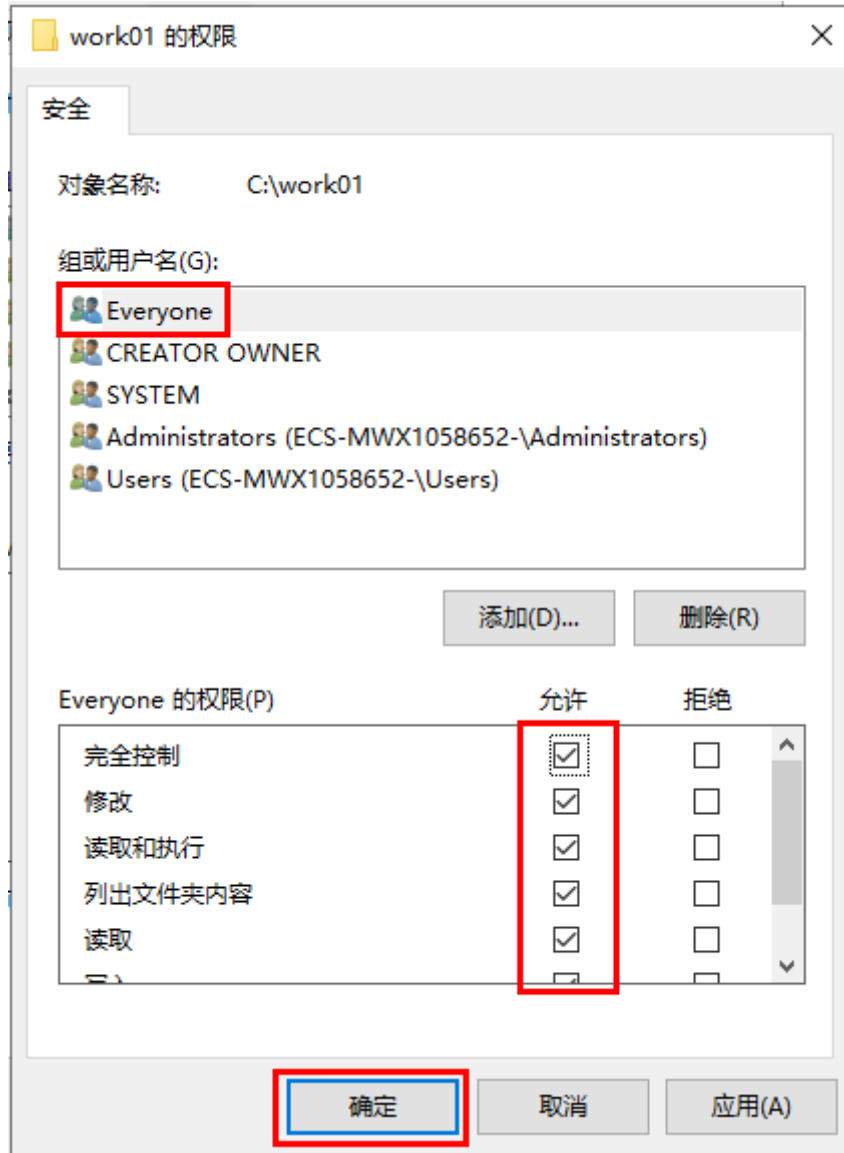
2. 在“安全”页签，选择“Everyone”，单击“编辑”。

如果没有“Everyone”用户可以直接选择，需要先进行添加，添加方法请参见[FAQ](#)。



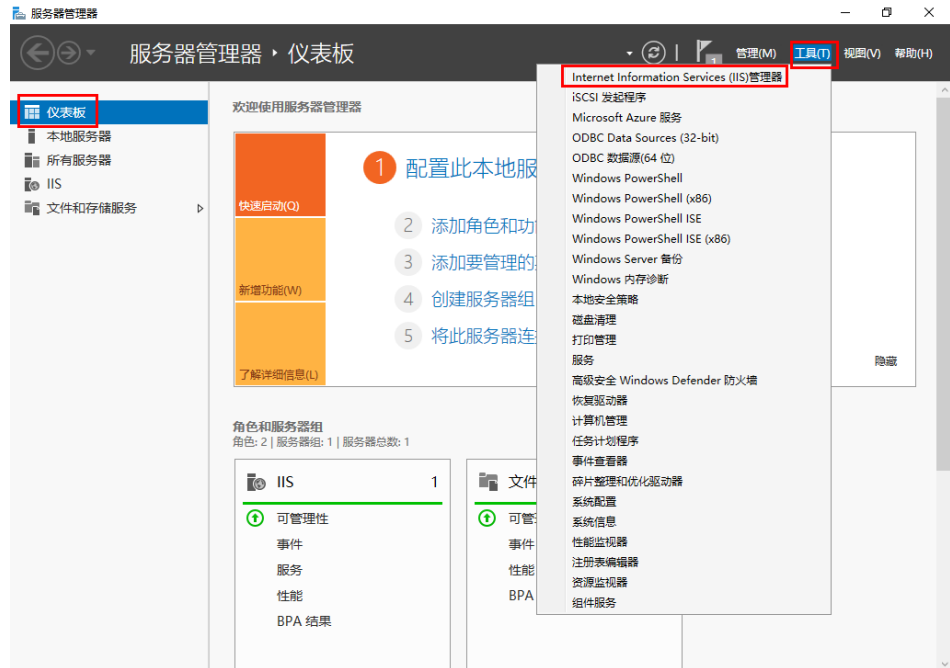
3. 选择“Everyone”，然后根据需要，选择“Everyone”的权限，并单击“确定”。  
此处以允许所有权限为例。



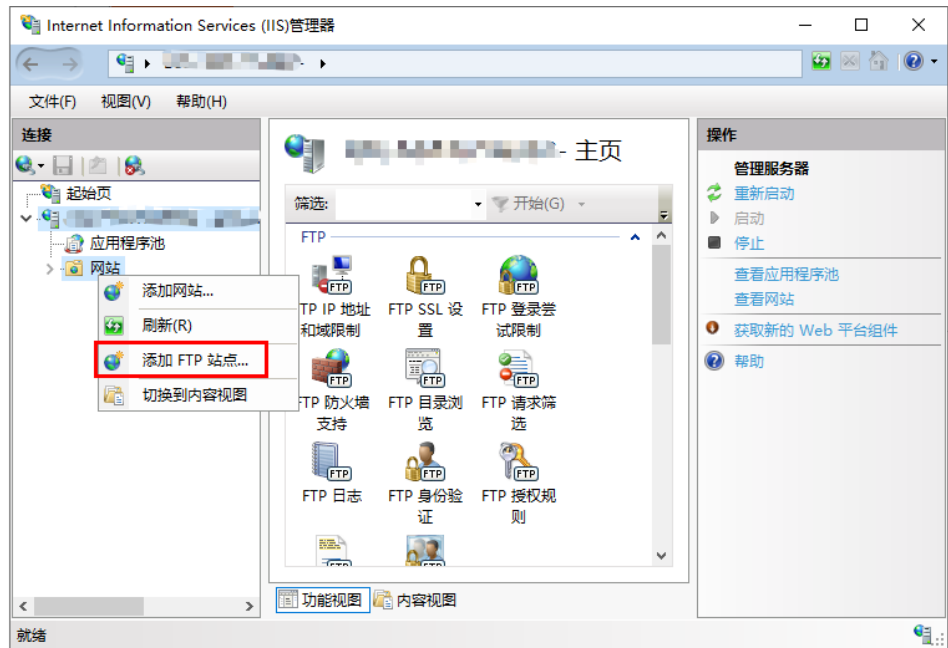


**步骤4** 添加及设置FTP站点。

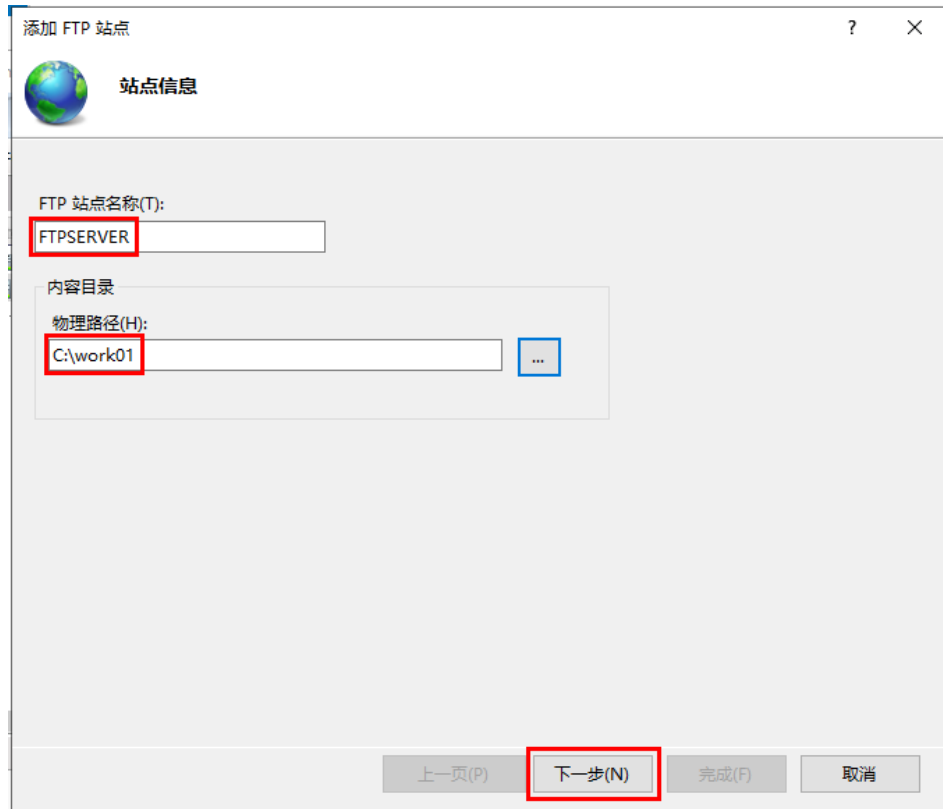
1. 在“服务器管理器”中，选择“仪表盘 > 工具 > Internet Information Services (IIS)管理器”。



2. 选择“网站”并单击右键，然后选择“添加FTP站点”。



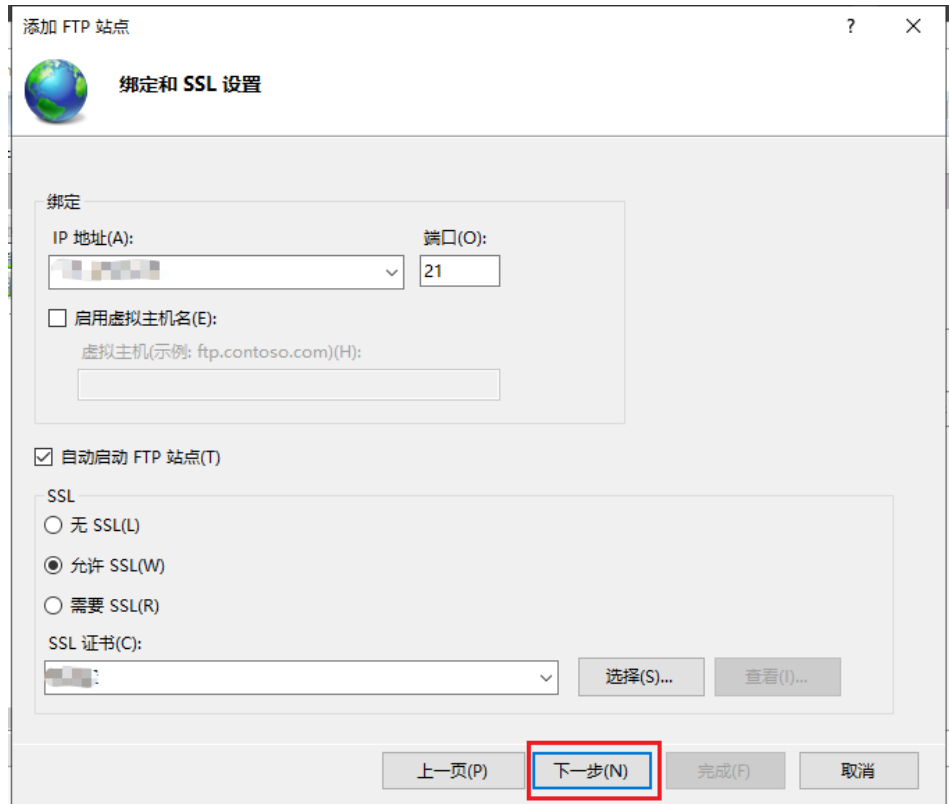
3. 在弹出的窗口中，填写FTP站点名称及共享文件夹的物理路径，然后单击“下一步(N)”。  
此处站点名称以“FTPSEVER”为例。



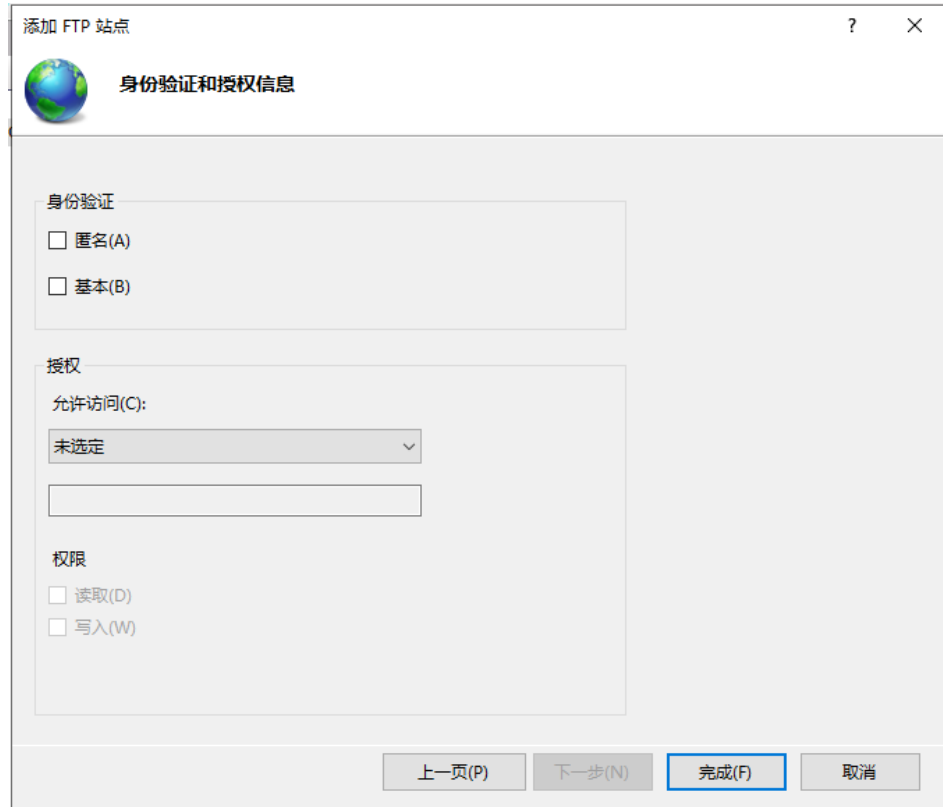
4. 输入该弹性云服务器的私有IP地址以及端口号，并设置SSL，单击“下一步(N)”。
  - 端口号 默认为21，也可自行设置。
  - SSL根据需要进行设置。
    - 无：不需要SSL加密。
    - 允许：允许FTP服务器与客户端的非SSL和SSL连接。
    - 需要：需要对FTP服务器和客户端之间的通信进行SSL加密。

#### 📖 说明

当SSL选择“允许”和“需要”时，需要选择SSL证书。可以选择已有的SSL证书，也可以制作一个SSL证书，具体制作证书的方法请参见3。

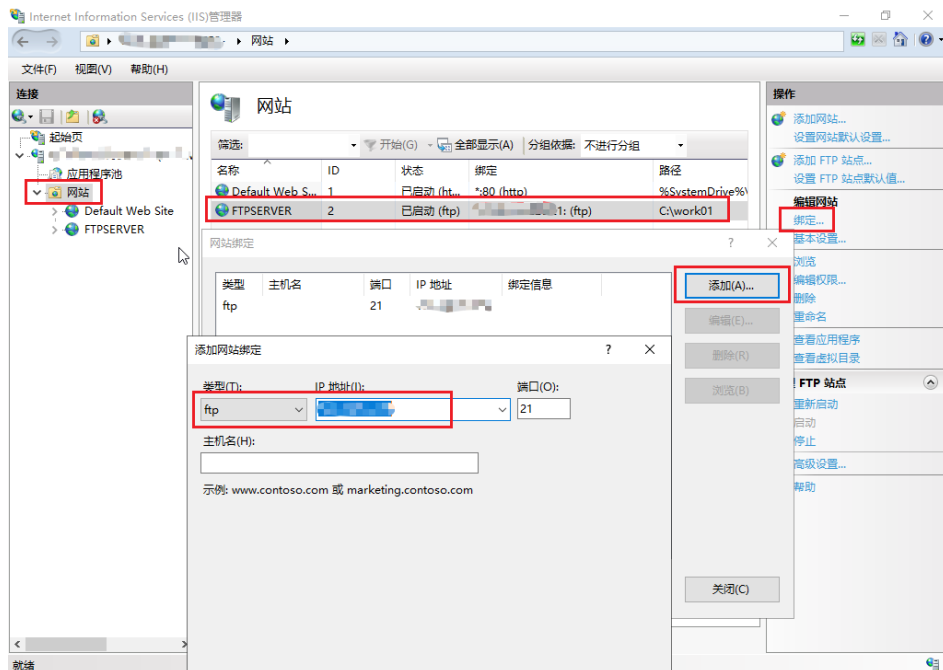


5. 设置身份认证和授权信息，并单击“完成”。
  - 身份认证
    - **匿名**：允许任何仅提供用户名“anonymous”或“ftp”的用户访问内容。
    - **基本**：需要用户提供有效用户名和密码才能访问内容。但是基本身份验证通过网络传输密码时不加密，因此建议在确认客户端和FTP服务器之间的网络连接安全时使用此身份验证方法。
  - 授权
    - 允许访问
      - **所有用户**：所有用户均可访问相应内容。
      - **匿名用户**：匿名用户可访问相应内容。
      - **指定角色或用户组**：仅指定的角色或用户组的成员才能访问相应内容。如果选择此项，需要在下面输入框中输入指定的角色或用户组。
      - **指定用户**：仅指定的用户才能访问相应内容。如果选择此项，需要在下面输入框中输入指定的用户。
    - 权限：选择经过授权的用户“读取”和“写入”权限。



6. 绑定弹性云服务器的私网IP。

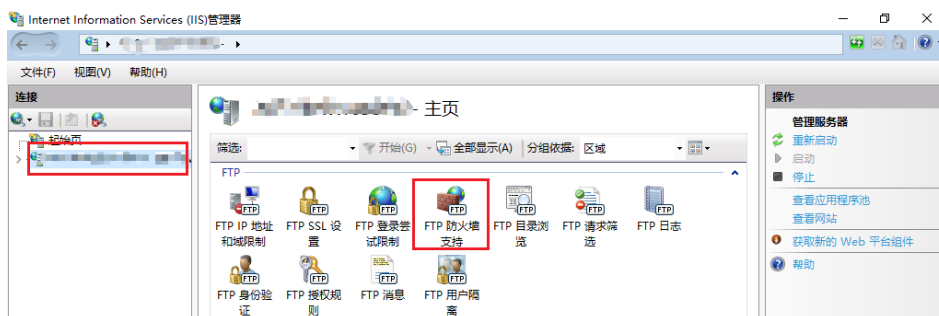
选择“网站”，选中创建的FTP站点，单击“绑定”；在弹出的“网站绑定”窗口单击“添加”，然后在弹出的窗口中添加弹性云服务器的私网IP地址，并单击“确定”。



步骤5 （可选）配置FTP防火墙支持。

- 如果需要使用FTP服务器的被动模式，则需要配置FTP防火墙支持。

- 如果华为云上的服务器需要通过公网IP地址访问华为云上的实例搭建的FTP服务器时，需要配置FTP服务器的被动模式。
1. 双击“FTP防火墙支持”，打开FTP防火墙支持的配置界面。



2. 配置相关参数，并单击“应用”。
  - 数据通道端口范围：指定用于被动连接的端口范围。可指定的有效端口范围为1025-65535。请根据实际需求进行设置。
  - 防火墙的外部IP地址：输入该弹性云服务器的公网IP地址。



3. 重启云服务器使防火墙配置生效。

#### 步骤6 设置安全组及防火墙。

搭建好FTP站点后，需要在弹性云服务器安全组的入方向添加一条放行FTP端口的规则，具体步骤参见[为安全组添加安全组规则](#)。放通的端口请参考表6-2。

如果配置了“FTP防火墙支持”，需要在安全组中同时放行FTP站点使用的端口和FTP防火墙使用的数据通道端口。

服务器防火墙默认放行TCP的21端口用于FTP服务。如果选用其他端口，需要在防火墙中添加一条放行此端口的入站规则。

表 6-2 设置安全组规则

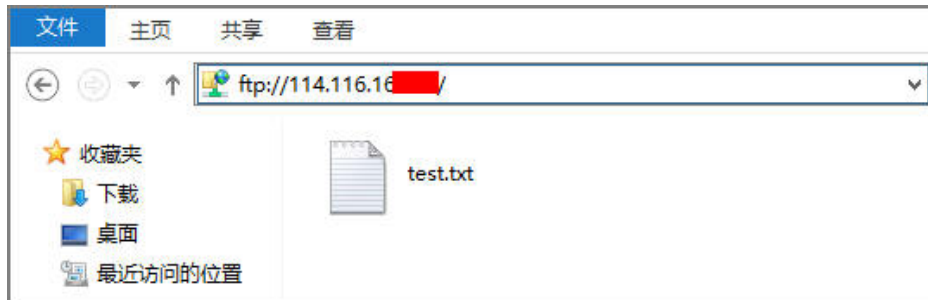
优先级	策略	类型	协议端口	源地址
1	允许	IPv4	基本协议/自定义TCP：20-21端口	0.0.0.0/0
1	允许	IPv4	基本协议/自定义TCP：1024-65535间的端口（例如5000-6000）	0.0.0.0/0

#### 步骤7 客户端测试。

打开客户端的计算机，在路径栏输入“ftp://FTP服务器公网IP地址:FTP端口”（如果不填端口则默认访问21端口）。弹出输入用户名和密码的对话框表示配置成功，正确的输入用户名和密码后，即可对FTP文件进行相应权限的操作。

### 说明

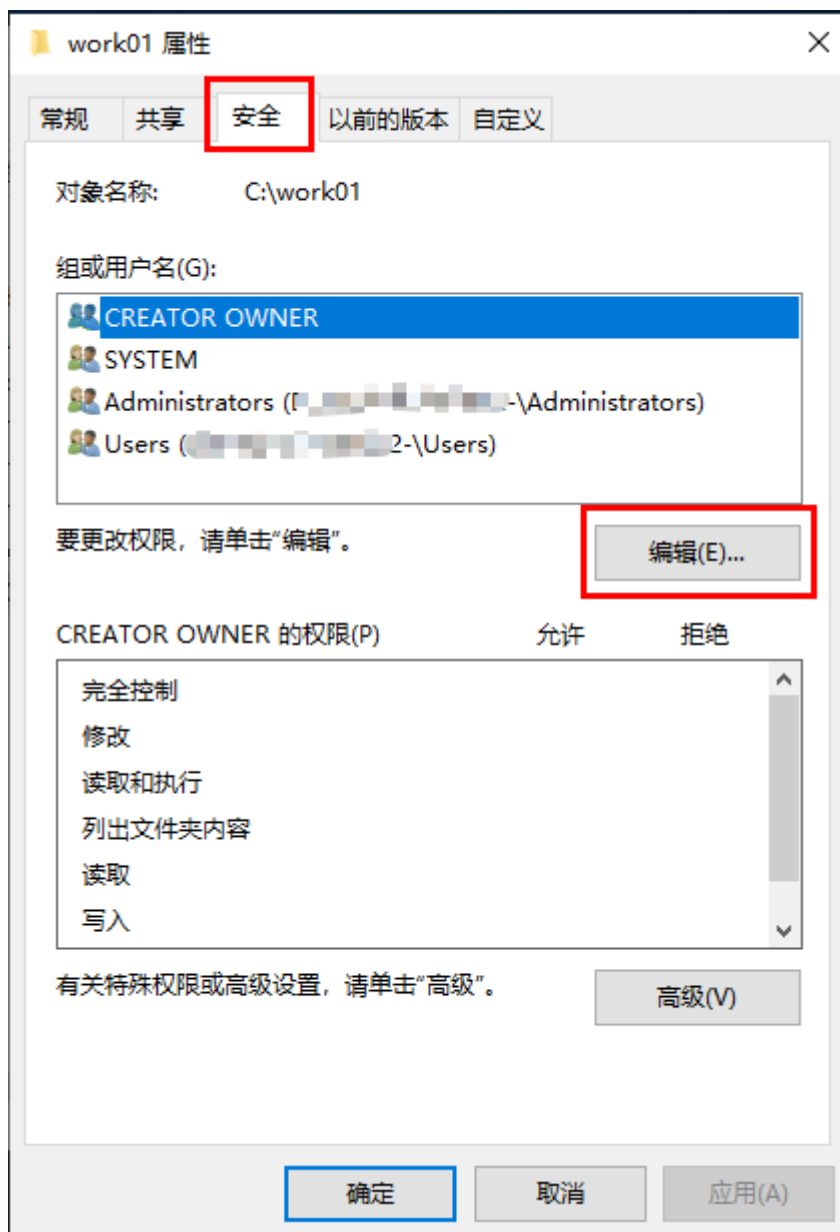
如果没有配置“FTP防火墙支持”，客户端使用此方法访问FTP站点时，需要对IE浏览器进行设置，才能打开FTP的文件夹。打开IE浏览器，选择“设置 > Internet 选项 > 高级”。勾选“启用FTP文件夹视图”，取消勾选“使用被动FTP”。



----结束

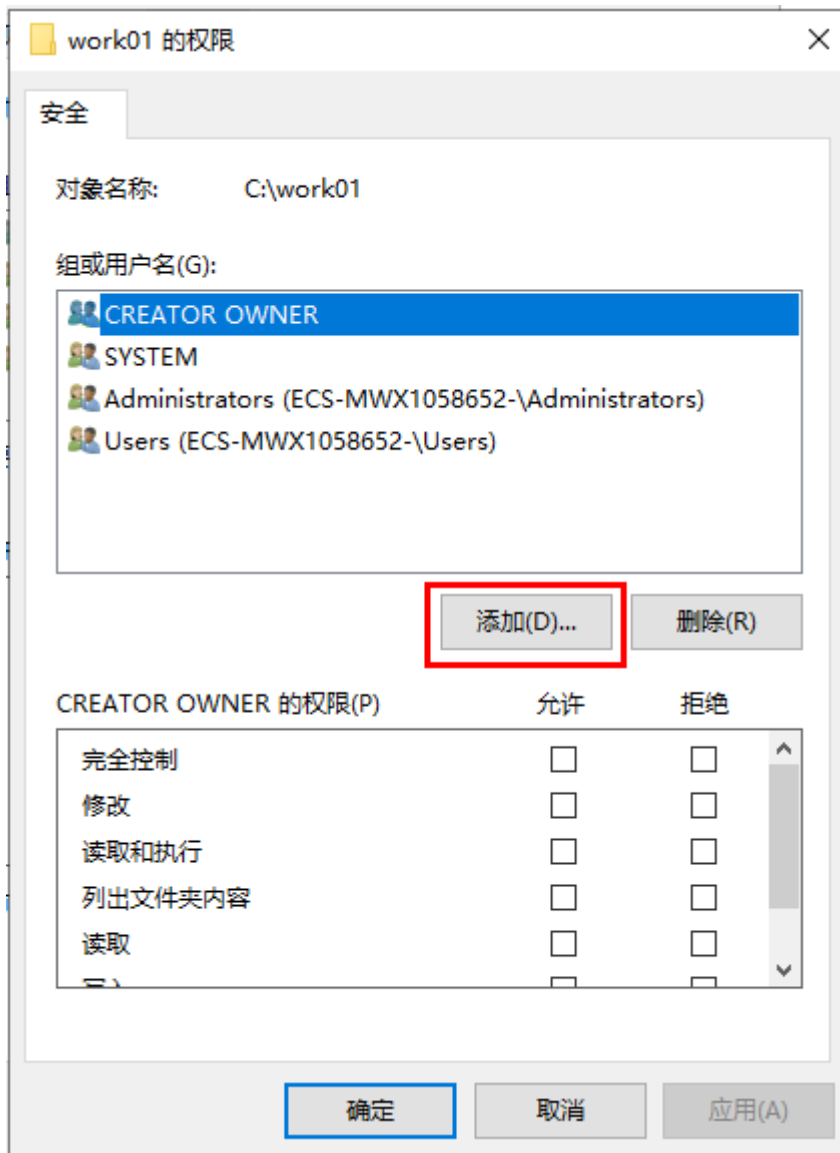
## FAQ

1. 使用Windows系统搭建FTP站点的更多信息请参见[微软官方文档](#)。
2. 如果设置文件夹的属性时，没有“Everyone”用户可直接选择，可按照如下步骤添加“Everyone”用户。
  - a. 在“安全”页签，单击“编辑”。



- b. 在新弹出的窗口中，单击“添加”。





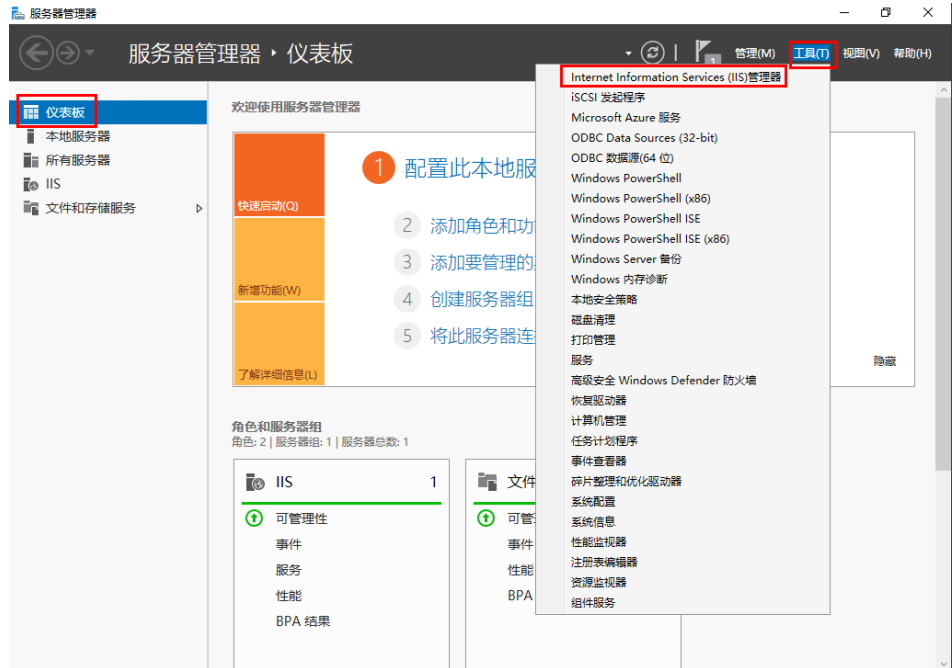
- c. 在新弹出的窗口中，单击“高级”。



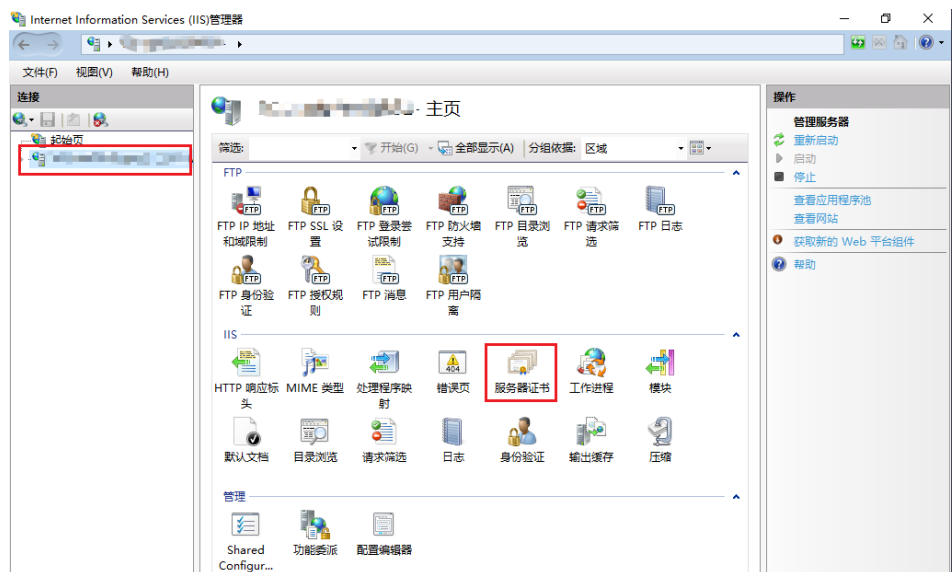
- d. 在新弹出的窗口中，单击“立即查找(N)”，然后在搜索结果中选择“Everyone”并单击“确定”。



- e. 单击“确定”，返回权限窗口。
  - f. 单击“确定”，完成添加。
3. 制作服务器证书。
- a. 在“服务器管理器”中，选择“仪表板 > 工具 > Internet Information Services (IIS)管理器”。



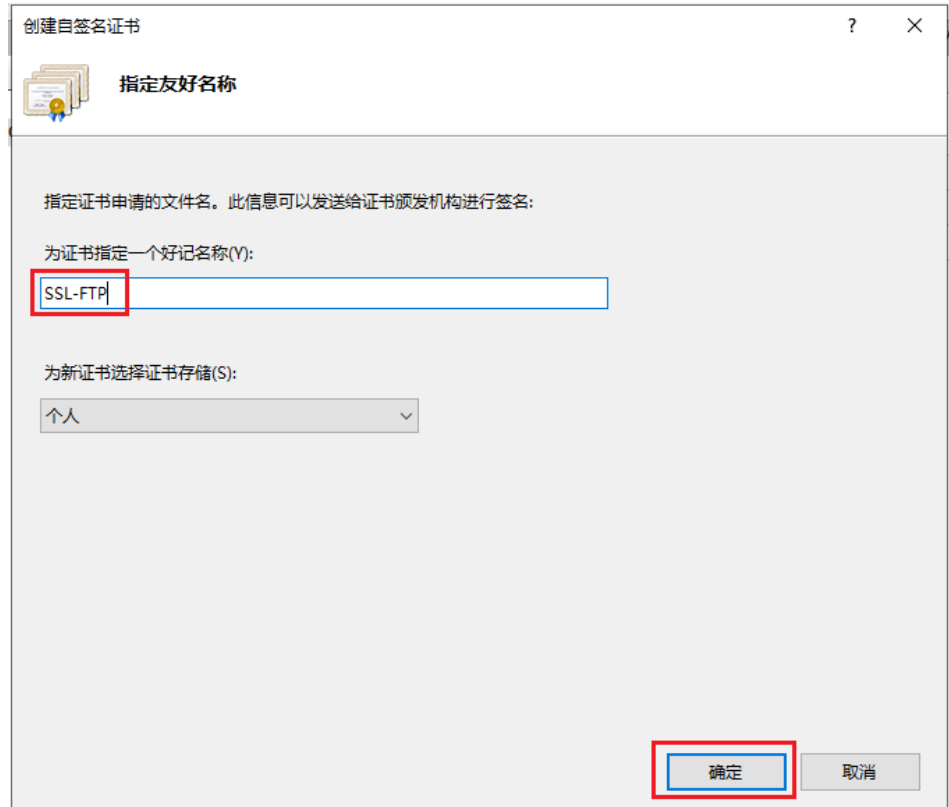
b. 在左侧列表单击服务器，然后在服务器主页“IIS”区域，双击“服务器证书”，进入“服务器证书”页面。



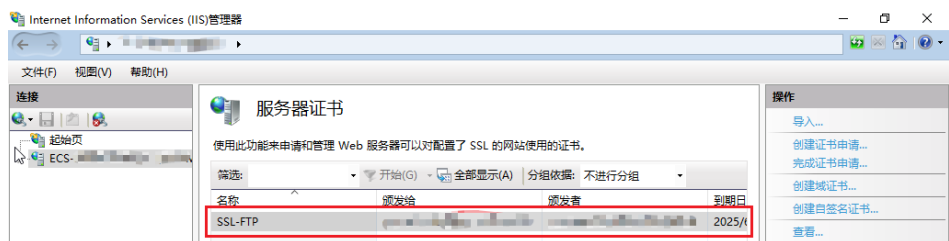
c. 单击“创建自签名证书”。



d. 输入证书的名称，并选择证书存储类型，单击“确定”。



创建成功后会在服务器证书界面显示已经创建的证书。



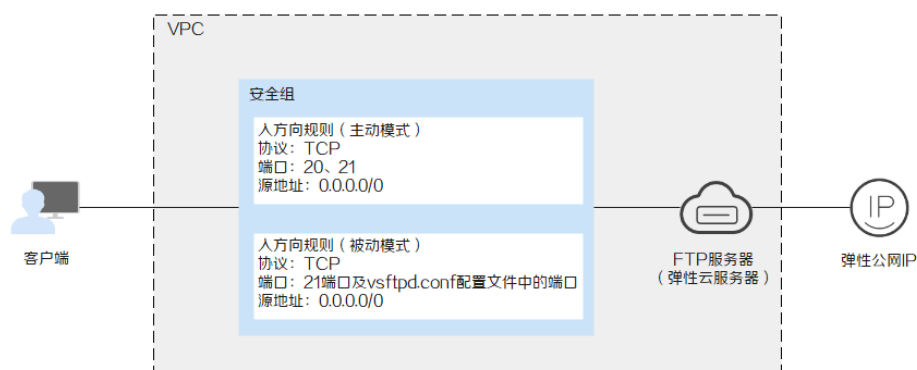
### 6.1.3 快速构建 FTP 站点 (Linux)

#### 应用场景

本文介绍了在华为云上如何使用弹性云服务器的Linux实例使用vsftpd软件搭建FTP站点。vsftpd全称是“very secure FTP daemon”，是一款在Linux发行版中使用较多的FTP服务器软件。该指导具体操作以CentOS 7.2 64位操作系统为例。

## 方案架构

图 6-1 快速搭建 FTP 站点示意图 (Linux)



## 方案优势

- 快速构建站点，组网架构简单。
- 网站安全易用。

## 资源和成本规划

表 6-3 资源和成本规划

资源	资源说明	成本说明
虚拟私有云VPC	VPC网段: 192.168.0.0/16	免费
虚拟私有云子网	<ul style="list-style-type: none"><li>• 可用区: 可用区1</li><li>• 子网网段: 192.168.0.0/24</li></ul>	免费

资源	资源说明	成本说明
安全组	入方向规则（主动模式）： <ul style="list-style-type: none"><li>● 优先级：1</li><li>● 策略：允许</li><li>● 类型：IPv4</li><li>● 协议端口：TCP: 20-21</li><li>● 源地址：0.0.0.0/0</li></ul> 入方向规则（被动模式）： <ul style="list-style-type: none"><li>● 优先级：1</li><li>● 策略：允许</li><li>● 类型：IPv4</li><li>● 协议端口：TCP: 21以及vsftpdconf配置文件中的端口</li><li>● 源地址：0.0.0.0/0</li></ul>	免费
弹性云服务器	<ul style="list-style-type: none"><li>● 计费模式：包年/包月</li><li>● 可用区：可用区1</li><li>● 规格：s6.large.2</li><li>● 镜像：CentOS 7.2 64bit</li><li>● 系统盘：40G</li><li>● 弹性公网IP：现在购买</li><li>● 线路：全动态BGP</li><li>● 公网带宽：按流量计费</li><li>● 带宽大小：5 Mbit/s</li></ul>	ECS涉及以下几项费用： <ul style="list-style-type: none"><li>● 云服务器</li><li>● 云硬盘</li><li>● 弹性公网IP</li></ul> 具体的计费方式及标准请参考 <a href="#">计费模式概述</a> 。
vsftpd	是一款免费、开源的ftp软件	免费

## 搭建 FTP 站点操作流程

Linux实例手动搭建FTP站点的具体操作步骤如下：

1. [安装vsftpd。](#)
2. [配置vsftpd。](#)
3. [设置安全组。](#)
4. [客户端测试。](#)

## 实施步骤

### 步骤1 安装vsftpd。

1. 登录弹性云服务器。
2. 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。
3. 执行以下命令安装vsftpd。

```
yum install -y vsftpd
```

回显如下类似信息时，表示软件安装成功。

```
Dependencies Resolved
=====
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: 169 k
Installed size: 348 k
Downloading packages:
vsftpd-3.0.2-22.e17.x86_64.rpm | 169 kB 00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : vsftpd-3.0.2-22.e17.x86_64      1/1
  Verifying  : vsftpd-3.0.2-22.e17.x86_64      1/1

Installed:
vsftpd.x86_64 0:3.0.2-22.e17
```

4. 执行以下命令设置FTP服务开机自启动。

```
systemctl enable vsftpd.service
```

5. 执行以下命令启动FTP服务。

```
systemctl start vsftpd.service
```

6. 执行以下命令查看FTP服务端口。

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

回显如下类似信息。

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

### 步骤2 配置vsftpd。

vsftpd安装后默认开启了匿名FTP的功能，使用匿名FTP，用户无需输入用户名密码即可登录FTP服务器，但没有权限修改或上传文件。用户如果试图使用Linux操作系统中的账号登录服务器，将会被vsftpd拒绝，但可以在vsftpd里配置用户账号和密码登录。以下操作以在vsftpd 里配置用户账号和密码登录FTP服务器为例。

1. 执行以下命令创建“ftpadmin”用户。  
此处“ftpadmin”用户为示例，可根据实际情况创建相应的用户。  

```
useradd ftpadmin
```
2. 执行以下命令并按照提示设置“ftpadmin”用户密码。  

```
passwd ftpadmin
```
3. 执行以下命令创建供FTP使用的文件目录，此处以“/var/ftp/work01”为例。  

```
mkdir /var/ftp/work01
```
4. 执行以下命令将创建的文件目录所有者改为用于登录FTP的本地用户。  

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



## 5. 修改“vsftpd.conf”配置文件。

- a. 执行以下命令打开配置文件“vsftpd.conf”。

```
vi /etc/vsftpd/vsftpd.conf
```

- b. 按i键进入编辑模式。

- c. 修改打开的“vsftpd.conf”文件。

可根据实际需求选择将FTP配置为主动模式或者被动模式。如果华为云上的服务器需要通过公网IP地址访问华为云上的实例搭建的FTP服务器时，需要将FTP服务器配置为被动模式。

- 主动模式需要配置的参数如下：

#设置以下参数，不允许匿名登录FTP服务器，允许本地用户登录FTP服务器，并指定FTP本地用户使用的文件目录。

```
anonymous_enable=NO      #不允许匿名登录FTP服务器
local_enable=YES         #允许本地用户登录FTP服务器
local_root=/var/ftp/work01 #FTP本地用户使用的文件目录
```

#设置以下参数，限制用户只能访问自身的主目录。

```
chroot_local_user=YES    #所有用户都被限制在其主目录
chroot_list_enable=YES   #启用例外用户名单
chroot_list_file=/etc/vsftpd/chroot_list #例外用户名单
allow_writeable_chroot=YES
```

- 被动模式除了需要配置主动模式所需的所有参数外，还需要配置的参数如下：

#设置以下参数，配置FTP支持被动模式。并指定FTP服务器的公网IP地址，以及可供访问的端口范围，端口范围请根据实际环境进行设置。

```
listen=YES
listen_ipv6=NO
pasv_address=xx.xx.xx.xx #FTP服务器的公网IP地址

pasv_min_port=3000      #被动模式下的最小端口
pasv_max_port=3100     #被动模式下的最大端口
```

- d. 按Esc键退出编辑模式，并输入:wq保存后退出。

- e. 在“/etc/vsftpd/”目录下创建“chroot\_list”文件。

```
touch chroot_list
```

“chroot\_list”文件是限制在主目录下的例外用户名单。如果需要设置某个用户不受只可以访问其主目录的限制，可将对应的用户名写入该文件。如果没有例外也必须要要有“chroot\_list”文件，内容可为空。

## 6. 执行以下命令重启vsftpd服务使配置生效。

```
systemctl restart vsftpd.service
```

## 步骤3 设置安全组。

搭建好FTP站点后，需要在弹性云服务器安全组的入方向添加一条放行FTP端口的规则，具体步骤参见[为安全组添加安全组规则](#)。

表 6-4 设置安全组规则

优先级	策略	类型	协议端口	源地址
1	允许	IPv4	基本协议/自定义TCP: 20-21端口	0.0.0.0/0
1	允许	IPv4	基本协议/自定义TCP: 1024-65535间的端口（例如5000-6000）	0.0.0.0/0

#### 步骤4 客户端测试。

打开客户端的计算机，在路径栏输入“ftp://FTP服务器IP地址:FTP端口”（如果不填端口则默认访问21端口）。弹出输入用户名和密码的对话框表示配置成功，正确的输入用户名和密码后，即可对FTP文件进行相应权限的操作。

#### 📖 说明

- 如果FTP服务器配置为主动模式，客户端使用此方法访问FTP站点时，需要对IE浏览器进行设置，才能打开FTP的文件夹。打开IE浏览器，选择“工具 > Internet 选项 > 高级”。勾选“启用FTP文件夹视图”，取消勾选“使用被动FTP”。
- 使用浏览器访问FTP服务器出错时，建议您清除浏览器缓存后再尝试。

----结束

## 6.1.4 搭建 FTP 站点（Huawei Cloud EulerOS 2.0）

### 简介

vsftpd（very secure FTP daemon）是Linux下的一款小巧轻快、安全易用的FTP服务器软件。本教程介绍如何在HCE 2.0上安装并配置vsftpd。

### 准备工作

- 准备一台ECS实例，并分配公网IP或者弹性公网IP（EIP）。
- 安全组的入方向规则已放行21端口。

### 操作步骤

#### 步骤1 安装vsftpd软件并启动。

1. 执行如下命令安装vsftpd。  
`dnf install vsftpd`
2. 执行如下命令启动vsftpd服务。  
`systemctl start vsftpd`
3. 执行如下命令查看服务状态。  
`systemctl status vsftpd`

如果显示**active (running)**则表示启动成功，类似效果如下图。

```
[root@hce2 ~]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-10-10 15:55:11 CST; 1s ago
     Process: 21033 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
    Main PID: 21034 (vsftpd)
       Tasks: 1 (limit: 198730)
      Memory: 408.0K
   CGroup: /system.slice/vsftpd.service
           └─ 21034 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf
```

#### 📖 说明

如果需要将vsftpd设置为开机自启动，则需要再执行如下命令。

```
systemctl enable vsftpd
```

#### 步骤2 为FTP服务添加用户。

1. 执行如下命令为FTP服务创建一个用户。

```
adduser ftp
```

2. 执行如下命令为ftp用户设置密码。

```
passwd ftp
```

### 步骤3 配置vsftpd服务。

1. 执行如下命令为FTP服务创建目录和文件（可根据个人需要修改目录）。

```
mkdir -p /data/ftp/  
touch /data/ftp/test.txt
```

2. 执行如下命令将上述目录的拥有者设置为新用户。

```
chown -R ftp:ftp /data/ftp/
```

3. 打开“/etc/vsftpd/vsftpd.conf”文件，找到如下参数进行配置。

```
# 监听IPv4 sockets。  
listen=YES  
# 根据需要选择是否配置监听IPv6  
listen_ipv6=YES  
  
# 在配置文件的末尾添加下列参数：  
# 设置本地用户登录后所在目录。  
local_root=/data/ftp/hce  
#全部用户被限制在主目录。  
chroot_local_user=YES  
#开启被动模式。  
pasv_enable=YES  
pasv_address=<FTP服务器公网IP地址>  
chroot_list_enable=NO # 是否允许用户访问其他目录  
# 如果chroot_list_enable配置为YES，则需要配置该选项；该配置为一个文件，包含哪些用户可以访问其他目录  
# chroot_list_file=/etc/vsftpd/chroot_list  
# 设置被动模式下，可使用的端口范围，建议把端口范围设置在一段比较高的范围内，有助于提高访问FTP服务器的安全性。  
# 可使用的端口范围的最小值  
pasv_min_port=<port number>  
# 可使用的端口范围的最大值。  
pasv_max_port=<port number>
```

#### 说明

除上述提及的参数，其他参数保持默认值即可。

#### 注意

无论是否配置chroot\_list\_enable，都需要创建“/etc/vsftpd/chroot\_list”文件。

4. 执行如下命令重启vsftpd服务。

```
systemctl restart vsftpd
```

### 步骤4 验证。

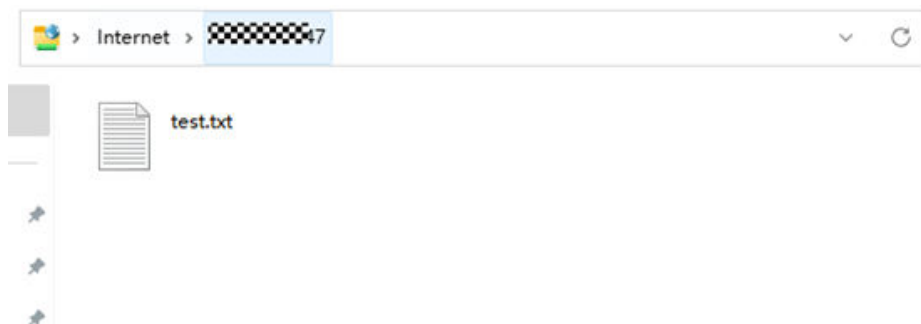
1. 执行如下命令查看vsftpd服务所使用的端口。

```
netstat -natp | grep vsftpd
```

默认情况下所使用的端口是21。

2. 在安全组界面，入方向放开21端口和上述配置的5000~5010端口。

3. 在windows文件管理器中输入ftp://<FTP服务器公网IP>:21访问FTP服务，输入密码后效果如下图。

**注意**

如果遇到以下错误，需要在“/etc/vsftpd/vsftpd.conf”文件末尾增加 allow\_writeable\_chroot=YES配置，然后再重启vsftpd服务。

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

----结束

## 6.2 搭建 Microsoft SharePoint Server 2016

### 6.2.1 购买并登录弹性云服务器

在华为云上购买弹性云服务器，并根据系统要求设置服务器规格和安装操作系统。


1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
4. 单击“购买弹性云服务器”。  
系统进入购买页。
5. 在购买页，设置弹性云服务器。  
弹性云服务器设置的具体原则请参见[自定义购买ECS](#)。

图 6-2 设置弹性云服务器规格

实例类型	规格名称	vCPUs	内存	CPU	标准 / 最大带宽	内网收发包	
<input type="radio"/>	通用计算型s6	s6.medium.2	1vCPUs	2GiB	Intel Cascade Lake 2.6GHz	0.1 / 0.8 Gbit/s	10万PPS
<input type="radio"/>	通用计算型s6	s6.medium.4	1vCPUs	4GiB	Intel Cascade Lake 2.6GHz	0.1 / 0.8 Gbit/s	10万PPS
<input checked="" type="radio"/>	通用计算型s6	s6.large.2	2vCPUs	4GiB	Intel Cascade Lake 2.6GHz	0.2 / 1.5 Gbit/s	15万PPS
<input type="radio"/>	通用计算型s6	s6.large.4	2vCPUs	8GiB	Intel Cascade Lake 2.6GHz	0.2 / 1.5 Gbit/s	15万PPS
<input type="radio"/>	通用计算型s6	s6.xlarge.2	4vCPUs	8GiB	Intel Cascade Lake 2.6GHz	0.35 / 2 Gbit/s	25万PPS
<input type="radio"/>	通用计算型s6	s6.xlarge.4	4vCPUs	16GiB	Intel Cascade Lake 2.6GHz	0.35 / 2 Gbit/s	25万PPS
<input type="radio"/>	通用计算型s6	s6.2xlarge.2	8vCPUs	16GiB	Intel Cascade Lake 2.6GHz	0.75 / 3 Gbit/s	50万PPS

图 6-3 设置网络

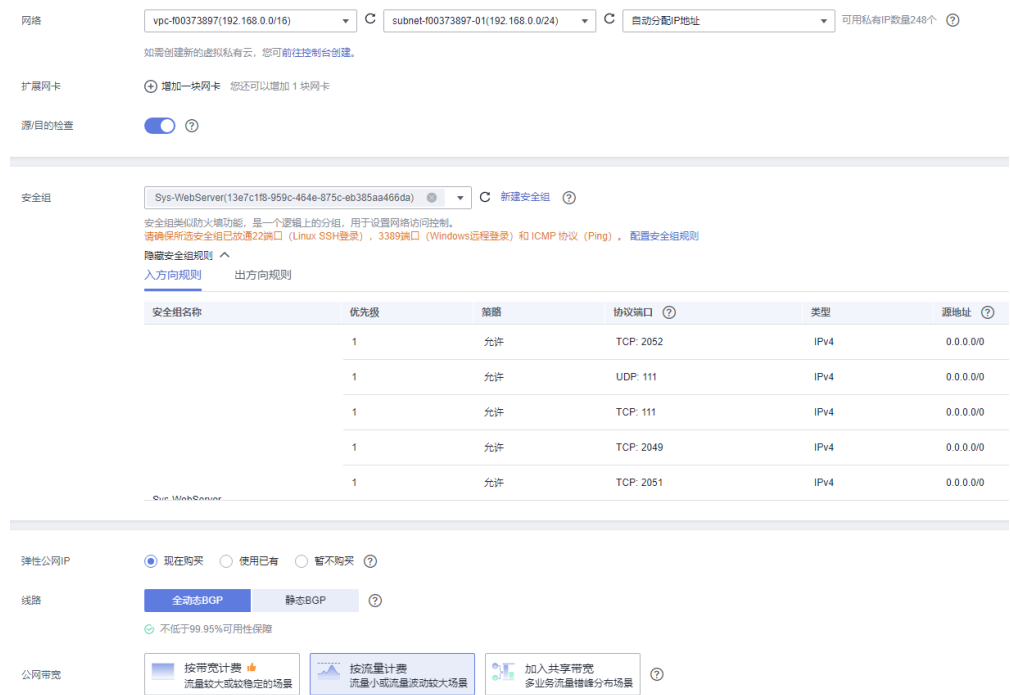


图 6-4 设置登录方式及云服务器名称

云服务器名称   允许重名

购买多台云服务器时，支持自动增加数字后缀命名或者自定义规则命名。 ?

描述  0/85

登录凭证  密码  密钥对  创建后设置

用户名 Administrator

密码 请牢记密码，如忘记密码可登录ECS控制台重置密码。

确认密码

---

云备份 使用云备份服务，需购买备份存储库，存储库是存放服务器产生的备份副本的容器。

现在购买  使用已有  暂不购买 ?

备份可以帮助您在服务器故障时恢复数据，为了您的数据安全，强烈建议您启用备份。

---

云服务器组（可选）  反亲和性 ?

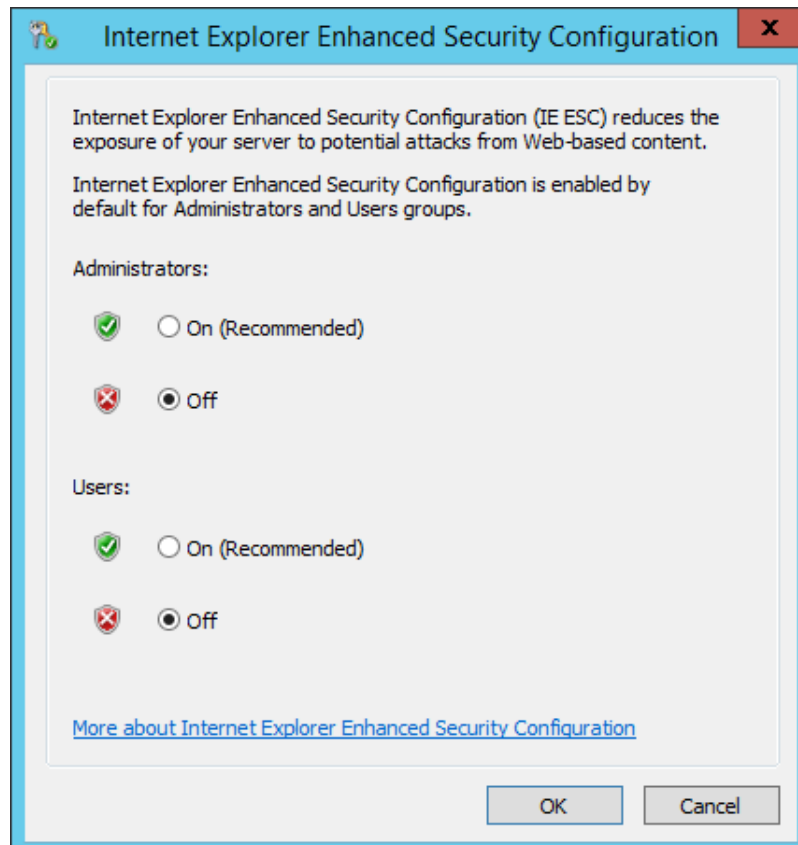
[新建云服务器组](#)

6. 确认弹性云服务器配置信息，阅读并勾选同意协议。
7. 单击“立即购买”，等待弹性云服务器创建完成。
8. 在弹性云服务器列表中，单击创建的弹性云服务器“操作”列的“远程登录”。
9. 根据界面提示，输入弹性云服务器密码，登录弹性云服务器。
10. 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。

## 6.2.2 添加 AD、DHCP、DNS、IIS 服务

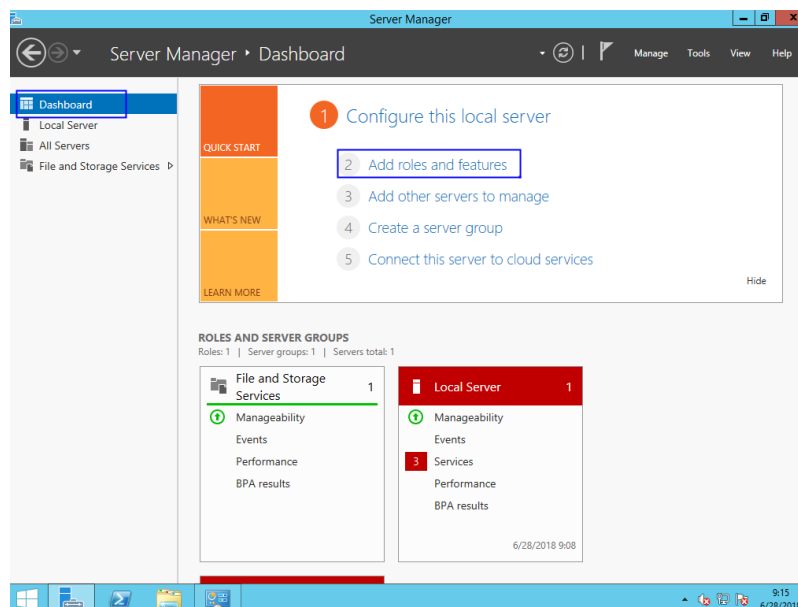
1. 在“Server Manger > Local Server”中设置“IE Enhanced Security Configuration”为“Off”，关闭IE增强安全设置。

图 6-5 IE 增强安全设置



2. 选择“Server Manger > Dashboard”。
3. 单击“Add roles and features”，为服务器添加新的角色和功能，包括DNS、DHCP、IIS、Net Framework3.5。

图 6-6 Add Roles and Features



4. 在“Server Roles”导航栏中，勾选“Active Directory Domain Services”、“DHCP Server”、“DNS Server”和“Web Server (IIS)”。

图 6-7 Select Server Roles 1

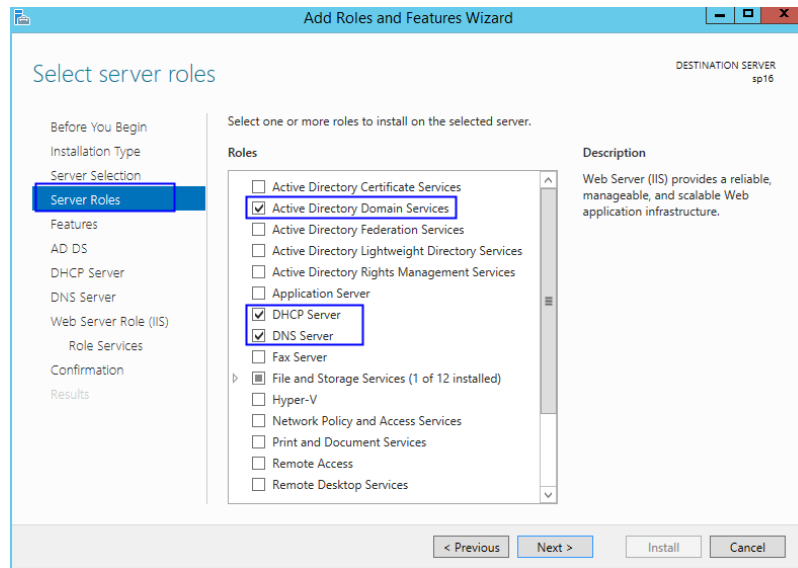
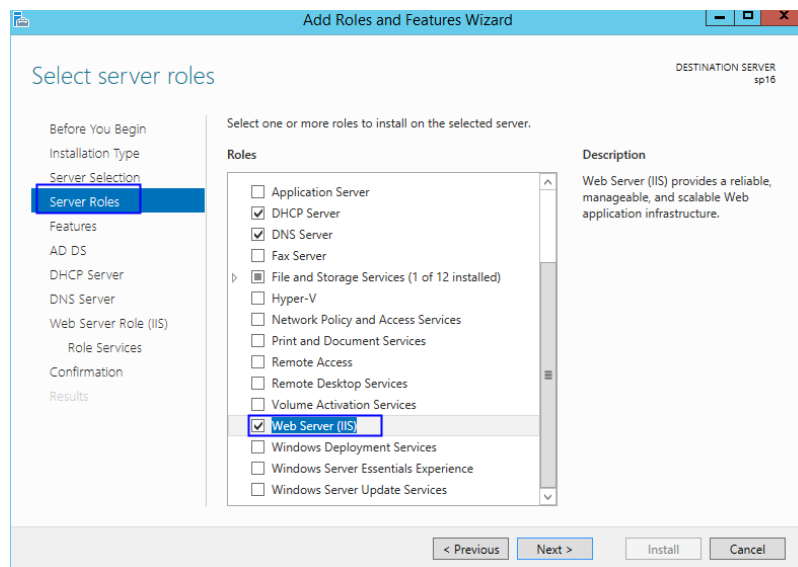


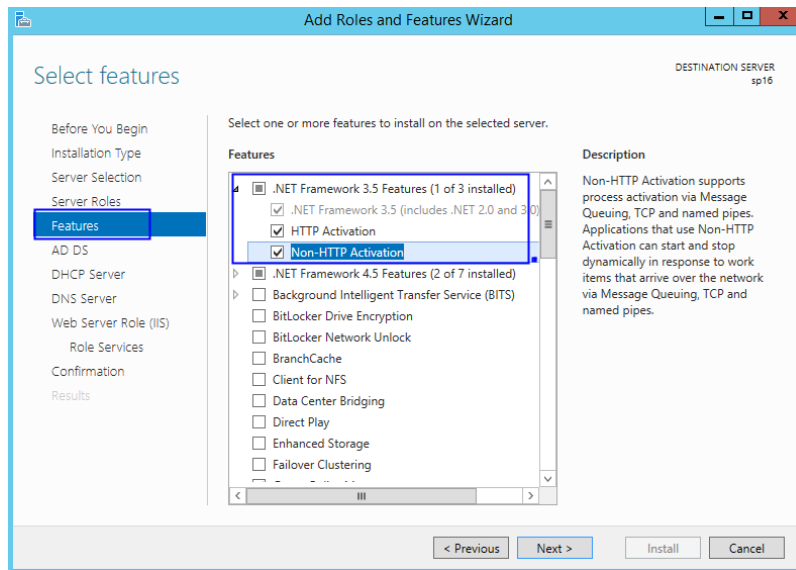
图 6-8 Select Server Roles 2



5. 单击“Next”。
6. 在“Features”导航栏中，勾选“.NET Framework 3.5 Features”。

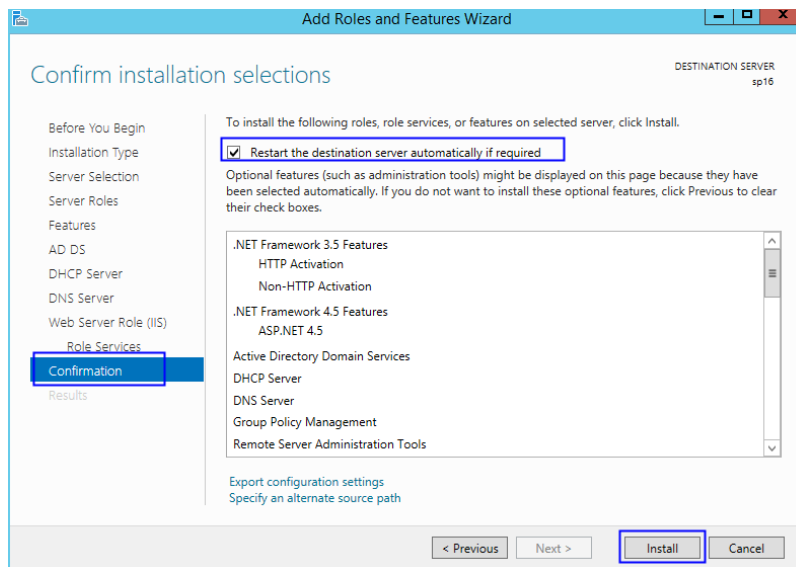


图 6-9 Select Features



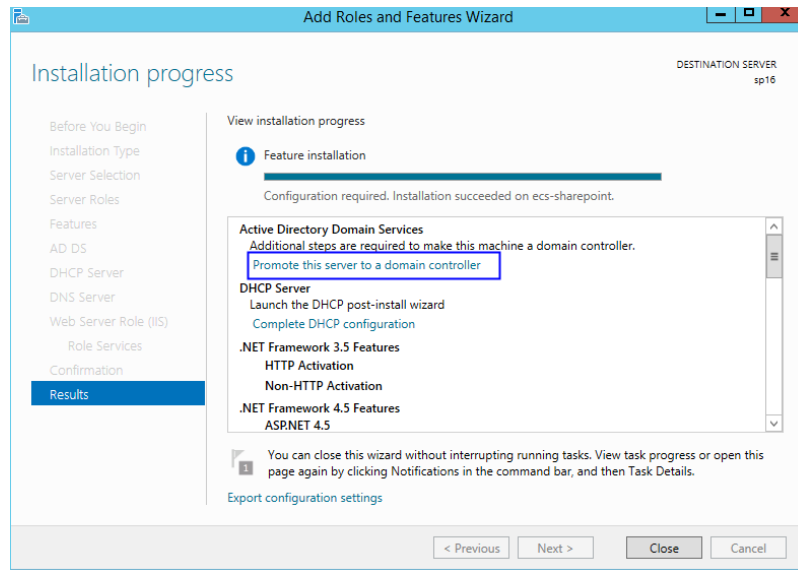
7. 单击“Next”，直至完成。
8. 在“Confirmation”导航栏中，勾选“Restart the destination server automatically if required”。

图 6-10 Confirm Installation Selections



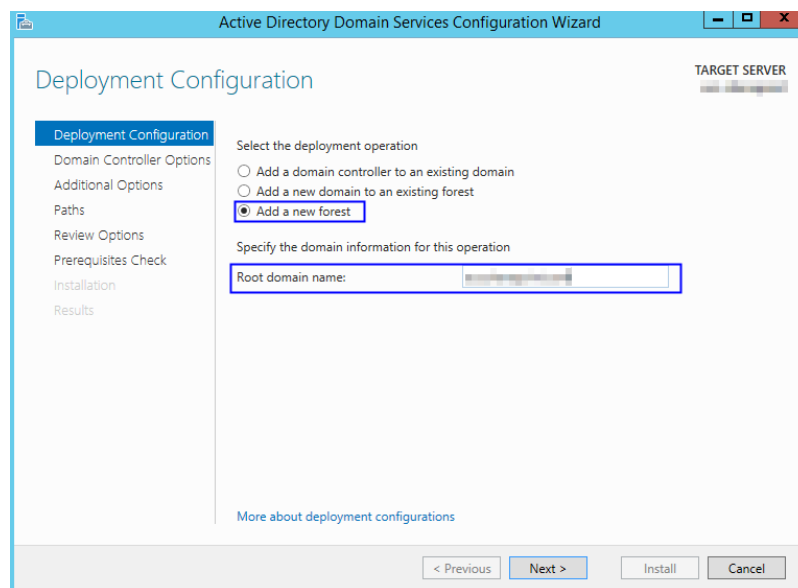
9. 单击“Install”，开始安装。
10. 安装完成后，单击“Promote this server to a domain controller”，开始配置AD服务。

图 6-11 AD Configuration



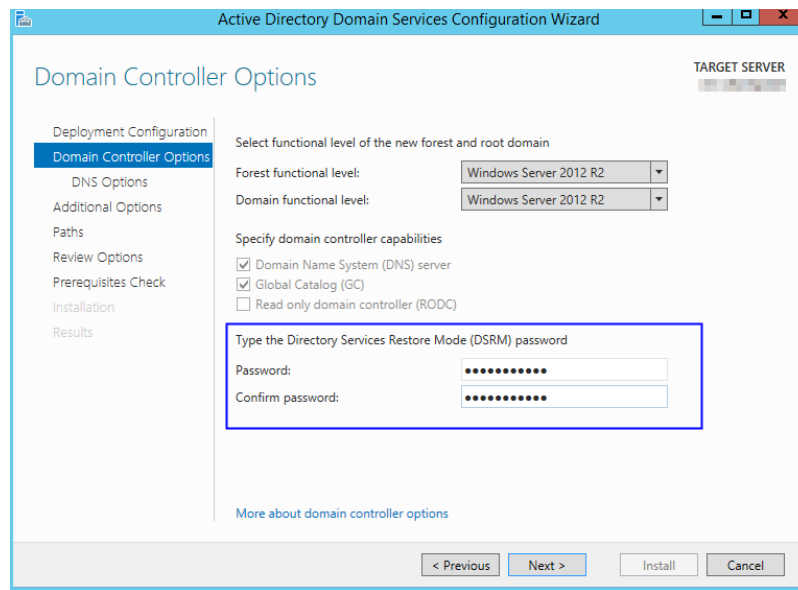
11. 因为没有已经存在的域环境，选择“Add a new forest”，创建一个新的forest。“Root domain name”设置为“sp160.com.cn”。

图 6-12 Add a new forest



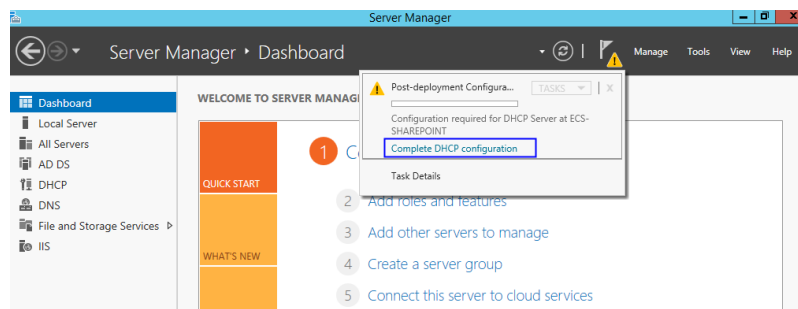
12. 单击“Next”。
13. 设置密码，该密码用于备份还原域控。

图 6-13 Set the Password



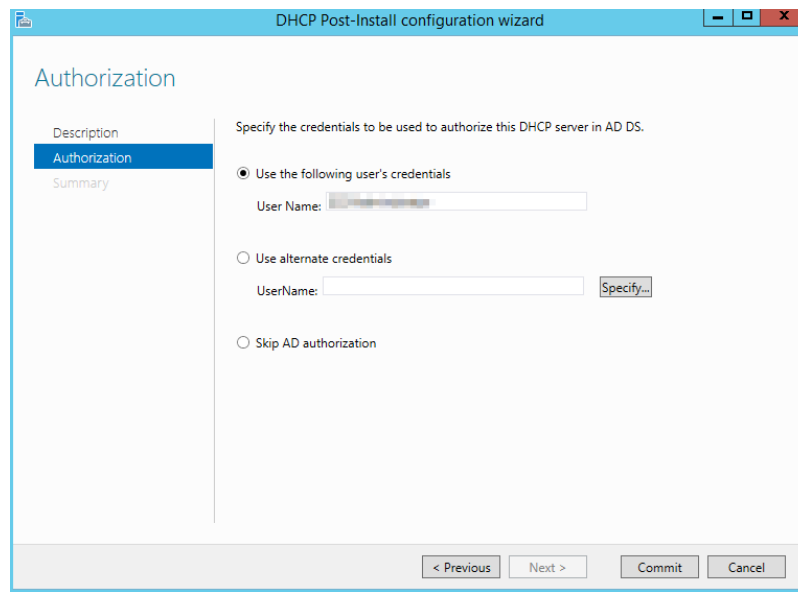
14. 单击“Next”，直至安装完成。
15. 单击“Complete DHCP Configuration”，开始配置DHCP功能。

图 6-14 DHCP Configuration 1



16. 单击“Next”，选择默认配置。

图 6-15 DHCP Configuration 2

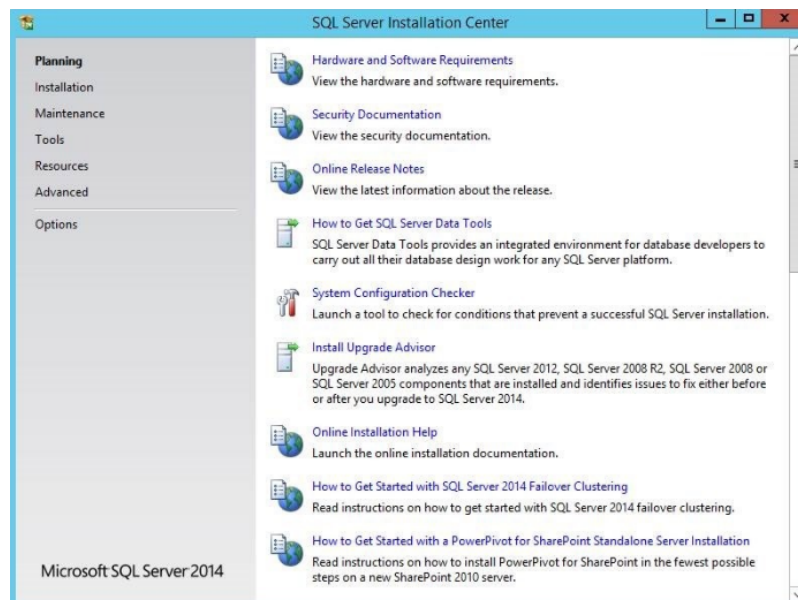


17. 单击“Commit”。
18. 配置完成，单击“Close”。

### 6.2.3 安装 SQL Server

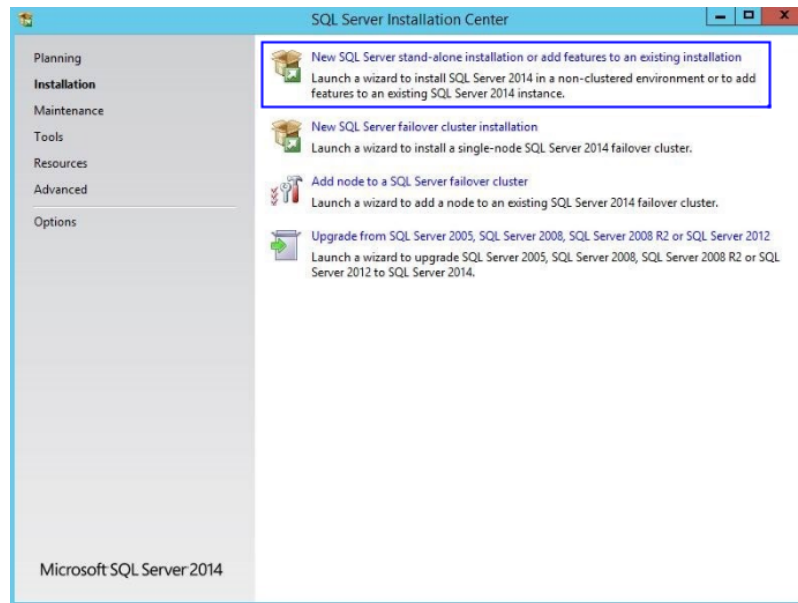
1. 双击“Setup.exe”文件，打开SQL Server安装向导。

图 6-16 SQL Server 安装向导



2. 在“Installation”导航栏中，单击第一个选项进行安装。

图 6-17 SQL Server 安装选项

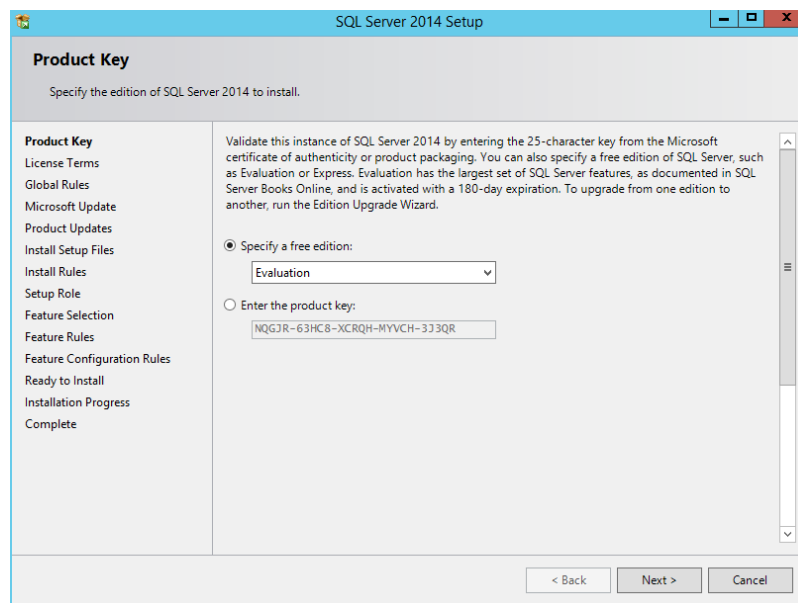


3. 选择“Specify a free edition”，采用免费镜像模式进行安装。

**说明**

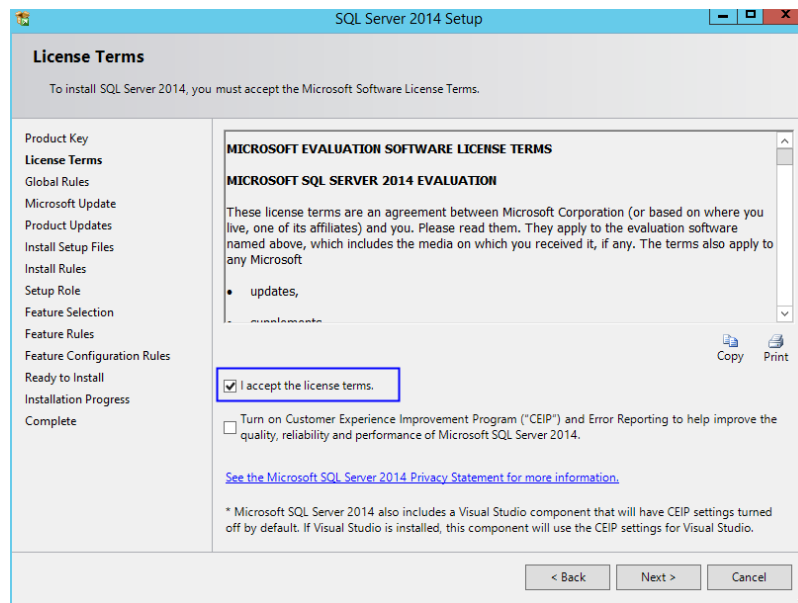
若要正式搭建Sharepoint，需要输入密钥安装SQL Server完整版本。

图 6-18 SQL Server 免费镜像



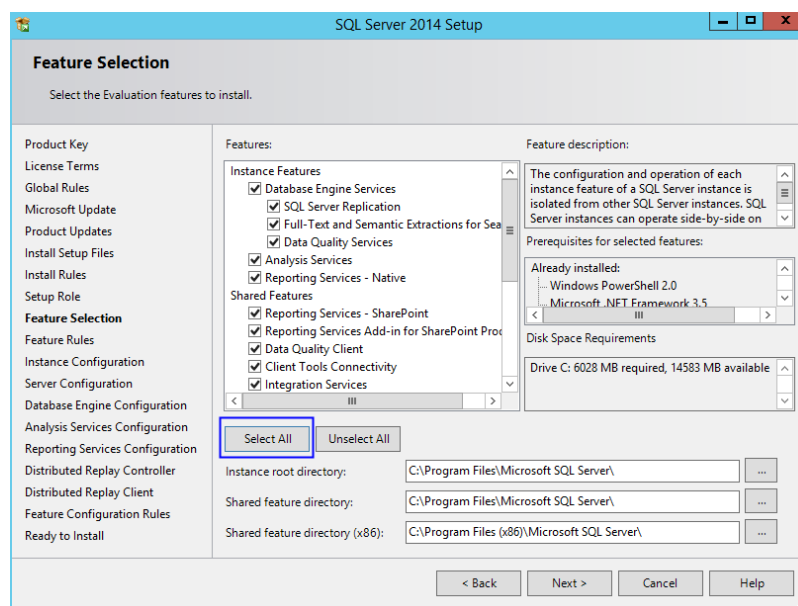
4. 勾选“I accept the license terms.”，单击“Next”。

图 6-19 SQL Server License 选项



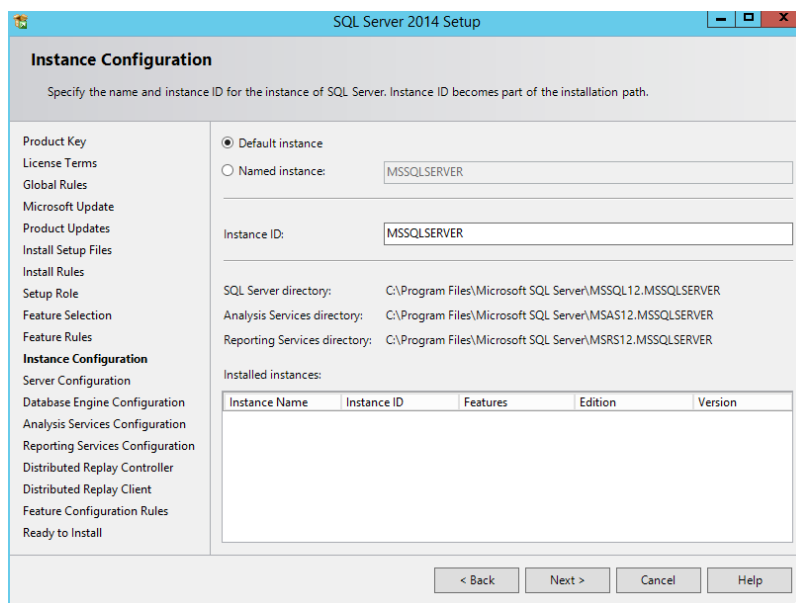
5. Microsoft Updates、Install Rules、Setup Role等安装采用系统默认项安装，单击“Next”继续安装。
6. 单击“Select ALL”选择安装全部功能，单击“Next”。

图 6-20 SQL Server Feature Selection



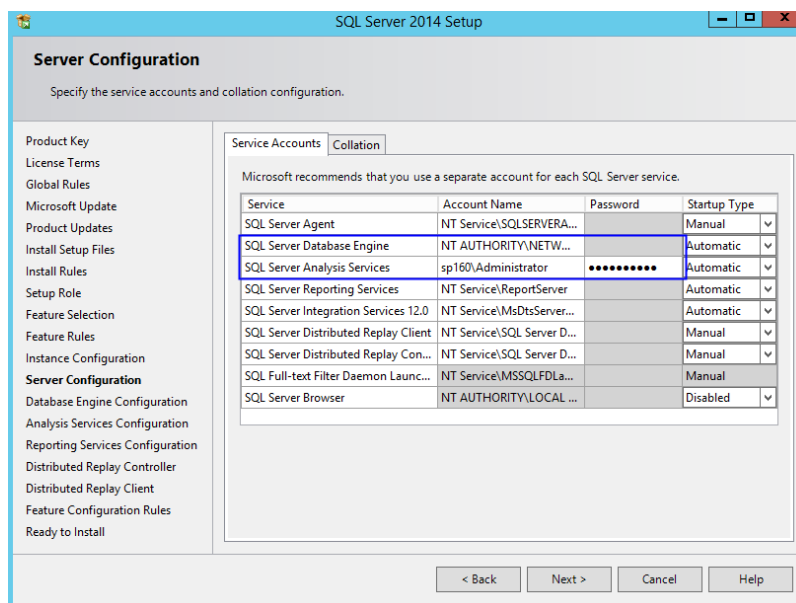
7. 勾选“Default instance”，使用默认值配置实例。

图 6-21 配置 SQL Server 实例



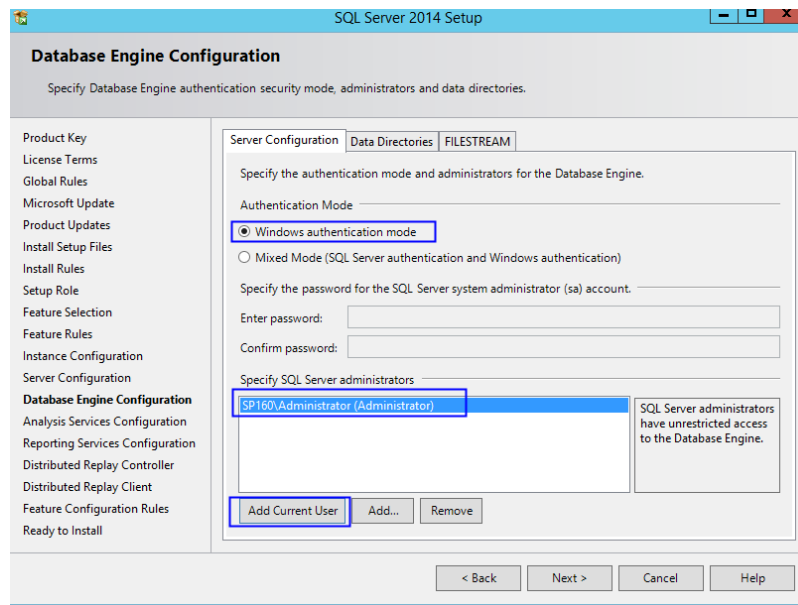
8. 设置SQL Server Configuration。
  - 修改“SQL Server Database Engine”的“Account Name”为“NT AUTHORITY\NETWORK SERVICE”。
  - 设置“SQL Server Analysis Services”为添加AD、DHCP、DNS、IIS服务中11~13设置的域账户及密码。

图 6-22 配置 SQL Server 服务账户



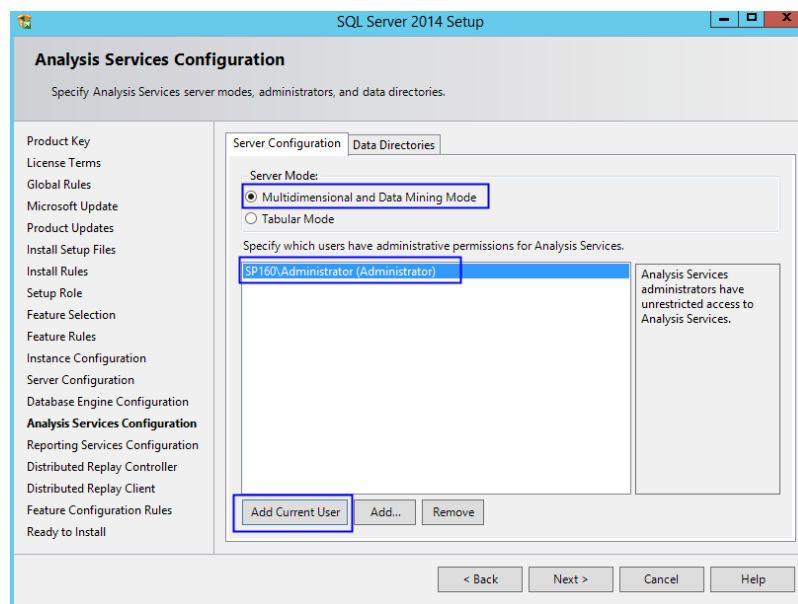
9. 单击“Add Current User”，将当前账号作为SQL Server的管理员账号，单击“Next”。

图 6-23 添加 SQL Server 管理员账号



10. 单击“Add Current User”，为当前账号添加Analysis Services的管理员权限，单击“Next”。

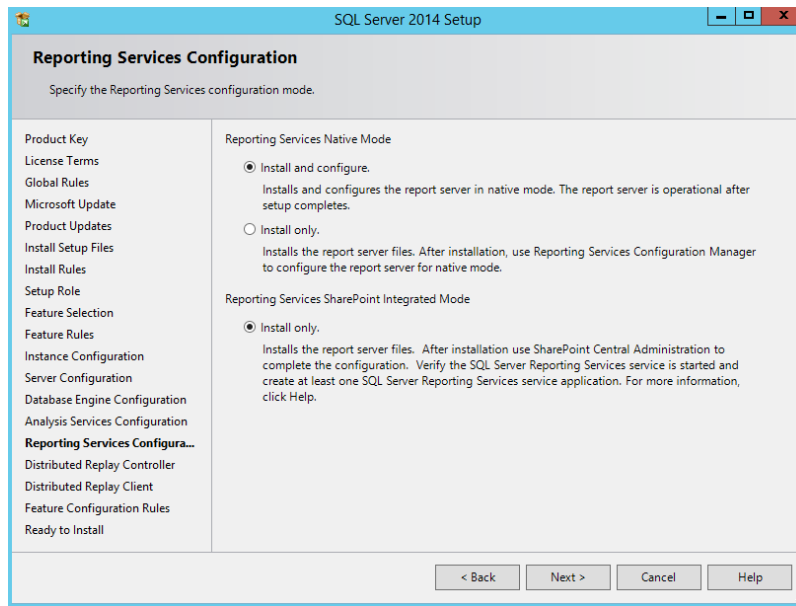
图 6-24 添加 SQL Server 管理员账号 2



11. 设置Reporting Services Configuration为默认值，单击“Next”。

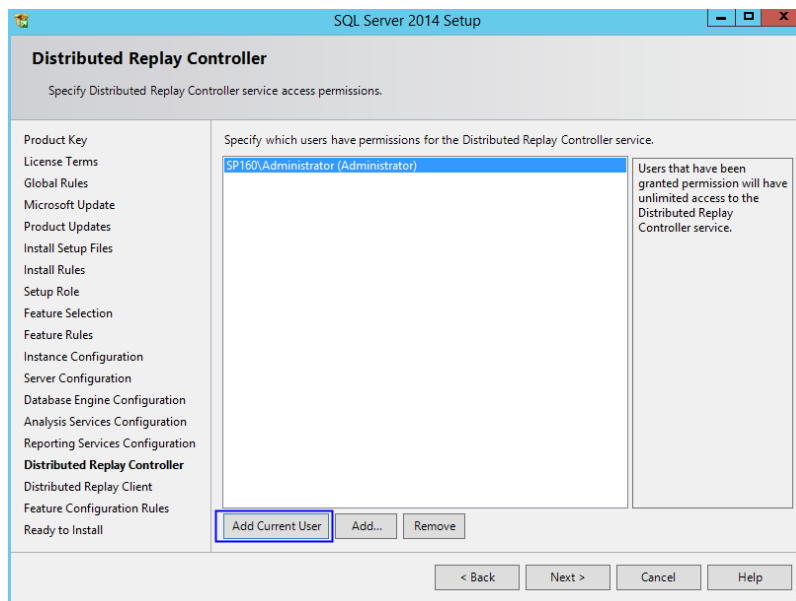


图 6-25 设置 Reporting Services Configuration



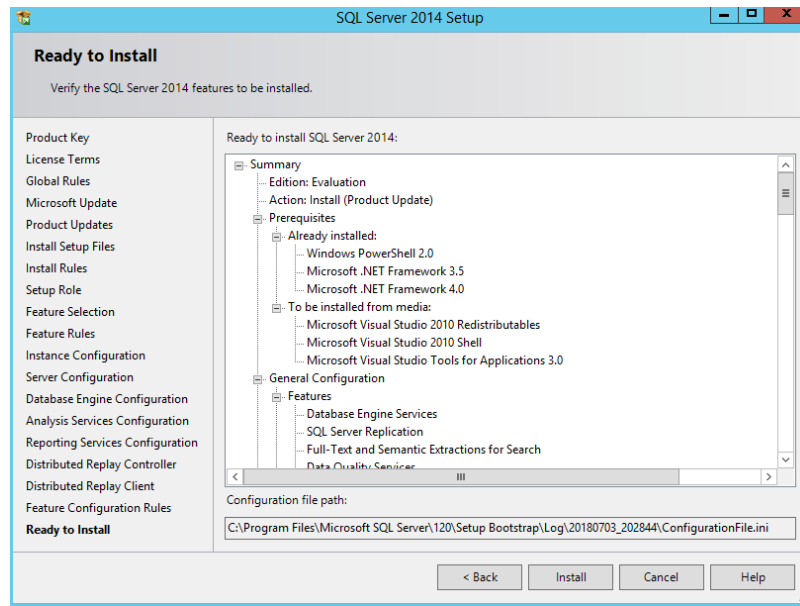
12. 单击“Add Current User”，为当前账号添加Distribution Replay Controller service的权限，单击“Next”。

图 6-26 设置 Distribution Replay Controller



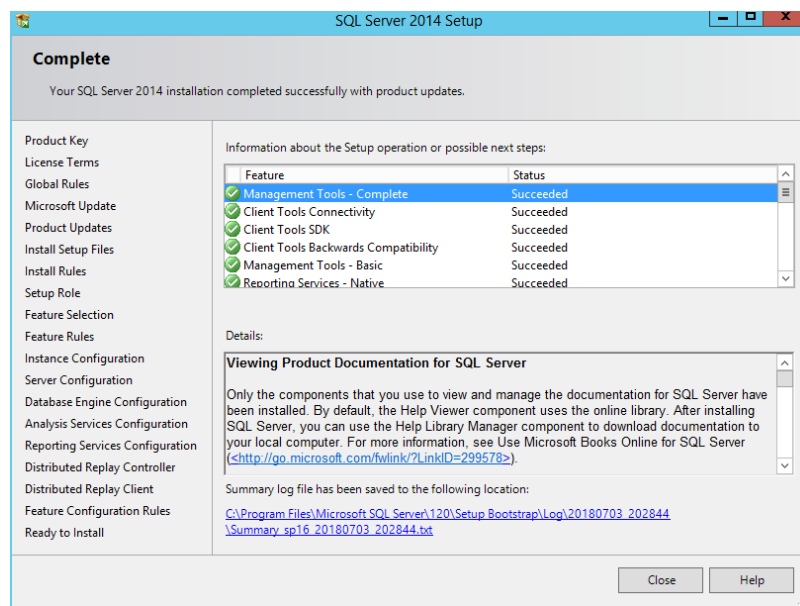
13. 确认SQL Server配置，单击“Install”开始安装。

图 6-27 SQL Server 安装准备完成



14. 单击“Close”，SQL Server安装完成。

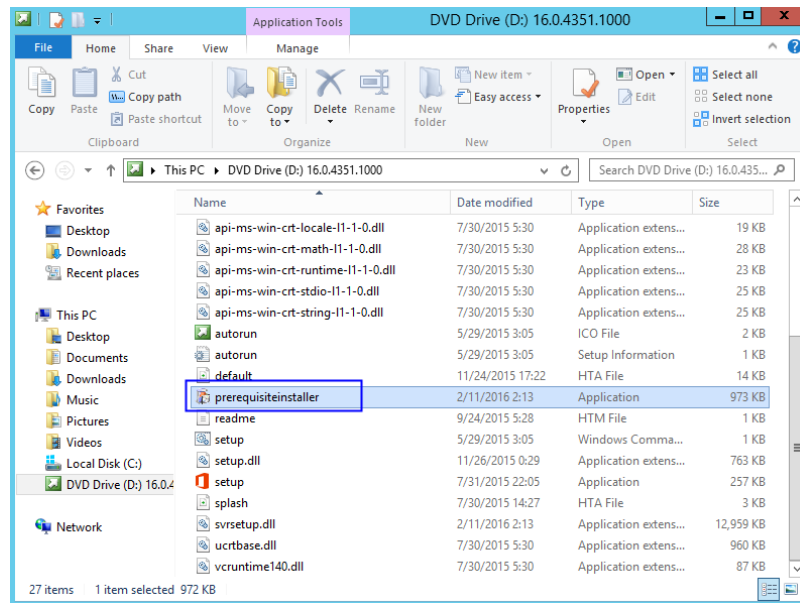
图 6-28 SQL Server 安装完成



## 6.2.4 安装 Sharepoint 2016

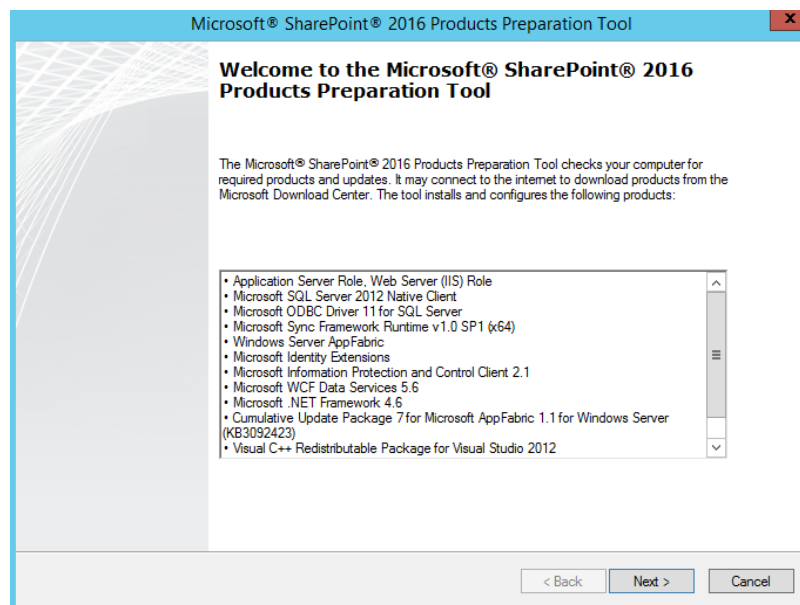
1. 打开镜像文件，双击准备工具的可执行文件，安装SharePoint 2016 准备工具。

图 6-29 Sharepoint 准备工具



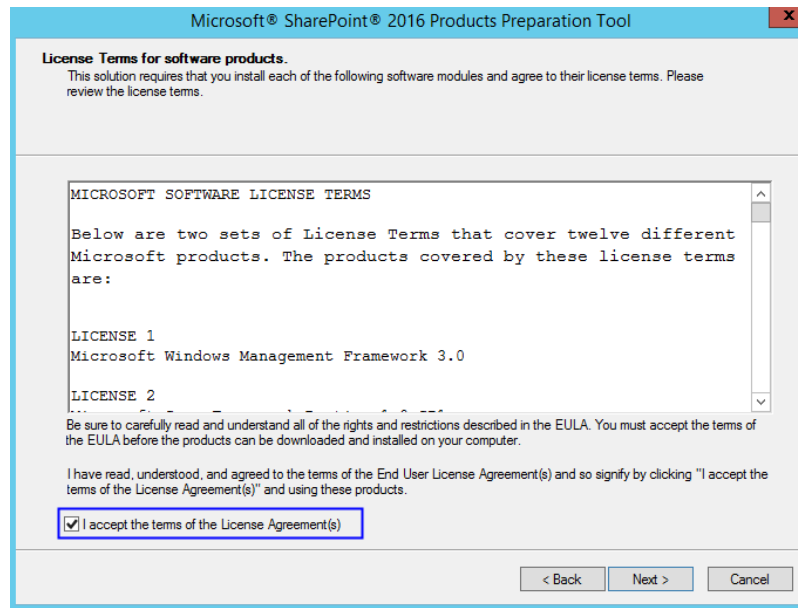
2. 打开Sharepoint准备工具的安装向导，单击“Next”。

图 6-30 Sharepoint 准备工具安装向导



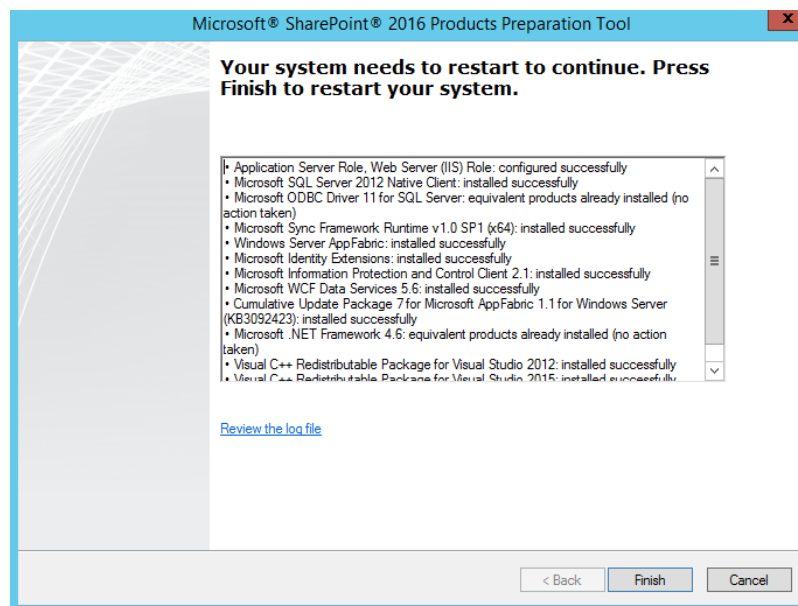
3. 勾选“I accept the terms of the License Agreement(s)”，接受License，单击“Next”。

图 6-31 Sharepoint 准备工具 License



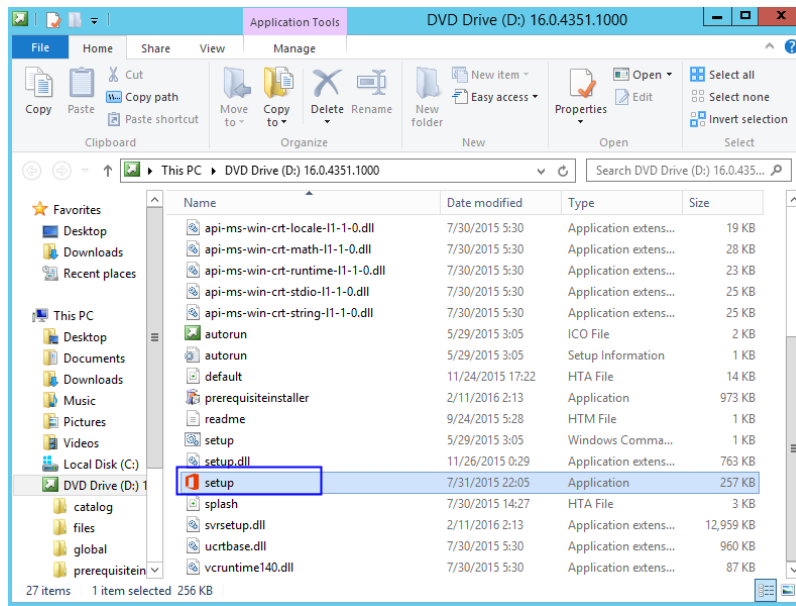
4. Sharepoint准备工具安装完成，单击“Finish”重启系统。

图 6-32 Sharepoint 准备工具安装完成



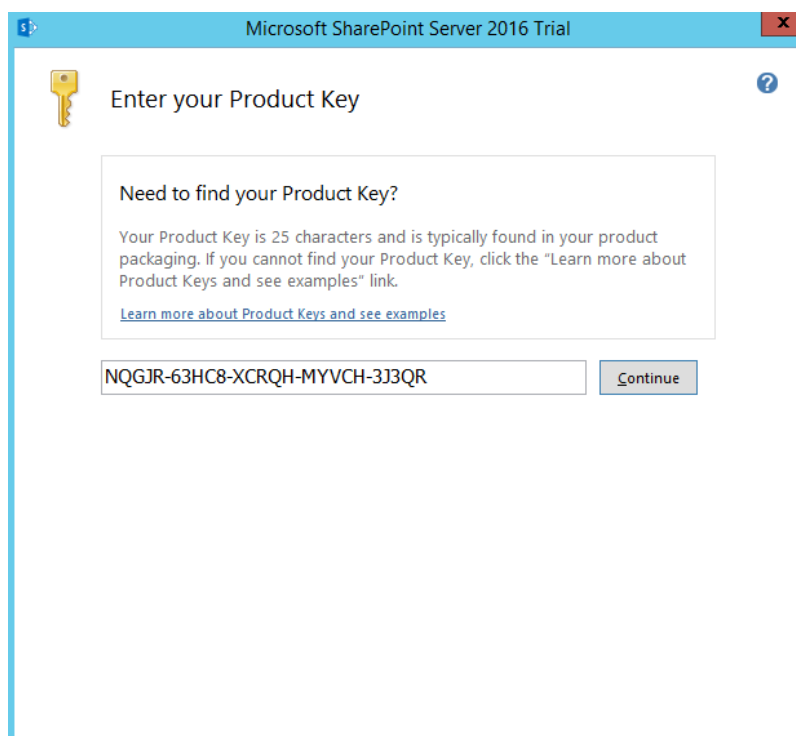
5. 双击安装文件，开始安装Sharepoint。

图 6-33 安装 Sharepoint



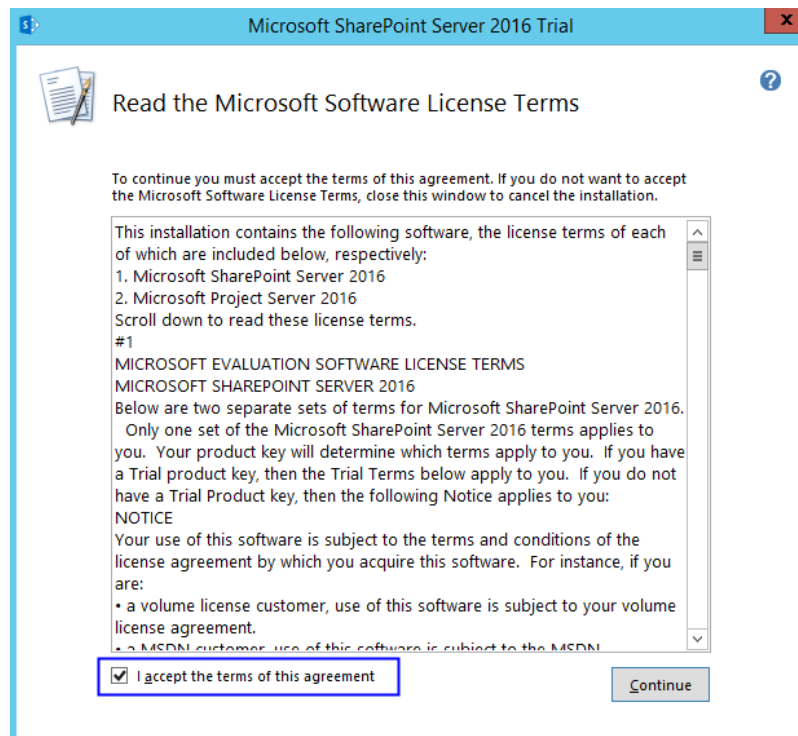
6. 输入Sharepoint产品密钥，Sharepoint 180天试用版Key为“NQGJR-63HC8-XCRQH-MYVCH-3J3QR”。

图 6-34 Sharepoint 产品密钥



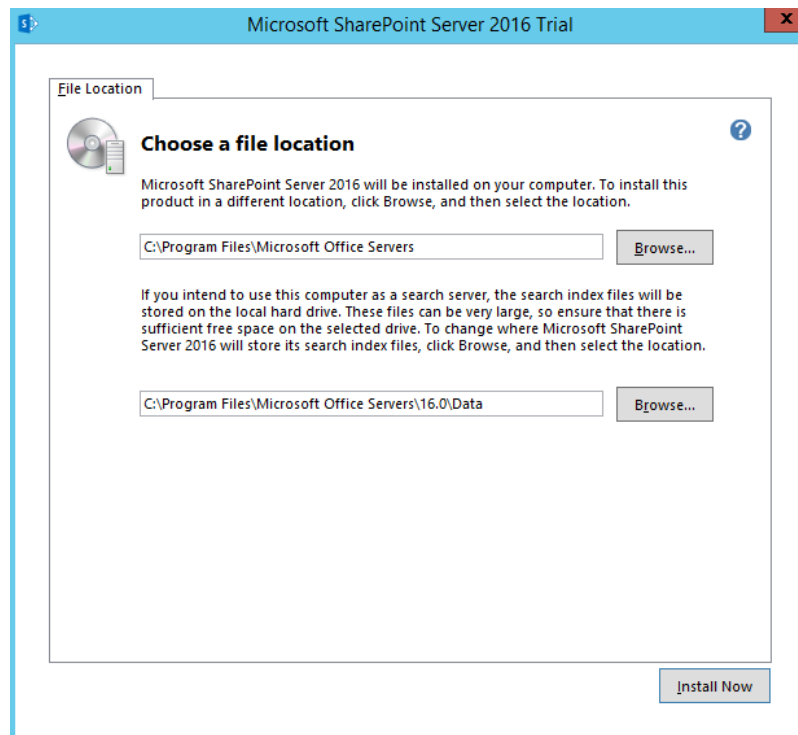
7. 接受Licesen，单击“Continue”。

图 6-35 Sharepoint License Terms



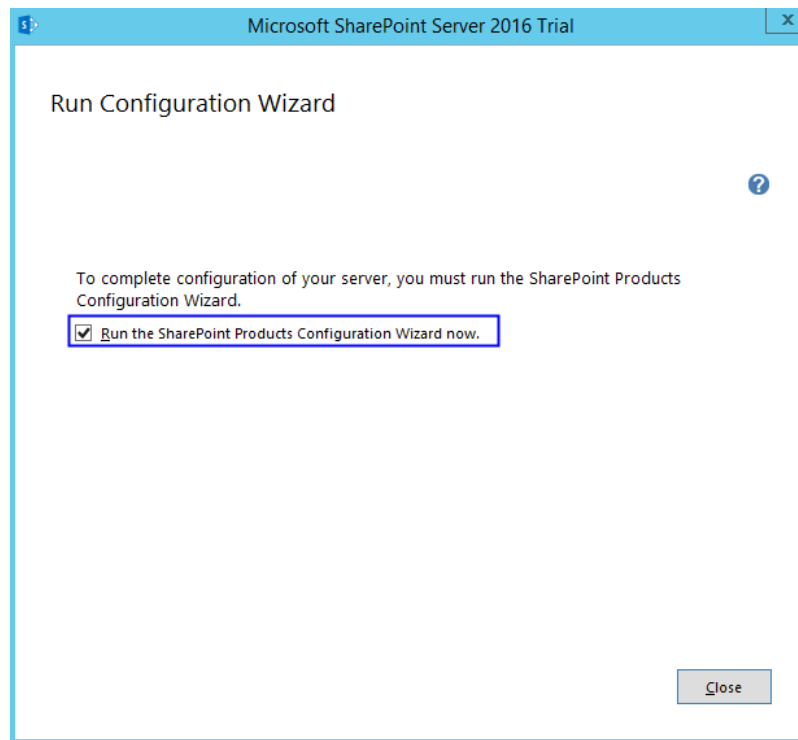
8. 选择安装文件路径，采用默认值。

图 6-36 Sharepoint 安装文件路径



9. 单击“Install Now”，开始安装。
10. Sharepoint安装完成，勾选“Run the Sharepoint Products Configuration Wizard now.”，在安装完成后运行Sharepoint产品配置向导。

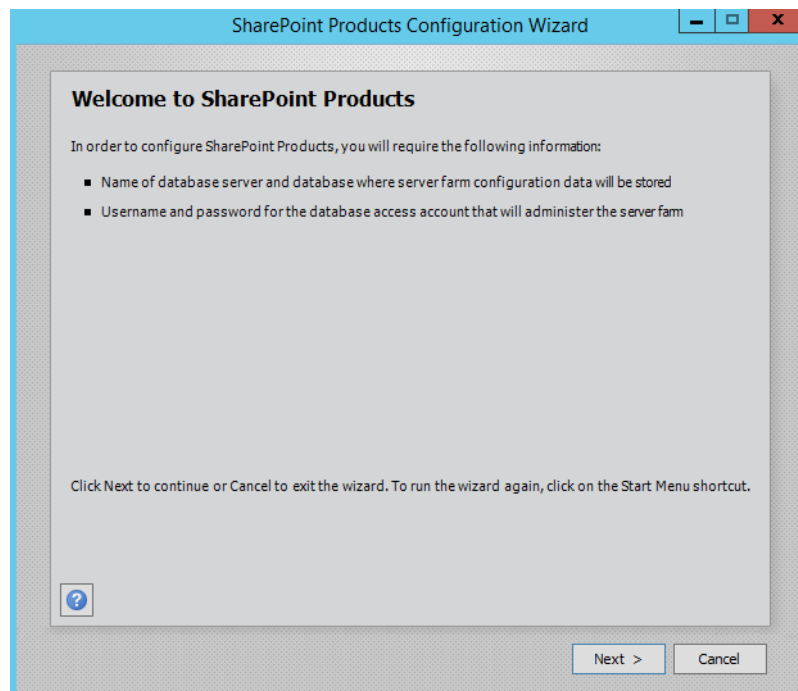
图 6-37 Sharepoint 安装完成



## 6.2.5 配置 Sharepoint 2016

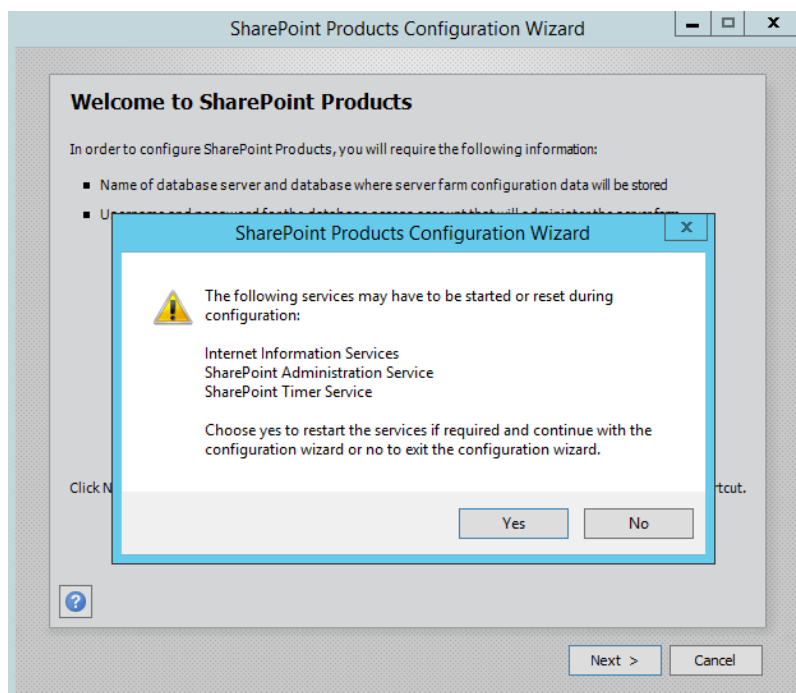
1. 在运行的Sharepoint产品配置向导中，单击“Next”。

图 6-38 Sharepoint 产品配置向导



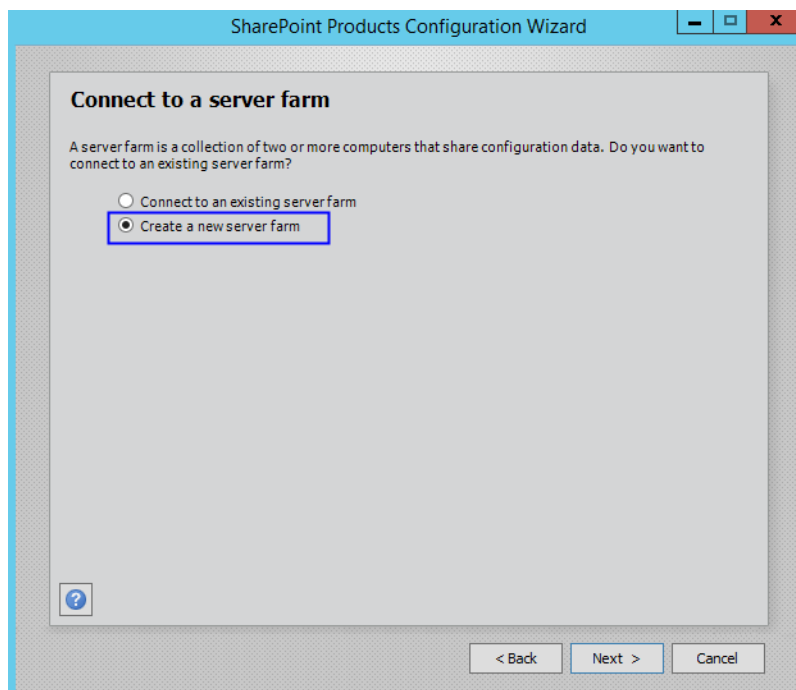
2. 单击“Yes”，允许在配置过程中重启服务。

图 6-39 重启服务提醒



3. 因为没有已经存在的服务器场，所以选择“Create a new server farm”，创建一个新的服务器场。

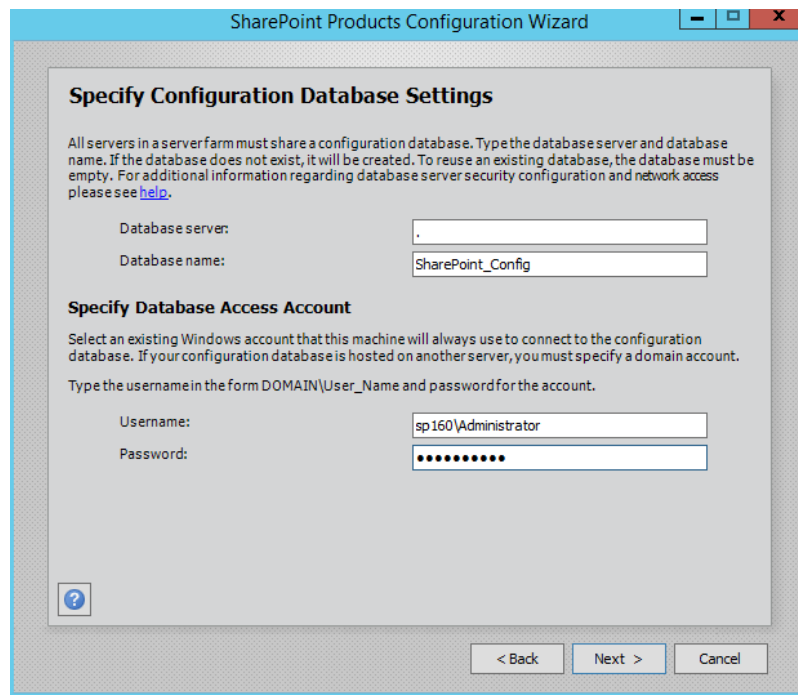
图 6-40 创建 Sharepoint 服务器场



4. 配置指定数据库设置，由于Sharepoint的数据库在本机，所以填写本机的数据库及账户，单击“Next”。

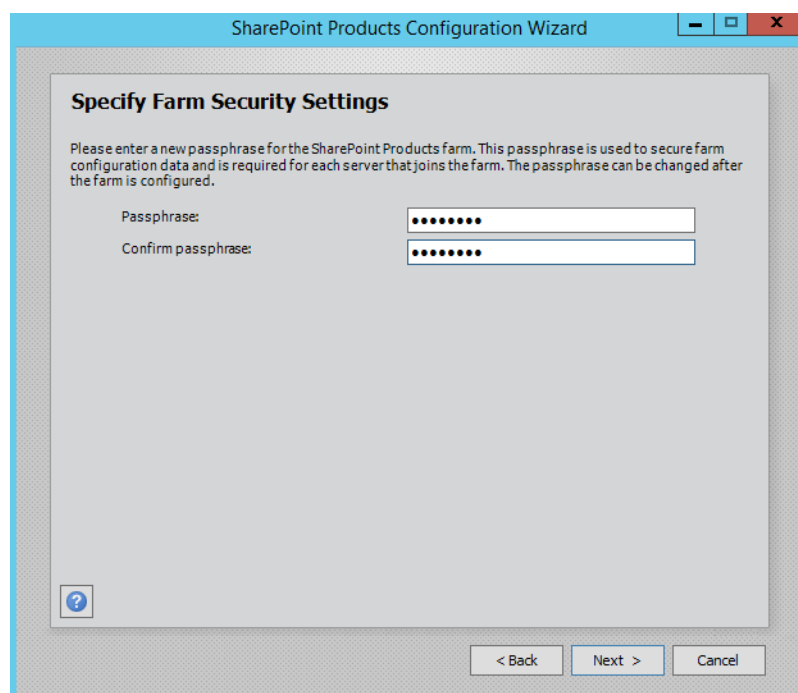


图 6-41 指定 Sharepoint 数据库设置



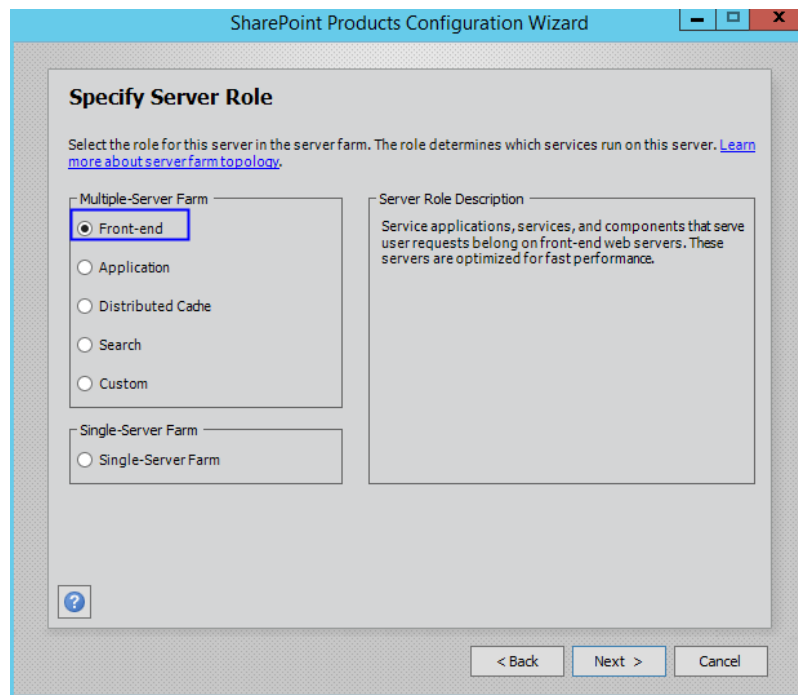
5. 填写服务器场的密码，单击“Next”。

图 6-42 设置 Sharepoint 服务器场密码



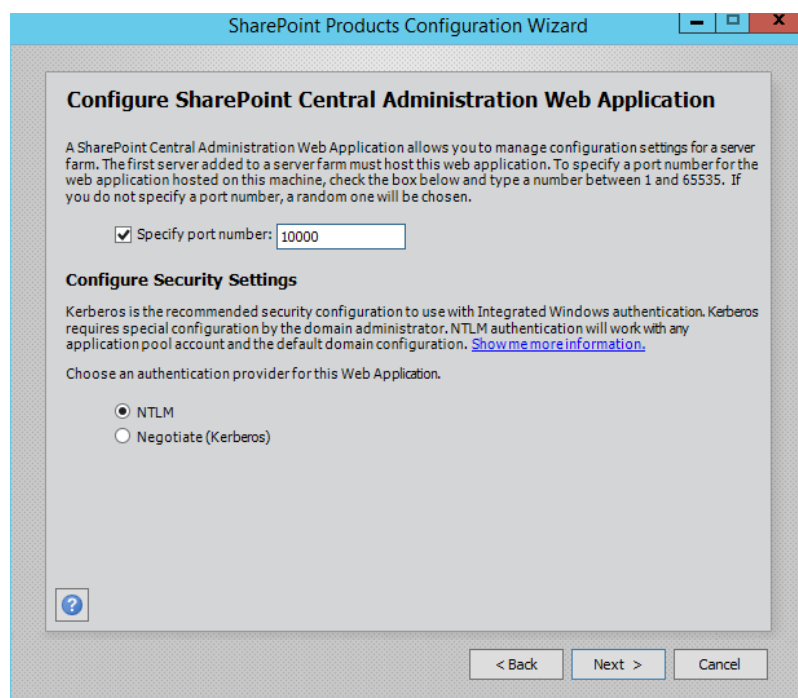
6. 设置服务器角色，选择“Front-end”，单击“Next”。

图 6-43 设置 Sharepoint 服务器角色



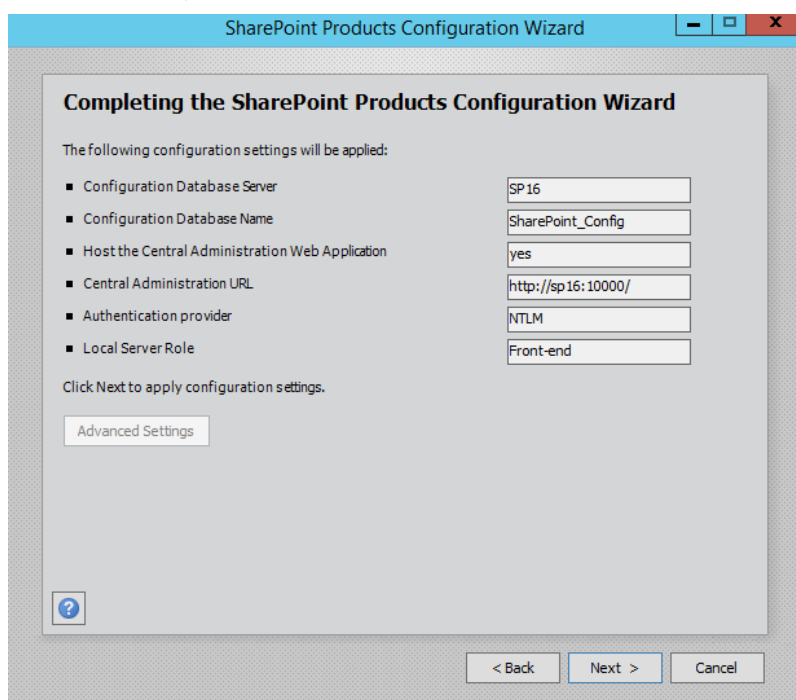
7. 设置Sharepoint管理中心的端口号为“10000”。

图 6-44 Sharepoint 管理中心端口号



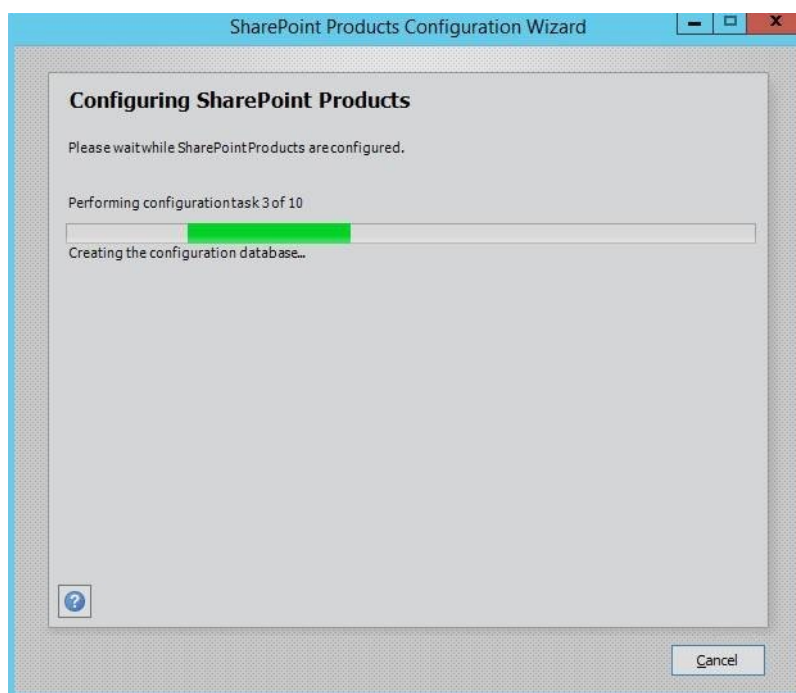
8. 查看并确认Sharepoint配置。

图 6-45 Sharepoint 配置



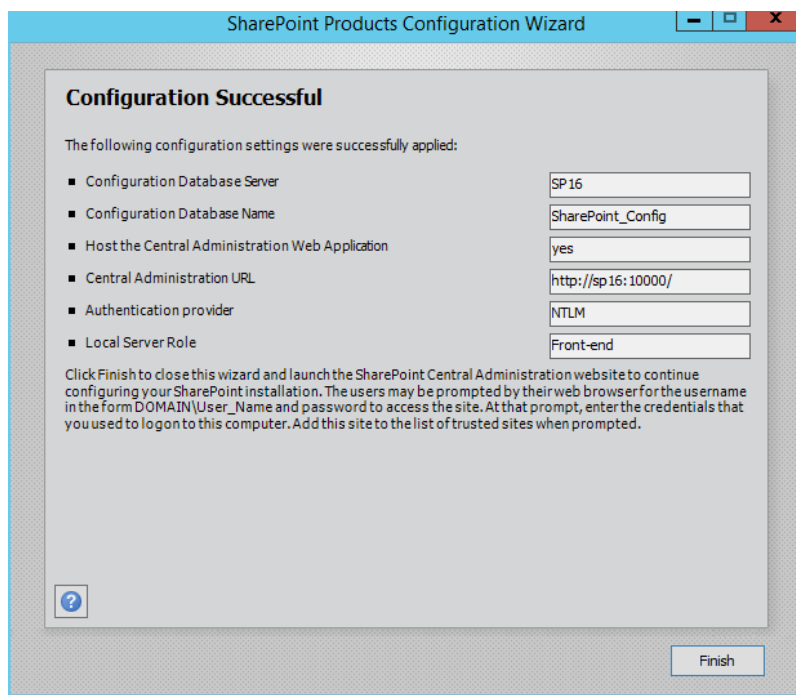
9. 单击“Next”，开始配置Sharepoint，共10步。

图 6-46 配置 Sharepoint 进度



10. Sharepoint配置成功，单击“Finish”。

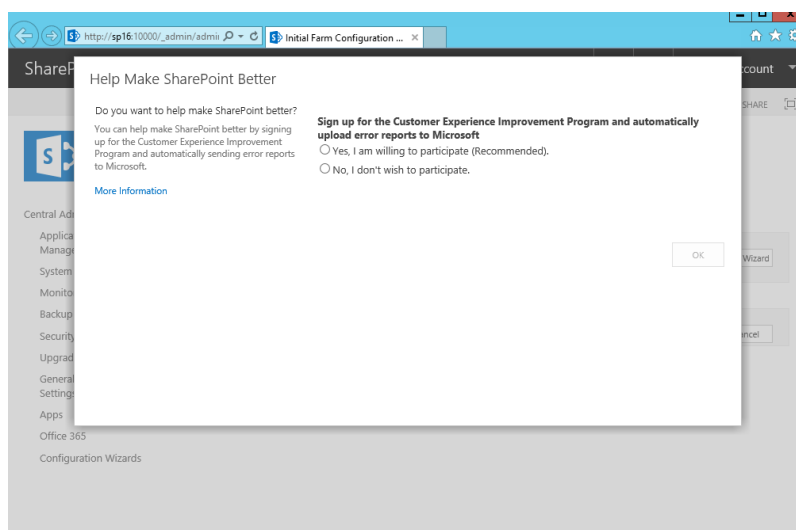
图 6-47 Sharepoint 配置成功



## 6.2.6 验证 Sharepoint 2016

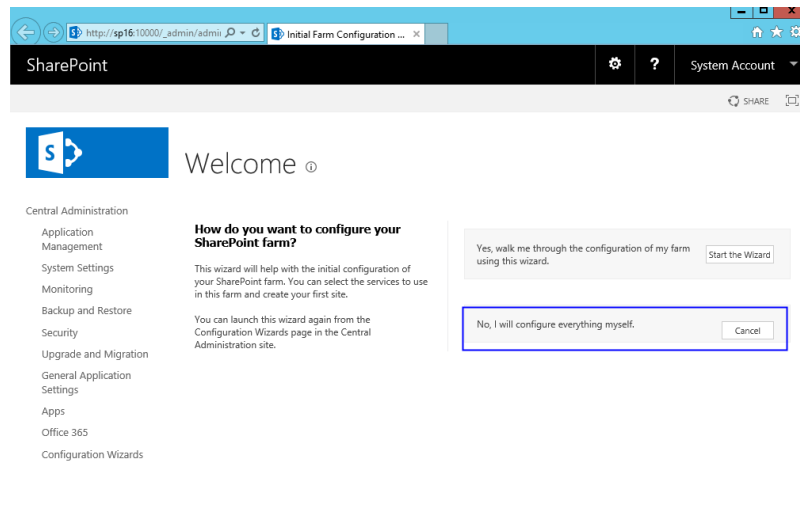
1. 通过配置的Sharepoint管理中心的URL，打开SharePoint的管理中心。

图 6-48 SharePoint 管理中心



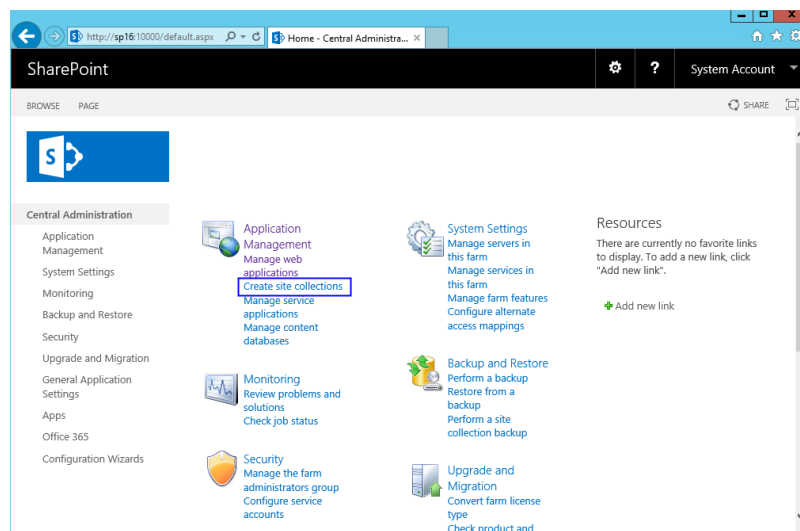
2. 选择Sharepoint Farm的配置方法，本操作采用自主配置，单击“Cancel”。若想要通过向导配置Sharepoint Farm，可以单击"Start the Wizard"。

图 6-49 SharePoint Farm 配置



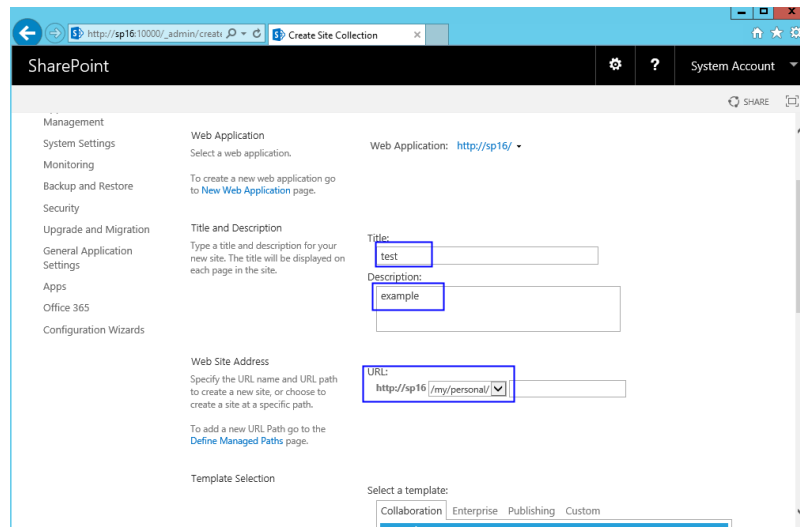
3. 在Sharepoint管理中心，单击“Create site collections”创建一个Sharepoint站点。

图 6-50 创建 Sharepoint 站点



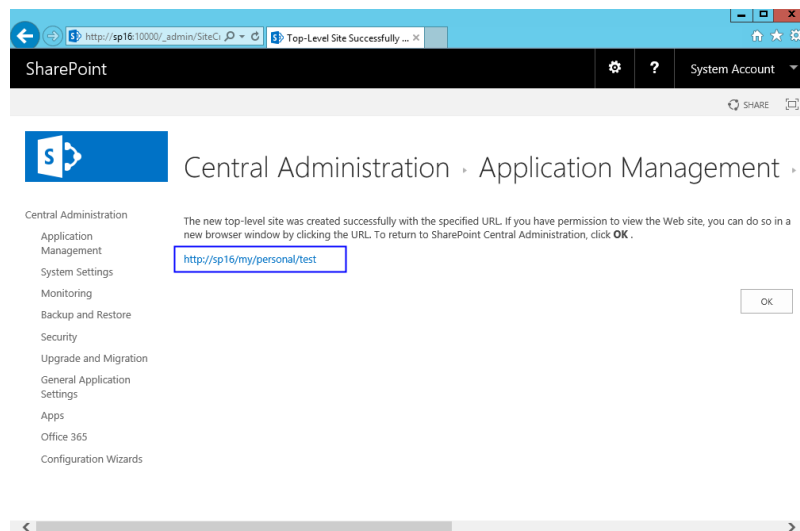
4. 根据界面提示内容，设置Sharepoint站点参数。

图 6-51 设置 Sharepoint 站点参数



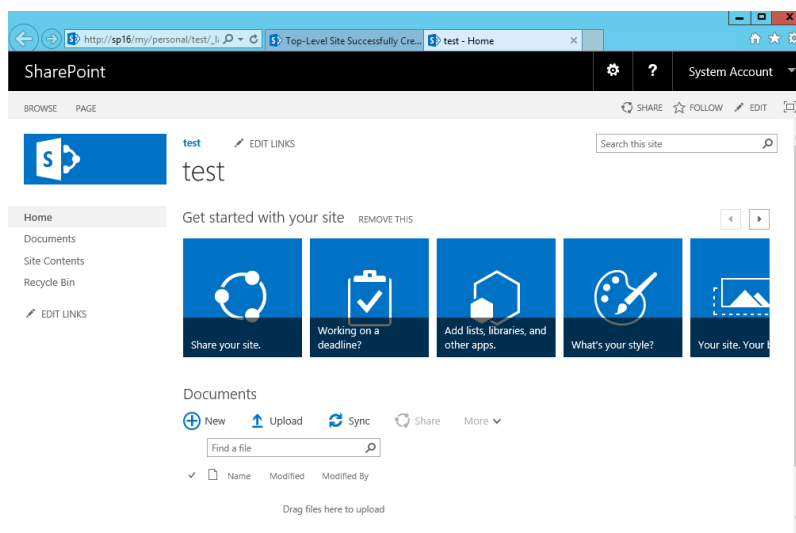
5. 创建Sharepoint Top-level站点成功，单击链接打开对应页面。

图 6-52 创建 SharePoint Top-level 站点成功



6. 在打开的Sharepoint站点，您可以根据界面提示设计您的网页。

图 6-53 Sharepoint 验证



## 6.3 部署 Docker

### 6.3.1 手工部署 Docker (CentOS 7.5)

#### 简介

本文介绍了如何在华为云上使用弹性云服务器的Linux实例手工部署Docker，并提供了Docker常用操作及简单的镜像制作过程。

表 6-5 Docker 相关术语

术语	解释
Docker	Docker是开发人员和系统管理员使用容器开发、部署和运行应用程序的平台。
镜像	Docker镜像是一个特殊的文件系统，除了提供容器运行时所需的程序、库、资源、配置等文件外，还包含了一些为运行时准备的配置参数（如匿名卷、环境变量、用户等）。镜像不包含任何动态数据，其内容在构建之后也不会被改变。
容器	镜像（Image）和容器（Container）的关系，就像是面向对象程序设计中的类和实例一样，镜像是静态的定义，容器是镜像运行时的实体。容器可以被创建、启动、停止、删除、暂停等。

更多关于Docker、镜像、容器的基础知识，请参见[Docker Documentation](#)。

该指导以“CentOS 7.5 64bit(40GiB)”操作系统为例，Docker要求64位的系统且内核版本至少为3.10。

## 前提条件

- 弹性云服务器需要绑定弹性公网IP，具体步骤参见[申请弹性公网IP](#)。
- 弹性云服务器所在安全组添加了如下表所示的安全组规则，具体步骤参见[添加安全组规则](#)。

表 6-6 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 80	0.0.0.0/0

## 部署 Docker

1. 登录弹性云服务器。
2. 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用华为云提供的epel镜像源\(x86\\_64和ARM\)?](#)。
3. 添加yum源。

```
yum install epel-release -y  
yum clean all
```

4. 安装yum-util。

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

5. 设置docker yum源。

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

6. 安装并运行Docker。

```
yum -y install docker-ce  
systemctl enable docker  
systemctl start docker
```

7. 检查安装结果。

```
docker --version
```

回显如下类似信息，表示Docker安装成功。

```
Docker version 26.1.4, build 5650f9b
```

## Docker 基本用法

1. Docker进程管理。

- 运行Docker

```
systemctl start docker
```

- 停止Docker

```
systemctl stop docker
```

- 重启Docker

```
systemctl restart docker
```

2. 镜像管理。



- a. 拉取镜像。此处以Apache和CentOS官方镜像为例。

```
docker pull httpd
docker pull centos
```

- b. 查看已有镜像

```
docker images
```

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

- c. 强制删除镜像

```
docker rmi centos
```

### 3. 容器管理。

- a. 创建一个容器并运行。

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

参数说明如下：

- `-i`：以交互模式运行容器，通常与`-t`同时使用。
- `-t`：为容器重新分配一个伪输入终端，通常与`-i`同时使用。
- `-d`：后台运行容器，并返回容器ID。
- `-p`：端口映射，格式为“宿主机端口:容器端口”。
- `--name`：为容器指定一个名称。
- `-v`：把主机上的一个目录挂载到镜像里，格式为“宿主机目录:镜像内挂载的路径”，必须为绝对路径。

#### 说明

上述参数说明中的宿主机表示所创建的弹性云服务器实例。

示例命令表示：使用镜像httpd，以交互模式启动一个容器，将容器的80端口映射到宿主机的80端口，宿主机的目录/data映射到容器的/var/www/httpd目录，并返回容器ID。

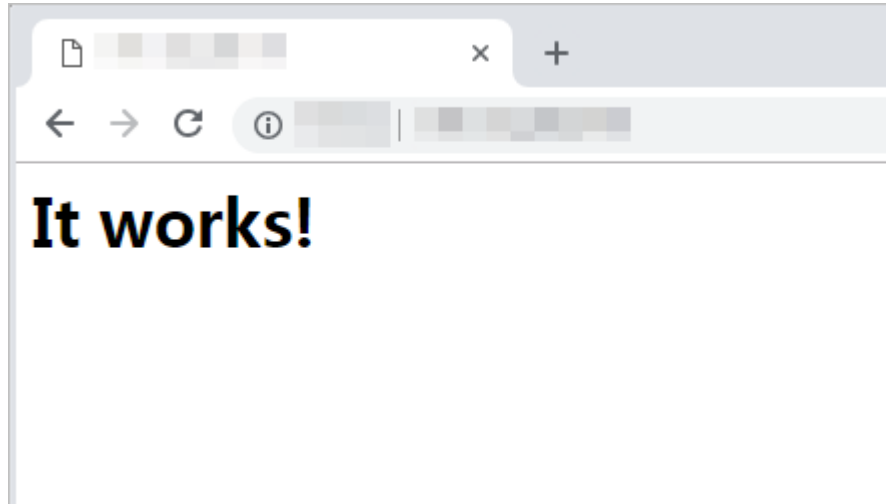
```
[root@ecs-b67a-docker ~]# docker run -it -d -p 80:80 --name datahttpd -v /data:/var/www/httpd/ httpd
6a514dea52a9465c1f6863c0f17ff41debda231ccff8bf66e3c0dbcc5f33cb20
[root@ecs-b67a-docker ~]#
```

- b. 查看容器启动情况。

```
docker ps -a
```

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

- c. 在浏览器输入弹性云服务器所绑定的弹性公网IP，访问测试容器运行情况。出现以下内容表示运行成功。



## 镜像制作

通过Dockerfile定制一个简单的Nginx镜像。

1. 创建一个名为Dockerfile的文件。

```
mkdir mynginx
cd mynginx
touch Dockerfile
```

2. 编辑Dockerfile。

```
vim Dockerfile
```

增加文件内容如下：

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

Dockerfile指令介绍如下。以下仅介绍简单指令，如需了解更多，请参见官方网站<https://docs.docker.com>。

- FROM语句：表示使用nginx镜像作为基础镜像，一个Dockerfile中FROM是必备的指令，并且必须是第一条指令。
- RUN语句：格式为RUN <命令>，表示执行echo命令，在显示器中显示一段“Hello, Docker!”的文字。

3. 构建镜像。

```
docker build -t nginx:v3 .
```

- -t nginx:v3：指定镜像的名称和版本。
- .：指定上下文路径，镜像构建命令将该路径下所有的内容打包给Docker引擎帮助构建镜像。

4. 查看部署的nginx镜像，版本为v3。

```
docker images
```

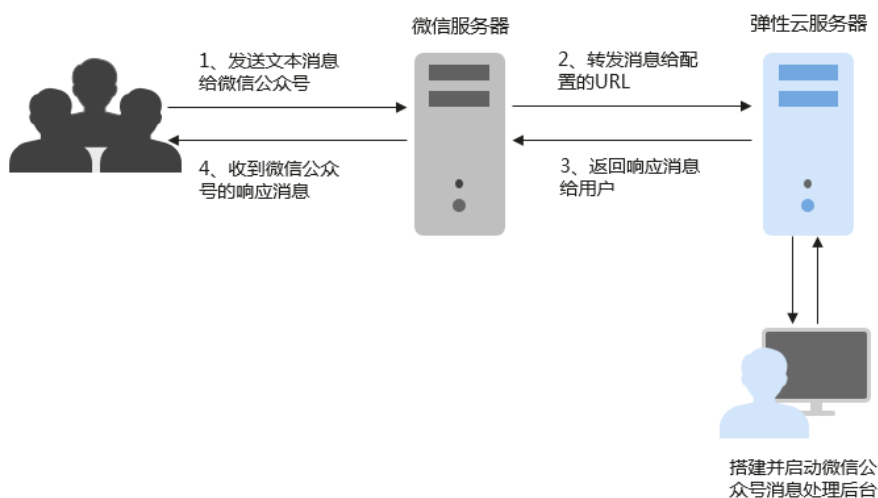
REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
nginx	v3	09422e465d96	10 seconds ago	109 MB

## 6.4 搭建微信公众号后台——收发文本消息

### 概述

在本教程中，您将学会使用弹性云服务器（以下简称 ECS）搭建微信公众号处理后台，使用Python语言编写对应的微信消息处理逻辑代码，接收从微信服务端转发过来的消息，并返回处理结果给最终用户，如图6-54所示。

图 6-54 流程简介

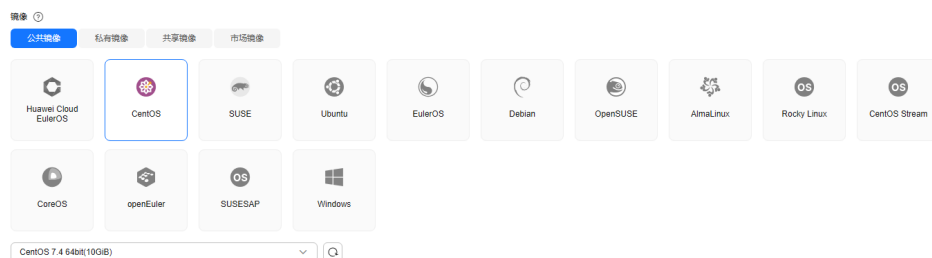


您需要了解的背景知识有：CentOS（Linux）操作系统、Python语言、Web.py框架、HTTP/XML协议。

### 准备事项

- 申请微信公众号  
微信公众号申请链接：<https://mp.weixin.qq.com/>  
本教程中使用订阅号“云图说”为例说明。
- 购买华为弹性云服务。  
如果没有华为账号，需[注册华为账号并开通华为云](#)。  
本教程中，使用公共镜像CentOS 7.4。

图 6-55 公共镜像



- 购买弹性公网IP  
建议同时购买弹性公网IP，后面需要在微信公众号上配置公网IP的地址。

图 6-56 弹性公网 IP



- 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。

## 安装基础软件

本教程中使用Python+Web.py组合完成微信公众号开发，需要安装或升级Python、pip、Web.py框架、WinSCP软件版本。

### 升级默认Python版本

CentOS 7.4自带Python版本比较老，建议升级到Python3。

1. 查看Python版本，使用如下命令：

```
python --version
```

图 6-57 查询 Python 版本

```
[root@ecs- ~]# python --version
Python 2.7.5
[root@ecs- ~]#
```

2. 下载Python安装包，这里以Python 3.6.0版本为例，使用命令：

```
wget https://www.python.org/ftp/python/3.6.0/Python-3.6.0a1.tar.xz
```

图 6-58 下载 Python 安装包

```
[root@ecs- ~]# wget https://www.python.org/ftp/python/3.6.0/Python-3.6.0a1.tar.xz
--2020-12-28 09:25:56-- https://www.python.org/ftp/python/3.6.0/Python-3.6.0a1.tar.xz
Resolving www.python.org (www.python.org)... 2a04:4e42:1a::223
Connecting to www.python.org (www.python.org)|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15328032 (15M) [application/octet-stream]
Saving to: 'Python-3.6.0a1.tar.xz'

100%[=====]
2020-12-28 09:25:57 (12.7 MB/s) - 'Python-3.6.0a1.tar.xz' saved [15328032/15328032]

[root@ecs- ~]#
```

3. 解压安装包，使用如下命令：  
**tar xvf Python-3.6.0a1.tar.xz**
4. 执行命令：  
**cd Python-3.6.0a1**  
**./configure**
  - 执行成功如图6-59所示：

图 6-59 执行成功

```
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
```

- 如果出现“configure: error: no acceptable C compiler found in \$PATH”异常提示，是因为未安装合适的编译器。

解决方法：

执行以下命令，安装/升级gcc及其他依赖的包。

```
sudo yum install gcc-c++
```

并在随后提示安装包是否OK时，输入y并回车。出现如图8提示说明依赖的包安装成功。

图 6-60 安装编译器

```
Installed:
gcc-c++.x86_64 0:4.8.5-44.e17

Dependency Installed:
libstdc++.devel.x86_64 0:4.8.5-44.e17

Dependency Updated:
cpp.x86_64 0:4.8.5-44.e17          gcc.x86_64 0:4.8.5-44.e17
```

在编译器安装完成后，重新执行./configure 命令。

5. 执行命令：  
**make && make install**  
执行成功。但提示pip错误，原因是我的系统中少了openssl-devel包，可以先忽略。

图 6-61 执行成功

```
rm -f /usr/local/bin/pyvenv
(cd /usr/local/bin; ln -s pyvenv-3.6 pyvenv)
if test "x" != "x" ; then \
    rm -f /usr/local/bin/python3-32; \
    (cd /usr/local/bin; ln -s python3.6-32 python3-32) \
fi
rm -f /usr/local/share/man/man1/python3.1
(cd /usr/local/share/man/man1; ln -s python3.6.1 python3.1)
if test "xupgrade" != "xno" ; then \
    case upgrade in \
        upgrade) ensurepip="--upgrade" ;; \
        install|*) ensurepip="" ;; \
    esac; \
    ./python -E -m ensurepip \
        $ensurepip --root=/ ; \
fi
Ignoring ensurepip failure: pip 8.1.1 requires SSL/TLS
```

- 查看Python3版本，使用命令：

```
python3 --version
```

图 6-62 查看 Python3 版本

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

- 执行命令：

```
python3
```

出现如下提示，则说明Python3安装成功。

图 6-63 Python3 安装成功

```
[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.
>>>
```

### 📖 说明

执行后续操作前需要先退出Python命令行，可通过输入以下任一命令再按回车键退出：

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

### 升级默认pip版本

pip是通用的Python包管理工具。提供了对Python包的查找、下载、安装、卸载功能。Python3安装成功后自带pip3，但版本比较老，建议升级到pip最新版本。同时前面安装python3提示“Ignoring ensurepip failure: pip 8.1.1 requires SSL/TLS”错误，导致pip未成功安装，所以需要重新安装pip。

- 安装openssl-devel包，使用命令：

```
yum install openssl-devel -y
```

图 6-64 安装 openssl-devel 包

```
Installed:
  openssl-devel.x86_64 1:1.0.2k-21.e17_9

Dependency Installed:
  keyutils-libs-devel.x86_64 0:1.5.8-3.e17      krb5-devel.x86_64 0:1.15.1-50.e17
  libselinux-devel.x86_64 0:2.5-15.e17         libsepol-devel.x86_64 0:2.5-10.e17
  zlib-devel.x86_64 0:1.2.7-18.e17

Dependency Updated:
  openssl.x86_64 1:1.0.2k-21.e17_9

Complete!
```

2. 执行命令:

```
make && make install
```

出现如下提示说明安装pip安装成功。

图 6-65 pip 安装成功

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

3. 升级pip3, 使用命令:

```
pip3 install --upgrade pip
```

出现如下提示说明升级pip到最新版本了。

图 6-66 pip3 升级成功

```
[root@ecs- Python-3.6.0a1]# pip3 install --upgrade pip
Collecting pip
  Downloading https://files.pythonhosted.org/packages/54/eb/4a36
  100% |████████████████████████████████████████████████████████████████████████████████| 1.5MB 32kB/s
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
```

## 安装Web.py框架

Web.py官方教程地址: <http://webpy.org/>, 使用如下命令安装web.py:

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

图 6-67 安装 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)
  |████████████████████████████████████████████████████████████████████████████████| 116 kB 76 kB/s
Using legacy 'setup.py install' for web.py, since package 'wheel'
Installing collected packages: web.py
  Running setup.py install for web.py ... done
Successfully installed web.py-0.40.dev0
```

## 安装WinSCP

通常情况下，在本地Windows操作系统上编辑代码，完成后再上传至ECS上（CentOS Linux系统）。WinSCP 是一个Windows环境下使用的SSH的开源图形化SFTP客户端，同时支持 SCP 协议。它的主要功能是在本地与远程计算机间安全地复制文件，并且可以直接编辑文件。

WinSCP安装链接：<https://winscp.net/eng/index.php>

## 上传代码

1. 新建main.py文件，复制如下代码：

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

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

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

2. 新建handle.py文件，复制如下代码：

```
# -*- 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 = "此处内容与公众号基本配置里Token字段取值保持一致"

            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)
            #打印消息体日志
```



```
recMsg = receive.parse_xml(webData)

if isinstance(recMsg, receive.Msg) and recMsg.MsgType == 'text':
    toUser = recMsg.FromUserName
    fromUser = recMsg.ToUserName
    content = "欢迎关注云图说!" + 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("不支持的消息类型: ",recMsg.MsgType)
    return "success"
except (Exception) as Argment:
    return Argment
```

### 3. 新建receive.py文件，复制如下代码：

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

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

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

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

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

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

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

class EventMsg(Msg):
```

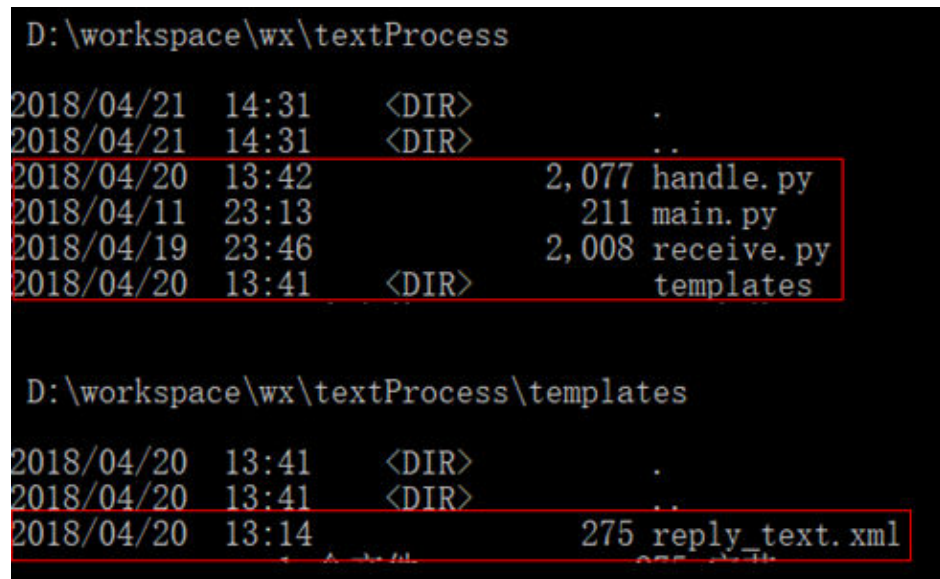
```
def __init__(self, xmlData):
    Event.__init__(self, xmlData)
    self.Event = xmlData.find('Event').text
```

- 新建templates文件夹，在文件夹下新建reply\_text.xml文件，复制如下代码：

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

- 最终本地代码文件形成如下：

图 6-68 本地文件

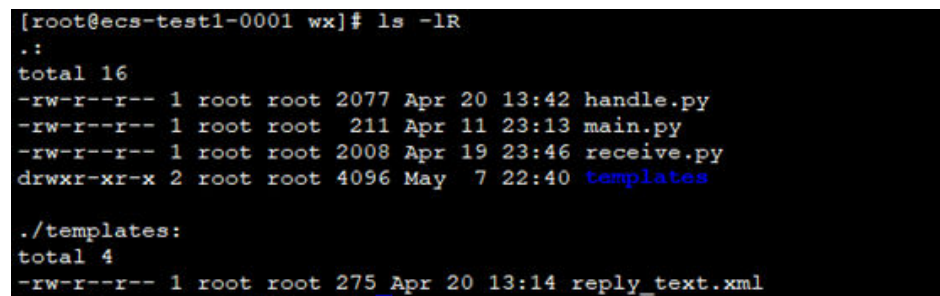


```
D:\workspace\wx\textProcess
2018/04/21 14:31 <DIR> .
2018/04/21 14:31 <DIR> ..
2018/04/20 13:42 2,077 handle.py
2018/04/11 23:13 211 main.py
2018/04/19 23:46 2,008 receive.py
2018/04/20 13:41 <DIR> templates

D:\workspace\wx\textProcess\templates
2018/04/20 13:41 <DIR> .
2018/04/20 13:41 <DIR> ..
2018/04/20 13:14 275 reply_text.xml
```

- 通过WinSCP工具将上述文件与目录上传至ECS指定目录下：

图 6-69 上传文件



```
[root@ecs-test1-0001 wx]# ls -lR
.:
total 16
-rw-r--r-- 1 root root 2077 Apr 20 13:42 handle.py
-rw-r--r-- 1 root root 211 Apr 11 23:13 main.py
-rw-r--r-- 1 root root 2008 Apr 19 23:46 receive.py
drwxr-xr-x 2 root root 4096 May 7 22:40 templates

./templates:
total 4
-rw-r--r-- 1 root root 275 Apr 20 13:14 reply_text.xml
```

## 启动服务

使用如下命令启动服务：

```
python3 main.py 80
```

启动成功如图6-70所示：

图 6-70 启动成功

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

## 启用开发者模式

1. 登录微信公众平台，选择“开发 > 基本配置”，单击“修改配置”。
2. 填写配置信息，单击“提交”。
  - URL: `https://ECS的弹性公网IP/wx`，不用添加80端口。
  - Token: 需要与handle.py中对应token取值完全一致。
  - EncodingAESKey: 随机生成。
  - 消息加解密方式: 此为示例，选择简单的“明文模式”。
3. 验证token成功，单击“启用”。

### 说明

如果token验证失败，请检查Token配置与handle.py中GET消息处理代码是否一致。

## 验证

使用微信关注公众号，任意发送一条文本消息，看是否能够收到回复。如能收到回复则表明系统处理正常。

## 6.5 手工部署 GitLab (CentOS7.2)

### 简介

本文主要介绍了在华为云上如何使用弹性云服务器的Linux实例手工部署GitLab。GitLab是一个开源的版本管理系统，使用Git作为代码管理工具。该指导具体操作以CentOS 7.2 64位操作系统为例。

### 前提条件

- 部署GitLab的实例内存要求不小于4GB。
- 弹性云服务器所在安全组添加了如下表所示的安全组规则，具体步骤参见[为安全组添加安全组规则](#)。

表 6-7 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 80	0.0.0.0/0

### 操作步骤

#### 步骤1 安装相关依赖包。

1. 登录弹性云服务器。



#### 步骤4 浏览器访问测试。

使用浏览器访问“<http://服务器弹性公网IP地址>”，显示如下页面，说明环境搭建成功。



----结束

## 后续操作

1. 获取GitLab的登录密码。

执行以下命令获取GitLab的登录密码：

```
sudo cat /etc/gitlab/initial_root_password
```

回显如下类似信息：

```
[root@server ~]# sudo cat /etc/gitlab/initial_root_password
# WARNING: This value is valid only in the following conditions
# 1. If provided manually (either via 'GITLAB_ROOT_PASSWORD' environment variable or via 'gitlab_rails['initial_root_password']' setting in 'gitlab.rb', it was provided before database was seeded for the first time (usually, the first reconfigure run).
# 2. Password hasn't been changed manually, either via UI or via command line.
#
# If the password shown here doesn't work, you must reset the admin password following https://docs.gitlab.com/ee/security/reset_user_password.html#reset-your-root-password.
Password: [REDACTED]
# NOTE: This file will be automatically deleted in the first reconfigure run after 24 hours.
```

### ⚠ 注意

由于保存默认密码的文件将在首次配置运行24小时后自动删除，建议您首次登录之后，立即修改初始密码。

2. 登录GitLab。

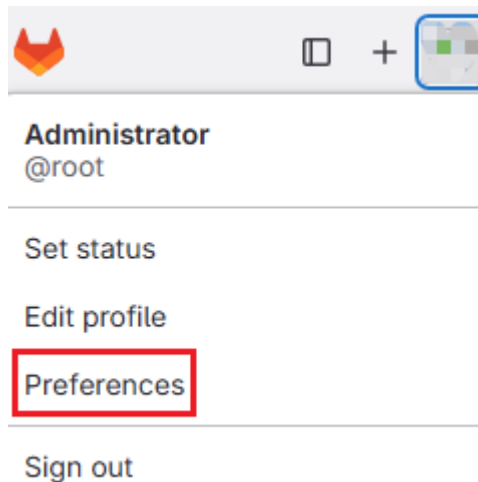
在浏览器的地址栏中，输入“<http://服务器弹性公网IP地址>”即可进入GitLab的登录界面。

首次登录使用用户名root，密码为1获取的密码。

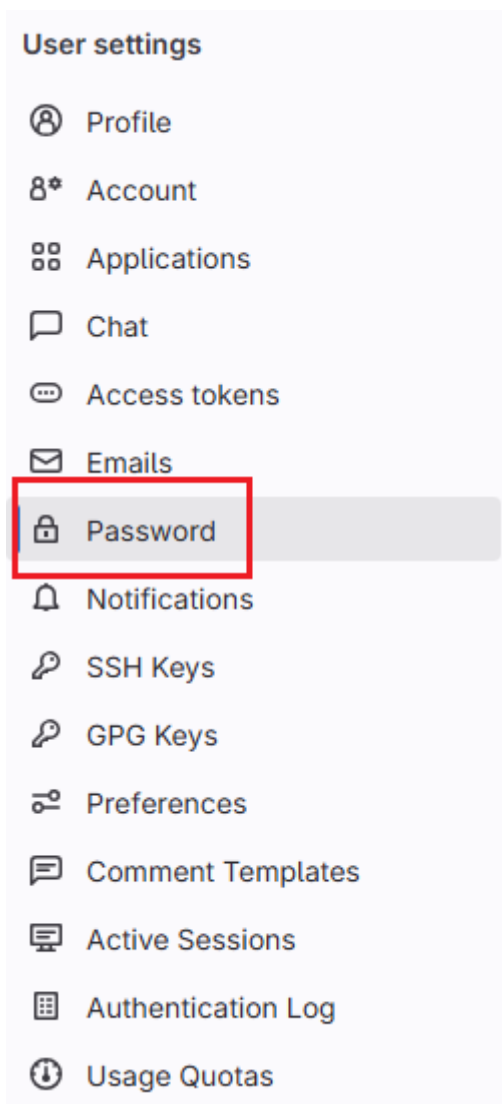


3. 修改初始密码

- a. 登录GitLab后，选择页面左上角的用户头像，在弹出菜单中选择“Preferences”。



- b. 在“User Settings”页面中，选择左侧导航栏的“Password”。



- c. 在页面中输入当前使用密码，新密码及确认新密码后，单击“Save Password”。

### Password

Change your password or recover your current one.

Current password

You must provide your current password in order to change it.

New password

Password confirmation

[Save password](#) [I forgot my password](#)

如果您想了解更多的GitLab操作，例如GitLab常用命令、数据备份、配置选项、用户管理、与其他服务集成、故障排除等，请参见GitLab官方文档。

## 6.6 手工部署 RabbitMQ ( CentOS 7.4 )

### 简介

本文介绍了如何在华为云上使用弹性云服务器的Linux实例部署RabbitMQ。RabbitMQ是采用Erlang语言实现AMQP（Advanced Message Queuing Protocol，高级消息队列协议）的消息中间件，它最初起源于金融系统，用于在分布式系统中存储转发消息。RabbitMQ凭借其高可靠、易扩展、高可用及丰富的功能特性成为目前非常热门的一款消息中间件。

### 前提条件

弹性云服务器所在安全组添加了如下表所示的安全组规则，具体步骤参见[为安全组添加安全组规则](#)。

表 6-8 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 5672	0.0.0.0/0
入方向	1	允许	IPv4	TCP: 15672	0.0.0.0/0

### 操作步骤

#### 步骤1 安装相关依赖包和perl。

1. 登录弹性云服务器。
2. 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。
3. 执行以下命令，安装相关依赖包。

```
yum -y install make gcc gcc-c++ m4 ncurses-devel openssl-devel  
unixODBC-devel
```

4. 执行如下命令，安装perl。

```
yum install perl
```

#### 步骤2 安装erlang。

关于erlang的安装请参考[Erlang官方资料](#)。

1. 添加erlang存储库到系统

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

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

或手动添加[存储库条目](#)



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

2. 在/etc/yum.repos.d/目录下新建一个文件rabbitmq-erlang.repo，然后将下面的粘帖进去

```
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
```

按**Esc**键退出编辑模式，并输入:**wq**保存后退出。

3. 执行以下命令安装erlang

```
sudo yum install erlang
```

执行以下命令安装esl-erlang

```
sudo yum install esl-erlang
```

4. 执行如下命令，检查安装结果。

```
erl -version
```

回显类似如下信息，说明erlang安装成功。

```
[root@ecs-rabbitmq ~]# erl -version  
Erlang (SMP,ASYNC_THREADS,HIPE) (BEAM) emulator version 11.1.7
```

### 步骤3 安装RabbitMQ

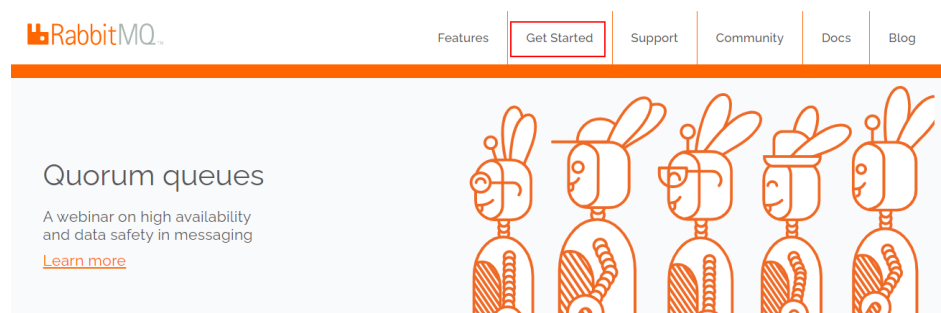
1. 执行如下命令，进入用户主目录。

```
cd
```

2. 执行如下命令，下载RabbitMQ安装包。

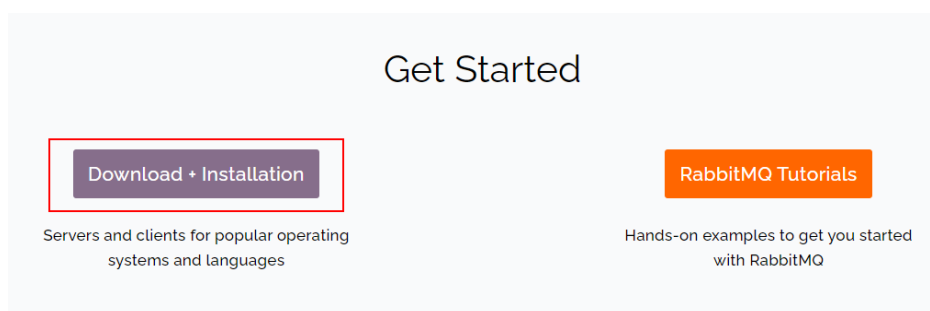
- a. 打开[Rabbit官网](#)。
- b. 单击“Get Started”。

图 6-71 Get Started



- c. 找到并单击“Download+Installation”。

图 6-72 Download+Installation



- d. 根据云服务器的操作系统选择下载地址。例如本例中使用的是CentOS 7.x的下载地址。

图 6-73 选择下载地址

Downloads [on GitHub](#)

- [Windows installer](#)
- [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. 在服务器上执行以下命令下载RabbitMQ安装包。

例如步骤3.2.d查找的下载地址是：

<https://github.com/rabbitmq/rabbitmq-server/releases/download/v3.8.12/rabbitmq-server-3.8.12-1.el7.noarch.rpm>

则执行的命令如下：

```
wget https://github.com/rabbitmq/rabbitmq-server/releases/download/v3.8.12/rabbitmq-server-3.8.12-1.el7.noarch.rpm
```

如果下载过程中提示“Unable to establish SSL connection.”

可以在wget命令后加--no-check-certificate，重复执行几次，即可下载。

例如：

```
wget https://github.com/rabbitmq/rabbitmq-server/releases/download/v3.8.12/rabbitmq-server-3.8.12-1.el7.noarch.rpm --no-check-certificate
```

- f. 执行以下命令安装RabbitMQ安装包。

```
yum install rabbitmq-server-3.8.12-1.el7.noarch.rpm
```

3. 安装完毕，启动RabbitMQ

```
service rabbitmq-server start
```

4. 查看RabbitMQ状态。

```
service rabbitmq-server status
```

**步骤4** 执行如下命令，启用RabbitMQ的web管理界面。

```
rabbitmq-plugins enable rabbitmq_management
```

回显类似如下信息：

```
[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_agent
rabbitmq_web_dispatch

started 3 plugins.
```

**步骤5** 执行如下命令，创建一个新用户。

```
rabbitmqctl add_user 用户名 密码
```

命令示例：

```
rabbitmqctl add_user root 123456
```

**步骤6** 执行如下命令，设置用户为管理员。

```
rabbitmqctl set_user_tags 用户名 administrator
```

命令示例：

```
rabbitmqctl set_user_tags root administrator
```

**步骤7** 执行如下命令，赋予用户所有权限。

```
rabbitmqctl set_permissions -p / 用户名 '.*' '.*' '.*'
```

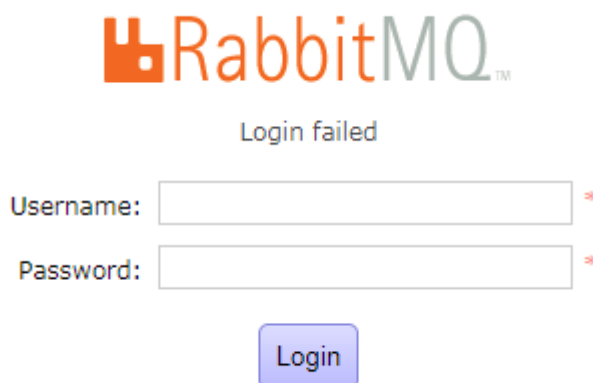
命令示例：

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

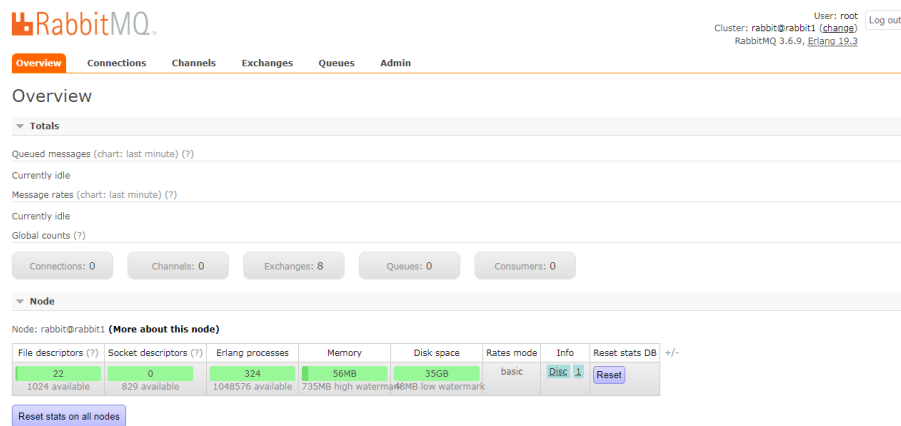
**步骤8** 执行如下命令，在后台启动RabbitMQ。

```
rabbitmq-server -detached
```

**步骤9** 使用浏览器访问“http://弹性公网IP:15672”，显示如下页面，说明RabbitMQ安装成功。



**步骤10** 输入**步骤5**创建的用户名和密码后单击“Login”，进入RabbitMQ管理界面。



----结束

## 6.7 PostgreSQL 本地 Slave 搭建步骤

### PostgreSQL 是什么？

PostgreSQL是一个开源对象关系型数据库管理系统，并侧重于可扩展性和标准的符合性。PostgreSQL面向企业复杂SQL处理的OLTP在线事务处理场景，支持NoSQL数据类型（JSON/XML/hstore），支持GIS地理信息处理，在可靠性、数据完整性方面有良好的声誉，适用于互联网网站、位置应用系统、复杂数据对象处理等应用场景。

本文指导您使用华为云弹性云服务器搭建PostgreSQL。

### 搭建前准备

- 创建弹性云服务器。
- 配置弹性云服务器安全组规则：开放 5432 端口。

#### 📖 说明

本文使用的云服务器操作系统：CentOS 7.6 64bit

本文使用的PostgreSQL版本：PostgreSQL (11.2)

- 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。

### 主节点配置

1. 依次执行以下命令，安装PostgreSQL。

```
# yum update -y
# yum install https://download.postgresql.org/pub/repos/yum/reposrums/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. 执行以下命令，切换到postgres用户（安装好生成默认的用户）。

```
# su - postgres
```

3. 执行以下命令，进入数据库。

```
# psql
```

4. 执行以下命令，创建账号并授权。

```
create role 账户名 login replication encrypted password '密码';
```

#### 📖 说明

上述命令中密码必须用单引号。

以创建的账号名为dbar，密码为xxxxx为例，命令如下：

```
create role dbar login replication encrypted password 'xxxxx';
```

5. 执行以下命令，修改/var/lib/pgsql/11/data/pg\_hba.conf配置文件，添加如下内容。

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

```
host all all 192.168.1.0/24 md5 #允许VPC网段中md5密码认证连接
```

```
host replication dbar 备库实际IP/24 md5 #允许用户从replication数据库进行数据同步
```

6. 执行以下命令，修改/var/lib/pgsql/11/data/postgresql.conf。

```
# vim postgresql.conf
```

```
wal_level = hot_standby #热备模式
```

```
max_wal_senders= 6 #可以设置最多几个流复制链接
```

```
wal_sender_timeout = 60s #流复制主机发送数据的超时时间
```

```
max_connections = 512 #从库的 max_connections要大于主库
```

```
archive_command=' cp %p /var/lib/pgsql/11/data/archivelog/%f' #归档
```

```
wal_keep_segments=10240
```

```
archive_mode = on #允许归档
```

```
listen_addresses= xxx.xx.xx.xx #实际的本地ip地址
```

7. 执行以下命令，重启服务。

```
# systemctl restart postgresql-11
```

## 从节点配置

1. 依次执行以下命令，完成从节点安装。

```
# 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. 执行以下命令，复制master配置相关文件。

```
# pg_basebackup -h 主节点ip -U dbar -D /var/lib/pgsql/11/data -X stream -P
```

```
# cp /usr/pgsql-11/share/recovery.conf.sample /var/lib/pgsql/11/data/recovery.conf
```

```
[root@ecs-22f5-0002 ~]# pg_basebackup -D /var/lib/pgsql/11/data -h 192.168.1.100 -p 5432 -U test -X stream -P
Password:
24508/24508 kB (100%), 1/1 tablespace
[root@ecs-22f5-0002 ~]#
```

3. 执行以下命令，修改recovery.conf文件。

```
# vim recovery.conf
```

```
standby_mode = on # 声明此节点为从库
primary_conninfo = 'host=主节点IP port=5432 user=dbar password=xxxxx (此处密码不能加单引号)
trigger_file = '/var/lib/pgsql/11/data/trigger.kenyon' #主从切换时的触发文件
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' #清除过期归档
```

4. 执行以下命令，修改postgresql.conf文件。  
**# chown -R postgres.postgres /var/lib/pgsql/11/data**
5. 修改/var/lib/pgsql/11/data/postgresql.conf。  
**listen\_addresses= xxx.xx.xx.xx #实际的本地ip地址**  
**max\_connections = 600**
6. 执行以下命令，启动服务，设置开机自启。  
**#systemctl enable postgresql-11**  
**#systemctl start postgresql-11**

## 验证部署完成

1. 执行以下命令，在主节点中可查看到sender进程。

```
# ps aux |grep sender
```

```
[root@ecs-22f5-0001 ~]# ps aux |grep sender
postgres 14406 0.0 0.3 397240 3620 ? Ss 20:19 0:00 postgres: walsender test (53052) streaming 0/3000140
```

2. 执行以下命令，从节点中可查看到receiver进程。

```
# ps aux | grep receiver
```

```
[root@ecs-22f5-0002 ~]# ps aux |grep receiver
postgres 4390 0.0 0.3 403500 3632 ? Ss 20:19 0:00 postgres: walreceiver streaming 0/3000140
```

3. 执行以下命令，主库中可查看到从库状态。

```
# su - postgres
```

```
-bash-4.2# psql
```

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

```
postgres=# select * from pg_stat_replication;
 pid | usesysid | username | application_name | client_addr | client_hostname | client_port |          backend_start          | backend_xmin | state | se
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
 14406 |    16384 | test     | walreceiver      |             |                 |             | 2019-03-26 20:19:15.693053+08 |             | streaming | 0/
 3000140 | 0/3000140 | 0/3000140 | 0/3000140       |             |                 |             | 0 | async
(1 row)
```

4. 在主库建一个库，验证备库是否可以同步。
  - a. 在主库执行以下命令  
**postgres=# create database testdb;**  
**postgres=# \l**
  - b. 在备库执行以下命令查看。  
**postgres=# \l**

## 6.8 手工安装宝塔面板（CentOS 7.2）

### 应用场景

本文主要介绍了在华为云上如何在弹性云服务器的Linux实例上手工安装宝塔面板。宝塔面板是一款使用方便、功能强大且终身免费的服务器管理软件，支持Linux与Windows系统。一键配置LAMP、LNMP、网站、数据库、FTP、SSL，通过Web端轻

松管理服务器。该指导具体操作以CentOS 7.2 64位操作系统安装宝塔Linux面板6.9为例。

## 方案优势

- 快速创建管理项目
- 预览服务器资源使用情况
- 轻松安装软件及部署源码

## 约束与限制

- 弹性云服务器实例规格和操作系统：
  - 内存要求最低512MB，推荐768MB以上，纯面板约占系统60MB内存。
  - 100M以上可用硬盘空间（纯面板约占20M磁盘空间）。
  - 宝塔Linux6.0版本是基于Centos7开发的，强烈建议使用CentOS 7.x 系统。
  - 需要是全新的干净系统，没有安装过Apache、Nginx、php、MySQL。
- 弹性云服务器所在安全组添加了如表6-9所示的安全组规则，具体步骤参见[为安全组添加安全组规则](#)。

### 📖 说明

宝塔面板的端口通常为8888，但可能会因安装环境不同而改变，请您以3中对应的面板地址使用的端口和后续面板系统设置的端口为准）。

表 6-9 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 8888	0.0.0.0/0

## 安装宝塔面板操作流程

Linux实例手工安装宝塔面板的具体操作步骤如下：

1. [安装宝塔面板](#)。
2. [登录宝塔面板](#)。

## 实施步骤

### 步骤1 安装宝塔面板。

1. 登录弹性云服务器。
2. 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。
3. 执行以下命令，下载并安装宝塔面板。

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

当出现以下提示信息时，输入“y”：

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

安装完成后，回显如下类似信息：

```
=====
Congratulations! Installed successfully!
=====
1# https://dg2.bt.cn/ssl/baota_root.pfx# www.bt.cn#
2# https://www.bt.cn/bbs/thread-117246-1-1.html
=====
# 27832 #
# : https://1.92.146.36:27832/0677640c
# : https://192.168.0.198:27832/0677640c
username: ewih2973
password:
=====
https://www.bt.cn/new/wechat_customer
=====
Time consumed: 1 Minute! e a l s s m m i l
to /usr/lib/systemd/systemd.service.
```

### 📖 说明

请记录上图回显信息中红框部分的地址信息、“username”和“password”的参数值。

### 步骤2 登录宝塔面板。

1. 在浏览器地址栏中输入记录的地址，例如：`https://1.92.xxx.xx:27832/0677640c`。此示例中的端口号为27832，则安全组中需要添加的端口号为27832，否则会提示“无法访问此网站”。
2. 输入记录的账户和密码。
3. 勾选我已阅读并同意“《用户协议》”，单击“进入面板”。
4. 绑定宝塔官网账号。
5. 根据业务需要可以通过面板安装相关的套件并部署网站。

----结束

## 6.9 基于弹性云服务器安装及部署 Jenkins

### 准备工作

- 在安装Jenkins之前，需要购买弹性云服务器（推荐配置：4GB+内存，40GB+硬盘），操作系统选择CentOS 7.6。同时购买弹性公网IP，绑定到购买的弹性云服务器上。
- ECS购买成功后，将下表中列出的入网规则添加到ECS所属的安全组。具体操作请参考[添加安全组规则](#)。

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 8080	0.0.0.0/0

### 操作步骤

#### 步骤1 安装JDK

##### 📖 说明

考虑到和Jenkins版本的兼容性，选择安装OpenJDK 11([支持的Java版本](#))。



1. 远程登录已购买的ECS设备。
2. 执行以下命令查看当前JDK版本。  
**java -version**  
如果存在JDK且当前版本低于11，则执行如下命令卸载原有的JDK。  
**rpm -qa | grep java | xargs rpm -e --nodeps**
3. 继续执行以下命令安装新版本JDK。  
**yum install -y java-11-openjdk**
4. 重启ECS服务器。
5. 执行以下命令查看是否安装成功。  
**java -version**

```
[root@ecs-jenkins ~]# java -version
openjdk version "11.0.16" 2022-07-19 LTS
OpenJDK Runtime Environment (Red_Hat-11.0.16.0.8-1.el7_9) (build 11.0.16+8-LTS)
OpenJDK 64-Bit Server VM (Red_Hat-11.0.16.0.8-1.el7_9) (build 11.0.16+8-LTS, mixed mode, sharing)
```

## 步骤2 安装Jenkins

1. 依次执行以下3条命令安装Jenkins。  
**sudo wget -O /etc/yum.repos.d/jenkins.repo https://pkg.jenkins.io/redhat-stable/jenkins.repo**  
**sudo rpm --import https://pkg.jenkins.io/redhat-stable/jenkins.io.key**  
**yum install -y jenkins --nogpgcheck**
2. 执行以下命令编辑Jenkins文件。  
**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. 分别执行以下命令启动Jenkins并查看当前状态。  
**systemctl start jenkins**  
**systemctl status jenkins**

```
[root@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.war --webroot=/C/jenkins/war
```

## 步骤3 激活Jenkins

1. 在本地浏览器访问地址<http://Jenkins所在主机绑定的EIP:8080>，出现解锁界面。



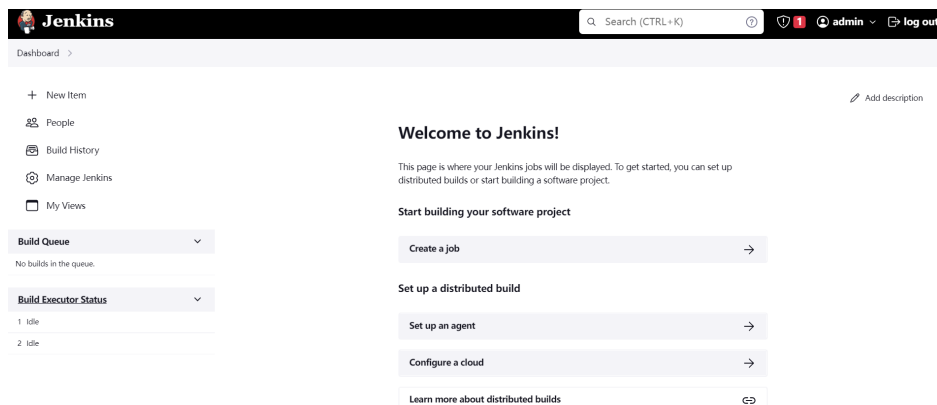
2. 登录弹性云服务器。
3. 执行以下命令获取激活密码。  

```
cat /var/lib/jenkins/secrets/initialAdminPassword
```

```
[root@ecs-jenkins ~]# cat /var/lib/jenkins/secrets/initialAdminPassword  
f4360f0b[REDACTED]32f7f
```
4. 返回解锁界面输入激活密码，单击“继续”。
5. 选择安装推荐的插件，等待安装完成后，选择使用admin账户继续下一步。



6. 选择保存并完成，进入Jenkins主界面。



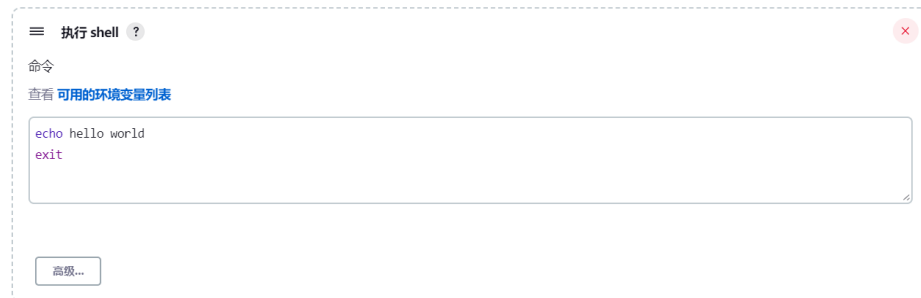
---结束

## 后续验证

### 单一任务执行

1. 创建任务，选择自由项目，输入项目名称，单击“OK”。
2. 在构建步骤，选择“执行shell”，填入`echo hello world; exit`，其他不设置，单击“保存”。

#### Build Steps



3. 单击“立即构建”。
4. 等待左下方构建任务执行完成，单击进入，选择控制台输出，看到执行成功并输出hello world。

### 控制台输出

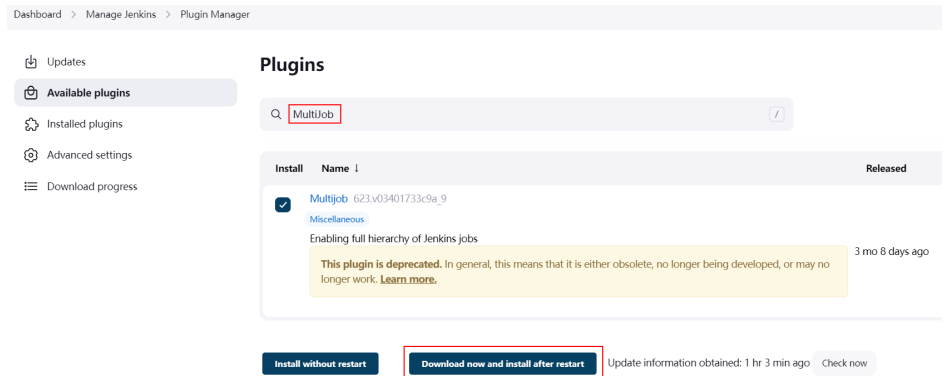
```
Started by user admin
Running as SYSTEM
Building in workspace /var/lib/jenkins/workspace/Demo
[Demo] $ /bin/sh -xe /tmp/jenkins11962229540495089218.sh
+ echo hello world
hello world
+ exit
Finished: SUCCESS
```

### 多任务顺序执行

1. 在插件管理界面，搜索并安装MultiJob插件。

## 说明

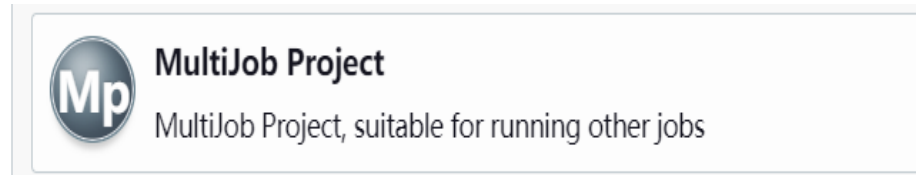
- 插件安装后需要重启Jenkins方可生效，选择安装后重启选项。



- 重启Jenkins后，需要在已安装的插件界面，查看MultiJob插件是否生效。



2. 创建多任务项目，选择MultiJob项目，输入项目名称，单击“OK”。

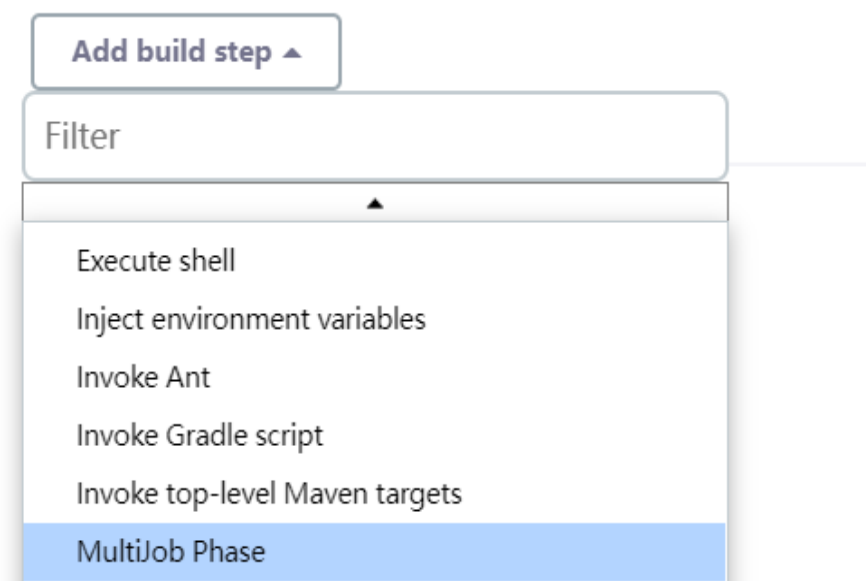


## 说明

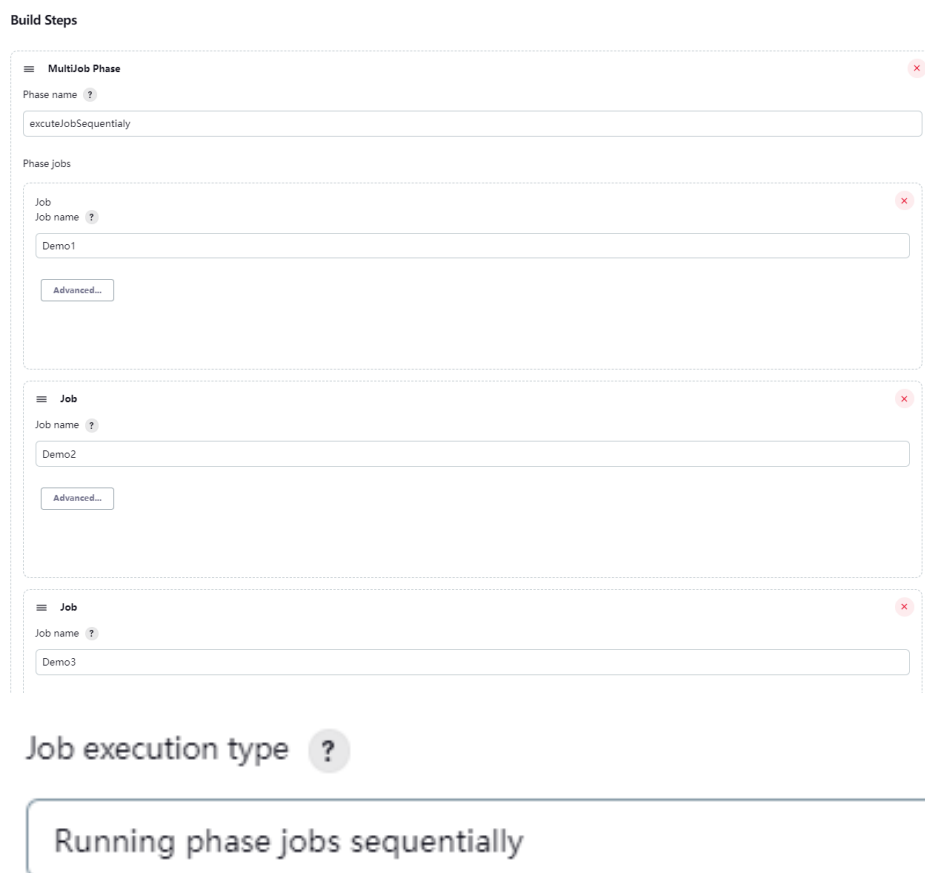
创建MultiJob项目前，需先创建三个单一任务子项目。

3. 在构建步骤，选择MultiJob Phase。

## Build Steps



4. 增加如下3个子任务，并设置按顺序运行。



5. 单击“保存”，任务创建完成。
6. 单击“立即构建”，即可看到3个任务按顺序构建成功。

Multijob Project multijobDemo

[Add description](#)  
[Disable Project](#)

S	W	Job	Last Success	Last Failure	Last Duration	Console	Built On
🟢	🔄	multijobDemo	28 sec #2	N/A	7.5 sec	<a href="#">Console output</a>	<a href="#">Jenkins</a>
🟢	🔄	executeJobSequentially					
🟢	🔄	Demo1	28 sec #2	N/A	8 ms	<a href="#">Console output</a>	<a href="#">Jenkins</a>
🟢	🔄	Demo2	25 sec #5	N/A	9 ms	<a href="#">Console output</a>	<a href="#">Jenkins</a>
🟢	🔄	Demo3	23 sec #4	N/A	9 ms	<a href="#">Console output</a>	<a href="#">Jenkins</a>

Icons: [S](#) [M](#) [L](#) [Icon legend](#) [Atom feed for all](#) [Atom feed for failures](#) [Atom feed for just latest builds](#)

[Workspace](#)  
[Recent Changes](#)  
Downstream Projects  
[Demo1](#)  
[Demo2](#)  
[Demo3](#)

## 6.10 如何使用 auditd 记录 Linux 系统文件改动

auditd是Linux审计系统的用户空间组件，可以记录操作系统中的操作日志，包括文件读写、系统调用的记录等，出现问题可以用于审计。本文以CentOS 7.4 64位操作系统为例介绍auditd工具的安装和配置。

### auditd 相关工具命令与配置文件

#### 相关工具命令：

- auditctl：即时控制审计守护进程的行为的工具，比如添加规则。
- aureport：查看和生成审计报告的工具。
- ausearch：查找审计事件的工具。
- audispd：转发事件通知给其他应用程序，而不是写入到审计日志文件中。
- autrace：一个用于跟踪进程的命令。

#### 相关配置文件：

- /etc/audit/auditd.conf：auditd工具的配置文件
- /etc/audit/rules.d/audit.rules：包含审核规则的文件
- /etc/audit/audit.rules：记录审计规则的文件。

### 操作步骤

#### 安装auditd

1. 执行以下命令安装auditd工具。

```
yum install -y auditd*
```

#### 📖 说明

首次安装auditd后，审计规则默认为空，可通过sudo auditctl -l命令查询。

2. 执行以下命令查看运行状态。

```
service auditd status
```

图 6-74 运行状态

```
[root@ecs ~]# service auditd status
Redirecting to /bin/systemctl status auditd.service
● auditd.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2023-08-28 10:46:20 CST; 45min ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Main PID: 400 (auditd)
    CGroup: /system.slice/auditd.service
           └─400 /sbin/auditd

Aug 28 10:46:20 localhost.localdomain augenrules[404]: lost 0
Aug 28 10:46:20 localhost.localdomain augenrules[404]: backlog 0
Aug 28 10:46:20 localhost.localdomain augenrules[404]: enabled 1
Aug 28 10:46:20 localhost.localdomain augenrules[404]: failure 1
Aug 28 10:46:20 localhost.localdomain augenrules[404]: pid 400
Aug 28 10:46:20 localhost.localdomain augenrules[404]: rate_limit 0
Aug 28 10:46:20 localhost.localdomain augenrules[404]: backlog_limit 8192
Aug 28 10:46:20 localhost.localdomain augenrules[404]: lost 0
Aug 28 10:46:20 localhost.localdomain augenrules[404]: backlog 0
Aug 28 10:46:20 localhost.localdomain systemd[1]: Started Security Auditing Service.
```

### 配置审计规则

1. 执行以下命令配置监控文件和目录的更改。

```
auditctl -w /etc/passwd -p rwx
```

其中，

- w path：指定要监控的路径，上面的命令指定了监控的文件路径 /etc/passwd
- p：指定触发审计的文件/目录的访问权限
- rwx：指定的触发条件，r-读取权限，w-写入权限，x-执行权限，a-属性

2. 执行以下命令对/production目录的所有访问进行审计。

```
mkdir production
```

```
auditctl -w /production/
```

3. 执行以下命令查看所有已配置的规则。

```
auditctl -l
```

```
-w /etc/passwd -p rwx
-w /production -p rwx
```

4. 规则添加后，执行以下命令查看审计日志。

```
ausearch -f /etc/passwd
```

图 6-75 审计日志

```
time->Mon Aug 28 14:57:10 2023
type=PROCTITLE msg=audit(1693205830.281:154): proctitle=7375646f0061757365617266368002d66002f6574632f706173737764
type=PATH msg=audit(1693205830.281:154): item=0 name="/etc/passwd" inode=1314178 dev=fd:01 mode=0100644 ouid=0 ogid=0 rdev=00:00
_objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1693205830.281:154): cwd="/root"
type=SYSCALL msg=audit(1693205830.281:154): arch=c000003e syscall=2 success=yes exit=4 a0=7f9205d96552 a1=00000 a2=1b6 a3=24 ite
ms=1 ppid=7919 pid=18923 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=ttty1 ses=1 comm="sudo" exe="/usr/bin
/sudo" key=(null)
```

图6-75显示文件未被改动。其中各参数含义如下：

- time：审计时间。
- name：审计对象
- cwd：当前路径
- syscall：相关的系统调用
- auid：审计用户ID

- uid 和 gid : 访问文件的用户ID和用户组ID
  - comm : 用户访问文件的命令
  - exe : 上面命令的可执行文件路径
5. 修改监控文件添加一个用户“test”。  
**useradd test**
  6. 重新查看审计日志。  
**ausearch -f /etc/passwd**

**图 6-76 查看变更后的审计日志**

```
time->Mon Aug 28 15:35:52 2023
type=PROCTITLE msg=audit(1693208152.845:203): proctitle=7375646F0061757365561726368002D66002F6574632F706173737764
type=PATH msg=audit(1693208152.845:203): item=0 name="/etc/passwd" inode=1315998 dev=fd:81 mode=0100644 ouid=0 ogid=0 rdev=00:00
objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1693208152.845:203): cwd="/root"
type=SYSCALL msg=audit(1693208152.845:203): arch=c000003e syscall=2 success=yes exit=4 a0=7fd42775552 a1=00000 a2=1b6 a3=24 ite
ms=1 ppid=7919 pid=19834 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty1 ses=1 comm="sudo" exe="/usr/bin
/sudo" key="null"
```

**图6-76**显示在指定的时间，/etc/passwd被root用户(uid=0, gid=0)在/root目录下修改。/etc/passwd文件是使用/usr/bin/sudo访问的。

7. 此时，通过执行以下命令查看日志无内容。  
**ausearch -f /production**

```
[root@ecs ~]# ausearch -f /production
<no matches>
```

8. 使用root账户修改目录权限，并重新查看审计日志。  
**chmod -R 777 /test/**  
**ausearch -f /test/**
9. 执行以下命令查看审计报告。  
**aureport**



图 6-77 查看审计报告

```
[root@ecs ~]# aureport
Summary Report
=====
Range of time in logs: 01/01/1970 08:00:00.000 - 08/28/2023 18:11:02.564
Selected time for report: 01/01/1970 08:00:00 - 08/28/2023 18:11:02.564
Number of changes in configuration: 4
Number of changes to accounts, groups, or roles: 1
Number of logins: 4
Number of failed logins: 0
Number of authentications: 1
Number of failed authentications: 0
Number of users: 2
Number of terminals: 4
Number of host names: 3
Number of executables: 7
Number of commands: 3
Number of files: 0
Number of AUC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 12
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 15
Number of events: 140
```

10. 执行以下命令查看授权失败的详细信息。

```
aureport -au
```

图 6-78 查看授权失败信息

```
[root@ecs ~]# aureport -au
Authentication Report
=====
# date time acct host term exe success event
=====
1. 08/28/2023 17:33:52 root ecs-... tty1 /usr/bin/login yes 60
```

11. 执行以下命令查看所有账户与修改相关的事件。

```
aureport -m
```

图 6-79 查看账户修改相关事件

```
[root@ecs ~]# aureport -m
Account Modifications Report
=====
# date time auid addr term exe acct success event
=====
1. 08/28/2023 17:26:24 -1 ? ? /usr/sbin/chpasswd ? yes 50
```

12. (可选) 执行以下命令清空定义的规则。

```
auditctl -D
auditctl -l
```

图 6-80 清空规则

```
[root@ecs-... ~]# auditctl -D
No rules
[root@ecs-... ~]# auditctl -l
No rules
```

## 6.11 通过 Extundelete 恢复弹性云服务器误删除数据 (Linux)

### 应用场景

Extundelete是一款文件恢复工具，支持恢复ext3及ext4文件系统类型的误删除文件。

#### 须知

误删除文件的恢复程度与如下因素有关：

- 文件删除后是否被写覆盖
- 元数据是否存留在journal

如果误删除的数据位于系统盘，且一直有业务进程或系统进程在写入文件，则可能无法通过此方法进行恢复。

为了提高数据安全性，建议您通过[创建快照](#)、[创建私有镜像](#)、[创建云硬盘备份](#)等方式定期进行数据备份。

本文以操作系统为CentOS 7.5的云服务器为例，介绍如何使用开源工具Extundelete快速恢复被误删除的数据。

### 前提条件

在执行数据恢复操作前，请完成以下准备工作：

- 参考[创建快照](#)或[创建私有镜像](#)完成数据备份，以确保数据恢复出现问题时可恢复至初始状态。
- 停止相关业务程序继续写数据到该文件系统。若需执行恢复操作的为数据盘，则先对数据盘执行umount操作。

### 实施步骤

**步骤1** 安装Extundelete。

1. 登录弹性云服务器。
2. 依次执行以下命令，安装 Extundelete 所需依赖及库。

```
yum install libcom_err e2fsprogs-devel
```

```
yum install gcc gcc-c++
```

3. 在出现如下提示时，输入“y”。

```
Installed size: 25 M
Is this OK [y/d/N]: y
```

4. 执行以下命令，[下载](#) Extundelete 源码。  
`wget https://github.com/curu/extundelete/archive/refs/tags/v1.0.tar.gz`
5. 执行以下命令，解压 v1.0.tar.gz 文件。  
`tar xf v1.0.tar.gz`
6. 依次执行以下命令，进行编译安装。  
`cd extundelete-1.0`  
`./configure`  
`make`
7. 执行以下命令，进入 src 目录，可查看已编译好的 Extundelete 文件。  
`cd ./src`

**步骤2** 执行以下命令，尝试恢复数据。

```
./extundelete --restore-all /dev/对应盘
```

恢复后的文件位于同级目录的“RECOVERED\_FILES”文件夹下。

----结束

## 6.12 搭建 ThinkPHP 框架

### 简介

ThinkPHP遵循Apache2开源许可协议发布，是一个免费、开源、快速、简单的面向对象的轻量级PHP开发框架，是为了敏捷WEB应用开发和简化企业应用开发而诞生。本文介绍如何在华为云上使用CentOS 7.2操作系统的实例搭建ThinkPHP框架。

### 前提条件

- 已购买一台弹性云服务器，且已为其绑定弹性公网IP。
- 弹性云服务器所在安全组添加了如下表所示的安全组规则，具体步骤参见[为安全组添加安全组规则](#)。

表 6-10 安全组规则

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	TCP: 22	0.0.0.0/0
入方向	1	允许	IPv4	TCP: 443	0.0.0.0/0
入方向	1	允许	IPv4	TCP: 8000	0.0.0.0/0

- 为了更好的获取和更新系统和软件，建议您更新镜像源为华为云镜像源，详细操作，请参见[如何使用自动化工具配置华为云镜像源\(x86\\_64和ARM\)?](#)。

### 操作步骤

1. 安装PHP。

- a. 执行以下命令，安装EPEL源和Remi仓库。

```
sudo yum install -y epel-release
sudo yum install -y https://rpms.remirepo.net/enterprise/remi-release-7.rpm
```

- b. 执行以下命令，启用PHP 8.0仓库。

```
sudo yum -y install yum-utils
sudo yum-config-manager --enable remi-php80
```

- c. 执行以下命令，安装PHP。

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

- d. 执行以下命令，验证PHP的安装版本。

```
php -v
```

回显如下类似信息：

```
PHP 8.0.30 (cli) (built: Jun 4 2024 15:19:49) ( NTS gcc x86_64 )
Copyright (c) The PHP Group
Zend Engine v4.0.30, Copyright (c) Zend Technologies
```

## 2. 安装Composer。

Composer是PHP编程语言的包管理器，提供管理PHP软件依赖和所需库的标准格式。

- a. 执行以下命令，安装Composer所需依赖。

```
sudo yum install -y unzip git
```

- b. 执行以下命令，安装Composer。

```
curl -sS https://getcomposer.org/installer | php
sudo mv composer.phar /usr/local/bin/composer
```

- c. 执行以下命令，查看Composer版本。

```
composer --version
```

回显如下类似信息：

```
Composer version 2.7.7 2024-06-10 22:11:12
PHP version 8.0.30 (/usr/bin/php)
```

## 3. 安装ThinkPHP。

- a. 使用Composer创建一个新的ThinkPHP应用程序。

该命令会在当前目录下创建一个名为my-thinkphp-app的目录，并下载ThinkPHP的核心文件和依赖项。

```
composer create-project tophink/think my-thinkphp-app
```

- b. 切换到新创建的ThinkPHP应用程序目录，启动ThinkPHP内置服务器进行开发。

```
cd my-thinkphp-app
```

```
php think run
```

回显如下类似信息，表示ThinkPHP已启动。

```
[root@ ~]# cd my-thinkphp-app
[root@ ~ my-thinkphp-app]# php think run
ThinkPHP Development server is started On <http://0.0.0.0:8000/>
You can exit with `CTRL-C`
Document root is: /root/my-thinkphp-app/public
[Thu Jul 4 16:07:47 2024] PHP 8.0.30 Development Server (http://0.0.0.0:8000) started
```

- c. 安装完成后，可通过浏览器访问“<http://云服务器弹性公网IP:8000>”，显示如下页面，说明ThinkPHP安装成功。

# 7 云服务器安全

## 7.1 Linux 云服务器 SSH 登录的安全加固

Linux云服务器常用的登录方式是SSH，对于密码登录方式创建的云服务器，如何保证登录安全性呢？本文以CentOS 7.6为例，对SSH登录进行安全加固。

表 7-1 弹性云服务器详细信息

参数	取值
名称	ecs-f5a2
操作系统	CentOS 7.6 64bit
弹性公网IP	119.3.xxx.x
登录方式	密码

### 修改默认端口

1. 通过**SSH密码方式**远程登录云服务器。
2. 执行以下命令，修改SSH登录的默认端口，比如修改为“5000”。

```
vim /etc/ssh/sshd_config
```

按“i”进入编辑模式，在第17行，将注释符“#”删掉，修改为“Port 5000”。

图 7-1 修改前

```
#  
#Port 22  
#AddressFamily any  
#ListenAddress 0.0.0.0  
#ListenAddress ::
```

图 7-2 修改后

```
Port 5000
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

- 按“Esc”，输入:wq保存并退出。

## 增加防火墙规则：开放指定端口

CentOS 7系列操作系统的默认防火墙是fireware，而不是iptables。因此，如果系统是默认防火墙，则不需要执行本节操作；如果安装过iptables，则要参考本节指导开放SSH登录的5000端口。

- 执行以下命令，检查是否安装了iptables。

### service iptables status

- 如果提示如下类似信息，表示未安装iptables，跳过本节，继续[添加安全组规则](#)操作。

```
[root@ecs-~]# service iptables status
Redirecting to /bin/systemctl status iptables.service
Unit iptables.service could not be found.
[root@ecs-~]#
```

- 如果提示如下类似信息，表示安装了iptables，并且为“active”状态。继续执行步骤2。

```
[root@ecs-~]# service iptables status
Redirecting to /bin/systemctl status iptables.service
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; disabled; vendor preset: disabled)
   Active: active (exited) since Tue 2019-04-16 10:42:53 CST; 3s ago
     Process: 23744 ExecStart=/usr/libexec/iptables/iptables.init start (code=exited, status=0/SUCCESS)
    Main PID: 23744 (code=exited, status=0/SUCCESS)

Apr 16 10:42:53 ecs- systemd[1]: Starting IPv4 firewall with iptables...
Apr 16 10:42:53 ecs- iptables.init[23744]: iptables: Applying firewall rules: [ OK ]
Apr 16 10:42:53 ecs- systemd[1]: Started IPv4 firewall with iptables.
```

- 执行以下命令增加iptables规则，开放5000端口。

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


- 执行以下命令查看iptables现有规则是否已包含5000端口。

### iptables -L -n

```
chain INPUT (policy ACCEPT)
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
```

## 添加安全组规则

安全组中的入方向规则默认开启了22端口，当云服务器的SSH登录端口修改为5000时，需要为安全组新加一条规则。

- 登录管理控制台。
- 选择“计算 > 弹性云服务器”，进入云服务器控制台。
- 单击云服务器名称“ecs-f5a2”进入详情页面。
- 选择“安全组”页签，单击  展开安全组规则详情，单击列表右上角的“更改安全组规则”。

5. 添加一条入方向规则，如图7-3所示。

图 7-3 安全组规则



优先级	策略	类型	协议端口	源地址	描述
1	允许	IPv4	TCP: 5000	0.0.0.0/0	-
1	允许	IPv4	TCP: 22	0.0.0.0/0	-
1	允许	IPv4	TCP: 443	0.0.0.0/0	允许使用HTTPS协议访问网站

## 关闭密码登录，采用密钥登录

在管理控制台创建一个密钥对，绑定至云服务器，使云服务器登录方式切换为密钥。

1. 登录管理控制台。
2. 选择“计算 > 弹性云服务器”，进入云服务器控制台。
3. 参考[创建密钥对](#)创建一个密钥对，妥善保管好私钥文件。
4. 选择“服务列表 > 安全 > 数据加密服务”，单击左侧导航中的“密钥对管理”。
5. 选择“云服务器列表”页签，在“ecs-f5a2”所在行，单击操作列的“绑定”。按照图7-5进行配置，单击“确定”。

关闭密码登录，请在绑定密钥对页面勾选“关闭密码登录方式。”或编辑“ssh\_config”配置文件，禁止密码登录。

图 7-4 绑定密钥对



绑定密钥对

系统将对服务器进行密钥对配置，执行此操作后可直接使用密钥登录服务器。出于安全考虑，建议关闭服务器的密码登录方式，只使用密钥登录服务器。

ECS名称: [模糊]

IP: [模糊]

状态: 运行中

\* 新密钥对: KeyPair-[模糊]

\* root密码: [模糊]

关闭密码登录方式。了解详情

我已经阅读并同意《密钥对管理服务免责声明》。

确定 取消

6. 登录云服务器操作系统，编辑“ssh\_config”配置文件，禁止密码登录。

```
vim /etc/ssh/sshd_config
```

按“i”进入编辑模式，在最后几行按下图进行配置。



```
# override default of no subsystems
Subsystem sftp /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
PermitRootLogin yes
UseDNS no
PasswordAuthentication no
```

参数说明：

- PermitRootLogin：是否允许root账户登录，配置为“yes”。
- UseDNS：是否允许DNS解析，配置为“no”。
- PasswordAuthentication：是否允许使用密码登录，配置为“no”。

#### 📖 说明

在步骤5中为云服务器绑定密钥对时，已勾选了“关闭密码登录方式”，此处的“PasswordAuthentication”必为“no”，只需验证即可。

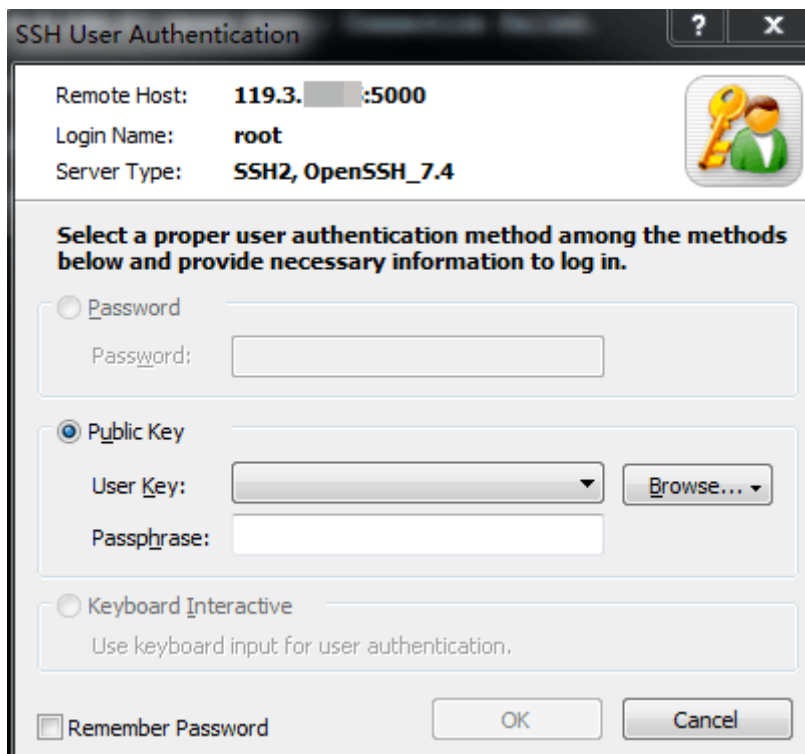
按“Esc”，输入:wq保存并退出。

7. 完成后，重启sshd服务。

**systemctl restart sshd**

8. 通过Xshell或其他SSH客户端连接云服务器，密码登录会被限制（如图7-5所示，密码输入项置灰），则证明配置成功。

图 7-5 Xshell 登录云服务器



## 编辑 hosts.allow 和 hosts.deny

“/etc/hosts.allow”和“/etc/hosts.deny”是控制远程访问的文件，通过配置该文件可以允许或者拒绝某个IP或者IP段的客户访问Linux云服务器的某项服务。

比如SSH服务，通常只对管理员开放，那就可以禁用不必要的IP，而只开放管理员可能使用到的IP段。

因为云服务器需要在不同地点登录，建议编辑“/etc/hosts.allow”允许所有IP地址登录，这样不会影响正常使用。

**vim /etc/hosts.allow**

在最后一行增加“sshd:ALL”。

```
#          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
```

可以通过一些方法识别云服务器的安全风险，比如检查SSH状态，查看疑似恶意登录的IP，然后在“/etc/hosts.deny”中将这些地址禁止。

## 7.2 使用虚拟 IP 和 Keepalived 搭建高可用 Web 集群

### 应用场景

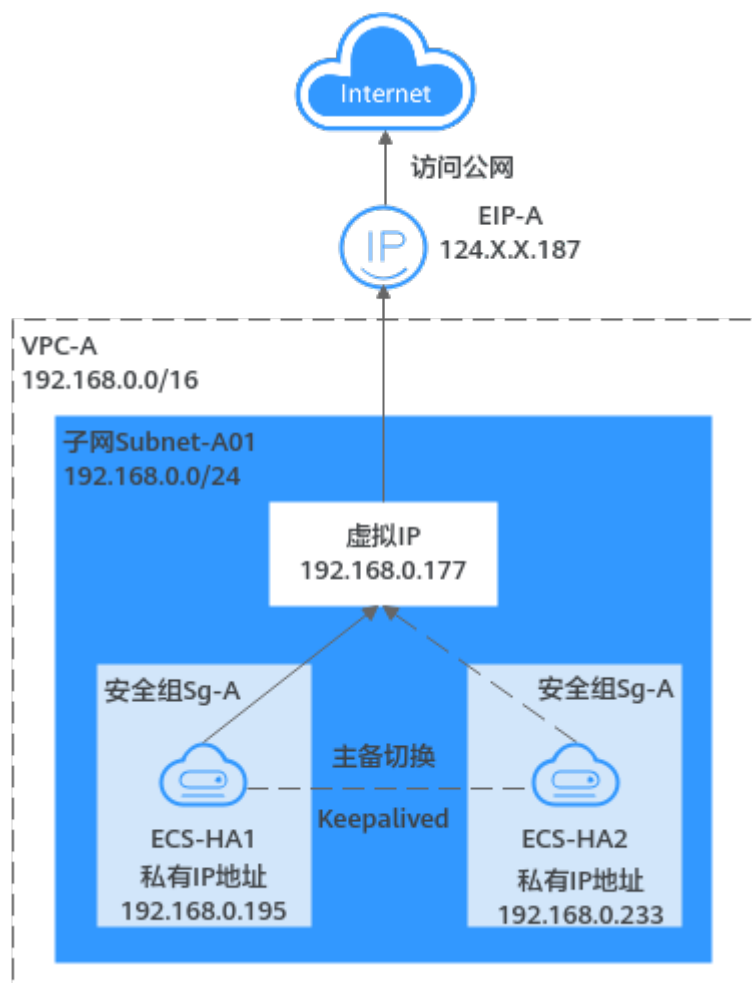
虚拟IP（Virtual IP Address）是从VPC子网网段中划分的一个内网IP地址，通常搭配高可用软件（比如Keepalived）使用，主要用来搭建高可用的主备集群。多个云服务器形成主备集群，当主云服务器发生故障无法对外提供服务时，系统动态将虚拟IP切换到备云服务器，通过备云服务器继续对外提供服务。本文档为您介绍详细介绍使用虚拟IP和Keepalived搭建高可用Web集群的方法。

### 方案架构

本示例中，高可用Web集群架构如图7-6所示，将虚拟IP同时绑定至ECS-HA1和ECS-HA2，使用Keepalived搭建一个高可用集群。同时，为虚拟IP绑定EIP，该集群具备公网访问能力，可以面向公网提供Web访问服务。实现原理如下：

1. ECS-HA1作为主云服务器，通过与虚拟IP绑定的EIP对外提供服务，ECS-HA2作为备云服务器不承载实际业务。
2. 当ECS-HA1发生故障时，此时会自动启用ECS-HA2，ECS-HA2将会接管业务并对外提供服务，实现业务不中断的高可用需求。

图 7-6 使用虚拟 IP 和 Keepalived 搭建高可用 Web 集群



## 方案优势

基于虚拟IP和Keepalived能力，采用“一主一备”或“一主多备”的方法组合使用云服务器，这些云服务器对外呈现为一个虚拟IP。当主云服务器故障时，备云服务器可以转为主云服务器并继续对外提供服务，以此达到高可用性HA（High Availability）的目的，可以解决用户由于云服务器故障导致的对外服务中断问题。

## 约束与限制

使用虚拟IP搭建的高可用集群，所有服务器必须位于同一个虚拟私有云的子网内。

## 资源规划说明

本示例中，虚拟私有云VPC和子网、虚拟IP、弹性公网IP以及弹性云服务器ECS等资源只要位于同一个区域内即可，可用区可以任意选择，无需保持一致。

### 📖 说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

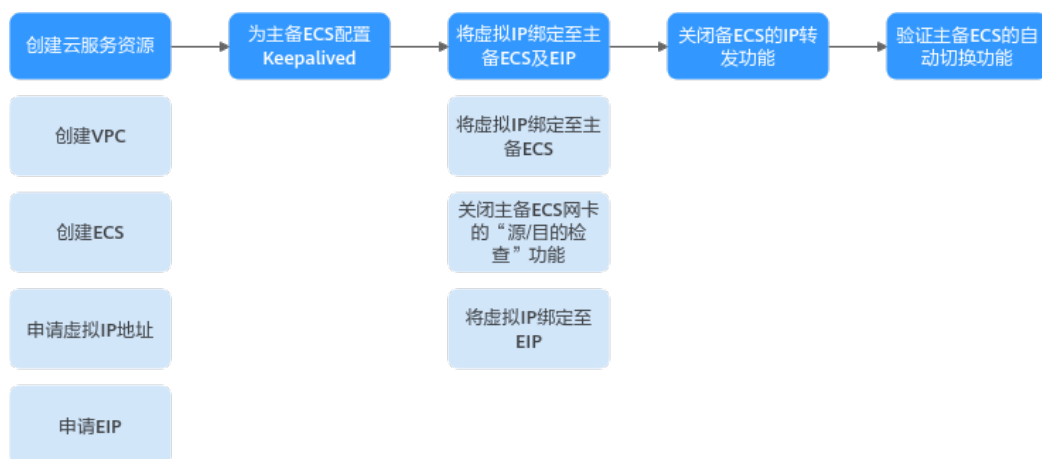
表 7-2 使用虚拟 IP 和 Keepalived 搭建高可用 Web 集群资源规划总体说明

资源类型	资源数量	说明
虚拟私有云 VPC和子网	1	<ul style="list-style-type: none"><li>● VPC名称：请根据实际情况填写，本示例为VPC-A。</li><li>● IPv4网段：请根据实际情况填写，本示例为 192.168.0.0/16。</li><li>● 子网名称：请根据实际情况填写，本示例为Subnet-A01。</li><li>● 子网IPv4网段：请根据实际情况填写，本示例为 192.168.0.0/24。</li></ul>
弹性云服务器 ECS	2	<p>本示例中，需要两个ECS作为主备倒换，配置说明如下：</p> <ul style="list-style-type: none"><li>● 名称：根据实际情况填写，本示例分别为ECS-HA1和ECS-HA2。</li><li>● 镜像：请根据实际情况选择，本示例为公共镜像（CentOS 7.8 64bit）。</li><li>● 系统盘：通用型SSD盘，40GB。</li><li>● 数据盘：本示例未选购数据盘，请您根据实际业务需求选购数据盘，并切实考虑两个ECS节点之间的业务数据一致性问题。</li><li>● 网络：<ul style="list-style-type: none"><li>- 虚拟私有云：选择您的虚拟私有云，本示例为VPC-A。</li><li>- 子网：选择子网，本示例为Subnet-A01。</li></ul></li><li>● 安全组：请根据实际情况选择，本示例中ECS-HA1和ECS-HA2使用同一个安全组，安全组名称为Sg-A。</li><li>● 私有IP地址：ECS-HA1为192.168.0.195，ECS-HA2为192.168.0.233</li></ul>
虚拟IP	1	<p>在子网Subnet-A01中申请虚拟IP地址：</p> <ul style="list-style-type: none"><li>● 创建方式：根据实际情况填写，本示例为自动分配。</li><li>● 虚拟IP地址：本示例为192.168.0.177。</li><li>● 绑定实例：将虚拟IP绑定至ECS-HA1和ECS-HA2。</li><li>● 绑定弹性公网IP：将虚拟IP绑定至EIP-A。</li></ul>
弹性公网IP	1	<ul style="list-style-type: none"><li>● 计费模式：请根据情况选择计费模式，本示例为按需计费。</li><li>● EIP名称：请根据实际情况填写，本示例为EIP-A。</li><li>● EIP地址：EIP地址系统随机分配，本示例为 124.X.X.187。</li></ul>

## 操作流程

使用虚拟IP和Keepalived搭建高可用Web集群，流程如图7-7所示。

图 7-7 使用虚拟 IP 和 Keepalived 搭建高可用 Web 集群



## 步骤一：创建云服务资源

1. 创建1个VPC和1个子网。  
具体方法请参见[创建虚拟私有云和子网](#)。
2. 创建2个ECS，分别作为主ECS和备ECS。  
具体方法请参见[自定义购买ECS](#)。

本示例中，ECS的网络配置详情如下：

- 网络：选择已创建的虚拟私有云和子网，VPC-A和Subnet-A01。
- 安全组：新建一个安全组Sg-A，并添加入方向和出方向规则。您在创建安全组的时候，系统会自动添加部分规则，您需要根据实际情况进行检查修改。

本示例中，ECS-HA1和ECS-HA2属于同一个安全组，您需要确保表7-3中的规则均已正确添加。

表 7-3 安全组 Sg-A 规则说明

方向	策略	类型	协议端口	源地址/目的地址	描述
入方向	允许	IPv4	TCP: 22	源地址: 0.0.0.0/0	放通安全组内ECS的SSH(22)端口，用于远程登录Linux ECS。
入方向	允许	IPv4	TCP: 3389	源地址: 0.0.0.0/0	放通安全组内ECS的RDP(3389)端口，用于远程登录Windows ECS。
入方向	允许	IPv4	TCP: 80	源地址: 0.0.0.0/0	放通安全组内ECS的HTTP(80)端口，用于外部通过HTTP协议访问ECS上部署的网站。
入方向	允许	IPv4	全部	源地址: 当前安全组Sg-A	针对IPv4，用于安全组内ECS之间网络互通。
入方向	允许	IPv6	全部	源地址: 当前安全组Sg-A	针对IPv6，用于安全组内ECS之间网络互通。

方向	策略	类型	协议端口	源地址/目的地址	描述
出方向	允许	IPv4	全部	目的地址： 0.0.0.0/0	针对IPv4，用于安全组内ECS访问外部，允许流量从安全组内ECS流出。
出方向	允许	IPv6	全部	目的地 址：::/0	针对IPv6，用于安全组内ECS访问外部，允许流量从安全组内ECS流出。

### 须知

本示例中，源地址设置为0.0.0.0/0表示允许所有外部IP远程登录云服务器，为了确保安全，建议您遵循最小原则，根据实际情况将源IP设置为特定的IP地址，比如，源地址设置为您的本地PC地址。

如果您的ECS位于不同的安全组，比如ECS-HA1属于Sg-A，ECS-HA2属于Sg-B，则除了在两个安全组中分别配置表7-3中的规则，您还需要添加表7-4中的规则，放通两个安全组之间的内网网络流量。

表 7-4 安全组 Sg-A 和 Sg-B 规则说明

安全组	方向	策略	类型	协议端口	源地址/目的地址	描述
Sg-A	入方向	允许	IPv4	全部	源地址： Sg-B	针对全部IPv4协议，允许来自Sg-B内实例的流量访问Sg-A内的实例。
Sg-B	入方向	允许	IPv4	全部	源地址： Sg-A	针对全部IPv4协议，允许来自Sg-A内实例的流量访问Sg-B内的实例。

- 弹性公网IP：选择“暂不购买”。
- 3. 在子网Subnet-A01内，申请虚拟IP地址。  
具体方法请参见[申请虚拟IP地址](#)。
- 4. 申请弹性公网IP。  
具体方法请参见[购买弹性公网IP](#)。

## 步骤二：为主备 ECS 配置 Keepalived

1. 执行以下操作，为ECS-HA1配置Keepalived。
  - a. 将EIP绑定至ECS-HA1。  
具体方法请参见[绑定弹性公网IP](#)。
  - b. 远程登录ECS-HA1。  
ECS有多种登录方法，具体请参见[登录弹性云服务器](#)。

- c. 执行以下命令，安装Nginx、Keepalived软件包及相关依赖包。

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

回显类似如下信息，表示安装完成。

```
[root@ecs-ha1 ~]# yum install nginx keepalived -y
Loaded plugins: fastestmirror
Determining fastest mirrors
base
           | 3.6 kB  00:00:00
epel
           | 4.3 kB  00:00:00
extras
           | 2.9 kB  00:00:00
updates
           | 2.9 kB  00:00:00
(1/7): epel/x86_64/
group
       | 399 kB  00:00:00
(2/7): epel/x86_64/
updateinfo
       | 1.0 MB  00:00:00
(3/7): base/7/x86_64/
primary_db
       | 6.1 MB  00:00:00
(4/7): base/7/x86_64/
group_gz
       | 153 kB  00:00:00
(5/7): epel/x86_64/
primary_db
       | 8.7 MB  00:00:00
(6/7): extras/7/x86_64/
primary_db
       | 253 kB  00:00:00
(7/7): updates/7/x86_64/primary_db

.....
Dependency Installed:
  centos-indexhtml.noarch 0:7-9.el7.centos          gperftools-libs.x86_64
  0:2.6.1-1.el7           lm_sensors-libs.x86_64 0:3.4.0-8.20160601gitf9185e5.el7_9.1
  net-snmp-agent-libs.x86_64 1:5.7.2-49.el7_9.4    net-snmp-libs.x86_64
  1:5.7.2-49.el7_9.4      nginx-filessystem.noarch 1:1.20.1-10.el7
  openssl11-libs.x86_64 1:1.1.1k-7.el7

Complete!
```

- d. 执行以下操作，修改Nginx配置文件，添加80端口相关配置。

- i. 执行以下命令，打开“/etc/nginx/nginx.conf”文件。

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

- ii. 按i进入编辑模式。

- iii. 将文件中原有的内容，全部替换成以下内容。

```
user root;
worker_processes 1;
#error_log logs/error.log;
#error_log logs/error.log notice;
#error_log logs/error.log info;
#pid logs/nginx.pid;
events {
    worker_connections 1024;
}
http {
    include mime.types;
    default_type application/octet-stream;
    #log_format main '$remote_addr - $remote_user [$time_local] "$request" '
    # '$status $body_bytes_sent "$http_referer" '
    # '"$http_user_agent" "$http_x_forwarded_for"';
    #access_log logs/access.log main;
```

```
sendfile on;
#tcp_nopush on;
#keepalive_timeout 0;
keepalive_timeout 65;
#gzip on;
server {
    listen 80;
    server_name localhost;
    #charset koi8-r;
    #access_log logs/host.access.log main;
    location / {
        root html;
        index index.html index.htm;
    }
    #error_page 404 /404.html;
    # redirect server error pages to the static page /50x.html
    error_page 500 502 503 504 /50x.html;
    location = /50x.html {
        root html;
    }
}
```

- iv. 按ESC退出，并输入:wq!保存配置。
- e. 执行以下操作，修改index.html文件内容，用来验证网站的访问情况。
  - i. 执行以下命令，打开“/usr/share/nginx/html/index.html”文件。

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

- ii. 按i进入编辑模式。
  - iii. 将文件中原有的内容，全部替换成以下内容。  
Welcome to ECS-HA1
  - iv. 按ESC退出，并输入:wq!保存配置。
- f. 执行以下命令，设置Nginx服务开机自启动，并启动Nginx服务。

```
systemctl enable nginx
```

```
systemctl start nginx.service
```

回显类似如下信息：

```
[root@ecs-ha1 ~]# systemctl enable nginx
Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service to /usr/lib/systemd/system/nginx.service.
[root@ecs-ha1 ~]# systemctl start nginx.service
```

- g. 打开浏览器，并输入EIP地址（124.X.X.187），验证Nginx单节点的访问情况。

网页如下图所示，表示ECS-HA1的Nginx配置成功。

图 7-8 ECS-HA1 访问验证



Welcome to ECS-HA1

- h. 执行以下操作，修改Keepalived配置文件。
    - i. 执行以下命令，打开“/etc/keepalived/keepalived.conf”文件。  
**vim /etc/keepalived/keepalived.conf**
    - ii. 按i进入编辑模式。



- iii. 根据实际情况，替换配置文件中的IP参数，并将文件中原有的内容，全部替换成以下内容。
  - o mcast\_src\_ip和unicast\_src\_ip：替换为ECS-HA1的私有IP地址，本示例为192.168.0.195。
  - o virtual\_ipaddress：替换为虚拟IP地址，本示例为192.168.0.177。

```
! Configuration File for keepalived
global_defs {
router_id master-node
}
vrrp_script chk_http_port {
script "/etc/keepalived/chk_nginx.sh"
interval 2
weight -5
fall 2
rise 1
}
vrrp_instance VI_1 {
state BACKUP
interface eth0
mcast_src_ip 192.168.0.195
virtual_router_id 51
priority 100
advert_int 1
authentication {
auth_type PASS
auth_pass 1111
}
unicast_src_ip 192.168.0.195
virtual_ipaddress {
192.168.0.177
}
track_script {
chk_http_port
}
}
```

- iv. 按ESC退出，并输入:wq!保存配置。
- i. 执行以下操作，配置Nginx监控脚本。
  - i. 执行以下命令，打开“/etc/keepalived/chk\_nginx.sh”文件。

```
vim /etc/keepalived/chk_nginx.sh
```

- ii. 按i进入编辑模式。
- iii. 将文件中原有的内容，全部替换成以下内容。

```
#!/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
```

- iv. 按ESC退出，并输入:wq!保存配置。
- j. 执行以下命令，为“chk\_nginx.sh”文件添加执行权限。

```
chmod +x /etc/keepalived/chk_nginx.sh
```
- k. 执行以下命令，设置Keepalived服务开机自启动，并启动Keepalived服务。

```
systemctl enable keepalived
systemctl start keepalived.service
```

- l. 将EIP和ECS-HA1解绑定。  
具体方法请参见[解绑弹性公网IP](#)。
2. 执行以下操作，为ECS-HA2配置Keepalived。
  - a. 将EIP绑定至ECS-HA2。  
具体方法请参见[绑定弹性公网IP](#)。
  - b. 远程登录ECS-HA2。  
ECS有多种登录方法，具体请参见[登录弹性云服务器](#)。
  - c. 执行以下命令，安装Nginx、Keepalived软件包及相关依赖包。

### **yum install nginx keepalived -y**

回显类似如下信息，表示安装完成。

```
[root@ecs-ha2 ~]# yum install nginx keepalived -y
Loaded plugins: fastestmirror
Determining fastest mirrors
base                                | 3.6 kB  00:00:00
epel                                | 4.3 kB  00:00:00
extras                              | 2.9 kB  00:00:00
updates                             | 2.9 kB  00:00:00
(1/7): epel/x86_64/
group                               | 399 kB  00:00:00
(2/7): epel/x86_64/
updateinfo                          | 1.0 MB  00:00:00
(3/7): base/7/x86_64/
primary_db                          | 6.1 MB  00:00:00
(4/7): base/7/x86_64/
group_gz                             | 153 kB  00:00:00
(5/7): epel/x86_64/
primary_db                          | 8.7 MB  00:00:00
(6/7): extras/7/x86_64/
primary_db                          | 253 kB  00:00:00
(7/7): updates/7/x86_64/primary_db

.....
Dependency Installed:
  centos-indexhtml.noarch 0:7-9.el7.centos          gperftools-libs.x86_64
  0:2.6.1-1.el7           lm_sensors-libs.x86_64 0:3.4.0-8.20160601gitf9185e5.el7_9.1
  net-snmp-agent-libs.x86_64 1:5.7.2-49.el7_9.4      net-snmp-libs.x86_64
  1:5.7.2-49.el7_9.4      nginx-filessystem.noarch 1:1.20.1-10.el7
  openssl11-libs.x86_64 1:1.1.1k-7.el7

Complete!
```

- d. 执行以下操作，修改Nginx配置文件，添加80端口相关配置。
  - i. 执行以下命令，打开“/etc/nginx/nginx.conf”文件。

### **vim /etc/nginx/nginx.conf**

- ii. 按i进入编辑模式。

- iii. 将文件中原有的内容，全部替换成以下内容。

```
user root;
worker_processes 1;
#error_log logs/error.log;
#error_log logs/error.log notice;
```

```
#error_log logs/error.log info;
#pid logs/nginx.pid;
events {
    worker_connections 1024;
}
http {
    include mime.types;
    default_type application/octet-stream;
    #log_format main '$remote_addr - $remote_user [$time_local] "$request" '
    # '$status $body_bytes_sent "$http_referer" '
    # '"$http_user_agent" "$http_x_forwarded_for"';
    #access_log logs/access.log main;
    sendfile on;
    #tcp_nopush on;
    #keepalive_timeout 0;
    keepalive_timeout 65;
    #gzip on;
    server {
        listen 80;
        server_name localhost;
        #charset koi8-r;
        #access_log logs/host.access.log main;
        location / {
            root html;
            index index.html index.htm;
        }
        #error_page 404 /404.html;
        # redirect server error pages to the static page /50x.html
        error_page 500 502 503 504 /50x.html;
        location = /50x.html {
            root html;
        }
    }
}
```

- iv. 按ESC退出，并输入:wq!保存配置。
- e. 执行以下操作，修改index.html文件内容，用来验证网站的访问情况。
  - i. 执行以下命令，打开“/usr/share/nginx/html/index.html”文件。  
**vim /usr/share/nginx/html/index.html**
  - ii. 按i进入编辑模式。
  - iii. 将文件中原有的内容，全部替换成以下内容。  
Welcome to ECS-HA2
  - iv. 按ESC退出，并输入:wq!保存配置。
- f. 执行以下命令，设置Nginx服务开机自启动，并启动Nginx服务。

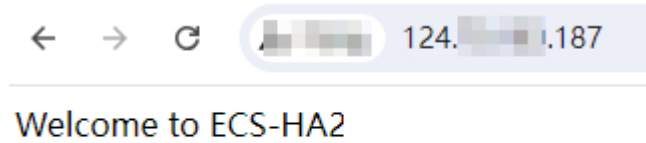
```
systemctl enable nginx
systemctl start nginx.service
```

回显类似如下信息：

```
[root@ecs-ha2 ~]# systemctl enable nginx
Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service to /usr/lib/
systemd/system/nginx.service.
[root@ecs-ha2 ~]# systemctl start nginx.service
```

- g. 打开浏览器，并输入EIP地址（124.X.X.187），验证Nginx单节点的访问情况。  
网页如下图所示，表示ECS-HA2的Nginx配置成功。

图 7-9 ECS-HA2 访问验证



- h. 执行以下操作，修改Keepalived配置文件。
- 执行以下命令，打开“/etc/keepalived/keepalived.conf”文件。  
**vim /etc/keepalived/keepalived.conf**
  - 按*i*进入编辑模式。
  - 根据实际情况，替换配置文件中的IP参数，并将文件中原有的内容，全部替换成以下内容。
    - mcast\_src\_ip和unicast\_src\_ip：替换为ECS-HA2的私有IP地址，本示例为192.168.0.233。
    - virtual\_ipaddress：替换为虚拟IP地址，本示例为192.168.0.177。

```
! Configuration File for keepalived
global_defs {
    router_id master-node
}
vrrp_script chk_http_port {
    script "/etc/keepalived/chk_nginx.sh"
    interval 2
    weight -5
    fall 2
    rise 1
}
vrrp_instance VI_1 {
    state BACKUP
    interface eth0
    mcast_src_ip 192.168.0.233
    virtual_router_id 51
    priority 100
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    unicast_src_ip 192.168.0.233
    virtual_ipaddress {
        192.168.0.177
    }
}
track_script {
    chk_http_port
}
```

- 按ESC退出，并输入:wq!保存配置。
- 执行以下操作，配置Nginx监控脚本。
  - 执行以下命令，打开“/etc/keepalived/chk\_nginx.sh”文件。  
**vim /etc/keepalived/chk\_nginx.sh**
  - 按*i*进入编辑模式。
  - 将文件中原有的内容，全部替换成以下内容。

```
#!/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
```

- iv. 按ESC退出，并输入:wq!保存配置。
- j. 执行以下命令，为“chk\_nginx.sh”文件添加执行权限。  
**chmod +x /etc/keepalived/chk\_nginx.sh**
- k. 执行以下命令，设置Keepalived服务开机自启动，并启动Keepalived服务。  
**systemctl enable keepalived**  
**systemctl start keepalived.service**
- l. 将EIP和ECS-HA2解绑定。  
具体方法请参见[解绑弹性公网IP](#)。

### 步骤三：将虚拟 IP 绑定至主备 ECS 及 EIP


1. 将虚拟IP分别绑定至主备ECS上，本示例中需要绑定ECS-HA1和ECS-HA2。  
具体操作请参见[将虚拟IP地址绑定至实例或EIP](#)。
2. 关闭主备ECS网卡的“源/目的检查”功能。  
将虚拟IP绑定至ECS时，系统会自动关闭ECS网卡的“源/目的检查”功能，您需要参考以下操作检查关闭情况。如果未关闭，则请关闭该功能。
  - a. 在ECS列表中，单击目标ECS的名称。  
进入ECS详情页。
  - b. 选择“弹性网卡”页签，并单击  展开ECS的网卡详情区域，可以查看“源/目的检查”功能。  
如[图7-10](#)所示，表示“源/目的检查”功能已关闭。

图 7-10 关闭网卡的“源/目的检查”功能



3. 将虚拟IP绑定至EIP上，本示例中需要绑定EIP-A。  
具体操作请参见[将虚拟IP地址绑定至实例或EIP](#)。

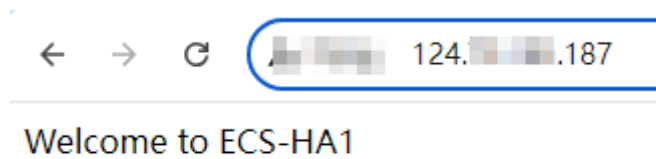
## 步骤四：关闭备 ECS 的 IP 转发功能

使用虚拟IP构建主备场景的高可用集群时，需要关闭备ECS的IP转发功能，当主备ECS切换后，则需要确保新的备ECS也关闭IP转发功能。

为了避免ECS主备切换后遗漏配置，建议您将主备ECS的IP转发功能全都关闭。

1. 打开浏览器，并输入EIP地址（124.X.X.187），通过网页确认主ECS。  
网页如下图所示，表示此时主ECS是ECS-HA1。

图 7-11 主 ECS 验证



2. 远程登录备ECS，本示例是ECS-HA2。  
ECS有多种登录方法，具体请参见[登录弹性云服务器](#)。
3. 请根据ECS的操作系统，在[表7-5](#)中选择关闭IP转发功能的操作，本示例ECS为Linux操作系统。

表 7-5 关闭 IP 转发功能

操作系统	操作指导
Linux系统	<ol style="list-style-type: none"><li>1. 执行以下命令，切换root用户。 <b>su root</b></li><li>2. 执行以下命令，查看IP转发功能是否已开启。 <b>cat /proc/sys/net/ipv4/ip_forward</b> 回显结果：1为开启，0为关闭，默认为0。<ul style="list-style-type: none"><li>• 回显为0，任务结束。</li><li>• 回显为1，继续执行以下操作。</li></ul></li><li>3. 以下提供两种方法修改配置文件，二选一即可。 方法一：<ol style="list-style-type: none"><li>a. 执行以下命令，打开“/etc/sysctl.conf”文件。 <b>vim /etc/sysctl.conf</b></li><li>b. 按i进入编辑模式。</li><li>c. 修改net.ipv4.ip_forward = 0。</li><li>d. 按ESC退出，并输入:wq!保存配置。</li></ol>方法二： 执行sed命令，命令示例如下： <b>sed -i '/net.ipv4.ip_forward/s/1/0/g' /etc/sysctl.conf</b></li><li>4. 执行以下命令，使修改生效。 <b>sysctl -p /etc/sysctl.conf</b></li></ol>
Windows系统	<ol style="list-style-type: none"><li>1. 在搜索框中输入cmd，打开Windows系统的“命令提示符”窗口，执行以下命令。 <b>ipconfig/all</b><ul style="list-style-type: none"><li>• 回显结果中，“IP路由已启用”为“否”，表示IP转发功能已关闭。</li><li>• 回显结果中，“IP路由已启用”为“是”，表示IP转发功能未关闭，继续执行以下操作。</li></ul></li><li>2. 在搜索框中输入regedit，打开注册表编辑器。</li><li>3. 编辑HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters下的IPEnableRouter值为0。<ul style="list-style-type: none"><li>• 指定值为 0：关闭 IP 转发。</li><li>• 指定值为 1：启用 IP 转发。</li></ul></li></ol>

## 步骤五：验证主备 ECS 的自动切换功能

1. 执行以下操作，分别重启主备ECS。
  - a. 远程登录ECS-HA1。  
ECS有多种登录方法，具体请参见[登录弹性云服务器](#)。
  - b. 执行以下命令，重启ECS-HA1。  
**reboot**

- c. 参考1.a~1.b, 重启ECS-HA2。
2. 执行以下操作, 验证主ECS的网页访问情况。
    - a. 打开浏览器, 并输入EIP地址 ( 124.X.X.187 ), 验证主ECS的网页访问情况。网页如下图所示, 表示此时主ECS是ECS-HA1, 且网页访问正常。

图 7-12 主 ECS 验证 ( ECS-HA1 )



Welcome to ECS-HA1

- b. 远程登录ECS-HA1, 并执行以下命令, 查看虚拟IP是否已绑定到ECS-HA1的eth0网卡上。

#### ip addr show

回显类似如下信息, 可以看到虚拟IP ( 192.168.0.177 ) 已绑定至eth0网卡上, 再次确认ECS-HA1为主ECS。

```
[root@ecs-ha1 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether fa:16:3e:fe:56:19 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.195/24 brd 192.168.0.255 scope global noprefixroute dynamic eth0
        valid_lft 107898685sec preferred_lft 107898685sec
    inet 192.168.0.177/32 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fefe:5619/64 scope link
        valid_lft forever preferred_lft forever
```

- c. 执行以下命令, 停止主ECS的Keepalived服务, 本示例中主ECS为ECS-HA1。

#### systemctl stop keepalived.service

3. 执行以下命令, 验证主ECS是否切换到ECS-HA2。

- a. 远程登录ECS-HA2, 并执行以下命令, 查看虚拟IP是否已绑定到ECS-HA2的eth0网卡上。

#### ip addr show

回显类似如下信息, 可以看到虚拟IP ( 192.168.0.177 ) 已绑定至eth0网卡上, 此时确认ECS-HA2为主ECS。

```
[root@ecs-ha2 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether fa:16:3e:fe:56:3f brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.233/24 brd 192.168.0.255 scope global noprefixroute dynamic eth0
        valid_lft 107898091sec preferred_lft 107898091sec
    inet 192.168.0.177/32 scope global eth0
```

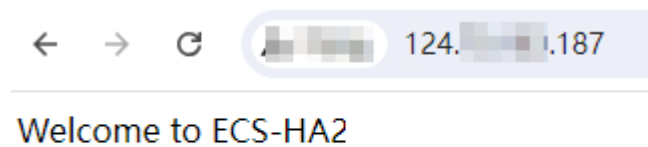


```
valid_lft forever preferred_lft forever
inet6 fe80::f816:3eff:fe56:563f/64 scope link
valid_lft forever preferred_lft forever
```

- b. 打开浏览器，并输入EIP地址（124.X.X.187），验证ECS-HA2作为主ECS时的网页访问情况。

网页如下图所示，表示此时主ECS是ECS-HA2，且网页访问正常。

图 7-13 主 ECS 验证（ECS-HA2）



# 8 云服务器迁移

## 8.1 最佳实践-主机迁移

### 背景信息

由于公有云“敏捷弹性、安全可靠、简单易用、节省成本”等特点，越来越多的企业将自己的IT应用和负载迁移到公有云，如何方便快捷地将已有的服务器系统迁移到华为云或者从其他的公有云迁移到华为云，有着非常重要的意义。华为云支持把X86物理服务器，或者私有云、公有云平台上的虚拟机迁移到华为云弹性云服务器上。

可以通过以下两种方式进行迁移。

- 主机迁移服务（推荐）
- 镜像导入方式

本文主要介绍如何使用以上两种方式帮助您把服务器上的应用和数据迁移到华为云。

### 主机迁移服务（推荐）

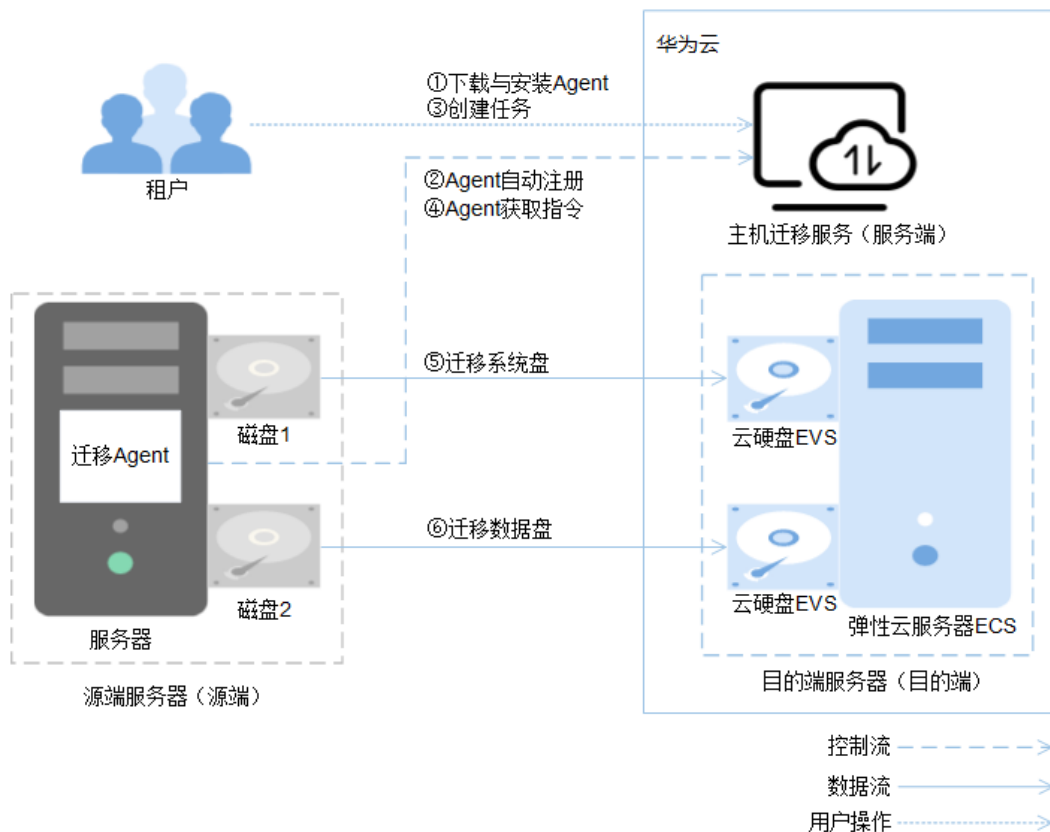
#### 服务简介

**主机迁移服务**（Server Migration Service）是一种P2V/V2V迁移服务，可以帮您把X86物理服务器，或者私有云、公有云平台上的虚拟机迁移到华为云弹性云服务器上，从而帮助您轻松地把服务器上的应用和数据迁移到华为云。

主机迁移服务支持迁移的源端服务器OS类型请参见[兼容性列表](#)。

使用主机迁移服务时，对于源端服务器的约束与限制请参见[约束与限制](#)。

图 8-1 主机迁移服务工作原理



主机迁移服务的工作原理如下，其中第1步和第3步需要用户操作，其余步骤由主机迁移服务自动完成。

1. 用户在源端服务器上安装迁移Agent，具体操作方法请您参见[安装Agent](#)。
2. 源端服务器上的迁移Agent向主机迁移服务注册自身连接状态并将源端服务器信息上报到主机迁移服务，完成迁移可行性检查。
3. 通过迁移可行性检查后，用户开始创建迁移任务，具体操作方法请您参见[创建迁移任务](#)。
4. 迁移Agent获取并执行主机迁移服务发送的迁移指令。
5. 开始迁移源端服务器系统盘。
6. 开始迁移源端服务器数据盘。

#### 说明

- **源端：**指迁移任务中的源端服务器。
- **目的端：**指迁移任务中的目的端服务器。
- **服务端：**指主机迁移服务。

#### 服务入口

主机迁移服务的操作步骤：[创建迁移任务](#)。

主机迁移服务的详细介绍：[主机迁移服务](#)。

## 镜像导入方式

1. 制作镜像。例如可通过QEMU制作镜像，可参见[此处](#)获取相应的使用帮助。
2. 创建私有镜像，详细操作可参见[此处](#)。
3. 根据私有镜像创建弹性云服务器，请参见[自定义购买ECS](#)。

## 8.2 跨账号跨区域迁移云服务器

### 操作场景

本节操作介绍华为云上云服务器的跨账号跨区域迁移，建议采用镜像迁移方式。

服务器迁移的常见场景与常用的迁移方式请参考[迁移的背景知识](#)。

跨账号跨区域迁移的方法请参考[方案介绍](#)。

### 迁移的背景知识

常见的服务器迁移场景包括物理服务器与云服务器之间、VMware等虚拟化平台与华为云服务器之间、华为云上的云服务器之间（不同账号或地域之间）、其他云平台的云服务器和华为云服务器、线下制作成镜像文件导入华为云，推荐的迁移方式请参考[表 8-1](#)。

表 8-1 常见的服务器迁移场景

迁移场景	适用条件	推荐方式	备注
x86物理服务器 → 华为云服务器 示例：P2V	服务器能够访问公网	主机迁移服务	-
VMware等虚拟化平台的虚拟机 → 华为云服务器	虚拟机能够访问公网	主机迁移服务	-
	虚拟机不能访问公网	1. 先从VMware虚拟化平台导出虚拟机的镜像文件。 2. 然后使用 <a href="#">镜像导入</a> 。	如果镜像文件格式不在vhd、vmdk、qcow2、raw、vhdx、qcow、vdi、qed、zvhd、zvhd2范围，需要先转换格式。
华为云上的云服务器（不同账号或地域之间） 示例：账号A在“华北-北京四”区域的云服务器 → 账号B的“华东-上海一”区域。	云服务器能够访问公网	主机迁移服务	-

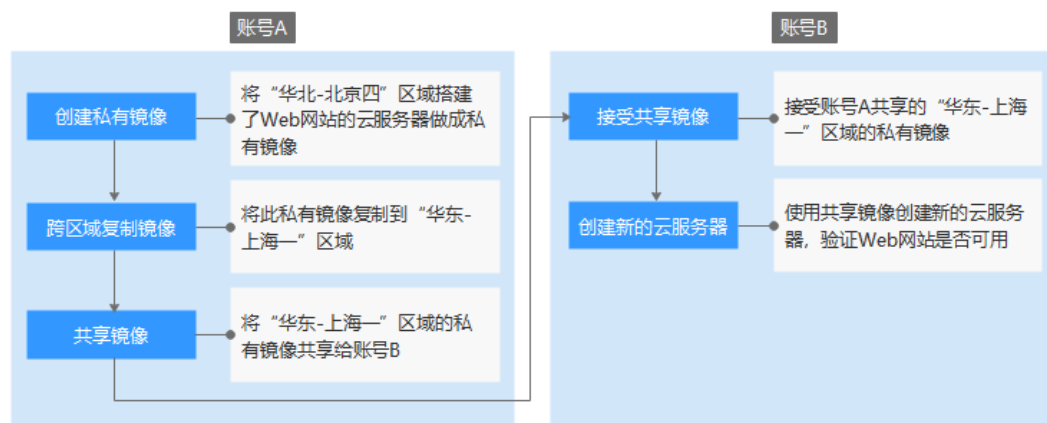
迁移场景	适用条件	推荐方式	备注
	云服务器不能访问公网	<p><b>(推荐)</b></p> <ul style="list-style-type: none"> <li>不同账号间迁移：<b>共享镜像</b> 将云服务器的系统盘制作成系统盘镜像、数据盘制作成数据盘镜像，或者直接将云服务器制作成整机镜像，然后共享给其他账号。</li> <li>不同地域间迁移：<b>跨区域复制镜像</b> 将云服务器的系统盘制作成系统盘镜像、数据盘制作成数据盘镜像，或者直接将云服务器制作成整机镜像，然后复制到其他区域。</li> <li>不同账号、不同地域间迁移：<b>共享镜像</b>和<b>跨区域复制镜像</b>结合使用。</li> </ul>	<p>只有通过云备份创建的整机镜像，才支持共享。</p> <p>跨区域复制的镜像大小不能超过128GB。</p>
其他云平台的云服务器 示例：阿里云/腾讯云 → 华为云	云服务器能够访问公网	主机迁移服务	-
	云服务器不能访问公网	<ol style="list-style-type: none"> <li>先从其他云平台导出镜像。</li> <li>然后使用<b>镜像导入</b>。</li> </ol>	如果镜像文件格式不在vhd、vmdk、qcow2、raw、vhdx、qcow、vdi、qed、zvhd、zvhd2范围，需要先转换格式。
安装盘映像 示例：线下制作成镜像文件导入华为云	已有所需操作系统的ISO格式的安装盘映像	<p><b>使用VirtualBox创建镜像并上传到华为云</b></p> <p>或</p> <p><b>使用控制台的导入ISO文件方式创建镜像</b></p>	-

## 方案介绍

跨账号跨区域迁移云服务器的方案为：账号A将区域A的云服务器做成私有镜像，将此私有镜像复制到同账号的区域B，再共享给账号B；账号B接受账号A的共享镜像后，使用该镜像创建新的云服务器。

例如，账号A在“华北-北京四”区域的云服务器上搭建了Web网站，想要将云服务器迁移到账号B的“华东-上海一”，操作流程如下：

图 8-2 操作流程



1. **步骤一：创建私有镜像**
2. **步骤二：跨区域复制镜像**
3. **步骤三：共享镜像**
4. **步骤四：接受共享镜像**
5. **步骤五：创建新的云服务器**

### 步骤一：创建私有镜像

账号A将“华北-北京四”区域搭建了Web网站的云服务器做成私有镜像。假设云服务器Web访问地址为：<http://121.36.xxx.xxx/index.html>



1. 账号A登录管理控制台，在左上角切换区域为“华北-北京四”。
2. 选择“服务列表 > 计算 > 弹性云服务器”。  
进入弹性云服务器列表页面。

3. 在搭建了Web网站的云服务器（假设为ecs-fe9e）所在行，单击操作列的“更多 > 镜像/磁盘/备份 > 创建镜像”。  
进入创建私有镜像页面。
4. 填写如下参数：

图 8-3 创建私有镜像



- 创建方式：整机镜像  
由于数据盘包含了业务数据，本例中使用弹性云服务器携带其挂载的数据盘一起创建整机镜像。
  - 选择镜像源：云服务器，并选择“ecs-fe9e”
  - 选择“云服务器备份存储库”，用于存放备份。如果云服务器已绑定存储库，系统会默认选择已绑定的存储库。  
创建的整机镜像及中间产物备份副本会默认存放在备份存储库中，因此必须选择一个云服务器备份存储库。  
如果没有可用的存储库，请单击“新建云服务器备份存储库”进行创建，注意“保护类型”需选择“备份”。
  - 名称：输入私有镜像名称，如“migrate\_test”
  - 企业项目：选择默认项目“default”
5. 单击“立即创建”。
  6. 确认无误后，阅读并勾选协议，单击“提交申请”。
  7. 返回私有镜像列表，等待几分钟后，私有镜像创建成功。

图 8-4 查看私有镜像

<input type="checkbox"/>	名称	状态	操作系统类型	操作系统	镜像类型
<input type="checkbox"/>	migrate_test	正常	Linux	CentOS 7.2 64bit	ECS整机镜像(x86)

## 步骤二：跨区域复制镜像

账号A将**步骤一：创建私有镜像**中创建的私有镜像复制到“华东-上海一”区域。在跨区域复制前，需要先创建IAM委托，详见以下步骤。

1. 创建IAM委托。
  - a. 单击右上方登录的用户名，在下拉列表中选择“统一身份认证”。
  - b. 在左侧导航栏中，单击“委托”。
  - c. 在“委托”页面，单击“创建委托”。
  - d. 在“创建委托”页面，设置如下参数：
    - 委托名称：按需填写，例如“ims\_administrator\_agency”。

图 8-5 创建委托

The screenshot shows a form for creating an IAM delegation. The fields are as follows:

- \* 委托名称**: Text input field containing "ims\_administrator\_agency".
- \* 委托类型**: Radio button selection. "普通帐号" (General Account) is unselected, and "云服务" (Cloud Service) is selected. Below the radio buttons, there are two lines of explanatory text: "将帐号内资源的操作权限委托给其他华为云帐号。" and "将帐号内资源的操作权限委托给华为云服务。".
- \* 云服务**: Dropdown menu showing "镜像服务 IMS".
- \* 持续时间**: Dropdown menu showing "永久".
- 描述**: Text area with the placeholder "请输入委托信息." and a character count "0/255" at the bottom right.

At the bottom of the form, there are two buttons: a red "下一步" (Next) button and a white "取消" (Cancel) button.

- 委托类型：选择“云服务”。
  - 云服务：（“委托类型”选择“云服务”时出现此参数项。）单击“选择”，在弹出的“选择云服务”页面选择“镜像服务 IMS”，单击“确定”。
  - 持续时间：选择“永久”。
  - 描述：非必选，可以填写“拥有IMS Administrator权限的委托”。
- e. 单击“下一步”，为委托选择策略。
  - f. 勾选“IMS Administrator”策略。

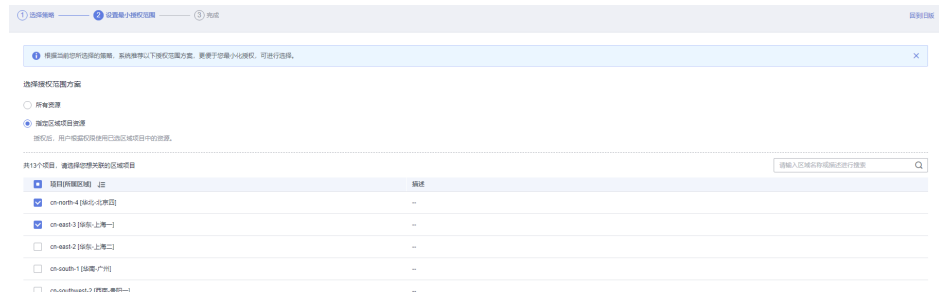


图 8-6 选择策略



- g. 单击“下一步”，选择授权区域。
- h. 在“项目[所属区域]”中选择“华北-北京四”和“华东-上海一”，单击“确定”。

图 8-7 选择区域

**注意**

配置权限时，请勿选择所有项目，否则委托将不生效。

- i. 单击“完成”，在“基本信息”页签查看创建的委托。

图 8-8 查看委托

委托名称ID [注]	委托对象 [注]	委托时长 [注]	创建时间 [注]	描述 [注]	操作
ims_administrator_agency	云服务 镜像服务 MIS	永久	2022/02/25 15:50:34 GMT+08:00	--	授权 修改 删除

2. 选择“服务列表 > 计算 > 镜像服务”，单击“私有镜像”页签。进入私有镜像列表页。
3. 在私有镜像“migrate\_test”所在行，单击操作列的“更多 > 复制”。弹出“复制镜像”对话框。
4. 填写如下参数：

图 8-9 复制镜像

复制类型: 本区域内复制 | 跨区域复制

\* 名称: copy\_cn-north-4\_migrate\_test

\* 目的区域: 华东-上海一

\* 目的项目: cn-east-3

\* 目的云服务器备份存储库: vault-2398 | 0/100(GB) [新建云服务器备份存储库](#)  
只允许选择类型为复制的云服务器备份存储库。

\* IAM委托: ims\_administrator\_agency [查看委托](#) ?

描述:   
0/1,024

[确定](#) [取消](#)

- 名称：保持默认值copy\_cn-north-4\_migrate\_test
  - 目的区域：华东-上海一
  - 目的项目：cn-east-3
  - 目的云服务器备份存储库：vault-2398
  - IAM委托：选择1中创建好的委托“ims\_administrator\_agency”。
5. 单击“确定”。
  6. 在控制台左上角切换区域为“华东-上海一”，等待几分钟后，私有镜像复制成功。

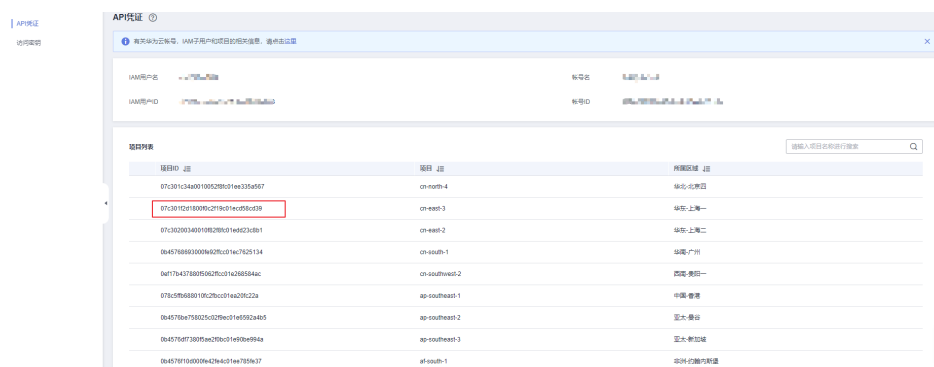
图 8-10 查看私有镜像

<input type="checkbox"/>	名称 展开	状态	操作系统类型	操作系统	镜像类型
<input type="checkbox"/>	copy_cn-north-4_...	正常	Linux	CentOS 7.2 64bit	ECS整机镜像(x86)

### 步骤三：共享镜像

账号A将“华东-上海一”区域的私有镜像共享给账号B。需要提前在“我的凭证”中获取获取账号B“华东-上海一”区域的项目ID。

图 8-11 获取项目 ID



1. 在“华东-上海一”区域，选择“服务列表 > 计算 > 镜像服务”，单击“私有镜像”页签。  
进入私有镜像列表页。
2. 在私有镜像“copy\_cn-north-4\_migrate\_test”所在行，单击操作列的“更多 > 共享”。  
弹出“共享镜像”对话框。
3. 在“共享镜像”页签，输入账号B的项目ID，单击“添加”。

图 8-12 共享镜像



4. 单击“确定”。

## 步骤四：接受共享镜像

账号B接受账号A共享的“华东-上海一”区域的私有镜像。

1. 账号B登录管理控制台，在左上角切换区域为“华东-上海一”。
2. 选择“服务列表 > 计算 > 镜像服务”，单击“共享镜像”页签。  
进入镜像列表页面。
3. 在提示信息中，勾选“copy\_cn-north-4\_migrate\_test”，单击“接受”。

图 8-13 接受共享镜像



接受后，该私有镜像将显示在共享镜像列表中。

图 8-14 共享镜像列表

名称	操作系统类型	操作系统	镜像类型
copy_cn-north-4_migrate_test	Linux	CentOS 7.2 64bit	ECS整机镜像(x86)

## 步骤五：创建新的云服务器

账号B使用共享镜像创建新的云服务器，并验证Web网站是否可用。

1. 在共享镜像“copy\_cn-north-4\_migrate\_test”所在行，单击操作列的“申请服务器”。  
进入弹性云服务器购买向导页面。
2. 按需选择计费模式、可用区、规格、网络等参数，镜像保持默认值，按界面提示完成云服务器创建。

图 8-15 选择镜像



3. 返回云服务器列表，等待几分钟，云服务器创建成功。
4. 尝试访问云服务器的Web网站，验证是否可用。  
浏览器中输入http://云服务器弹性公网IP/index.html，假设为http://124.70.xxx.xxx/index.html。经验证可以正常访问，表示云服务器迁移成功，任务结束。

图 8-16 验证 Web 网站

124.70. /index.html

# Welcome to nginx!

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

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

# 9 在 ECS 上通过内网访问 OBS

## 9.1 概述

### 场景介绍

某企业基于弹性云服务器（Elastic Cloud Server，ECS）构建好基础的业务后，随着数据增长，硬盘已无法满足大量的图片、视频等数据存取需求。了解到华为云提供有海量、弹性的云存储服务OBS后，决定将OBS作为数据存储资源池，以减轻服务器负担。

在ECS上可以通过公网和华为云内网两种网络访问OBS。当有存取对象数据的需求时，公网方式响应速度会因为网络质量而受到影响，读取数据还将收取一定的流量费用。为最大化的优化性能、节省开支，企业管理者希望通过内网的方式访问OBS。

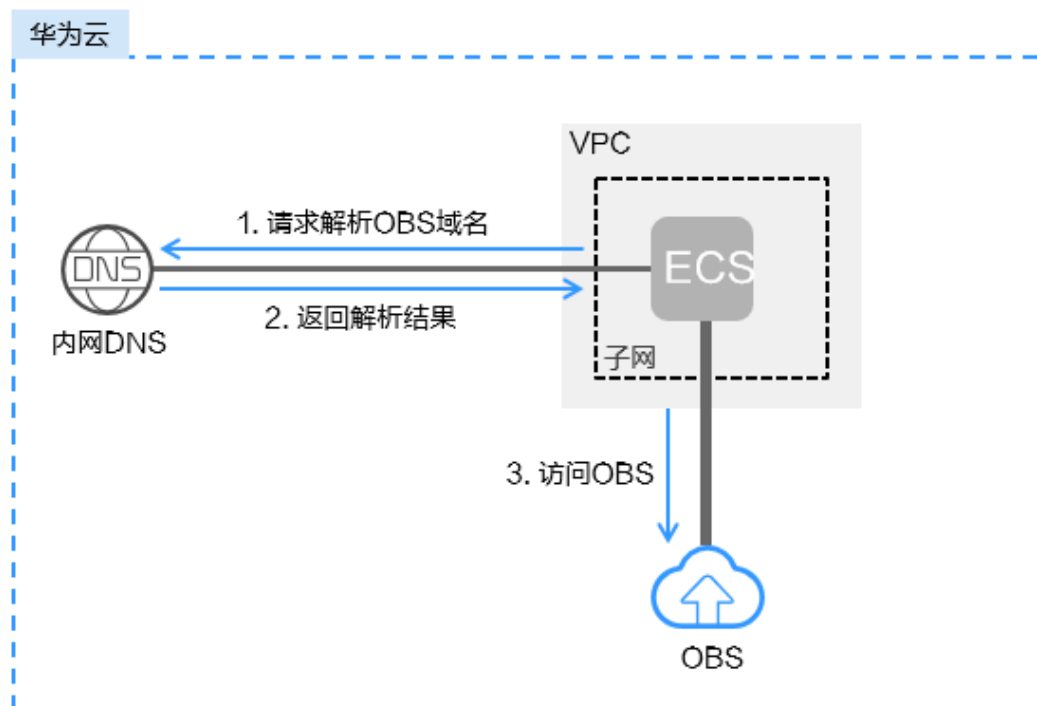
#### 📖 说明

当通过内网访问OBS时，需要确保待访问的OBS资源与ECS属于同一个区域，如果不属于同一个区域，将采用公网访问。

### 方案

在已搭建的ECS上通过配置内网DNS，由内网DNS解析OBS域名，即可实现在ECS上经由内网访问OBS。访问过程示意图如[图9-1](#)所示。

图 9-1 内网访问 OBS 示意图



示意图中各服务说明如表9-1所示。

表 9-1 服务说明

服务	说明
虚拟私有云（VPC）	VPC主要负责为ECS构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云中资源的安全性，简化用户的网络部署。 子网是VPC中用来为ECS提供IP地址管理、DNS服务的一个网络，子网内ECS的IP地址都属于该子网。
云解析服务（DNS）	DNS提供内网DNS，专门用于处理华为云内网域名以及OBS域名的解析请求，简化域名解析流程，减少因访问公网产生的流量费用。

- 对于Windows ECS，推荐使用OBS Browser+工具，实现内网访问OBS的目的，详细操作请参见：  
[在Windows ECS上使用OBS Browser+通过内网访问OBS](#)
- 对于Linux ECS，推荐使用obsutil工具，实现内网访问OBS的目的，详细操作请参见：  
[在Linux ECS上使用obsutil通过内网访问OBS](#)

当在ECS上通过内网访问OBS时，即可在内网进行数据读取、备份归档等业务，而不影响公网带宽。

## 9.2 在 Windows ECS 上使用 OBS Browser+通过内网访问 OBS

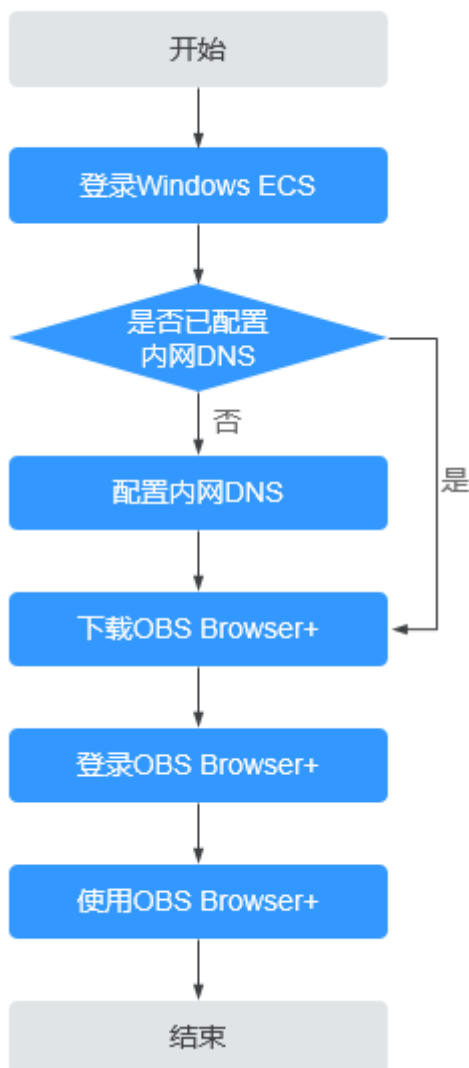
OBS Browser+是一款用于访问和管理对象存储服务的图形化工具，支持通过配置内网 DNS 服务器地址的方式，使在华为云上的 Windows ECS 通过内网直接访问 OBS，下面将介绍具体其操作流程和操作步骤。

### ⚠ 注意

OBS Browser+需通过公网下载，或者从其他可以访问公网的云服务器下载后传到当前云服务器安装。

### 流程

图 9-2 在 Windows ECS 上使用 OBS Browser+通过内网访问 OBS 的流程



## 操作步骤

### 步骤1 登录Windows ECS

1. 登录[华为云](#)，在页面右上角单击“控制台”，进入“管理控制台”页面。
2. 在打开的控制台首页，选择“计算 > 弹性云服务器”。
3. 选择待登录的云服务器，登录弹性云服务器。

Windows弹性云服务器提供“VNC远程登录方式”和“MSTSC方式”两种登录方式。具体操作请参见[如何登录弹性云服务器?](#)。

### 步骤2 查看Windows ECS是否已配置内网DNS

在Windows ECS上，您可以通过图形界面和命令行两种方式查看当前的DNS配置。此处以通过命令行方式为例，介绍如何查看DNS配置。

1. 成功登录弹性云服务器后，打开cmd命令行。
2. 运行`ipconfig /all`命令，查看“DNS服务器”是否为当前ECS所在区域的内网DNS地址。

#### 📖 说明

华为云针对各区域提供了不同的内网DNS服务器地址。具体请参见[华为云提供的内网DNS服务器地址](#)。

- 否，执行[步骤3](#)。
- 是，执行[步骤5](#)。

### 步骤3 配置内网DNS

修改ECS的DNS服务器地址为华为云提供的内网DNS，可以通过修改VPC子网DNS地址和修改本地DNS配置两种方式实现。

#### • 方式一：修改VPC子网DNS地址

确定ECS所在VPC，并修改VPC子网的DNS服务器地址为内网DNS地址后，可以使整个VPC内的ECS都通过内网DNS进行解析，从而访问在华为云内网的OBS服务。详细操作请参见[修改子网网络信息](#)。

#### 📖 说明

内网DNS服务器地址需根据ECS所在区域选择内网DNS服务器地址，具体的地址信息请参见[华为云提供的内网DNS服务器地址](#)。

#### • 方式二：修改本地DNS配置

采用此方式配置的内网DNS会在ECS每次重启后失效，在重启后需要重新配置内网DNS才可以内网访问OBS。此处以通过命令行配置为例，介绍如何在本地修改DNS配置。

1. 打开cmd命令行。
2. 运行以下命令，配置首选DNS服务器地址。

```
netsh interface ip set dns name="本地连接" source=static addr=内网DNS服务器地址 register=primary
```

#### 📖 说明

- 本地连接：网卡名称，需要根据实际正在使用的网卡进行修改。
  - 内网DNS服务器地址：需要根据ECS所在区域选择内网DNS服务器地址，具体的地址信息请参见[华为云提供的内网DNS服务器地址](#)。
3. (可选) 运行以下命令，配置备份DNS服务器地址。  

```
netsh interface ip add dns name="本地连接" addr=备选DNS服务器地址 index=2
```



#### 说明

- 本地连接：网卡名称，需要根据实际正在使用的网卡进行修改。
- 备选DNS服务器地址：是在首选DNS服务器出现故障、不可用或无法解析请求的域名时使用的DNS服务器，因此您可以设置为华为云内网DNS服务器的地址（需要根据ECS所在区域选择内网DNS服务器地址，具体的地址信息请参见[华为云提供的内网DNS服务器地址](#)。），也可以设置成公网DNS服务器地址，具体以实际业务为准。

#### 步骤4 确认是否已经是内网访问OBS

具体方法请参见[如何判断是否内网访问OBS?](#)

OBS桶的全局域名格式为：[桶名.obs.my-kualalumpur-1.alphaedge.tmone.com.my](#)

#### 步骤5 下载OBS Browser+

OBS Browser+下载地址及具体操作请参见[下载OBS Browser+](#)。

#### 步骤6 登录OBS Browser+

由于OBS Browser+默认使用公网访问OBS，因此在登录OBS Browser+添加账号时，“服务提供商”和“服务器地址”需要按照以下要求填写：

- 服务器地址：根据ECS所在区域输入OBS在此区域的终端节点（Endpoint）和端口号（HTTPS协议端口号为“443”，HTTP协议端口号为“80”。系统默认服务器为HTTPS服务器，如需使用HTTP服务器，请单击OBS Browser+页面右上角的



图标并单击“系统配置”，在弹出的“系统配置”窗口，取消对“启用HTTPS安全传输协议”的勾选。）。

示例：[obs.ap-southeast-1.myhuaweicloud.com:443](#)

#### 说明

OBS区域和终端节点信息请参见[地区和终端节点](#)。

#### 步骤7 开始使用OBS Browser+

成功登录OBS Browser+后，便可以在Windows ECS上直接通过内网访问OBS，进行基本的数据存取操作以及其他的高级设置操作。

详细使用指南请参见[对象存储服务工具指南（OBS Browser+）](#)。

----结束

## 9.3 在 Linux ECS 上使用 obsutil 通过内网访问 OBS

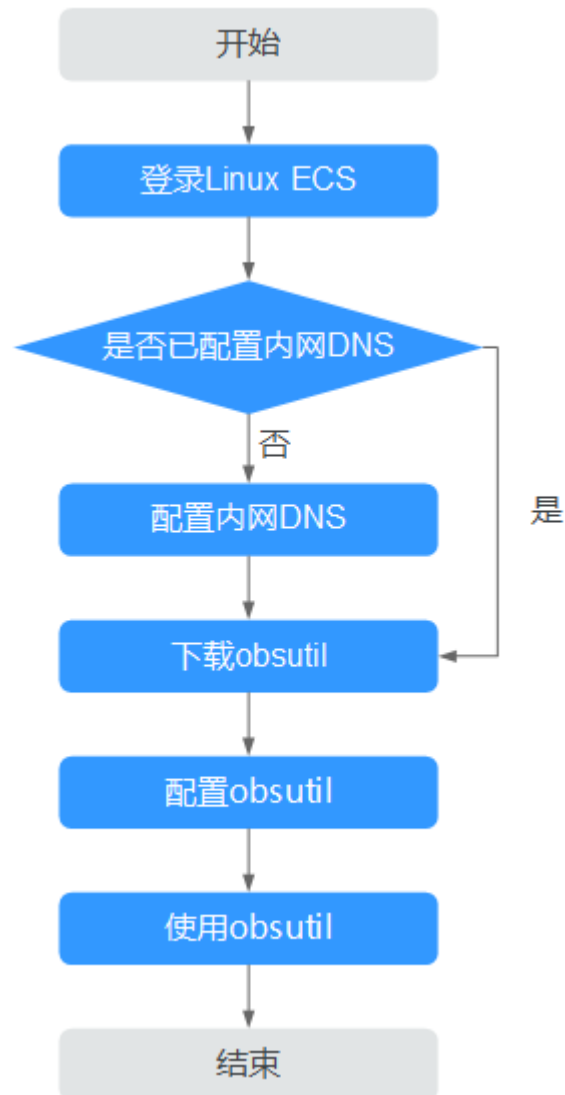
obsutil是适用于Windows、macOS和Linux操作系统的命令行工具，支持通过配置内网DNS服务器地址的方式，使在华为云上的Linux ECS通过内网直接访问OBS，下面将介绍其具体操作流程和操作步骤。

#### 说明

obsutil需通过公网下载，或者从其他可以访问公网的云服务器下载后传到当前云服务器安装。

## 流程

图 9-3 在 Linux ECS 上使用 obsutil 通过内网访问 OBS 的流程



## 操作步骤

### 步骤1 登录Linux ECS

1. 登录[华为云](#)，在页面右上角单击“控制台”，进入“管理控制台”页面。
2. 在打开的控制台首页，选择“计算 > 弹性云服务器”。
3. 选择待登录的云服务器，登录弹性云服务器。  
由于购买Linux ECS时设置的登录鉴权方式不同，登录方式因此也存在差异。  
不同方式登录的具体操作请参见[如何登录弹性云服务器？](#)。

### 步骤2 查看Linux ECS是否已配置内网DNS

1. 成功登录Linux ECS后，打开命令行终端。
2. 运行`cat /etc/resolv.conf`命令，查看首行“nameserver”后的IP地址是否为当前ECS所在区域的内网DNS地址。

### 📖 说明

华为云针对各区域提供了不同的内网DNS服务器地址。具体请参见[华为云提供的内网DNS服务器地址](#)。

- 否，执行[步骤3](#)。
- 是，执行[步骤5](#)。

## 步骤3 配置内网DNS

修改ECS的DNS服务器地址为华为云解析服务提供的内网DNS，可以通过修改VPC子网DNS地址和修改本地DNS配置两种方式实现。

### • 方式一：修改VPC子网DNS地址

确定ECS所在VPC，并修改VPC子网的DNS服务器地址为内网DNS地址后，可以使整个VPC内的ECS都通过内网DNS进行解析，从而访问在华为云内网的OBS服务。详细操作请参见[修改子网网络信息](#)。

### 📖 说明

内网DNS服务器地址需根据ECS所在区域选择内网DNS服务器地址，具体的地址信息请参见[华为云提供的内网DNS服务器地址](#)。

### • 方式二：修改本地DNS配置

此处以CentOS 6.x 64bit弹性云服务器为例，介绍如何修改本地DNS配置。

- 打开命令行终端。
- 运行以下命令，打开“/etc/resolv.conf”文件。

```
vi /etc/resolv.conf
```
- 按下i键进入编辑模式，在“/etc/resolv.conf”文件中按照以下格式，在原有的DNS服务器地址之前新增内网DNS服务器地址。

```
nameserver 内网DNS服务器地址
```

### 📖 说明

- 内网DNS服务器地址需根据ECS所在区域选择内网DNS服务器地址，具体的地址信息请参见[华为云提供的内网DNS服务器地址](#)。
  - 新增的DNS服务器地址必须位于所有原有的DNS服务器地址之前。
  - DNS服务器按照nameserver顺序选择，且仅在前一个DNS服务器出现故障、不可用或无法解析请求的域名时，才选择下一个DNS服务器。因此，后续如果想切换成公网方式，需要将首行DNS地址改为公网的DNS，或者在已有DNS服务器地址前增加一条公网DNS服务器地址。
- 按下Esc键，并输入:wq!，保存并退出文件。

### 📖 说明

修改后的DNS地址在保存“/etc/resolv.conf”文件的修改操作后立即生效。

## 步骤4 确认是否已经是内网访问OBS

具体方法请参见[如何判断是否内网访问OBS?](#)

## 步骤5 下载obsutil

obsutil最新版本和下载链接请参见[下载obsutil](#)。

## 步骤6 配置obsutil

使用obsutil之前，您需要配置obsutil与OBS的对接信息，包括OBS终端节点（Endpoint）和访问密钥（AK和SK）。

具体操作请参见obsutil指南的[初始化配置](#)章节。

#### 说明

其中OBS终端节点（Endpoint）需要根据ECS所在区域输入。

OBS区域和终端节点信息请参见[地区和终端节点](#)。

### 步骤7 使用obsutil

obsutil配置成功后，便可以在Linux ECS上直接通过内网访问OBS，进行基本的数据存取操作以及其他的高级设置操作。

常见的数据存储操作请参见：

- [上传对象](#)
- [下载对象](#)

详细使用指南请参见[对象存储服务工具指南（obsutil）](#)。

----结束

# 10 使用 VNC Viewer 连接 Linux 云服务器

Linux云服务器一般采用SSH连接方式，使用密钥对进行安全地无密码访问。但是SSH连接一般都是字符界面，有时需要使用图形界面进行一些复杂操作。本文以Ubuntu 20.04操作系统为例，介绍如何为云服务器安装VNC Server，以及如何使用VNC Viewer连接云服务器。

## 准备工作

- 已创建一台Ubuntu 20.04操作系统的云服务器，并且为云服务器绑定弹性公网IP，确保可以连接互联网。  
具体操作请参见[自定义购买ECS](#)、[申请弹性公网IP](#)。
- 已在本地PC安装VNC Viewer客户端。

### 说明

VNC Viewer下载地址：<https://www.realvnc.com/en/connect/download/viewer/>

## 安装 VNC Server

默认情况下，Ubuntu 20.04操作系统没有安装图形环境或VNC Server。本示例中，桌面环境使用Xfce，它是一个精简的轻量化桌面，与Gnome和KDE相比更小巧，并且界面美观、对用户友好，适合云服务器远程连接场景下使用。

1. 远程登录云服务器。  
账号：root；密码：您在创建云服务器时设置的密码。
2. 执行以下命令，更新软件列表。  
**sudo apt update**
3. 安装Xfce桌面环境。  
**sudo apt install xfce4 xfce4-goodies**
4. 执行完成后，安装TightVNC服务器。  
**sudo apt install tightvncserver**
5. 执行完成后，使用vncserver命令进行配置。  
当您第一次运行vncserver时，它会创建一个默认启动脚本。按照提示进行配置：

```
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- :~#
```

- 密码：长度为6~8个字符。超过8个字符的密码将自动截断。请牢记该密码，VNC Viewer连接云服务器时会使用。
- 验证密码：再次输入密码。
- 是否创建仅查看密码：使用仅查看密码登录的用户将无法使用鼠标或键盘控制云服务器。此处输入“n”。

## 配置 VNC Server

1. 首先停止第一个虚拟桌面。

```
vncserver -kill :1
```

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

2. 修改xstartup文件。

```
vim ~/.vnc/xstartup
```

按“i”进入编辑模式，添加以下内容：

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

其中，

- 第一个命令“xrdp \$HOME/.Xresources”告诉VNC的GUI框架读取服务器用户的“.Xresources”文件。用户可以在“.Xresources”中更改图形桌面的某项设置，如终端颜色、光标主题和字体渲染。
- 第二个命令“startxfce4 &”告诉服务器启动Xfce。

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

3. 为了保证VNC服务正常启动，需要配置可执行。

```
sudo chmod +x ~/.vnc/xstartup
```

4. 重启VNC Server。

```
vncserver
```

第二次运行vncserver时，它将创建日志文件。

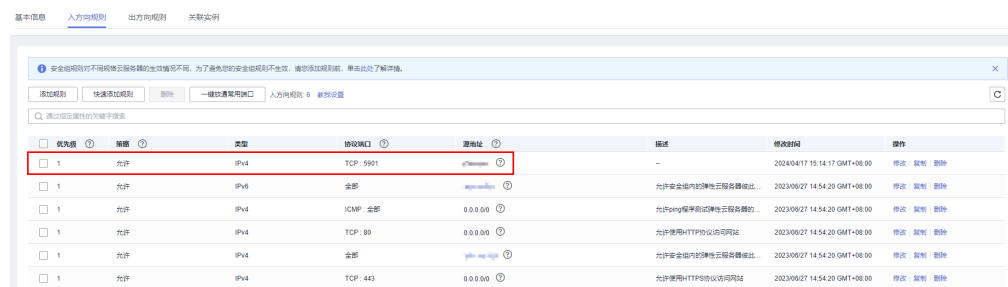
```
root@ecs-9240-:~# vncserver
New 'X' desktop is ecs-9240-:1
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/ecs-9240-:1.log
root@ecs-9240-:~#
```

回显信息中出现类似这样的一条信息：Log file is /root/.vnc/xxx:1.log。其中，“1”表示当前用户分配的是VNC的第一个虚拟桌面。

## 云服务器控制台配置

1. 登录云服务器管理控制台。
2. 单击弹性云服务器名称，进入详情页面。
3. 在“安全组”页签，单击“更改安全组规则”，放行5901端口。

图 10-1 更改安全组规则

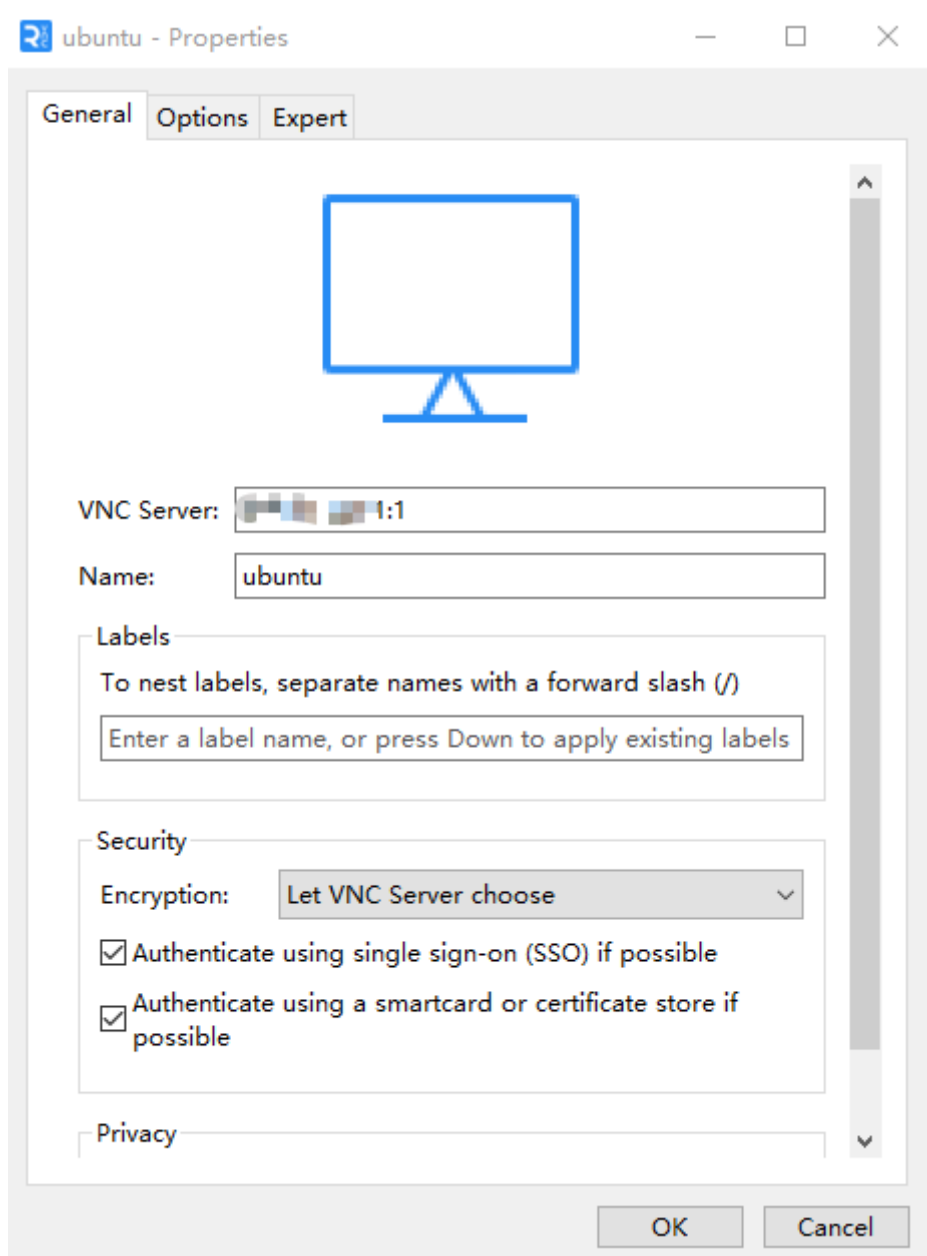


## 使用 VNC Viewer 连接云服务器

1. 在本地PC打开VNC Viewer客户端，输入云服务器的弹性公网IP.1，设置名称，单击“OK”。

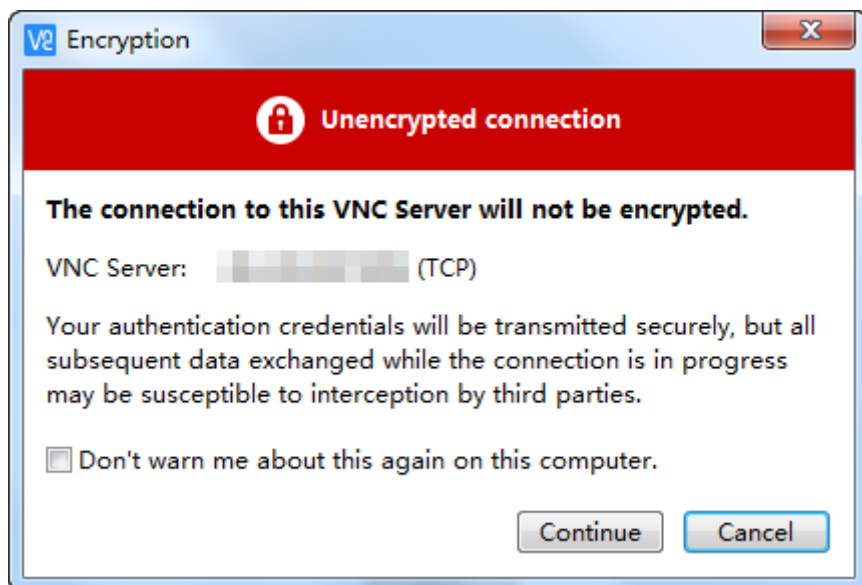
### 说明

端口号由4中回显的日志文件名决定，如果为“xxx:1.log”，则输入1。

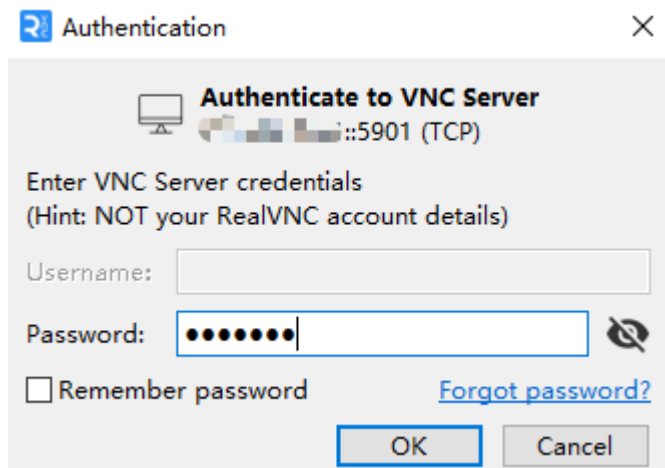


2. 弹出如下界面，直接单击“Continue”。





3. 输入5中设置的密码，单击“OK”。



4. 建立连接后，即可看到Ubuntu 20.04的图形化界面。

