华为认证 Cloud 系列教程

HCIP-Cloud Service Solutions Architect

实验指导手册

版本：3.0

华为技术有限公司

商标声明


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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://e.huawei.com

华为认证体系介绍

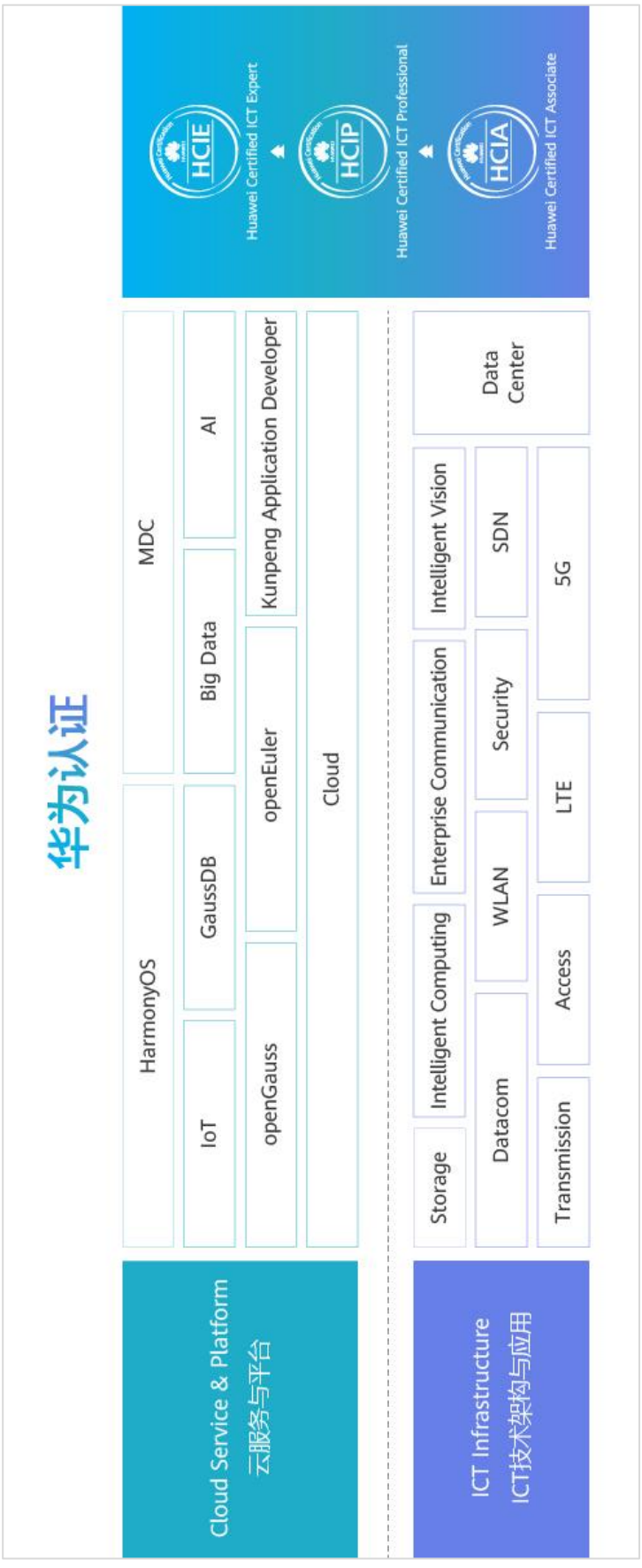
华为认证是华为公司基于“平台+生态”战略，围绕“云-管-端”协同的新 ICT 技术架构，打造的覆盖 ICT（Information and Communications Technology，信息通信技术）全技术领域的认证体系，包含 ICT 技术架构与应用认证、云服务与平台认证两类认证。

根据 ICT 从业者的学习和进阶需求，华为认证分为工程师级别、高级工程师级别和专家级别三个认证等级。

华为认证覆盖 ICT 全领域，符合 ICT 融合的技术趋势，致力于提供领先的人才培养体系和认证标准，培养数字化时代新型 ICT 人才，构建良性 ICT 人才生态。

HCIP-Cloud Service Solutions Architect V3.0 认证包含企业 IT 演进趋势，传统应用云上架构，云原生应用架构，业界创新技术及华为云方案，华为云解决方案等内容。

华为认证协助您打开行业之窗，开启改变之门，屹立在云服务世界的潮头浪尖！


华为认证
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate
Cloud Service & Platform
云服务与平台
ICT Infrastructure
ICT技术架构与应用
HarmonyOS
IoT
GaussDB
openGauss
openEuler
MDC
Big Data
AI
Kunpeng Application Developer
Cloud
Storage
Intelligent Computing
Datacom
WLAN
Transmission
Access
Enterprise Communication
Security
LTE
Intelligent Vision
SDN
5G
Data Center

前 言

简介

本实验指导手册为 HCIP-Cloud Service Solutions Architect 认证培训教程，适用于准备参加 HCIP-Cloud Service Solutions Architect 考试的学员或者希望了解 HCIP-Cloud Service Solutions Architect 基础知识，包括想要了解企业 IT 演进趋势、传统应用云上架构、云上弹性计算、存储、网络、数据库和安全方案设计、容器与云原生、企业核心业务未来架构演进及华为云方案、物联网等技术的读者。

内容描述

本实验指导手册共包含八个实验，逐一介绍了计算架构设计实验、网络架构设计实验、存储架构设计实验、数据库架构设计实验、安全架构设计实验、容器应用部署实验、微服务应用部署实验和运维实验。

- 实验一为计算架构实验，通过 WordPress 网站的搭建及高可用配置帮助读者掌握计算架构云服务的使用，通过弹性伸缩服务中文本注入功能的配置帮助读者在资源配置管理工作中更加得心应手。
- 实验二为网络架构设计实验，使用云上的不同 Region 来模拟线下局点和云上资源，模拟线下局点接入云上资源运维、云上资源互通和云上资源公网访问等业务场景，帮助读者深入理解华为云上网络架构和使用原理。
- 实验三为存储架构设计实验，通过搭建视频流媒体服务的业务场景，综合运用云上各项存储服务，帮助读者理解华为云存储服务的架构和原理。
- 实验四为数据库架构设计实验，本实验使用弹性云服务器和云数据库实例搭建网页站点并为其配置 Redis 服务，通过数据库实例等模块的配置帮助读者理解华为云数据库的架构原理和使用方法。
- 实验五为安全架构设计实验，包括了主机安全、双因子认证、地址组、DEW 密钥托管和 Web 应用防火墙的相关实验配置，帮助读者深入了解华为云上安全架构及使用原理。
- 实验六为容器应用部署实验，本实验通过制作容器镜像并上传华为 SWR 并重新部署于云容器引擎 CCE 的实验步骤，帮助读者理解并掌握 Dockerfile 镜像构建方式以及云容器引擎的原理和使用，通过函数工作流刷新对象存储桶内对象版本，做到在桶内始终只保留最新的 3 个版本数据，帮助读者掌握函数工作流 FunctionGraph 的配置方式和使用原理。
- 实验七为微服务应用部署实验，包括了 ServiceStage 部署微服务以及 weathermap 微服务的搭建，帮助读者理解并掌握 ServiceStage 微服务构建的方式与原理。
- 实验八为云上运维实验，包括了云监控服务 CES、应用运维管理 AOM、应用性能监控 APM 的相关实验，帮助读者多维度理解华为云上运维服务的架构原理及使用。

学员知识背景

本课程为华为认证课程，为了更好地掌握本书内容，阅读本书的读者应首先具备以下基本条件：

- 具有基本的 HCIA-Cloud Service 知识背景，同时熟悉基础的云计算知识。
- 具备 Linux 相关基础知识。

实验环境说明

本实验环境为真实的华为公有云平台 https://www.huaweicloud.com/，前期不需要购买任何实验设备。本实验手册中所有产品的操作及使用均在该平台上进行。在学习过程中可通过华为云帮助中心 https://support.huaweicloud.com/进行咨询或拨打华为云客服电话 4000-955-988 获得专业的技术支持。

目录

1 计算架构设计实验

1.1 实验介绍

1.1.1 关于本实验

本实验将在华为云上通过虚拟私有云（Virtual Private Cloud，简称 VPC）中，搭建弹性云服务器（Elastic Cloud Server，简称 ECS）+云数据库（Relational Database Service，简称 RDS）服务搭建 WordPress 网站，需要进行对应的云上架构设计。考虑流量分发控制和业务冗余性，实验中使用弹性负载均衡器（Elastic Load Balance，简称 ELB）提供流量分发服务并提升应用系统的容错能力。考虑业务波峰波谷对资源的弹性伸缩需求，实验中使用弹性伸缩服务（Auto Scaling，简称 AS）来保证服务质量和计算资源利用率。考虑后端数据库地址或其他信息变动的可能性，实验中通过在弹性伸缩服务中配置文本注入，来修改由镜像自动创建的云主机中后端数据库的地址连接信息，避免多次手工介入修改。通过本实验的练习，读者可以掌握计算架构云服务的使用原理。

1.1.2 实验目的

理解云上计算架构设计中各云服务的使用。

掌握对云上资源可用性、可扩展性、性能等方面的设计方法。

1.1.3 软件介绍

WordPress 是一个免费的开源项目，同时它也是一款个人博客系统，用户可以在支持 PHP 和 MySQL 数据库的服务器上通过 WordPress 架设属于自己的网站。

1.1.4 实验组网

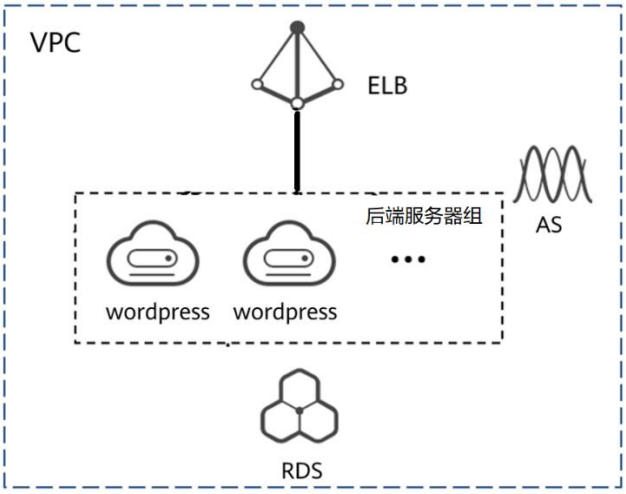


图1-1

1.2 实验配置

1.2.1 创建 VPC、安全组

步骤 1 打开华为云官网 https://www.huaweicloud.com/，登录华为云账号， 选择“北京一”区域（本实验以“北京一”区域为例，学员可以根据实际情况选择相应区域），在服务列表中选择“虚拟私有云 VPC”。

图1-2

步骤 2 点击“创建虚拟私有云”（本实验的后续资源将在此 VPC 中创建）。

图1-3

步骤 3 按照以下要求填写参数并点击“立即创建”。

基本信息

- 区域：华北-北京一（本实验以“北京一”区域为例，学员可以根据自己实际情况选择相应区域）
- 名称：vpc-1
- IPv4 网段：192.168.0.0/16

默认子网

- 可用区：可用区 3（本实验以“可用区 3”为例，学员可以根据实际情况选择相应区域）
- 名称：vpc-1-subnet
- 子网 IPv4 网段：192.168.1.0/24

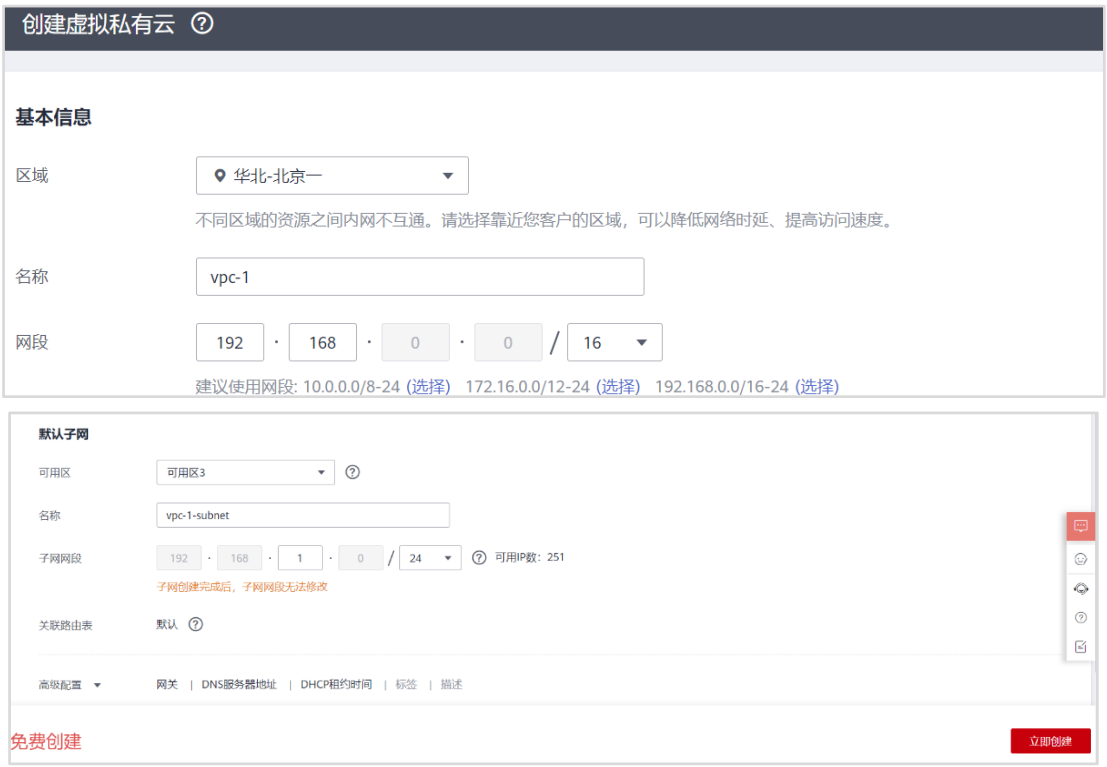


图1-4

步骤 4 在网络控制台的“访问控制”页签中选择“安全组”，点击右上方“创建安全组”。

图1-5

步骤 5 按以下配置创建安全组（该安全组供后续 RDS 服务使用，需要放通 3306 端口）。

- 名称：sg-rds
- 模板：自定义

图1-6

步骤 6 在弹出的对话框中选择配置规则。

图1-7

步骤 7 选择“入方向规则”页签下的“添加规则”。

图1-8

步骤 8 按以下配置完成规则创建。

- 优先级：1
- 策略：允许
- 协议：TCP

- 端口：3306
- 源地址：IP 地址|0.0.0.0

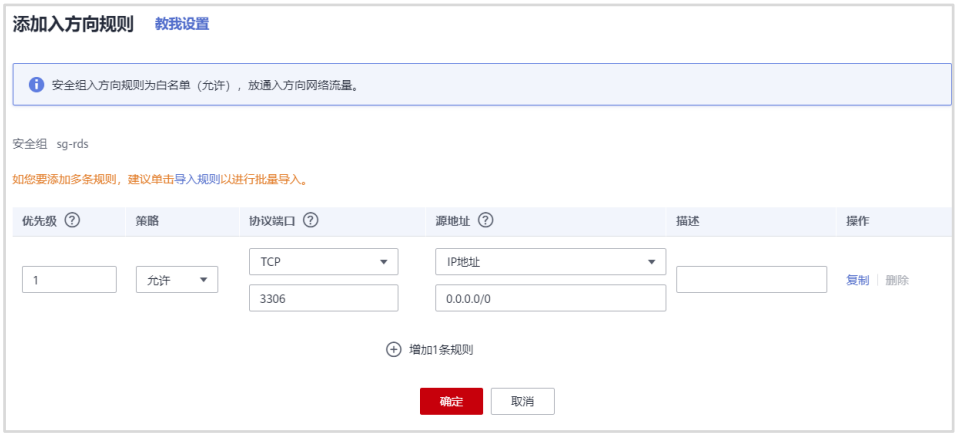


图1-9

步骤 9 点击“确定”后完成创建。

图1-10

步骤 10 重复步骤 4 创建安全组“sg-web”，并将模板选择为“通用 Web 服务器”（该安全组供本实验中的 ECS 使用）。

图1-11

1.2.2 创建 RDS

步骤 1 在服务列表中选择“云数据库 RDS”。

图1-12

步骤 2 点击右上方“购买数据库实例”。

说明：后续需要在该实例中创建数据库，对接 WordPress。

图1-13

步骤 3 按照以下配置购买数据库。

- 计费模式：按需计费
- 区域：华北-北京一（本实验以“北京一”区域为例，学员可以根据实际情况选择相应区域）
- 实例名称：rds-wordpress
- 数据库引擎：MySQL
- 数据库版本：8.0
- 实例类型：单机
- 可用区：可用区二（本实验以“可用区二”为例，学员可以根据实际情况选择相应区域）
- 性能规格：2 vCPU|4 GB
- 存储空间：40 GB
- 磁盘加密：不加密

图1-14

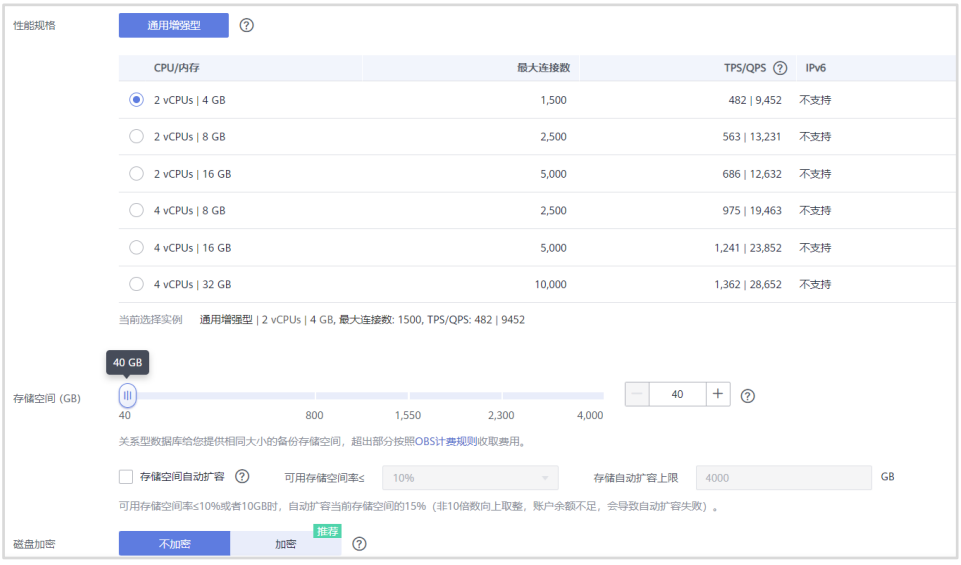


图1-15

- 虚拟私有云：vpc-1
- 子网：vpc-1-subnet
- 安全组：sg-rds
- 管理员密码：自定义

- 其他配置：默认配置即可

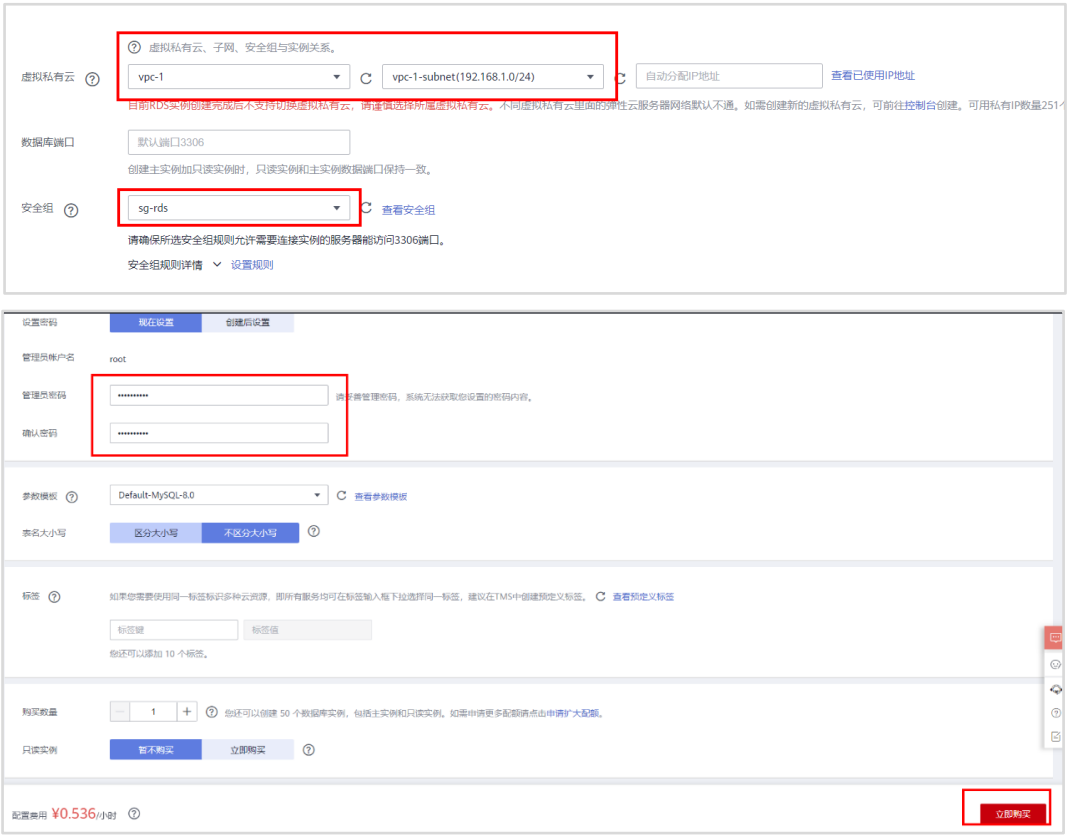


图1-16

步骤 4 确认配置后点击“立即购买”。

步骤 5 在云数据库列表界面选择刚刚创建的数据库右侧的“更多”选项，选择“登录”。

图1-17

步骤 6 输入用户名密码后，点击“测试连接”并登录。

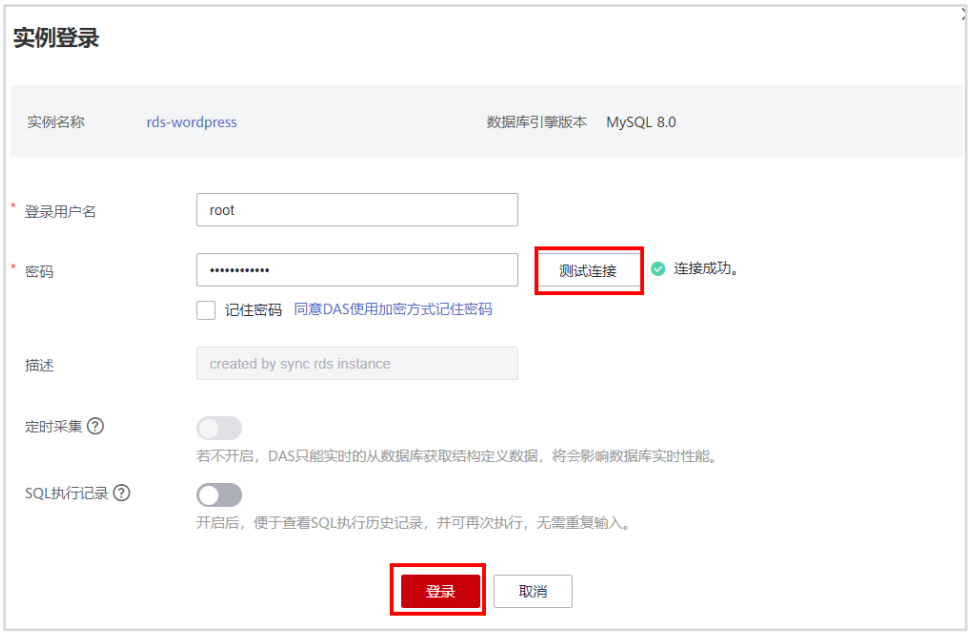


图1-18

步骤 7 选择“新建数据库”（后续使用该数据库对接 WordPress）。

图1-19

步骤 8 输入数据库名称“wordpress”，字符集采用默认即可，点击“确定”。

图1-20

步骤 9 在数据库列表界面点击刚创建的数据库名称进入基本信息界面。

图1-21

步骤 10 记录数据库的内网地址、端口等信息备用。

说明：在配置 WordPress 时需要在配置文件中填入相应参数。

图1-22

1.2.3 创建 ECS

步骤 1 在服务列表中选择“弹性云服务器 ECS”，点击右上角“购买弹性云服务器”。

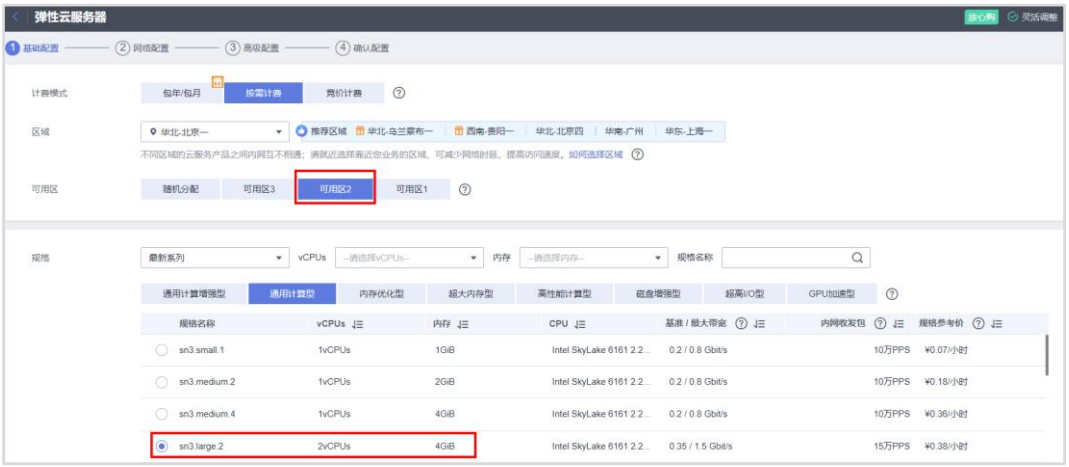
图1-23

步骤 2 按照以下配置购买云服务器。

云主机“ecs-wordpress”配置：

- 计费模式：按需计费
- 区域：华北-北京一（本实验以“北京一”区域为例，学员可以根据实际情况选择相应区域）
- 可用区：可用区 2（本实验以“可用区 2”为例，学员可以根据实际情况选择相应区域）
- CPU 架构：x86 计算
- 规格：2 vCPUs | 4 GiB

- 镜像：公共镜像 | CentOS 7.6 64 bit
- 主机安全：开通主机安全（基础版）
- 网络：vpc-1 | vpc-1-subnet | 自动分配 IP 地址
- 安全组：sg-web
- 弹性公网 IP：现在购买
- 线路：全动态 BGP
- 公网带宽：按流量计费
- 带宽大小：10 Mbit/s
- 系统盘：高 IO | 40 GiB
- 云服务器名称：ecs-wordpress
- root 密码：自定义



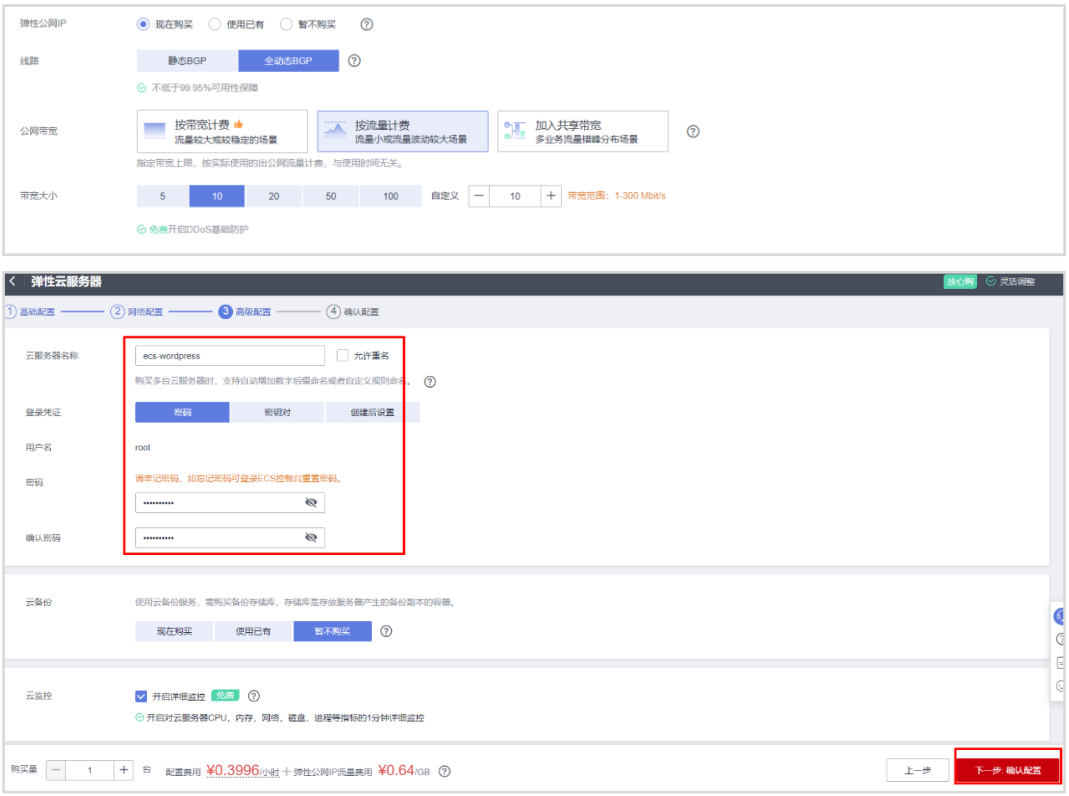


图1-24

步骤 3 确认配置后点击“购买”。

1.2.4 安装 WordPress

步骤 1 在弹性云服务器列表中找到刚购买的 ECS，使用对应操作栏中的“远程登录”登录云主机。

图1-25

步骤 2 输入如下命令安装 LAMP 环境，并开启相应服务。

```
[root@ecs-wordpress ~]# yum install -y httpd php php-fpm php-server php-mysql mysql
```

图1-26

步骤 3 输入以下命令进行编辑配置 httpd 服务。

```
[root@ecs-wordpress ~]# vim /etc/httpd/conf/httpd.conf
```

步骤 4 在打开的配置文件界面，单击快捷键“shift+g”，进入配置文件最后一行。单击快捷键“i”进入编辑模式，移动光标至配置文件末尾，回车换行，拷贝粘贴以下配置代码。

说明：设置用于服务器辨识本身的主机名和端口号，为了增强可靠性和可预测性，使用 ServerName 显示的指定主机名和端口号。

```
ServerName localhost:80
```

```
#
# Specify a default charset for all content served; this enables
# interpretation of all content as UTF-8 by default.  To use the
# default browser choice (ISO-8859-1), or to allow the META tags
# in HTML content to override this choice, comment out this
# directive:
#
AddDefaultCharset UTF-8

<IfModule mime_magic_module>
    #
    # The mod_mime_magic module allows the server to use various hints from the
    # contents of the file itself to determine its type.  The MIMEMagicFile
    # directive tells the module where the hint definitions are located.
    #
    MIMEMagicFile conf/magic
</IfModule>

#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#

#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files.  This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ServerName localhost:80
```

图1-27

步骤 5 单击快捷键“ESC”退出编辑模式，输入“:wq”，回车执行保存并退出配置文件。

```
# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ServerName localhost:80
:wq
```

图1-28

步骤 6 使用如下命令，下载 WordPress 安装软件。

```
[root@ecs-wordpress ~]# wget -c https://cloudservice-v3.obs.cn-east-3.myhuaweicloud.com/wordpress-4.9.1_zh.tar.gz
```

图1-29

步骤 7 输入如下命令，将 WordPress 安装包解压到目录/var/www/html。

```
[root@ecs-wordpress ~]# tar -zxvf wordpress-4.9.1_zh.tar.gz -C /var/www/html/
```

运行至“wordpress/readme.html”行结束，显示如下图所示。

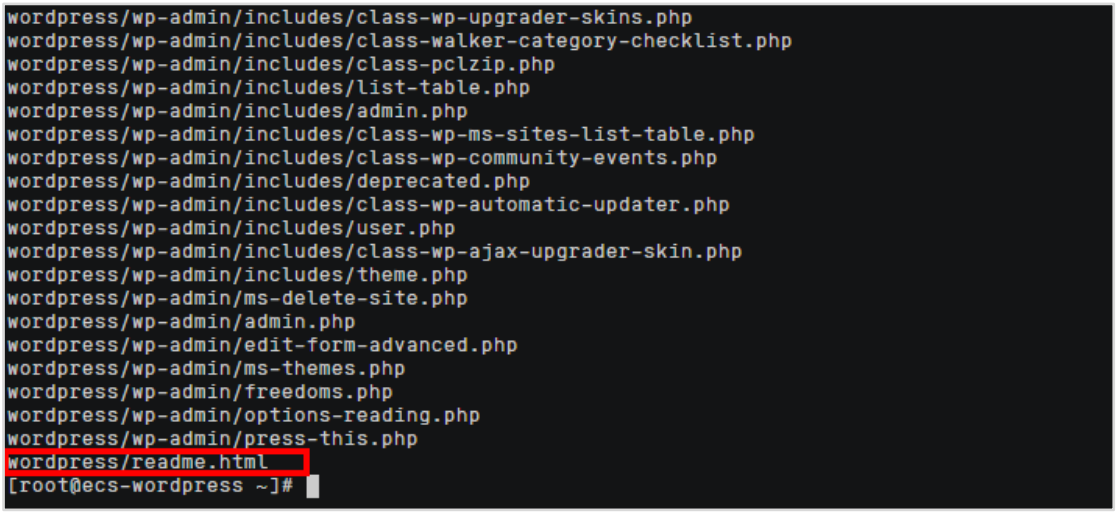


图1-30

步骤 8 使用如下命令，创建 wp-config.php 文件。

```
[root@ecs-wordpress ~]# cd /var/www/html/wordpress
[root@ecs-wordpress wordpress]# cp wp-config-sample.php wp-config.php
```

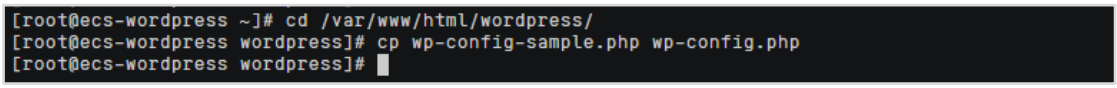


图1-31

步骤 9 使用如下命令修改 wp-config.php 文件，配置数据库参数对接之前创建的“wordpress”数据库。

```
[root@ecs-wordpress wordpress]# vi wp-config.php
```

修改 wp-config.php 文件中数据库的配置参数，如下内容：

- 数据库名称：wordpress
- 数据库用户名：root
- 数据库密码：学员自定义
- 数据库主机：RDS 实例的内网 IP 地址：端口号（端口号默认 3306）

```
// ** MySQL 设置 - 具体信息来自您正在使用的主机 ** //
/** WordPress数据库的名称 */
define('DB_NAME', 'wordpress');

/** MySQL数据库用户名 */
define('DB_USER', 'root');

/** MySQL数据库密码 */
define('DB_PASSWORD', 'Huawei123!@#');

/** MySQL主机 */
define('DB_HOST', '192.168.1.137:3306');

/** 创建数据表时默认的文字编码 */
define('DB_CHARSET', 'utf8');

/** 数据库整理类型。如不确定请勿更改 */
define('DB_COLLATE', '');

/**#@+
 * 身份认证密钥与盐。
 *
```

图1-32

步骤 10 输入如下命令，赋予文件所在目录读写权限。

```
[root@ecs-wordpress wordpress]# chmod -R 777 /var/www/html
```

```
[root@ecs-wordpress wordpress]# chmod -R 777 /var/www/html
```

图1-33

步骤 11 输入如下命令，开启 httpd 服务和 php-fpm 服务。

```
[root@ecs-wordpress wordpress]# systemctl start httpd.service
[root@ecs-wordpress wordpress]# systemctl start php-fpm.service
```

步骤 12 输入如下命令，查看 httpd 服务状态，可以看到服务状态为“active (running)”，证明服务已正常开启。

```
[root@ecs-wordpress wordpress]# systemctl status httpd
```

```
[root@ecs-wordpress wordpress]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since [redacted] CST; 1min 9s ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 8103 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/sec"
   CGroup: /system.slice/httpd.service
           ├─8103 /usr/sbin/httpd -DFOREGROUND
           ├─8105 /usr/sbin/httpd -DFOREGROUND
           ├─8106 /usr/sbin/httpd -DFOREGROUND
           ├─8107 /usr/sbin/httpd -DFOREGROUND
           ├─8108 /usr/sbin/httpd -DFOREGROUND
           └─8109 /usr/sbin/httpd -DFOREGROUND

[redacted] ecs-wordpress systemd[1]: Starting The Apache HTTP Server...
[redacted] ecs-wordpress systemd[1]: Started The Apache HTTP Server.
[root@ecs-wordpress wordpress]#
```

图1-34

步骤 13 输入如下命令，查看 php-fpm 服务状态，可以看到服务状态为“active (running)”，证明服务已正常开启。

```
[root@ecs-wordpress wordpress]# systemctl status php-fpm
```

```
[root@ecs-wordpress wordpress]# systemctl status php-fpm
● php-fpm.service - The PHP FastCGI Process Manager
   Loaded: loaded (/usr/lib/systemd/system/php-fpm.service; disabled; vendor preset: disabled)
   Active: active (running) since [redacted] CST; 1min 23s ago
 Main PID: 8116 (php-fpm)
   Status: "Processes active: 0, idle: 5, Requests: 0, slow: 0, Traffic: 0req/sec"
   CGroup: /system.slice/php-fpm.service
           ├─8116 php-fpm: master process (/etc/php-fpm.conf)
           ├─8118 php-fpm: pool www
           ├─8119 php-fpm: pool www
           ├─8120 php-fpm: pool www
           ├─8121 php-fpm: pool www
           └─8122 php-fpm: pool www

[redacted] ecs-wordpress systemd[1]: Starting The PHP FastCGI Process Manager...
           ecs-wordpress systemd[1]: Started The PHP FastCGI Process Manager.
[root@ecs-wordpress wordpress]#
```

图1-35

步骤 14 输入如下命令，将 httpd 和 php-fpm 服务设为开机启动。

```
[root@ecs-wordpress wordpress]# systemctl enable httpd
[root@ecs-wordpress wordpress]# systemctl enable php-fpm
```

```
[root@ecs-wordpress wordpress]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@ecs-wordpress wordpress]# systemctl enable php-fpm
Created symlink from /etc/systemd/system/multi-user.target.wants/php-fpm.service to /usr/lib/systemd/system/php-fpm.service.
[root@ecs-wordpress wordpress]#
```

图1-36

步骤 15 打开浏览器，输入：http://ECS-WordPress 的外网 IP/wordpress/index.php。（本实验是：http://119.3.199.107/wordpress/index.php），如下图所示，证明云主机与数据库对接成功。

图1-37

1.2.5 制作镜像、申请云服务器

步骤 1 在服务列表中选择“镜像服务 IMS”。

图1-38

步骤 2 选择右上角“创建私有镜像”。

说明：后续将使用该镜像绑定弹性伸缩服务并发放云主机。

图1-39

步骤 3 按照以下配置填写参数并点击“立即创建”。

- 区域：华北-北京一（本实验以“北京一”区域为例，学员可以根据实际情况选择相应区域）
- 创建方式：系统盘镜像
- 镜像源：云服务器（选择之前步骤中创建的云主机 ecs-wordpress）
- 名称：wordpress

图1-40

步骤 4 选择创建好的镜像“wordpress”操作栏的“申请服务器”。

说明：此步骤使用镜像手动发放云主机供后续弹性负载均衡服务使用，与之前创建的云主机 ecs-wordpress 组成后端云服务器组。

步骤 5 按照下图配置完成云服务器申请。

- 计费模式：按需计费
- 区域：华北-北京一（本实验以“北京一”区域为例，学员可以根据实际情况选择相应区域）
- 可用区：可用区 2（本实验以“可用区 2”为例，学员可以根据实际情况选择相应区域）
- CPU 架构：x86 计算
- 规格：2 vCPUs | 4 GiB
- 镜像：私有镜像 | wordpress
- 网络：vpc-1 | vpc-1-subnet | 自动分配 IP 地址
- 安全组：sg-web
- 弹性公网 IP：暂不购买
- 系统盘：高 IO | 40 GiB
- 云服务器名称：ecs-wordpress
- root 密码：自定义（或选择使用镜像密码）

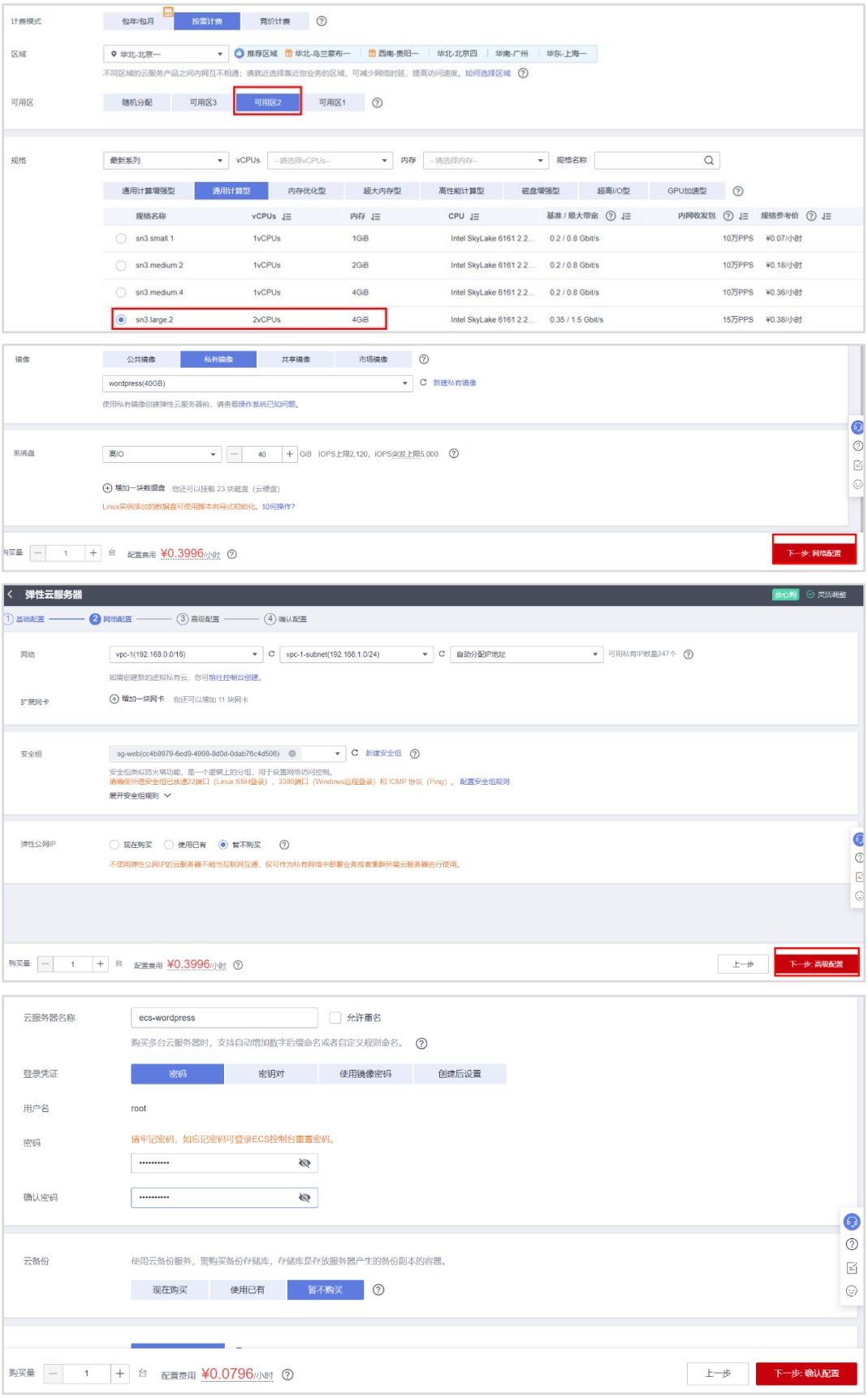

计费模式
包年/包月
按需计费
竞价计费
区域
华北-北京一
可用区
随机分配
可用区3
可用区2
可用区1
规格
最新系列
vCPUs
内存
规格名称
通用计算增强型
通用计算型
内存优化型
超大内存型
高性能计算型
磁盘增强型
超高I/O型
GPU加速型
规格名称
vCPUs
内存
CPU
内网收发包
规格参考价
sn3.small.1
1vCPUs
1GiB
sn3.medium.2
2GiB
sn3.medium.4
4GiB
sn3.large.2
2vCPUs
4GiB
Intel SkyLake 6161 2.2...
0.2 / 0.8 Gbit/s
0.35 / 1.5 Gbit/s
10万PPS
15万PPS
¥0.07/小时
¥0.18/小时
¥0.36/小时
¥0.38/小时
镜像
公共镜像
私有镜像
共享镜像
市场镜像
wordpress(40GB)
系统盘
高IO
40
GiB
购买量
1
台
配置费用
¥0.3996/小时
下一步 网络配置
弹性云服务器
网络
vpc-1(192.168.0.0/16)
vpc-1-subnet(192.168.1.0/24)
自动分配IP地址
扩展网卡
安全组
弹性公网IP
现在购买
使用已有
暂不购买
上一步
下一步 高级配置
云服务器名称
ecs-wordpress
允许重名
登录凭证
密码
密钥对
使用镜像密码
创建后设置
用户名
root
密码
确认密码
云备份
现在购买
使用已有
暂不购买
¥0.0796/小时
下一步: 确认配置

图1-41

1.2.6 创建弹性负载均衡

步骤 1 按下图指示解绑“ecs-wordpress”云主机上的弹性公网 IP。

说明：后续需要将该弹性公网 IP 绑定至弹性负载均衡器中。

图1-42

步骤 2 在服务列表中选择“弹性负载均衡 ELB”。

图1-43

步骤 3 选择右上角“购买弹性负载均衡”。

步骤 4 按照下图配置完成弹性负载均衡创建。

- 实例规格类型：共享型

- 区域：华北-北京一（本实验以“北京一”区域为例，学员可以根据实际情况选择相应区域）
- 网络类型：公网
- 所属 VPC：vpc-1
- 子网：vpc-1-subnet
- 私有 IP 地址：自动分配 IP 地址

图1-44

- 弹性公网 IP：使用已有（将刚解绑的弹性公网 IP 分配给该弹性负载均衡）
- 名称：elb-wordpress

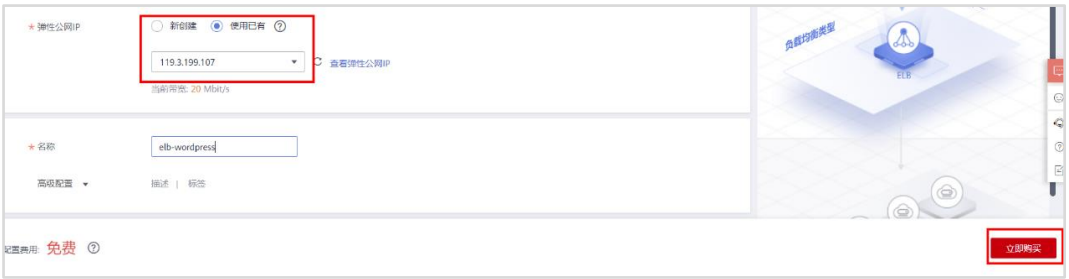


图1-45

步骤 5 在负载均衡器列表中找到刚创建的“elb-wordpress”，点击“点我开始配置”。

图1-46

步骤 6 按照以下参数完成负载均衡器配置。

- 名称：listener-wordpress
- 前端协议：TCP
- 前端端口：80（即负载均衡器提供服务时接收请求的端口）

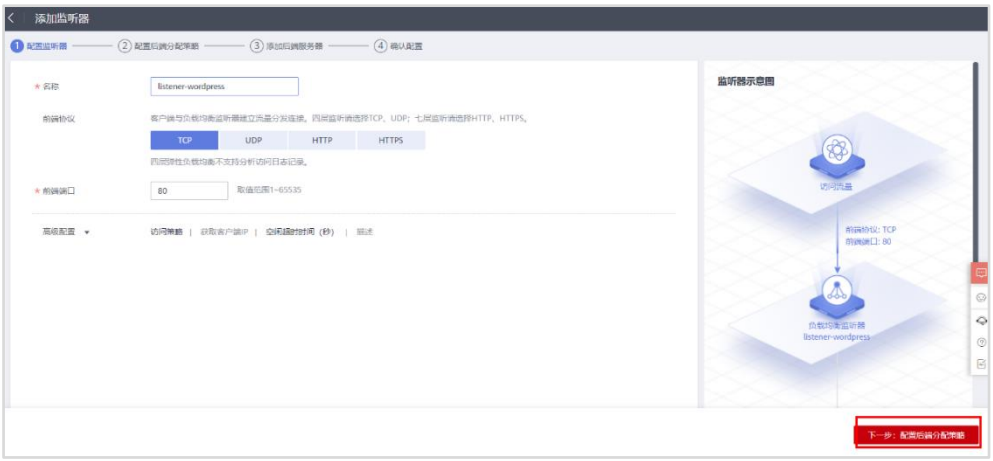


图1-47

- 打开会话保持（使得负载均衡器可以识别客户与服务器之间交互过程的关联性，在实现负载均衡的同时，保持将其他相关联的访问请求分配到同一台服务器上），其他参数保持默认即可，点击“下一步 添加后端服务器”。

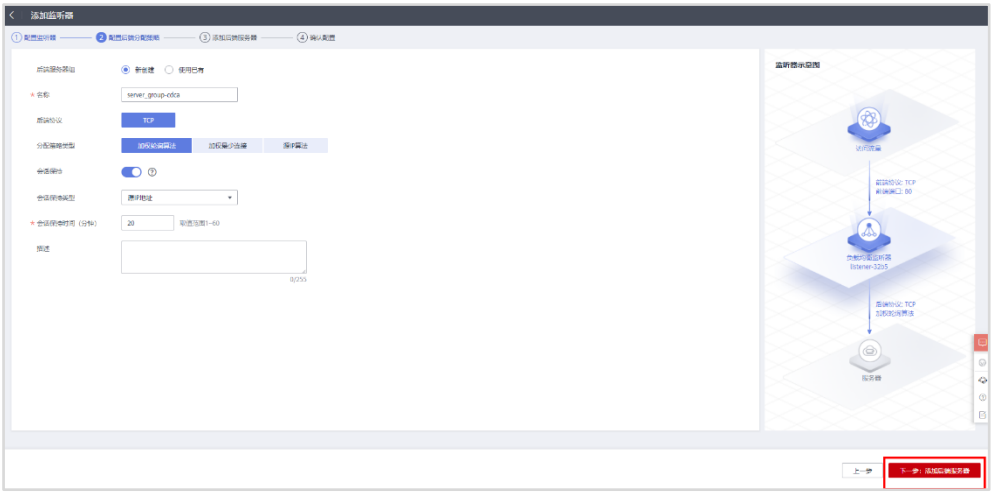


图1-48

- 点击“添加云服务器”。

图1-49

- 选择云主机“ecs-wordpress”和用镜像创建的云主机“ecs-wordpress-0001”。

图1-50

- 批量添加 80 端口（该端口是指后端云服务器自身提供的网络服务的协议端口），其他配置保持默认即可，确认配置后购买。

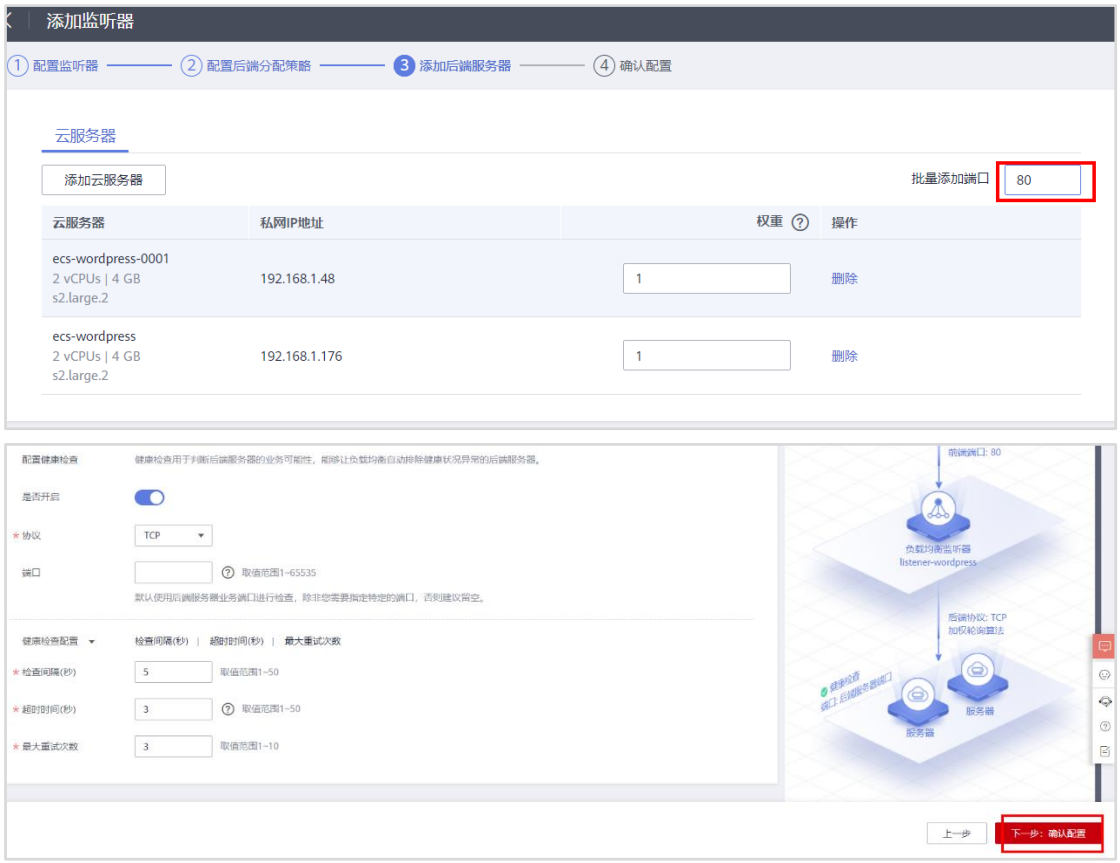


图1-51

- 创建完成后，点击“监听器-后端服务器组”查看健康检查结果为正常。

图1-52

- 在列表页面查看购买的负载均衡器。

图1-53

步骤 7 创建完成后，重新浏览器登录“http://119.3.199.107（ELB 的弹性公网 IP）/wordpress/index.php”验证，如下图结果证明弹性负载均衡器部署成功。

图1-54

1.2.7 创建弹性伸缩服务

步骤 1 在服务列表中选择“数据加密服务 DEW”。

图1-55

步骤 2 在密钥对管理中选择“创建密钥对”（供后续创建弹性伸缩服务使用）。

图1-56

- 配置名称为“KeyPair-wordpress”点击“确定”。

说明：本实验中该密钥对用于创建弹性伸缩服务，不参与实际应用。

图1-57

步骤 3 在服务列表中选择“弹性伸缩 AS”。

图1-58

步骤 4 选择右上角“创建伸缩配置”。

图1-59

步骤 5 按照以下配置完成伸缩配置创建。

- 计费模式：按需计费
- 区域：华北-北京一（本实验以“北京一”区域为例，学员可以根据实际情况选择相应区域）
- 名称：as-config-wordpress
- 配置模板：使用新模板

图1-60

- 规格：2 vCPU|4 GiB
- 镜像：私有镜像|wordpress
- 磁盘：云硬盘|高 IO|40 GB
- 安全组：sg-web
- 弹性公网 IP：不使用

图1-61

- 选择密钥对，选择高级设置。参照以下命令，注入文本，用以修改镜像中 wp-config.php 文件里的数据库的地址信息（本例中是将原来“DB_HOST”后面的字段覆写为“192.168.1.137”）。

```
#!/bin/bash
sed -i -E "s/'DB_HOST',\s*'.*?'/'DB_HOST', '192.168.1.137'/" /var/www/html/wordpress/wp-config.php
```

说明：其中“192.168.1.137”为本例中后端数据库内网地址，实验时请按实际数据库地址填写。

图1-62

步骤 6 完成伸缩配置创建后，点击右上角“创建弹性伸缩组”。

图1-63

步骤 7 按照以下配置完成弹性伸缩组创建。

- 区域：华北-北京一（本实验以“北京一”区域为例，学员可以根据实际情况选择相应区域）
- 可用区：默认配置
- 多可用区扩展策略：均衡分布
- 名称：as-group-wordpress
- 最大实例数：4
- 期望实例数：2（考虑实验环境容量，建议本实验中期望实例配置为 2）
- 最小实例数：1
- 伸缩配置：as-config-wordpress
- 虚拟私有云：vpc-1
- 子网：vpc-1-subnet
- 负载均衡：使用弹性负载均衡
- 负载均衡器：elb-wordpress（选择之前创建的负载均衡器）
- 后端服务器组：“elb-wordpress”负载均衡器中的后端服务器组

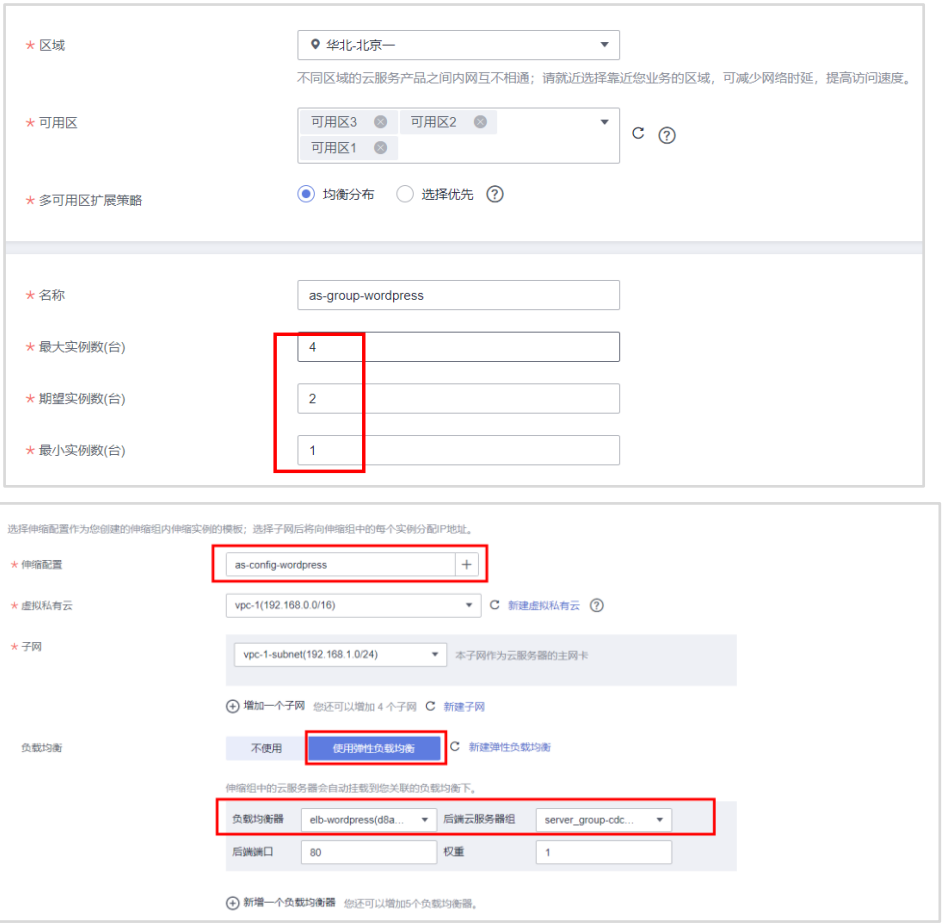


图1-64

- 其他配置保持默认，点击“立即创建”。

图1-65

步骤 8 在伸缩实例列表查看已创建的弹性伸缩组状态为“已启用”。

图1-66

步骤 9 此时在弹性云服务器列表界面可以看到两台由 AS 创建的两台云服务器。

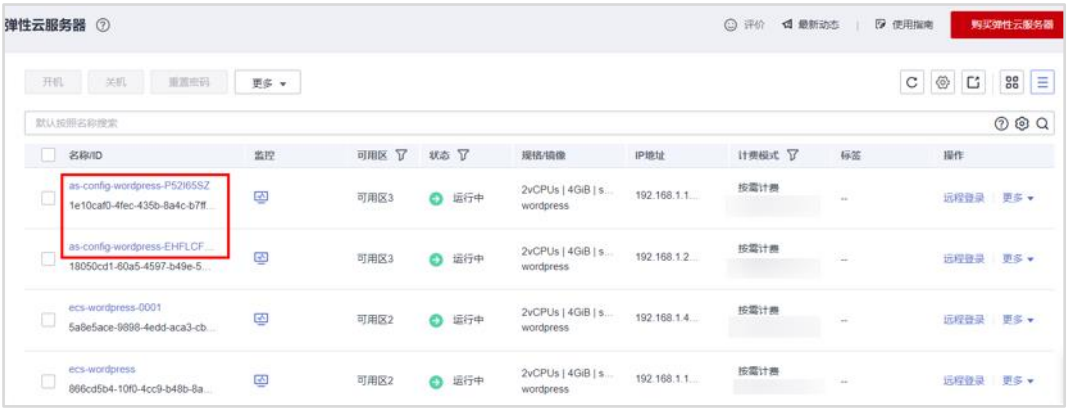


图1-67

步骤 10 此时任选一台，使用页面上的“远程登录”登录云主机，使用如下命令查看云主机中 wp-config.php 文件配置，发现原先 192.168.1.137:3306 已被修改为 192.168.1.137.（此操作只为验证文本注入功能，不影响登录，默认使用 3306 端口）。

```
[root@ecs-wordpress ~]# cat /var/www/html/wordpress/wp-config.php
```

说明：通过这种方式，在后端数据库地址发生改变（或其他类似问题）的情况下，可以直接通过 AS 文本注入的方式修改绑定镜像中的相应位置数据来保证业务连续性，无需重构镜像。

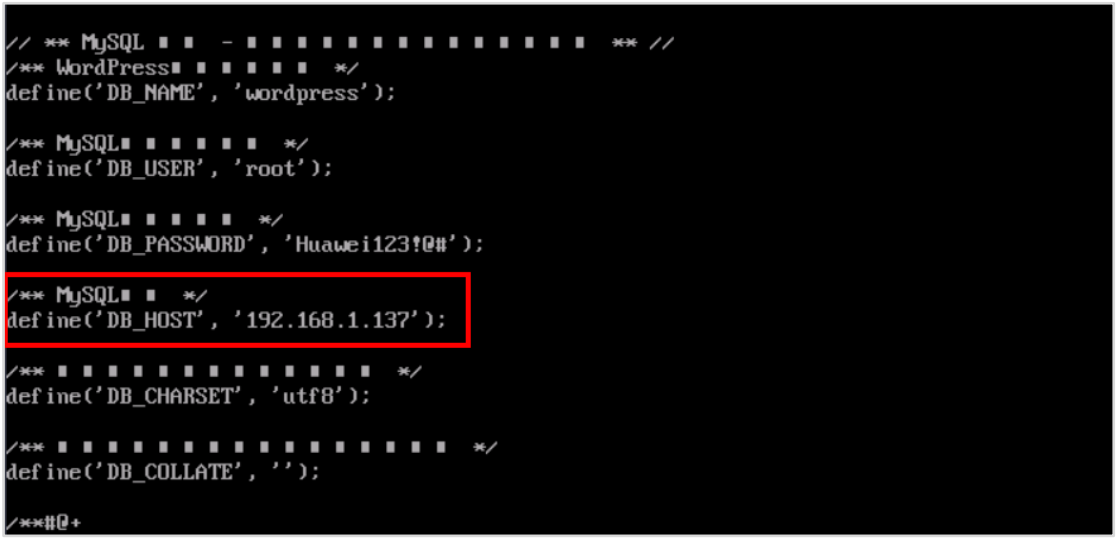


图1-68

步骤 11 此时删除原手动创建的“esc-wordpress”和“ecs-wordpress-0001”云主机。

说明：该步骤是为了验证由弹性负载均衡服务发放的云主机是否可以正常提供服务。

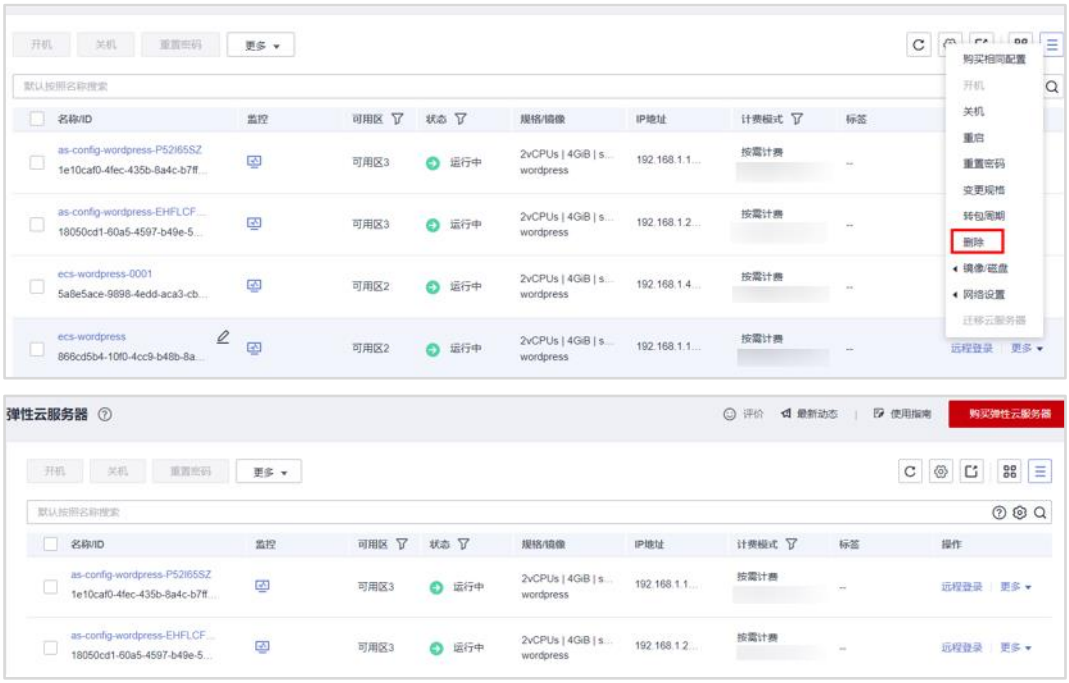


图1-69

步骤 12 浏览器重新登录“http://119.3.199.107（ELB 的弹性公网 IP）/wordpress/index.php”验证。

图1-70

步骤 13 填入注册信息后点击“安装 WordPress”，验证可正常登录，证明由弹性伸缩服务注入文本并生成的云主机可以正常提供服务，本实验成功完成。

- 站点标题：HCIP
- 用户名：huawei（可学员自定义）
- 密码：学员自定义
- 电子邮件：学员自定义

图1-71

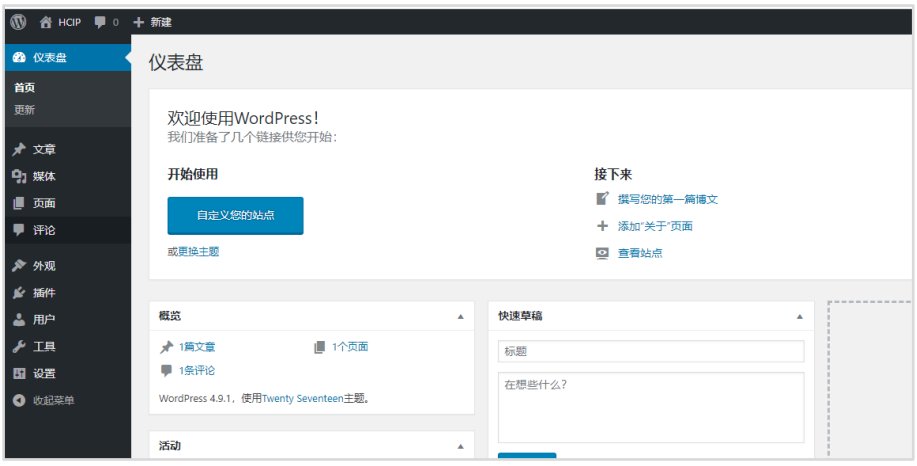


图1-72

1.3 实验恢复

步骤 1 删除弹性伸缩服务。

- 在服务列表中点击“弹性伸缩 AS”，在“弹性伸缩组”列表中找到创建的弹性伸缩组，点击操作栏的“更多-删除”。
- 点击“伸缩配置”，在列表中找到本实验中创建的伸缩配置，点击操作栏的“删除”。

步骤 2 删除密钥对。

- 在服务列表中选择“数据加密服务 DEW”，在“密钥对管理”页签中选择“私有密钥对”。
- 找到本实验中创建的密钥对，点击对应操作栏的“删除”。

步骤 3 删除弹性负载均衡。

- 在服务列表中选择“弹性负载均衡 ELB”。在负载均衡器列表中点击创建的负载均衡器名称并选择“后端服务器组”页签。勾选所有后端服务器，点击“移除”。

图1-73

- 选择“监听器页签”，点击页面中的删除按钮，删除监听器。

图1-74

- 返回负载均衡器列表，点击操作栏的“删除”按钮删除负载均衡器。
- 在弹出的对话框中勾选“释放该负载均衡绑定的弹性公网 IP”。

图1-75

步骤 4 删除镜像。

- 在服务列表中选择“镜像服务 IMS”，在私有镜像列表中找到本实验中创建的镜像 wordpress，在操作栏中点击“更多-删除”。

步骤 5 删除 RDS。

- 在服务列表中选择“云数据库 RDS”，在云数据库列表中找到本实验创建的数据库实例，点击操作栏中的“更多-删除实例”。

步骤 6 删除 ECS。

- 在服务列表中选择“云服务器 ECS”，找到本实验创建的云服务器，点击操作栏中的“更多-删除”。
- 在弹出的对话框中勾选下图中选项，点击“是”。

图1-76

步骤 7 删除安全组。

- 在服务列表中选择“虚拟私有云 VPC”，在“访问控制-安全组”中找到本实验创建的安全组，点击操作栏的“更多-删除”。

步骤 8 删除 VPC。

- 在服务列表中选择“虚拟私有云 VPC”，点击“子网”页签，在列表中找到本实验创建的子网，点击操作栏中的“删除”。
- 点击“虚拟私有云”页签，找到本实验创建的 VPC，点击操作栏中的“删除”。

1.4 思考题

问题：在弹性负载均衡器的健康检查配置中，如果开启健康检查后，不填写健康检查端口，健康检查会如何进行?

参考答案：默认会使用后端服务器端口进行健康检查，如果配置了健康检查端口，会使用配置的健康检查端口进行健康检查。

2 网络架构设计实验

2.1 实验介绍

2.1.1 关于本实验

本实验将使用华为云模拟用户线下局点以及用户云上资源，通过华为云相关网络服务实现云上资源远程运维、云上资源互通和云上资源访问互联网的需求。

本实验将使用上海一区域的 VPC1 模拟线下局点，其云主机模拟局点运维主机。北京四区域中 VPC2、VPC3 及其云主机模拟云上资源。

考虑云上资源互通的需求，北京四区域中 VPC2 和 VPC3 内云主机设计通过对等连接实现互相通信。考虑云上资源远程运维的需求，上海一区域（局点）和北京四区域（云上）内云主机设计通过虚拟专用网络（Virtual Private Network，简称 VPN）VPN 网关+对等连接实现互通，模拟局点运维主机远程管理云上资源。考虑云上资源公网访问需求，设计于北京四区域中的 VPC2 内部署 NAT 网关，使得 VPC3 和 VPC2 内云主机均可通过 VPC2 中创建的 NAT 网关访问互联网。

说明：本实验以“上海一”和“北京四”区域为例，学员可以根据实际情况选择相应区域进行实验。

2.1.2 实验目的

理解云上网络服务架构中各云服务的使用。

掌握对云上网络可扩展性、延展性等方面的设计方法，掌握云上云下资源统一管理、互相通信的设计方法。

2.1.3 实验组网

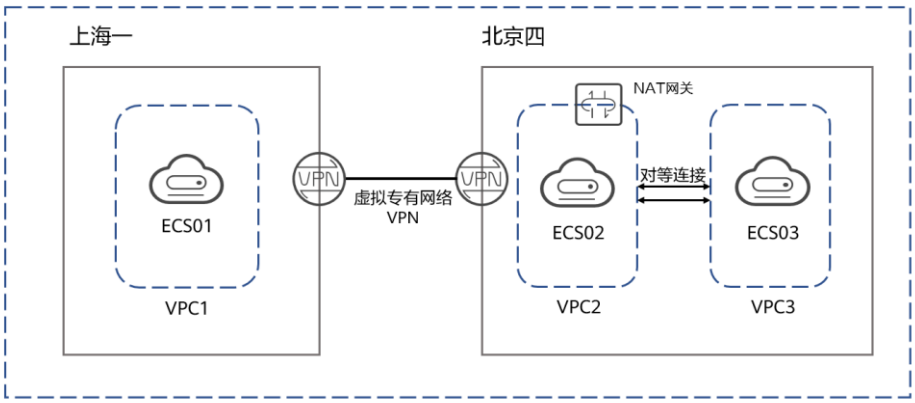


图2-1

2.2 实验配置

2.2.1 创建 VPC

步骤 1 打开华为云官网 https://www.huaweicloud.com/，登录华为云账号，如果是 IAM 账号，请切换成统一身份认证服务 IAM 用户登录。

图2-2

图2-3

步骤 2 点击控制台，选择“华东-上海一”区域。

步骤 3 在服务列表里，选择“虚拟私有云 VPC”。

步骤 4 点击右上角“创建虚拟私有云”。

图2-4

步骤 5 按照以下要求填写参数，并点击“立即创建”。

说明：该 VPC 在本实验中用于模拟用户线下局点网络。

基本信息

- 区域：华东-上海一
- 名称：vpc-1
- IPv4 网段：192.168.0.0/16

默认子网

- 可用区：可用区 3（本 VPC 可用区以“可用区 3”为例，学员可以根据实际情况选择相应区域，下文类似资源不再赘述）
- 名称：vpc-1-subnet
- 子网 IPv4 网段：192.168.1.0/24

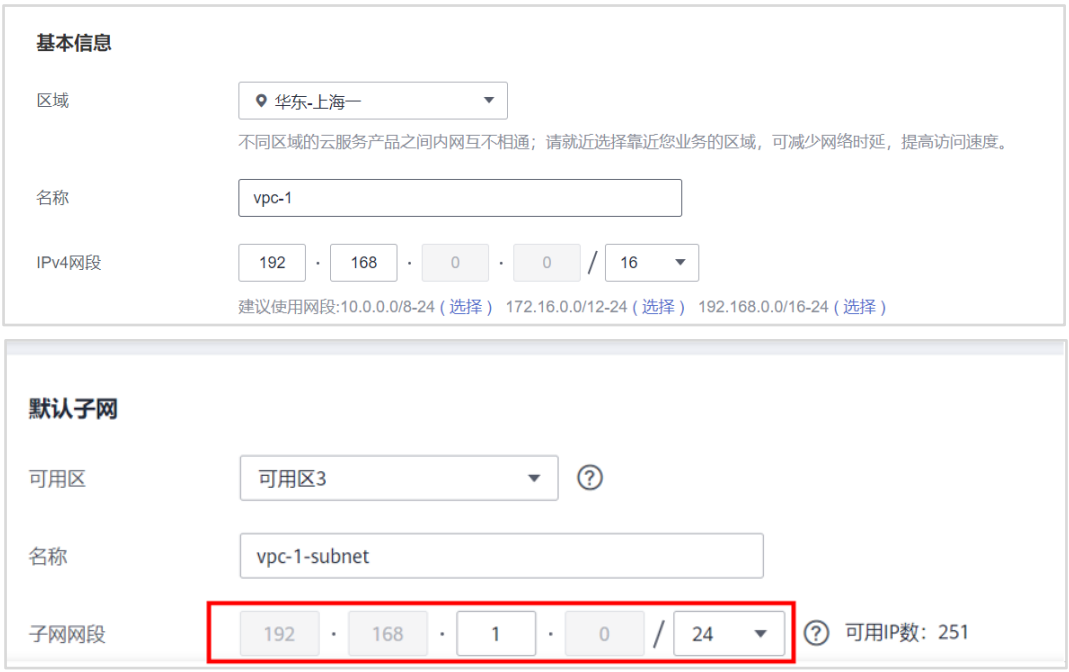


图2-5

步骤 6 重复上述步骤，按如下配置创建 VPC2 和 VPC3。

说明：VPC2 和 VPC3 本实验中用于模拟用户云上网络资源。

基本信息

- 区域：华北-北京四
- 名称：vpc-2
- IPv4 网段：192.168.0.0/16

默认子网

- 可用区：可用区 1
- 名称：vpc-2-subnet
- 子网 IPv4 网段：192.168.2.0/24

基本信息

- 区域：华北-北京四
- 名称：vpc-3
- IPv4 网段：192.168.0.0/16

默认子网

- 可用区：可用区 1
- 名称：vpc-3-subnet
- 子网 IPv4 网段：192.168.3.0/24

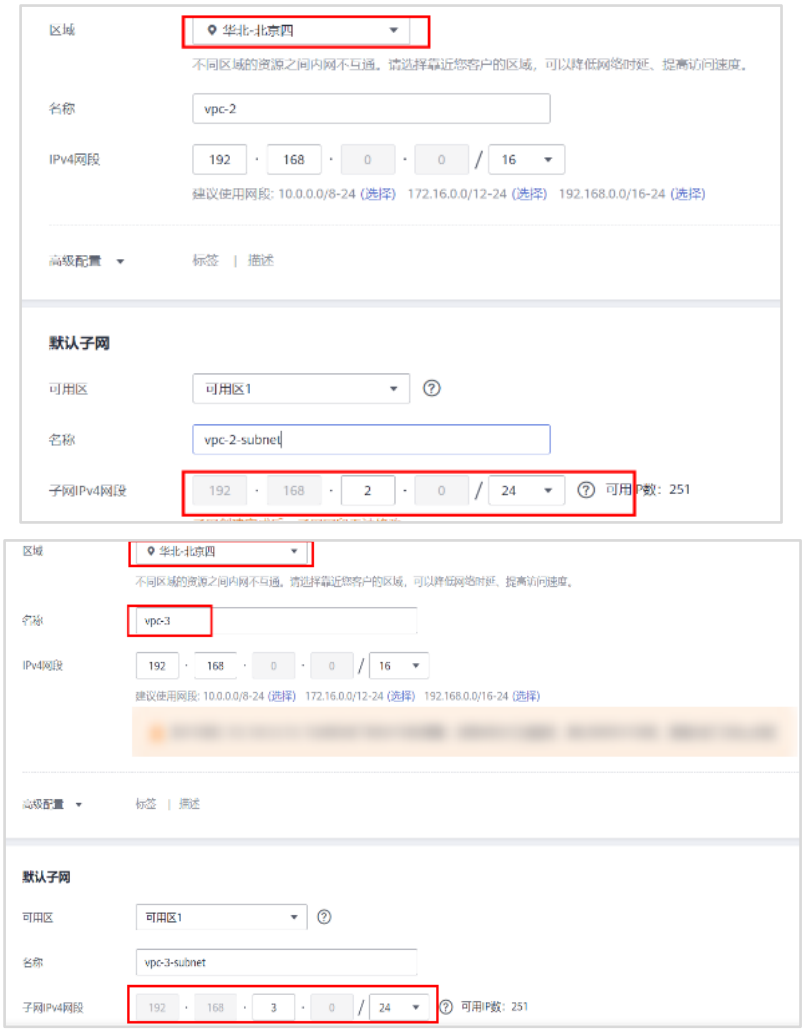


图2-6

2.2.2 创建安全组

步骤 1 在“上海一”中选择“网络控制台>访问控制>安全组”，点击右上角“创建安全组”。

图2-7

步骤 2 按照以下参数进行配置，并点击“确定”。

说明：该安全组供后续 VPC1 中云主机使用，需要放通 ICMP 协议和 22 端口，其中 ICMP 协议用于连通性测试，22 端口用于 SSH 登录测试。

- 名称：sg-1
- 模板：自定义

图2-8

步骤 3 在弹出的提示框中选择“配置规则”。

图2-9

步骤 4 按如下配置添加第一条入方向规则。

- 优先级：1
- 策略：允许
- 协议：ICMP
- 端口：全部
- 源地址：IP 地址|0.0.0.0/0

图2-10

步骤 5 按如下配置添加第二条入方向规则。

- 优先级：1
- 策略：允许
- 协议：TCP
- 端口：22
- 源地址：IP 地址|0.0.0.0/0

图2-11

步骤 6 重复以上安全组创建步骤，以相同配置在“华北-北京四”中创建安全组 sg-4。

说明：安全组 sg-4 供后续北京四区域中云主机使用，同样需要放通 ICMP 协议和 22 端口。

2.2.3 创建云主机

步骤 1 在“华东-上海一”中点击右上角“购买弹性云服务器”。

图2-12

步骤 2 按照以下配置购买云服务器。

说明：云主机“ecs-01”用于模拟线下局点的运维主机。

云主机“ecs-01”配置：

- 计费模式：按需计费
- 区域：华东-上海一
- 可用区：随机分配
- CPU 架构：x86 计算

- 规格：1 vCPUs | 2 GiB
- 镜像：公共镜像 | CentOS 7.6 64 bit
- 主机安全：开通主机安全（基础版）
- 网络：vpc-1 | vpc-1-subnet | 自动分配 IP 地址
- 安全组：sg-1
- 弹性公网 IP：暂不购买
- 系统盘：高 IO | 40 GiB
- 云服务器名称：ecs-01
- root 密码：自定义

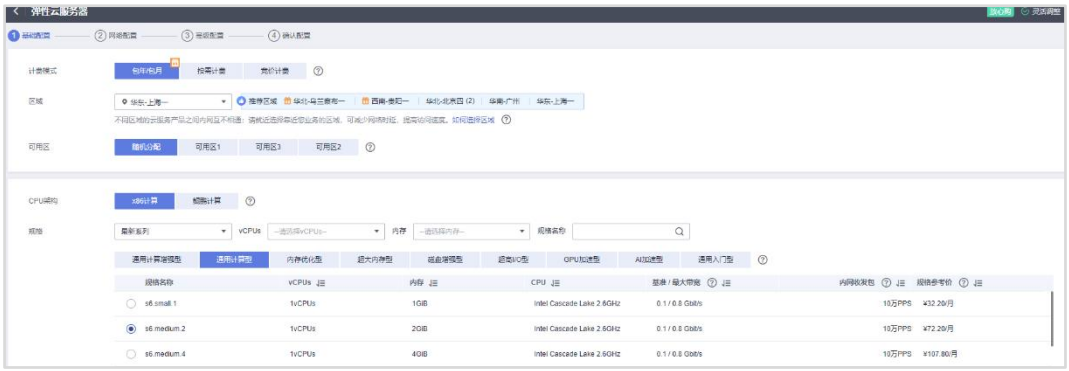


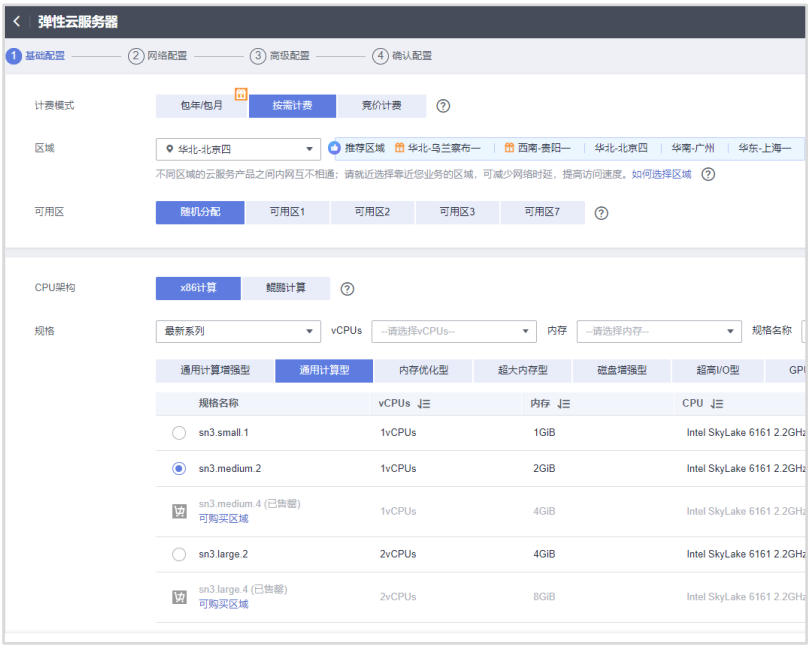
图2-13

步骤 3 重复以上步骤 1-2，在“华北-北京四”继续购买 ECS02 和 ECS03。

说明：云主机“ecs-02”和“ecs-03”用于模拟用户云上资源。

云主机“ecs-02”配置：

- 计费模式：按需计费
- 区域：华北-北京四
- 可用区：随机分配
- CPU 架构：x86 计算
- 规格：1 vCPUs | 2 GiB
- 镜像：公共镜像 | CentOS 7.6 64 bit
- 主机安全：开通主机安全（基础版）
- 网络：vpc-2 | vpc-2-subnet | 自动分配 IP 地址
- 安全组：sg-4
- 弹性公网 IP：暂不购买
- 系统盘：高 IO| 40 GiB
- 云服务器名称：ecs-02
- root 密码：自定义



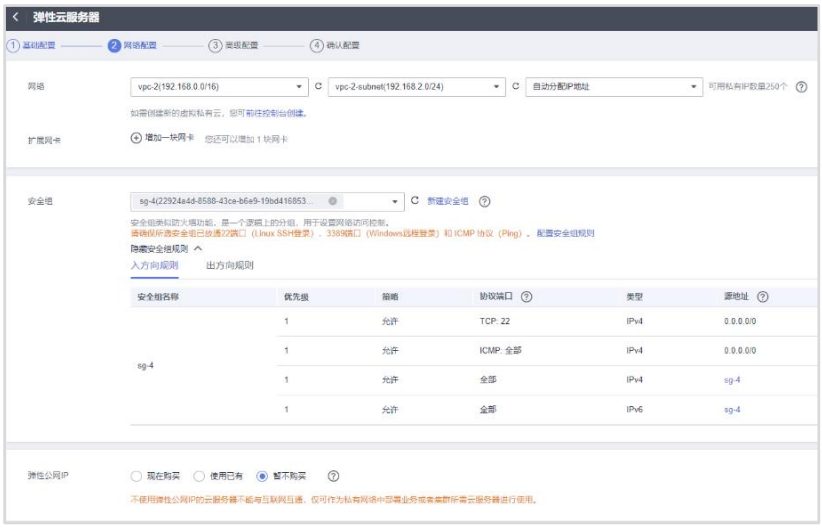
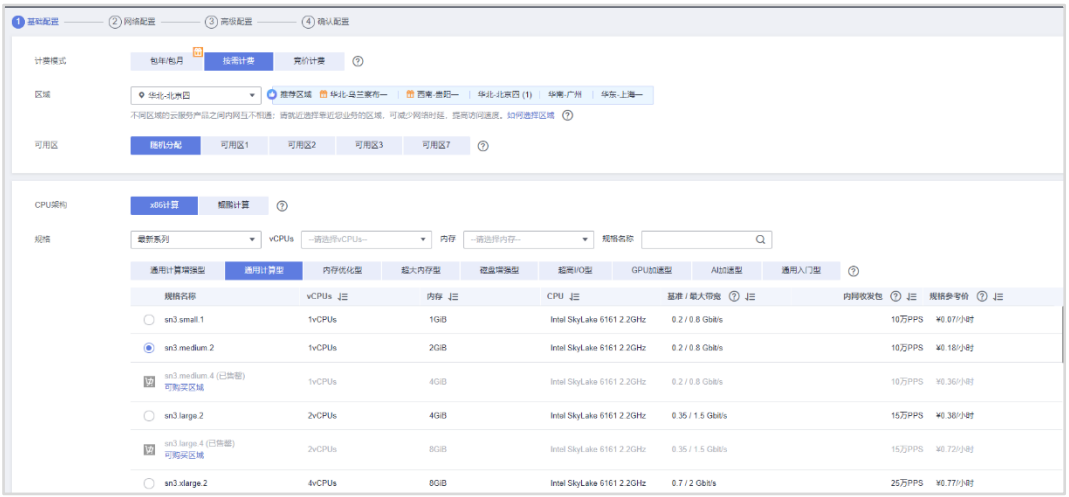


图2-14

云主机“ecs-03”配置：

- 计费模式：按需计费
- 区域：华北-北京四
- 可用区：随机分配
- CPU 架构：x86 计算
- 规格：1 vCPUs | 2 GiB

- 镜像：公共镜像 | CentOS 7.6 64 bit
- 主机安全：开通主机安全（基础版）
- 网络：vpc-3 | vpc-3-subnet | 自动分配 IP 地址
- 安全组：sg-4
- 弹性公网 IP：暂不购买
- 系统盘：高 IO | 40 GiB
- 云服务器名称：ecs-03
- root 密码：自定义



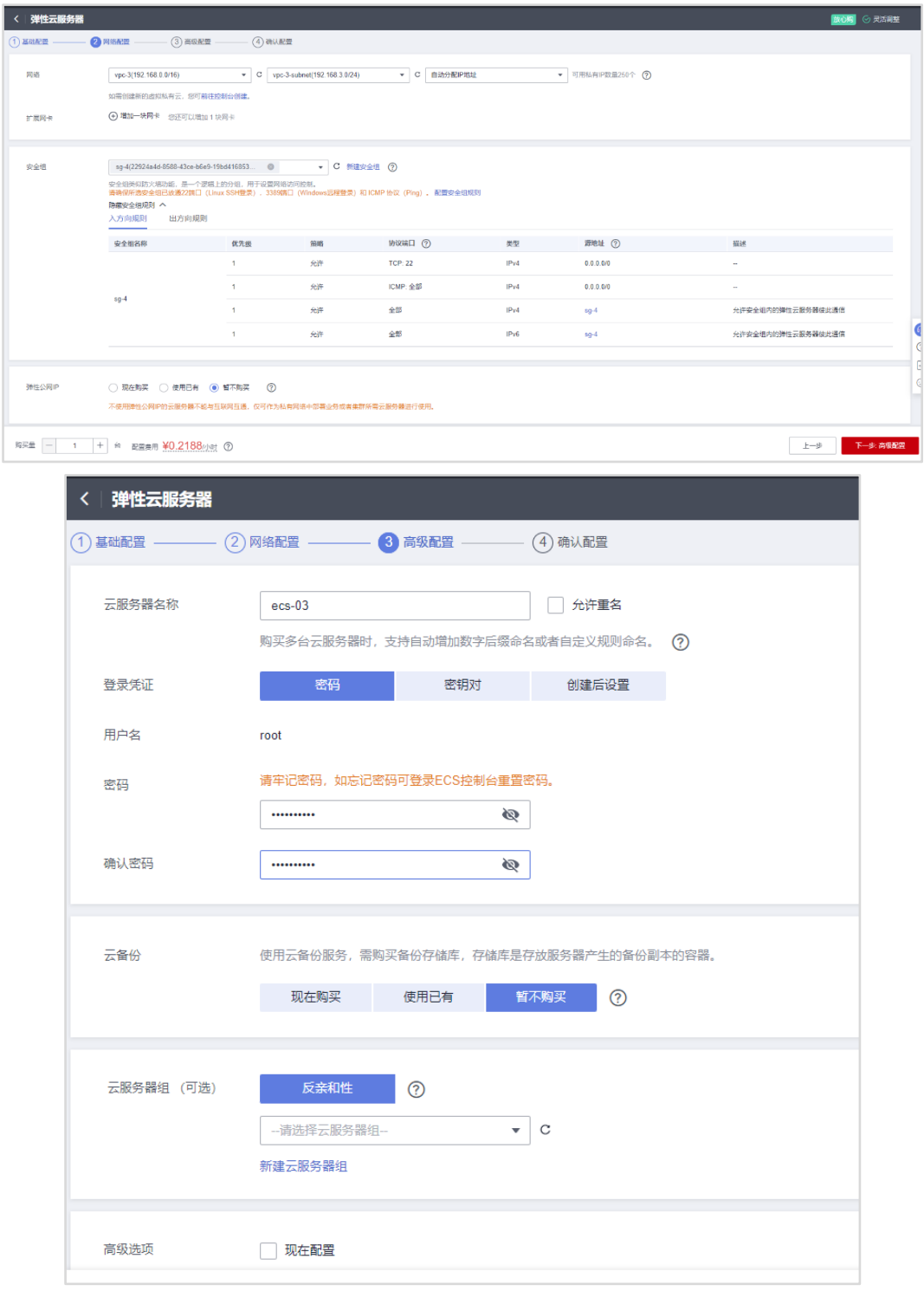


图2-15

2.2.4 创建对等连接

步骤 1 在“华北-北京四”中选择“网络控制台>对等连接”，点击右上方“创建对等连接”。

说明：该对等连接用来连通用户云上 VPC2 和 VPC3 的资源。

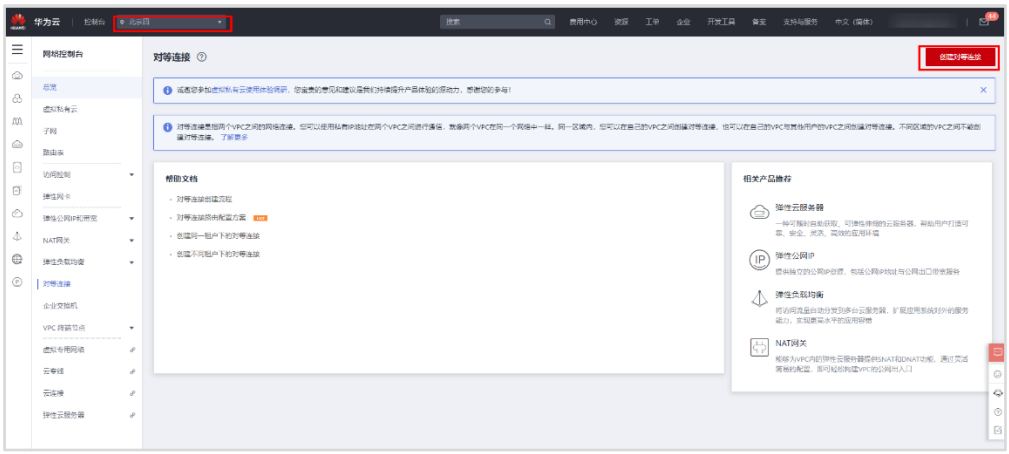


图2-16

步骤 2 按如下配置填入相关配置参数。

- 名称：vpc2-vpc3
- 本端 VPC：vpc-2
- 账户：当前账户
- 对端项目：cn-north-4
- 对端 VPC：vpc-3

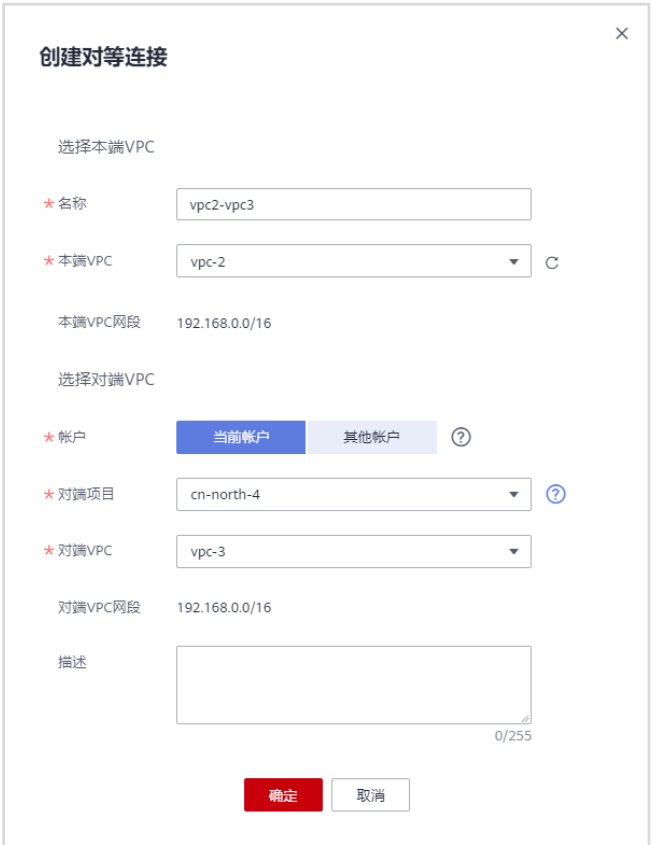


图2-17

步骤 3 回到对等连接主页面，查看已创建的对等连接“vpc2-vpc3”，点击名称进入该对等连接视图。

图2-18

步骤 4 此时需要配置本端和对端路由，点击图中红框位置的“路由表”进入 VPC-2 路由表管理界面。

图2-19

步骤 5 选择“添加路由”。

图2-20

步骤 6 在弹出的配置框中按如下内容进行配置。完成后选择“确定”。

说明：该配置是在 VPC2 的路由表中添加指向 VPC3 子网的路由。

- 目的地址：192.168.3.0/24
- 下一跳类型：对等连接
- 下一跳：vpc2-vpc3

图2-21

步骤 7 完成 VPC-2 的路由配置后（本端路由），需要继续配置 VPC-3 的路由（对端路由），进入路由表管理界面，选择进入 VPC-3 的路由表“rtb-vpc-3”。

图2-22

步骤 8 选择“添加路由”。

图2-23

步骤 9 在弹出的配置框中按如下内容进行配置。完成后选择“确定”。

说明：该配置是在 VPC3 的路由表中添加指向 VPC2 子网的路由。

- 目的地址：192.168.2.0/24
- 下一跳类型：对等连接
- 下一跳：vpc2-vpc3

图2-24

步骤 10 按以下步骤登录 ECS03，验证 ECS02 与 ECS03 通信。

- 点击 ECS03 操作栏中的“远程登录”

图2-25

- 选择“CloudShell”登录。

图2-26

- 输入 root 密码，其他配置保持默认，点击“连接”。

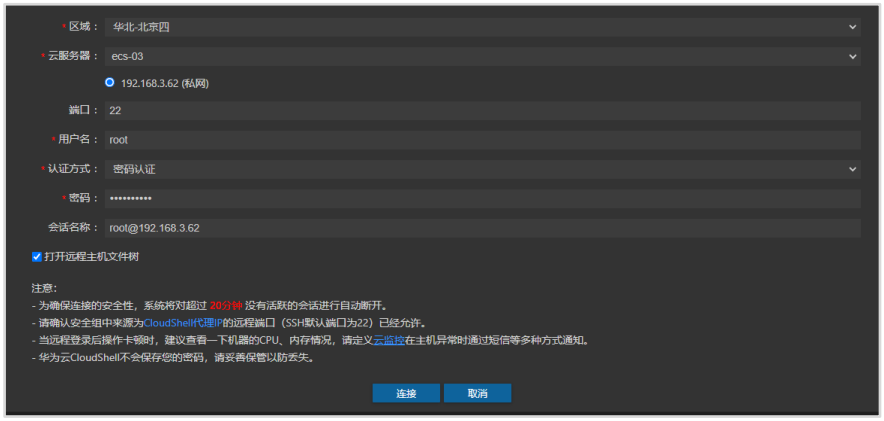


图2-27

- 在 ECS03 中使用“ping”命令测试 ECS02 和 ECS03 云主机之间的通信。

说明：192.168.2.180 为 ECS02 的 VPC 内私网 IP 地址。

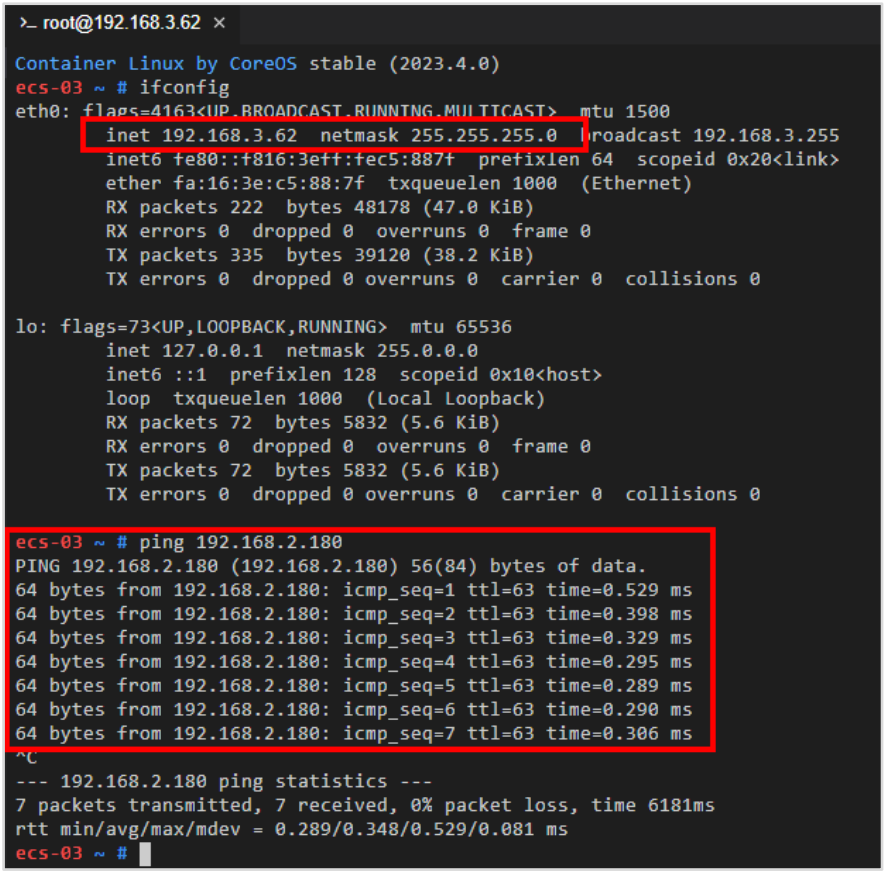


图2-28

2.2.5 配置虚拟专用网络

步骤 1 在“华东-上海一”中选择“网络控制台>虚拟专用网络>VPN 网关”，点击右上角“创建 VPN 网关”。

图2-29

步骤 2 按如下配置填入相应参数创建 VPN 网关。

说明：该 VPN 网关用来连接线下局点（上海一区域）和云上资源（北京四区域）。

- 计费模式：按需计费
- 区域：华东-上海一

图2-30

VPN 网关配置：

- 名称：vpngw-vpc1
- 虚拟私有云：vpc-1
- 类型：IPsec
- 计费方式：按带宽计费
- 带宽大小：5 Mbit/s

图2-31

VPN 连接配置：

- 名称：vpn-1
- 本端子网：子网|vpc-1-subnet

- 远端网关：100.100.100.100（此处使用该地址填充，后续需要使用创建的真实远端网关 IP 替换）
- 远端子网：192.168.2.0/24,192.168.3.0/24

说明：此处需要填写 VPC2 和 VPC3 中的子网网段。该配置是为了在本端指定 IPsec 的兴趣流量，方便后续业务报文触发 IPsec 封装。

- 预共享密钥：自定义

图2-32

步骤 3 确认配置后选择“提交”。

步骤 4 在主页面中查看刚创建的 VPN 网关，并记录网关 IP 备用（此处为 49.4.126.85）。

说明：在创建对端 VPN 网关时，需要填入当前本端 VPN 网关的 IP。

图2-33

步骤 5 在“华北-北京四”中选择“网络控制台>虚拟专用网络>VPN 网关”，点击右上角“创建 VPN 网关”。按如下配置填入相应配置参数。

说明：该配置是在云上（北京四区域）创建 VPN 网关，用以连接线下局点（上海一区域）的 VPN 网关。

- 区域：北京四
- 名称：vpngw-vpc2

- 虚拟私有云：vpc-2
- 类型：IPSec
- 计费方式：按带宽计费
- 带宽大小：5 Mbit/s

图2-34

步骤 6 这里注意需要将刚刚记录的网关 IP 填入这里的“远端网关”中。

- 名称：vpn-1-2
- 本端子网：子网|vpc-2-subnet
- 远端网关：49.4.126.85
- 远端子网：192.168.1.0/24

说明：此处需要填写 VPC1 中的子网网段。该配置是为了在本端指定 IPSec 的兴趣流量，方便后续业务报文触发 IPSec 封装。

- 预共享密钥：自定义
- 高级配置：默认配置

图2-35

步骤 7 在主页面查看创建好的 VPN 网关，并记录网关 IP 地址（此处为 123.60.251.196）。

说明：需要在对端的（上海一中的）VPN 网关中将“远端网关”地址修改为当前记录的地址。

图2-36

步骤 8 返回“华东>上海一”选择“VPN 连接”。

图2-37

步骤 9 选择“更多>修改”。

图2-38

步骤 10 将“远端网关”地址修改为刚刚记录的 123.60.251.196，完成修改后点击“确定”。

- 修改前：

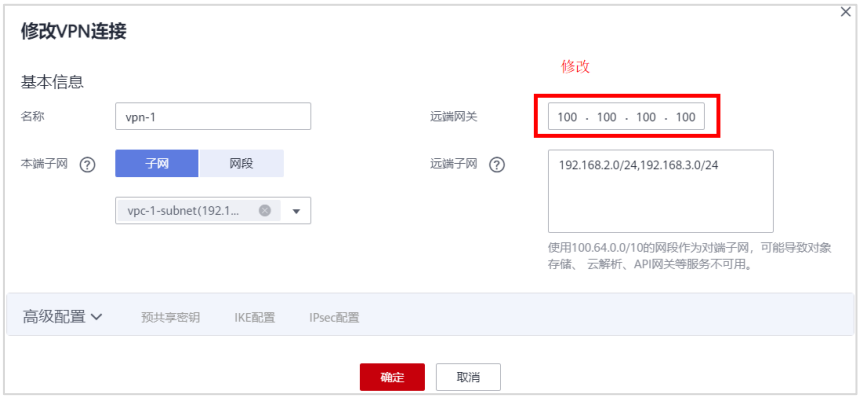


图2-39

- 修改后：

说明：将远端网关替换为刚才记录的地址 123.60.251.196。

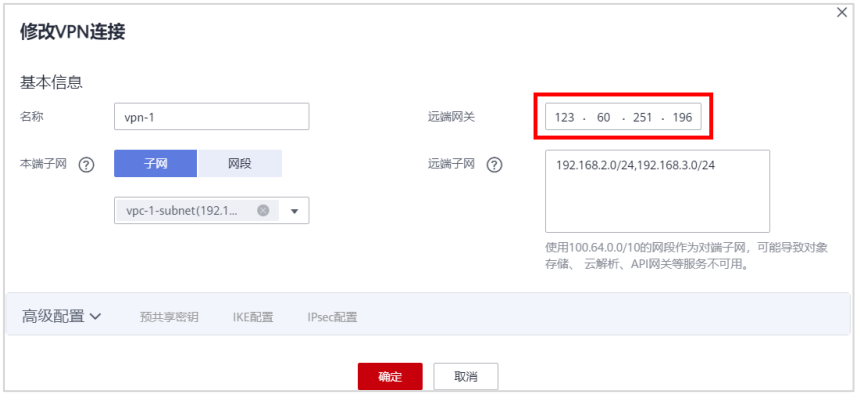


图2-40

步骤 11 查看 VPN 连接状态为“更新中”。

说明：没有流量触发 IPSec SA 协商，状态暂时会保持在“更新中”。

图2-41

步骤 12 登录 ECS01，使用“ping”命令测试与 ECS02 的连通性，触发兴趣流量和 IPsec SA 协商。

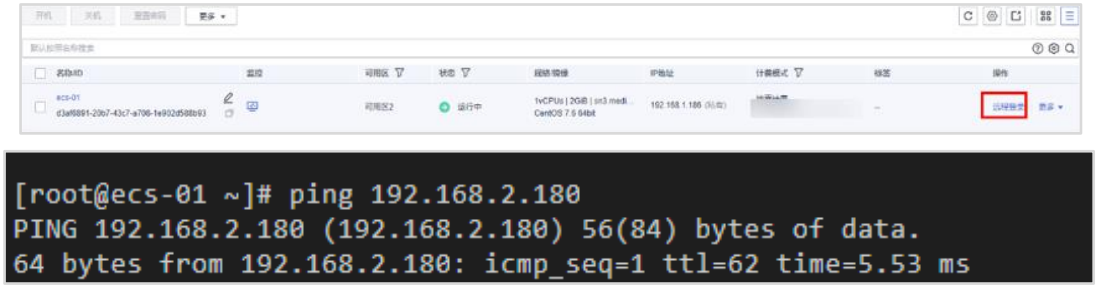


图2-42

步骤 13 刷新 VPN 连接页面，此时显示连接正常。

说明：此时证明 VPN 连接建立成功，且 IPSec SA 协商成功，可以正常传输报文。

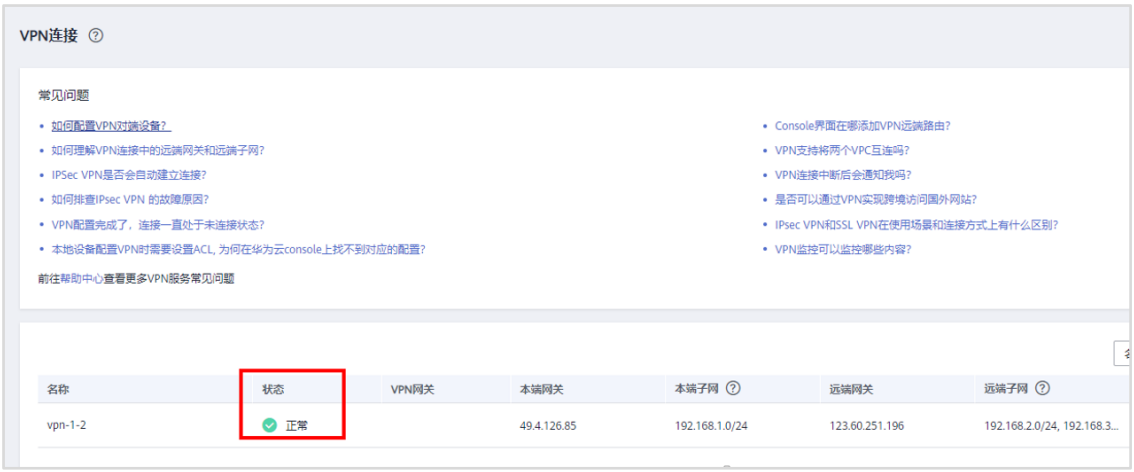


图2-43

2.2.6 配置 ECS01 登录管理 ECS03

当前 VPN 连接已正常，ECS01 与 ECS02 可正常通信，如果需要使用 ECS01 登录 ECS03 进行管理，则需要进行如下配置：

- VPC-3 的路由表中增加去往 192.168.1.0/24 网段（VPC-1 子网）路由，并指向与 VPC-2 的对等连接。
- 需将 VPC-2 的 VPN 连接中“本端子网”类型改为“网段”，并加入 192.168.3.0/24 网段。

步骤 1 进入“华北-北京四”中路由表管理界面，选择 VPC-3 的路由表“rtb-vpc-3”进入。

图2-44

步骤 2 选择“添加路由”。

图2-45

步骤 3 按以下配置添加 192.168.1.0/24 的路由，指向对等连接。完成后点击“确定”。

说明：该配置是在 VPC3 中添加去往 VPC1 的路由。

- 目的地址：192.168.1.0/24
- 下一跳类型：对等连接
- 下一跳：vpc2-vpc3

图2-46

步骤 4 在“华北-北京四”中选择“网络控制台>虚拟专用网络>VPN 连接”，修改 VPN 连接“vpn-1-2”中的“本端子网”类型为“网段”，并加入 192.168.3.0/24 网段。

- 修改前：

图2-47

- 修改后：

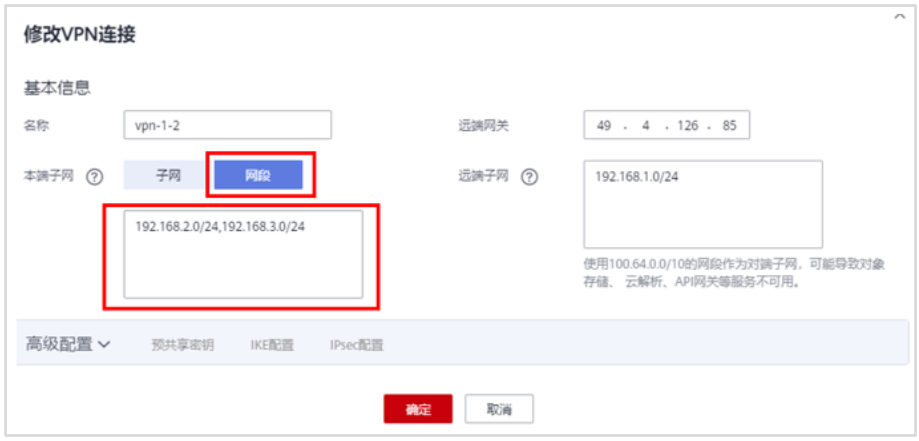


图2-48

说明：修改完成后，VPC-3 中拥有了去往 192.168.1.0/24 的路由，（北京四区域中的）VPN 连接中本端子网也包含了 192.168.3.0/24 网段，当报文到达 VPC-2 时，会正常触发 IPSec 封装。

2.2.7 创建 NAT 网关

步骤 1 在“华北-北京四”中，选择“网络控制台>虚拟私有云>弹性公网 IP 和带宽>弹性公网 IP”，点击右上角“购买弹性公网 IP”，按以下配置内容填写相关参数后，选择“立即购买”。

说明：该 NAT 网关创建在 VPC2 中，将为 VPC2 和 VPC3 中的资源提供公网访问服务。

- 计费模式：按需计费
- 区域：华北-北京四
- 线路：全动态 BGP
- 公网带宽：按流量计费
- 带宽大小：5 Mbit/s
- 弹性公网名称：NAT-IP

说明：其他配置保持默认即可。

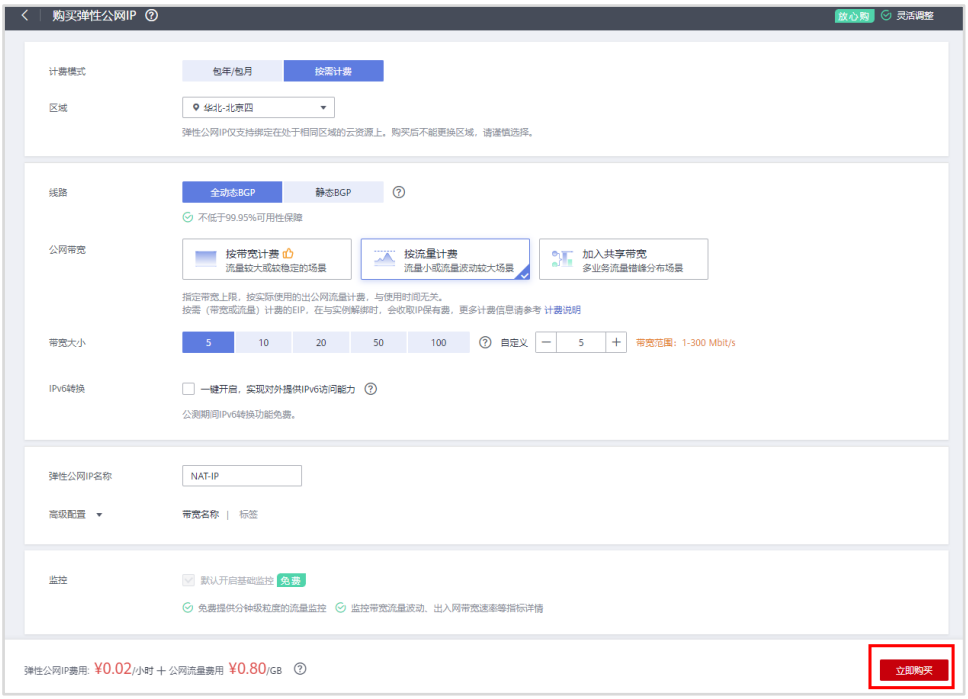


图2-49

步骤 2 “华北-北京四”中，选择“网络控制台>NAT 网关>公网 NAT 网关”，点击右上角“购买公网 NAT 网关”。

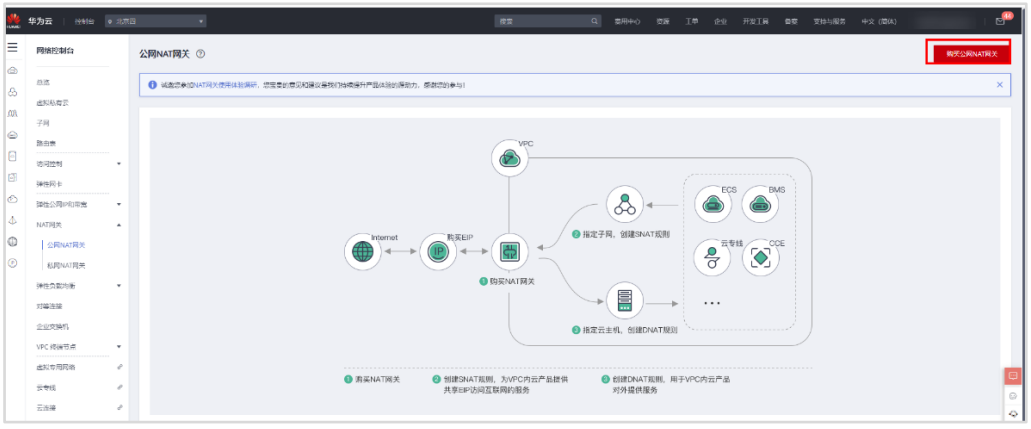


图2-50

步骤 3 按以下配置内容填写相关配置参数后购买。

- 计费模式：按需计费
- 区域：华北-北京四
- 名称：nat-vpc2
- 虚拟私有云：vpc-2
- 子网：vpc-2-subnet
- 规格：小型

图2-51

步骤 4 在弹出的提示框中选择“添加规则”。

图2-52

步骤 5 按照以下配置添加第一条 SNAT 规则，提供 VPC-2 内 192.168.2.0/24 网段主机访问公网服务。

- 使用场景：虚拟私有云
- 子网：使用已有|vpc-2-subnet
- 弹性公网 IP：121.36.79.241（选择刚创建的弹性公网 IP）

图2-53

步骤 6 按照以下配置添加第二条 SNAT 规则，提供 VPC-3 内 192.168.3.0/24 网段主机访问外网服务。

- 使用场景：云专线/云连接|192.168.3.0/24
- 弹性公网 IP：121.36.79.241（选择刚创建的弹性公网 IP）

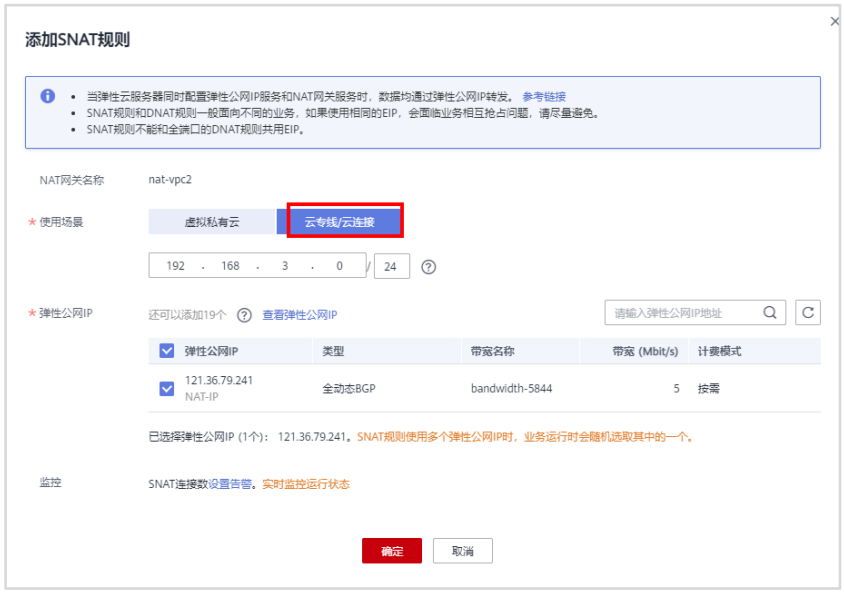


图2-54

步骤 7 查看当前 SNAT 规则列表，可以看到两条使用场景分别为“云专线/云连接”和“虚拟私有云”的 SNAT 规则。

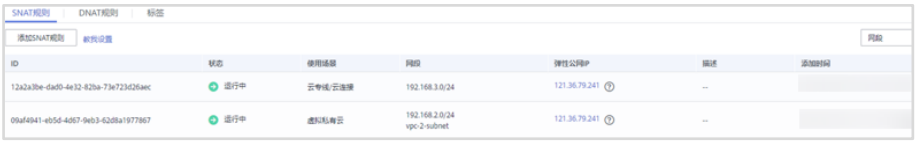


图2-55

步骤 8 在 VPC-3 路由表“rtb-vpc-3”中选择“添加路由”。

图2-56

步骤 9 按照以下配置添加默认路由，指向对等连接，完成配置后点击“确定”。

说明：该默认路由配置是为了引流 VPC3 中公网访问流量通过对等连接至 VPC2 中，通过 VPC2 再匹配 NAT 网关的 SNAT 规则，从而访问公网。

- 目的地址：0.0.0.0/0
- 下一跳类型：对等连接
- 下一跳：vpc2-vpc3

图2-57

2.3 实验验证

2.3.1 运维主机登录远端资源

步骤 1 在“华东-上海一”中登录 ECS01，分别 SSH 登录 ECS02 和 ECS03。

```
[root@ecs-01 ~]# ssh 192.168.2.180
[root@ecs-02 ~]# exit
[root@ecs-01 ~]# ssh 192.168.3.62
[root@ecs-03 ~]
```

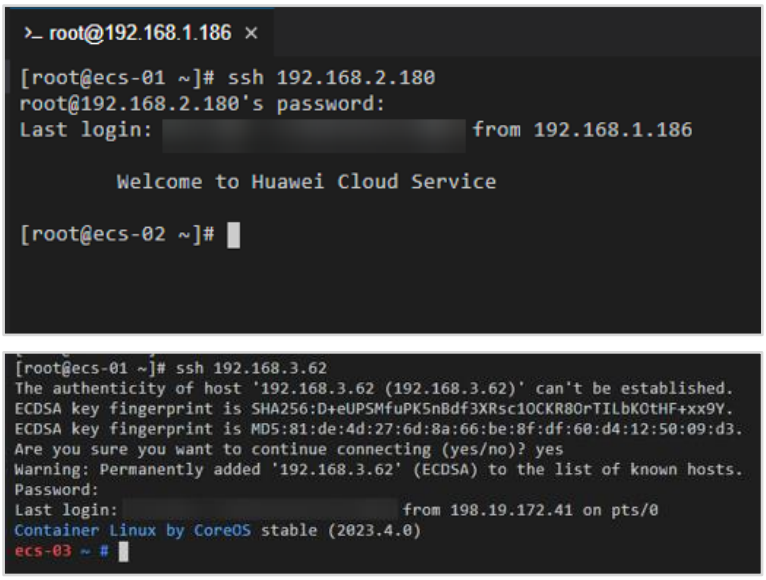


图2-58

如上结果证明，通过以上配置，ECS01 可以正常使用 SSH 登录 ECS02 和 ECS03，线下局点的运维主机（ECS01）可以对云上资源进行远程运维。

2.3.2 云上资源通过 NAT 网关访问公网

步骤 1 在“华北-北京四”中登录 ECS03，ping 测访问公网地址。

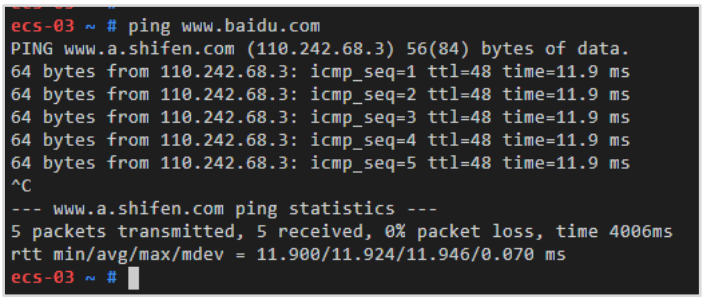


图2-59

步骤 2 在“华北-北京四”中登录 ECS02，ping 测访问公网地址。

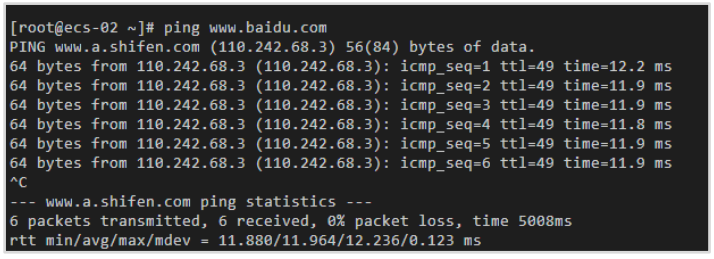


图2-60

如上结果证明，通过以上配置，云上 VPC2 和 VPC3 中的云主机均可以通过 VPC2 中的 NAT 网关进行公网访问。

2.4 实验恢复

步骤 1 删除 NAT 网关。

- 在服务列表中选择“NAT 网关 NAT”，在网关列表中找到本实验创建的 NAT 网关，在操作栏里选择“更多>删除”。

步骤 2 删除 VPN 网关。

- 在服务列表中选择“虚拟私有网络 VPN”，在页签中选择“VPN 连接”，在列表中找到本实验创建的 VPN 连接，点击操作栏中的“更多>删除”。
- 在页签中选择“VPN 网关”，在列表中找到本实验创建的 VPN 网关，点击操作栏中的“更多>删除”。

步骤 3 删除 ECS。

- 在服务列表中选择“云服务器 ECS”，找到创建的云服务器，点击操作栏中的“更多>删除”。
- 在弹出的对话框中勾选下图中选项，点击“是”。

图2-61

步骤 4 删除对等连接。

- 在服务列表中选择“虚拟私有云 VPC”，在页签中选择“对等连接”，在列表中找到本实验创建的对等连接，点击操作栏中的“删除”。

步骤 5 安全组。

- 在服务列表中选择“虚拟私有云 VPC”，在“访问控制>安全组”中找到本实验创建的安全组，点击操作栏的“更多>删除”。

步骤 6 删除 VPC。

- 在服务列表中选择“虚拟私有云 VPC”，点击“子网”页签，在列表中找到本实验创建的子网，点击操作栏中的“删除”。
- 点击“虚拟私有云”页签，找到本实验创建的 VPC，点击操作栏中的“删除”。

2.5 思考题

问题：VPN 连接配置中，“本端子网”和“远端子网”的配置分别是指什么?

参考答案：本端子网指需要通过 VPN 访问用户本地网络的 VPC 子网。远端子网指需要通过 VPN 访问 VPC 的用户本地子网。

3 存储架构设计实验

3.1 实验介绍

3.1.1 关于本实验

本实验将使用华为云搭建视频流媒体服务，通过配置弹性云服务器（Elastic Cloud Server，简称 ECS）、弹性云硬盘（Elastic Volume Service，简称 EVS）、弹性文件服务（Scalable File Service，简称 SFS）、对象存储服务（Object Storage Service，简称 OBS）搭建视频网站，通过弹性负载均衡 ELB 将请求分发到不同的可用区，实现视频网站的高可用部署。

说明：本实验以“北京一”区域为例，学员可以根据实际情况选择相应区域进行实验。

3.1.2 实验目的

掌握华为云存储服务的操作原理和配置方法。

理解数据云上管理、配置的业务场景。

3.1.3 实验组网

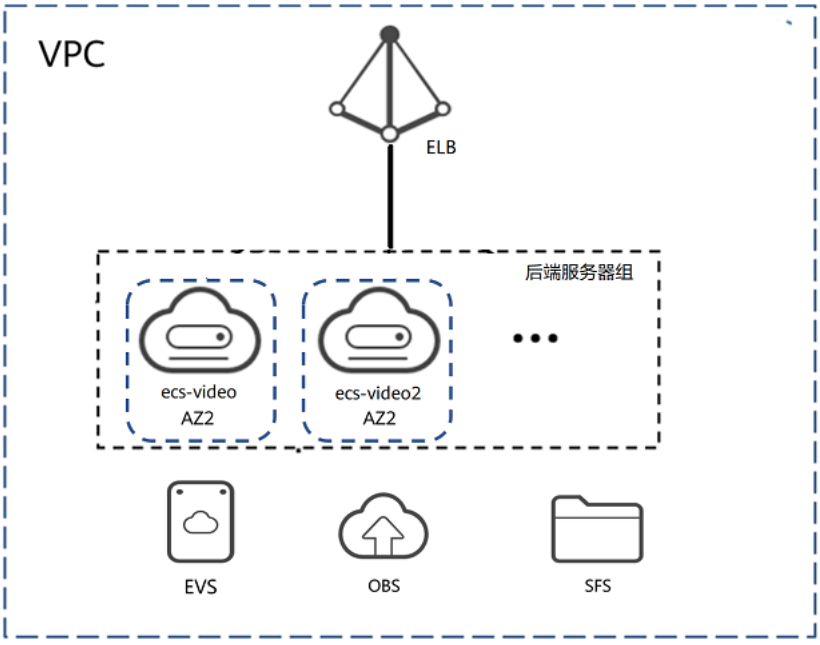


图3-1

3.1.4 软件介绍

Nginx 是一款轻量级的 Web 服务/反向代理服务及电子邮件（IMAP/POP3）代理服务，在 BSD-like 协议下发行。其特点是占有内存少，并发能力强。

3.2 实验配置

3.2.1 实验准备

步骤 1 下载 video 文件。

- 在本地电脑通过浏览器打开以下链接下载实验文件：https://cloudservice-v3.obs.cn-east-3.myhuaweicloud.com/video.zip
- 实验文件介绍：

huawei-cloud.jpg、index.html、nginx-1.15.9.tar.gz、SampleVideo_1280x720_5mb.mp4、video.js 等。

图3-2

3.2.2 创建 VPC

步骤 1 在“华北-北京一”中按以下配置创建 VPC（本实验的后续资源将在此 VPC 中创建）。

基本信息：

- 区域：华北-北京一
- 名称：vpc-video
- 网段：10.1.0.0/16

默认子网：

- 可用区 1（本 VPC 以可用区 1 为例，学员可根据实际情况选择相应可用区，后续类似资源不再赘述）
- 名称：subnet-video
- 子网网段：10.1.10.0/24

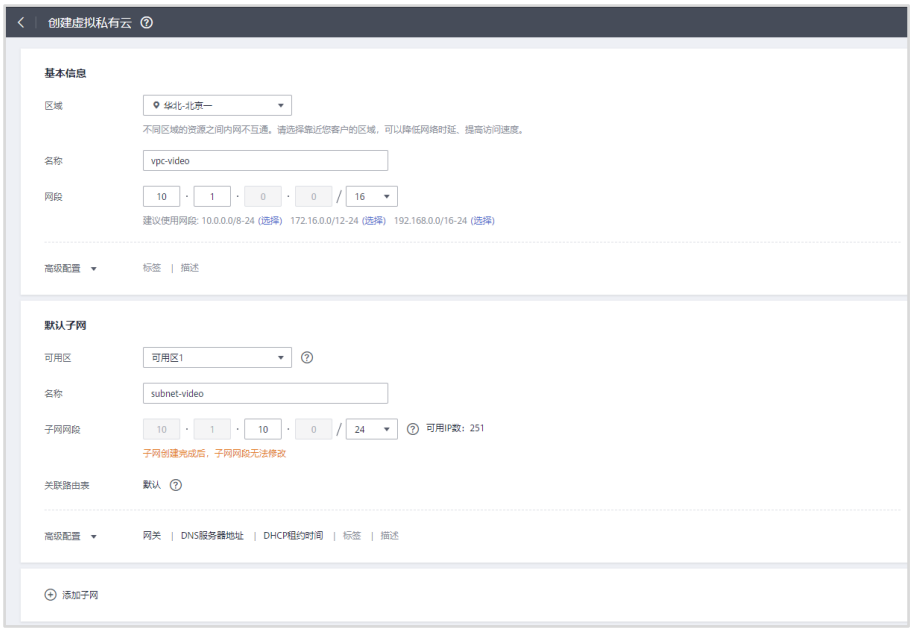


图3-3

3.2.3 创建安全组

步骤 1 在“华北-北京一”中按以下配置创建安全组（该安全组供本实验中视频流媒体服务器使用）。

- 名称：sg-video
- 模板：通用 Web 服务器

图3-4

步骤 2 查看此安全组规则，可以看到入方向规则中已经放通了 80 端口，方便后续 ECS 正常提供服务。

图3-5

3.2.4 创建 SFS 服务

步骤 1 在“华北-北京一”中选择“弹性文件服务>SFS Turbo”，点击右上角“创建文件系统”。

说明：后续实验中需要将该弹性文件服务挂载至 ECS。

图3-6

步骤 2 按照以下配置填写相应参数，确认配置后，选择“立即创建”。

- 计费模式：按需计费
- 区域：华北-北京一
- 可用区：可用区 1
- 存储类型：标准型
- 容量：500 GB
- 协议类型：NFS

图3-7

- 选择网络：vpc-video|subnet-video
- 安全组：sg-video
- 名称：sfs-video
- 其他配置：默认即可

图3-8

步骤 3 查看已创建的 SFS 服务，发现状态为“可用”。

图3-9

3.2.5 创建 OBS 服务

步骤 1 在“华北-北京一”中选择“对象存储服务-桶列表”，点击右上角“创建桶”。

说明：实验准备中下载的“video.zip”文件需要上传至对象桶中，供后续实验使用。

图3-10

步骤 2 按照以下配置填写配置参数后选择“立即创建”。

- 区域：华北-北京一
- 桶名称：video
- 默认存储类别：标准存储
- 桶策略：公共读
- 归档数据直读：关闭

图3-11

步骤 3 点击已创建的 OBS 桶名称进入桶管理界面。

图3-12

步骤 4 点击“上传对象”。

图3-13

步骤 5 选择“添加文件”，在本地目录中找到下载好的“video.zip”文件，点击“上传”。

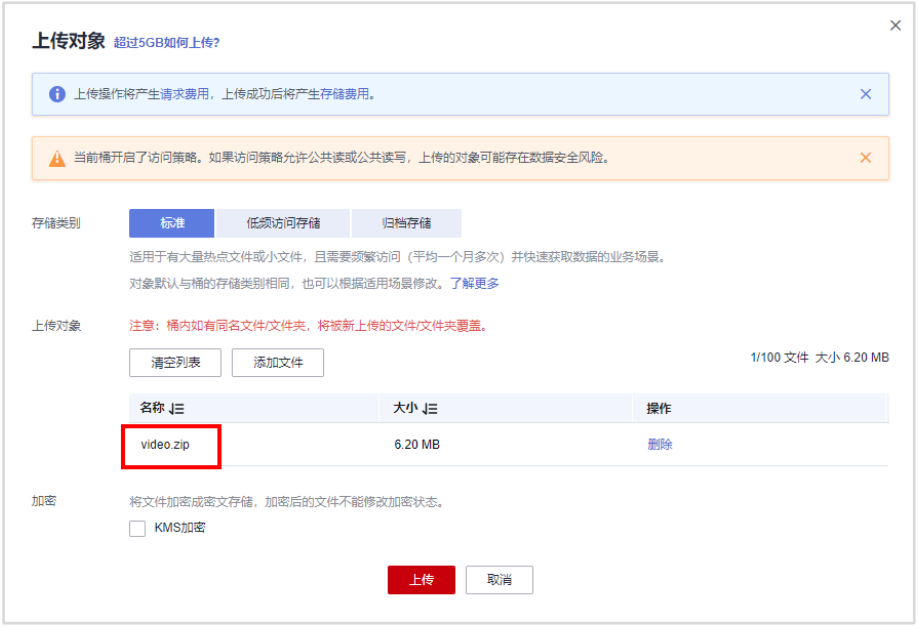


图3-14

步骤 6 在“概览>对象”的对象列表中查看已上传的文件。

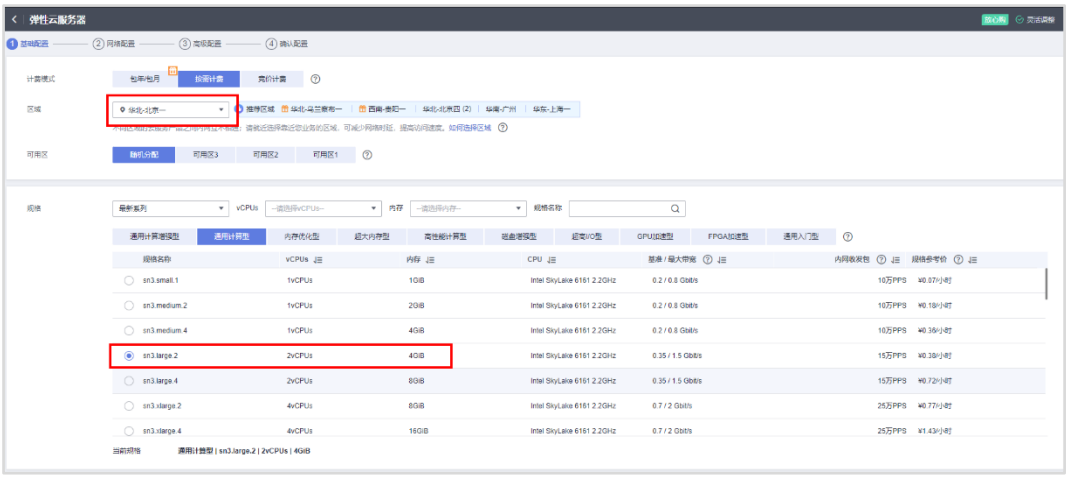
图3-15

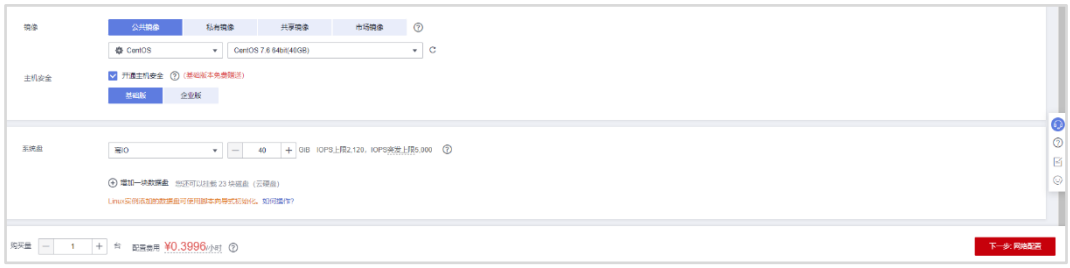
3.2.6 创建 ECS 服务

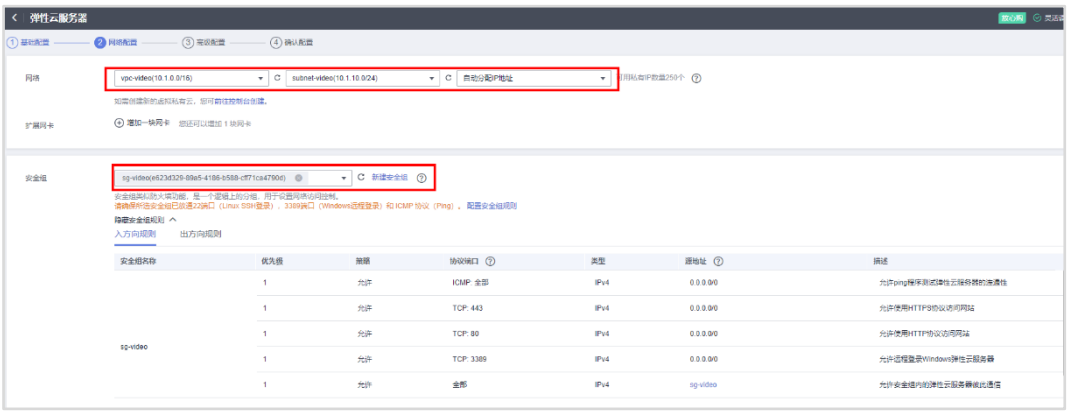
步骤 1 在“华北-北京一”中，按照以下配置选择相应配置参数。确认配置后选择“立即购买”。

说明：该 ECS 用来部署视频流媒体服务。

- 计费模式：按需计费
- 区域：华北-北京一
- 可用区：随机分配
- 规格：2 vCPU|4 GiB
- 镜像：公共镜像|CentOS 7.6 64 bit（40 GB）
- 主机安全：基础版
- 系统盘：高 IO|40 GB
- 网络：vpc-video | subnet-video | 自动分配 IP 地址
- 安全组：sg-video
- 弹性公网 IP：现在购买
- 线路：静态 BGP
- 公网带宽：按流量计费
- 带宽大小：10 Mbit/s
- 云服务器名称：ecs-video
- root 密码：自定义


弹性云服务器
计费模式
区域
华北-北京一
可用区
规格
vCPUs
内存
规格名称
sn3.small.1
sn3.medium.2
sn3.medium.4
sn3.large.2
sn3.large.4
sn3.xlarge.2
sn3.xlarge.4
当前规格


镜像
公共镜像
私有镜像
共享镜像
市场镜像
CentOS
CentOS 7.6 64bit(40GB)
主机安全
系统盘
购买量
¥0.3996/小时
下一步: 网络配置


弹性云服务器
网络
vpc-video(10.1.0.0/16)
subnet-video(10.1.10.0/24)
自动分配IP地址
扩展网卡
安全组
入方向规则
出方向规则
安全组名称
优先级
策略
协议端口
类型
源地址
描述
sg-video


弹性公网IP
现在购买
使用已有
暂不购买
线路
静态BGP
全动态BGP
不低于99%可用性保障
公网带宽
按带宽计费
流量较大或较稳定的场景
按流量计费
流量小或流量波动较大场景
加入共享带宽
多业务流量错峰分布场景
指定带宽上限，按实际使用的出公网流量计费，与使用时间无关。
带宽大小
5
10
20
50
100
自定义
带宽范围：1-300 Mbit/s
免费开启DDoS基础防护
购买量
台
配置费用 ¥0.3996/小时 + 弹性公网IP流量费用 ¥0.64/GB

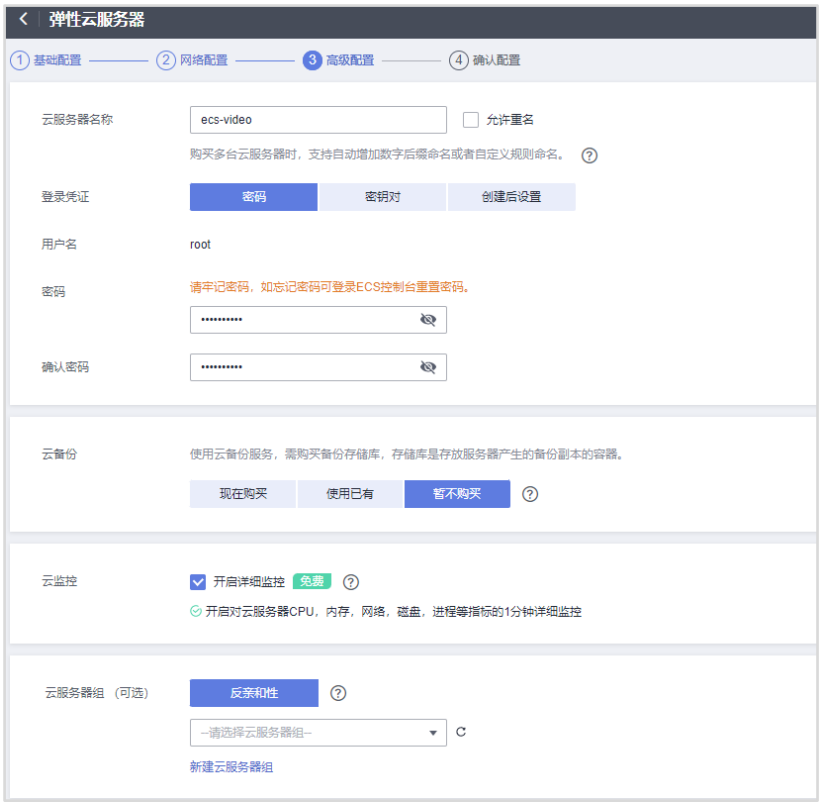


图3-16

3.2.7 挂载 SFS 服务

步骤 1 在弹性云服务器列表中，点击“远程登录”，使用 CloudShell 登录 ecs-video 云主机。

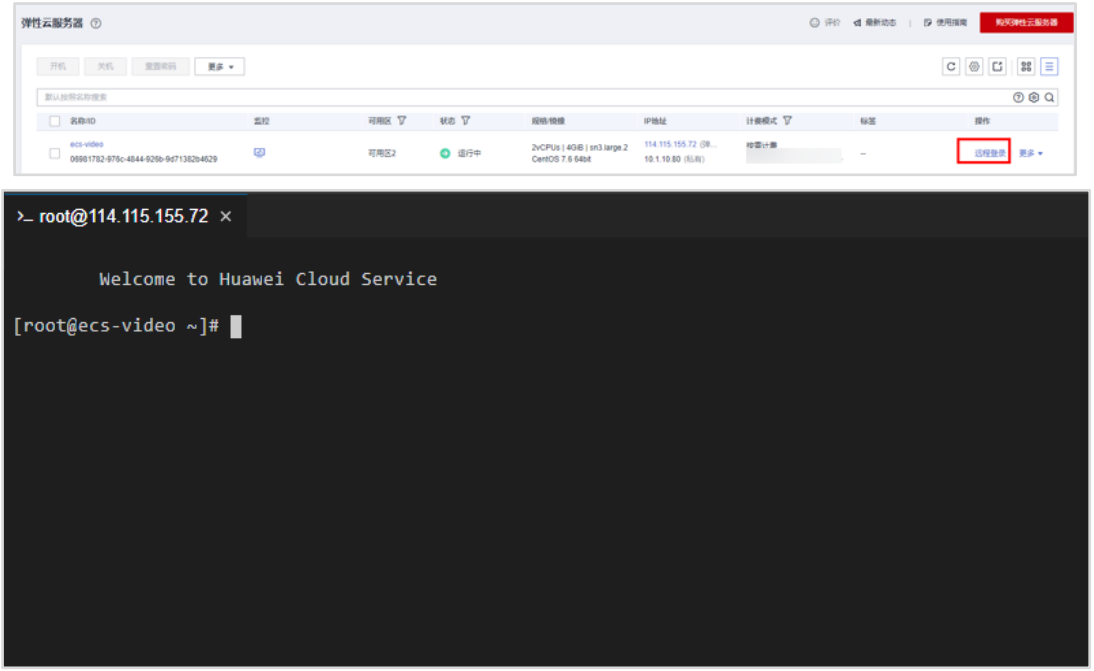


图3-17

步骤 2 使用如下命令创建 video 文件夹并安装 NFS 客户端。

```
[root@ecs-video ~]# mkdir /video
[root@ecs-video ~]# yum -y install nfs-utils
```

图3-18

- 看到如下“complete”证明安装完成。

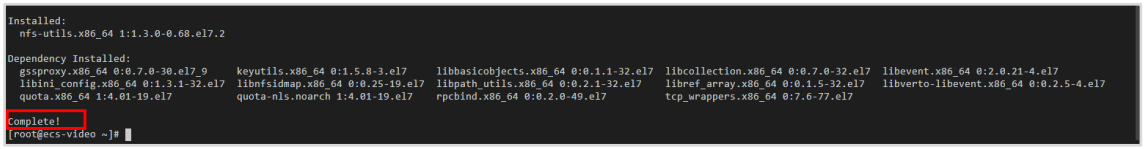


图3-19

步骤 3 返回华为云界面，选择“弹性文件服务-SFS Turbo”，点击已创建的 SFS 服务名称进入配置概览界面。

步骤 4 记录挂载命令。

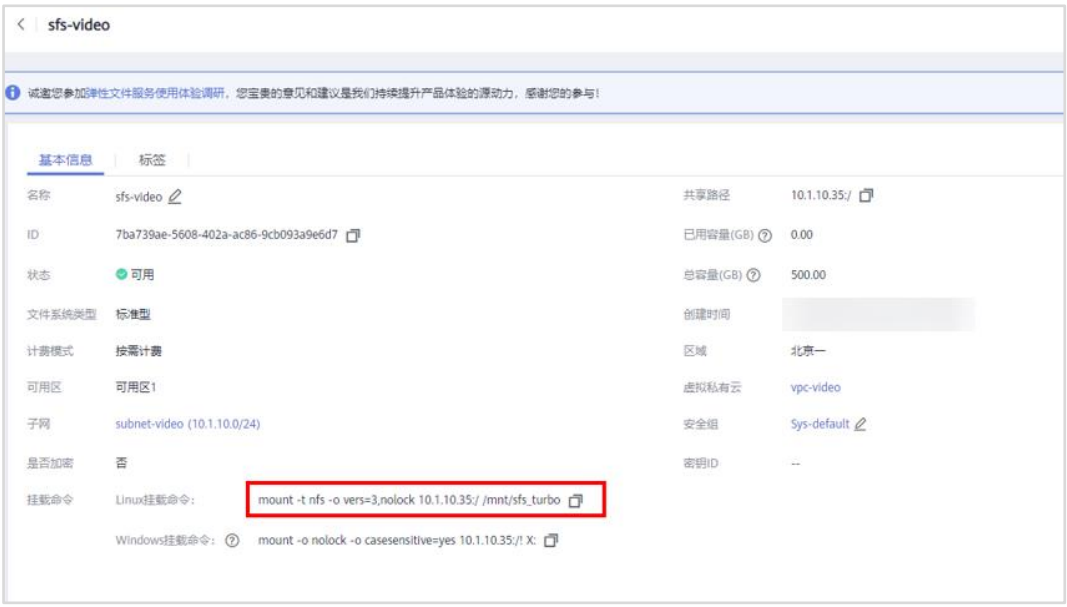


图3-20

步骤 5 登录 esc-video，使用如下命令挂载 SFS。

```
[root@ecs-video ~]# mount -t nfs -o vers=3,nolock 10.1.10.35:/ /video
```

说明：命令中“mount -t nfs -o vers=3,nolock 10.1.10.35:/”部分请学员使用上一步中记录的挂载命令替换。

```
Complete!
[root@ecs-video ~]# mount -t nfs -o vers=3,nolock 10.1.10.35:/ /video
[root@ecs-video ~]#
```

图3-21

步骤 6 使用如下命令验证挂载是否成功。如下图所示，即挂载成功。

```
[root@ecs-video ~]# mount|grep video
```

```
[root@ecs-video ~]# mount|grep video
10.1.10.35:/ on /video type nfs (rw,relatime,vers=3,rsize=1048576,wsize=1048576,namlen=255,hard,nolock,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=10.1.10.35,mountvers=3,mountport=20048,mountproto=tcp,local_lock=all,addr=10.1.10.35)
```

图3-22

步骤 7 使用如下命令配置永久挂载。

```
[root@ecs-video ~]#echo "10.1.10.35:/ /video nfs
vers=3,timeo=600,nolock,rsize=1048576,wsize=1048576,hard,retrans=2,noresvport,async,noatime,nodiratime 0 0" >>/etc/fstab
```

说明：命令中地址“10.1.10.35”请学员使用 SFS 服务实际地址替换。

```
[root@ecs-video ~]# echo  "10.1.10.35:/ /video nfs vers=3,timeo=600,nolock,rsize=1048576,wsize=1048576,hard,retrans=2,noresvport,async,noatime,nodiratime 0 0" >>/etc/fstab
[root@ecs-video ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=4fde6d8c-b0bb-4d16-a95f-c578b5f9c2a6 /                       ext4    defaults        1 1
10.1.10.35:/ /video nfs vers=3,timeo=600,nolock,rsize=1048576,wsize=1048576,hard,retrans=2,noresvport,async,noatime,nodiratime 0 0
```

图3-23

步骤 8 使用如下命令验证永久挂载是否成功。如下图所示，即永久挂载成功。

```
[root@ecs-video ~]# umount /video
[root@ecs-video ~]# mount -a
[root@ecs-video ~]# mount |grep video
```

```
[root@ecs-video ~]#
[root@ecs-video ~]# umount /video
[root@ecs-video ~]# mount -a
[root@ecs-video ~]# mount |grep video
10.1.10.35:/ on /video type nfs (rw,noatime,nodiratime,vers=3,rsize=1048576,wsize=1048576,namlen=255,hard,nolock,noresvport,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=10.1.10.35,mountvers=3,mountport=20048,mountproto=tcp,local_lock=all,addr=10.1.10.35)
```

图3-24

3.2.8 下载 OBS 对象文件

步骤 1 登录华为云，在“华北-北京一”中选择“对象存储服务>桶列表”，选择已创建的桶“video-jam”进入配置界面。

图3-25

步骤 2 选择对象列表中的“video.zip”。

图3-26

步骤 3 查看并记录链接地址。

图3-27

步骤 4 登录 esc-video 主机，使用如下命令下载对象文件。

```
[root@ecs-video ~]# cd /video
[root@ecs-video video]# wget https://video.obs.cn-north-1.myhuaweicloud.com/video.zip
```

说明：命令中“https://video.obs.cn-north-1.myhuaweicloud.com/video.zip”部分请学员使用上一步骤中记录的链接地址替换。

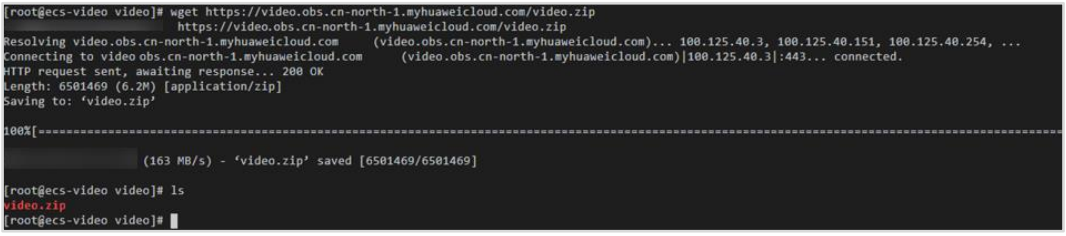


图3-28

3.2.9 挂载 EVS 服务

步骤 1 登录华为云，在“华北-北京一”中选择“云硬盘-磁盘”，点击右上方“购买磁盘”。

说明：该硬盘需要被挂载至云主机 ecs-video 中，后续实验需要将 Nginx 编译安装至该磁盘。

图3-29

步骤 2 按以下配置填写相应配置参数，确认配置后选择“立即购买”。

- 计费模式：按需计费
- 区域：华北-北京一
- 可用区：可用区 2
- 磁盘类型：超高 IO
- 磁盘大小：10 GB
- 云备份：暂不购买
- 磁盘名称：volume-video

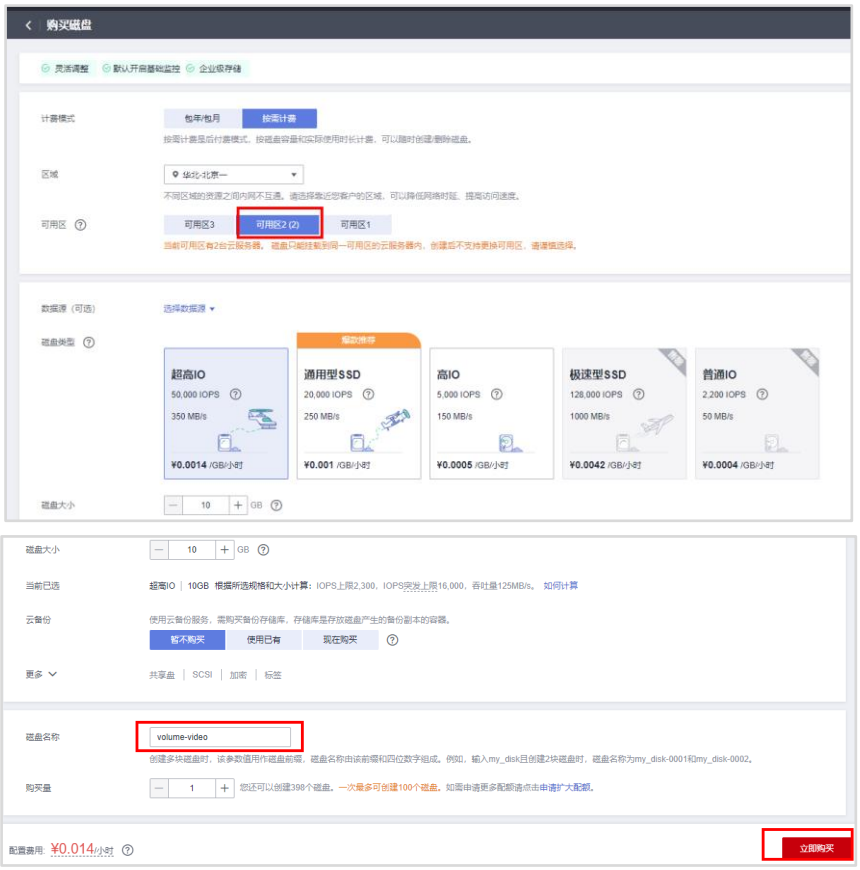


图3-30

步骤 3 在云硬盘列表查看已创建的 ecs-video 磁盘，点击“挂载”。

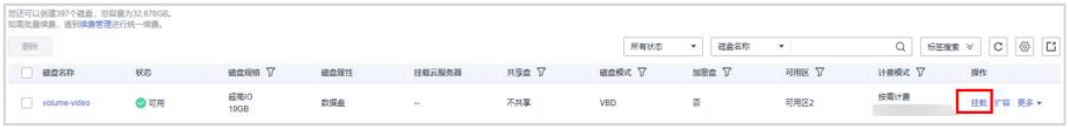


图3-31

步骤 4 在弹出的配置框中选择“弹性云服务器”，选择云主机 ecs-video，点击“确定”。

图3-32

步骤 5 登录 ecs-video，使用如下命令查看磁盘信息：

```
[root@ecs-video video]# fdisk  -l
```

```
[root@ecs-video video]# fdisk -l

Disk /dev/vda: 42.9 GB, 42949672960 bytes, 83886080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000aa138

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1   *        2048    83886079    41942016   83  Linux

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

[root@ecs-video video]#
```

图3-33

步骤 6 使用如下命令为该磁盘创建文件系统。请根据实际情况输入新磁盘的路径。

```
[root@ecs-video video]# mkfs -t ext4 /dev/vdb
```

```
[root@ecs-video video]# mkfs -t ext4 /dev/vdb
mke2fs 1.42.9 (
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
655360 inodes, 2621440 blocks
131072 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

[root@ecs-video video]#
```

图3-34

步骤 7 使用如下命令将该磁盘挂载至/opt 目录并查看是否挂载成功。

```
[root@ecs-video /]# mount /dev/vdb /opt
[root@ecs-video /]# mount |grep opt
```

```
[root@ecs-video /]# mount /dev/vdb /opt
[root@ecs-video /]# mount |grep opt
/dev/vdb on /opt type ext4 (rw,relatime,data=ordered)
[root@ecs-video /]#
```

图3-35

步骤 8 使用如下命令配置自动挂载。

```
[root@ecs-video /]# echo -e "/dev/vdb/\t/opt\text4\tdefaults\t1 1" >>/etc/fstab
```

```
[root@ecs-video /]# echo -e "/dev/vdb/\t/opt\text4\tdefaults\t1 1" >>/etc/fstab
[root@ecs-video /]#
[root@ecs-video /]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=4fde6d8c-b0bb-4d16-a95f-c578b5f9c2a6 /                       ext4    defaults        1 1
10.1.10.35:/ /video nfs vers=3,timeo=600,nolock,rsize=1048576,wsize=1048576,hard,retrans=2,noresvport,async,noatime,nodiratime 0 0
/dev/vdb/       /opt    ext4    defaults        1 1
[root@ecs-video /]#
```

图3-36

步骤 9 使用如下命令验证自动挂载是否配置成功。

```
[root@ecs-video ~]# umount /opt
[root@ecs-video ~]# mount -a
[root@ecs-video ~]# mount |grep opt
```

```
[root@ecs-video /]# umount /opt
[root@ecs-video /]# mount -a
[root@ecs-video /]# mount |grep opt
/dev/vdb on /opt type ext4 (rw,relatime,data=ordered)
[root@ecs-video /]#
```

图3-37

3.2.10 编译安装 Nginx

步骤 1 登录 ecs-video 云主机，使用如下命令编译安装 Nginx 至刚挂载的磁盘中。

```
cd /video
yum install -y unzip
unzip -o video.zip
cd video
cp nginx-1.15.9.tar.gz /opt/
cd /opt
yum install -y pcre*
yum install -y zlib*
tar -xvf   nginx-1.15.9.tar.gz
cd nginx-1.15.9
./configure --prefix=/opt/nginx
make && make install
```

步骤 2 使用如下命令编辑 nginx.conf 文件。

```
[root@ecs-video nginx-1.15.9]# cd /opt/nginx/conf
[root@ecs-video conf]# sed -i "0,/root    html/s/root    html/root    \/video\/video/" nginx.conf
```

```
[root@ecs-video nginx-1.15.9]# cd /opt/nginx/conf
[root@ecs-video conf]# sed -i "0,/root    html/s/root    html/root    \/video\/video/" nginx.conf
[root@ecs-video conf]#
```

图3-38

步骤 3 使用如下命令启动 Nginx。

```
[root@ecs-video conf]# cd /opt/nginx/sbin/
[root@ecs-video sbin]# ./nginx
```

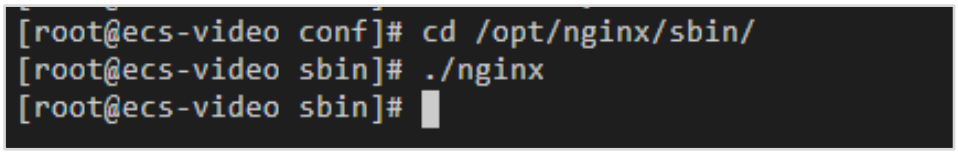


图3-39

步骤 4 使用如下命令设置开机自启。

```
[root@ecs-video sbin]# echo -e "\n#start nginx\nsleep 10\ncd /opt/nginx/sbin\n./nginx" >> /etc/rc.local
[root@ecs-video sbin]# chmod +x /etc/rc.d/rc.local
```

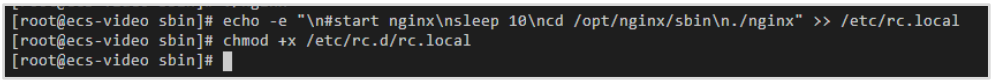


图3-40

步骤 5 使用本地 PC 浏览器登录 ecs-video 公网 IP 地址，验证视频播放。如下图所示，视频可以正常播放，证明通过以上配置，视频流媒体服务已完成搭建。

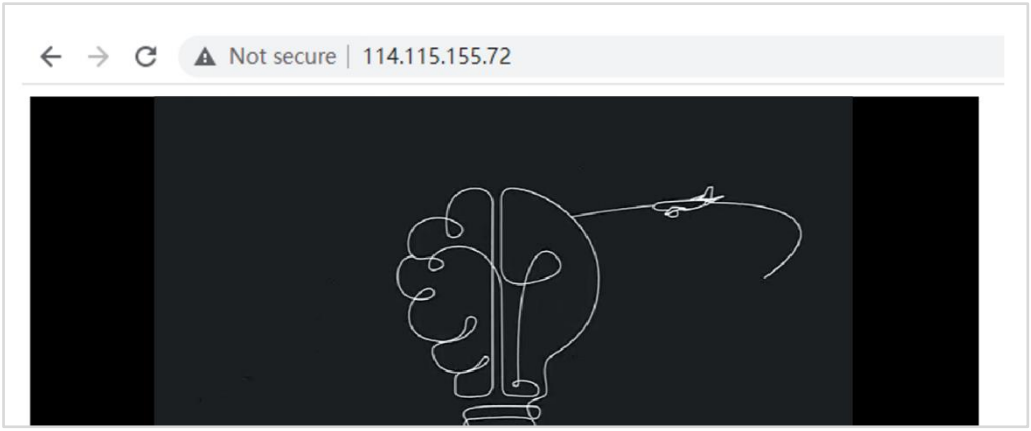


图3-41

3.2.11 高可用配置

步骤 1 登录华为云，在“华北-北京一”中选择“存储-云服务器备份”，点击右上角“购买云服务器备份存储库”。按照以下配置选择相应参数，点击“立即购买”。

说明：因后续实验中需要制作整机镜像，这里需要提前购买云服务器备份存储库。

- 计费模式：按需计费
- 区域：北京一
- 保护类型：备份
- 选择服务器：暂不配置
- 存储库容量：100 GB

- 其他配置：默认配置即可

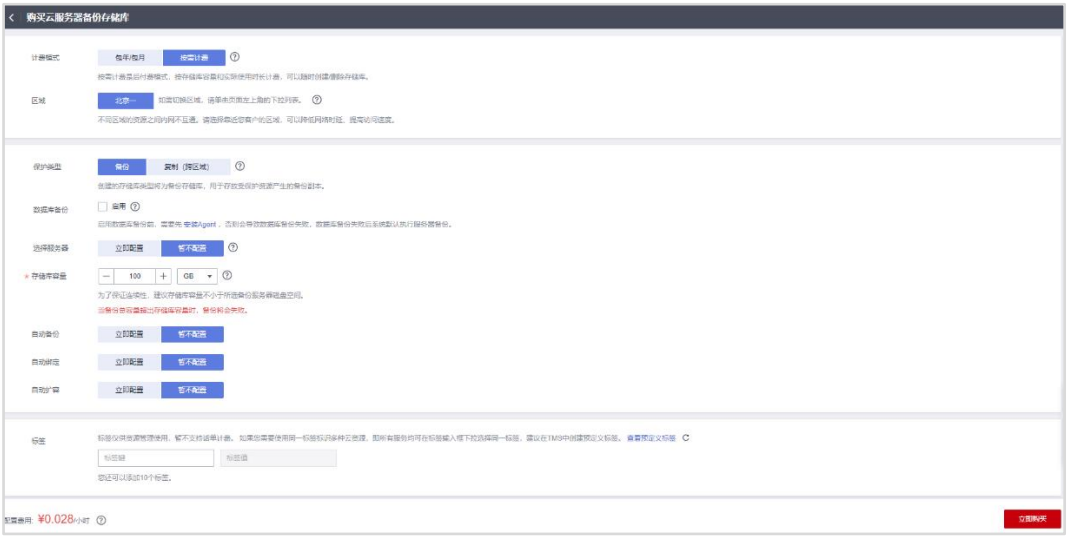


图3-42

步骤 2 查看已创建的云服务器备份存储库。

图3-43

步骤 3 在“华北-北京一”中选择“镜像服务”，点击右上角“创建私有镜像”。

说明：需要使用该私有镜像发放虚拟机，与原 ecs-video 云主机构成弹性负载均衡器的后端服务器组。

图3-44

步骤 4 按照以下配置选择相应配置参数，确认后选择“立即创建”。

- 区域：华北-北京一
- 创建方式：整机镜像

- 选择镜像源：云服务器|ecs-video
- 云服务器备份存储库：vault-video
- 名称：ecs-video

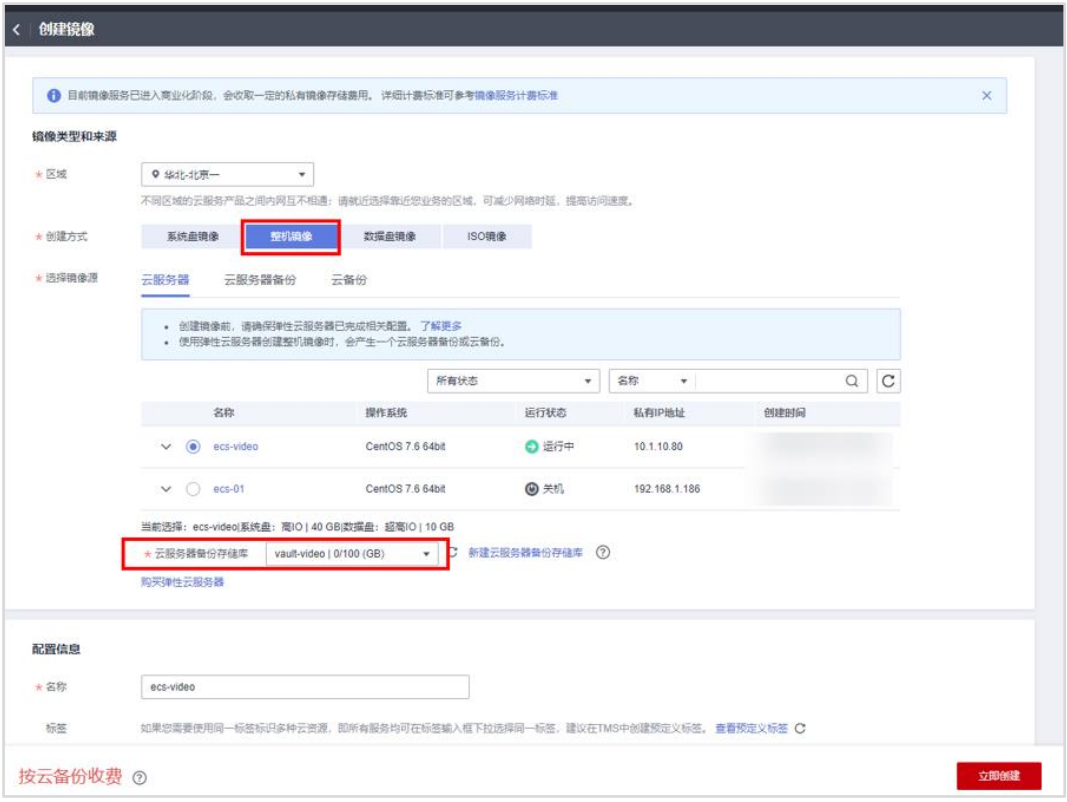


图3-45

步骤 5 点击“申请服务器”，使用该镜像在可用区 1 创建云主机 ecs-video2。（云主机 ecs-video 分配在了可用区 2）

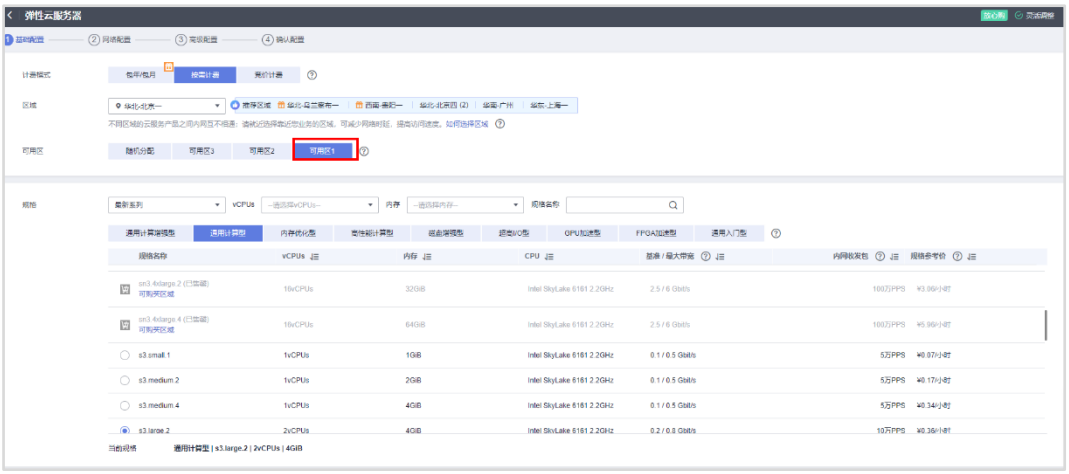
说明：为了保证高可靠性，“ecs-video”和“ecs-video2”云主机规划部署在不同可用区，学员可根据实际情况调整可用区选择。

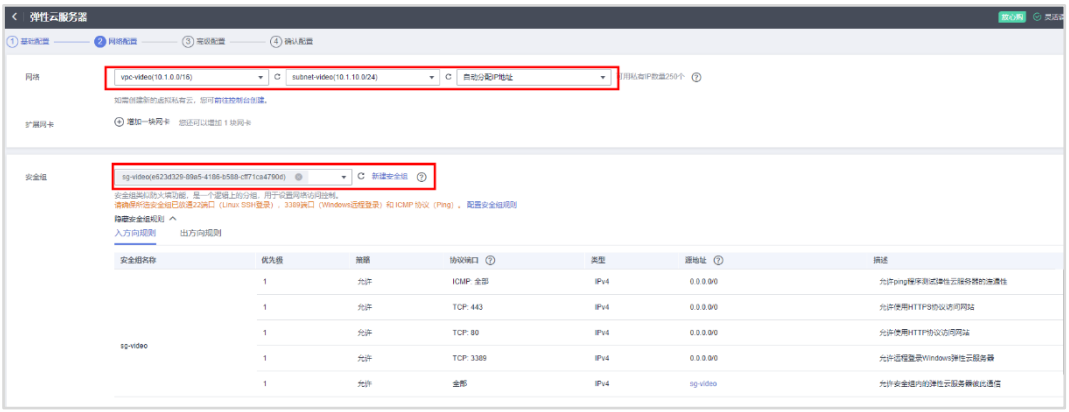
图3-46

步骤 6 按照以下配置填入相应配置参数。

- 计费模式：按需计费
- 区域：华北-北京一
- 可用区：可用区 1

- 规格：2 vCPU|4 GiB
- 镜像：私有镜像|ecs-video
- 系统盘：高 IO|40 GB
- 数据盘：超高 IO|10 GB
- 网络：vpc-video|subnet-video
- 安全组：sg-video
- 弹性公网 IP：暂不购买
- 云服务器名称：ecs-video2
- root 密码：自定义





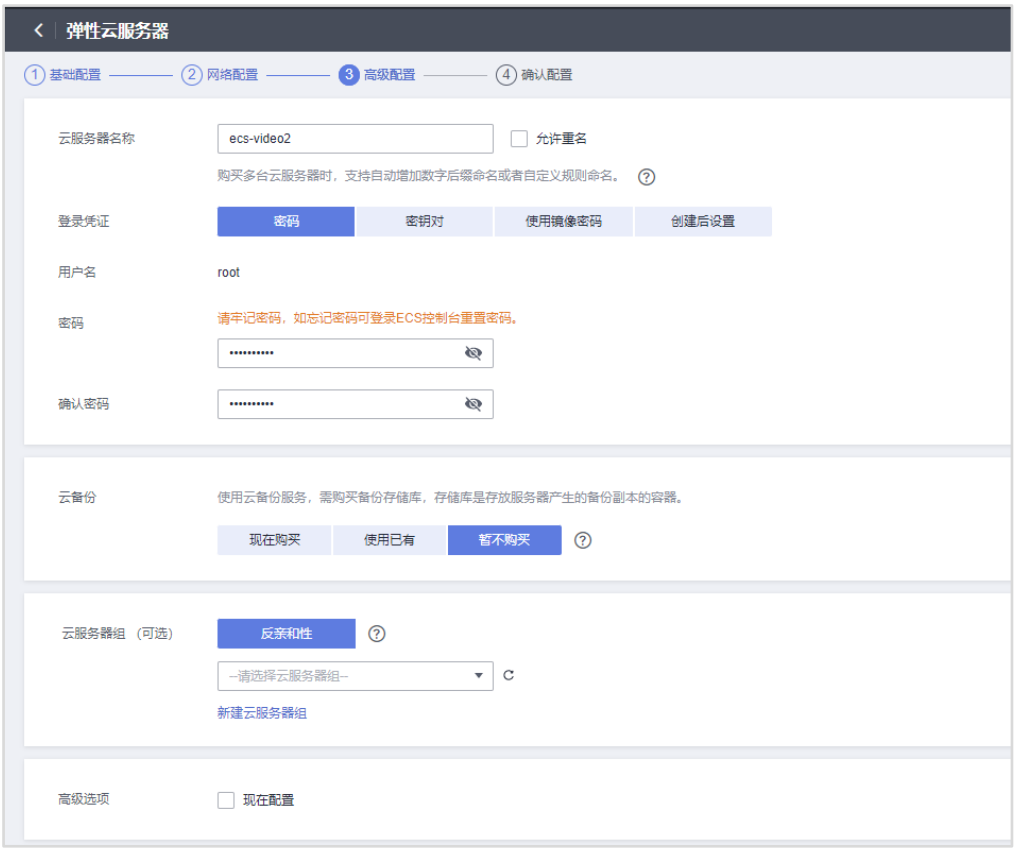


图3-47

步骤 7 在弹性云服务器列表中找到已创建好的云主机 esc-video2，点击操作栏的“远程登录”，通过 CloudShell 登录云主机。

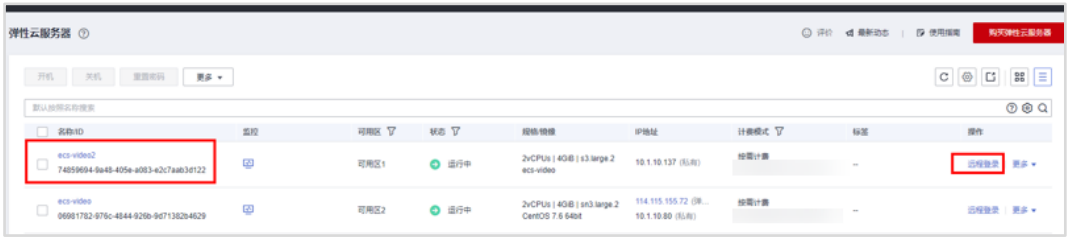


图3-48

步骤 8 通过如下命令确认服务状态。如下图所示，则证明 Nginx 服务正常开启。

```
[root@ecs-video2 ~]# netstat -ntpule
```

```
Last login:                    from 121.36.59.153

       Welcome to Huawei Cloud Service

[root@ecs-video2 ~]# netstat -ntpule
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      0          13315      532/rpcbind
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      0          15709      951/nginx: master p
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          17588      1207/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      0          15539      751/master
tcp6       0      0 :::111                  :::*                    LISTEN      0          13318      532/rpcbind
tcp6       0      0 :::22                   :::*                    LISTEN      0          17588      1207/sshd
tcp6       0      0 ::1:25                  :::*                    LISTEN      0          15540      751/master
udp        0      0 0.0.0.0:68              0.0.0.0:*                           0          15427      694/dhclient
udp        0      0 0.0.0.0:111             0.0.0.0:*                           0          13313      532/rpcbind
udp        0      0 127.0.0.1:323           0.0.0.0:*                           0          13336      544/chronyd
udp        0      0 0.0.0.0:696             0.0.0.0:*                           0          13314      532/rpcbind
udp6       0      0 :::111                  :::*                                0          13316      532/rpcbind
udp6       0      0 ::1:323                 :::*                                0          13337      544/chronyd
udp6       0      0 :::696                  :::*                                0          13317      532/rpcbind
[root@ecs-video2 ~]#
```

图3-49

步骤 9 在服务列表中选择“弹性公网 IP EIP”，在 IP 地址列表中找到已绑定实例为“ecs-video”的 EIP，点击操作栏中的“解绑”，解绑云主机 ecs-video 上的 EIP。

说明：后续需要将该 EIP 绑定至弹性负载均衡器中。

图3-50

步骤 10 在“华北-北京一”中选择“弹性负载均衡”，点击右上角“购买弹性负载均衡”。

图3-51

步骤 11 按照以下配置选择相应配置参数并购买。

- 实例规格类型：共享型
- 区域：华北-北京一
- 网络类型：公网
- 所属 VPC：vpc-video
- 子网：subnet-video
- 私有 IP 地址：自动分配 IP 地址

- 弹性公网 IP：使用已拥有|114.115.155.72（选择步骤 9 中从 ECS 中解绑的 EIP）
- 名称：elb-video

图3-52

步骤 12 查看已购买的负载均衡器，点击“点我开始配置”。

图3-53

步骤 13 按照以下配置内容创建监听器。

- 名称：listener-video（学员可自定义）
- 前端协议：TCP
- 前端端口：80（即负载均衡器提供服务时接收请求的端口）
- 其他配置：默认配置即可

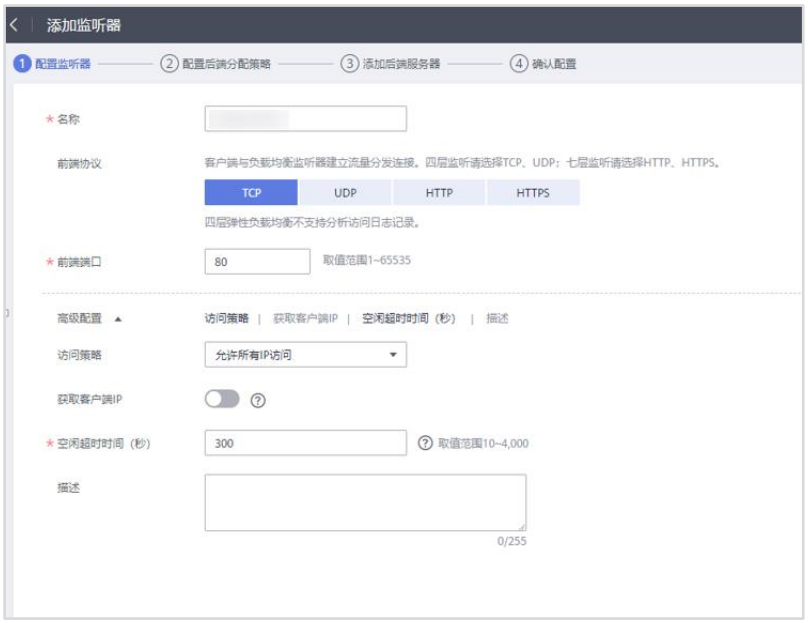


图3-54

步骤 14 按照以下内容配置后端分配策略。

- 名称：server-group-video（学员可自定义）
- 后端协议：TCP
- 分配策略类型：加权轮询算法
- 其他配置：默认配置即可

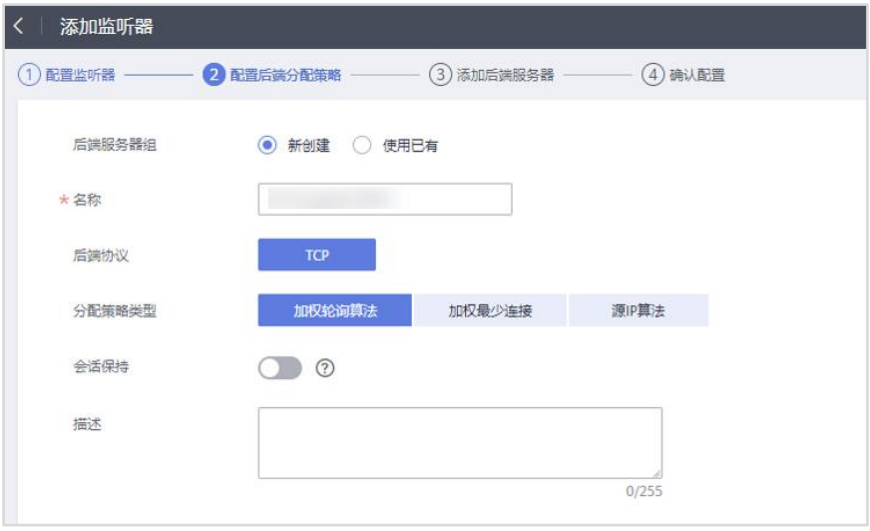


图3-55

步骤 15 点击“添加云服务器”后，在弹出的配置框中选择两台已创建好的 video 云主机，点击“完成”。

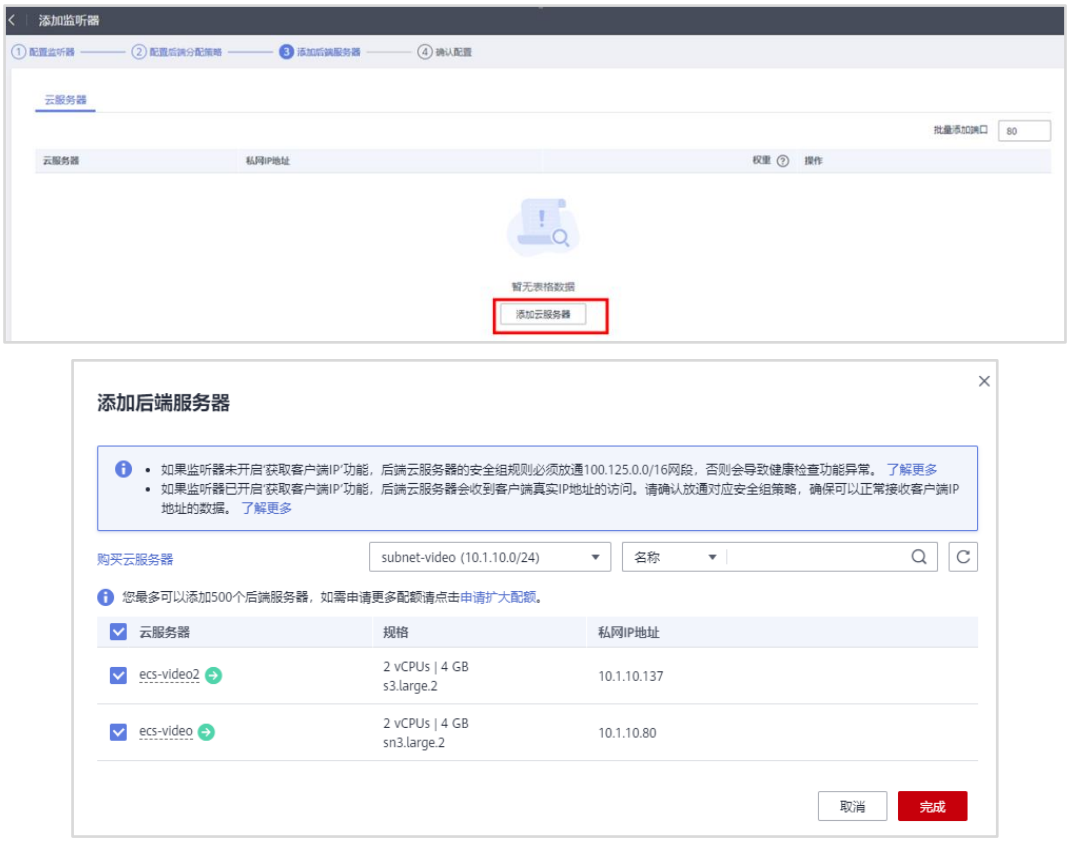


图3-56

步骤 16 在“批量配置端口”处填写“80”（该端口是指后端云服务器自身提供的网络服务的协议端口）。

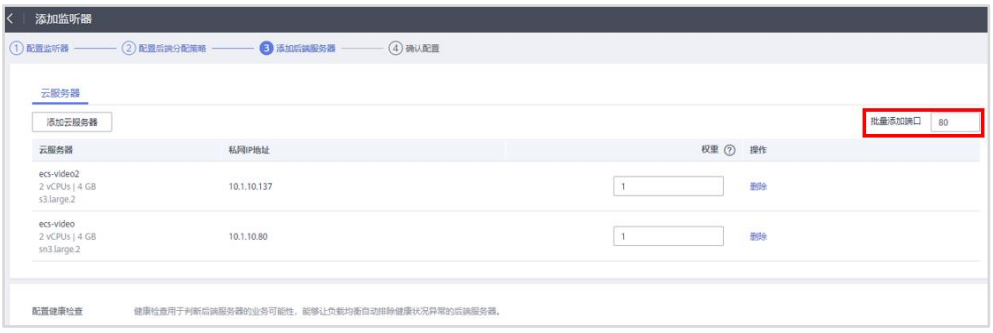


图3-57

步骤 17 确认配置后点击“提交”。

图3-58

步骤 18 查看已创建的负载均衡器，记录其弹性公网 IP 地址供后续登录使用。

图3-59

3.3 实验验证

步骤 1 使用本地 PC 浏览器登录上一步骤中记录的 elb-video 的 EIP 地址，验证视频播放。如下图所示，证明通过以上配置流媒体服务完成搭建且 ELB 服务正常运行，本实验成功完成。

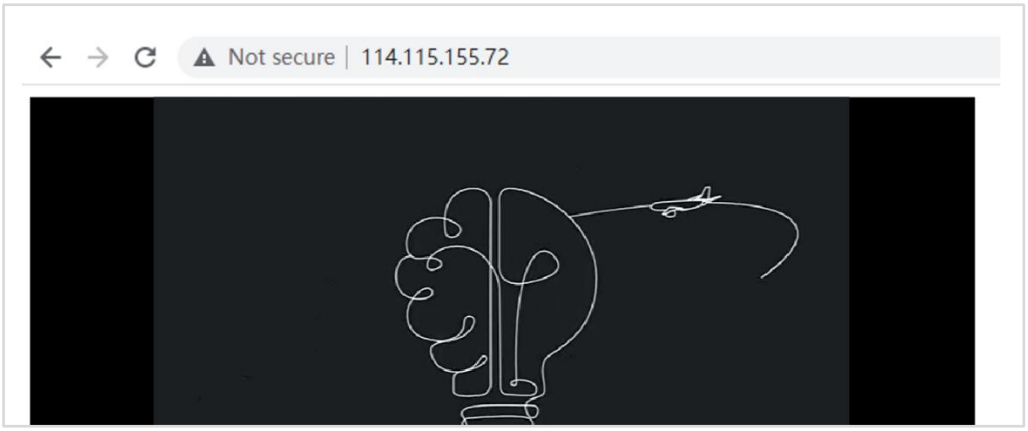


图3-60

3.4 实验恢复

步骤 1 删除弹性负载均衡。

- 在服务列表中选择“弹性负载均衡 ELB”。在负载均衡器列表中点击创建的负载均衡器名称并选择“后端服务器组”页签。勾选所有后端服务器，点击“移除”。

图3-61

- 选择“监听器页签”，点击页面中的删除按钮删除监听器。

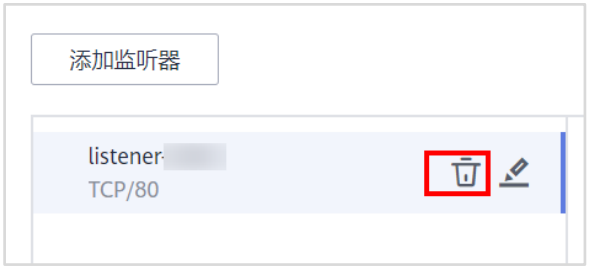


图3-62

- 返回负载均衡器列表，点击操作栏的“删除”按钮删除负载均衡器。
- 在弹出的对话框中勾选“释放该负载均衡绑定的弹性公网 IP”。

图3-63

步骤 2 删除 ECS。

- 在服务列表中选择“云服务器 ECS”，找到创建的云服务器，点击操作栏中的“更多>删除”。
- 在弹出的对话框中勾选下图中选项，点击“是”。

图3-64

步骤 3 删除 SFS。

- 在服务列表中选择“弹性文件服务 SFS”，找到本实验创建的文件系统，点击操作栏中的“更多>删除”。

步骤 4 删除 OBS。

- 在服务列表中选择“对象存储服务 OBS”，在桶列表中找到本实验创建的桶，点击操作栏中的“删除”。

步骤 5 删除安全组。

- 在服务列表中选择“虚拟私有云 VPC”，在“访问控制>安全组”中找到本实验创建的安全组，点击操作栏的“更多>删除”。

步骤 6 删除 VPC。

- 在服务列表中选择“虚拟私有云 VPC”，点击“子网”页签，在列表中找到本实验创建的子网，点击操作栏中的“删除”。
- 点击“虚拟私有云”页签，找到本实验创建的 VPC，点击操作栏中的“删除”。

3.5 思考题

问题：本实验在进行高可用配置时，使用了整机镜像来进行云服务器发放。该配置中为什么没有选择使用系统盘镜像来执行云服务器发放操作?

参考答案：本实验中云主机 ecs-video 挂载了云硬盘，需要选择整机镜像，将云服务器及其上挂载的数据盘一起创建镜像，此镜像包含操作系统、应用软件，以及用户的业务数据。

4 数据库架构设计实验

4.1 实验介绍

4.1.1 关于本实验

本实验将使用华为云搭建 WordPress 网站，通过配置弹性云服务器 ECS、云数据库 GaussDB（for Mysql）搭建 WordPress 网站，通过部署 GaussDB（for Redis）实例对接 WordPress 提供 Redis 服务，实现 WordPress 网站的页面加速。

说明：本实验以“北京四”区域为例，学员可以根据实际情况选择相应区域进行实验。

4.1.2 实验目的

理解云数据库服务架构中各云服务的使用。

掌握对云数据库服务可用性、统一管理等方面的设计方法。

4.1.3 实验组网

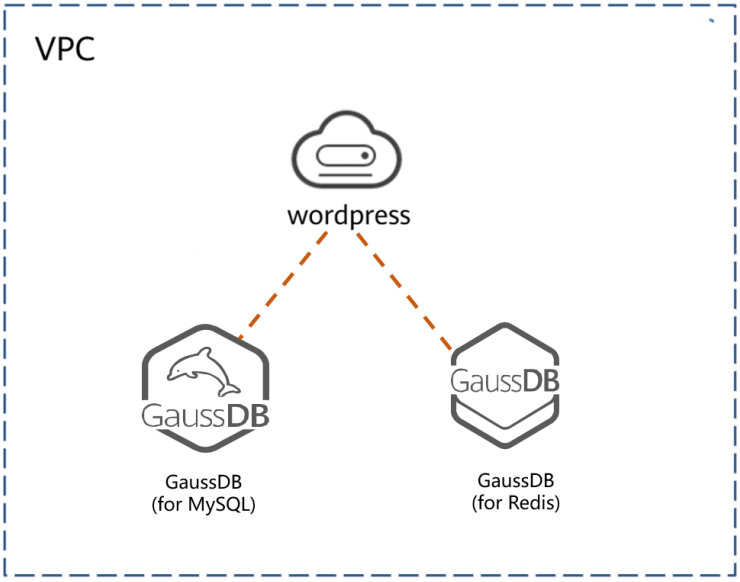


图4-1

4.1.4 软件介绍

Redis（Remote Dictionary Server），即远程字典服务，是一个开源的使用 ANSI C 语言编写、支持网络、可基于内存亦可持久化的日志型、Key-Value 数据库，并提供多种语言的 API，是一个高性能的 key-value 数据库。

4.2 实验配置

4.2.1 创建安全组

步骤 1 登录华为云，在“华北-北京四”中选择“网络控制台-访问控制-安全组”，点击右上角“创建安全组”，按照以下配置创建安全组 sg-rds。

说明：该安全组供后续 GaussDB 数据库实例使用，需要放通 3306 端口。

- 名称：sg-rds
- 模板：自定义

图4-2

步骤 2 按照以下配置添加一条入方向规则，放通 3306 端口。

- 优先级：1
- 策略：允许
- 协议端口：TCP|3306
- 类型：IPv4
- 源地址：IP 地址|0.0.0.0/0

图4-3

步骤 3 按照以下配置创建安全组 sg-wordpress。

说明：该安全组用于后续搭建 WordPress 的云服务器，需要使用通用 Web 服务器模板。

- 名称：sg-wordpress
- 模板：通用 Web 服务器

图4-4

步骤 4 按照以下配置创建安全组 sg-redis。

说明：此安全组放通 8635 端口是为了后续的 GaussDB（for Redis）服务。

- 名称：sg-redis
- 模板：自定义

图4-5

- 优先级：1
- 策略：允许
- 协议端口：TCP|8635
- 类型：IPv4
- 源地址：IP 地址|0.0.0.0/0

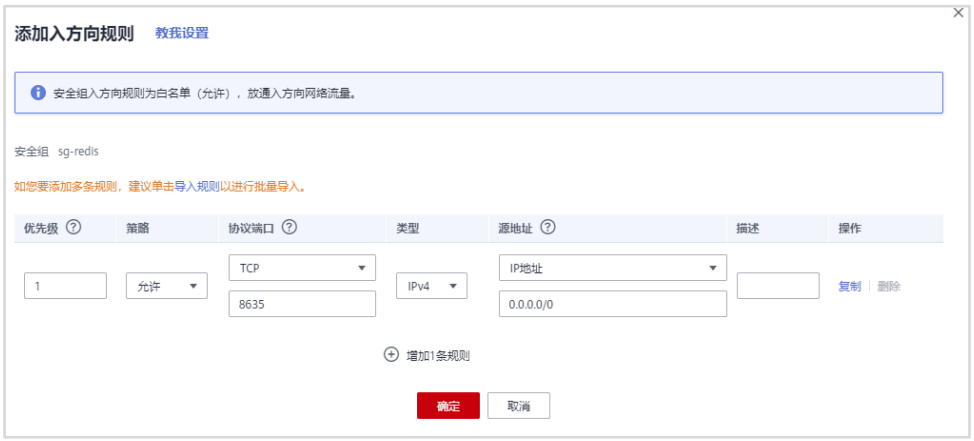


图4-6

4.2.2 创建 VPC

步骤 1 在服务列表中选择“虚拟私有云 VPC”，点击右上角“创建虚拟私有云”。

说明：本实验的后续资源将在此 VPC 中创建。

图4-7

步骤 2 按照以下配置创建虚拟私有云“vpc-2”。

基本信息：

- 区域：华北-北京四
- 名称：vpc-2
- IPv4 网段：192.168.0.0/16

默认子网：

- 可用区：可用区 1（本 VPC 以可用区 1 为例，学员可根据实际情况选择相应可用区，后续类似资源不再赘述）
- 名称：vpc-2-subnet
- 子网 IPv4 网段：192.168.2.0/24

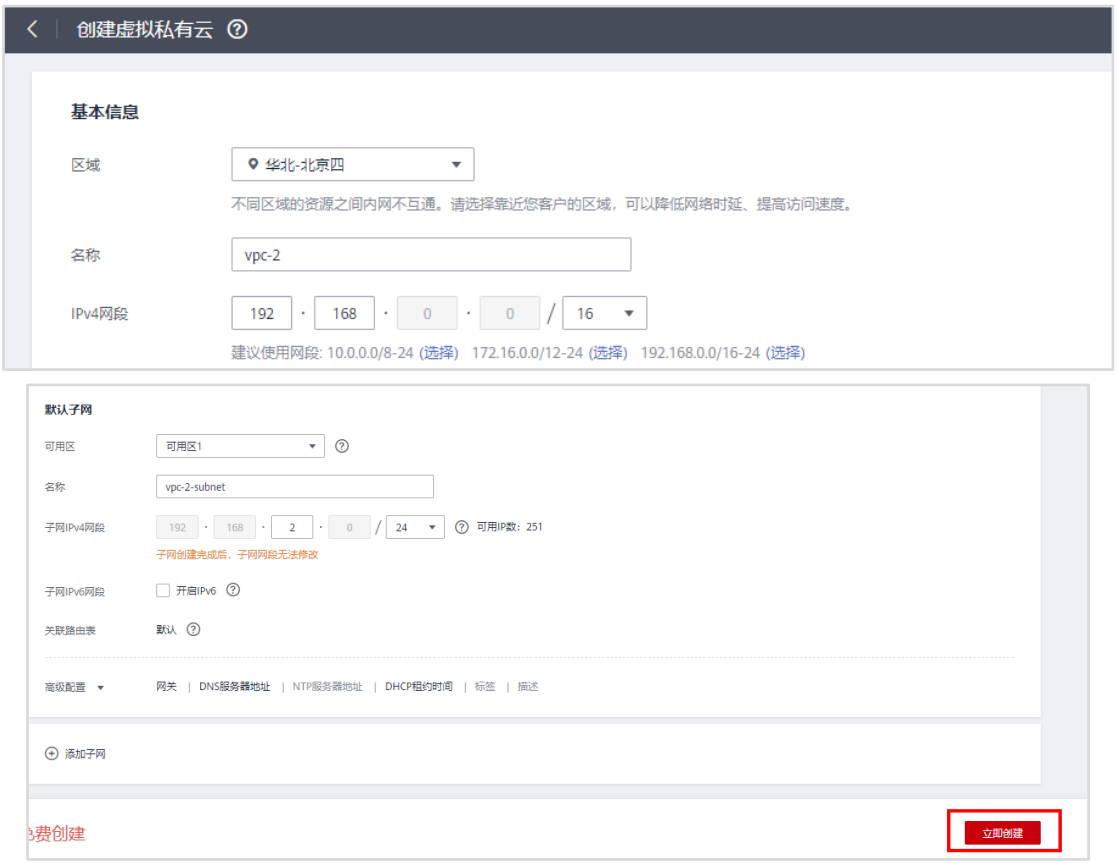


图4-8

4.2.3 购买云数据库实例

步骤 1 在“华北-北京四”服务列表，选择“云数据库 GaussDB”。

图4-9

步骤 2 点击右上角“购买数据库实例”。

说明：后续需要在该实例中创建数据库，对接 WordPress。

步骤 3 按照以下要求填写参数，并点击“立即购买”。

- 计费模式：按需计费
- 区域：华北-北京四
- 实例名称：rds-wordpress
- 数据库引擎：GaussDB（for MySQL）
- 兼容数据库版本：MySQL 8.0
- 可用区类型：单可用区
- 可用区：可用区一
- 时区：UTC+08:00
- 性能规格：独享版 | 4 vCPU | 16 GB
- 虚拟私有云：vpc-2 | vpc-2-subnet | 自动分配 IP 地址
- 安全组：sg-rds
- 管理员密码：自定义
- 参数模板：Default-GaussDB-for-MySQL 8.0
- 购买数量：1


购买数据库实例
计费模式
包年/包月
按需计费
区域
华北-北京四
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。
实例名称
rds-wordpress
购买多个数据库时，名称自动按序增加4位数字后缀。例如输入instance，从instance-0001开始命名；若已有instance-0010，
数据库引擎
GaussDB(for MySQL)
兼容的数据库版本
MySQL 8.0
可用区类型
单可用区
可用区
可用区一
可用区二
可用区三
可用区七
时区
UTC+08:00 北京，重庆，香港，乌鲁...


性能规格
独享版
CPU架构
x86
CPU | 内存
最大连接数
4 vCPUs | 16 GB
5,000
4 vCPUs | 32 GB
10,000
8 vCPUs | 32 GB
10,000
16 vCPUs | 128 GB
18,000
32 vCPUs | 128 GB
30,000
32 vCPUs | 256 GB
30,000
当前选择实例 独享版 x86 4 vCPUs 16 GB
只读节点数量
1
存储设置
购买时无需选择存储容量，存储费用按照实际使用量每小时计费。


虚拟私有云、子网、安全组与实例关系。
虚拟私有云
vpc-2
vpc-2-subnet(192.168.2.0/24)
自动分配IP地址
查看已使用IP地址
目前GaussDB实例创建完成后不支持切换虚拟私有云，请谨慎选择所属虚拟私有云。如需创建新的虚拟私有云，可前往控制台创建。批量创建数据库实例时，不支持指定IP地址。 可用私有IP数量251个
为确保实例创建成功，请确认子网、IP地址是否充足。
内网安全组
sg-rds
查看内网安全组
内网安全组可以设置数据库访问策略，内网安全组内规则的修改会对相关联的数据库立即生效。
实例的内网安全组规则必须允许100.125.0.0/16网段访问，否则部分网络访问异常。
请确保所选安全组规则允许需要连接实例的服务器能访问3306端口。
安全组规则详情
设置规则

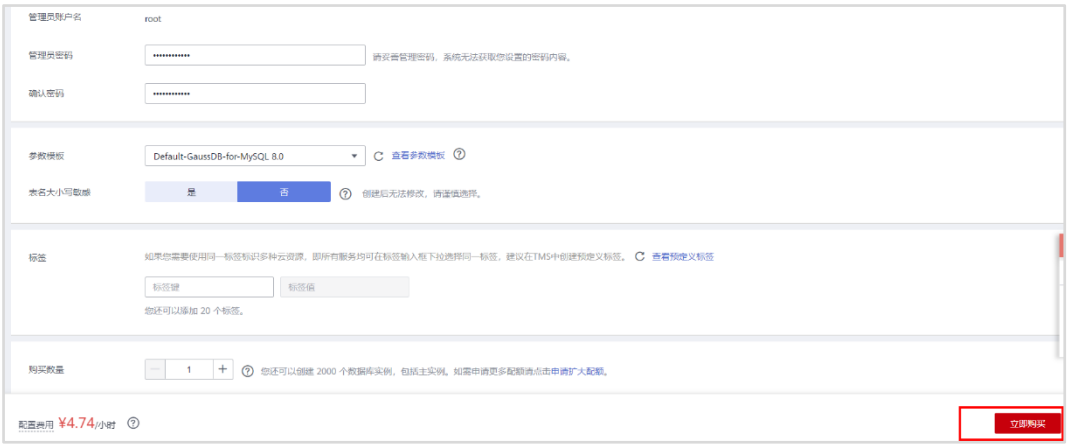


图4-10

步骤 4 确认配置后点击“提交”等待 5-10 分钟，实例创建完毕。

4.2.4 为 WordPress 创建数据库

步骤 1 在实例管理界面，记录数据库“读写内网地址”（本实验为 192.168.2.40），点击刚创建的实例右侧“登录”按钮，登录数据库。

图4-11

步骤 2 输入用户名密码后点击“测试连接”，通过后选择“登录”。

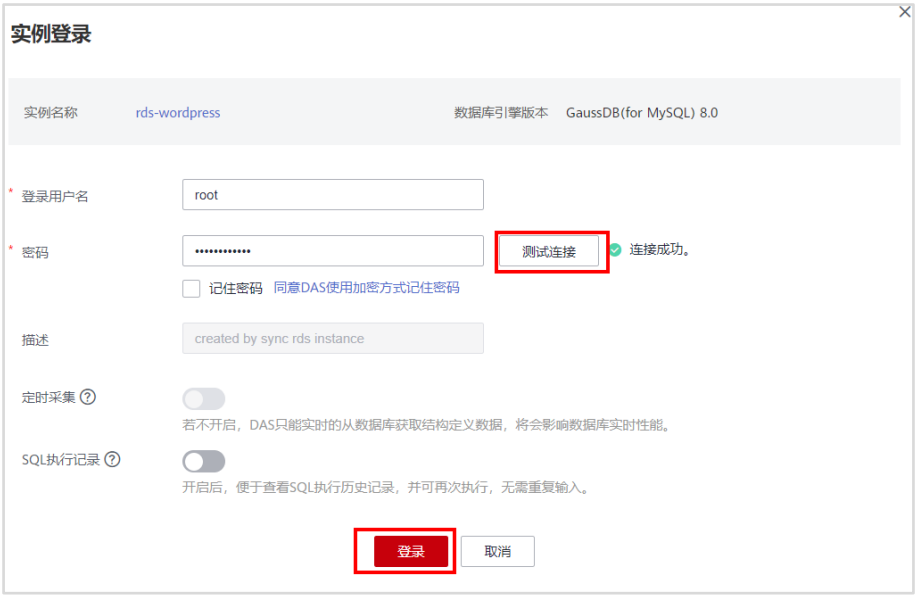


图4-12

步骤 3 在首页选择“新建数据库”（后续使用该数据库对接 WordPress）。

图4-13

步骤 4 按以下配置填入数据库名称和字符集后单击“确定”。

- 数据库名称：wordpress
- 字符集：utf8（默认配置）

步骤 5 创建完成后可以在数据库列表查看刚创建的数据库 wordpress。

图4-14

4.2.5 安装部署 WordPress

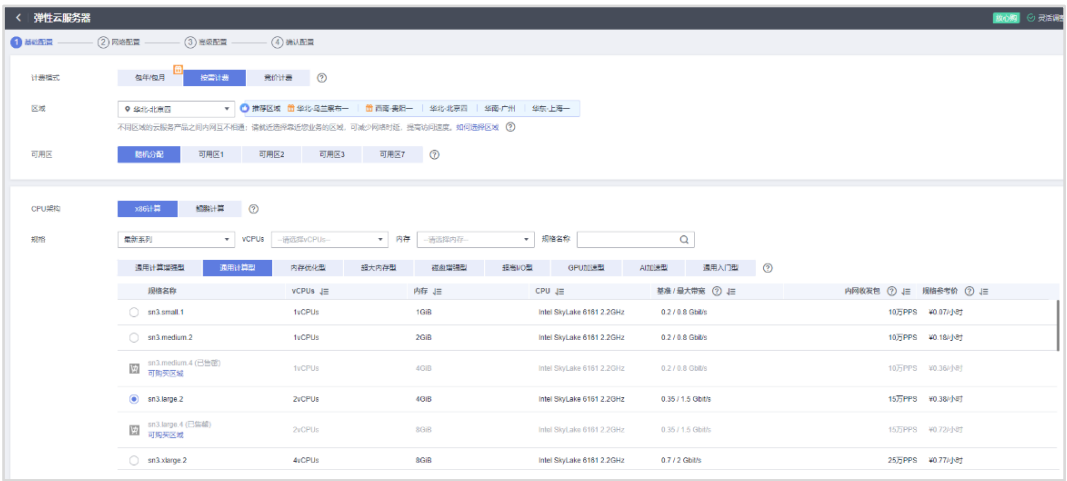
步骤 1 在服务列表中选择“弹性云服务器 ECS”，点击右上角“购买弹性云服务器”。

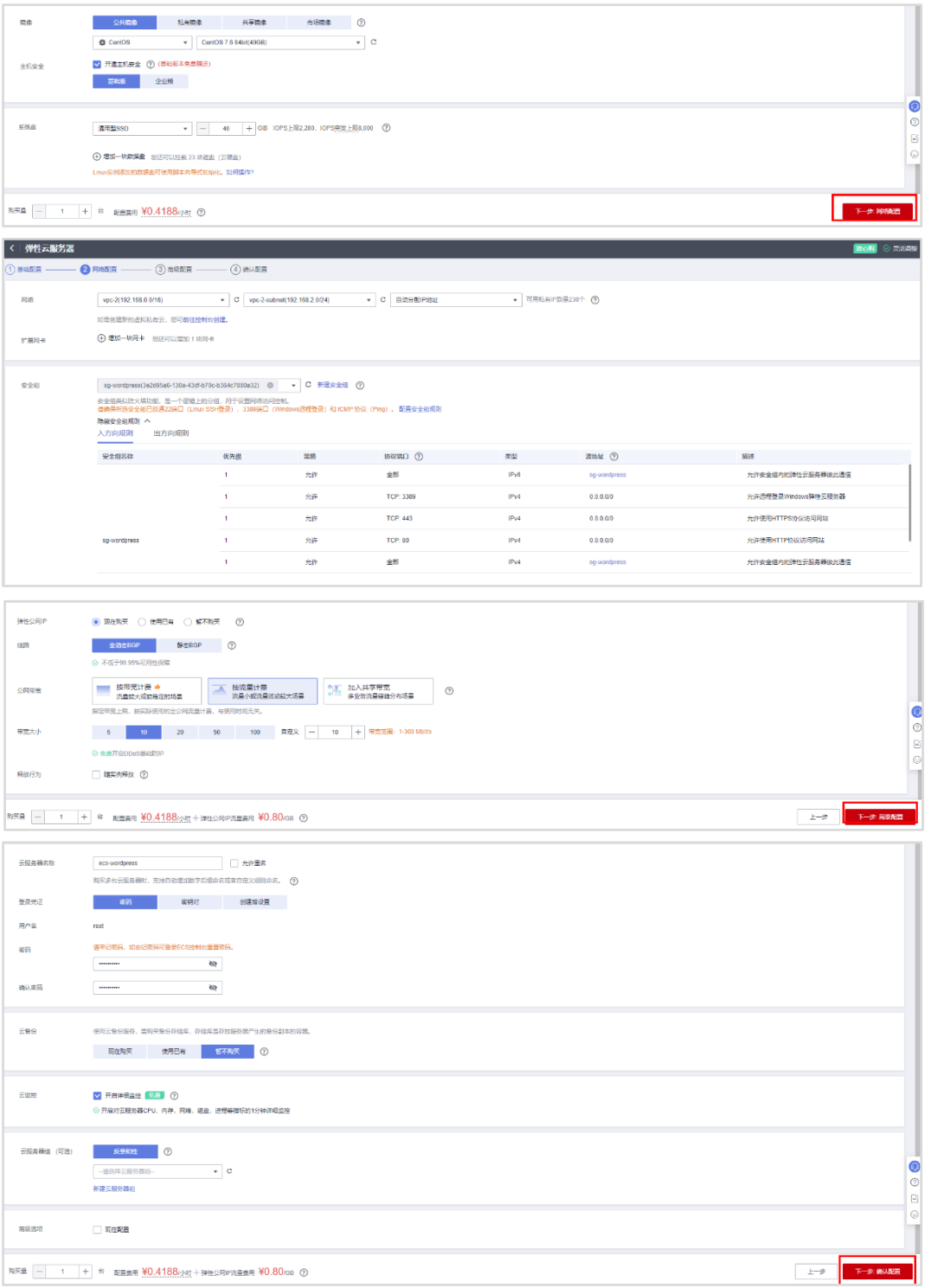
说明：该云服务器用于部署 WordPress。

图4-15

步骤 2 按以下配置选择相应参数，创建云服务器。

- 计费模式：按需计费
- 区域：华北-北京四
- 可用区：随机分配
- 规格：2 vCPUs|4 GiB
- 镜像：公共镜像|CentOS 7.6 64 bit（40 GB）
- 主机安全：基础版
- 系统盘：高 IO|40 GB
- 网络：vpc-2 | vpc-2-subnet | 自动分配 IP 地址
- 安全组：sg-wordpress
- 弹性公网 IP：现在购买
- 线路：全动态 BGP
- 公网带宽：按流量计费
- 带宽大小：10 Mbit/s
- 云服务器名称：ecs-wordpress
- root 密码：自定义





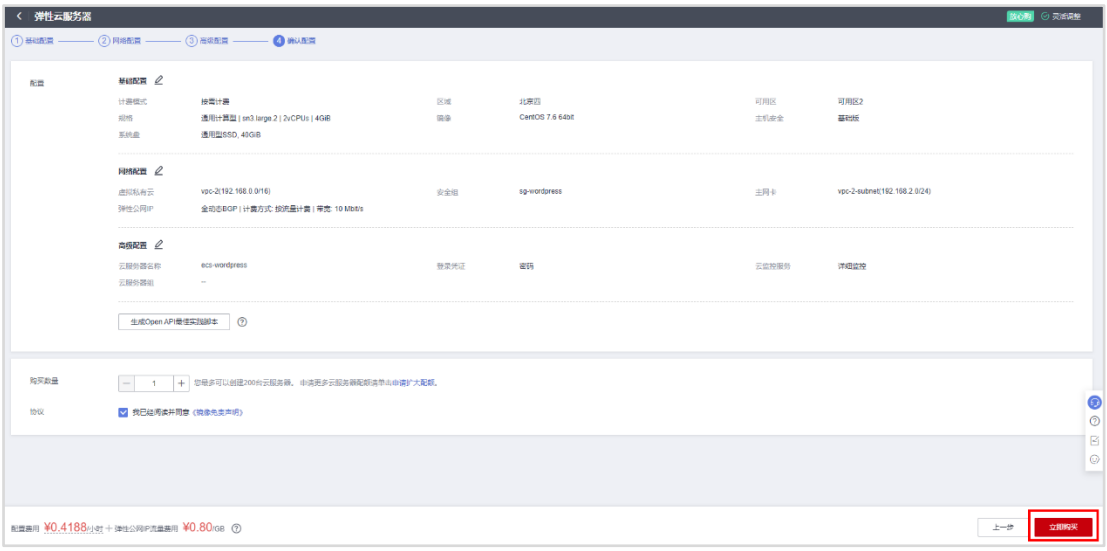


图4-16

步骤 3 在弹性云服务器列表中点击操作栏的“远程登录”，使用 CloudShell 登录 esc-wordpress 云主机。

图4-17

步骤 4 通过以下命令安装 Apache。

```
[root@ecs-wordpress ~]# yum install httpd -y
```

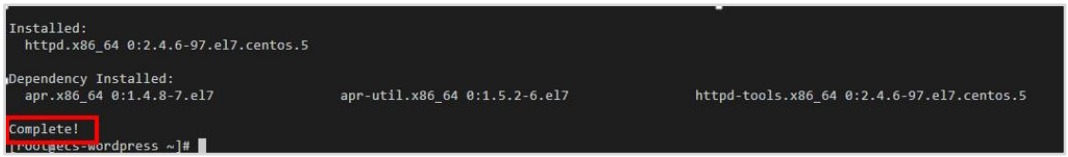


图4-18

步骤 5 通过以下命令安装 php。

```
[root@ecs-wordpress ~]# rpm -ivh http://rpms.famillecollet.com/enterprise/remi-release-7.rpm
[root@ecs-wordpress ~]# yum install --enablerepo=remi --enablerepo=remi-php56 php php-opcache php-devel php-mysqlnd php-gd php-redis
```

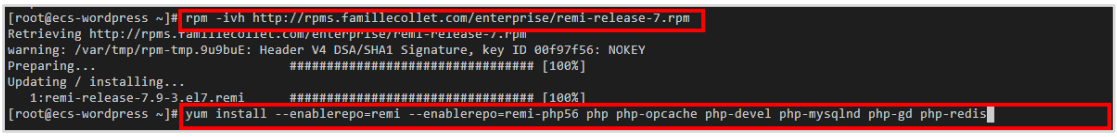


图4-19

步骤 6 连续两次输入“y”进行确认。

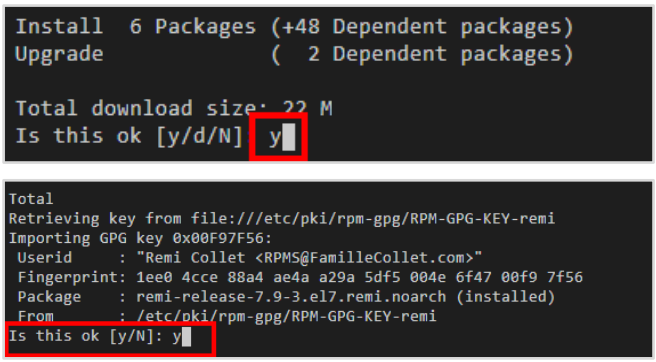


图4-20

步骤 7 使用如下命令下载 WordPress 安装包并解压。

```
[root@ecs-wordpress ~]# wget https://cloudservice-v3.obs.cn-east-3.myhuaweicloud.com/wordpress-5.2.3_zh.zip
[root@ecs-wordpress ~]# unzip wordpress-5.2.3-zh_CN.zip
[root@ecs-wordpress ~]# ls -l
```

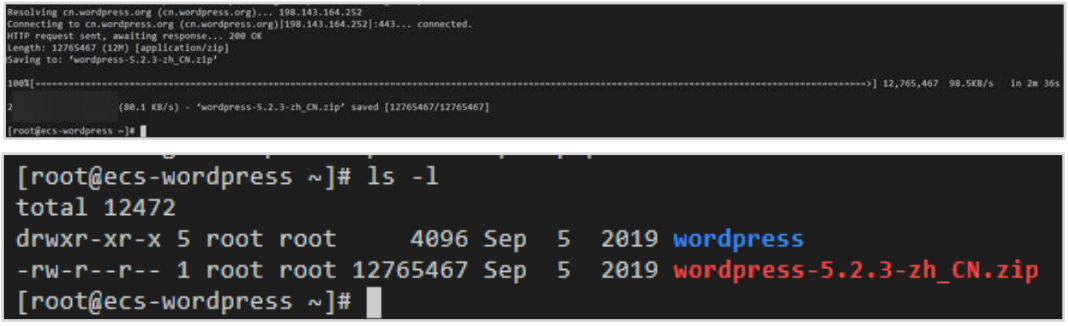


图4-21

步骤 8 使用如下命令拷贝 WordPress 文件夹到 Apache 的工作目录“/var/www/html”。

```
[root@ecs-wordpress ~]# cp -rf wordpress /var/www/html/
```

步骤 9 通过以下命令切换到 httpd 的工作目录，并复制配置文件。

```
[root@ecs-wordpress ~]# cd /var/www/html/wordpress
[root@ecs-wordpress wordpress]# cp wp-config-sample.php wp-config.php
```

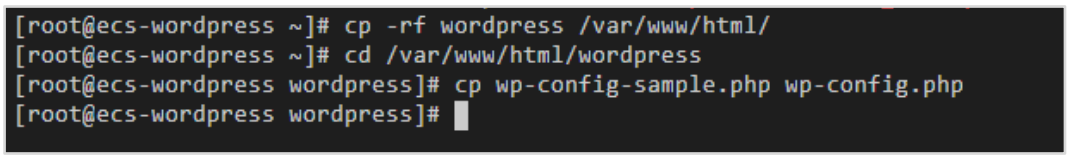


图4-22

步骤 10 使用如下命令修改 wp-config.php 文件，配置数据库参数对接之前创建的“wordpress”数据库。

```
[root@ecs-wordpress wordpress]# vi wp-config.php
```

修改 wp-config.php 文件中数据库的配置参数，如下内容：

- 数据库名称：wordpress
- 数据库用户名：root
- 数据库密码：Huawei123!@#（学员可自定义）
- 数据库主机：192.168.2.40:3306（数据库实例的*内网 IP 地址：端口号*）

```
// ** MySQL 设置 - 具体信息来自您正在使用的主机 ** //
/** WordPress数据库的名称 */
define( 'DB_NAME', 'wordpress' );

/** MySQL数据库用户名 */
define( 'DB_USER', 'root' );

/** MySQL数据库密码 */
define( 'DB_PASSWORD', 'Huawei123!@#' );

/** MySQL主机 */
define( 'DB_HOST', '192.168.2.40:3306' );

/** 创建数据表时默认的文字编码 */
define( 'DB_CHARSET', 'utf8' );

/** 数据库整理类型。如不确定请勿更改 */
define( 'DB_COLLATE', '' );
```

图4-23

步骤 11 通过以下命令配置 WordPress 目录权限。

```
[root@ecs-wordpress ~]# cd /var/www/html/wordpress
[root@ecs-wordpress wordpress]# echo -e "define(\"FS_METHOD\",
\"direct\");\ndefine(\"FS_CHMOD_DIR\", 0777);\ndefine(\"FS_CHMOD_FILE\", 0777);" >> wp-config.php
[root@ecs-wordpress wordpress]# tail -n 10 wp-config.php
[root@ecs-wordpress wordpress]# chmod -R 777 wp-content/
```

```
[root@ecs-wordpress ~]# cd /var/www/html/wordpress
[root@ecs-wordpress wordpress]# echo -e "define(\"FS_METHOD\", \"direct\");\ndefine(\"FS_CHMOD_DIR\", 0777);\ndefine(\"FS_CHMOD_FILE\", 0777);" >> wp-config.php
[root@ecs-wordpress wordpress]# tail -n 10 wp-config.php
/**                                                    */
if ( ! defined( 'ABSPATH' ) ) {
        define( 'ABSPATH', dirname( __FILE__ ) . '/' );
}

/**                                                    */
require_once( ABSPATH . 'wp-settings.php' );
define("FS_METHOD", "direct");
define("FS_CHMOD_DIR", 0777);
define("FS_CHMOD_FILE", 0777);
[root@ecs-wordpress wordpress]# chmod -R 777 wp-content/
[root@ecs-wordpress wordpress]#
```

图4-24

步骤 12 通过以下命令开启 Apache 服务并查看，如下图所示，证明服务正常开启。

```
[root@ecs-wordpress ~]# systemctl start httpd
[root@ecs-wordpress ~]# ps -ef |grep httpd
```

```
[root@ecs-wordpress ~]# systemctl start httpd
[root@ecs-wordpress ~]# ps -ef |grep httpd
root      8424     1  0 18:16 ?        00:00:00 /usr/sbin/httpd -DFOREGROUND
apache    8425  8424  0 18:16 ?        00:00:00 /usr/sbin/httpd -DFOREGROUND
apache    8426  8424  0 18:16 ?        00:00:00 /usr/sbin/httpd -DFOREGROUND
apache    8427  8424  0 18:16 ?        00:00:00 /usr/sbin/httpd -DFOREGROUND
apache    8428  8424  0 18:16 ?        00:00:00 /usr/sbin/httpd -DFOREGROUND
apache    8429  8424  0 18:16 ?        00:00:00 /usr/sbin/httpd -DFOREGROUND
root      8431  8323  0 18:17 pts/1    00:00:00 grep --color=auto httpd
```

图4-25

步骤 13 打开本地 PC 浏览器，输入：ECS-WordPress 的 EIP/wordpress/index.php。登录后完成以下配置内容，点击“Install WordPress”（本实验是：121.36.79.241/wordpress/index.php）。

- 站点标题：HCIP
- 用户名：huawei（学员可自定义）
- 密码：自定义
- 电子邮件：自定义

图4-26

步骤 14 点击“Log in”重新登录。

图4-27

步骤 15 输入刚设置的用户名和密码登录 WordPress，如下图所示，证明 WordPress 搭建完成。

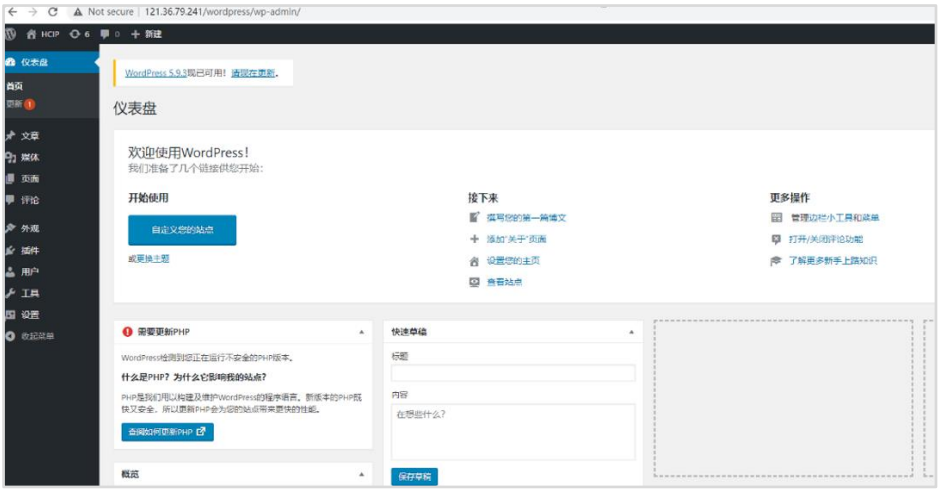


图4-28

步骤 16 在左侧页签中选择“插件-安装插件”。

图4-29

步骤 17 在右侧的搜索栏中输入“redis”，找到“Redis Object Cache”，点击“现在安装”（为后续对接 Redis 服务做好插件准备）。

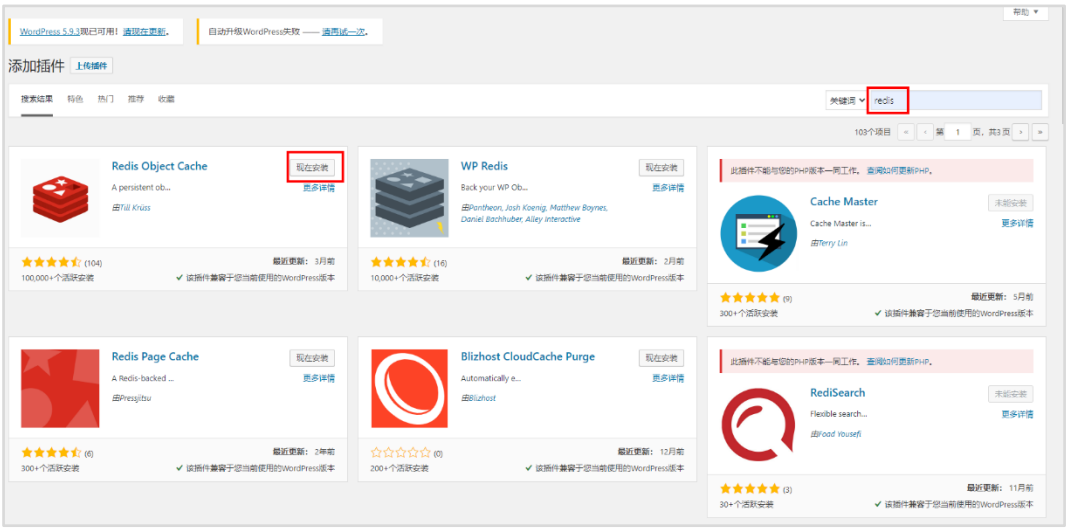


图4-30

4.2.6 创建 GaussDB（for Redis）服务

步骤 1 在“华北-北京四”的服务列表中选择“云数据库 GaussDB（for Redis）”服务，点击右上角“购买数据库实例”，按照以下配置购买数据库实例。

说明：本实验中使用该 GaussDB（for Redis）数据库实例为 WordPress 提供 Redis 服务。

- 计费模式：按需计费
- 区域：华北-北京四
- 实例名称：redis-wordpress
- 兼容接口：Redis
- 实例类型：Proxy 集群
- 版本：5.0
- 可用区：可用区一
- 节点规格：2vCPUs
- 节点数量：2
- 存储容量：16 GB
- 虚拟私有云：vpc-2
- 子网：vpc-2-subnet
- 内网安全组：sg-redis
- 数据库密码：Huawei123!@#（学员可自定义）

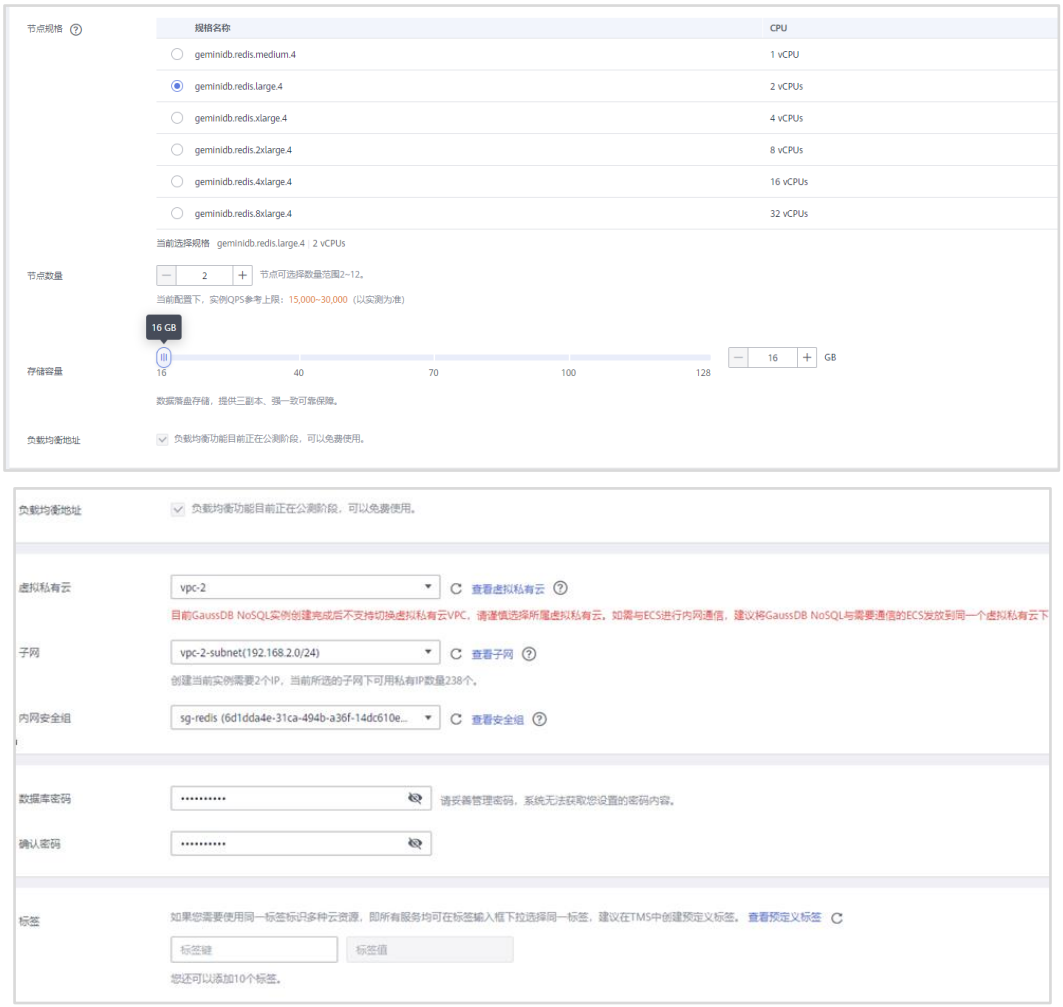


图4-31

步骤 2 查看并选中已购买的数据库实例。

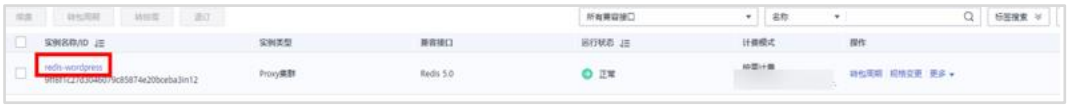


图4-32

步骤 3 在“基本信息”页签中查看并记录用户名、负载均衡地址、端口号和所配置的登录密码。

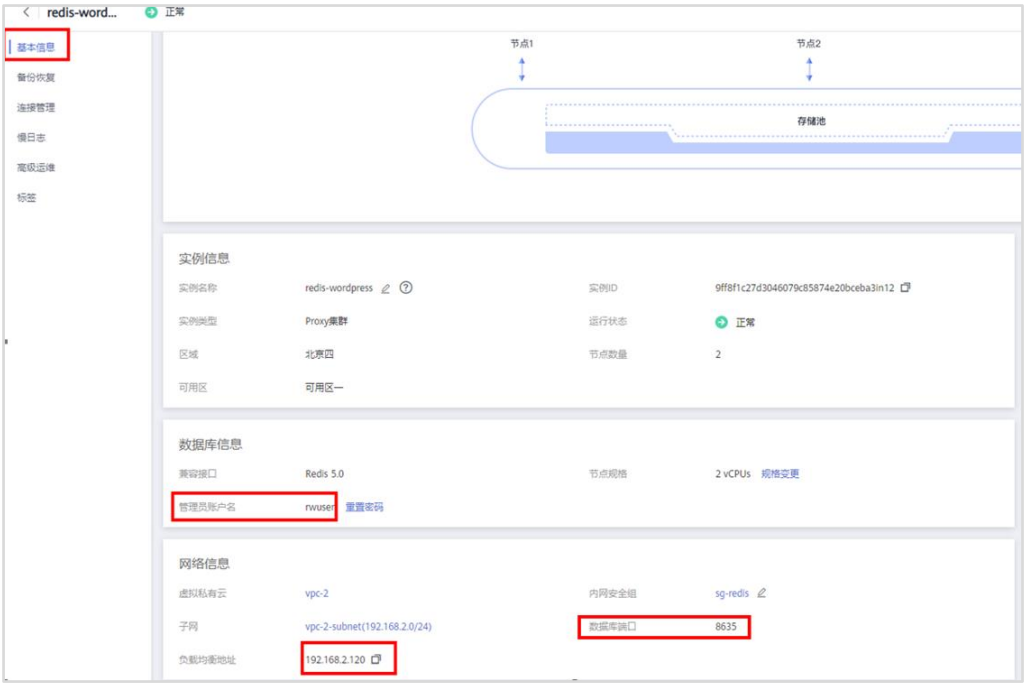


图4-33

步骤 4 登录云主机 ecs-wordpress，通过以下命令修改云主机的配置文件。

```
[root@ecs-wordpress ~]# cd /var/www/html/wordpress/
[root@ecs-wordpress wordpress]# vi wp-config.php
```

- 在该文件中增加以下内容用以对接 Redis 服务。

```
/*redis config*/
define('WP_REDIS_HOST', '192.168.2.120');
define('WP_REDIS_PORT', '8635');
define('WP_REDIS_PASSWORD', 'Huawei123!@#');
```

说明：以上内容中“192.168.2.120”为步骤 3 中 Redis 负载均衡服务地址，配置时请注意替换为实际服务地址。以上内容中“Huawei123!@#”为步骤 1 中设置的数据库密码，配置时请注意替换为实际密码。

```
// ** MySQL 设置 - 具体信息来自您正在使用的主机 ** //
/** WordPress数据库的名称 */
define( 'DB_NAME', 'wordpress' );

/** MySQL数据库用户名 */
define( 'DB_USER', 'root' );

/** MySQL数据库密码 */
define( 'DB_PASSWORD', 'Huawei123!@#' );

/** MySQL主机 */
define( 'DB_HOST', '192.168.2.40:3306' );

/** 创建数据表时默认的文字编码 */
define( 'DB_CHARSET', 'utf8' );

/** 数据库整理类型。如不确定请勿更改 */
define( 'DB_COLLATE', '' );

/*redis config*/
define('WP_REDIS_HOST', '192.168.2.120');
define('WP_REDIS_PORT', '8635');
define('WP_REDIS_PASSWORD', 'Huawei123!@#');
```

图4-34

步骤 5 通过以下命令保存退出。

```
:wq
```

4.2.7 启用 Redis

步骤 1 在启用 Redis 之前，浏览器中使用“F12”键，勾选“Disable cache”选项，查看页面加载时间。刷新 WordPress 界面，发现当前显示加载时间为“18.52s”。

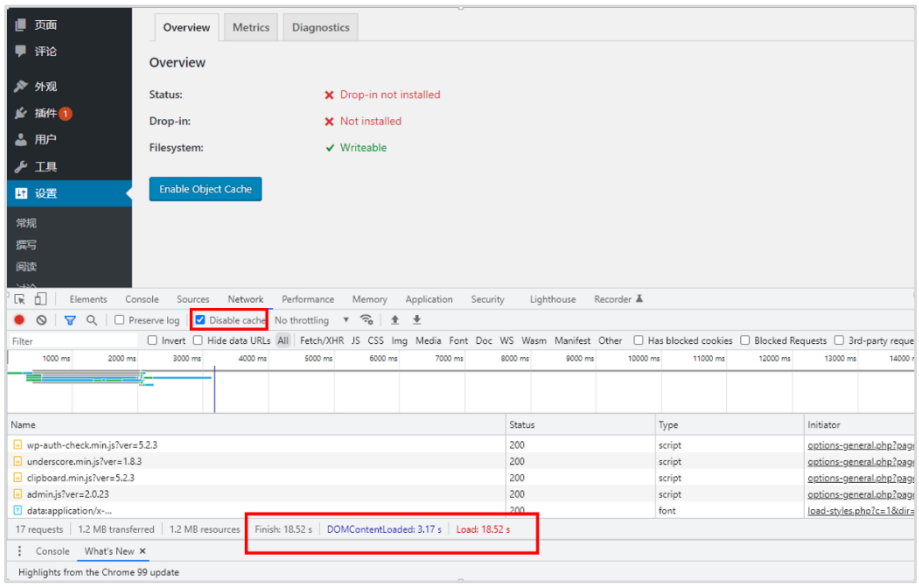


图4-35

步骤 2 本地 PC 浏览器登录 WordPress，选择“插件>已安装插件”，找到“Redis Object Cache”，点击“启用”。

图4-36

步骤 3 在“Overview”页签下点击“Enable Object Cache”。

图4-37

步骤 4 查看状态，显示“Connected”，证明 Redis 服务已成功对接并启用。

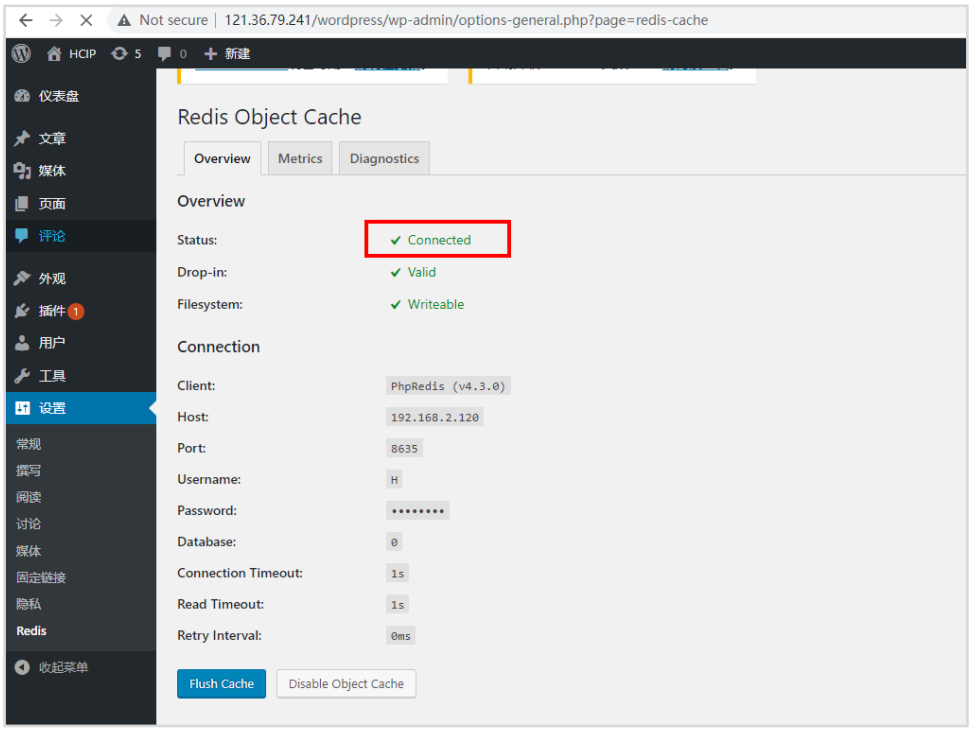


图4-38

4.3 实验验证

步骤 1 在浏览器中使用“F12”键，勾选“Disable cache”选项，查看启用 Redis 的页面加载时间。刷新页面，发现当前加载时间为“3.94s”，低于启用 Redis 服务之前的 18.52s，实现了通过启用 Redis 服务提升网站响应速度的需求，本实验成功完成。

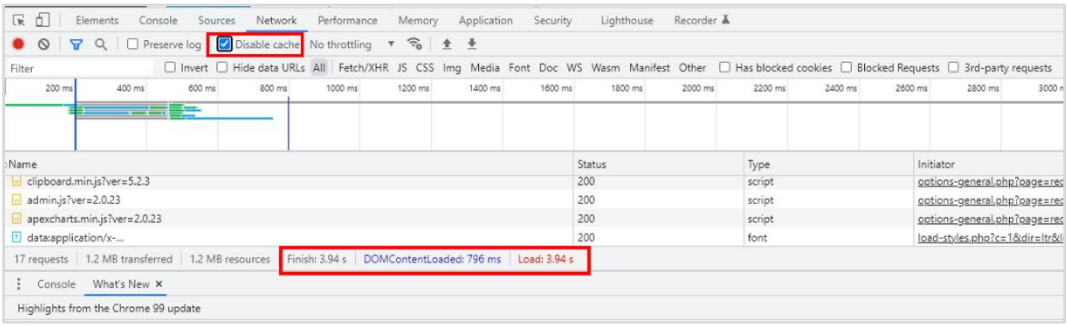


图4-39

4.4 实验恢复

步骤 1 删除 GaussDB（for Redis）实例。

- 在服务列表中选择“云数据库 GaussDB（for Redis）”，在列表中找到本实验创建的数据库实例，点击操作栏中的“更多>删除实例”

步骤 2 删除 GaussDB 数据库实例。

- 在服务列表中选择“云数据库 GaussDB”，在列表中找到本实验创建的数据库实例，点击操作栏中的“更多>删除实例”。

步骤 3 删除 ECS。

- 在服务列表中选择“云服务器 ECS”，找到本实验创建的云服务器，点击操作栏中的“更多>删除”。
- 在弹出的对话框中勾选下图中选项，点击“是”。

图4-40

步骤 4 删除安全组。

- 在服务列表中选择“虚拟私有云 VPC”，在“访问控制>安全组”中找到本实验创建的安全组，点击操作栏的“更多>删除”。

步骤 5 删除 VPC。

- 在服务列表中选择“虚拟私有云 VPC”，点击“子网”页签，在列表中找到本实验创建的子网，点击操作栏中的“删除”。
- 点击“虚拟私有云”页签，找到本实验创建的 VPC，点击操作栏中的“删除”。

4.5 思考题

问题：当我们想通过配置多个后端数据库实例来提升数据库服务的容量和性能，可以采用哪种方案?

参考答案：可以采用华为分布式数据库中间件服务（DDM），通过 DDM 可以做到数据库线性水平扩展，提升数据库处理能力，轻松应对高并发、实时交互业务场景。

5 安全架构设计实验

5.1 实验介绍

5.1.1 关于本实验

本实验分为以下 7 个部分：

1. DVWA（Damn Vulnerable Web Application，简称 DVWA）主机部署：通过 ECS 部署 DVWA 主机提供实验环境，以该主机为基础进行后续安全配置操作。

2. 主机安全：为 DVWA 主机购买企业主机安全（Host Security Service，简称 HSS）服务，通过 HSS 获取主机状态、查看当前风险总览提升主机安全管理能力。

3. 双因子认证：设计为 DVWA 主机配置双因子认证，实验中登录并验证该双因子认证，熟悉并掌握双因子认证的基本功能和使用。

4. 主机安全组：设计通过删除、添加安全组内 8080 端口的方式验证主机安全组的访问控制功能。

5. IP 地址组：设计将 test 云主机地址加入地址组，并将该地址组添加进安全组内的拒绝规则中，验证地址组配合安全组的原理和配置方法。

6. Web 应用防火墙：设计使用独享版 Web 应用防火墙（Web Application Firewall，简称 WAF），并将 DVWA 的 EIP 地址配置为防护网站，配置 WAF 负载均衡器接入防护网站。配置完成后进行攻击测试，通过发现攻击被拦截，验证 Web 应用防火墙的使用原理。

7. DEW 托管密钥（Data Encryption Workshop，简称 DEW）：本实验需要在数据加密服务 DEW 凭据管理中创建密钥，在统一身份认证中创建委托，在云主机中安装 KooCLI 客户端。设计通过以上配置，使用 KooCLI 客户端获取 DEW 凭据管理中托管的密钥信息。

说明：本实验以“北京一”区域为例，学员可以根据实际情况选择相应区域进行实验，注意独享版 WAF 需要提交工单申请开通。

5.1.2 实验目的

理解企业主机安全服务的使用原理。

掌握双因子认证、安全组、地址组的使用原理和配置方法。

掌握 Web 应用防火墙的使用原理和配置方法。

掌握使用弹性云主机获取 DEW 服务中托管密钥的原理和配置方法。

5.1.3 实验组网

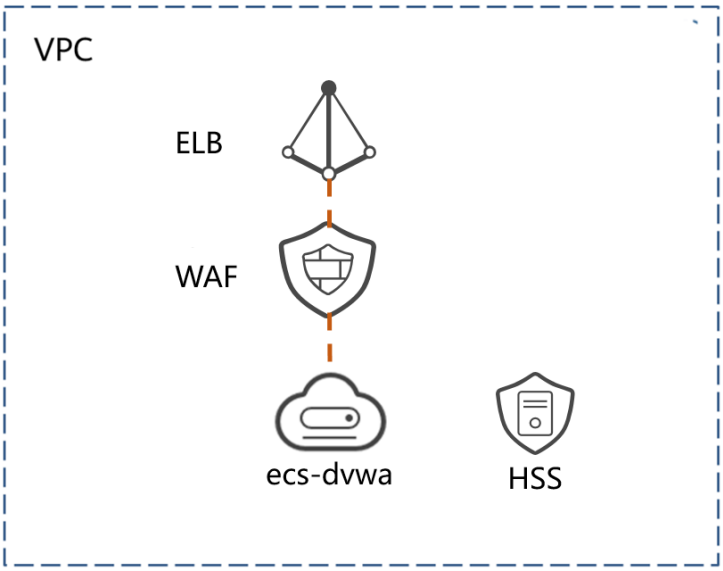


图5-1

5.1.4 软件介绍

1. DVWA（Dam Vulnerable Web Application）是用 PHP+Mysql 编写的一套用于常规 Web 漏洞教学工具。其主要目标是帮助安全专业人员在合法环境中测试他们的技能和工具，帮助 Web 开发人员更好地了解保护 Web 应用程序的过程，帮助教师、学生在课堂环境中教授、学习 Web 应用程序安全性，其中包含了 SQL 注入、XSS、盲注等常见的一些安全漏洞。

2. XAMPP 是一个易于安装且包含 MySQL、PHP 和 Perl 的 Apache 发行版，XAMPP 目的是让没有任何 Web 服务器安装、配置经验的人员也可以快速搭建一个 Web 服务器。

3. XSS 攻击：通常情况下，在 Web 应用的网页中，有些部分的显示内容会依据外界输入值而发生变化，如果生成这些 HTML 的程序中存在问题或漏洞，就会滋生名为跨站脚本（Cross-Site Scripting）攻击的安全隐患。XSS 其实是一种恶意代码的反弹攻击，它会将代码发送给有漏洞的网站，恶意代码会从该网站反弹给用户，用户侧执行恶意代码后，敏感信息就会遭到窃取。

4. KooCLI：华为云命令行工具，是为发布在 API Explorer 上的华为云服务 API 提供的命令行管理工具。可以通过此工具调用 API Explorer 中各云服务开放的 API，管理和使用各类云服务资源。

5.2 实验配置

5.2.1 DVWA 主机部署

步骤 1 在“北京一”区域的服务列表中选择“虚拟私有云 VPC”。

图5-2

步骤 2 点击右上角“创建虚拟私有云”（本实验中的资源将创建在该 VPC 中）。

图5-3

步骤 3 按照以下要求填写参数，并点击“立即创建”完成创建。

基本信息：

- 区域：华北-北京一
- 名称：vpc-1
- IPv4 网段：192.168.0.0/16

默认子网：

- 可用区：可用区 1
- 名称：subnet-20
- 子网 IPv4 网段：192.168.20.0/24

图5-4

步骤 4 在左侧页签中选择“访问控制”，选择“安全组”，点击右上角“创建安全组”。

说明：该安全组供后续 DVWA 主机使用，需要放通 22、443、80 和 8080 端口和 ICMP 协议。

图5-5

步骤 5 按照以下配置创建安全组。

- 名称：sg-dvwa
- 模板：自定义

图5-6

步骤 6 在弹出的对话框中选择“配置规则”。

图5-7

步骤 7 按照以下配置，在“入方向规则”中分别添加 22、8080、80、443 端口和 ICMP 协议规则。

- 优先级：1
- 策略：允许
- 协议端口：TCP|22
- 类型：IPv4
- 源地址：IP 地址|0.0.0.0/0

图5-8

- 优先级：1
- 策略：允许
- 协议端口：TCP|8080
- 类型：IPv4
- 源地址：IP 地址|0.0.0.0/0

图5-9

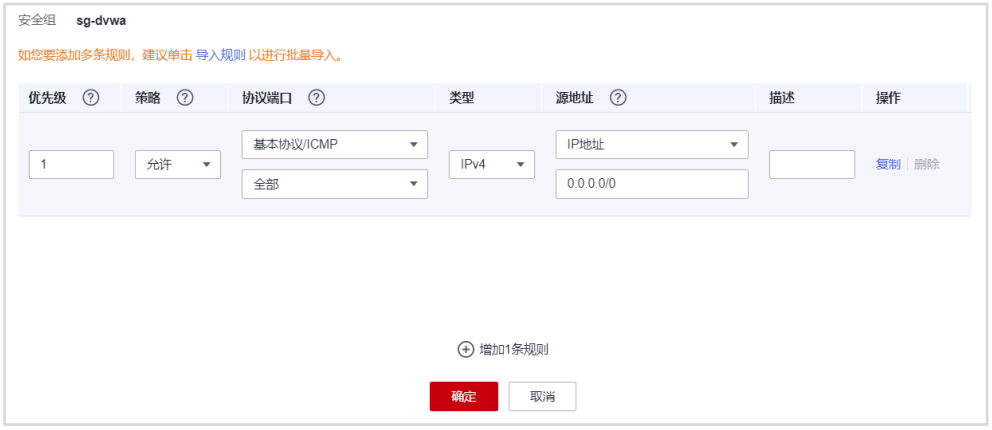
- 优先级：1
- 策略：允许
- 协议端口：TCP|443
- 类型：IPv4
- 源地址：IP 地址|0.0.0.0/0

图5-10

- 优先级：1
- 策略：允许
- 协议端口：TCP|80
- 类型：IPv4
- 源地址：IP 地址|0.0.0.0/0

图5-11

- 优先级：1
- 策略：允许
- 协议端口：ICMP|全部
- 类型：IPv4
- 源地址：IP 地址|0.0.0.0/0



步骤 8 配置完成后查看当前规则列表，可以看到 80、22、8080、443 端口和 ICMP 协议相关规则已被加入规则列表中。

图5-12

步骤 9 在服务列表中选择“弹性云主机 ECS”，并点击右上角购买弹性云服务器。

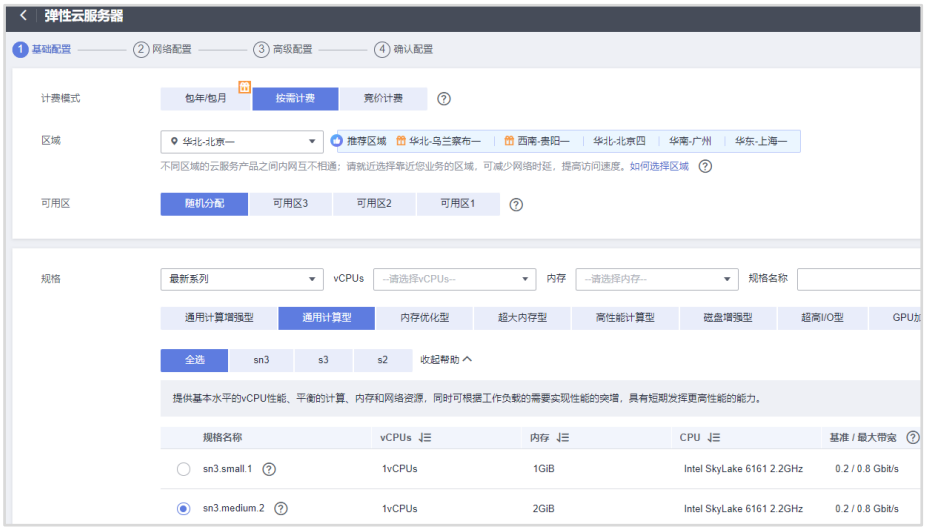
图5-13

步骤 10 按照如下配置完成云服务器创建。

说明：该云服务器将用于 DVWA 主机部署。

云主机“ecs-dvwa”配置：

- 计费模式：按需计费
- 区域：华北-北京一
- 可用区：随机分配
- CPU 架构：x86 计算
- 规格：1 vCPUs | 2 GiB
- 镜像：公共镜像 | CentOS 7.6 64 bit
- 主机安全：开通主机安全（基础版）
- 网络：vpc-1 | subnet-20 | 自动分配 IP 地址
- 安全组：sg-dvwa
- 弹性公网 IP：现在购买
- 线路：全动态 BGP
- 公网带宽：按流量计费
- 带宽大小：10 Mbit/s
- 系统盘：高 IO | 40 GiB
- 云服务器名称：ecs-dvwa
- root 密码：自定义



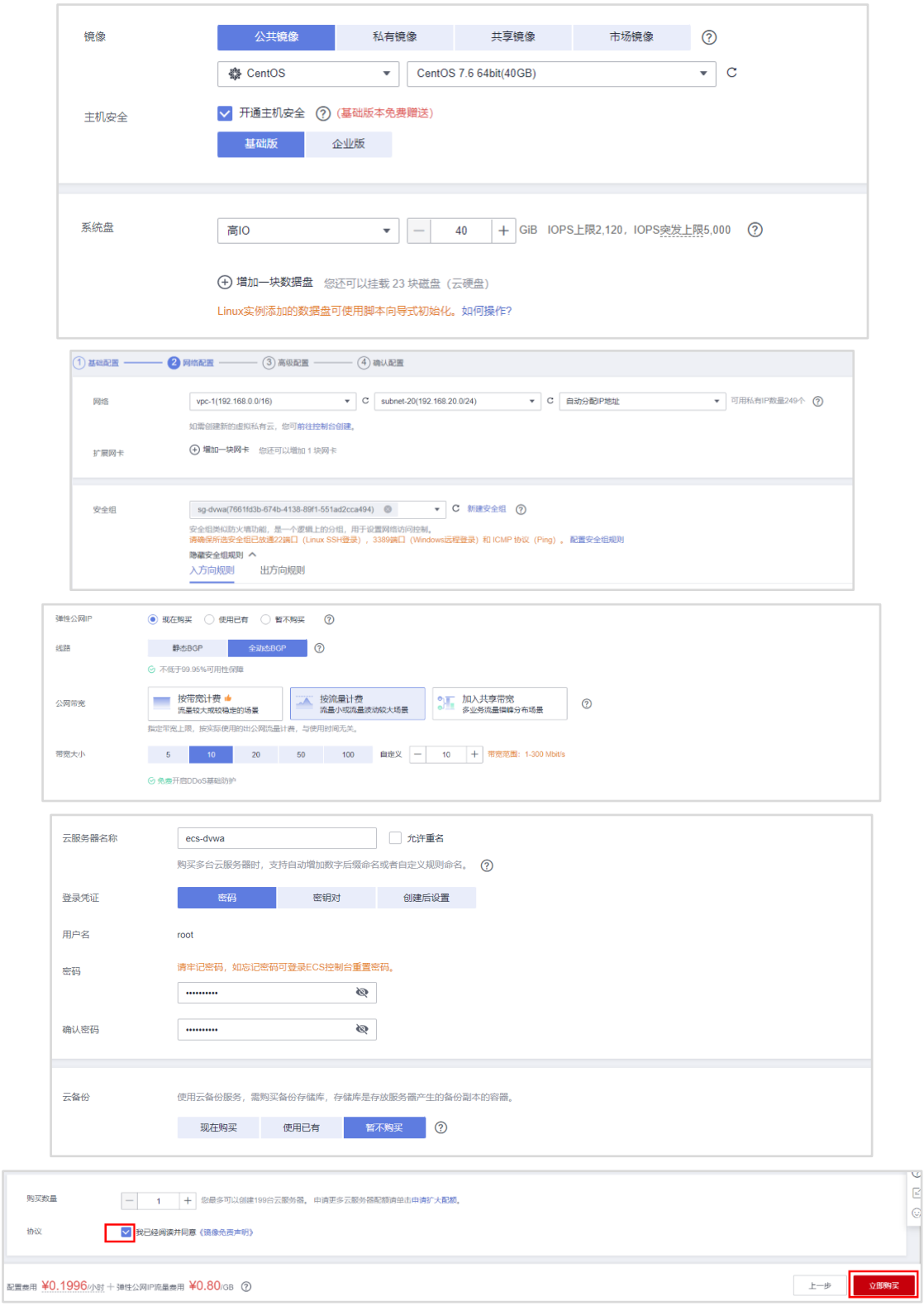


图5-14

步骤 11 使用华为云 CloudShell 登录 ECS，使用如下命令安装 docker。

```
[root@ecs-dvwa ~]# yum install docker
[root@ecs-dvwa ~]# systemctl enable docker
```

```
[root@ecs-dvwa ~]# systemctl start docker
```

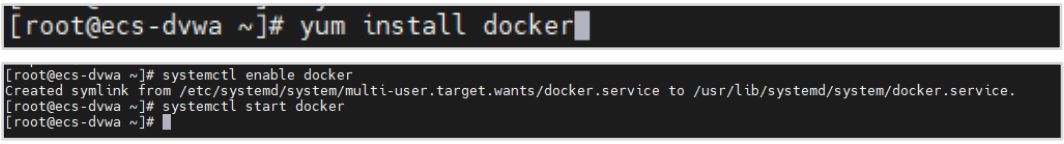


图5-15

步骤 12 使用如下命令下载 DVWA 容器镜像。

```
[root@ecs-dvwa ~]# docker pull docker.io/citizenstig/dvwa
```

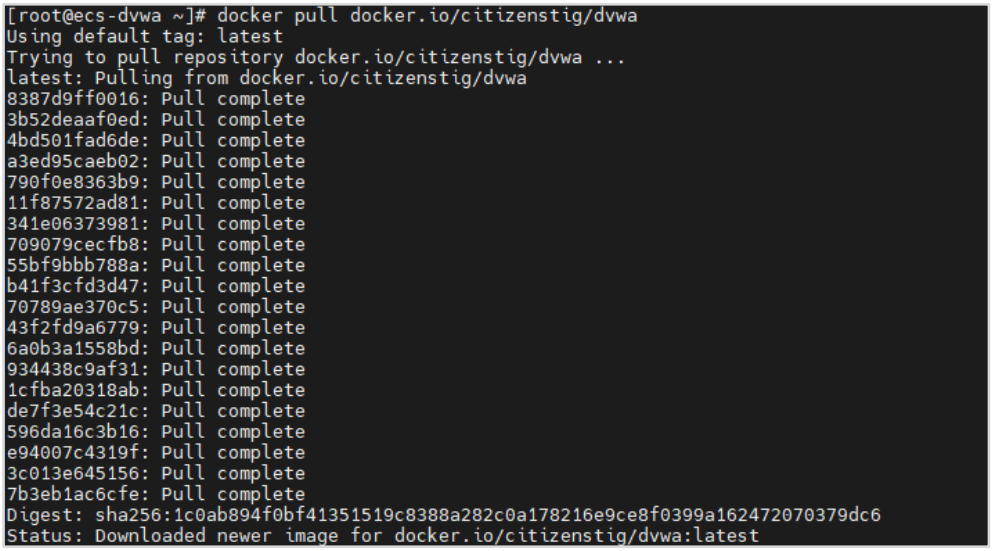


图5-16

步骤 13 使用如下命令查看当前镜像并运行镜像为容器。

```
[root@ecs-dvwa ~]# docker images
```

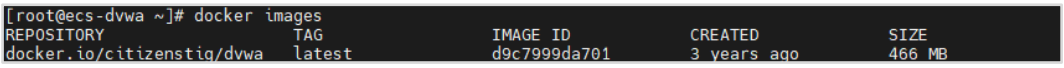


图5-17

步骤 14 使用如下命令将镜像运行为容器并将容器内 80 服务端口映射为 8080。

```
[root@ecs-dvwa ~]# docker run -dit -p 8080:80 docker.io/citizenstig/dvwa
3b3f5da35aadd8223818bdbab650e50d305ffaf7fb262c1f82eff63c5dc6190c
[root@ecs-dvwa ~]# docker ps
```

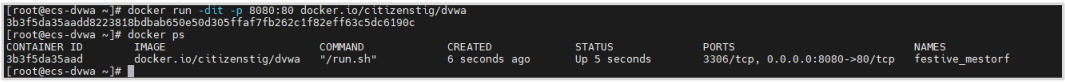


图5-18

步骤 15 在本地浏览器通过“http://119.3.196.178:8080”（其中 119.3.196.178 为云主机 ecs-dvwa 的弹性公网 IP 地址）打开 DVWA 的 Web 页面，点击“create/reset database”按钮进行初始化。

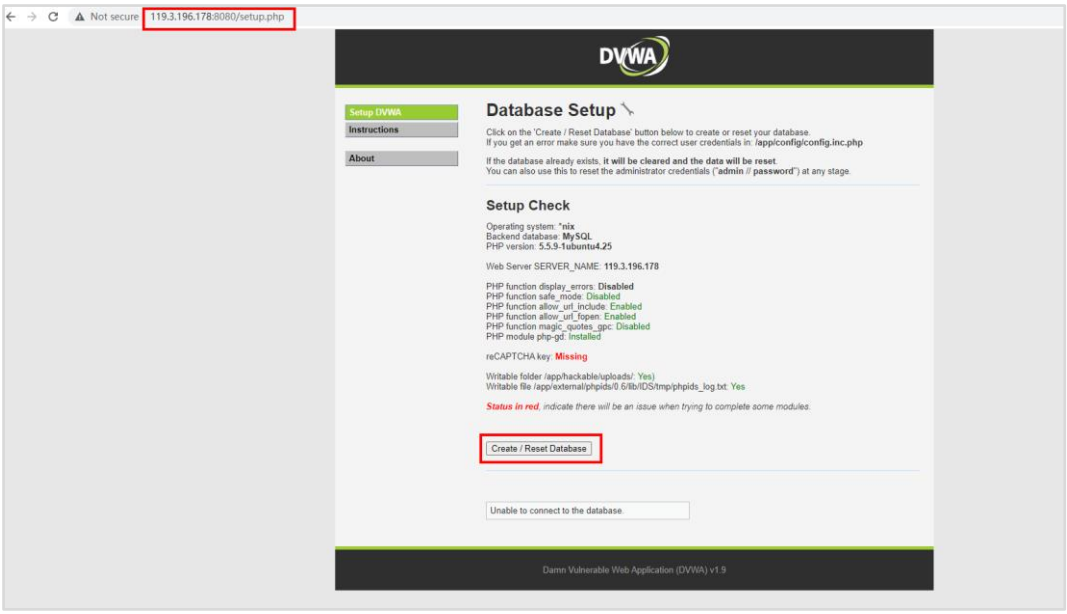
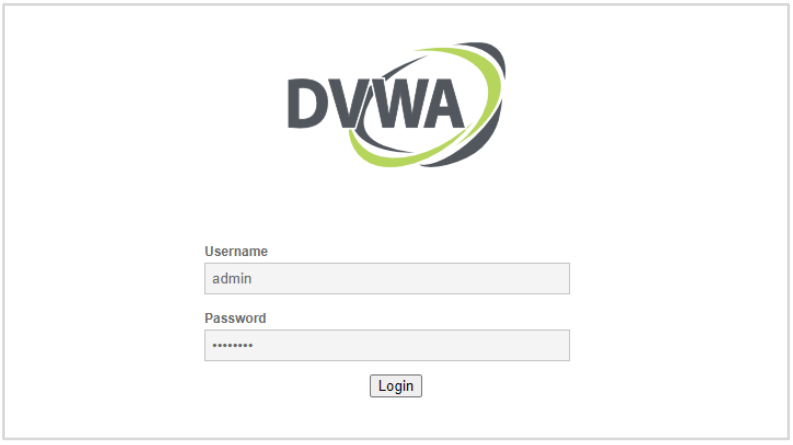


图5-19

步骤 16 初始化完成后，页面将自动跳转到登录页面，输入认证信息登录 DVWA。如下图所示，则证明 DVWA 主机部署成功。

说明：用户名/密码：admin/password



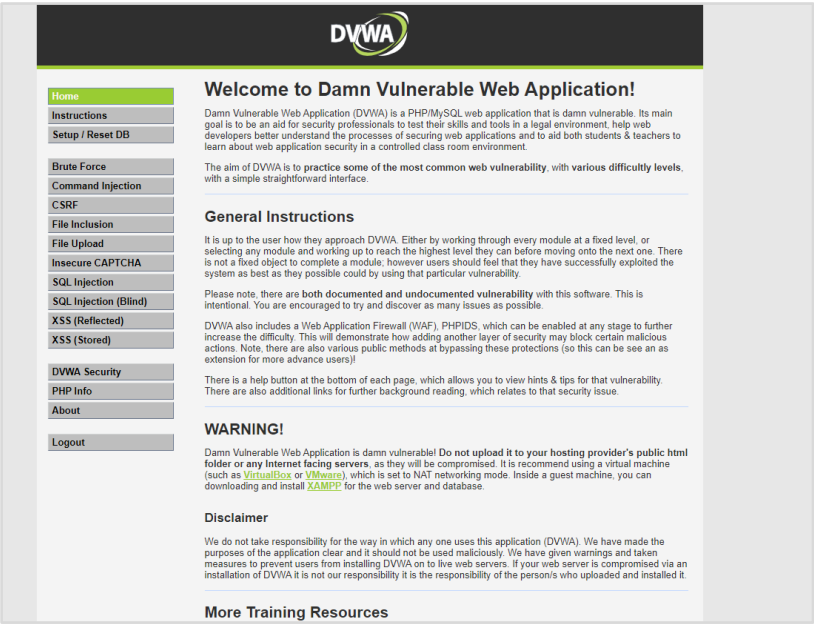


图5-20

步骤 17 使用华为云 CloudSell 登录 ECS，使用如下命令下载 XAMPP。

```
[root@ecs-dvwa ~]# wget https://cloudservice-v3.obs.cn-east-3.myhuaweicloud.com/xampp-linux-x64-7.3.6-2-installer.run
```

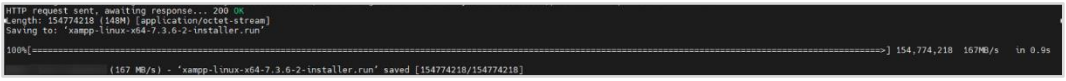


图5-21

- 使用如下命令修改权限并安装 XAMPP。

```
[root@ecs-dvwa ~]# chmod 755 xampp-linux-*-installer.run
[root@ecs-dvwa ~]# ./xampp-linux-*-installer.run
```

说明：执行命令后请按以下图示执行相应动作，完成安装。

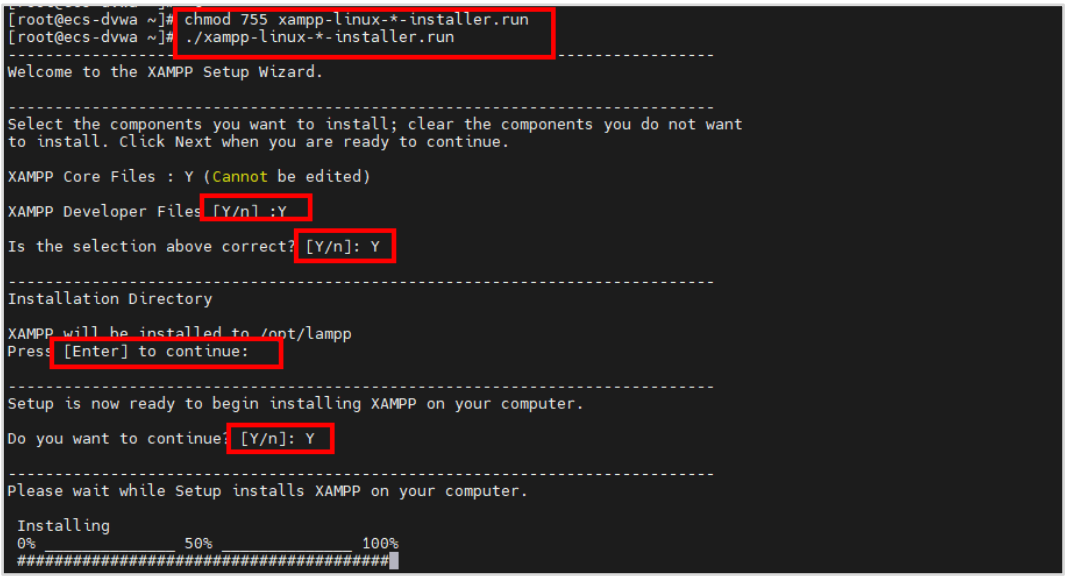


图5-22

步骤 18 本地浏览器访问 XAMPP 页面，输入 http://119.3.196.178（云主机 ecs-dvwa 的弹性公网 IP），可正常访问证明安装成功。

说明：请替换 ecs-dvwa-EIP 为 ecs-dvwa 的真实 EIP。

图5-23

5.2.2 主机安全

步骤 1 在服务列表中选择“企业主机安全 HSS”。

图5-24

步骤 2 点击右上方“购买主机安全”。

说明：主机安全可以通过资产管理、漏洞管理、基线检查、入侵检测、程序运行认证、文件完整性校验、安全运营、网页防篡改等功能全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为。

图5-25

步骤 3 按照以下配置完成主机安全购买并点击“立即开通”。

- 计费模式：按需
- 区域：华北-北京一
- 版本选择：企业版

图5-26

步骤 4 开通后会自动跳转至主机管理页面，在该页面中，选择点击“切换版本”。

图5-27

步骤 5 按照以下配置切换版本，勾选同意免责声明后点击“确定”。

说明：基础版免费使用，但只支持部分功能的检测能力，不支持防护能力，不支持等保认证。企业版可以满足等保二级认证、病毒木马查杀、漏洞一键修复、入侵检测等需求。

- 计费模式：按需计费
- 主机安全版本：企业版

图5-28

步骤 6 返回企业主机安全界面，点击“总览”可查看当前主机风险统计和主机防护统计。

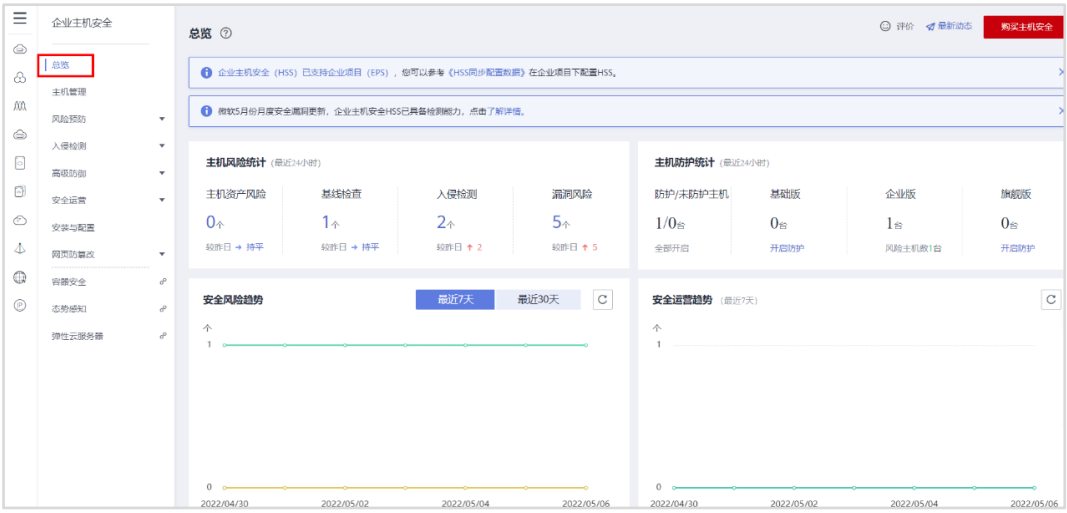


图5-29

步骤 7 点击“主机管理”页签，在云服务器列表中点击操作栏的“更多”，选择“查看详情”。

图5-30

步骤 8 在“入侵检测”页签下可查询当前检测的入侵攻击。

说明：证明主机在配置了企业版 HSS 后，已经具备入侵检测等功能，可实时识别并阻止入侵主机的行为，实时检测主机内部的风险异变，检测并查杀主机中的恶意程序。

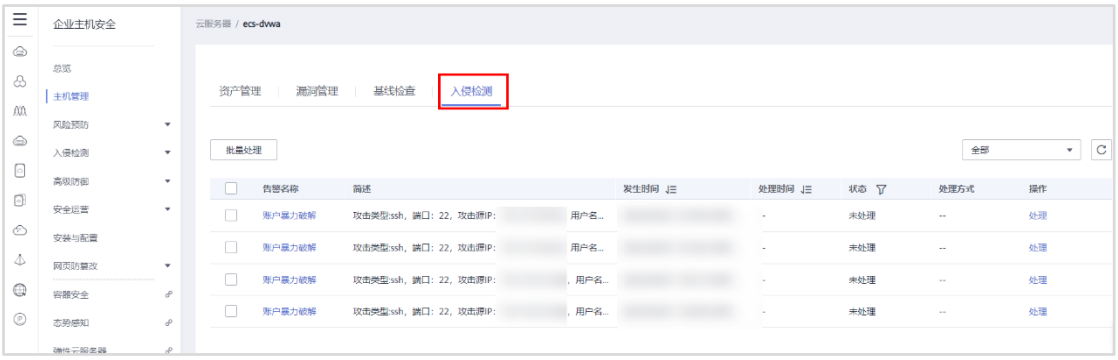


图5-31

5.2.3 双因子认证

在实际工作中，一些业务主机或运维主机对接入安全的要求较高，仅通过用户名密码做认证鉴权不够安全，此时可以通过配置双因子认证来满足主机登录多维度鉴权的需求。

步骤 1 配置消息通知服务。

说明：该消息通知服务（Simple Message Notification，简称 SMN）的配置供后续双因子认证使用。

- 在服务列表中选择“消息通知服务 SMN”。

图5-32

- 在“总览-我的资源”中选择“主题”。

图5-33

- 点击“创建主题”。

图5-34

- 填写主题名称“Auth”，点击“确定”。

图5-35

- 在主题的操作栏中选择“添加订阅”。

图5-36

- 按照以下配置添加订阅。

协议：短信

订阅终端：个人手机号（学员自定义）

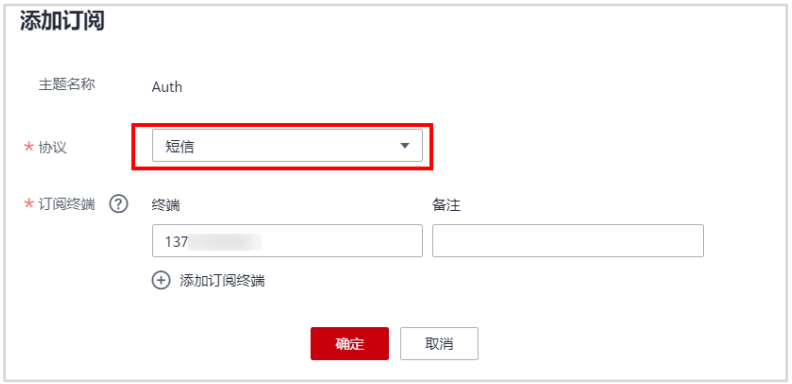


图5-37

- 在终端（手机短信）中确认后订阅生效。

步骤 2 创建双因子认证。

- 在服务列表中选择“企业主机安全 HSS”。

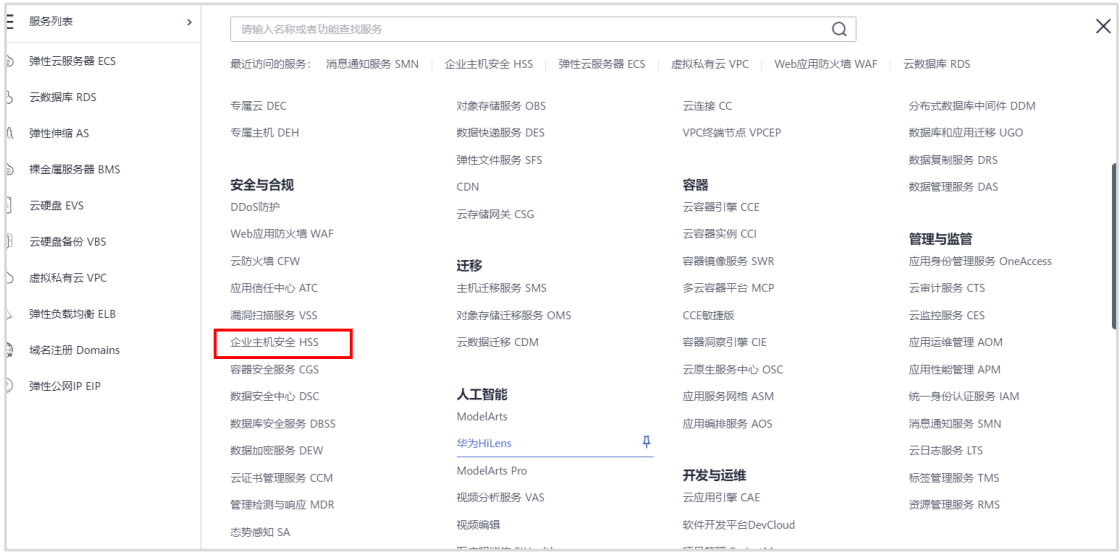


图5-38

- 在企业主机安全页面中，点击“安装与配置”页签，选择“双因子认证-开启双因子认证”。

图5-39

- 选择消息通知服务主题为刚创建的“Auth”，点击“确定”。

图5-40

- 使用华为云 CloudShell 登录 DVWA 主机。

输入用户名密码后，输入订阅中的手机号，将收到的短信验证码输入，登录主机。如下图所示，正常登录则证明双因子认证配置成功。通过这一小节内容，我们验证了双因子认证的基本功能和使用。

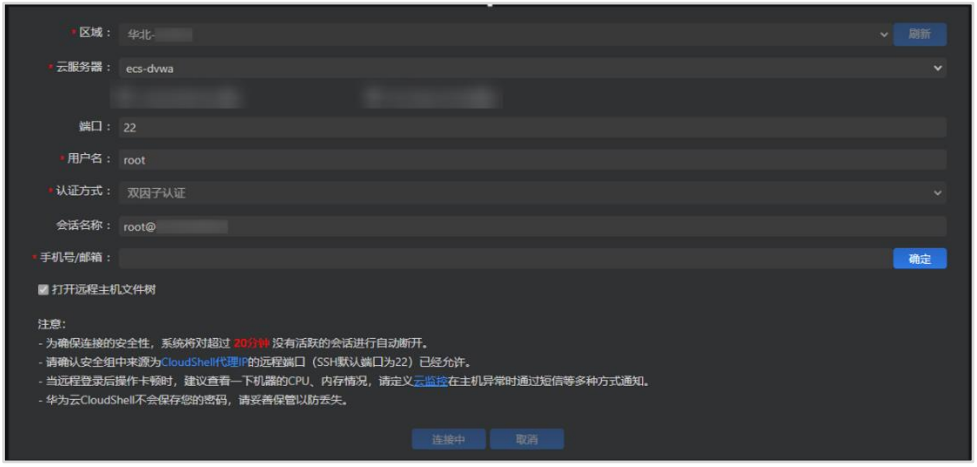


图5-41

5.2.4 主机安全组

步骤 1 在服务列表中选择“虚拟私有云 VPC”，在“访问控制”页签中选择“安全组”，在安全组列表中选择已创建好的“sg-dvwa”安全组。

图5-42

步骤 2 选择“入方向规则”，删除协议端口为“TCP:8080”的这条规则。

说明：此处将 8080 端口删除是为了拒绝 8080 端口请求，验证安全组的访问控制功能。

图5-43

步骤 3 在弹出的对话框中点击“是”。

图5-44

步骤 4 查看当前页面安全组规则列表，发现 8080 端口的相关规则已被删除。

图5-45

步骤 5 重新使用 http://119.3.196.178（DVWA 主机的 EIP）:8080 地址登录，刷新页面发现无法登录。证明此时安全组 sg-dvwa 做到了流量阻断，拒绝了 8080 端口的访问请求。

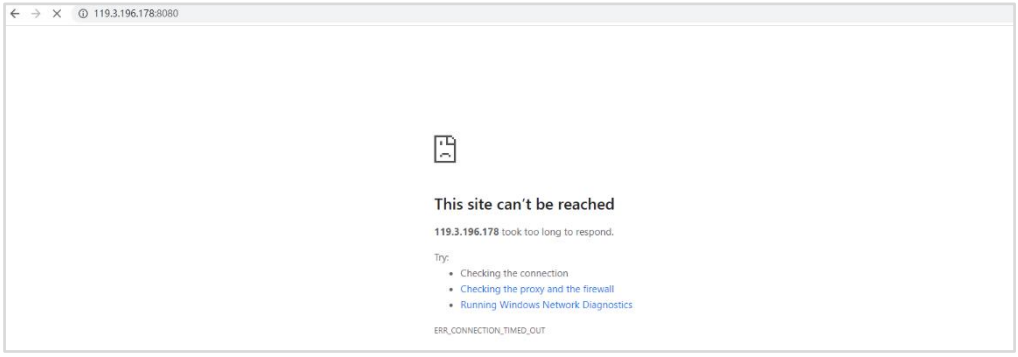


图5-46

步骤 6 在安全组中重新添加 8080 端口允许规则。

图5-47

步骤 7 重新刷新浏览器页面，发现可以登录。证明通过上一步骤配置，安全组 sg-dvwa 已允许 8080 端口访问。通过这一小节内容我们验证了安全组的基本功能和使用。

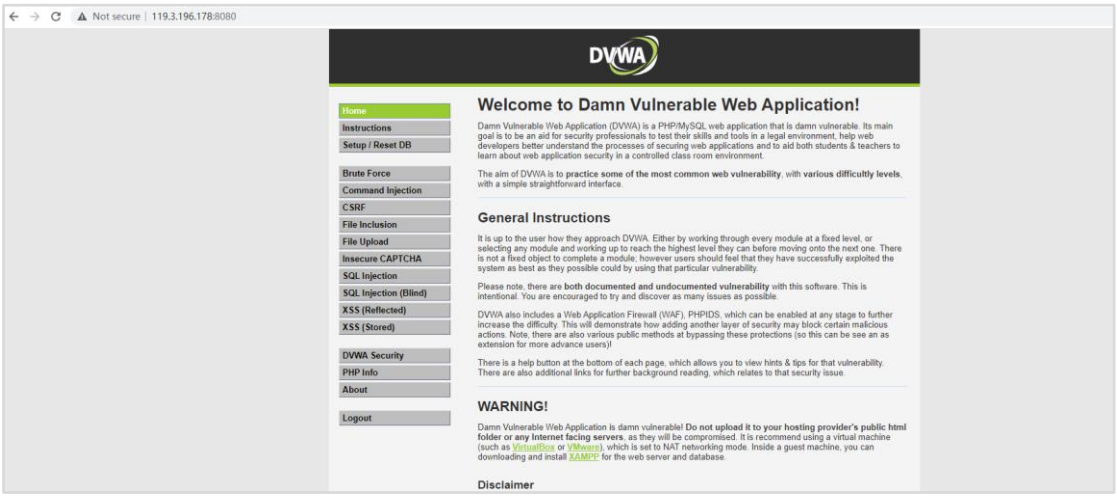


图5-48

5.2.5 IP 地址组

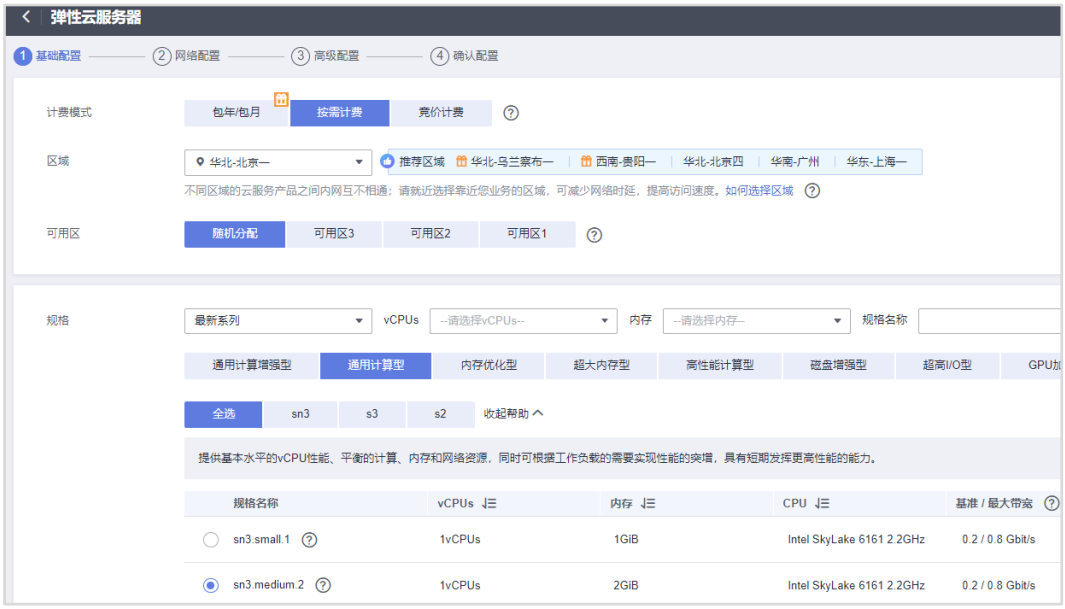
在对主机进行访问控制时，如果涉及对多个 IP 配置相同的安全组策略，可以通过配置 IP 地址组的方式来满足此需求。

步骤 1 参考“DVWA 主机部署”中步骤 3-4，在同 VPC 同子网内创建一台测试云主机。

说明：该云主机在本实验中仅作为连通性测试、验证主机，不参与应用部署。

云主机“test”配置：

- 计费模式：按需计费
- 区域：华北-北京一
- 可用区：随机分配
- CPU 架构：x86 计算
- 规格：1 vCPUs | 2 GiB
- 镜像：公共镜像 | CentOS 7.6 64 bit
- 主机安全：开通主机安全（基础版）
- 网络：vpc-1 | subnet-20 | 自动分配 IP 地址（选择与 ecs-dvwa 云主机相同的网络）
- 安全组：default（选择与 ecs-dvwa 云主机不同的安全组）
- 弹性公网 IP：暂不购买
- 系统盘：高 IO | 40 GiB
- 云服务器名称：test
- root 密码：自定义



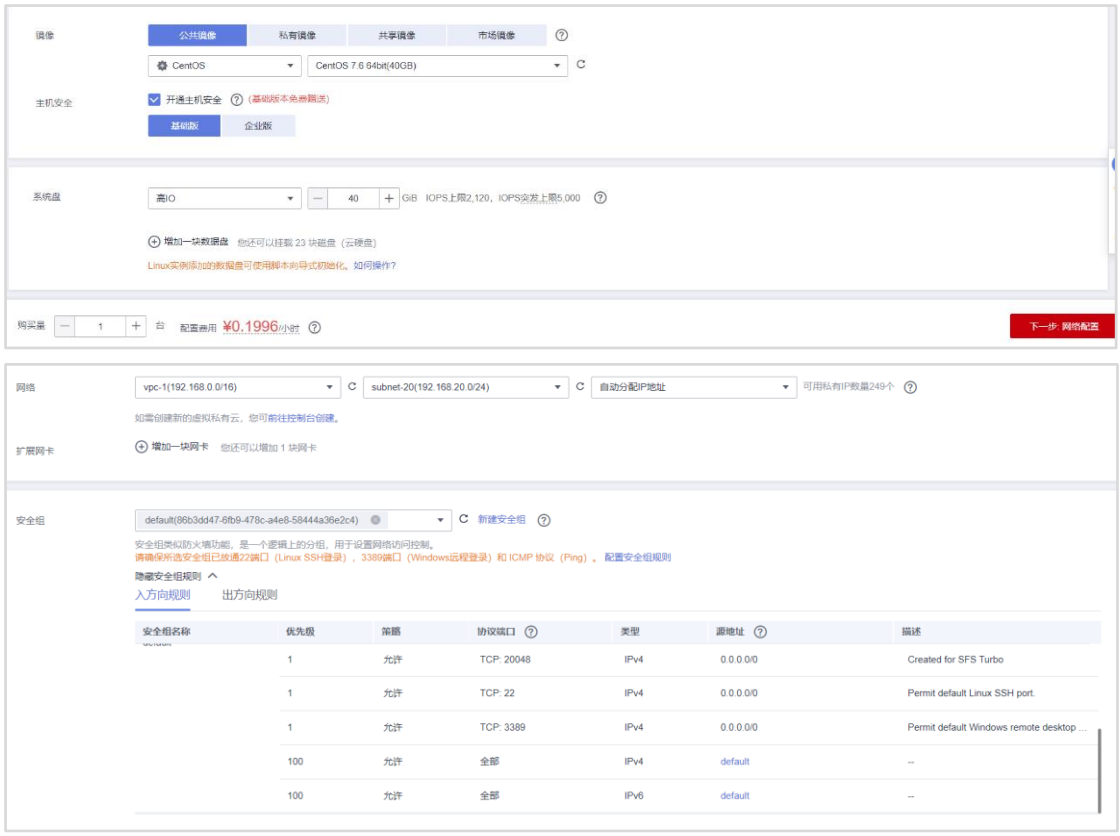


图5-49

步骤 2 使用华为云 CloudShell 登录该测试主机。

图5-50

步骤 3 使用“ping”命令测试与云主机 test，与 DVWA 主机的连通性。

说明：在配置地址组之前首先确保两台云主机可以互相通信。

```
test login: root
Password:

       Welcome to Huawei Cloud Service

[root@test ~]# ping 192.168.20.51
PING 192.168.20.51 (192.168.20.51) 56(84) bytes of data.
64 bytes from 192.168.20.51: icmp_seq=1 ttl=64 time=0.947 ms
64 bytes from 192.168.20.51: icmp_seq=2 ttl=64 time=0.190 ms
^C
--- 192.168.20.51 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.190/0.568/0.947/0.379 ms
[root@test ~]#
```

图5-51

步骤 4 使用“ifconfig”命令查看当前云主机 test 的 IP 地址并记录。

说明：后续需要将该 IP 地址加入地址组中。

```
[root@test ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.20.221  netmask 255.255.255.0  broadcast 192.168.20.255
        inet6 fe80::f816:3eff:fe9e:992e  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:9e:99:2e  txqueuelen 1000  (Ethernet)
        RX packets 14075  bytes 20382056 (19.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1472  bytes 118992 (116.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

图5-52

步骤 5 在网络控制台中选择“访问控制>IP 地址组”，点击右上方“创建 IP 地址组”。

说明：后续该地址组将被加入安全组中用于流量阻断测试。

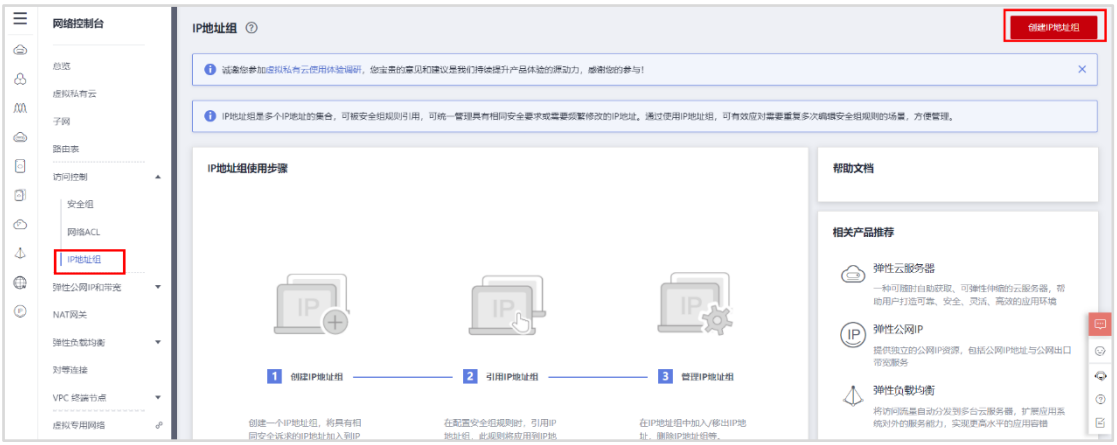


图5-53

步骤 6 按照如下配置完成地址组创建。

- 地址组名称：test
- IP 地址：云主机 test 的私网 IP 地址

图5-54

步骤 7 在安全组列表中，选择之前创建的“sg-dvwa”安全组对应操作栏的“配置规则”。

图5-55

步骤 8 选择“入方向规则”并点击“添加规则”，按照以下配置，将配置好的 IP 地址组加入该入方向规则中。

- 优先级：1
- 策略：拒绝
- 协议端口：ICMP|全部
- 源地址：IP 地址组|test

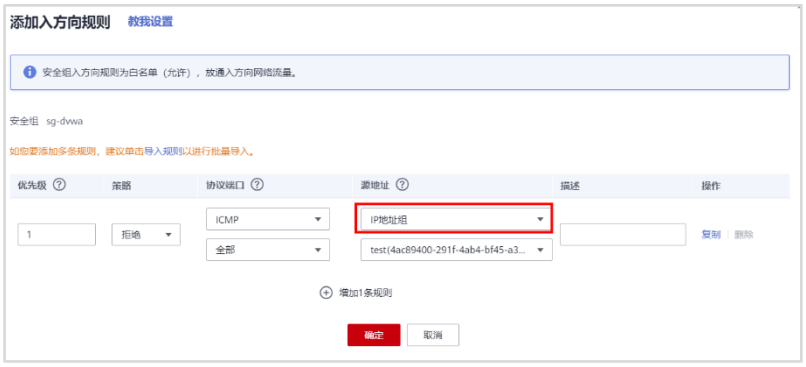


图5-56

步骤 9 再次登录云主机 test，重新测试云主机 test 与 DVWA 云主机连通性，发现已无法通信。证明通过以上配置，安全组内配置的地址组规则已经生效并成功阻断了相应请求。通过这一小节内容我们验证了地址组配合安全组的使用原理。

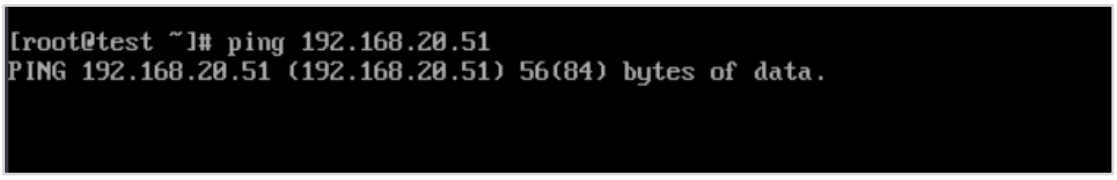


图5-57

5.2.6 Web 应用防火墙

再次提醒：实验开始前，需要提交工单申请开通独享 WAF，再进行实验。

5.2.6.1 使用 DVWA 进行攻击测试

步骤 1 参照之前步骤使用浏览器登录 DVWA 页面。选择“XSS（Reflected）”选项。

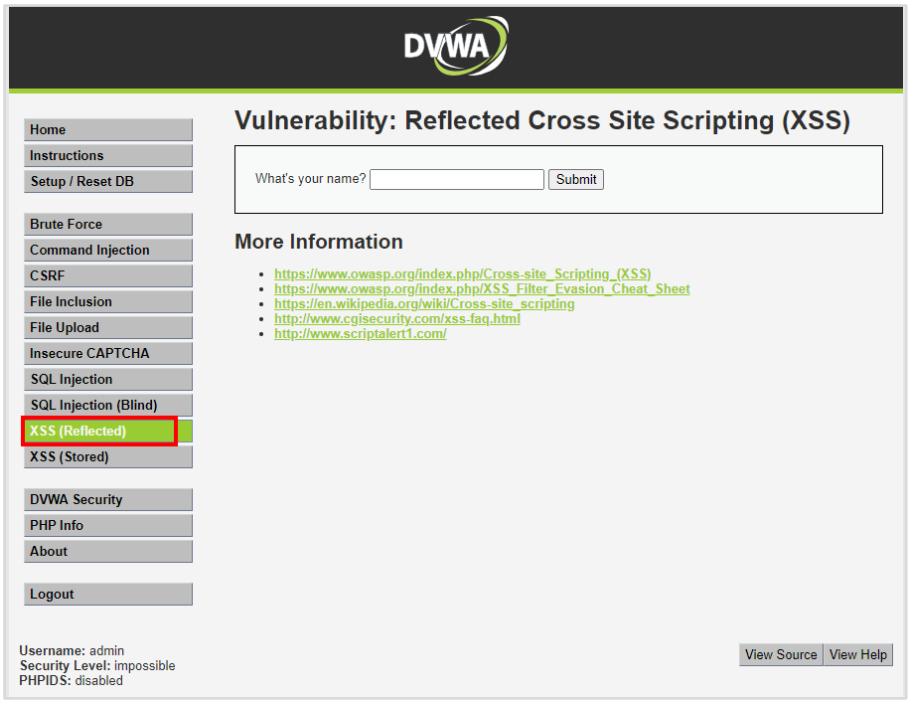


图5-58

步骤 2 在右边输入栏中输入以下字符并点击“submit”。

说明：以下字符内容用来模拟 XSS 攻击。

```
"></input><script>alret(1746)</script><input>
```

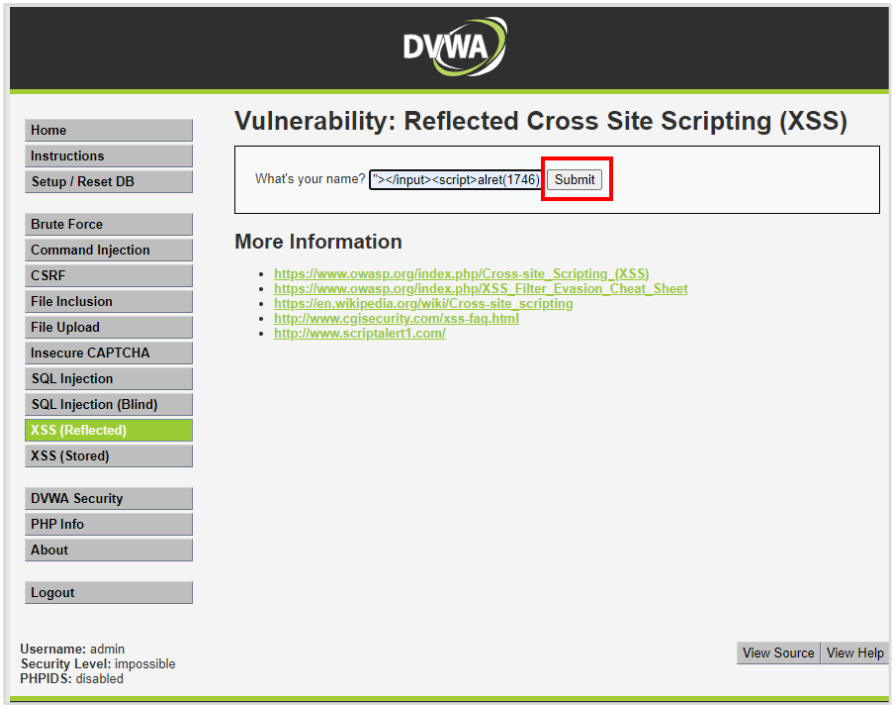


图5-59

步骤 3 看到页面中有如下回显，证明模拟攻击成功（页面回显直接打印之前输入的内容）。

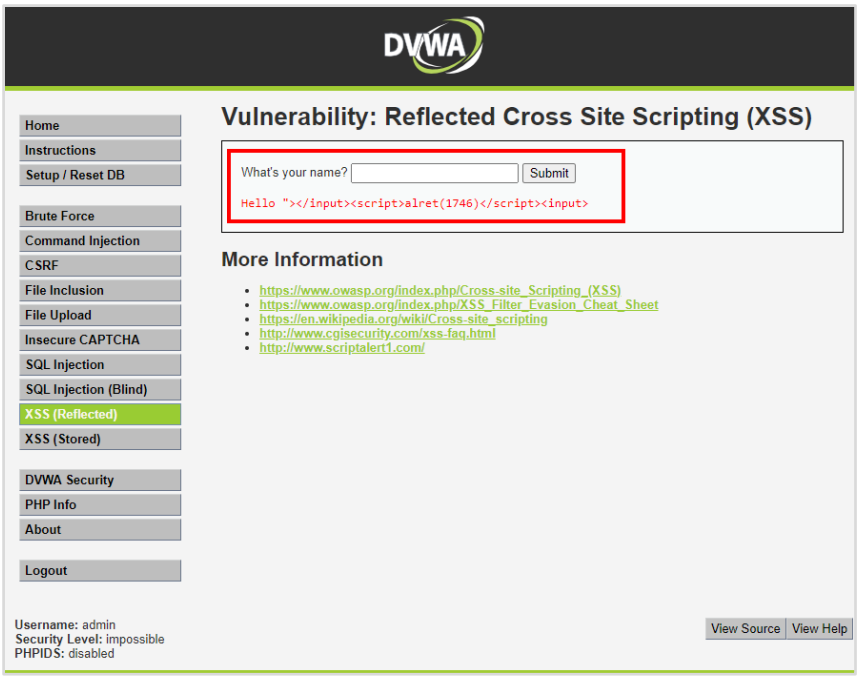
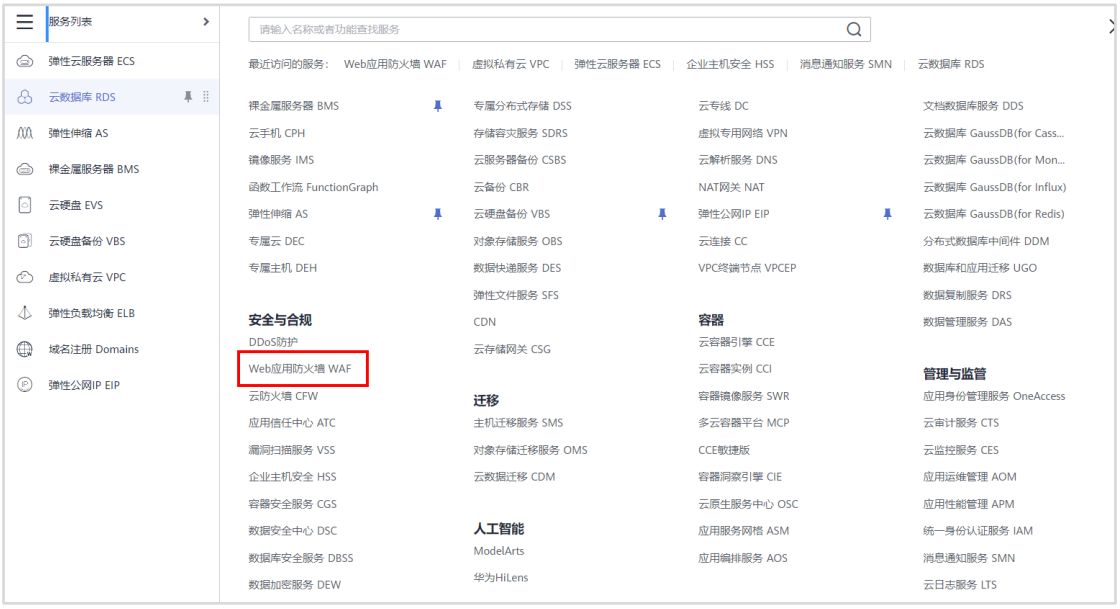


图5-60

5.2.6.2 创建 WAF

步骤 1 在服务列表中选择“Web 应用防火墙 WAF”，并点击购买。

说明：本实验中需要使用该 WAF 实例进行 XSS 攻击防护，阻断上一步骤中的攻击。



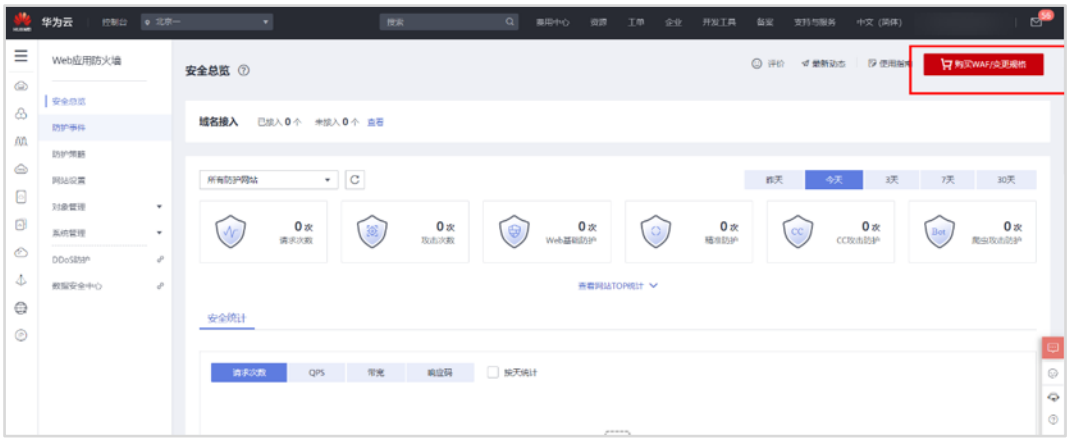


图5-61

步骤 2 选择独享模式（需要提交工单开通独享 WAF，再进行购买），按照以下配置购买 WAF 实例。

- 计费模式：按需计费
- 区域：华北-北京一
- 可用区：可用区 1
- WAF 实例名称前缀：test
- WAF 实例规格：WI-500
- WAF 实例创建类别：普通租户类（说明：本实验使用北京一区域创建，无需选择该参数，使用其他区域进行实验时，如果需要选择创建类别，请选择普通租户类。）
- CPU 架构：X86 计算
- ECS 规格：8 vCPUs|16 GB
- 虚拟私有云：vpc-1
- 子网：vpc-20
- 安全组：sg-dvwa

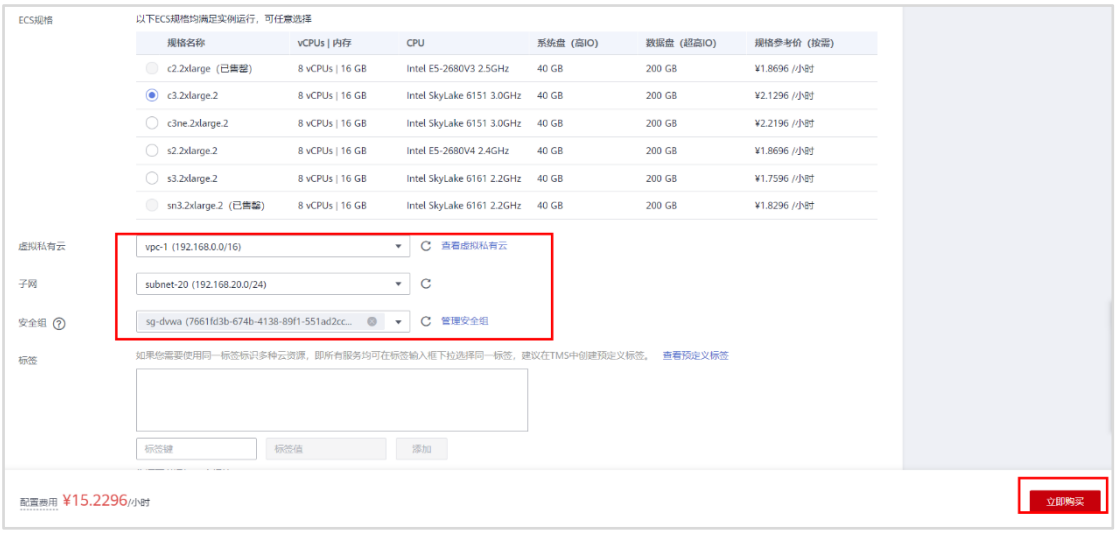


图5-62

说明：选择与 DVWA 云主机相同的 VPC、子网和安全组。

5.2.6.3 创建防护策略

步骤 1 在独享引擎列表中点击刚创建的实例名称。

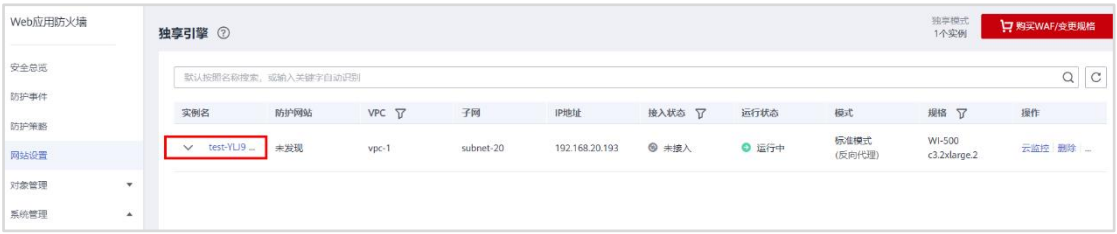


图5-63

步骤 2 在“防护策略”页签中选择“添加防护策略”。

图5-64

步骤 3 设置防护策略名称为“test”，点击“确定”。

图5-65

步骤 4 点击创建的防护策略名称。

图5-66

步骤 5 在“防护配置”中将防护模式修改为“拦截”。

说明：默认防护配置中模式为“仅记录”，实验现象不明显，这里需要改为拦截。

图5-67

5.2.6.4 添加防护网站

步骤 1 在“网站设置”中添加防护网站。其中防护域名填写 DVWA 云主机的 EIP 地址，端口选择 8080，服务器配置中源站地址配置为 DVWA 云主机 VPC 内私网地址。

防护网站配置：

- 网站名称：test
- 防护域名：119.3.196.178（DVWA 云主机的 EIP 地址）
- 端口：8080
- 对外协议：HTTP

- 源站协议：HTTP
- VPC：vpc-1
- 源站地址：IPv4|192.168.20.51
- 源站端口：8080

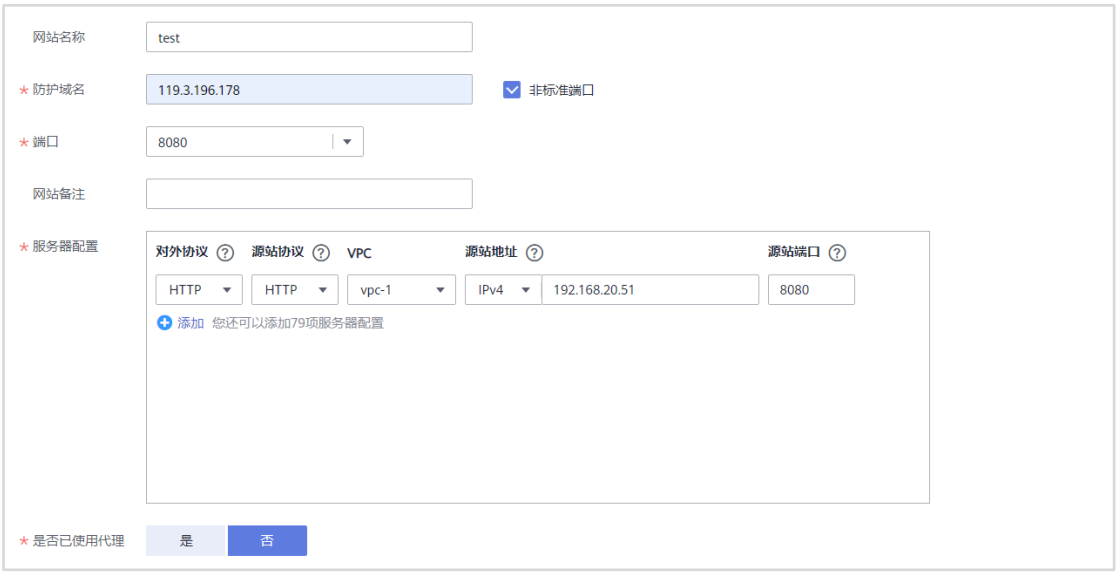


图5-68

- 选择防护策略为之前创建的“test”并点击“确定”。

图5-69

步骤 2 在防护网站列表页面中可以看到当前创建的防护网站为“未接入”状态。

说明：独享 WAF 需要将 WAF 实例接入 WAF 负载均衡器中，这里的接入状态才会正常。

图5-70

5.2.6.5 创建 WAF 负载均衡器

步骤 1 在云主机列表界面将 DVWA 云主机的弹性公网 IP 地址解除绑定。

说明：后续需要将该 EIP 绑定至负载均衡器中。

图5-71

步骤 2 在弹出的对话框中点击“是”。

图5-72

步骤 3 在网络控制台中选择“负载均衡器”并点击右上角“购买弹性负载均衡”。

说明：该负载均衡器将作为 WAF 实例的负载均衡器。

图5-73

步骤 4 按照以下配置完成负载均衡器创建。

- 实例规格类型：共享型
- 区域：“华北-北京一”
- 网络类型：公网
- 所属 VPC：vpc-1
- 子网：subnet-20
- 私有 IP 地址：自动分配 IP 地址

图5-74

- 弹性公网 IP：使用已有（选择刚从云主机 ecs-dvwa 上解绑的 EIP。）
- 名称：elb-waf

图5-75

步骤 5 在弹性负载均衡器列表中，点击负载均衡器 elb-waf 对应的“点我开始配置”。

图5-76

步骤 6 按照以下内容完成负载均衡器配置。

负载均衡器配置：

- 监听器名称：listener-waf
- 前端协议：TCP
- 前端端口：8080

图5-77

- 后端服务器组：新创建
- 名称：server_group-waf
- 后端协议：TCP
- 分配策略类型：加权轮询算法

图5-78

- 点击“添加云服务器”。

图5-79

- 将之前创建的独享 WAF（test-YLJ9）实例加入后端服务器。

图5-80

- 批量添加端口：8080
- 其他配置：默认配置

图5-81

步骤 7 确认配置后提交，在负载均衡器列表页面可以查看当前创建的负载均衡器，如下图所示，证明负载均衡器已创建完成。

图5-82

5.2.6.6 接入防护网站

步骤 1 在 Web 应用防火墙页面中，选择“网站设置”页签，点击右侧“接入状态”栏下方的刷新图标。

图5-83

步骤 2 刷新后接入状态变为“已接入”。

图5-84

5.2.6.7 攻击测试

步骤 1 使用本地浏览器登录 DVWA 主机 EIP 地址，例如：http://119.3.196.178:8080。

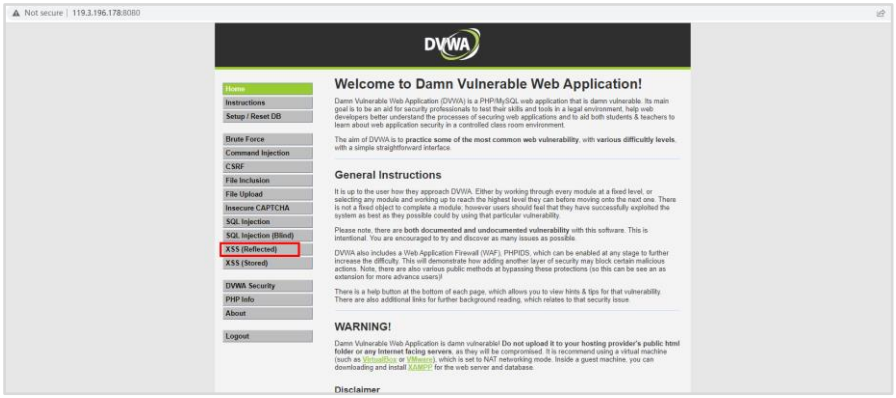


图5-85

步骤 2 选择“XSS（Reflected）”选项。

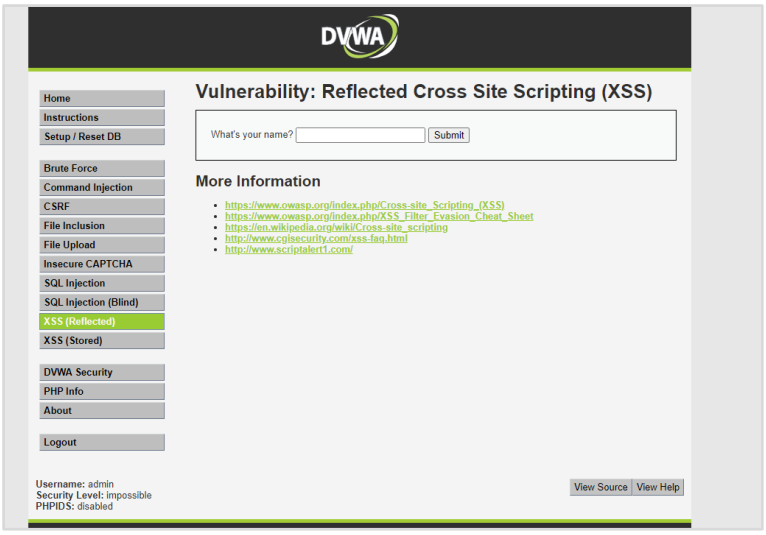


图5-86

步骤 3 在右边的输入框中输入以下字符，并点击右侧“submit”按钮。

```
"></input><script>alret(1746)</script><input>
```

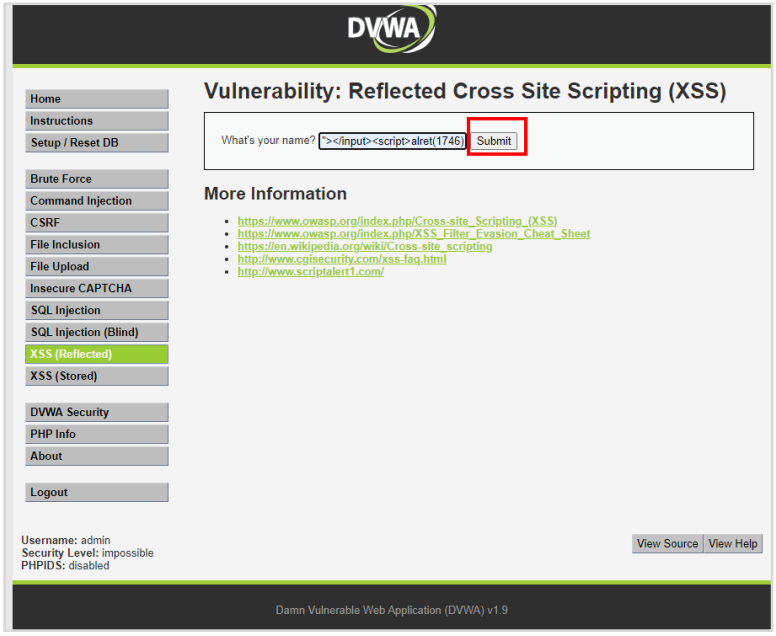


图5-87

步骤 4 返回防护网站列表，查看当前已防御了一次攻击。

图5-88

步骤 5 在 Web 应用防火墙的“安全总览”中可查看当前防护事件，可查看到防护域名为 DVWA 云主机 EIP 的事件条目。

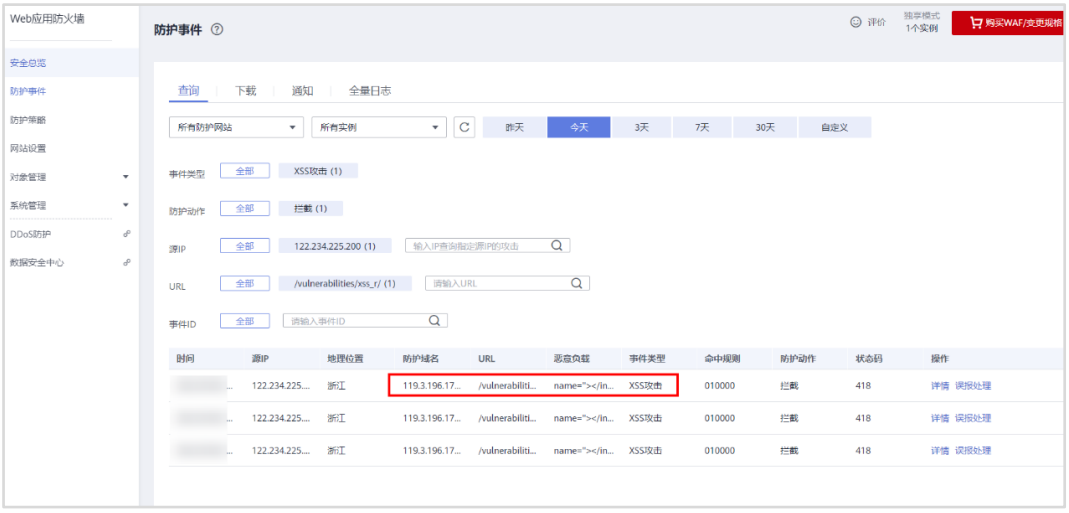


图5-89

步骤 6 点击该事件条目可查看事件详细信息，可以看到恶意负载中我们输入的模拟攻击内容。证明通过以上 Web 应用防火墙的配置，成功阻断了我们进行的模拟 XSS 攻击。通过本小节内容我们验证了 Web 应用防火墙的使用原理。

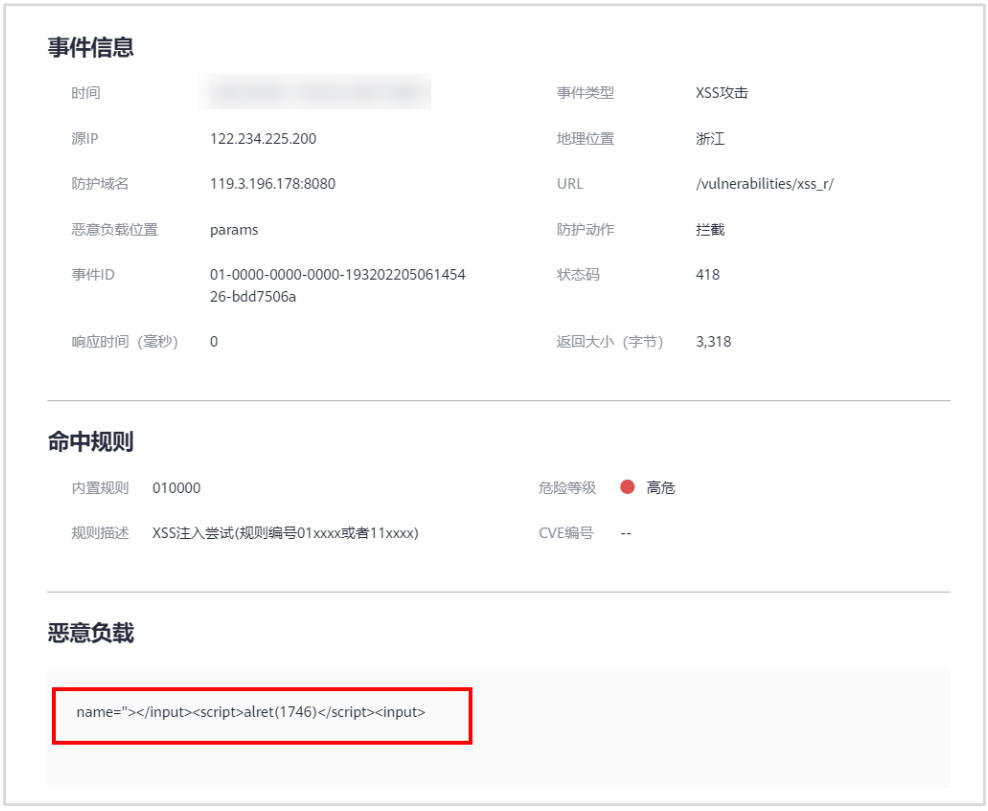


图5-90

5.2.7 DEW 托管密钥

5.2.7.1 获取 AK/SK

说明：后续 KooCLI 初始化中需要用到此处获取的 AK/SK。

步骤 1 点击右上方用户名，在下拉菜单中选择“我的凭证”。

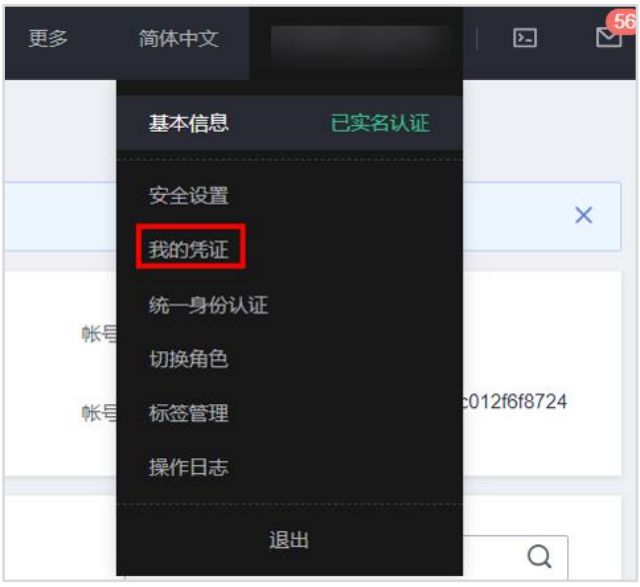


图5-91

步骤 2 在“访问密钥”页签中选择“新增访问密钥”。

图5-92

步骤 3 填入相应描述（学员可自定义）后点击“确定”。

图5-93

步骤 4 创建成功后点击“立即下载”。

图5-94

步骤 5 在本地保存好 AK/SK 备用。

图5-95

5.2.7.2 创建凭据

说明：该凭据托管在 DEW 中，后续需要被 ECS 服务通过 KooCLI 客户端获取。

步骤 1 在服务列表中选择“数据加密服务 DEW”。

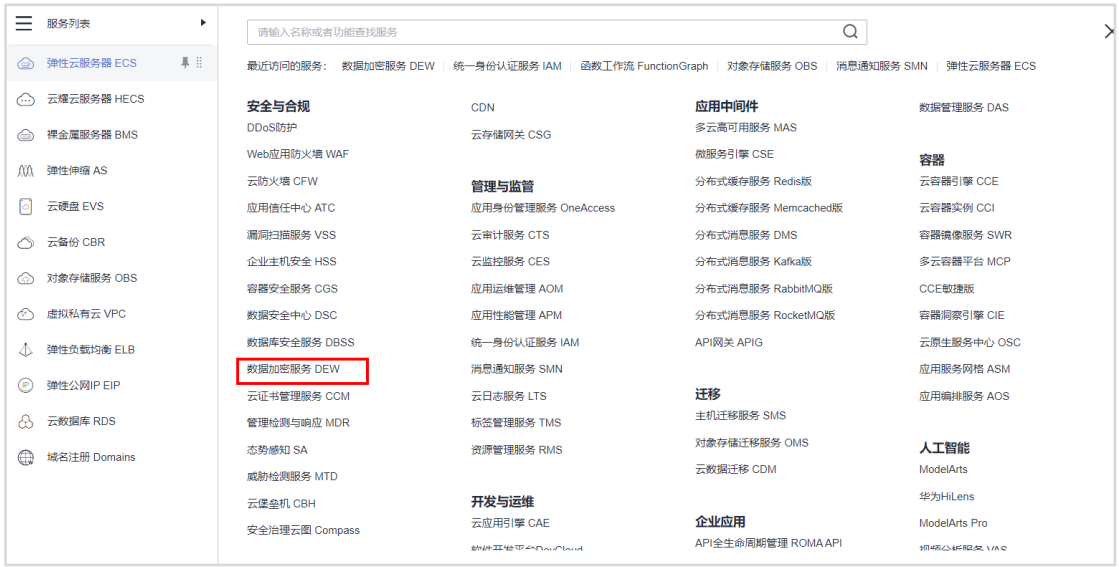


图5-96

步骤 2 在“凭据管理”页签中点击“创建凭据”。

图5-97

步骤 3 按照下图配置完成凭据创建。

- 凭据名称：test
- 设置凭据值：明文|HCIP@123（学员可自定义）
- 其他配置：默认配置

图5-98

步骤 4 点击凭据名称，可查看凭据详细信息，可以注意到当前凭据版本为 v1。

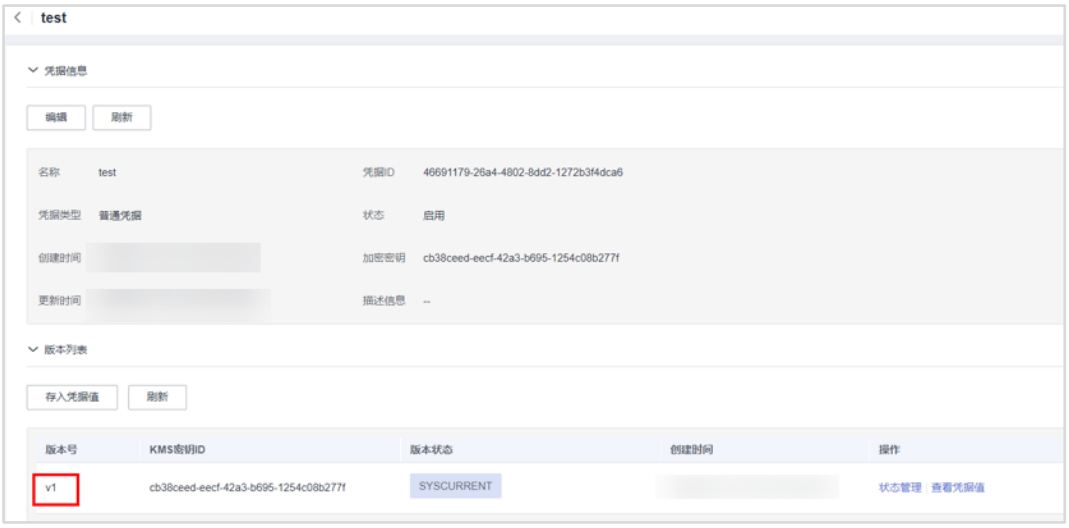


图5-99

5.2.7.3 创建委托

说明：需要通过该委托，赋予 ECS 服务相应权限，使得其可以通过 KooCLI 获取 DEW 中托管的密钥。

步骤 1 点击右上方用户名，在下拉菜单中选择“统一身份认证”。

图5-100

步骤 2 选择“委托”页签，点击右上角“创建委托”。

图5-101

步骤 3 按照以下配置创建委托并点击“下一步”。

- 委托名称：ECS-password
- 委托类型：云服务
- 云服务：弹性云服务器 ECS 裸金属服务器 BMS
- 持续时间：永久

图5-102

步骤 4 在策略选择中，选择“CSMS FullAccess”和“KMS CMKFullAccess”权限。

图5-103

步骤 5 最小授权范围保持默认，点击“确定”。

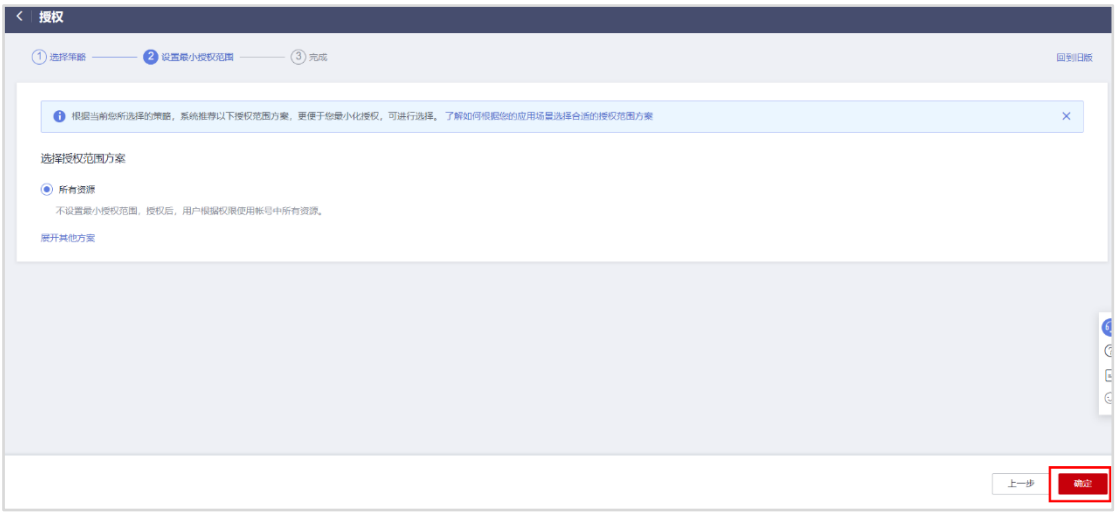


图5-104

步骤 6 创建完成后可在授权记录页签下查看当前委托的授权。

图5-105

5.2.7.4 KooCLI 安装

步骤 1 参照 DVWA 主机部署步骤 3-4 创建云主机 ecs-test（如果 5.2.5 步骤中创建的云主机 test 还未释放，可直接复用）。

说明：该云主机仅用于 KooCLI 安装及获取密钥测试。

云主机“ecs-test”配置：

- 计费模式：按需计费
- 区域：华北-北京一
- 可用区：随机分配
- CPU 架构：x86 计算
- 规格：1 vCPUs | 2 GiB
- 镜像：公共镜像 | CentOS 7.6 64 bit
- 主机安全：开通主机安全（基础版）
- 网络：vpc-1 | subnet-20 | 自动分配 IP 地址
- 安全组：default

- 弹性公网 IP：现在购买
- 线路：全动态 BGP
- 公网带宽：按流量计费
- 带宽大小：10 Mbit/s
- 系统盘：通用型 SSD | 40 GiB
- 云服务器名称：ecs-test
- root 密码：自定义

步骤 2 使用华为 CloudShell 登录云主机 ecs-test，使用以下命令安装 KooCLI 客户端。

```
[root@ecs-test ~]# curl -sSL https://hwcloudcli.obs.cn-north-1.myhuaweicloud.com/cli/latest/hcloud_install.sh -o ./hcloud_install.sh && bash ./hcloud_install.sh –y
```

图5-106

步骤 3 使用如下命令进行初始化配置，并输入 5.2.7.1 步骤中保存的 AK/SK。

```
[root@ecs-test ~]# hcloud configure init
Access Key ID [required]: 输入 AK
Secret Access Key [required]: 输入 SK
Region Name: 输入域名称，例如 cn-north-1
```

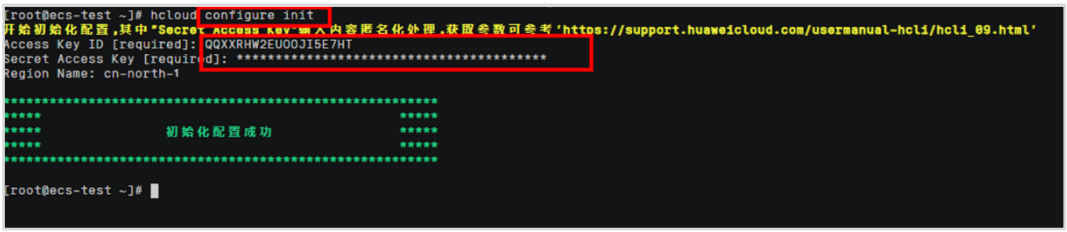


图5-107

5.2.7.5 使用 KooCLI 获取密钥

步骤 1 使用如下命令进入 KooCLI 交互模式。

```
[root@ecs-test ~]# hcloud –interactive
```

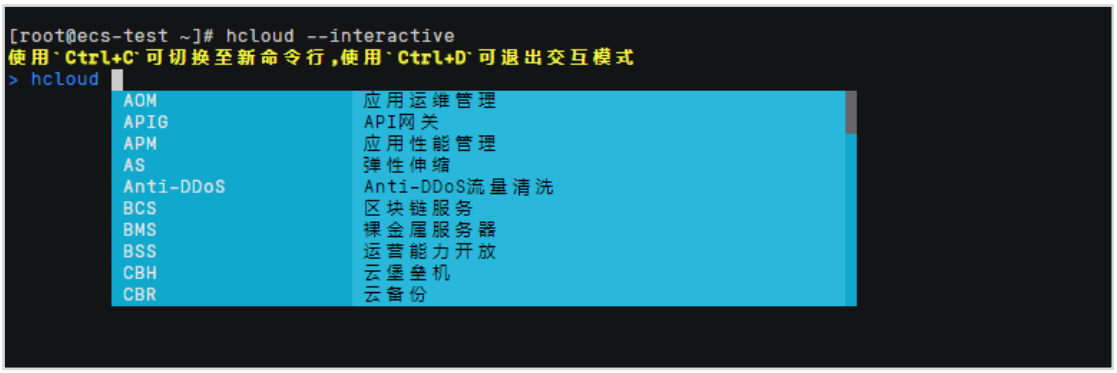


图5-108

步骤 2 使用如下命令查看之前在 DEW 中创建的密钥信息。如下图所示，可以看到已获取到密钥“HCIP@123”，证明通过以上配置，ECS 服务可以通过 KooCLI 客户端获取托管在 DEW 中的密钥信息。

```
> hcloud csms ShowSecretVersion --secret_name=test --version_id=v1 --cli-region="cn-north-1"
# --secret_name=创建的密钥名称
# --version_id=密钥的版本号
# --cli-region="当前所在区域"
```

图5-109

5.3 实验恢复

步骤 1 删除委托。

- 点击右上方用户名，在下拉菜单中选择“统一身份认证”。

图5-110

- 选择“委托”页签，在委托列表中找到本实验创建的委托，点击对应操作栏中的“删除”。

步骤 2 删除凭据。

- 在服务列表中选择“数据加密服务 DEW”，在左侧页签中选择“凭据管理”，在凭据列表中找到本实验创建的凭据，点击操作栏中的“删除”。
- 在弹出的对话框中勾选“立即删除”，点击“确定”。

步骤 3 删除 WAF。

- 在服务列表中选择“Web 应用防火墙 WAF”，在左侧页签中选择“防护网站”，点击对应操作栏中的“删除”。
- 在左侧页签中选择“防护策略”，找到本实验创建的防护策略，点击操作栏中的“删除”。
- 在左侧页签中选择“系统管理>独享引擎”，找到本实验创建的独享引擎，点击操作栏中的“删除”。

步骤 4 删除 ECS。

- 在服务列表中选择“云服务器 ECS”，找到本实验创建的云服务器，点击操作栏中的“更多>删除”。
- 在弹出的对话框中勾选下图中选项，点击“是”。

图5-111

步骤 5 删除双因子认证。

- 在服务列表中选择“企业主机安全 HSS”，在企业主机安全页面中，点击“安装与配置”页签，选择“双因子认证>开启双因子认证”，选择对应操作栏的“删除”。

步骤 6 删除 SMN 主题。

- 在服务列表中选择“消息通知服务 SMN”，在左侧页签中选择“主题管理>主题”，在右侧列表中找到本实验创建的主题，点击操作栏中的“更多>删除”。

步骤 7 删除地址组。

- 在服务列表中选择“虚拟私有云 VPC”，在“访问控制>IP 地址组”中找到本实验创建的地址组，点击操作栏的“删除”。

步骤 8 删除安全组。

- 在服务列表中选择“虚拟私有云 VPC”，在“访问控制>安全组”中找到本实验创建的安全组，点击操作栏的“更多>删除”。

步骤 9 删除 VPC。

- 在服务列表中选择“虚拟私有云 VPC”，点击“子网”页签，在列表中找到本实验创建的子网，点击操作栏中的“删除”。
- 点击“虚拟私有云”页签，找到本实验创建的 VPC，点击操作栏中的“删除”。

5.4 思考题

问题：企业版 HSS 除了可以做到实时入侵检测，还支持哪些功能?

参考答案：还支持病毒木马查杀、基线检查、漏洞一键修复、安全配置等功能。

6 容器应用部署实验

6.1 实验介绍

6.1.1 关于本实验

本实验分为以下两部分：

1.设计通过弹性云服务器 ECS 部署 Docker 引擎并部署容器提供 Web 服务，通过 Dockerfile 构建当前镜像并上传容器镜像服务（SoftWare Repository for Container，简称 SWR）。考虑需要测试已上传的镜像是否可用，设计通过云容器引擎（Cloud Container Engine，简称 CCE）拉取刚上传的镜像并部署，使用本地浏览器登录云容器引擎节点 EIP 验证 Web 页面是否正常。

2.设计通过函数工作流刷新对象存储桶内对象版本，做到在桶内始终只保留最新的 3 个版本数据。

说明：本实验以“北京一”和“上海一”区域为例，学员可以根据实际情况选择相应区域进行实验。

6.1.2 实验目的

掌握 Docker 引擎的使用原理和配置方法。

掌握容器镜像服务 SWR 的使用原理和配置方法。

掌握云容器引擎 CCE 的使用原理和配置方法。

掌握函数工作流 FunctionGraph 的配置方式和使用原理。

6.1.3 实验组网

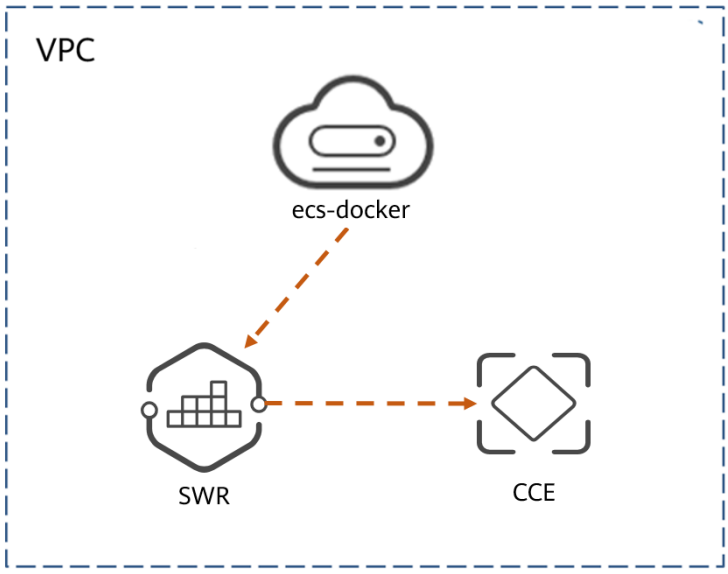


图6-1 容器实验组网

6.1.4 软件介绍

Docker 是一个开源的应用容器引擎，让开发者可以打包他们的应用以及依赖包到一个可移植的镜像中，然后发布到任何流行的 Linux 或 Windows 操作系统的机器上。

httpd 是 Apache 超文本传输协议（HTTP）服务器的主程序。它被设计为一个独立运行的后台进程，会建立一个处理请求的子进程或线程的池。

6.2 实验配置

6.2.1 容器部署&CCE

6.2.1.1 创建 VPC

步骤 1 点击控制台，选择“华北-北京一”区域。

步骤 2 在服务列表里，选择“虚拟私有云 VPC”。

步骤 3 点击右上角“创建虚拟私有云”（后续资源将在该 VPC 内创建）。

图6-2

步骤 4 按照以下要求填写参数，并点击“立即创建”。

- 区域：华北-北京一
- 名称：vpc-1
- IPv4 网段：192.168.0.0/16

默认子网

- 可用区：可用区 2
- 名称：vpc-1-subnet
- 子网 IPv4 网段：192.168.1.0/24

6.2.1.2 创建安全组

步骤 1 按照以下配置在“华北-北京一”创建安全组 sg-docker。

说明：该安全组供后续部署 Docker 引擎的云服务器使用。

- 名称：sg-docker
- 通用 Web 服务器

图6-3

6.2.1.3 创建云主机

步骤 1 按以下配置创建云主机 ecs-docker。

说明：该云主机用于部署 Docker 引擎。

云主机“ecs-docker”配置：

- 计费模式：按需计费
- 区域：华北-北京一

- 可用区：随机分配
- CPU 架构：x86 计算
- 规格：2 vCPUs | 4 GiB
- 镜像：公共镜像 | CentOS 7.6 64 bit
- 主机安全：开通主机安全（基础版）
- 网络：vpc-1 | vpc-1-subnet | 自动分配 IP 地址
- 安全组：sg-docker
- 弹性公网 IP：现在购买
- 线路：全动态 BGP
- 公网带宽：按流量计费
- 带宽大小：20 Mbit/s
- 系统盘：高 IO | 40 GiB
- 云服务器名称：ecs-docker
- root 密码：自定义

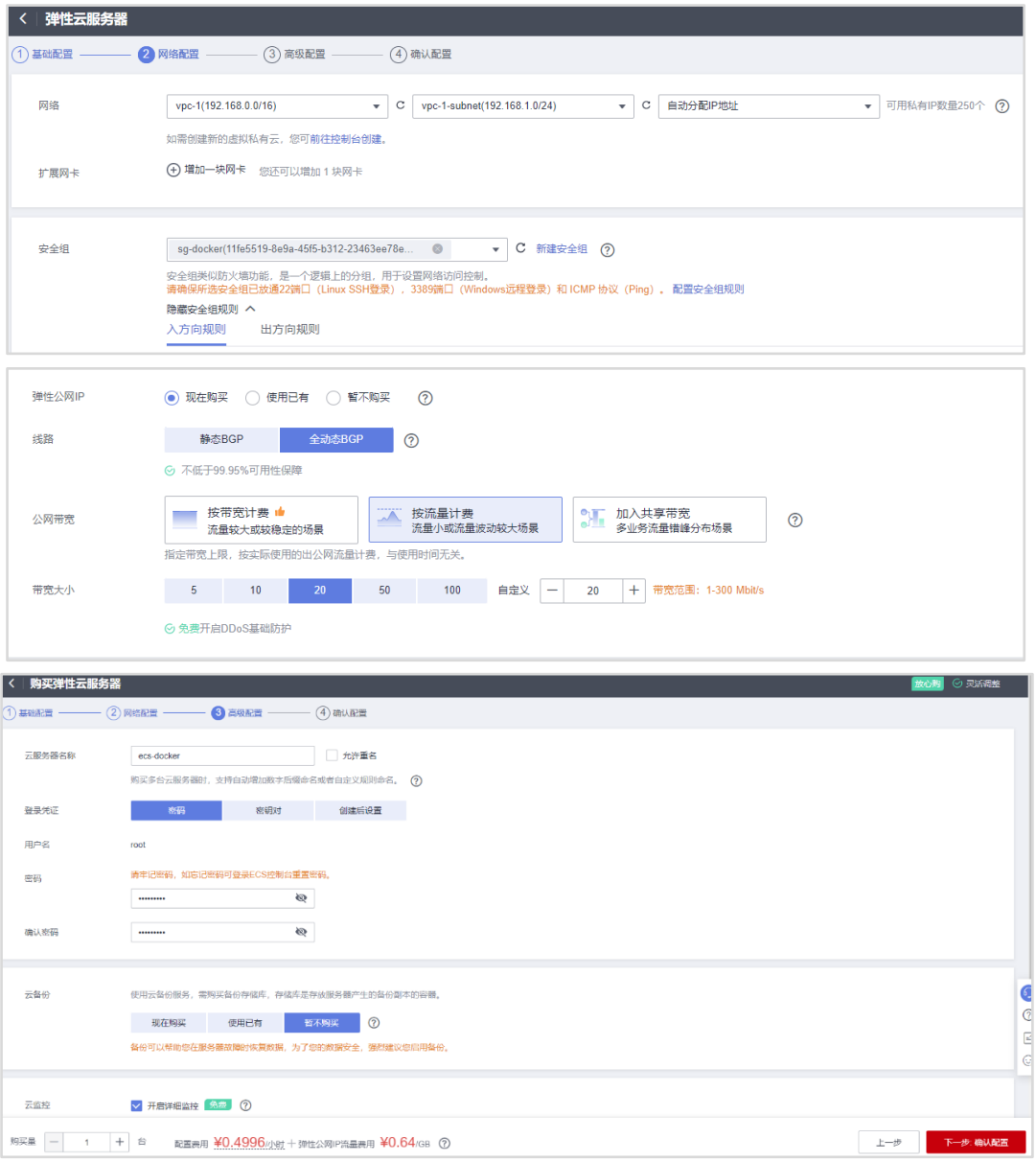


图6-4

6.2.1.4 安装部署 docker

步骤 1 使用华为云 CloudShell 登录云主机 ecs-docker。

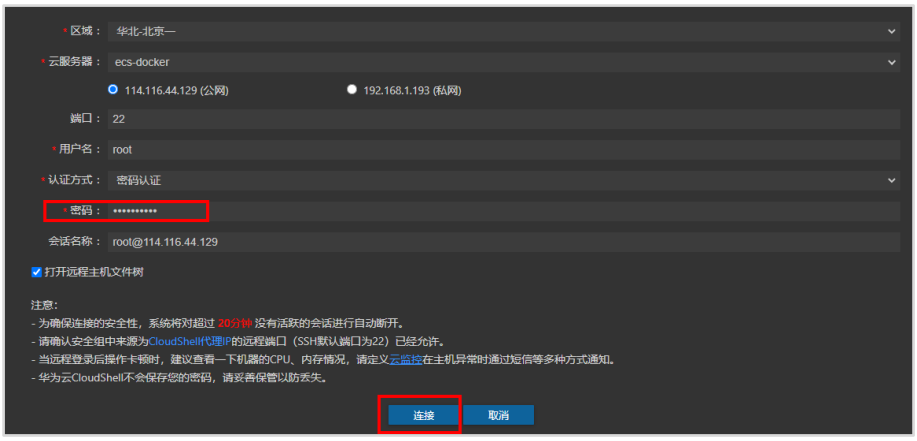


图6-5

步骤 2 使用如下命令安装 yum 单元。

说明：如果是非 root 用户，部分命令需要添加“sudo”执行。

```
[root@ecs-docker ~]# yum install -y yum-utils
```

图6-6

步骤 3 使用如下命令增加 yum 源赖。

```
[root@ecs-docker ~]# yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo
```

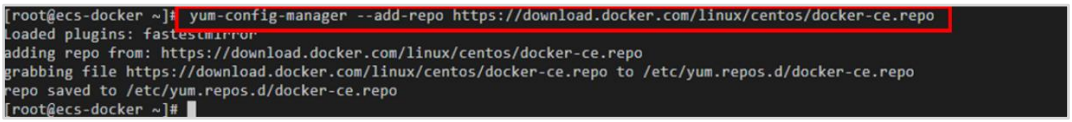


图6-7

步骤 4 使用如下命令安装 Docker。

```
[root@ecs-docker ~]# yum install docker-ce docker-ce-cli containerd.io
```

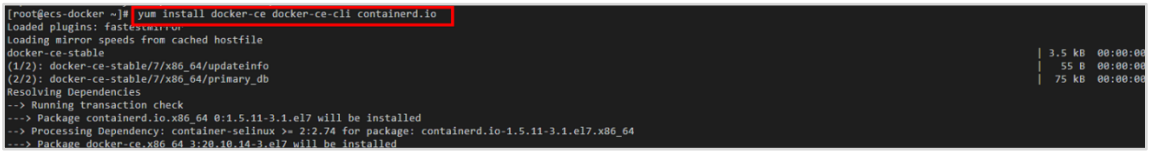
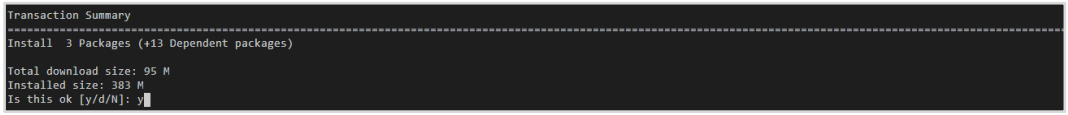


图6-8

步骤 5 连续两次输入“y”。



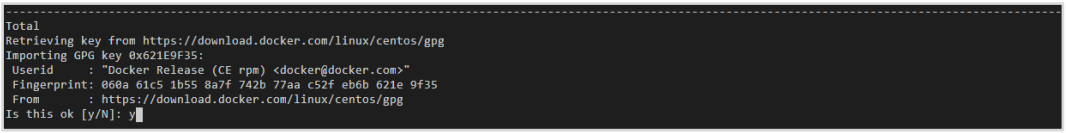


图6-9

步骤 6 当看到下图中的“Complete!”时，证明安装完成。

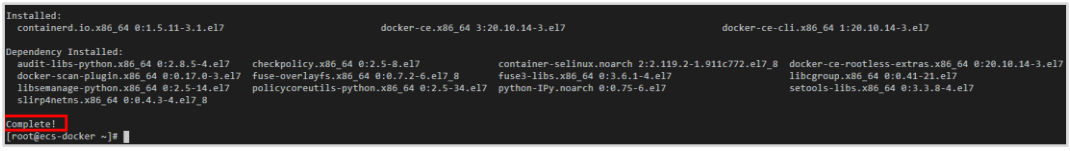


图6-10

步骤 7 使用如下命令启动 Docker。

```
[root@ecs-docker ~]# systemctl start docker
```

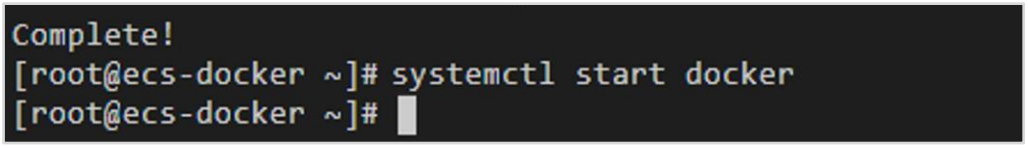


图6-11

步骤 8 使用如下命令测试 Docker 引擎工作是否正常。如下图所示，可以看到“Hello from Docker”字样，证明当前 Docker 引擎工作正常。

```
[root@ecs-docker ~]# docker run hello-world
```

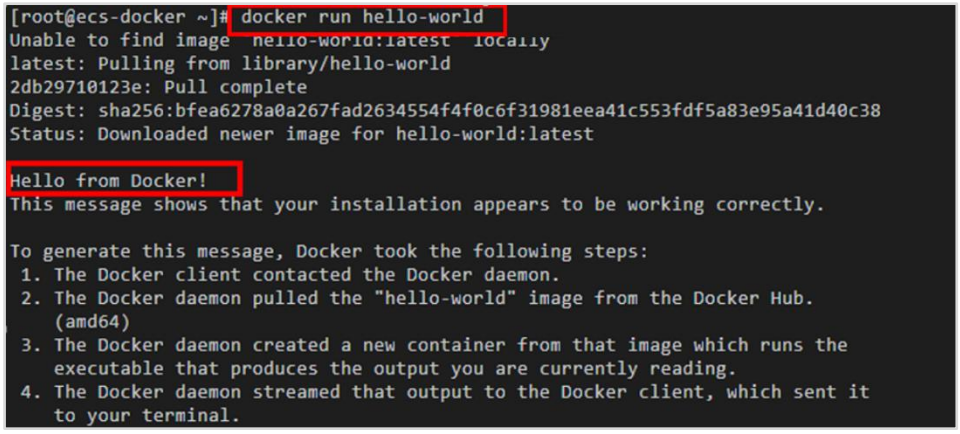


图6-12

步骤 9 使用如下命令配置镜像加速。

```
[root@ecs-docker ~]# vi /etc/docker/daemon.json
```

- 使用“i”键进入编辑模式，在该文件中输入：

```
{
  "registry-mirrors":["https://registry.docker-cn.com"]
}
```

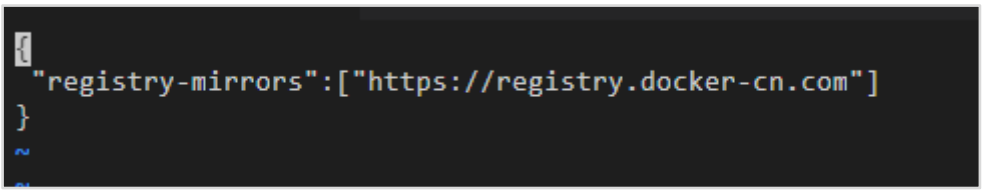


图6-13

步骤 10 使用 ESC 键退出编辑模式后，输入以下命令保存文件。

```
:wq
```

图6-14

步骤 11 使用以下命令重启 docker 进程。

```
[root@ecs-docker ~]# systemctl restart docker
```

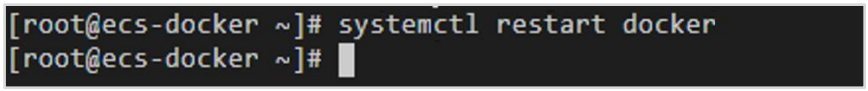


图6-15

步骤 12 使用如下命令验证是否配置成功。如下图所示，证明镜像加速配置成功。

```
[root@ecs-docker ~]# docker info
```

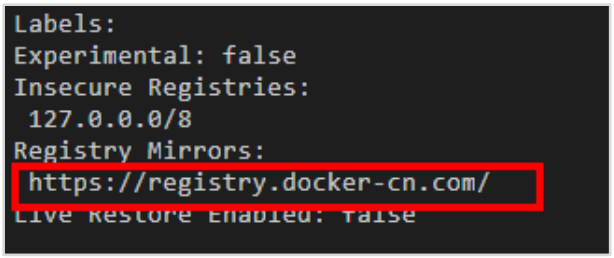


图6-16

6.2.1.5 拉取镜像，查看镜像

步骤 1 使用以下命令拉取 Nginx 镜像。

```
[root@ecs-docker ~]# docker pull nginx
```

图6-17

步骤 2 使用以下命令查看本地镜像。

```
[root@ecs-docker ~]# docker images
```

```
[root@ecs-docker ~]# docker images
REPOSITORY    TAG       IMAGE ID       CREATED         SIZE
nginx         latest    12766a6745ee   11 days ago     142MB
hello-world   latest    feb5d9fea6a5   6 months ago    13.3kB
[root@ecs-docker ~]#
```

图6-18

6.2.1.6 部署容器提供 Web 服务

步骤 1 使用如下命令拉取 httpd 镜像到本地。

```
[root@ecs-docker ~]# docker pull httpd
```

```
[root@ecs-docker ~]# docker pull httpd
Using default tag: latest
latest: Pulling from library/httpd
c229119241af: Already exists
1805d911aae4: Pull complete
e3709b515d9c: Pull complete
4f53b8f15873: Pull complete
3b60f356ab85: Pull complete
Digest: sha256:e3c40b99ffa305c6e52346a6618b1fb47ea0568c999b26f8900cd26febab1160
Status: Downloaded newer image for httpd:latest
docker.io/library/httpd:latest
[root@ecs-docker ~]#
```

图6-19

步骤 2 使用如下命令后台运行该镜像为容器，同时映射容器 80 端口到主机 80 端口。

```
[root@ecs-docker ~]# docker run -d -p 80:80 httpd
```

```
[root@ecs-docker ~]# docker run -d -p 80:80 httpd
511b4079be09f32c9d9406b8b83ea68bd78be2e803d0db0ae598dac03a9c6c30
[root@ecs-docker ~]#
```

图6-20

步骤 3 打开本地 PC 浏览器，登录该 ecs-docker 的公网地址。

图6-21

6.2.1.7 Dockerfile 构建镜像

步骤 1 使用以下命令进入该容器（让 CLI 变成这个容器的互动终端），查看 html 文件路径信息。

```
[root@ecs-docker ~]# docker container ls
[root@ecs-docker ~]# docker exec -it 511b4079be09    bash
```

说明：“511b4079be09”为容器 ID。

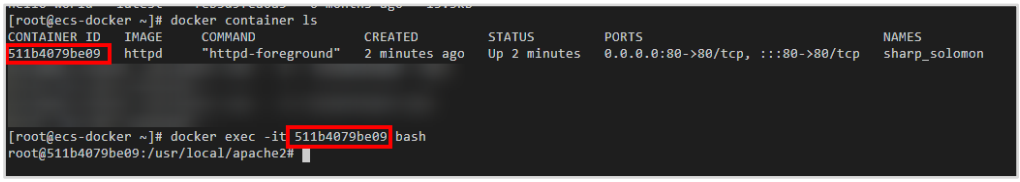


图6-22

步骤 2 通过“cat”命令在 htdocs 目录下查看 index.html 文件，发现网页内容“It works”。记录文件目录：/usr/local/apache2/htdocs。

```
root@511b4079be09:/usr/local/apache2# cd htdocs/
root@511b4079be09:/usr/local/apache2/htdocs# cat index.html
```

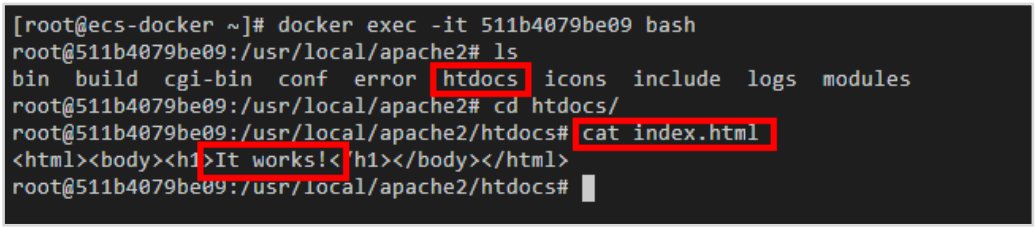


图6-23

步骤 3 使用“exit”命令退出容器后，执行如下命令在新路径中创建新 html 文件。

```
[root@ecs-docker ~]# mkdir -p /root/httpd
[root@ecs-docker ~]# cd    /root/httpd
```

图6-24

步骤 4 使用如下命令创建、编辑 html 文件，写入内容为“HCIP-Cloud Service”。

```
[root@ecs-docker httpd]# vi index.html                    #创建新 html 文件
HCIP-Cloud Service                                        #在 html 文件中填充内容
```

图6-25

步骤 5 使用如下命令创建并编辑 Dockerfile 文件。

```
[root@ecs-docker httpd]# vi Dockerfile                    #创建 Dockerfile 文件
FROM httpd
MAINTAINER huawei
COPY index.html /usr/local/apache2/htdocs                 #将当前目录下 html 文件覆盖至目标目录
```

```
[root@ecs-docker httpd]# vi Dockerfile
```

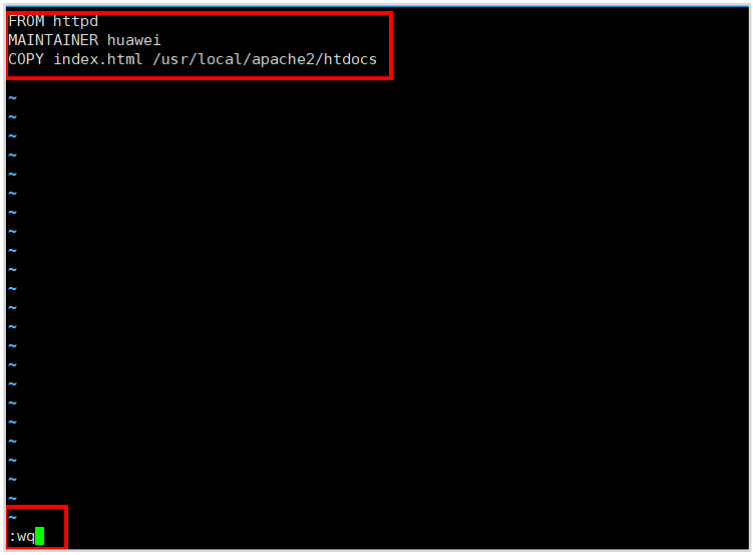


图6-26

步骤 6 使用如下命令使用当前 Dockerfile 文件构建新镜像 httpd2。

```
[root@ecs-docker httpd]# docker build -t   httpd2:v1 .
[root@ecs-docker httpd]# docker images
```

```
[root@ecs-docker ~]# docker images
REPOSITORY    TAG       IMAGE ID       CREATED          SIZE
httpd2        v1        8def57c4236d   30 minutes ago   144MB
httpd         latest    c30a46771695   2 days ago       144MB
hello-world   latest    feb5d9fea6a5   7 months ago     13.3kB
[root@ecs-docker ~]#
```

图6-27

步骤 7 使用如下命令关闭之前开启的 httpd 容器。

```
[root@ecs-docker ~]# docker ps -a                    #查看容器列表，找到 httpd 容器 ID
[root@ecs-docker ~]# docker stop e1                  #关闭 httpd 容器，”e1”是当前 httpd 容器 ID 简写
```

```
[root@ecs-docker ~]# docker ps -a
CONTAINER ID   IMAGE         COMMAND                  CREATED          STATUS
e1ee16e62c9a   httpd         "httpd-foreground"       37 minutes ago   Up 37 minutes
fee95e4f7d1c   hello-world   "/hello"                 42 minutes ago   Exited (0) 41 minutes ago
[root@ecs-docker ~]# docker stop e1
e1
```

图6-28

步骤 8 使用如下命令运行该镜像为容器。

```
[root@ecs-docker ~]# docker run -d -p 80:80 httpd2:v1
```

步骤 9 重新使用本地 PC 浏览器登录 ecs-docker 公网地址，查看内容，如下图所示，证明 Dockerfile 构建镜像成功。

图6-29

6.2.1.8 镜像上传 SWR

步骤 1 在服务列表中找到“容器镜像服务”，点击右上角“创建组织”。

说明：后续需要将制作好的镜像上传到该组织中。

图6-30

步骤 2 输入组织名称“hcip”（学员可自定义），点击“确定”。

图6-31

步骤 3 点击右上角“登录指令”来获取指令。

图6-32

步骤 4 复制该登录指令。

图6-33

步骤 5 使用华为云 CloudShell 登录 ecs-docker，执行刚记录的登录指令。

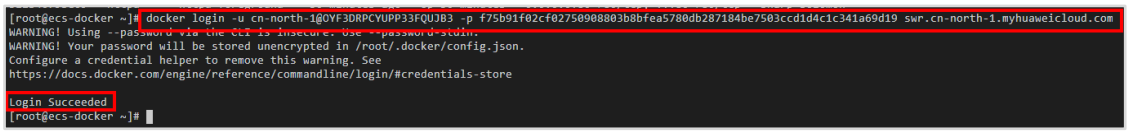


图6-34

步骤 6 显示登录成功后，在节点上使用如下命令查看 httpd2:v1 容器 ID。

```
[root@ecs-docker ~]# docker container ls
```

```
[root@ecs-docker ~]# docker container ls
CONTAINER ID   IMAGE       COMMAND              CREATED         STATUS         PORTS
          NAMES
f56106f9c554   httpd2:v1   "httpd-foreground"   2 minutes ago   Up 2 minutes   0.0.0.0:80->80/tcp, :::80->8
0/tcp   adoring_mcclintock
```

图6-35

步骤 7 将 httpd2:v1 容器持久化为镜像并修改镜像名称和标签。

```
[root@ecs-docker ~]# docker commit f56106f9c554 swr.cn-north-1.myhuaweicloud.com/hcip/hcip-cloudservice:v1
#f56106f9c554：容器 ID
#swr.cn-north-1.myhuaweicloud.com：SWR 地址，可以通过查看登录指令的最后一段进行确认
#hcip：组织名称
#hcip-cloudservice:v1：镜像名称：标签
[root@ecs-docker ~]# docker images
```

```
root@ecs-docker ~]# docker commit f56106f9c554 swr.cn-north-1.myhuaweicloud.com/hcip /hcip-cloudservice:v1
ha256:1b75ff775b80a65f1209942eb5573c44d6ae74171e04aedd1295b92757ab4489
root@ecs-docker ~]# docker images
EPOSITORY                                                TAG       IMAGE ID       CREATED          SIZE
wr.cn-north-1.myhuaweicloud.com/hcip /hcip-cloudservice   v1        1b75ff775b80   5 seconds ago    144MB
ttpd2                                                    v1        8def57c4236d   43 minutes ago   144MB
ttpd                                                     latest    c30a46771695   2 days ago       144MB
ello-world                                               latest    feb5d9fea6a5   7 months ago     13.3kB
root@ecs-docker ~]#
```

图6-36

步骤 8 使用如下命令上传该镜像至 SWR。

```
[root@ecs-docker ~]# docker push swr.cn-north-1.myhuaweicloud.com/hcip/hcip-cloudservice:v1
```

```
[root@ecs-docker ~]# docker push swr.cn-north-1.myhuaweicloud.com/hcip/hcip-cloudservice:v1
The push refers to repository [swr.cn-north-1.myhuaweicloud.com/      /hcip-cloudservice]
b456203fcd13: Pushed
e825bfd70e3d: Pushed
59fde81347af: Pushed
318410a5e575: Pushed
1bf88df2ac46: Pushed
608f3a074261: Pushed
v1: digest: sha256:3b118273d30b1ce82a28e3ec78f9136d306072a4709578feecd1187d49114559 size: 1577
[root@ecs-docker ~]#
```

图6-37

步骤 9 登录 SWR，查看镜像，如下图所示，证明通过以上配置镜像上传成功。点击镜像名称进入镜像详情页面。

图6-38

步骤 10 在镜像详情页面可以看到当前镜像版本为“v1”。

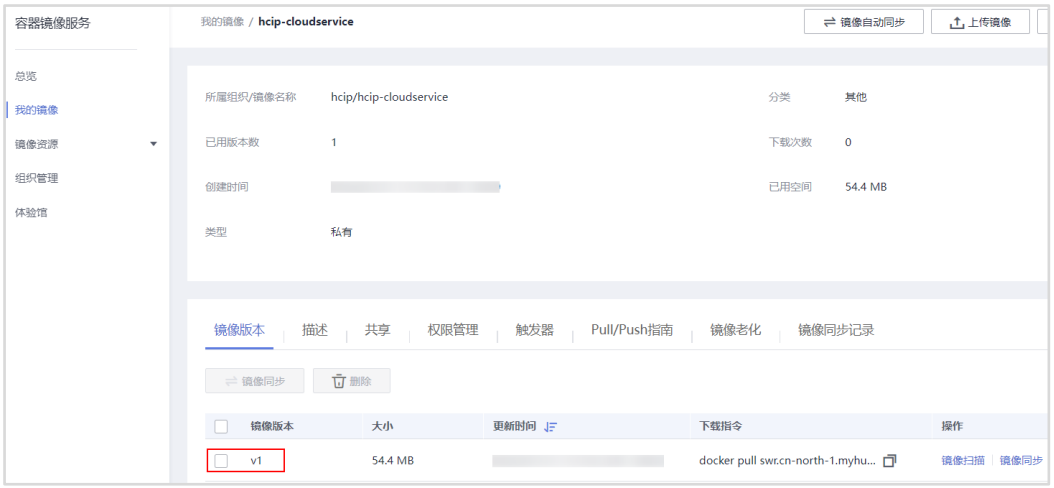


图6-39

6.2.1.9 创建 CCE，部署容器

步骤 1 登录华为云，在服务列表中选择“云容器引擎”，选择“同意授权”。

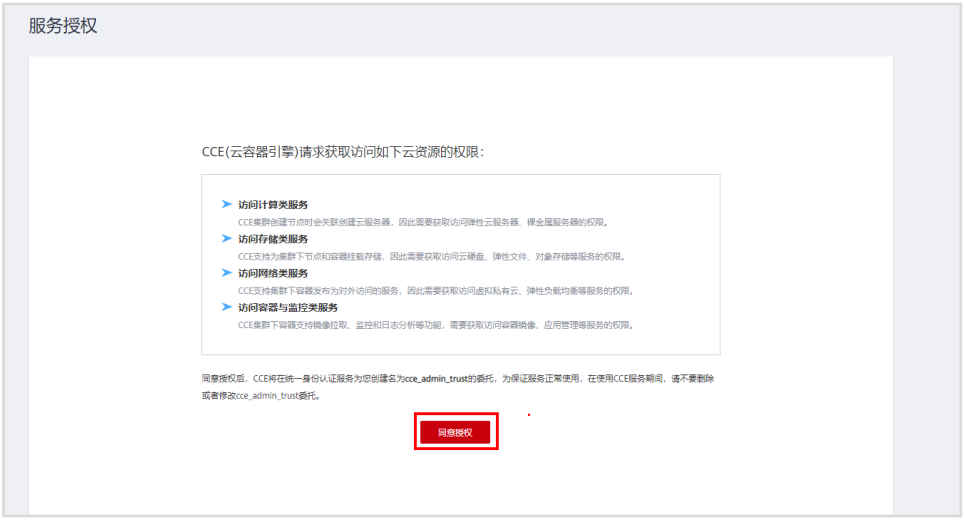


图6-40

步骤 2 在云容器引擎页面选择“创建”CCE 集群。

说明：后续需要通过该集群拉取 SWR 中上传的镜像并部署为容器。

图6-41

步骤 3 参照以下内容选择 CCE 集群配置参数。

CCE 集群：

- 计费模式：按需计费
- 集群名称：cluster-hcip（学员可自定义）
- 版本：v1.19
- 集群管理规模：50 节点
- 高可用：否（选“是”也可以，配置时间会略长）
- 网络模型：VPC 网络
- 虚拟私有云：vpc-1
- 所在子网：vpc-1-subnet
- 容器网段：10.10.0.0/16
- 服务网段：使用默认网段

图6-42

步骤 4 完成以上配置选择后，点击“创建”。在集群管理中可看到创建中的 CCE 集群，创建集群预计需要几分钟。

图6-43

步骤 5 在集群管理中查看已创建的 CCE 集群，当集群状态为“运行中”时，证明该集群创建完成。

图6-44

步骤 6 在集群管理页面，点击“创建节点”图标，为集群添加节点。或点击该集群右下角的“创建节点”链接，为集群添加节点。

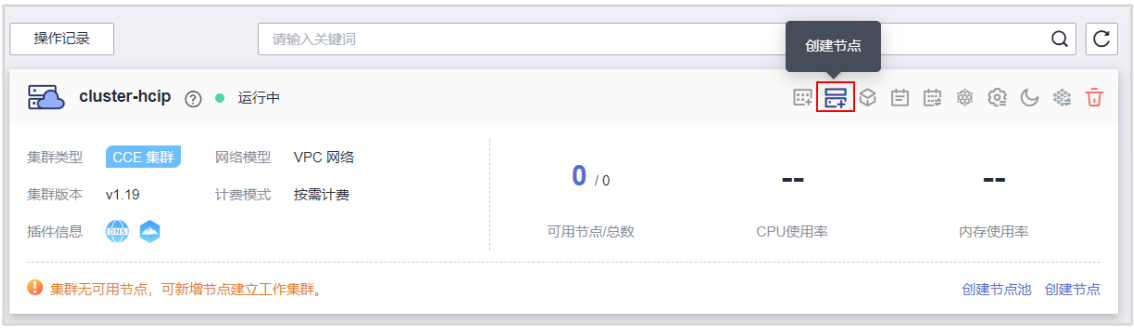


图6-45

步骤 7 参照以下内容选择相应配置参数，确认配置后，点击“提交”。

添加节点：

- 计费模式：按需计费
- 可用区：随机分配
- 节点类型：弹性云服务器-虚拟机
- 容器引擎：docker
- 节点规格：4 核|8 GB
- 操作系统：EulerOS 2.5
- 节点名称：默认即可
- 密码：用户自定义
- 系统盘：超高 IO|50 GiB
- 数据盘：超高 IO|100 GiB
- 节点子网：vpc-1-subnet

图6-46

步骤 8 创建完节点后，会自动跳转至节点管理页面。如果没有跳转或不小心退出，可在集群管理页面，点击集群名称，如本次实验中的集群“cluster-hcip”。

图6-47

步骤 9 点击左侧的“节点管理”，检查新增的节点是否已正常运行。

图6-48

步骤 10 左侧选择“工作负载>无状态负载”，点击右上角“创建负载”，参照以下参数，完成负载创建。

- 工作负载名称：hcip-httpd（学员可自定义）
- 命名空间：default
- 实例数量：1
- 容器名称：container-httpd（学员可自定义）
- 镜像名称：选择之前上传的镜像，如：hcip-cloudservice

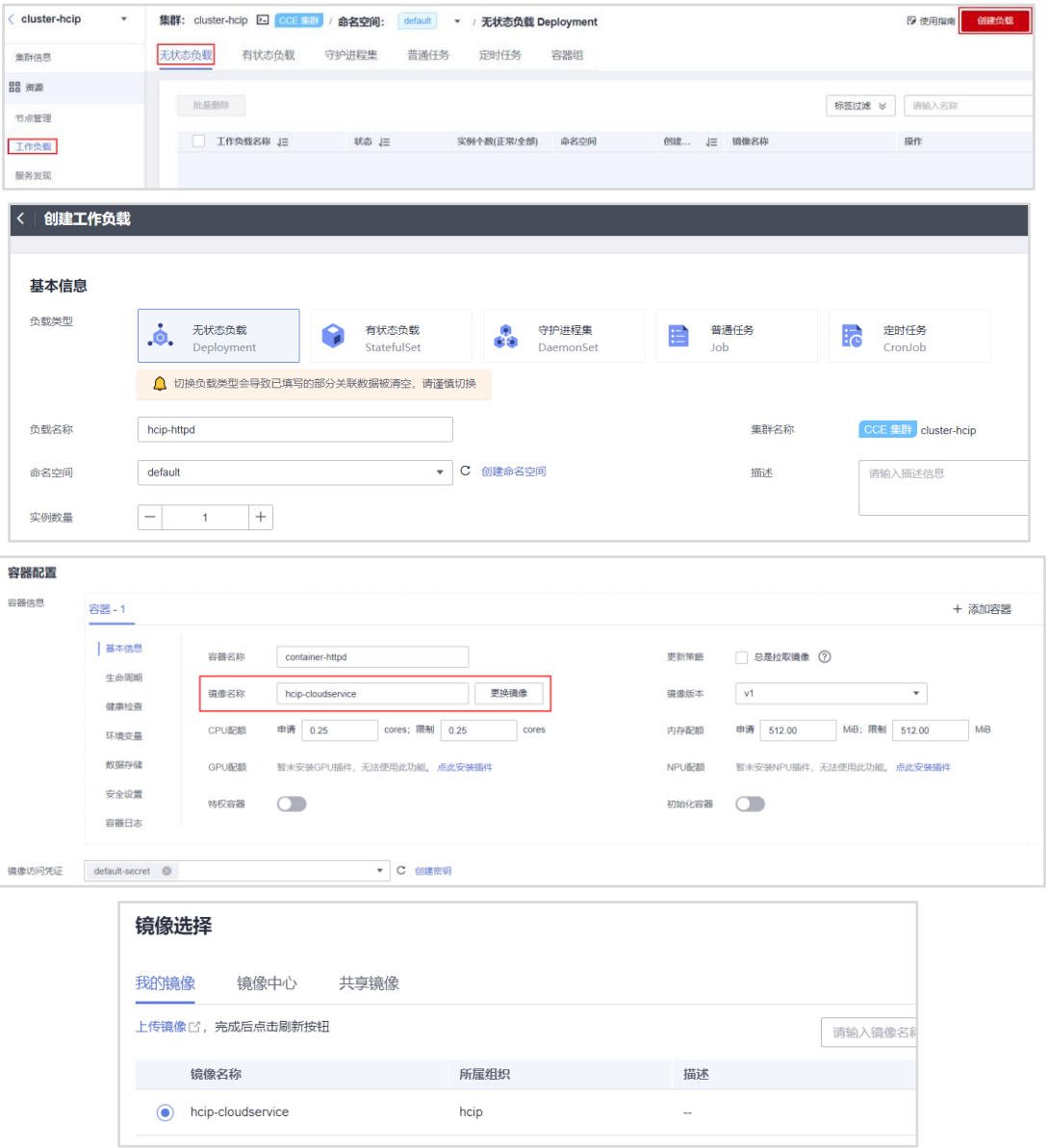


图6-49

步骤 11 完成负载创建后，可以在“无状态负载”页面中看到新建的工作负载。

图6-50

步骤 12 返回 ECS 页面，为 CCE 集群的节点购买并绑定弹性 IP，具体操作方法可以参见计算服务规划或网络服务规划章节。说明：需要使用此 EIP 为新部署容器负载实现外网访问功能。

- 计费模式：按需计费
- 公网带宽：按流量计费
- 带宽大小：10 Mbit/s
- 数量：1

图6-51

步骤 13 返回 CCE 集群管理页面，选择“工作负载>无状态负载>工作负载名称，如 hcip-httpd>访问方式”，点击“创建”。访问类型选择“节点访问”，服务端口当前用不到，但是是必填选项，可以设置为 80，容器端口设置为 80，访问端口指定为 30080（这里以 30080 端口为例，学员可根据实际情况选择相应端口）。

- Service 名称：hcip-httpd
- 访问类型：节点访问
- 服务亲和：节点级别
- 协议：TCP
- 服务端口/容器端口：80
- 访问端口：指定端口 | 30080

图6-52

步骤 14 使用本地 PC 浏览器，通过 http://EIP:30080 登录该地址查看。（本实验中为：http://117.78.38.200:30080），如下图所示，证明上传至 SWR 中的镜像在云容器引擎 CCE 中部署成功，该实验成功完成。

图6-53

6.2.2 函数工作流 FunctionGraph

FunctionGraph 是一项基于事件驱动的函数托管计算服务。使用 FunctionGraph 函数，只需编写业务函数代码并设置运行的条件，无需配置和管理服务器等基础设施，函数以弹性、免运维、高可靠的方式运行。

在实际业务场景中，可能因公司业务要求，需要频繁更新 OBS 中存储的对象版本，导致历史版本过多，而工作中只用最新的三个版本即可满足需要，需要定期安排人员进行人工删除，维护的操作较为繁琐，此时可以使用 FunctionGraph 函数来做到在桶内始终只保留最新的 3 个版本数据。

6.2.2.1 资源准备

步骤 1 通过 https://cloudservice-v3.obs.cn-east-3.myhuaweicloud.com/DeleteOldVersions.zip 下载代码文件至本地。

6.2.2.2 创建对象存储桶

步骤 1 在服务列表中选择“对象存储服务”。

说明：作为函数工作流执行的目标桶。

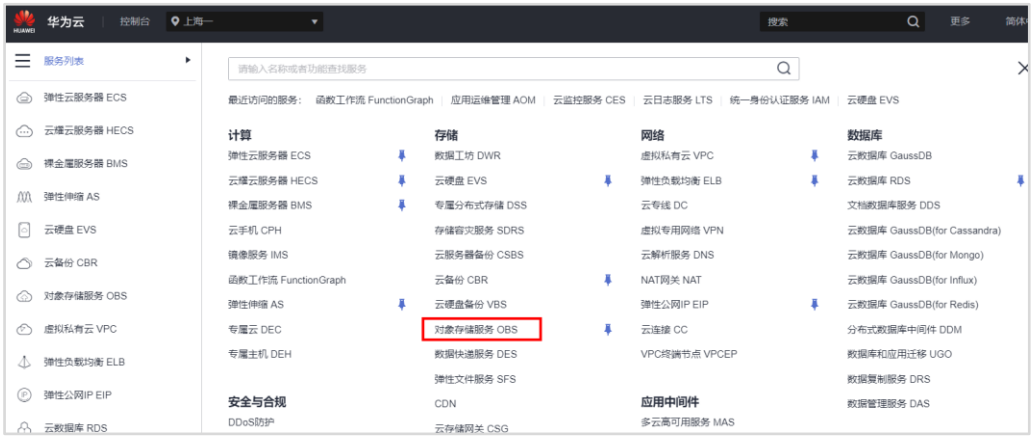


图6-54

步骤 2 点击右上角“创建桶”。

图6-55

步骤 3 按照以下配置完成桶的创建。

- 区域：华东-上海一（学员可以根据需要，自定义区域）
- 桶名称：obs-flash
- 其他配置：默认配置

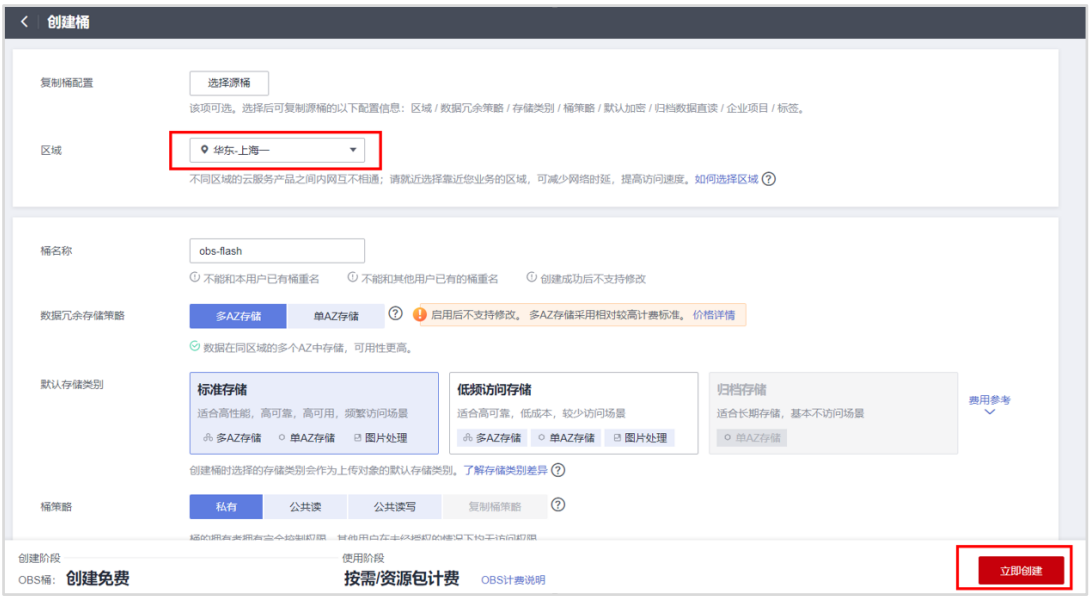


图6-56

6.2.2.3 创建委托

步骤 1 在用户名下拉菜单中选择“统一身份认证”。

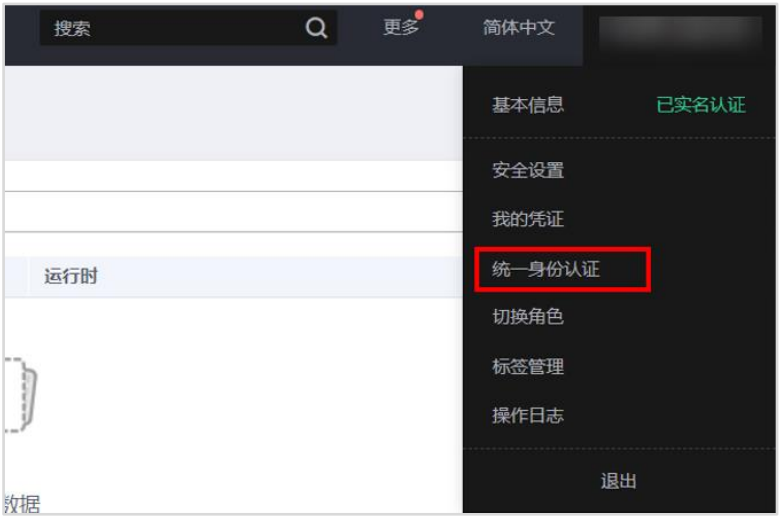


图6-57

步骤 2 在左侧页签中选择“委托”，点击右上角“创建委托”。

说明：后续需要使用该委托赋予函数工作流相关权限。

图6-58

步骤 3 按照以下内容配置委托名称、委托类型和云服务。

- 委托名称：fgh-commission
- 委托类型：云服务
- 云服务：函数工作流 FunctionGraph
- 持续时间：永久

图6-59

- 授权策略按照下图内容选择“OBS Administrator”和“LTS FullAccess”。

说明：后续函数工作流需要调用 OBS 服务和云日志服务。

图6-60

- 其他配置保持默认，点击“确定”。

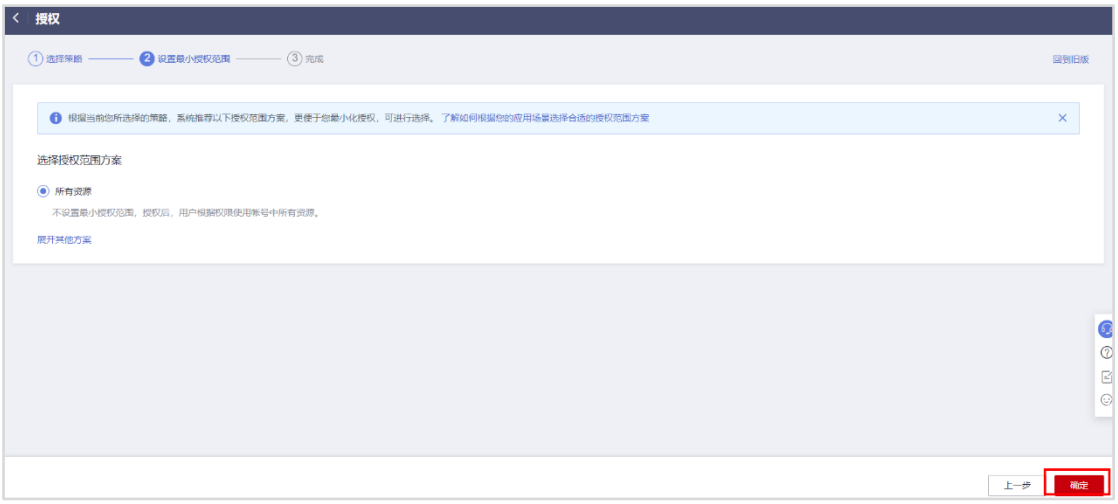


图6-61

步骤 4 在授权记录列表中可以查看当前的授权，如下图所示，证明委托创建成功。

图6-62

6.2.2.4 创建函数工作流

步骤 1 在服务列表中选择“函数工作流 FunctionGraph”。

图6-63

步骤 2 在函数工作流页面中，点击右上角“创建函数”。

图6-64

步骤 3 根据以下配置完成函数创建。

- FunctionGraph 版本：FunctionGraph v2
- 函数类型：事件函数
- 函数名称：obs-flash
- 委托名称：fgh-commission
- 运行时：Python 3.9

图6-65

6.2.2.5 配置消息通知服务 SMN

步骤 1 在服务列表中选择“消息通知服务 SMN”。

图6-66

步骤 2 在左侧页签中选择“主题”，点击右上角“创建主题”。

说明：后续实验中需要通过该 SMN 主题触发函数工作流的执行。

图6-67

步骤 3 创建名为“obs-flash”的主题，点击“确定”。

图6-68

步骤 4 点击 obs-flash 主题对应的“添加订阅”按钮，按照以下配置添加订阅。

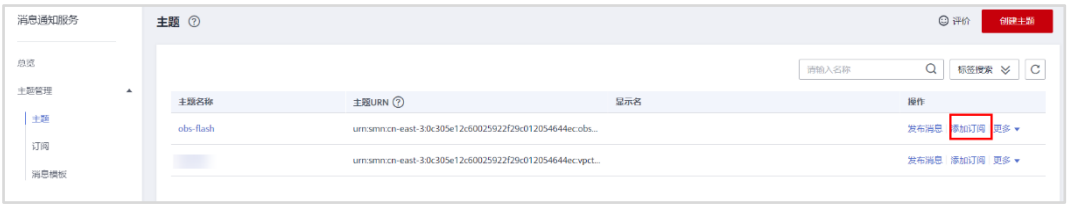


图6-69

- 协议选择“FunctionGraph（函数）”，订阅终端选择之前创建的函数“obs-flash”。

说明：订阅终端选择刚才创建的 FunctionGraph 函数，当相关服务触发 SMN 消息时，将会通知 FunctionGraph。

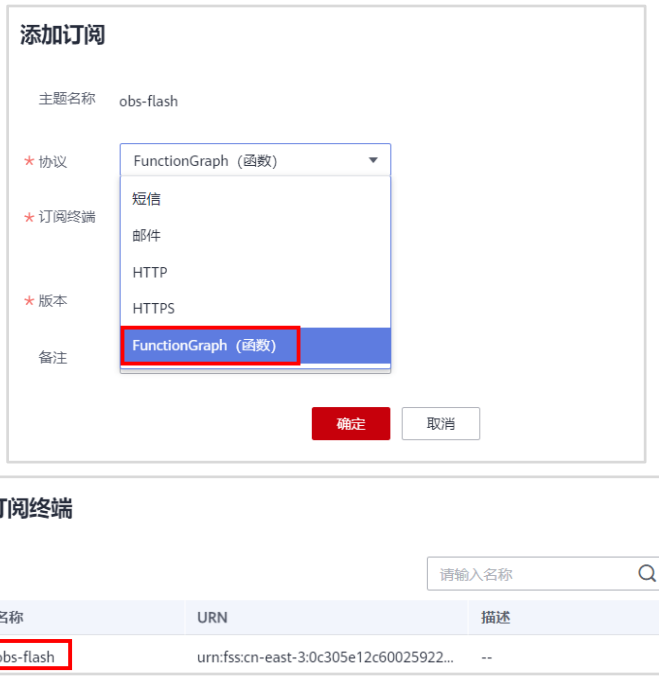


图6-70

- 按照以上配置选择完成后（版本不用选择），点击“确定”。

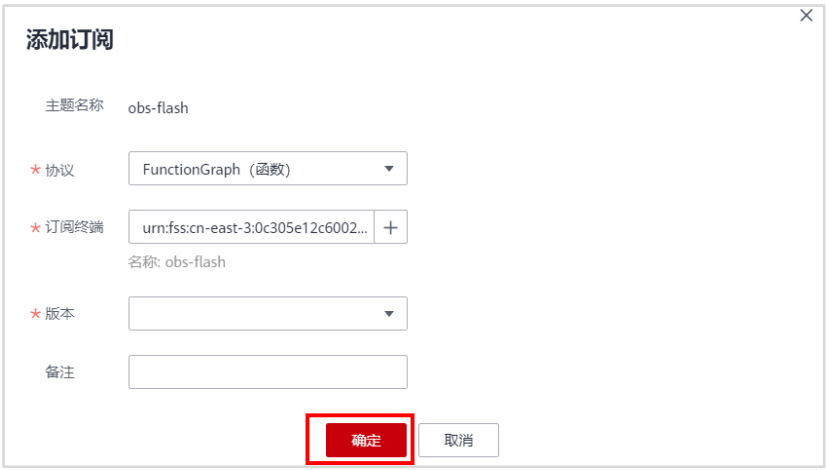


图6-71

步骤 5 点击 obs-flash 主题对应操作栏的“更多”，选择“设置主题策略”。

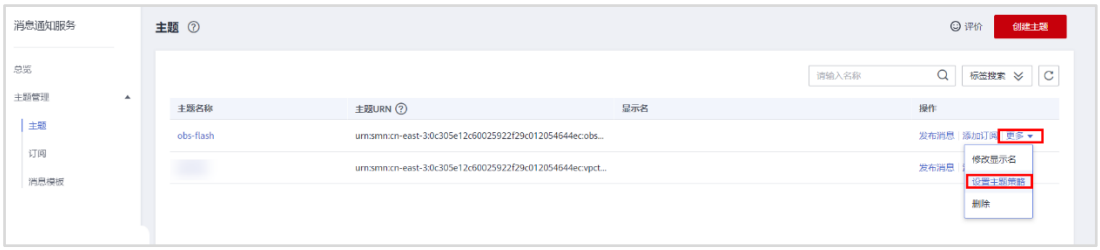


图6-72

- 勾选可发布消息的服务“OBS”，点击“确定”。

图6-73

6.2.2.6 配置函数工作流

步骤 1 在“函数工作流>函数>函数列表”，点击进入刚才创建的函数，如“obs-flash”，检查是否已经生成触发器。下图中的触发器“SMN”就是新生成的触发器。

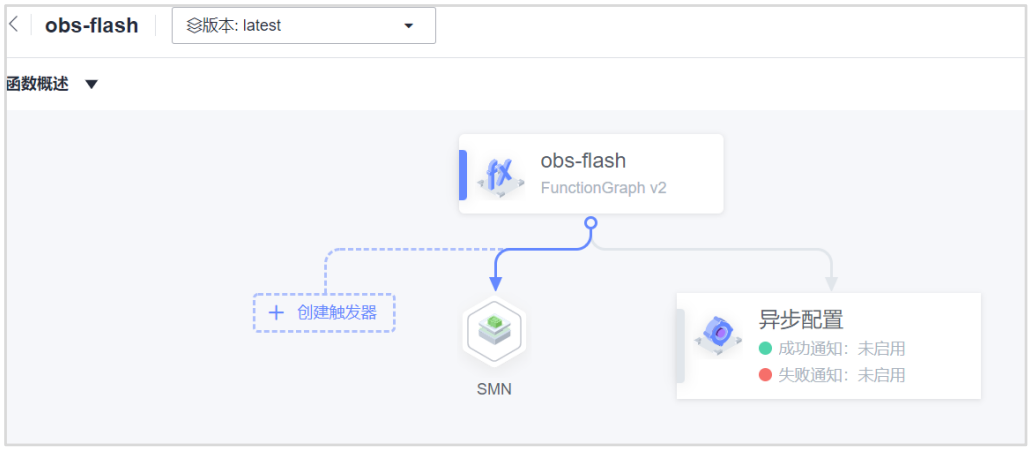


图6-74

步骤 2 在函数页面中点击“代码”页签。

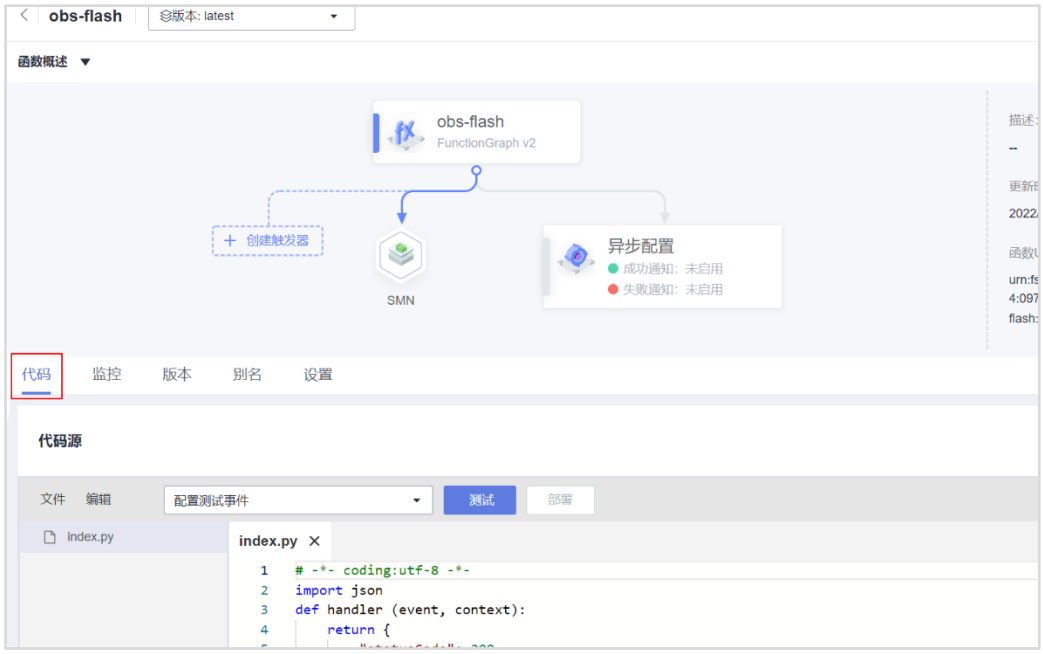


图6-75

步骤 3 将 6.2.2.1 中下载的代码文件中内容复制后，复制到“index.py”文件中（覆写原来的内容）。

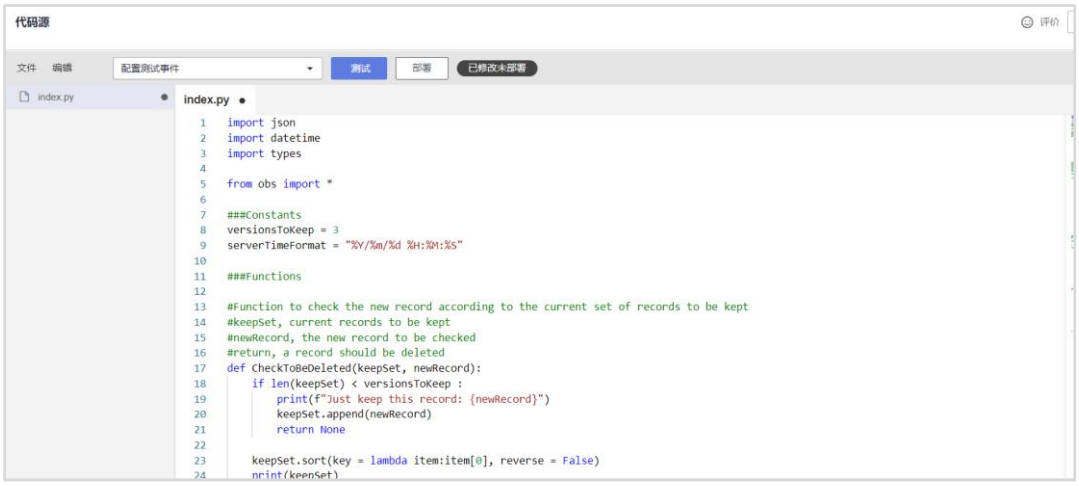


图6-76

步骤 4 点击“部署”按钮部署代码。

图6-77

6.2.2.7 配置对象存储桶

步骤 1 在服务列表中选择“对象存储服务 OBS”。

步骤 2 点击刚创建的桶名“obs-flash”。

图6-78

步骤 3 在左侧页签中选择“基础配置”中的“事件通知”，点击右侧“创建按钮”。

图6-79

步骤 4 按照以下配置创建事件通知。

说明：后续在桶内创建对象时，会通过该事件通知触发 SMN 消息，转发给 FunctionGraph。

- 事件通知名称：event
- 事件：ObjectCreated
- 通知类型：SMN 主题|华东-上海一|obs-flash

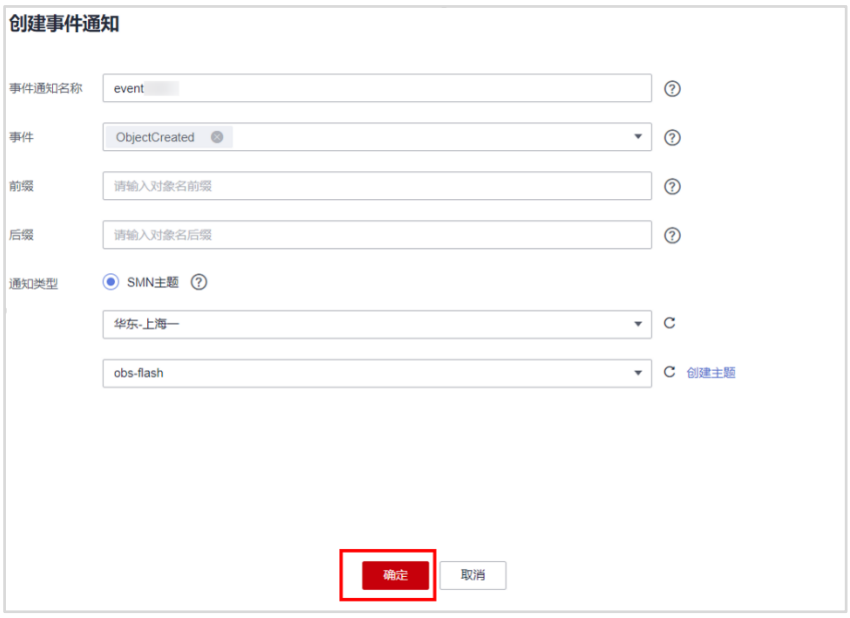


图6-80

步骤 5 在左侧“概览”页签中，选择“多版本控制”后面的“编辑”选项。

说明：需要将同一个对象上传多个版本，来测试 FunctionGraph 函数的执行。

图6-81

步骤 6 在弹出的对话框中选择“启用”，并点击“确定”。

图6-82

6.2.2.8 上传对象至对象存储桶中

步骤 1 在创建的 obs-flash 桶的“概览”页面中，选择“对象”页签。点击右侧“上传对象”按钮。

图6-83

步骤 2 点击“添加文件”。

图6-84

步骤 3 在本地选择测试文件（任选一个较小的文件即可），点击“上传”。

图6-85

步骤 4 再连续执行此上传动作两次，点击该对象名称。

图6-86

步骤 5 点击版本页签，查看当前已保存的 3 个版本文件，可以通过查看文件的修订时间，来进行版本判断。

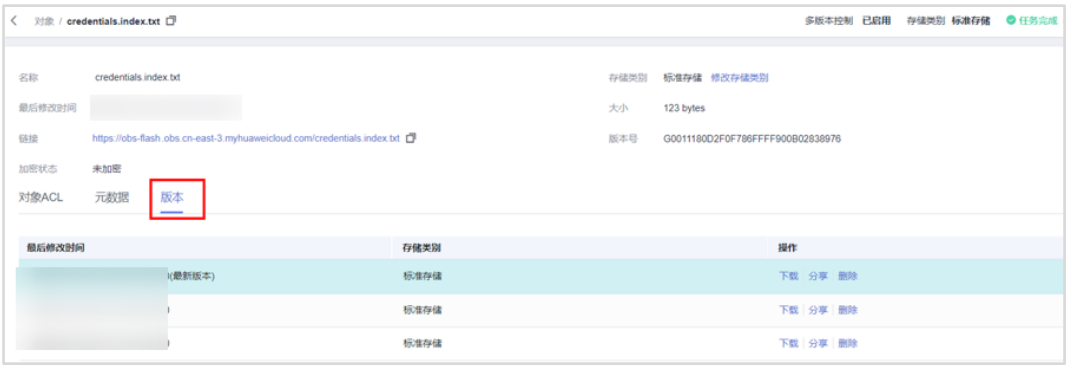


图6-87

步骤 6 此时再次执行上传动作，再次查看历史版本，发现只保留了最新的三个版本文件，最早上传的版本已被刷新。之前的旧版本已被刷新，证明函数工作流已触发执行并生效。

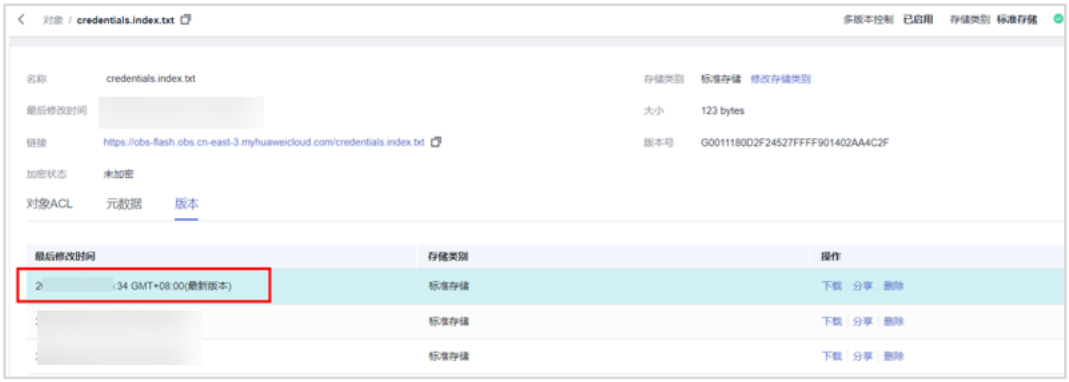


图6-88

6.2.2.9 查看函数工作流执行日志

步骤 1 在创建的 obs-flash 函数的“监控”页签中，选择“日志”页签，选择“点击开通”开通云日志服务 LTS，开通函数日志功能。

图6-89

步骤 2 回到 OBS 对象存储页面，再次上传相同文件（文件可多次上传），触发函数工作流删除历史版本。

步骤 3 返回 obs-flash 函数页面，点击“监控>日志”，可查看当前函数的调用情况。说明：完成 OBS 文件上传后，可能要等几分钟才能看到日志信息。

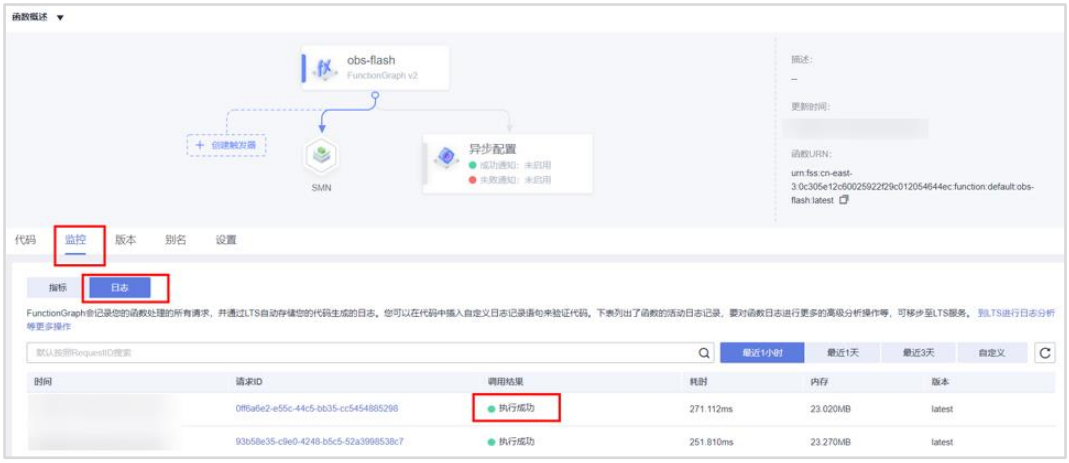


图6-90

6.3 实验恢复

步骤 1 删除工作负载。

- 在服务列表中选择“云容器引擎 CCE”，在“工作负载>无状态负载”页签中，找到本实验创建的无状态负载，点击操作栏的“更多>删除”。

步骤 2 删除 CCE 引擎。

- 服务列表中选择“云容器引擎 CCE”，在左侧页签中选择“节点管理”，在节点列表中找到本实验创建的引擎节点，点击操作栏的“更多>删除”。

步骤 3 删除 SWR 组织。

- 在服务列表中选择“容器镜像服务 SWR”，在左侧页签中选择“组织管理”，找到本实验创建的组织，点击组织名称进入详情页面。

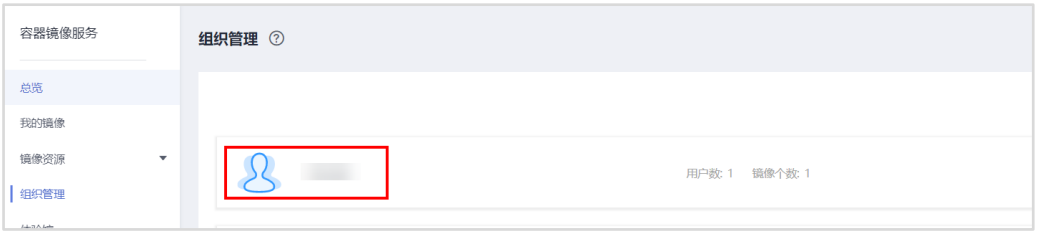


图6-91

- 点击右侧“镜像”选项，点击本实验中创建的镜像名称。

图6-92

- 在弹出的页面中勾选所有镜像版本，并点击“删除”。

图6-93

- 在左侧页签中选择“组织管理”，找到本实验创建的组织，点击组织名称进入详情页面，点击右上角删除按钮。

图6-94

步骤 4 删除 ECS。

- 在服务列表中选择“云服务器 ECS”，找到本实验创建的云服务器，点击操作栏中的“更多>删除”。
- 在弹出的对话框中勾选下图中选项，点击“是”。

图6-95

步骤 5 删除安全组。

- 在服务列表中选择“虚拟私有云 VPC”，在“访问控制>安全组”中找到本实验创建的安全组，点击操作栏的“更多>删除”。

步骤 6 删除 VPC。

- 在服务列表中选择“虚拟私有云 VPC”，点击“子网”页签，在列表中找到本实验创建的子网，点击操作栏中的“删除”。
- 点击“虚拟私有云”页签，找到本实验创建的 VPC，点击操作栏中的“删除”。

步骤 7 删除 FunctionGraph 函数。

- 在服务列表中选择“函数工作流 FunctionGraph”，在左侧“函数”页签中找到本实验创建的函数，选择操作栏中的“删除”。

步骤 8 删除 SMN。

- 在服务列表中选择“消息通知服务 SMN”，在左侧页签中选择“主题管理>主题”，在右侧列表中找到本实验创建的主题，点击操作栏中的“更多>删除”

步骤 9 删除委托。

- 点击右上方用户名，在下拉菜单中选择“统一身份认证”。

图6-96

- 选择“委托”页签，在委托列表中找到本实验创建的委托，点击对应操作栏中的“删除”。

步骤 10 删除 OBS 桶。

- 在服务列表中选择“对象存储服务 OBS”，在桶列表中找到本实验创建的桶，点击操作栏中的“删除”。

6.4 思考题

问题：华为云容器引擎 CCE 在基础设施与容器应用管理场景中，具有哪些优势?

参考答案：可以支持多种类型容器部署，支持部署无状态工作负载、有状态工作负载、守护进程集、普通任务、定时任务等。支持应用升级的同时也支持节点和工作负载的弹性伸缩功能，可以提升应用的部署效率和升级效率，实现升级时业务不中断以及统一的自动化运维。

7 微服务应用部署实验

7.1 实验介绍

7.1.1 关于本实验

天气预报微服务应用可以提供天气预报、紫外线和天气湿度展示等功能。本实验通过天气预报应用，展示了微服务架构设计理念的应用场景，以及使用 ServiceStage 管理运行环境、搭建流水线的最佳实践。

天气预报由前端应用和后端应用组成。前端应用 weathermapweb 采用 Node.js 进行开发，通过 Mesher 技术接入微服务引擎，实现前端应用发现后端应用。后端应用采用 Java 微服务开发框架实现，包括 fusionweather、forecast、weather、weather-beta 等微服务。

说明：本实验以“北京四”区域为例，学员可以根据实际情况选择相应区域进行实验。环境中涉及多个微服务组件，建议相关名称参照实验手册中的名称进行配置。

7.1.2 实验目的

理解微服务架构设计的理念和应用场景。

掌握使用 ServiceStage 管理运行环境、搭建流水线的配置方式。

掌握通过 ServiceStage 进行微服务构建、部署的配置方式和设计原理。

7.1.3 软件介绍

fusionweather 是一个聚合微服务，通过访问 weather 和 forecast 服务，提供全方位的天气预报功能。forecast 服务实现未来几天天气预报查询功能。weather 服务实现天气湿度查询功能。weather-beta 微服务是 weather 微服务的新版本，新增了查询指定城市紫外线情况的功能（灰度发布使用，本次实验可以不部署）。

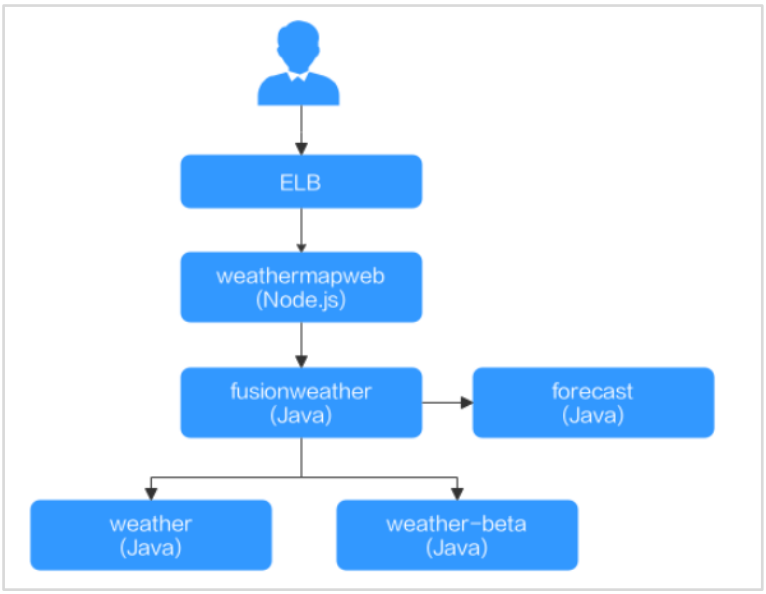


图7-1

GitHub 是一个面向开源及私有软件项目的托管平台，因为只支持 Git 作为唯一的版本库格式进行托管，故名 GitHub。

7.2 实验配置

7.2.1 实验准备

7.2.1.1 资源准备

步骤 1 登录华为云，选择“我的凭证”。

图7-2

步骤 2 选择“访问密钥”，点击右侧“新增访问密钥”。

说明：后续需要使用该访问密钥在 ServiceStage 中创建密钥。

图7-3

步骤 3 在弹出的提示框中选择“立即下载”并记录。

图7-4

步骤 4 创建 VPC 和子网（配置步骤参考之前实验内容）。

说明：后续 CCE 集群资源将在该 VPC 中创建。

基本配置：

- 区域：华北-北京四
- 名称：vpc-servicestage
- IPv4 网段：192.168.0.0/16

默认子网

- 可用区：可用区 2
- 名称：subnet-servicestage
- 子网 IPv4 网段：192.168.20.0/24

步骤 5 按照以下配置，创建 CCE 集群。

说明：后续实验中微服务需要使用该 CCE 集群进行容器部署。

图7-5

- 区域：华北-北京四
- 计费模式：按需计费
- 集群名称：cluster-servicestage
- 版本：v1.19
- 集群管理规模：50 节点
- 高可用：否

图7-6

- 网络模型：VPC 网络
- 虚拟私有云：vpc-servicestage
- 控制节点子网：subnet-servicestage
- 容器网段：保持默认配置

图7-7

步骤 6 待集群创建完成后，点击“创建节点”，为 CCE 集群创建节点。

图7-8

步骤 7 参照以下内容选择相应配置参数，确认配置无误后，点击“提交”。

- 计费模式：按需计费
- 可用区：随机分配
- 节点类型：弹性云服务器-虚拟机
- 容器引擎：docker
- 节点规格：8 核|16 GiB

图7-9

- 操作系统：默认配置即可
- 节点名称：用户自定义或默认配置
- 登录方式：密码
- 密码：用户自定义
- 系统盘：默认配置
- 数据盘：默认配置
- 节点子网：subnet-servicestage
- 节点 IP：随机分配
- 弹性公网 IP：自动创建
- 线路：默认
- 计费方式：按流量计费
- 带宽：10 Mbit/s

图7-10

步骤 8 确认配置后点击“提交”。

图7-11

步骤 9 提交后会跳转到“节点管理”页面，可以查看已创建的节点信息。

图7-12

7.2.1.2 创建环境

步骤 1 登录 ServiceStage 控制台，选择“环境管理”，单击“创建环境”。

图7-13

步骤 2 按照以下配置选择相应参数，点击“新增基础资源”。

说明：后续微服务需要选择该环境进行部署。

- 环境名称：test-env
- 虚拟私有云：vpc-1

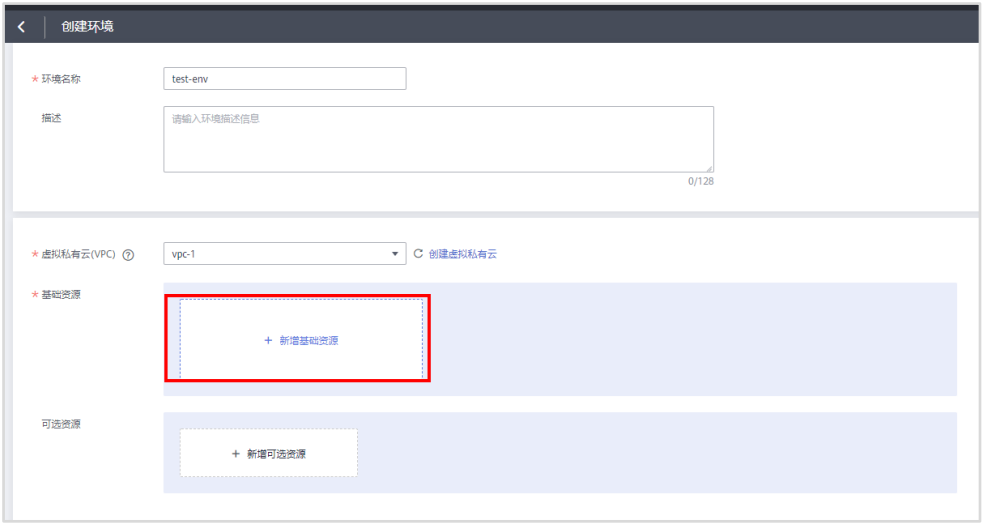


图7-14

步骤 3 在“云容器引擎（CCE）”页签下，选择已创建好的 CCE 集群，点击“确定”。

图7-15

步骤 4 点击“新增可选资源”。

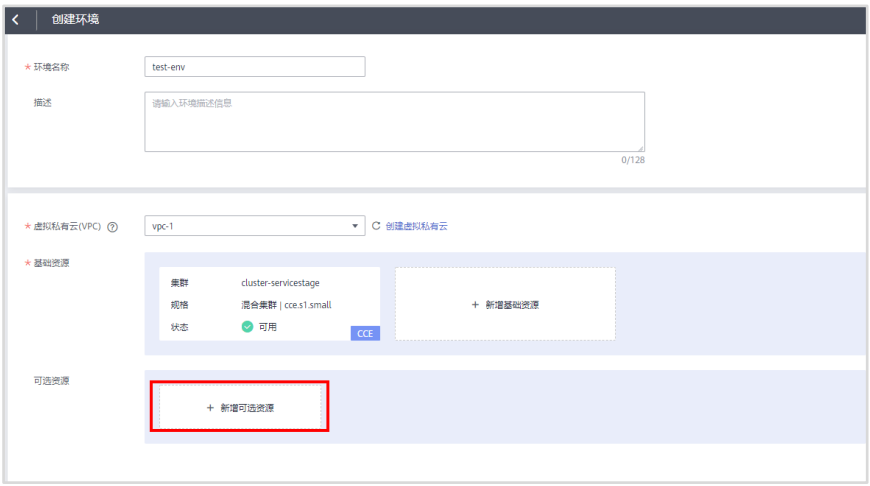


图7-16

步骤 5 在“微服务引擎 CSE”页签中选择“Cloud Service Engine”，点击“确定”后选择“立即创建”。

图7-17

步骤 6 在服务列表中选择“应用管理与运维平台”，在“应用列表”中点击右上角“创建应用”。

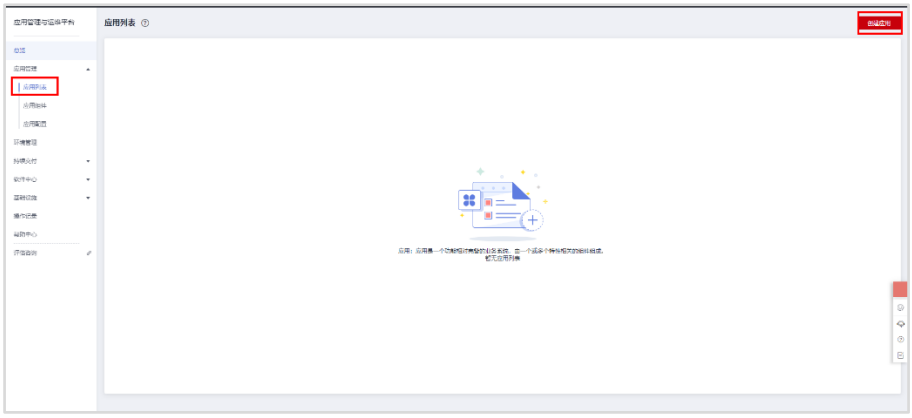


图7-18

步骤 7 配置“应用名称”为“weathermap”，点击“确定”。

图7-19

7.2.1.3 创建密钥

步骤 1 对资源准备时获取的 AK/SK 分别进行 base64 编码。请在 Linux 环境下，使用 echo -n '编码内容' | base64 命令。

```
echo -n ‘BM8QX6MNXVGIGXXXXXXX’| base64                          #AK
echo -n ‘FxRkLAJExA2lxnogHOMy7xYSr2McVEoXXXXXXXXXX’| base64      #SK
```

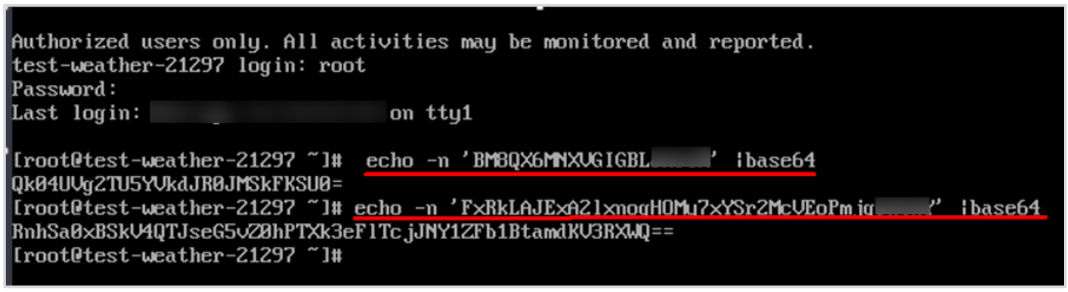


图7-20

步骤 2 登录 ServiceStage 控制台，选择“应用管理>应用配置>密钥>创建密钥”。

说明：本操作的主要目的是给基于 Mesher 框架的前端应用组件 weathermapweb 准备密钥。组件部署运行后，Mesher 会自动读取密钥信息。

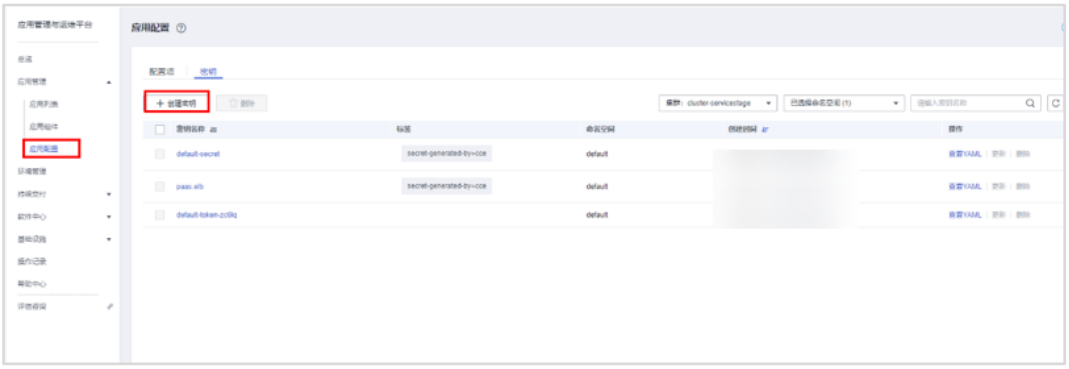


图7-21

步骤 3 按照以下配置内容填入相应参数。

- 创建方式：可视化
- 密钥名称：mesher-secret
- 所在集群：cluster-servicestage
- 命名空间：default
- 密钥类型：Opaque
- 密钥数据：cse_credentials_accessKey|编码后的 AK；cse_credentials_secretKey|编码后的 SK

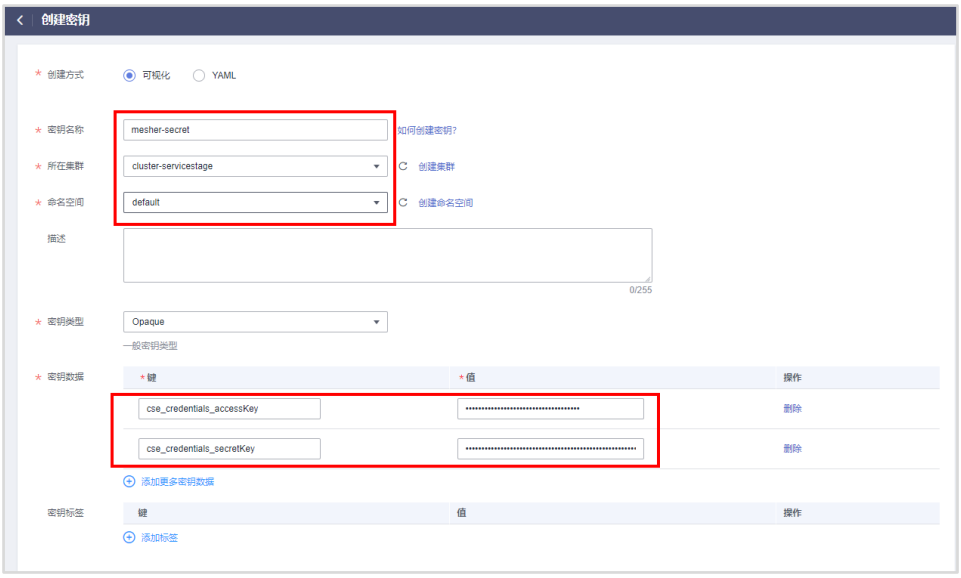


图7-22

步骤 4 在密钥列表中可以查看到已创建的密钥，证明密钥创建成功。

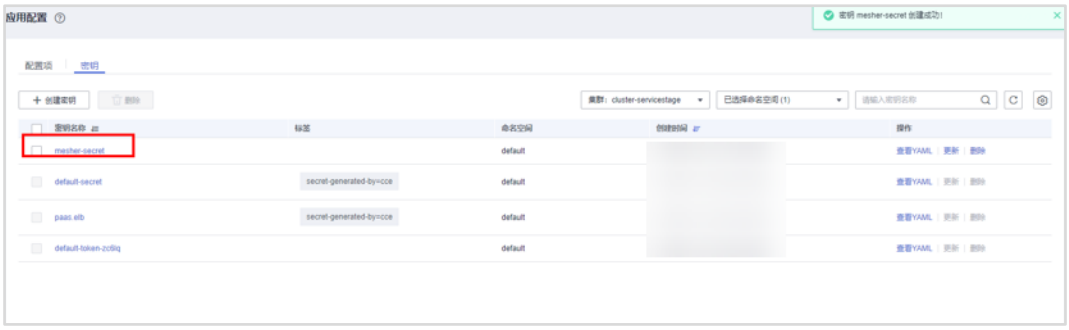


图7-23

7.2.1.4 准备天气预报源码

说明：如果没有 GitHub 账号，需要先登录 GitHub 官网进行账号注册。

步骤 1 登录 GitHub 帐号，在个人主页中点击“Repositories”页签。

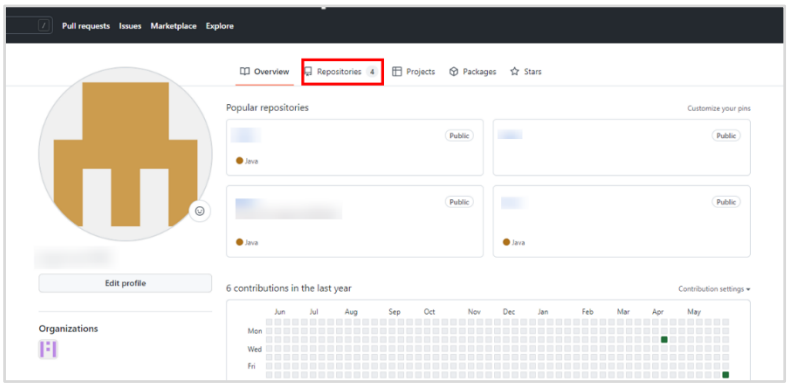


图7-24

步骤 2 点击“New”按钮创建新组织。

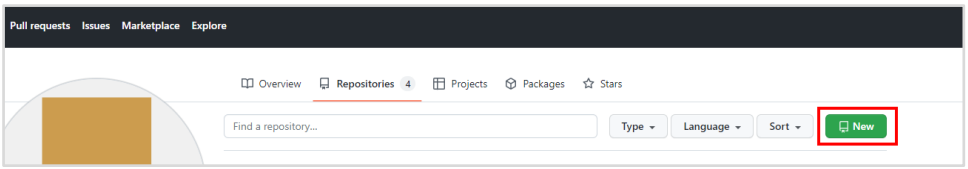


图7-25

步骤 3 按照以下配置创建仓库，并点击“Create repository”创建仓库。

- Repository name（仓库名称）：hcip
- 其他配置：默认配置

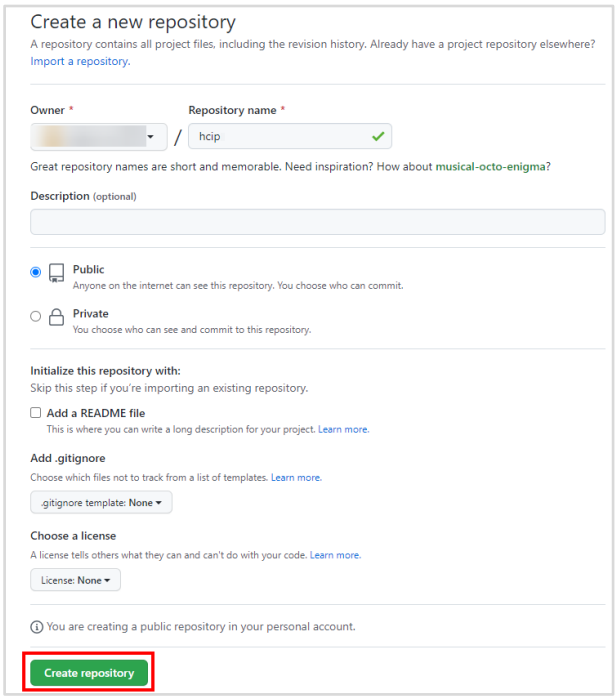


图7-26

步骤 4 在弹出的页面中点击“Import code”按钮导入源码。

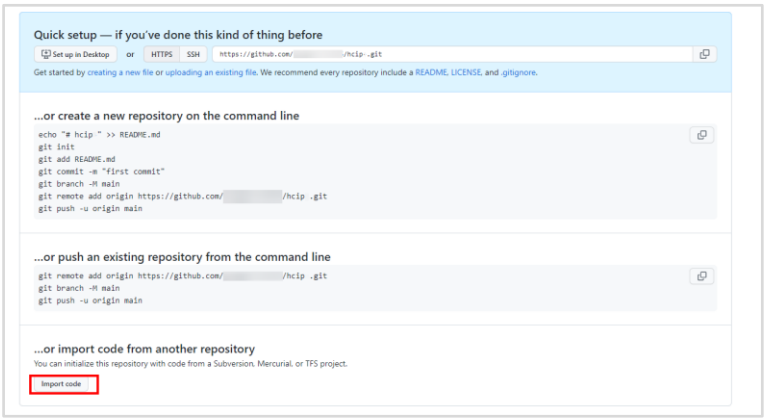


图7-27

步骤 5 在弹出的页面中输入源码地址：https://github.com/servicestage-demo/weathermap.git，点击“Begin import”按钮。

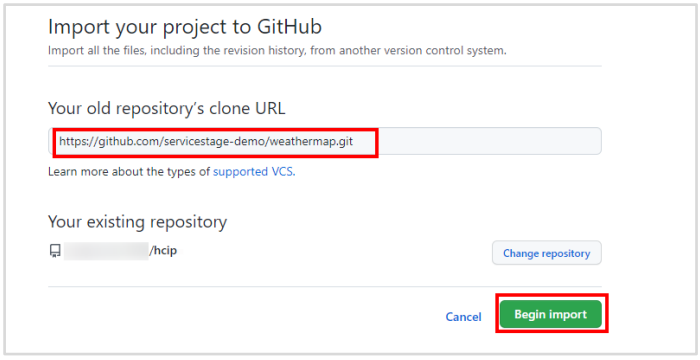


图7-28

步骤 6 如下图所示，可以看到在“hcip”仓库中已经成功导入了天气预报服务的相应源码文件。

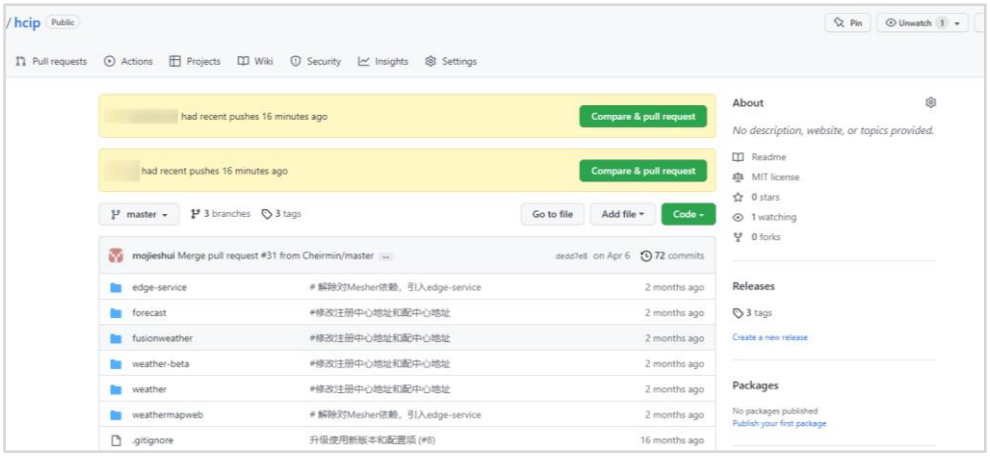


图7-29

7.2.1.5 设置 GitHub 仓库授权

步骤 1 登录 ServiceStage 控制台，选择“持续交付>仓库授权>新建授权”。

说明：在后续实验中需要使用该仓库授权进行微服务构建和微服务部署。

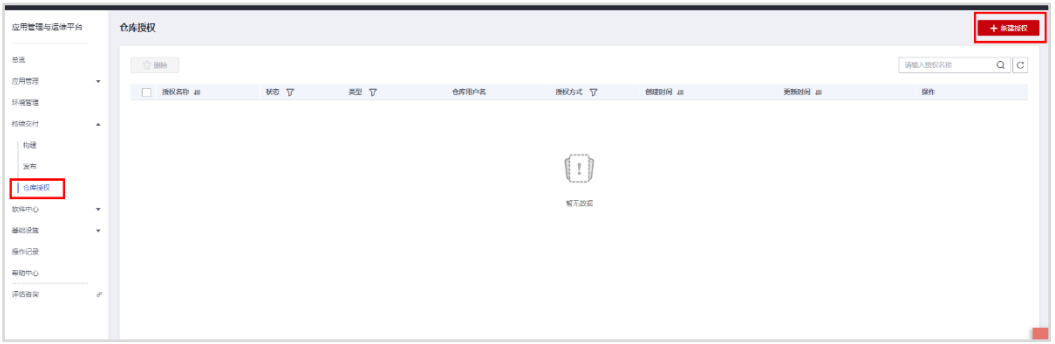


图7-30

步骤 2 按照以下配置设置授权参数。

- 授权名称：auth-github
- 仓库类型：GitHub
- 授权方式：OAuth|使用 OAuth 授权

图7-31

步骤 3 在弹出的授权框中点击“Authorize CPE-OAuth”。

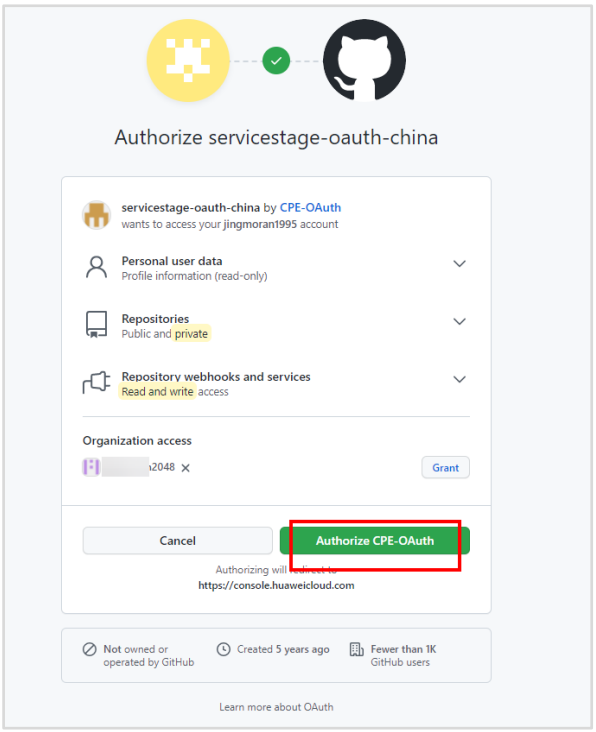


图7-32

步骤 4 在弹出的确认接入框中输入密码确认。

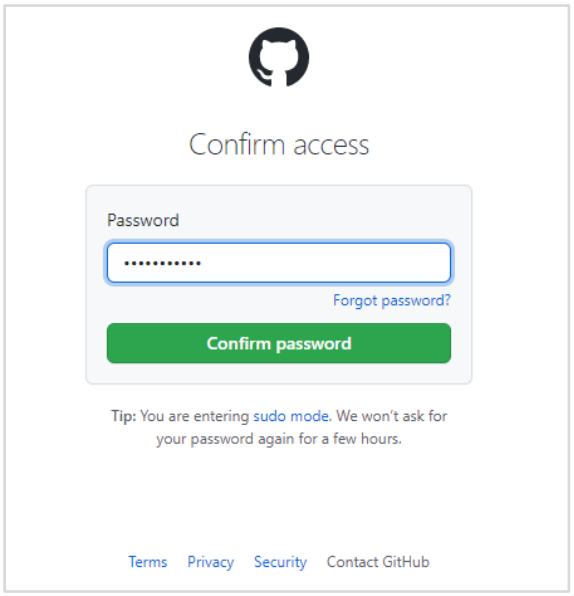


图7-33

步骤 5 查看已创建的授权，状态为“正常”，证明仓库授权创建成功。

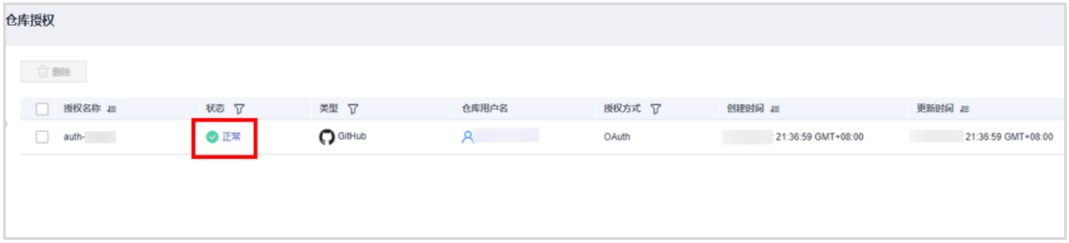


图7-34

7.2.1.6 创建组织

步骤 1 登录 ServiceStage 控制台，选择“软件中心>组织管理”。

说明：后续实验中的相关资源需要与该组织关联。

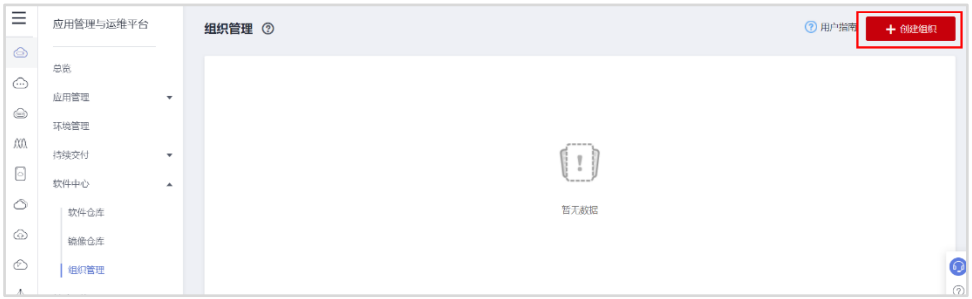


图7-35

步骤 2 点击“创建组织”，在弹出的页面中填写组织名称“hcip”，单击“确认”。

图7-36

7.2.2 微服务构建

ServiceStage 提供一键式应用交付流水线的能力，并支持灵活定制，企业可以基于源码、软件包的方式进行打包构建，使用流水线工程实现“源码拉取>编译>打包>归档>部署”的全流程自动化。在实际的场景中，能够帮助企业缩短业务上线周期，快速占领市场高地。

ServiceStage 提供对接 Devcloud、GitHub、Gitee、Bitbucket、GitLab 等源码仓库拉取源码。

在本实践中，用户可以基于源码的方式在 ServiceStage 上创建一个构建任务拉取 GitHub 上的 weathermap 源码，编译打包成镜像后归档到镜像仓库中。

7.2.2.1 创建后台应用构建任务

步骤 1 登录 ServiceStage 控制台，选择“持续交付>构建”，单击“基于源码构建”。

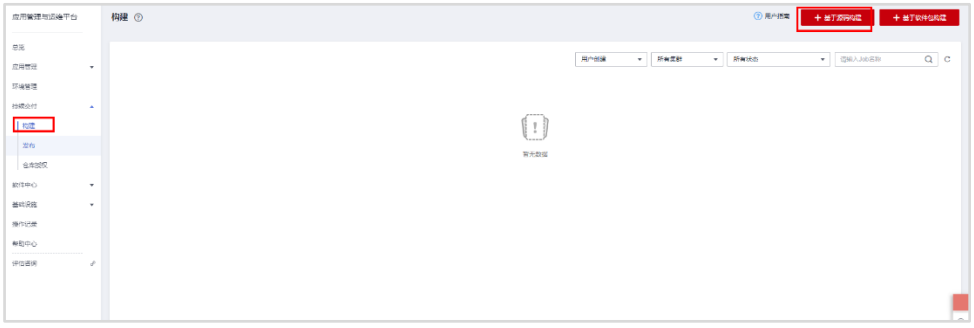


图7-37

步骤 2 按照以下配置设置构建工程参数。单击“下一步”进行环境设置。

- 名称：weathermap
- 代码来源：GitHub
- 授权信息：auth-github（选择实验准备步骤中创建的仓库授权）

- 用户名/组织：默认即可（学员 Github 账号的用户名/组织）
- 仓库名称：hcip（Github 中创建的仓库名称）
- 分支：master
- 构成集群：cluster-servicestage（选择资源准备步骤中创建的 CCE 集群）

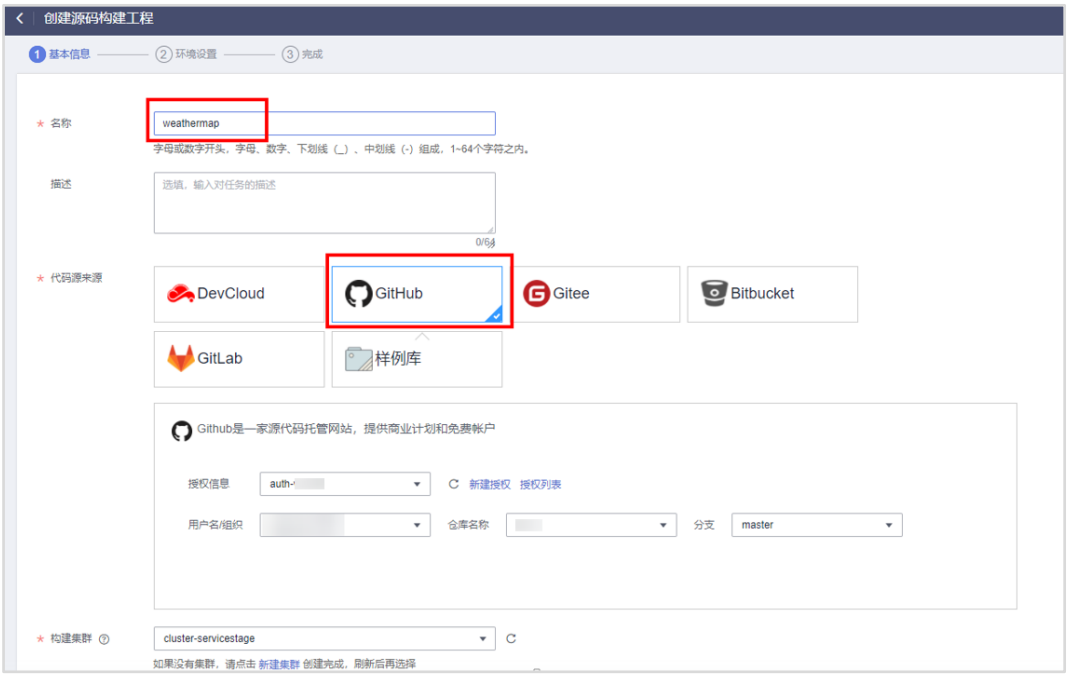


图7-38

步骤 3 选择“自定义”模板，点击“高级配置”。

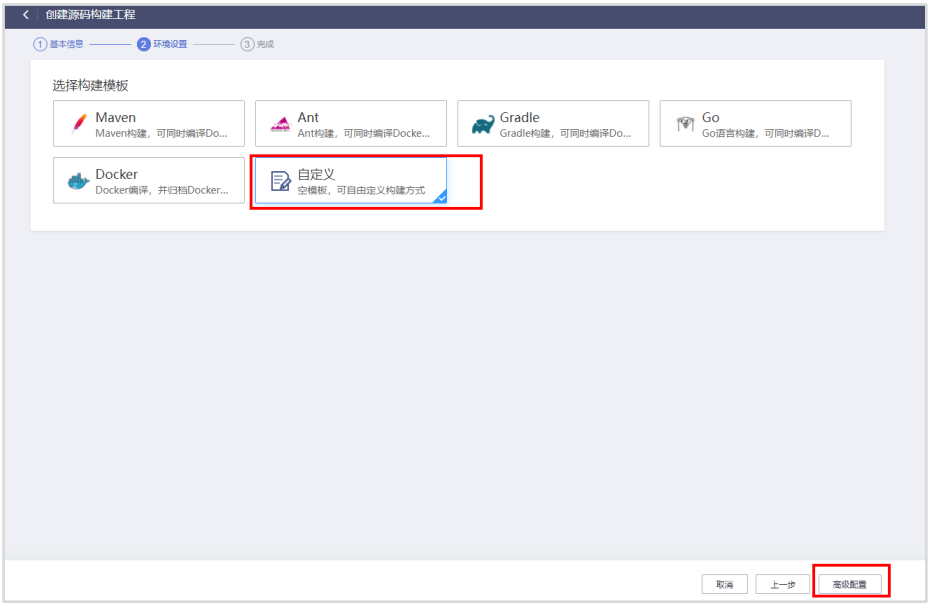


图7-39

步骤 4 在“编译”栏中，单击“添加插件”，选择“Build Common Cmd”，“语言”选择“Java”，设置通用命令行插件参数。

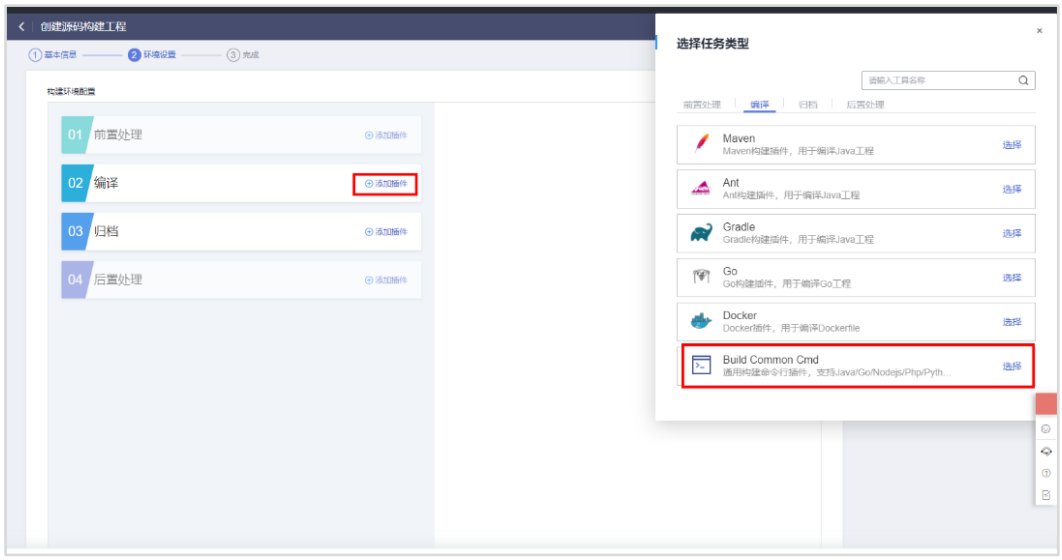


图7-40

- 任务名称：CommonCmd
- 语言：Java
- 版本：java-8

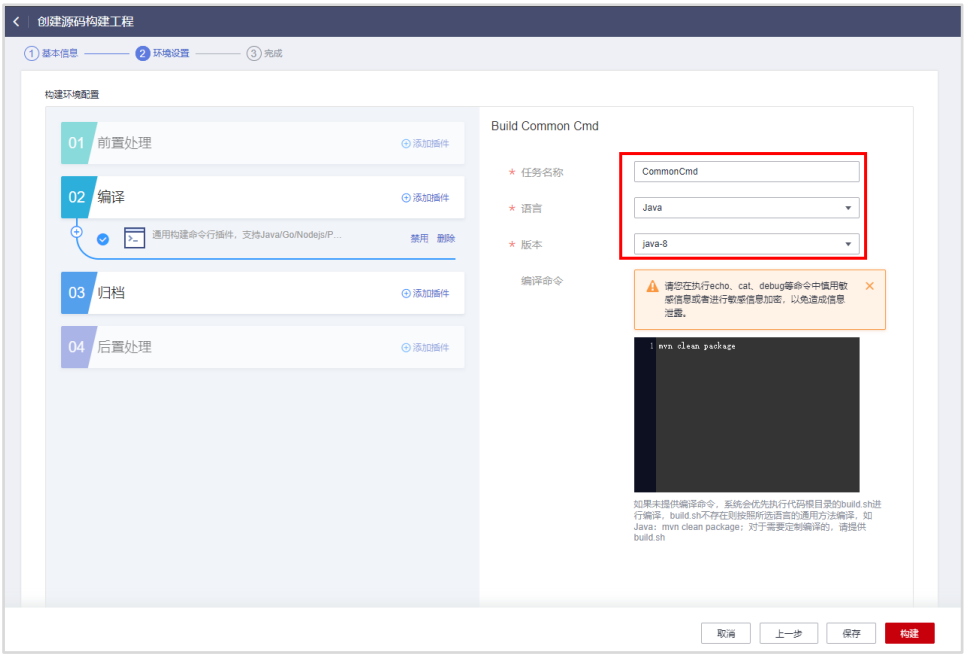


图7-41

步骤 5 在“编译”栏中，单击“添加插件”，选择“Docker”，分别添加四条构建任务。

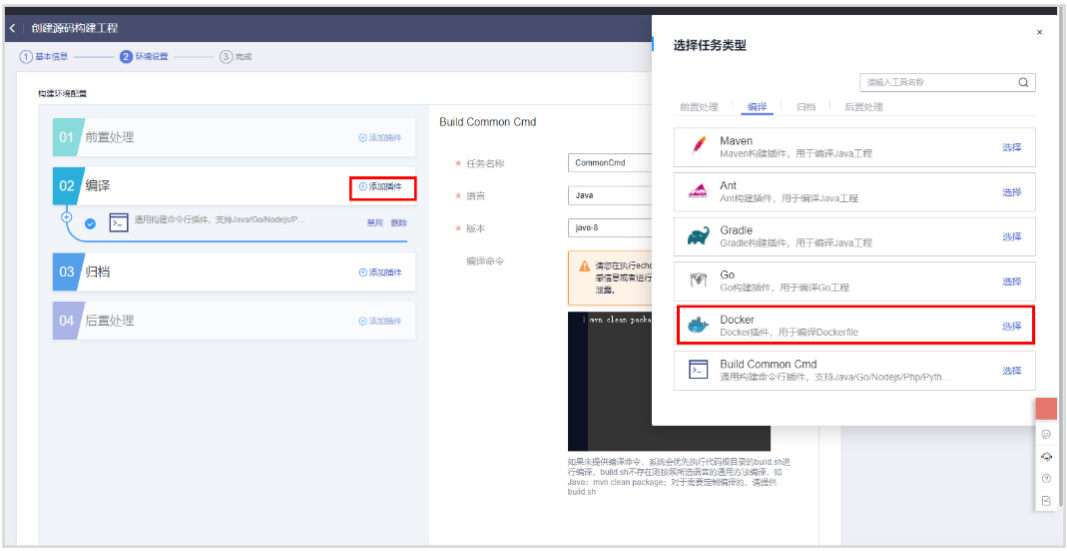


图7-42

步骤 6 按照以下配置创建第一条构建任务。

- 任务名称：Docker（保持默认即可，学员也可根据实际情况填写，下同）
- Dockerfile 路径：./weather/
- 镜像名称：weather
- 镜像版本：v1.0.${index}

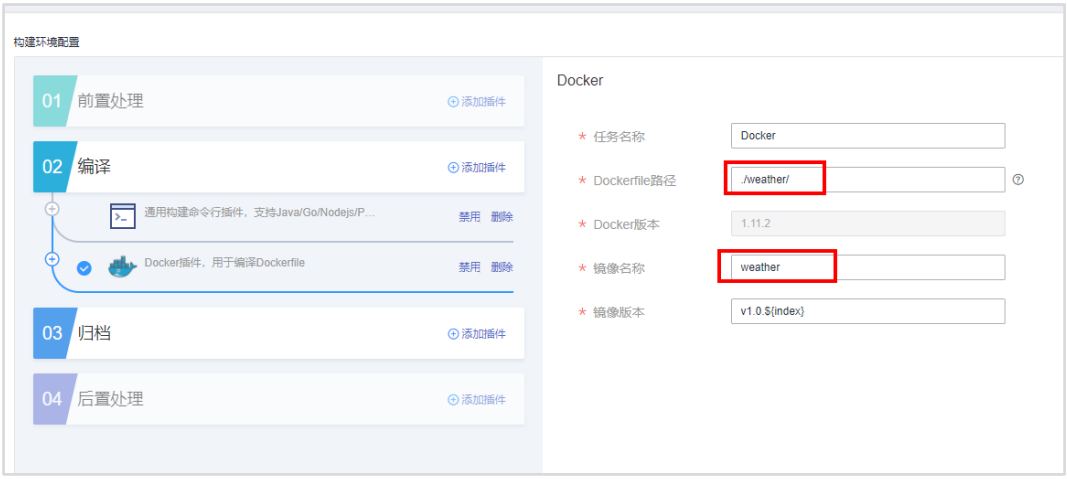


图7-43

步骤 7 重复上述步骤，创建第二条构建任务。

- 任务名称：Docker-4xsb8p
- Dockerfile 路径：./weather-beta/
- 镜像名称：weather-beta
- 镜像版本：v1.0.${index}

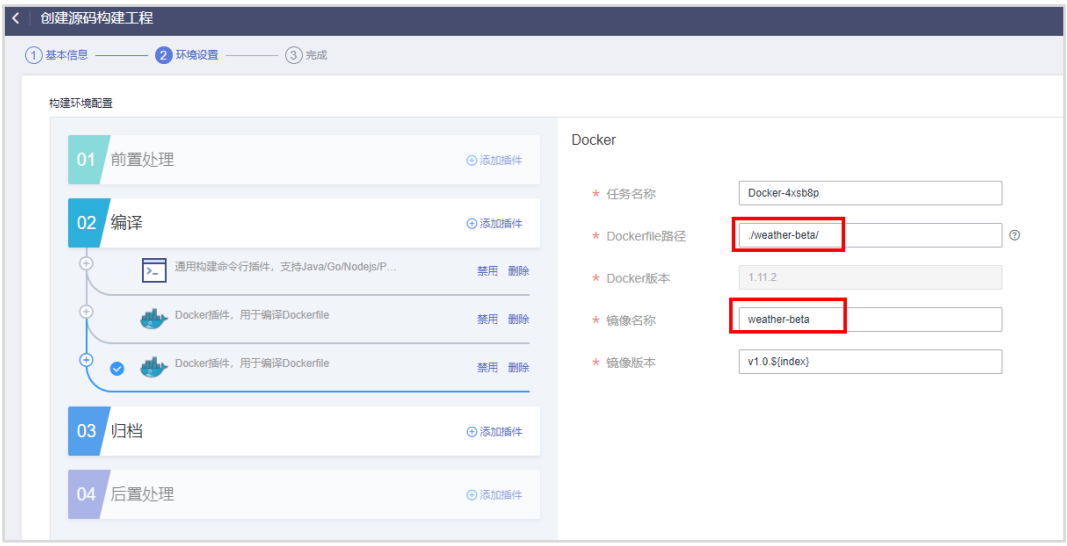


图7-44

步骤 8 重复上述步骤，创建第三条构建任务。

- 任务名称：Docker-5e40k3
- Dockerfile 路径：./forecast/
- 镜像名称：forecast
- 镜像版本：v1.0.${index}

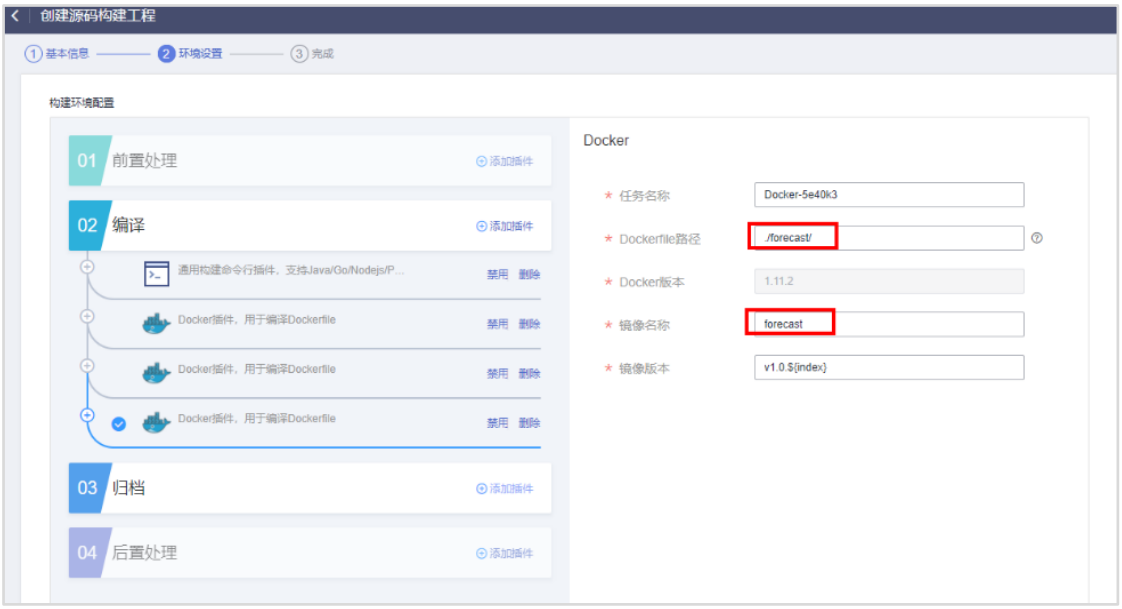


图7-45

步骤 9 重复上述步骤，创建第四条构建任务。

- 任务名称：Docker-aom49h
- Dockerfile 路径：./fusionweather/
- 镜像名称：fusionweather

- 镜像版本：v1.0.${index}

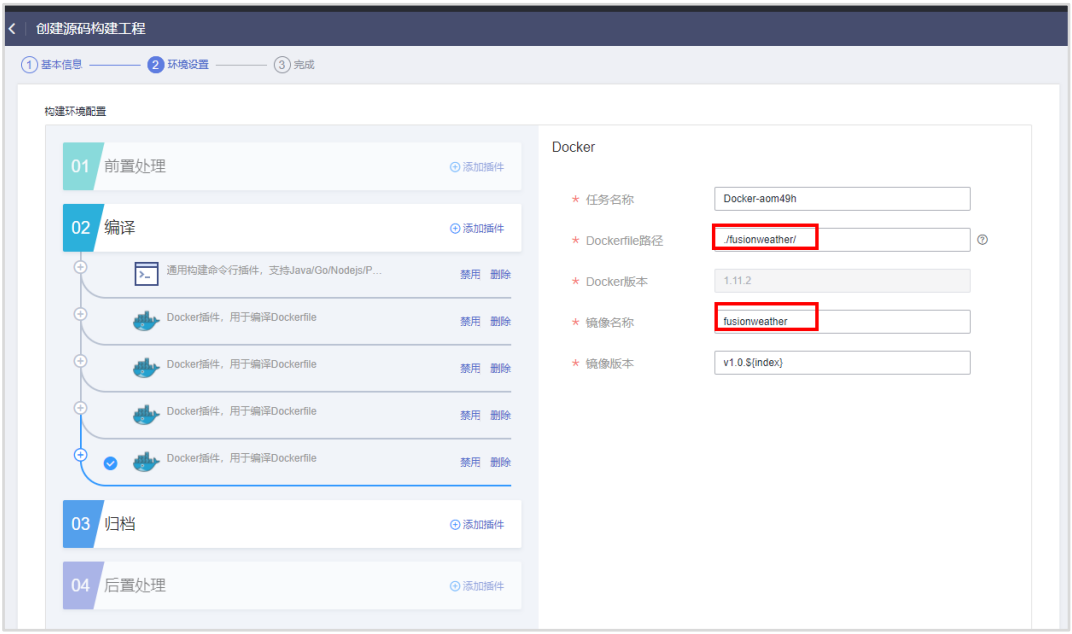


图7-46

步骤 10 在“归档”栏中，单击“添加插件”，选择“Publish Build Image”。

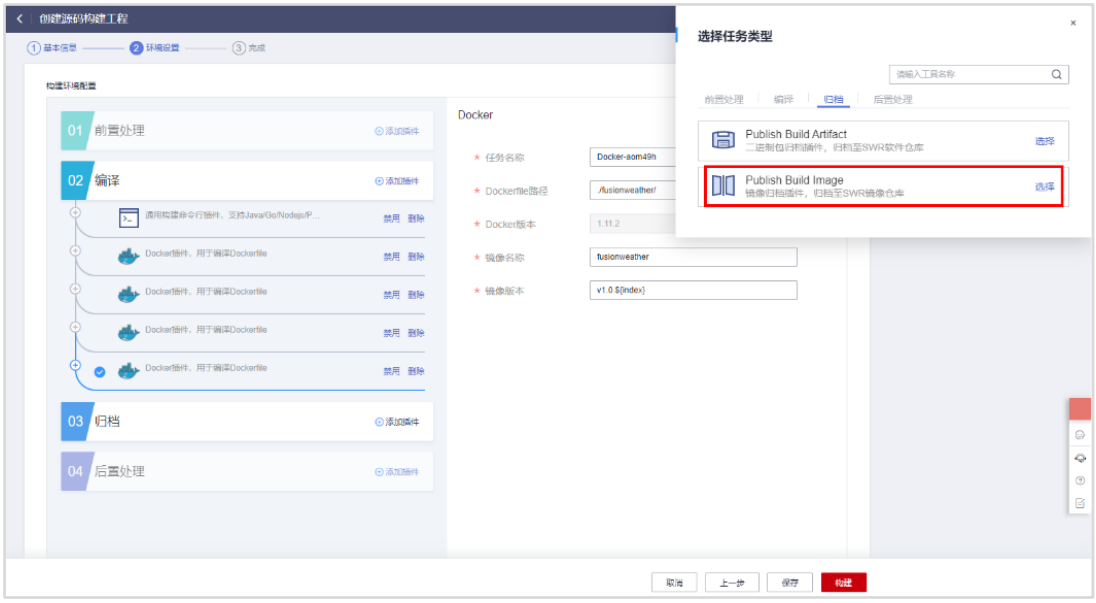
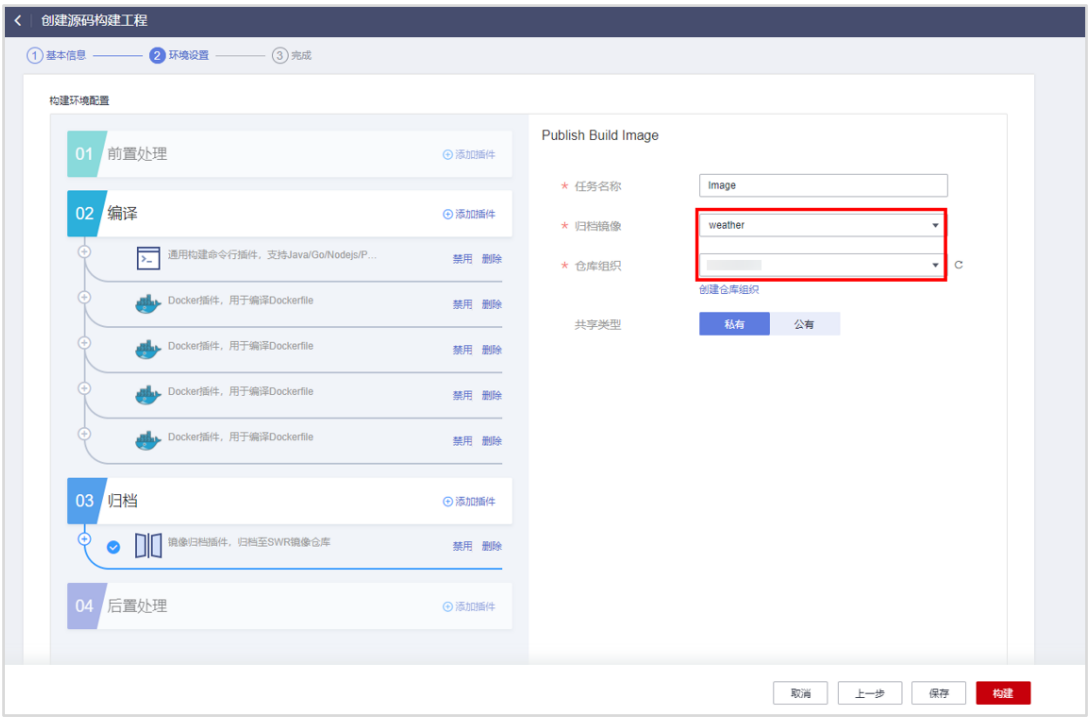
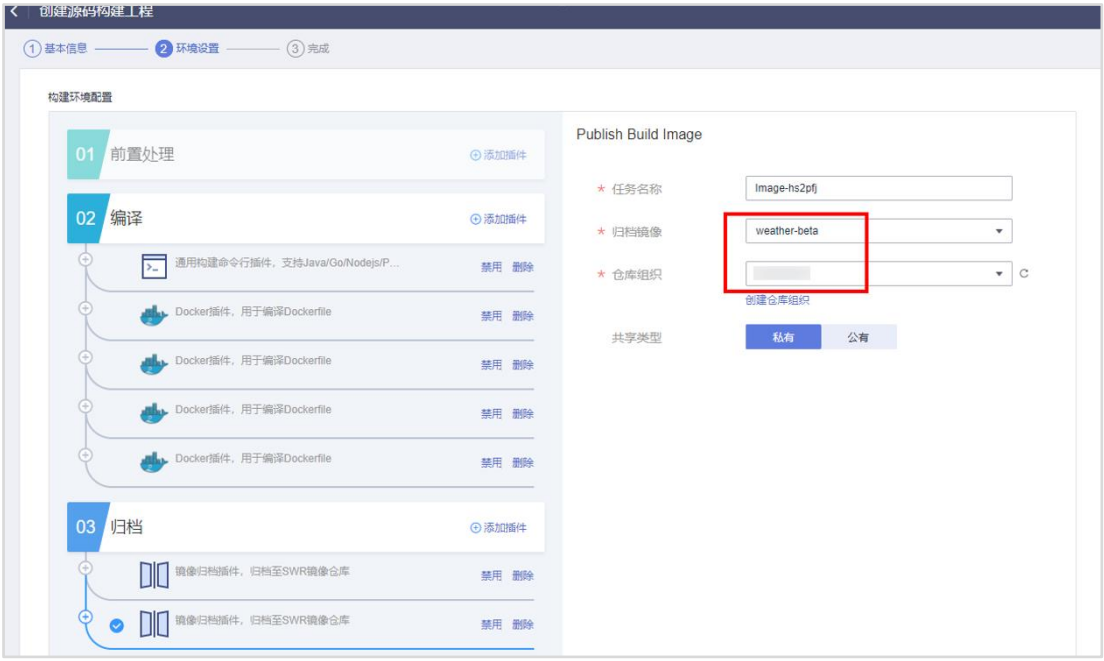


图7-47

步骤 11 在“归档镜像”中分别选择四个已创建的镜像名称（weather、weather-beta、forecast、fusionweather），任务名称保持默认即可，仓库组织选择之前创建的仓库组织“hcip”。

说明：该任务成功后，镜像包会自动归档到镜像仓库，供后续步骤使用。


创建源码构建工程
1 基本信息
2 环境设置
3 完成
构建环境配置
01 前置处理
添加插件
02 编译
添加插件
通用构建命令行插件，支持Java/Go/Nodejs/P...
禁用 删除
Docker插件，用于编译Dockerfile
禁用 删除
Docker插件，用于编译Dockerfile
禁用 删除
Docker插件，用于编译Dockerfile
禁用 删除
Docker插件，用于编译Dockerfile
禁用 删除
03 归档
添加插件
镜像归档插件，归档至SWR镜像仓库
禁用 删除
04 后置处理
添加插件
Publish Build Image
* 任务名称
Image
* 归档镜像
weather
* 仓库组织
创建仓库组织
共享类型
私有
公有
取消
上一步
保存
构建


创建源码构建工程
1 基本信息
2 环境设置
3 完成
构建环境配置
01 前置处理
添加插件
02 编译
添加插件
通用构建命令行插件，支持Java/Go/Nodejs/P...
禁用 删除
Docker插件，用于编译Dockerfile
禁用 删除
Docker插件，用于编译Dockerfile
禁用 删除
Docker插件，用于编译Dockerfile
禁用 删除
Docker插件，用于编译Dockerfile
禁用 删除
03 归档
添加插件
镜像归档插件，归档至SWR镜像仓库
禁用 删除
镜像归档插件，归档至SWR镜像仓库
禁用 删除
Publish Build Image
* 任务名称
Image-hs2pfj
* 归档镜像
weather-beta
* 仓库组织
创建仓库组织
共享类型
私有
公有

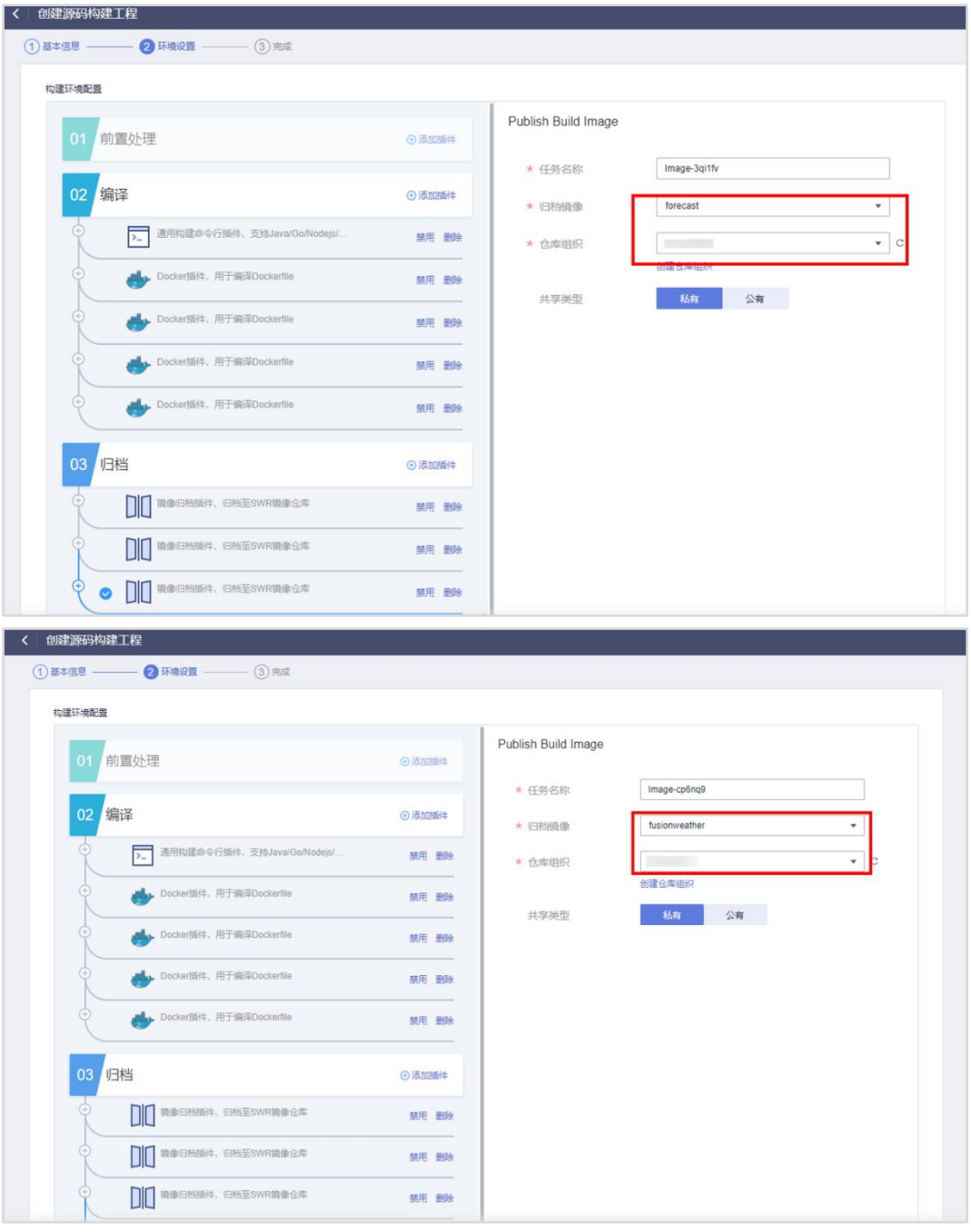


图7-48

步骤 12 单击“构建”，启动构建任务，如下图所示，证明后台应用 weathermap 构建成功。

图7-49

7.2.2.2 创建前台应用构建任务

步骤 1 登录 ServiceStage 控制台，选择“持续交付>构建”，单击“基于源码构建”。

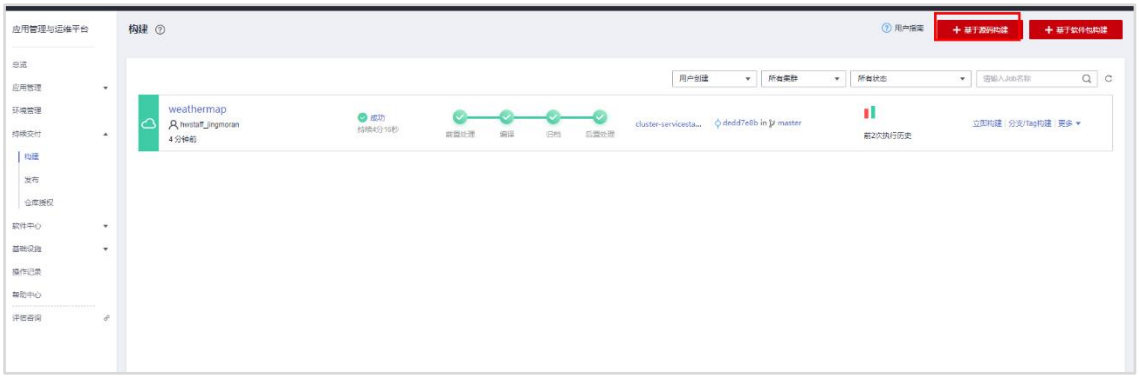


图7-50

步骤 2 按照以下内容配置基本信息。单击“下一步”。

- 名称：weathermapweb
- 代码来源：GitHub
- 授权信息：auth-github
- 用户名/组织：默认即可（学员 Github 账号的用户名/组织）
- 仓库名称：hcip
- 分支：master
- 构建集群：cluster-servicestage（选择资源准备步骤中创建的 CCE 集群）

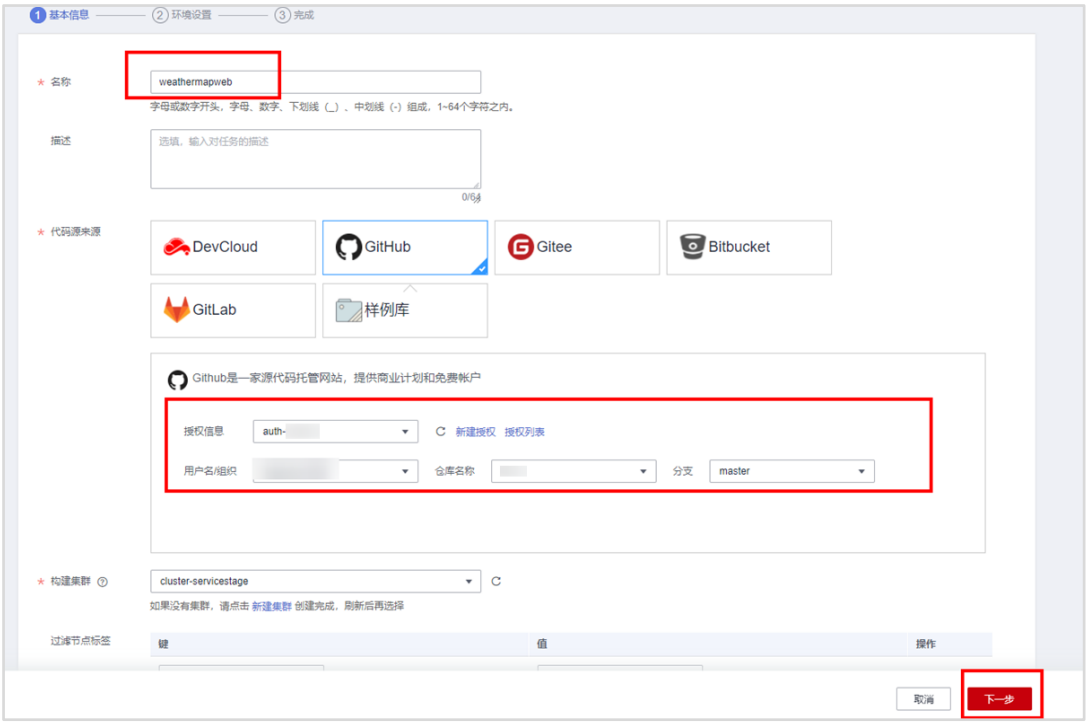


图7-51

步骤 3 选择 Docker 构建模板，并在必填项参数配置进行以下设置。

编译 Docker，添加一条构建任务，参数设置如下：

- Dockerfile 路径：./weathermapweb/
- 镜像名称：weathermapweb
- 仓库组织：hcip
- 其他参数保持默认

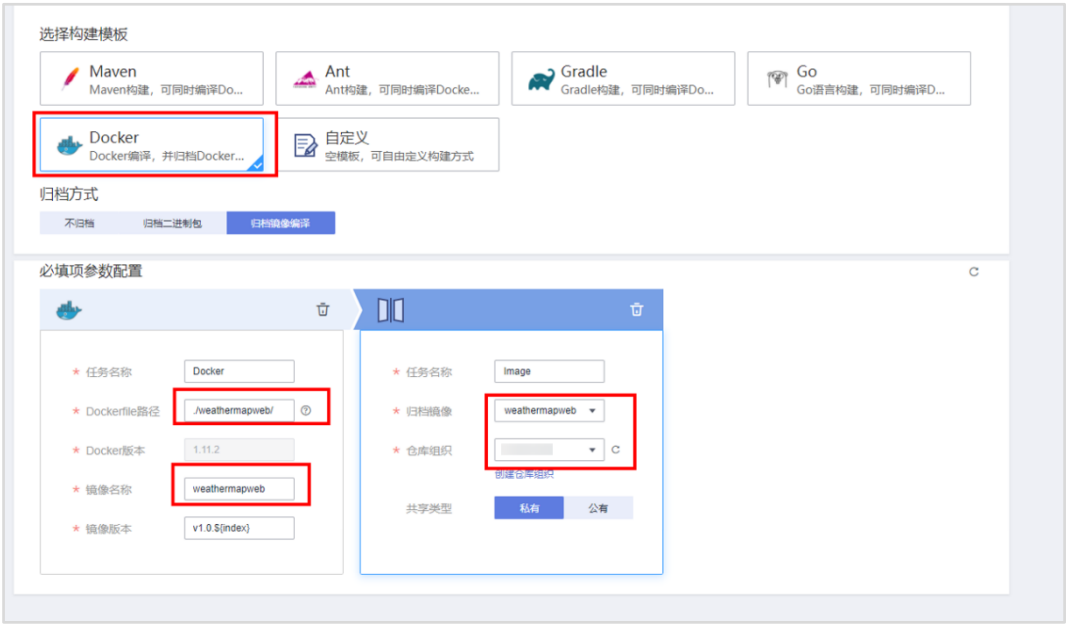


图7-52

步骤 4 单击“构建”，启动构建任务。如下图所示，证明前台应用 weathermapweb 构建成功。

图7-53

7.2.3 微服务部署

基于 ServiceStage 可以方便快捷地将微服务部署到容器（如 CCE）、虚拟机（如 ECS）或无服务器（如 CCI），同时支持源码部署、jar/war 包部署或 docker 镜像包部署。同时，ServiceStage 支持 Java、PHP、Node.js、Go、Python 多种编程语言应用的完全托管，包括部署、升级、回滚、启停和删除等。

本实践中使用了 Java 开发的后台组件和 Node.js 开发的前台组件。

7.2.3.1 创建并部署后台应用组件

说明：在本实验中，我们需要通过容器部署的方式部署应用并将微服务实例注册到微服务引擎 CSE 中。

步骤 1 登录 ServiceStage 控制台，选择“应用管理>应用列表”。

步骤 2 单击“操作”栏的“新增组件”。

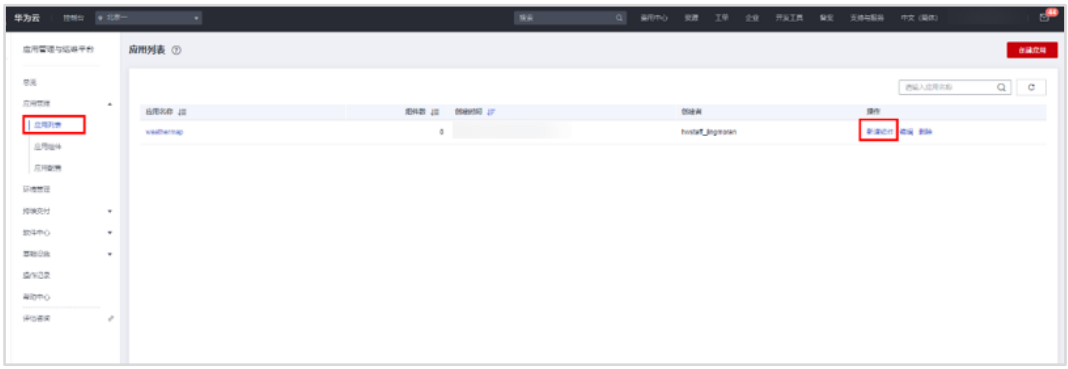


图7-54

步骤 3 “配置方式”选择“自定义配置”，“选择组件类型”选择“微服务”，单击“下一步”。

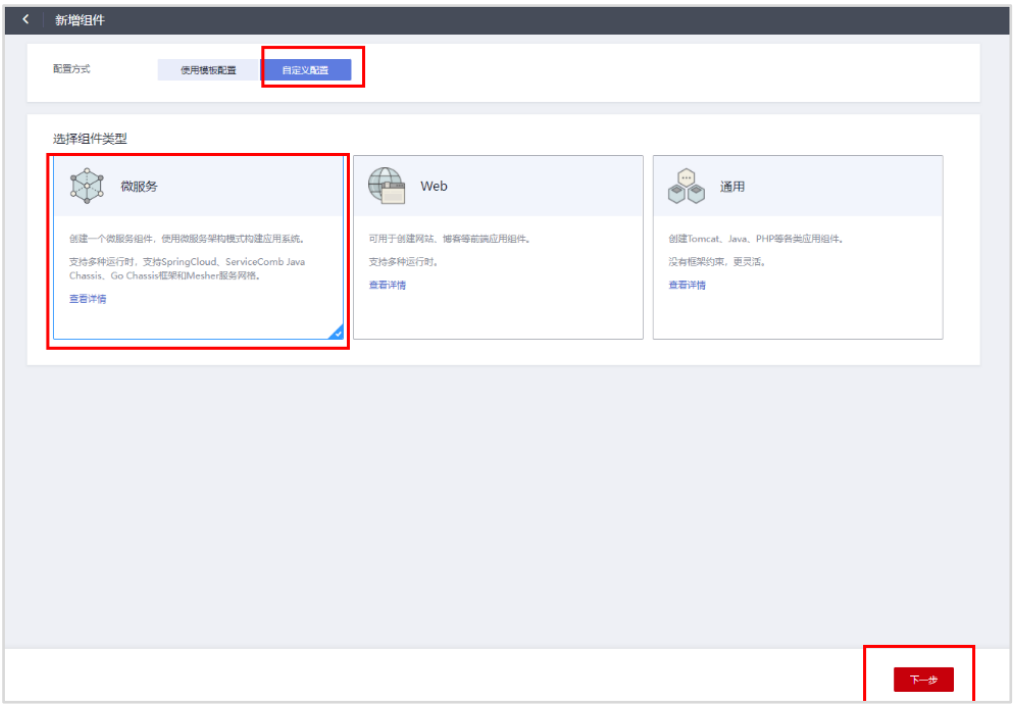


图7-55

步骤 4 “选择运行时”选择“Docker”，单击“下一步”。

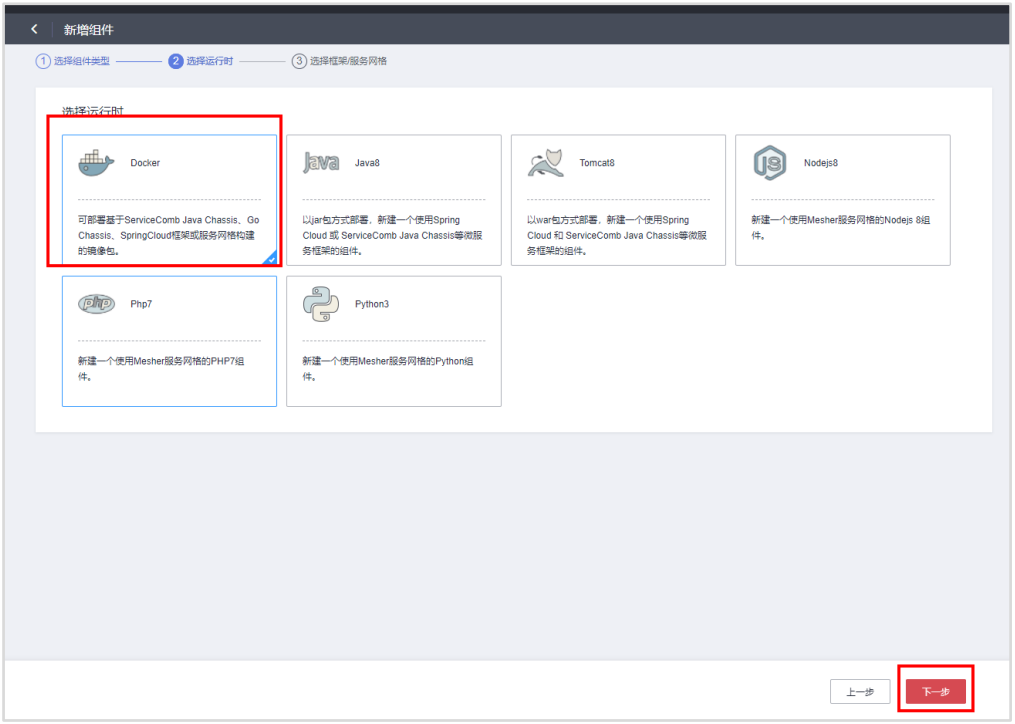


图7-56

步骤 5 选择 Java Chassis 框架/服务网格，组件名称填写“weather”。单击“创建并部署”，部署组件。

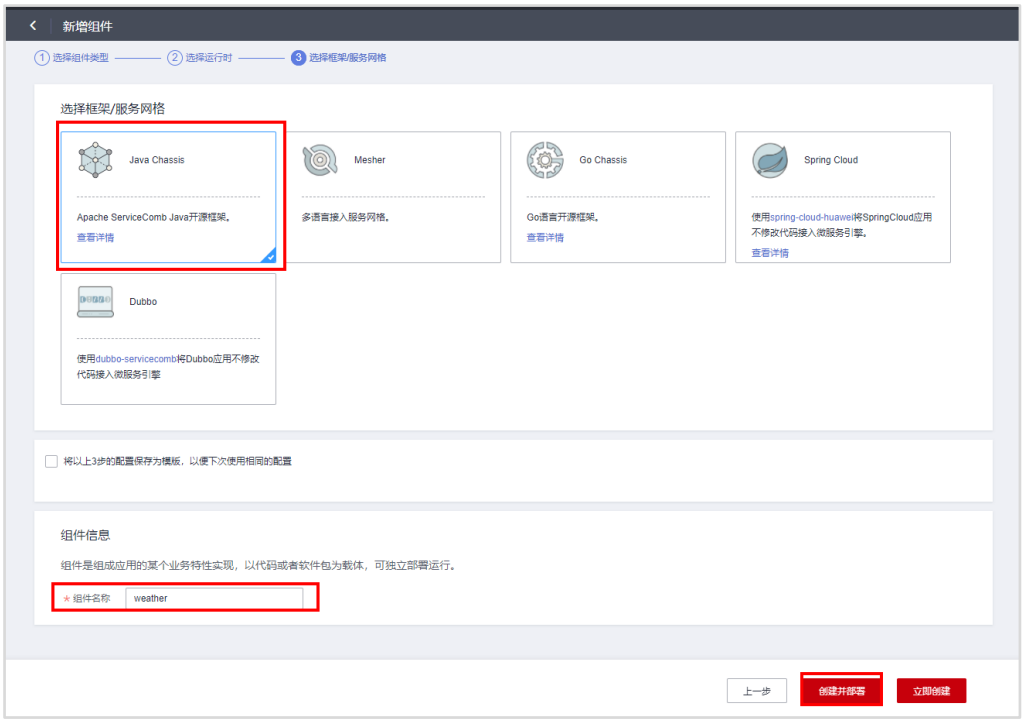


图7-57

步骤 6 按照以下配置填写相应参数，单击“下一步 组件配置”。

说明：应用组件部署以后，微服务会注册到设置的微服务引擎，所有应用组件需要注册到同一个微服务引擎，才能互相发现。

- 环境：test-env（选择资源准备步骤中创建的环境）
- 部署版本：1.0.0（根据列表提供的进行选择即可）
- 部署系统：云容器引擎
- 实例数量：1
- 其他配置：默认配置

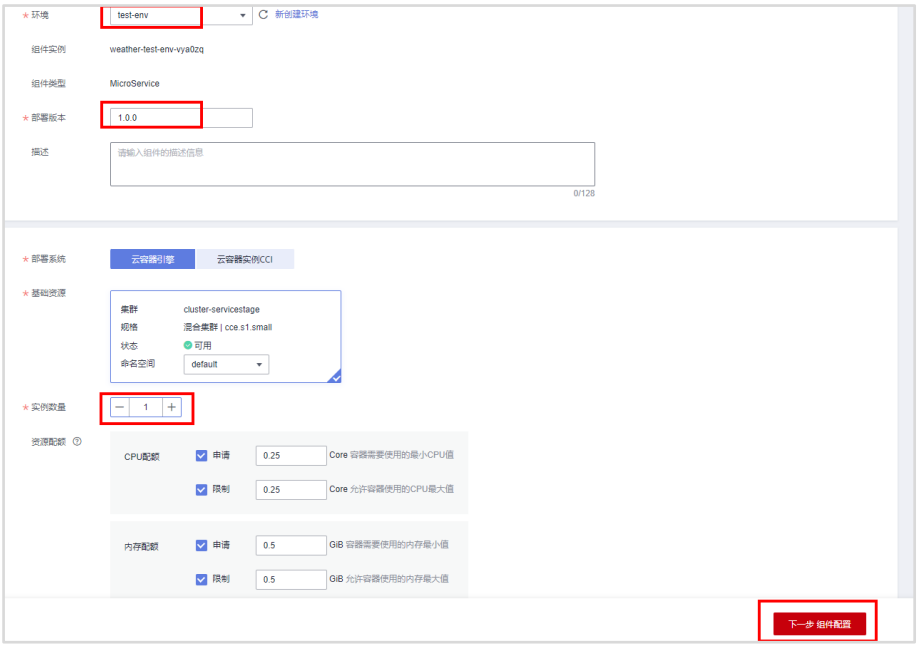


图7-58

步骤 7 点击“选择镜像”。

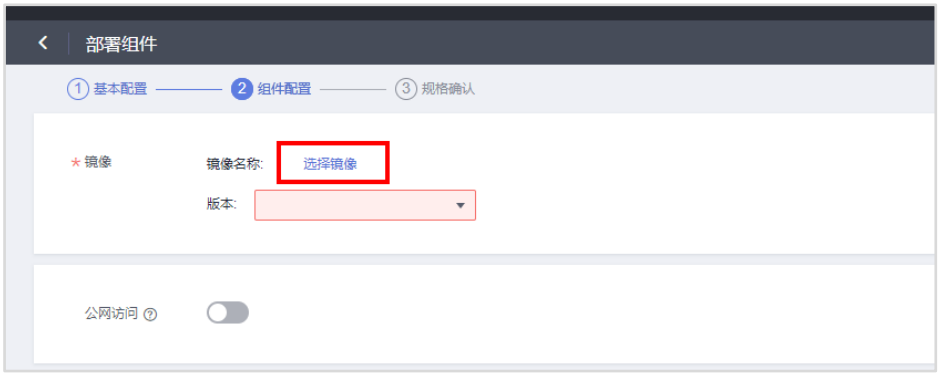


图7-59

步骤 8 在弹出的对话框中选择“weather”镜像。单击“确定”。

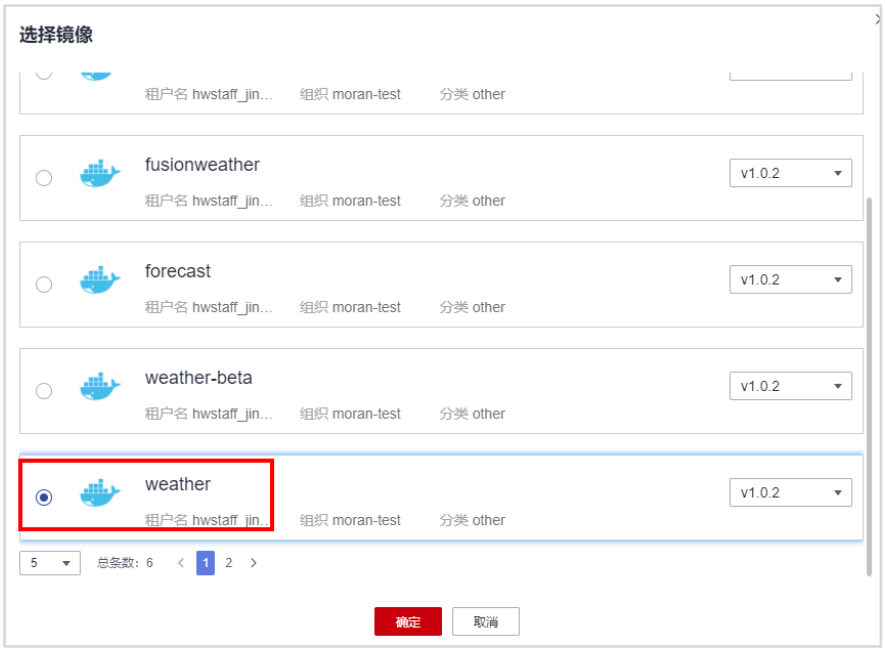


图7-60

步骤 9 以下其他配置：默认配置即可

图7-61

步骤 10 在“高级设置”中添加如下三条环境变量：

- MOCK_ENABLED：false

说明：资源准备时创建的 CCE 集群中的 ECS 节点如果已绑定弹性公网 IP 且能访问公网时，需设置该参数值为 false 或者不设置该参数。则应用所用到的天气数据为实时数据。

- servicecomb_credentials_accessKey：7.2.1.1 步骤中获取的 AK
- servicecomb_credentials_secretKey：7.2.1.1 步骤中获取的 SK

说明：仅当使用微服务引擎专业版时需要配置该 AK/SK。

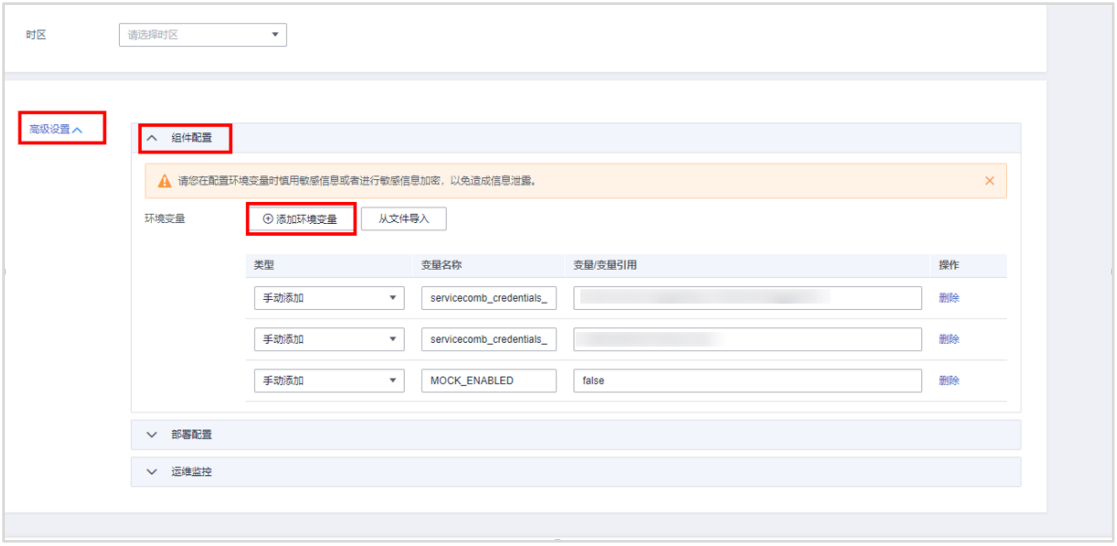


图7-62

步骤 11 单击“下一步 规格确认”，确认规格。单击“部署”，部署组件。

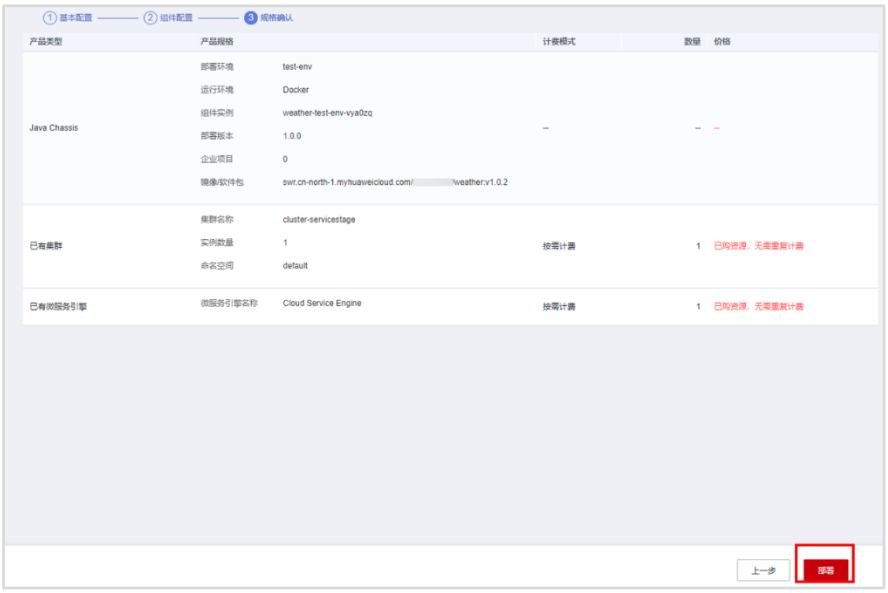


图7-63

步骤 12 查看已部署的服务。可以看到 weather 服务状态是“运行中”，证明该组件部署完成。

图7-64

步骤 13 重复上述步骤（如下图所示，具体步骤不再赘述），创建并部署 forecast 和 fusionweather 组件。

部署 forecast 组件：

- 框架/服务网格：Java Chassis
- 组件名称：forecast

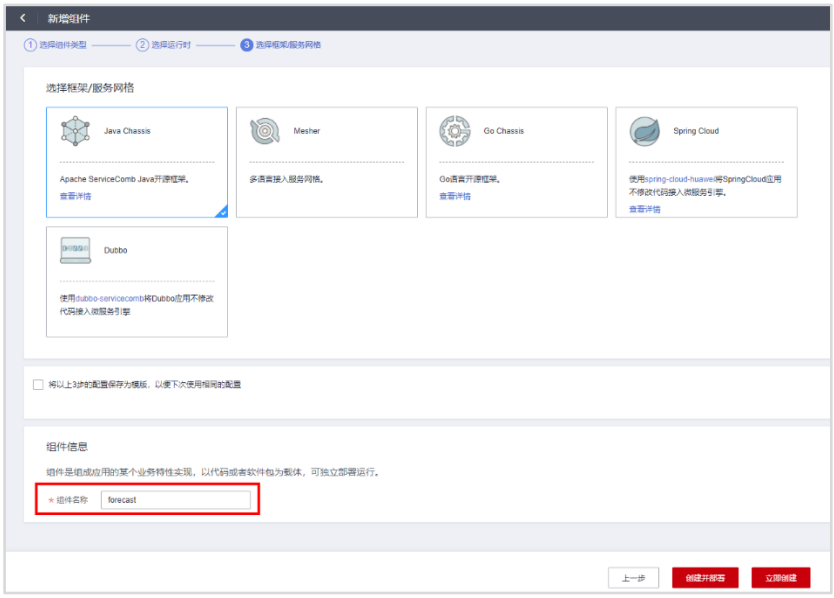


图7-65

- 环境：test-env

- 部署版本：1.0.0
- 部署系统：云容器引擎
- 实例数量：1
- 其他配置：默认配置

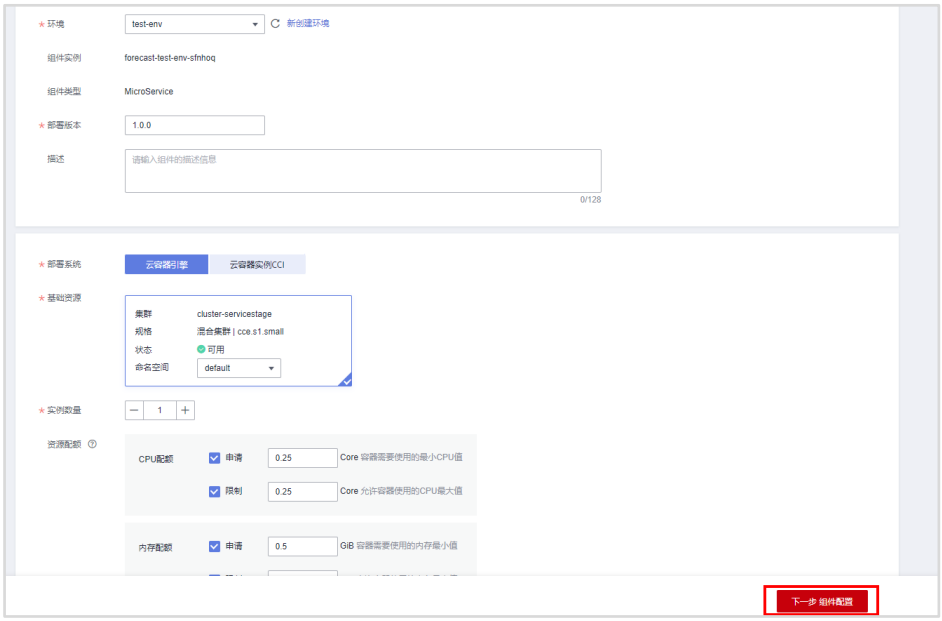


图7-66

- 选择镜像“forecast”

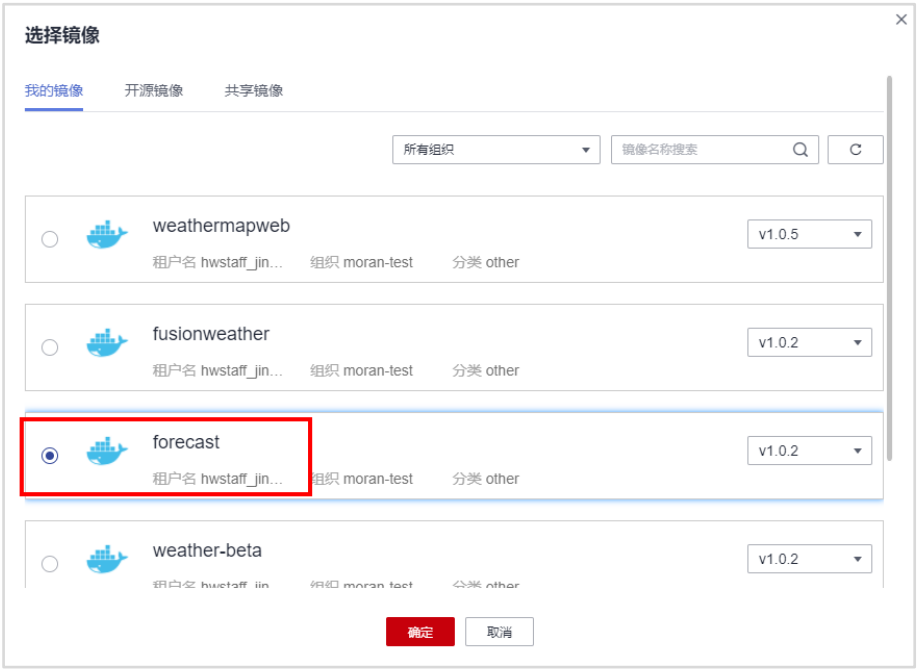


图7-67

在高级设置中添加如下环境变量。

- MOCK_ENABLED：false

- servicecomb_credentials_accessKey：7.2.1.1 步骤中获取的 AK
- servicecomb_credentials_secretKey：7.2.1.1 步骤中获取的 SK

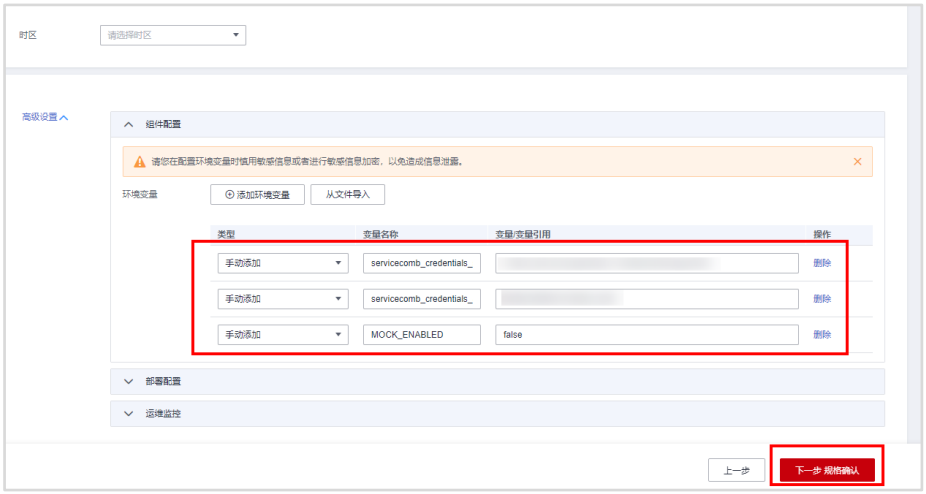


图7-68

部署 fusionweather 组件：

- 框架/服务网格：Java Chassis
- 组件名称：fusionweather

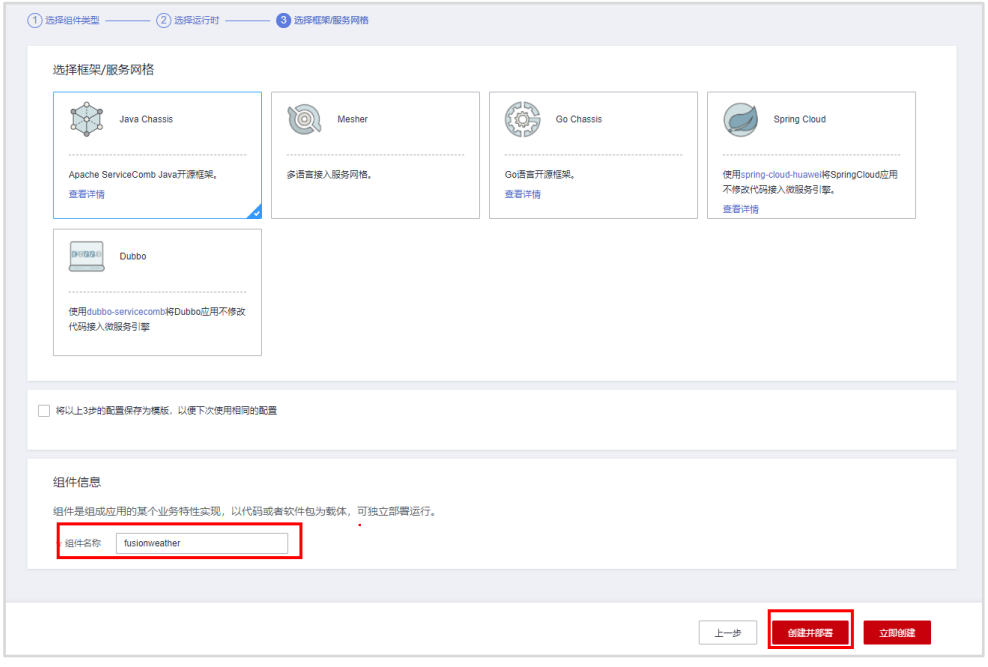


图7-69

- 环境：test-env
- 部署版本：1.0.0
- 部署系统：云容器引擎
- 实例数量：1

- 其他配置：默认配置

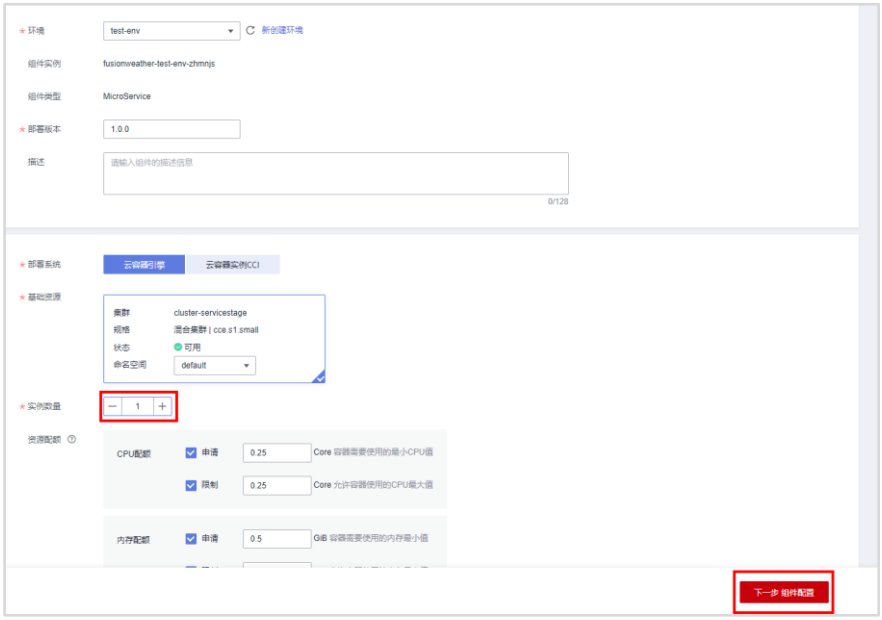


图7-70

- 选择 fusionweather 镜像

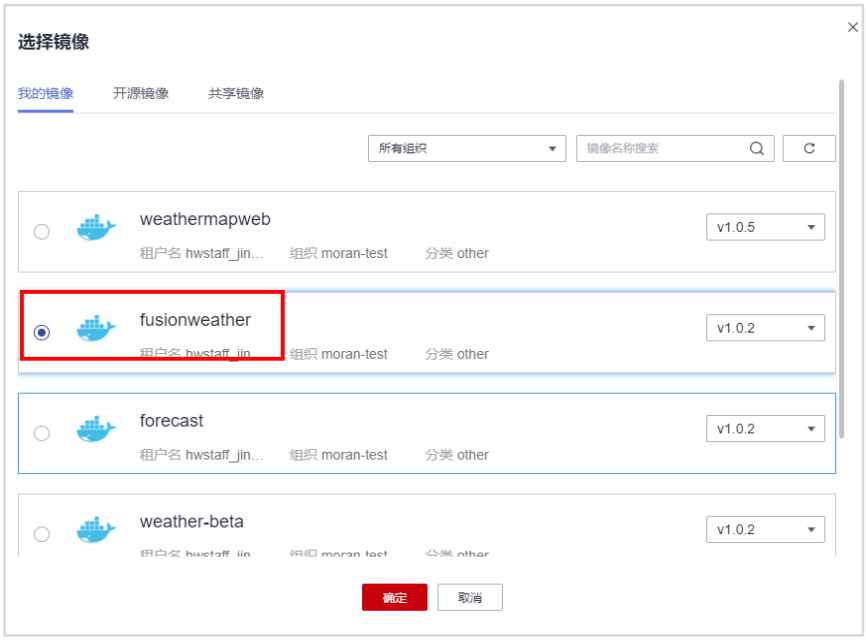


图7-71

在高级设置中添加如下环境变量。

- servicecomb_credentials_accessKey：7.2.1.1 步骤中获取的 AK
- servicecomb_credentials_secretKey：7.2.1.1 步骤中获取的 SK

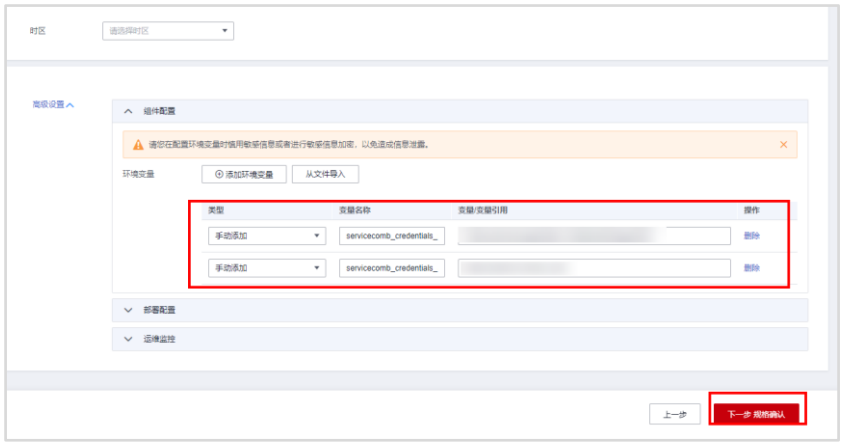


图7-72

步骤 14 在“应用管理与运维平台”界面点击已创建的应用名称“weathermap”查看微服务部署情况，如下图所示，三个服务状态都为“正常”，证明通过以上配置，后台应用组件 fusionweather、forecast、weather 部署完成。

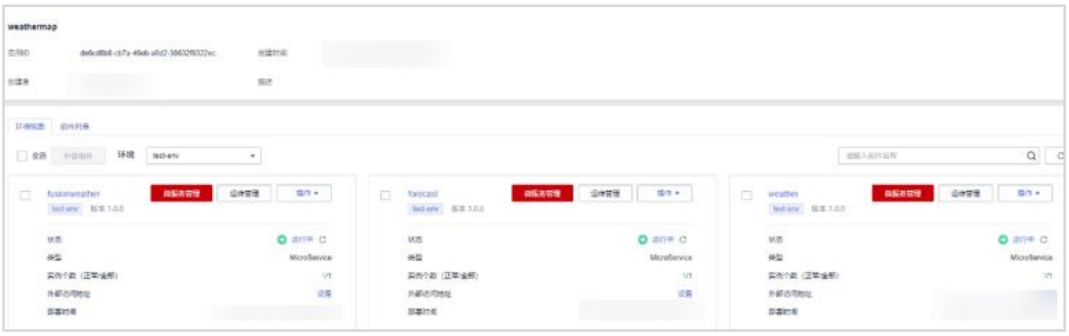


图7-73

7.2.3.2 创建并部署前台应用组件

步骤 1 登录 ServiceStage 控制台，选择“应用管理>应用列表”。

步骤 2 单击“操作”栏的“新增组件”。

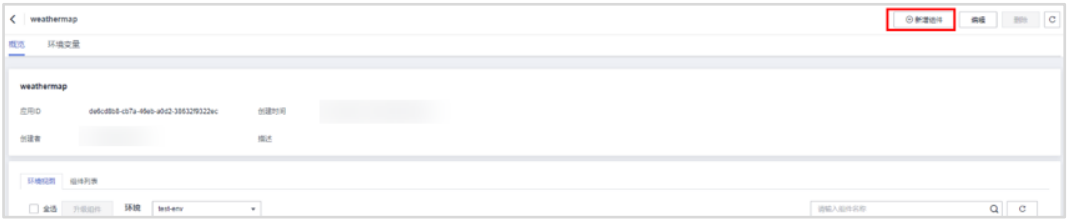


图7-74

步骤 3 “配置方式”选择“自定义配置”。组件类型选择“微服务”，单击“下一步”。

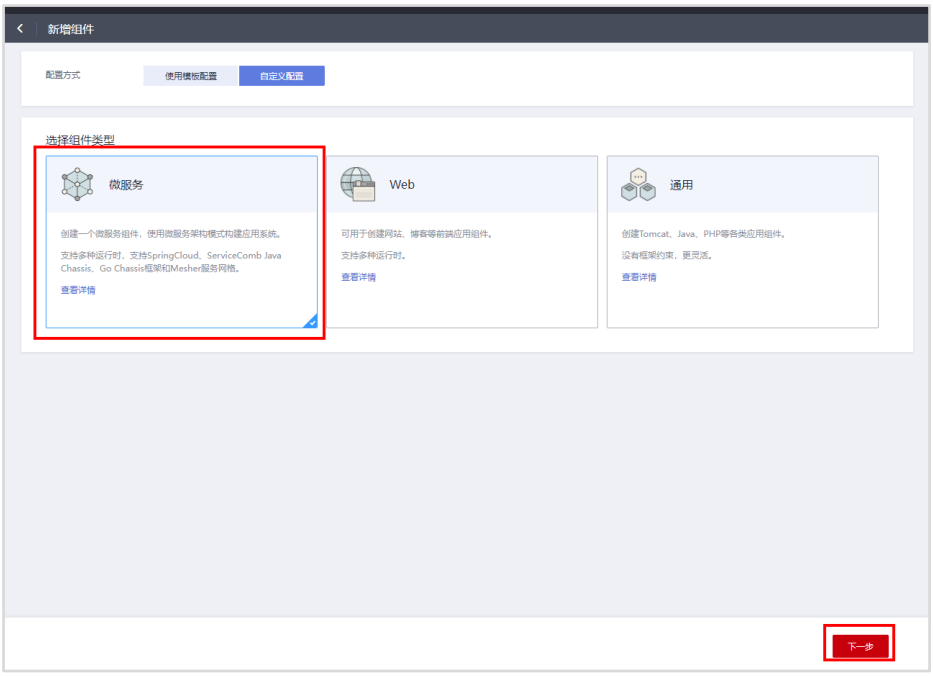


图7-75

步骤 4 “选择运行时”选择“Docker”，单击“下一步”。

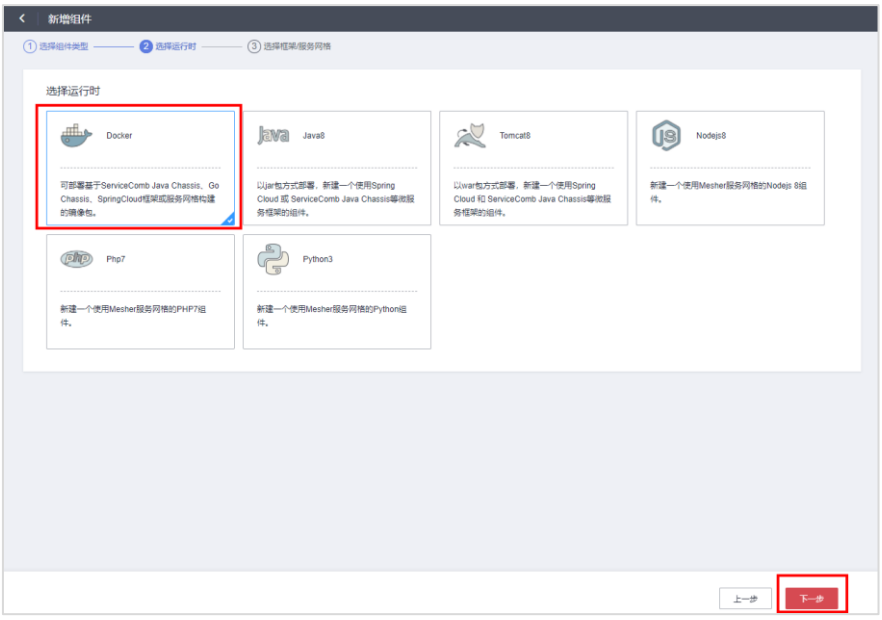


图7-76

步骤 5 按照以下配置创建服务组件。单击“下一步”。

- 框架/服务网格：Mesher
- 组件名称：weathermapweb

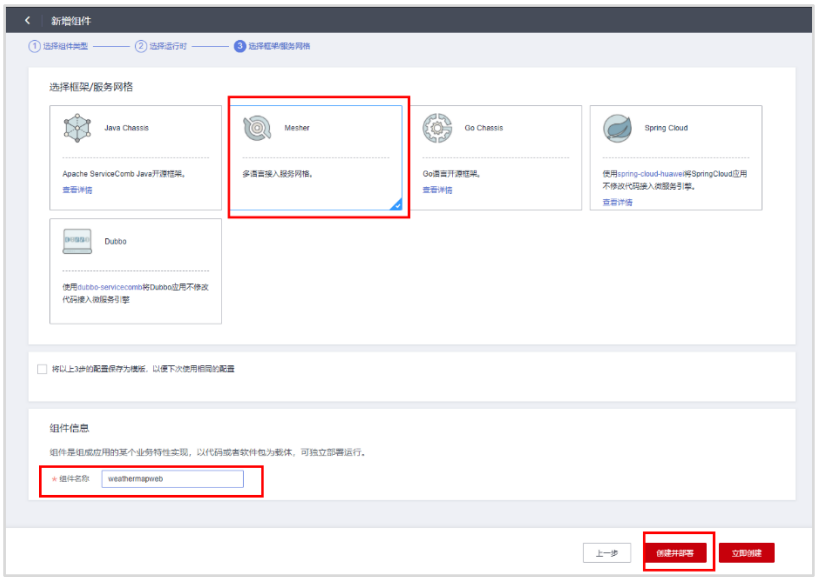


图7-77

步骤 6 按照以下配置内容填入相关参数。单击“下一步 组件配置”。

- 环境：test-env
- 部署版本：1.0.0
- 部署系统：云容器引擎
- 实例数量：1
- 其他配置：默认配置

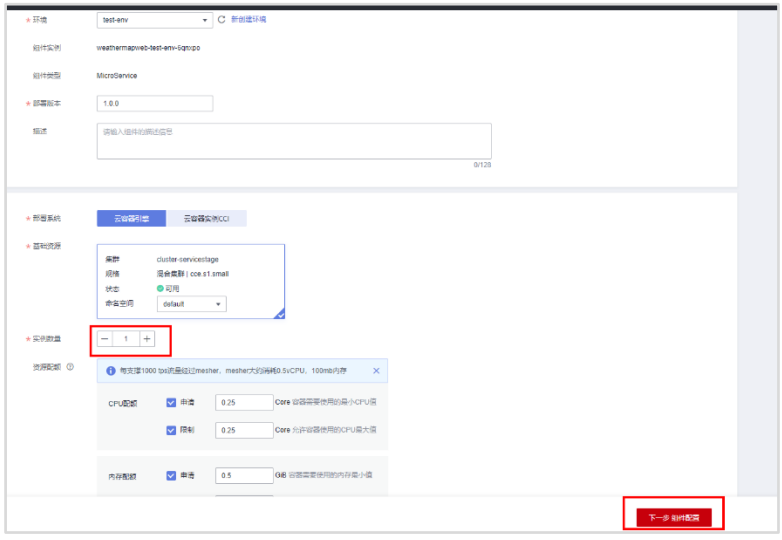


图7-78

步骤 7 单击“选择镜像”。

图7-79

步骤 8 在弹出的对话框中选择“weathermapweb”镜像。单击“确定”。

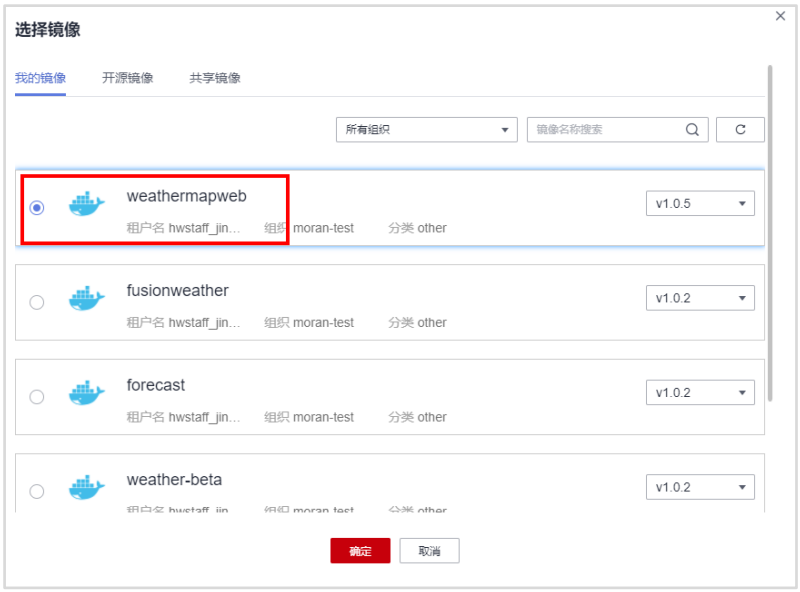


图7-80

步骤 9 其余保持默认配置。

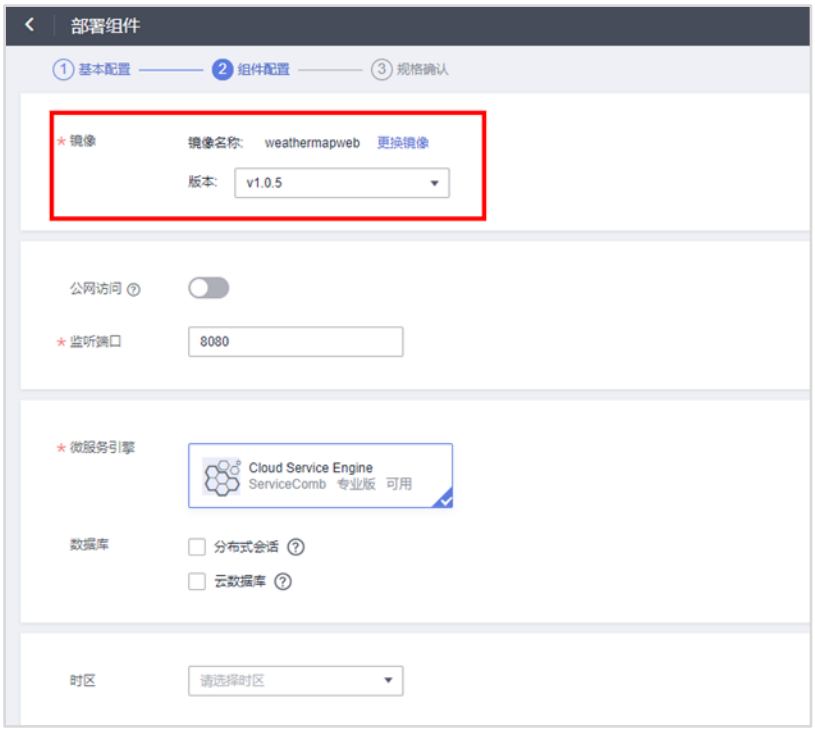


图7-81

步骤 10 单击“部署”，部署组件。

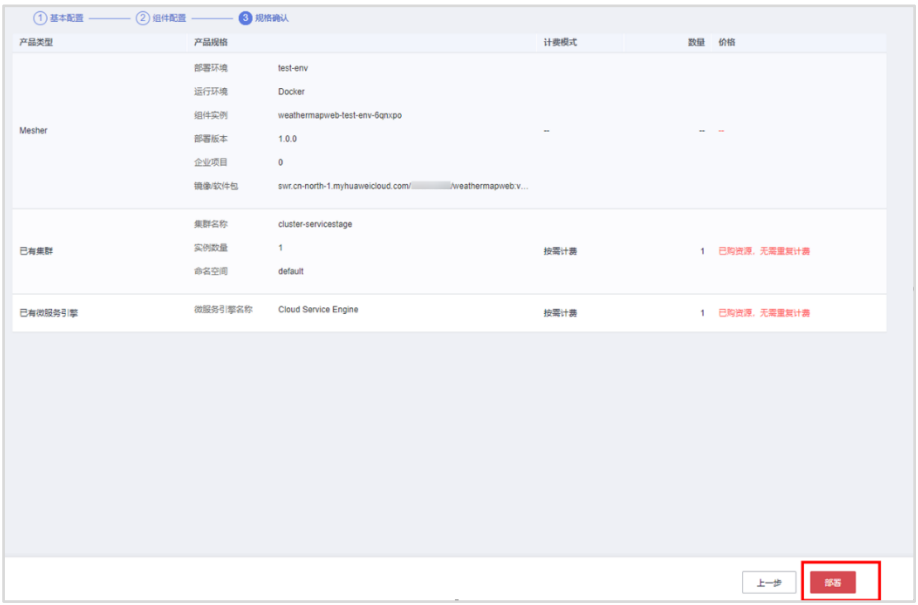


图7-82

步骤 11 查看已部署的微服务，可以看到 weathermapweb 服务状态为“运行中”，证明该服务组件部署完成。

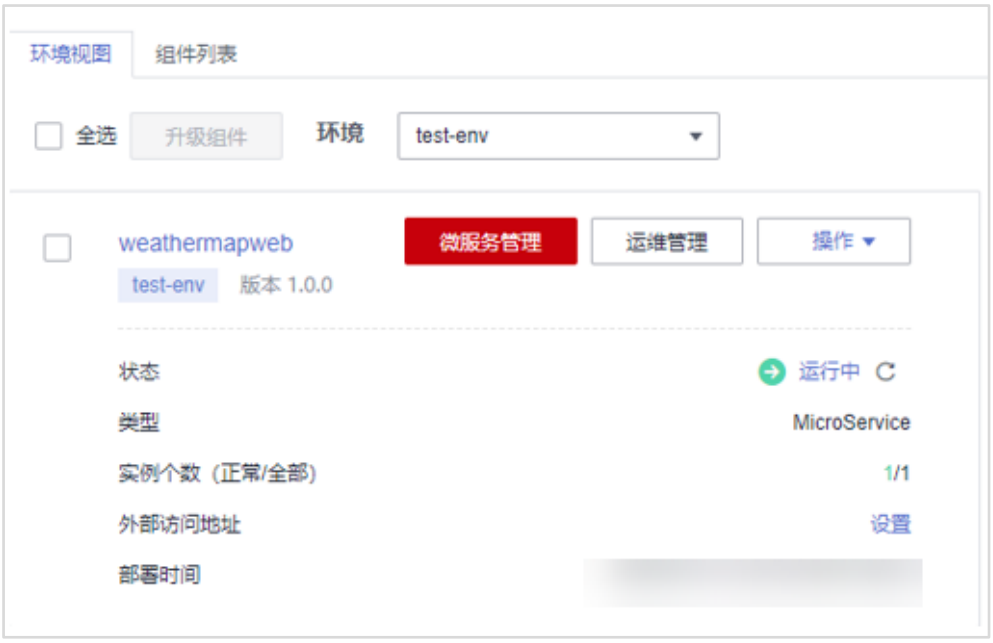


图7-83

步骤 12 登录 ServiceStage 控制台，选择“基础设施>微服务引擎（CSE）”。

步骤 13 选择创建环境时选择的微服务引擎，单击“查看控制台”

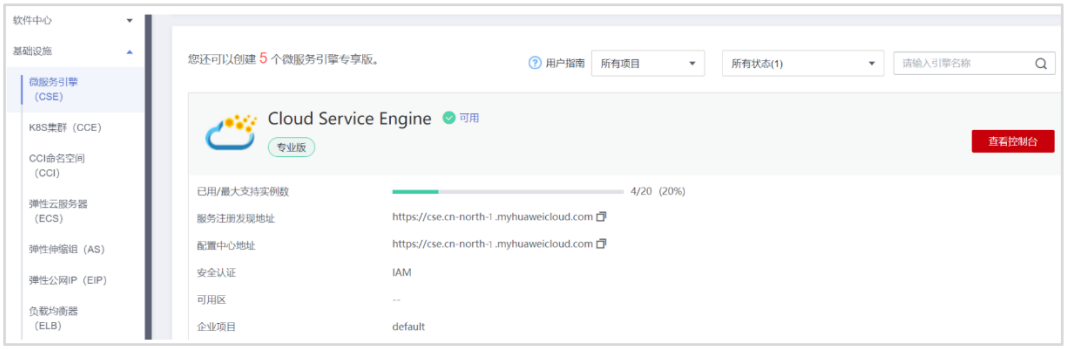


图7-84

步骤 14 在“服务目录>微服务列表”中，如果存在如下 4 个已部署的微服务，且各微服务实例数不为 0，则部署成功。

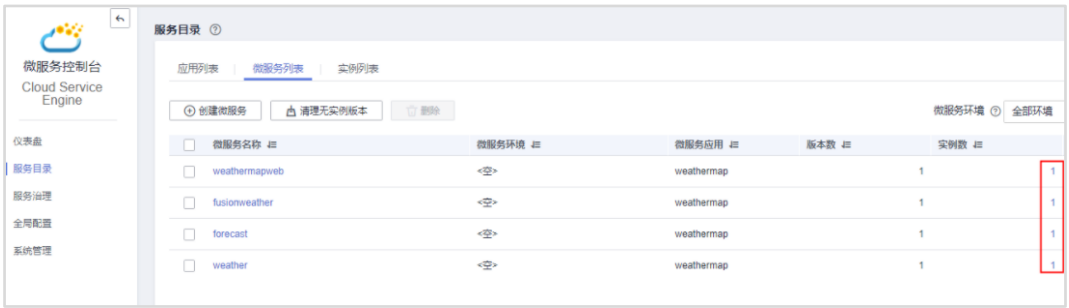


图7-85

7.2.3.3 添加访问方式

步骤 1 登录 ServiceStage 控制台，选择“应用管理>应用列表”。

步骤 2 单击“weathermap”应用名称，进入应用“概览”页。

步骤 3 单击“weathermapweb”服务名称，进入服务“概览”页。

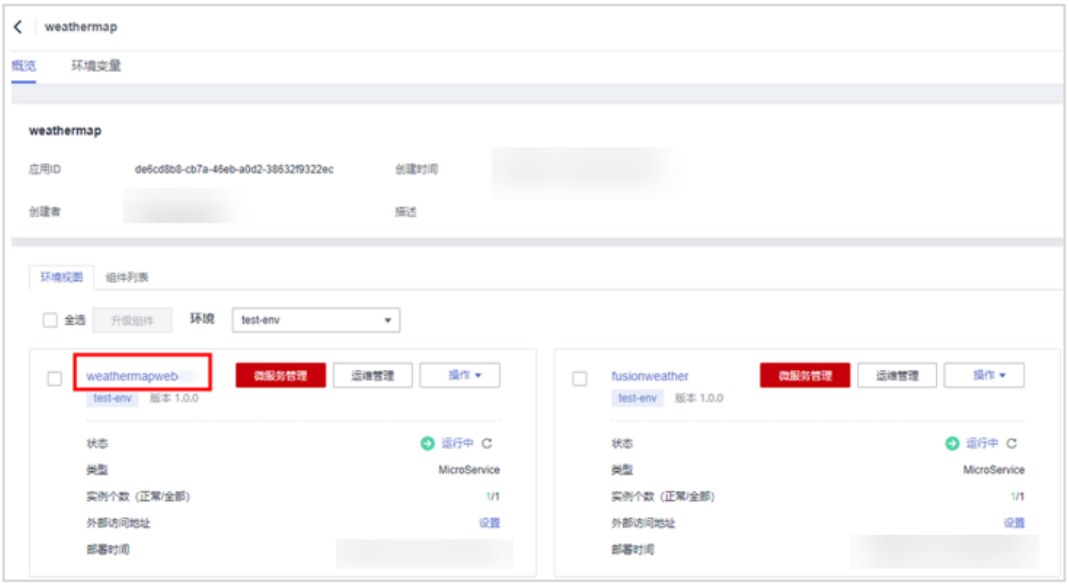


图7-86

步骤 4 在“访问方式”页签中，单击“添加服务”。

图7-87

步骤 5 按照以下配置填写相应参数。

- 服务名称：weathermapweb
- 访问方式：公网访问
- 访问类型：弹性 IP
- 服务亲和：集群级别
- 端口映射：TCP|3000|自动生成

图7-88

7.3 实验验证

步骤 1 登录 ServiceStage 控制台，选择“应用管理>应用列表”。

步骤 2 单击创建应用时创建的应用名称（例如 weathermap），进入应用“概览”页。

步骤 3 选择 weathermapweb 应用组件，单击“外部访问地址”后的链接。

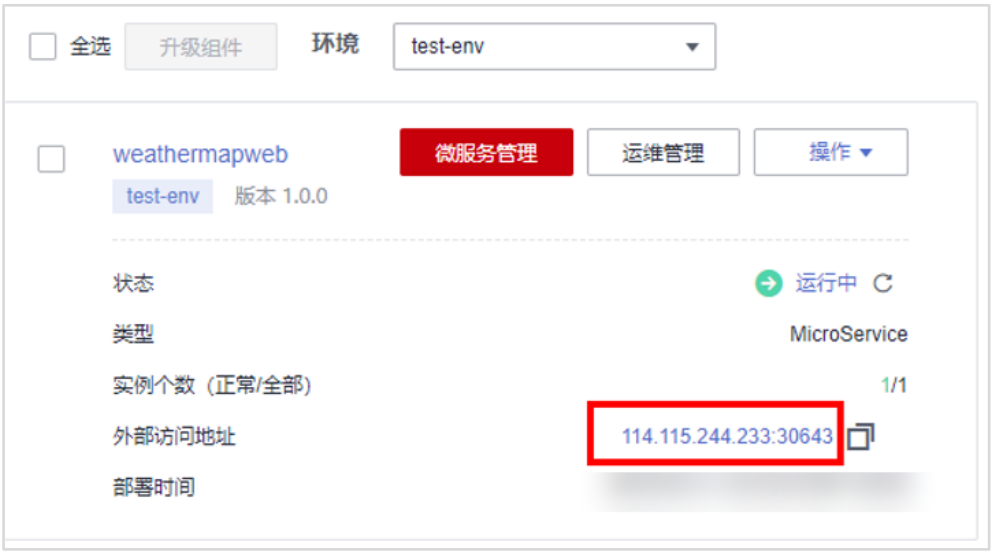


图7-89

步骤 4 如下图所示，证明通过以上配置，天气预报应用部署成功，该实验完成。

说明：首次访问应用时，weather 系统就绪需要一段时间。如果如上图所示页面没有出现，请持续刷新页面。

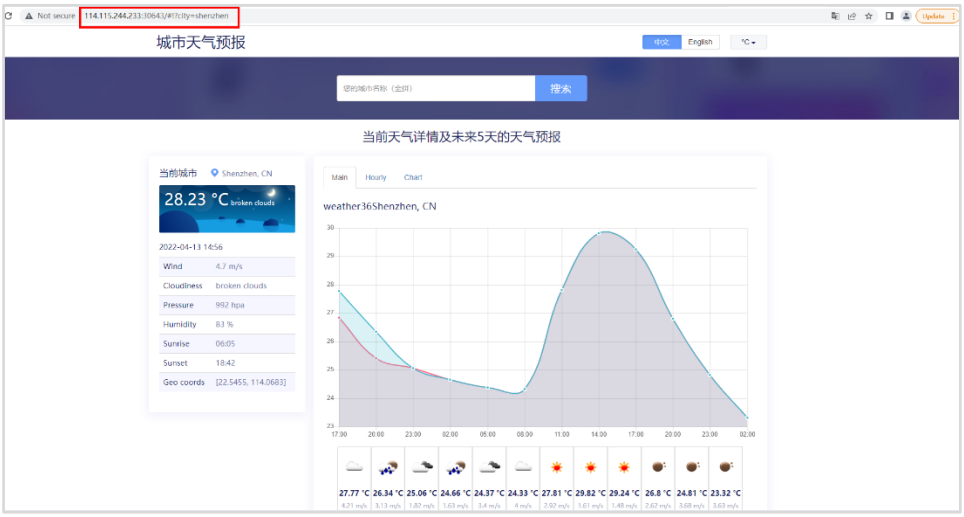


图7-90

7.4 实验恢复

步骤 1 删除微服务。

- 登录 ServiceStage 控制台，选择“应用管理>应用列表”，单击“weathermap”应用名称，进入应用“概览”页。
- 在“环境视图”页签下，选择本实验中创建组件右上角的“操作>删除”。
- 返回应用列表，点击本实验创建的应用“weathermap”操作栏中的“删除”。

步骤 2 删除构建任务。

- 登录 ServiceStage 控制台，选择“持续交付>构建”，选择本实验创建的构建任务对应操作栏中的“更多>删除”。

步骤 3 删除仓库授权。

- 登录 ServiceStage 控制台，选择“持续交付>仓库授权”，选择本实验创建的仓库授权对应的“删除”。

步骤 4 删除组织。

- 登录 ServiceStage 控制台，选择“软件中心>组织管理”，选择本实验创建组织对应操作栏中的“删除”。

步骤 5 删除环境。

- 登录 ServiceStage 控制台，选择“环境管理”，选择本实验创建的环境对应操作栏中的“删除”。

步骤 6 删除 CCE 节点。

- 服务列表中选择“云容器引擎 CCE”，在左侧页签中选择“节点管理”，在节点列表中找到本实验创建的引擎节点，点击操作栏的“更多>删除”。

步骤 7 删除 VPC。

- 在服务列表中选择“虚拟私有云 VPC”，点击“子网”页签，在列表中找到本实验创建的子网，点击操作栏中的“删除”。
- 点击“虚拟私有云”页签，找到本实验创建的 VPC，点击操作栏中的“删除”。

7.5 思考题

问题：应用组件部署完成后，状态显示为“未就绪”，表示应用组件部署失败，如何查看该应用组件部署失败的原因?

参考答案：登录 ServiceStage 控制台，选择“应用管理>应用列表”，单击应用名称，进入应用“概览”页，单击应用名称，进入应用“概览”页，选择状态异常的组件版本，单击组件名称，进入组件实例“概览”页，单击“实例列表”，单击实例名称前的箭头按钮，再单击“事件”，在事件列表中，查看事件描述信息，判断应用组件部署失败的原因。

8 云上运维设计实验

8.1 实验介绍

8.1.1 关于本实验

本实验分为以下 3 个部分：

1. 云监控服务 CES：查看云监控服务指标并设计使用云监控服务配置主机、站点、事件监控。

2. 应用运维管理 AOM：设计将云主机接入 AOM 并为其配置阈值告警规则、日志转储和分析。

3. 应用性能监控 APM：设计将 Tomcat 应用接入 APM，做到使用 APM 监控该应用组件性能数据。

说明：本实验以“北京四”区域为例，学员可以根据实际情况选择相应区域进行实验。

8.1.2 实验目的

理解云监控服务 CES 的配置和使用原理。

掌握通过应用运维管理 AOM 服务配置主机告警监控和日志采集分析的方法和原理。

掌握应用性能监控 APM 服务的配置方式和使用原理。

8.1.3 软件介绍

Tomcat 服务器是一个免费的开放源代码的 Web 应用服务器，属于轻量级应用服务器，在中小型系统和并发访问用户不是很多的场合下被普遍使用，是开发和调试 JSP 程序的首选。

JDK 全称 Java Development ToolKit，是 Java 语言开发工具包。JDK 是整个 JAVA 的核心，包括了 Java 运行环境（Java Runtime Envirnment）、Java 工具（javac/java/jdb 等）和 Java 基础的类库。

8.2 实验配置

8.2.1 资源准备

8.2.1.1 参照之前实验步骤创建 VPC

基本配置：

- 区域：华北-北京四
- 名称：vpc-3
- IPv4 网段：192.168.0.0/16

默认子网：

- 可用区：可用区 2
- 名称：vpc-3-subnet
- 子网 IPv4 网段：192.168.3.0/24

8.2.1.2 参照之前云主机创建步骤创建云主机 test

说明：该云主机仅用于本部分运维实验测试。

云主机“test”配置：

- 计费模式：按需计费
- 区域：华北-北京四
- 可用区：随机分配
- CPU 架构：x86 计算
- 规格：1 vCPUs | 2 GiB
- 镜像：公共镜像 | CentOS 7.6 64 bit
- 主机安全：开通主机安全（基础版）
- 网络：vpc-3 | vpc-3-subnet | 自动分配 IP 地址
- 安全组：default
- 弹性公网 IP：现在购买
- 线路：全动态 BGP
- 公网带宽：按流量计费
- 带宽大小：20 Mbit/s
- 系统盘：通用型 SSD | 40 GiB
- 云服务器名称：test
- root 密码：自定义

8.2.1.3 创建 SMN 服务主题

步骤 1 在服务列表中选择“消息通知服务 SMN”。

步骤 2 在左侧页签中选择“主题管理>主题”，点击右上角“创建主题”。

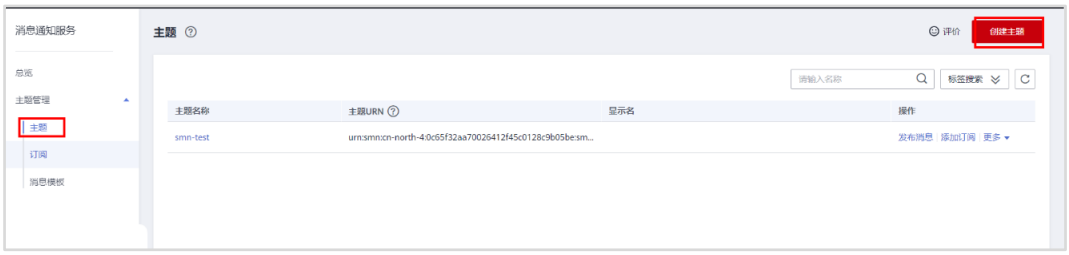


图8-1

步骤 3 配置主题名称并点击“确定”。

说明：本节实验后续多个服务共用该主题，主题名称学员可自定义，本实验中以“abc”为例。

图8-2

步骤 4 添加订阅。

- 在消息通知服务左侧页签中选择“订阅”，点击右上角“添加订阅”。

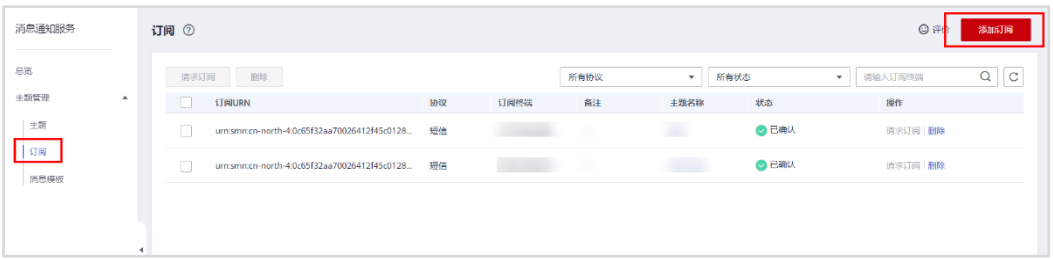


图8-3

- 主题名称选择刚创建的主题“abc”，协议可选邮件或短信等（这里以邮件为例），填写好订阅终端后点击“确定”。

图8-4

步骤 5 在订阅列表中可查看刚创建的订阅，点击“请求订阅”。

图8-5

步骤 6 在弹出的对话框中点击“是”。

图8-6

步骤 7 查看邮箱中收到的订阅邮件，点击“订阅确认”。

图8-7

步骤 8 返回订阅列表中查看当前订阅状态已变成“已确认”，证明订阅添加成功。

图8-8

8.2.1.4 创建 OBS 桶

步骤 1 在服务列表中选择“对象存储服务 OBS”。

说明：该桶供后续 AOM 日志转储使用。

图8-9

步骤 2 点击右上角“创建桶”。

图8-10

步骤 3 按照以下配置完成 OBS 桶创建。

- 区域：华北-北京四
- 桶名称：test-aom-hcip
- 桶策略：公共读写
- 其他配置：默认配置

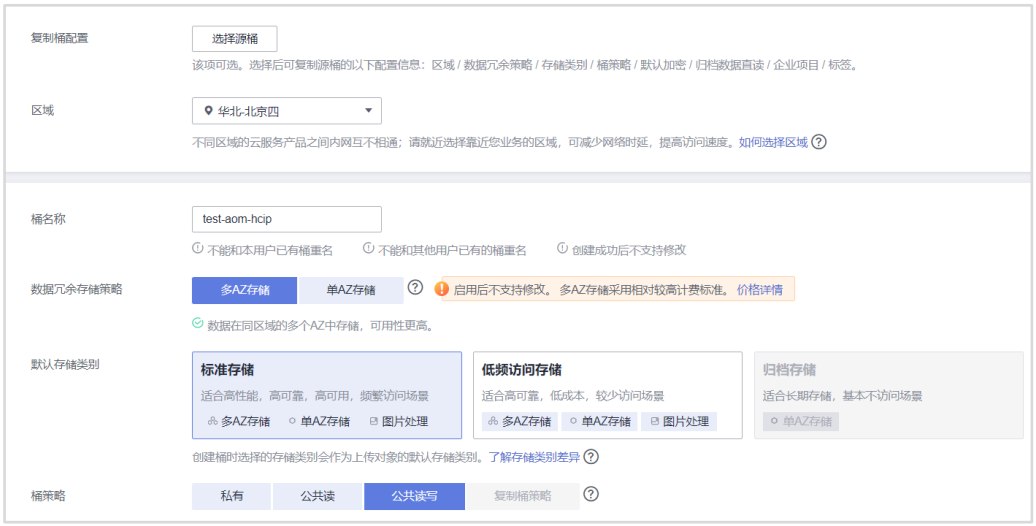


图8-11

8.2.2 云监控服务 CES

云监控服务（Cloud Eye Service，简称 CES）为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。可以让用户全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

在实际业务场景中，用户开通了云监控服务支持的云服务后，即可方便地在云监控 Console 页面查看云产品运行状态、各个指标的使用情况并对监控项创建告警规则。

配置主机监控后，可以通过监控云服务的 CPU 使用率、内存使用率、磁盘等基础指标，确保云服务的正常使用，避免因为对资源的过度使用造成业务无法正常运行。

配置站点监控服务后，可以探测站点的可用性、响应时间、丢包率等，让用户全面了解站点的可用性并在异常时及时处理。

事件监控提供了事件类型数据上报、查询和告警的功能。方便用户将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。

8.2.2.1 云监控服务指标

步骤 1 登录华为云管理控制台，在服务列表中选择“云监控服务”，进入“云服务监控”页面。

图8-12

步骤 2 选择待查看的云服务资源所在行（这里以云硬盘为例）的“查看监控指标”。进入“监控指标”页面。

说明：需要在 ECS 部署 7-8 分钟后再进行查看。

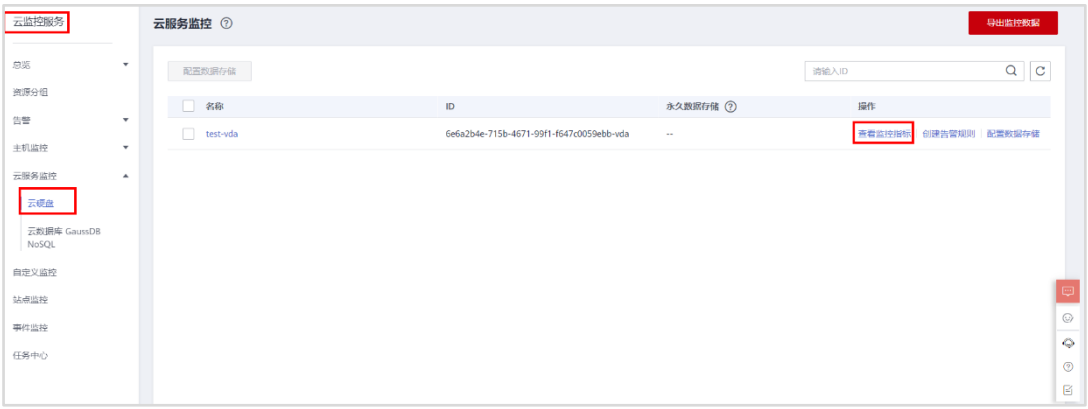


图8-13

说明：用户可以选择页面左上方的时间范围按钮，查看该云服务资源“近 1 小时”、“近 3 小时”、“近 12 小时”、“近 24 小时”和“近 7 天”的监控原始数据曲线图，同时监控指标视图右上角会动态显示对应时段内监控指标的最大值与最小值。也可以打开自动刷新开关来查看每分钟刷新的实时数据。

图8-14

步骤 3 单击页面右上角的“设置监控指标”，进入“设置监控指标”页面。

说明：可以选择要展示的指标名称，并且可以拖动选中指标对指标进行排序，方便自定义需要查看的指标运行状况。

步骤 4 鼠标滑动到对应指标后，单击指标视图右上角的图标  ，进入监控详情页面。

图8-15

说明：监控详情页面提供更长时间范围的指标情况。可以查看“近 1 小时”、“近 3 小时”、“近 12 小时”、“近 24 小时”、“近 7 天”和“近 30 天”6 个固定时长的监控周期，同时也支持以通过“自定义时间段”选择查看近六个月内任意时间段的历史监控数据。

图8-16

说明：若需要导出数据，可在云服务监控页面单击“导出监控数据”，根据界面提示选择参数后，单击“导出”完成导出数据。

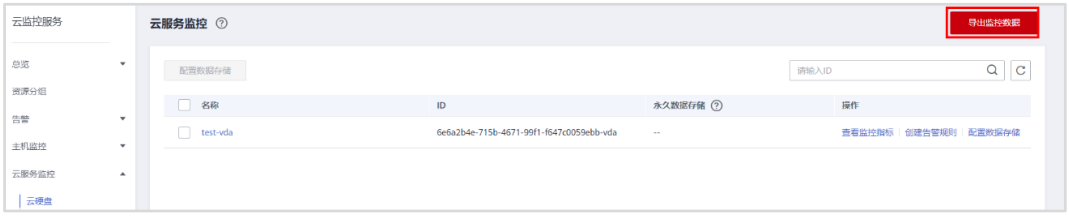


图8-17

8.2.2.2 主机监控

步骤 1 登录华为云控制台，在服务列表中选择“云监控服务”。

图8-18

步骤 2 在左侧页签中点击“主机监控”，进入“主机监控”页面。

图8-19

步骤 3 选择要安装 Agent 的 ECS，使用终端工具登录 ECS，通过如下命令手动安装 Agent 插件。当插件状态为“运行中”，说明 Agent 已安装成功。

说明：如果创建 ECS 时在“云监控”参数后勾选了“开启详细监控”选项，这里就不需要再手动安装 Agent 了。

```
[root@test ~]# cd /usr/local && curl -k -O https://obs.cn-north-4.myhuaweicloud.com/uniagent-cn-north-4/script/agent_install.sh && bash agent_install.sh
```

图8-20

说明：在北京一、上海二、上海一、广州区域，对于使用 CentOS 7.2-8.2 和 Ubuntu 20.04、18.04、16.04 版本镜像的服务器，可以在主机监控插件状态栏单击“未安装”来实现一键安装。

步骤 4 单击弹性云服务器右侧操作列的“查看监控指标”查看监控数据。

图8-21

说明：在此页面中可进行操作系统、基础和进程监控。

图8-22

8.2.2.3 站点监控

步骤 1 单击页面左侧页签中的“站点监控”，进入“站点监控”页面，选择右上角“创建站点监控”。

图8-23

步骤 2 参照以下配置参数，完成配置后点击“确定”。

- 名称：siteMonitor-huawei
- 类型：HTTP（S）
- 站点地址：www.huawei.com
- 监控频率：1 分钟
- 分布式探测点：全选
- 请求方式：HEAD
- 高级配置：暂不配置

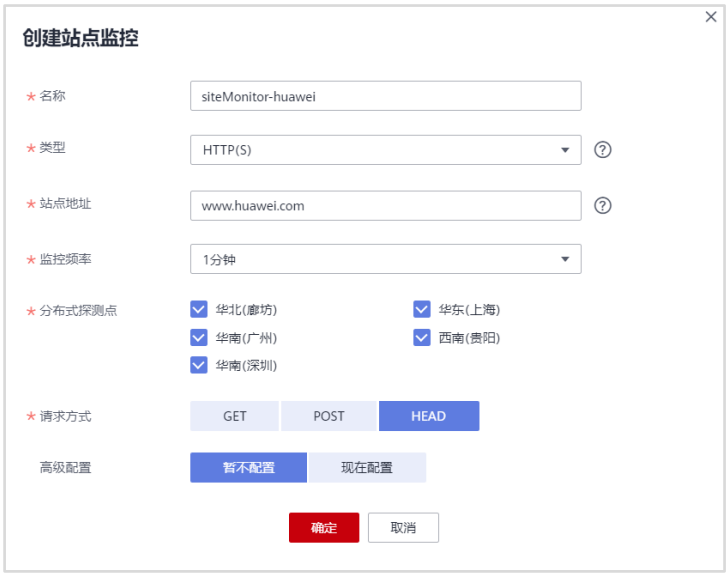


图8-24

步骤 3 进入“站点监控”页面。“站点监控”页面展示用户当前所有的站点概况，包括站点名称、监控频率、状态、响应时间等。单击站点名称所在行的“查看监控图表”。

图8-25

说明：进入监控图表页面，可以查看站点监控详情。

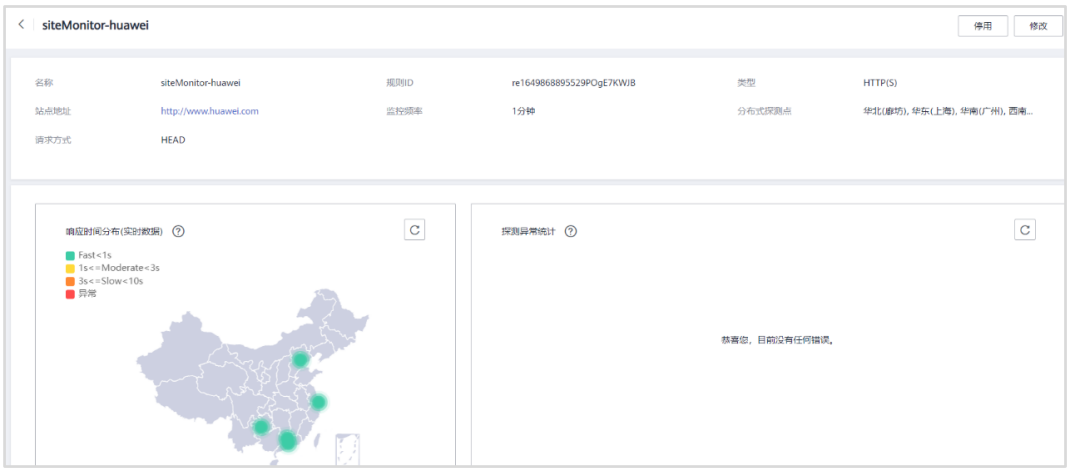


图8-26

8.2.2.4 事件监控

步骤 1 在云监控服务左侧页签中点击“事件监控”，在“事件监控”页面，默认展示近 24 小时的所有系统事件与自定义事件。单击具体事件右侧的操作列的“查看监控图表”，可查看具体事件的监控图表。

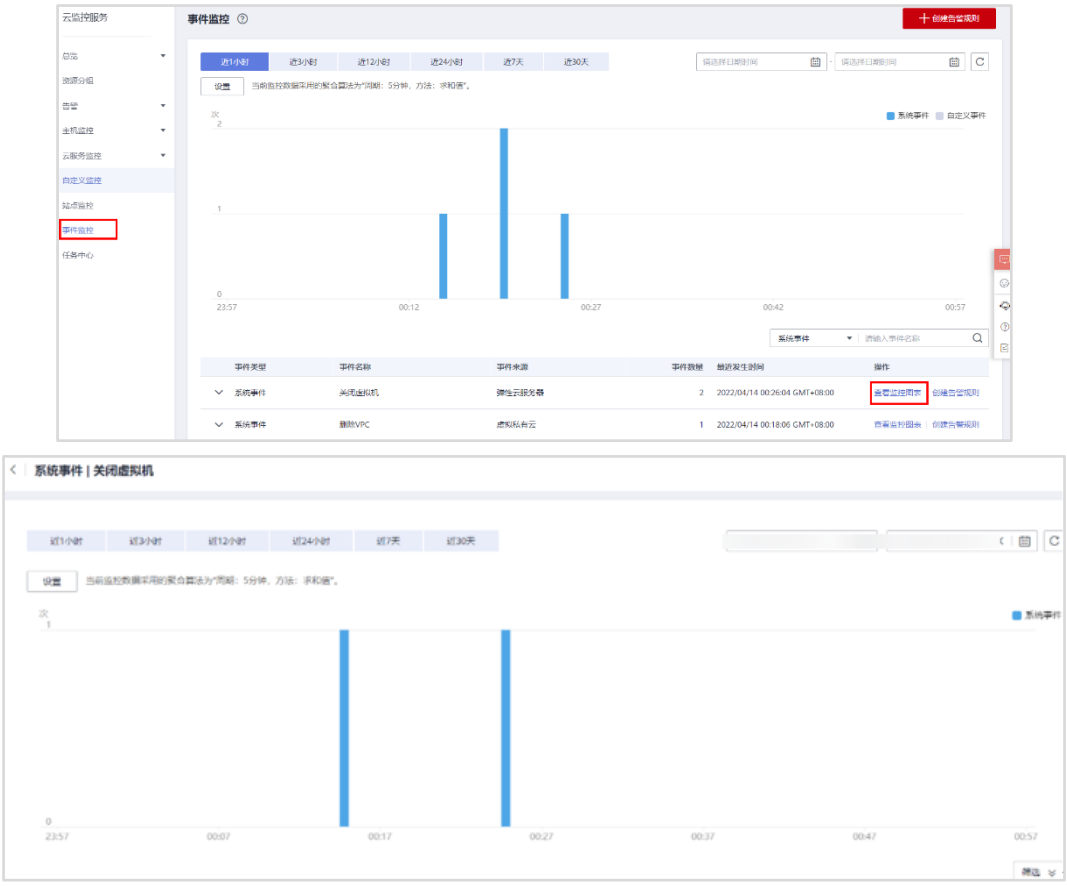


图8-27

步骤 2 进入“事件监控”页面，点击右上角“创建告警规则”。

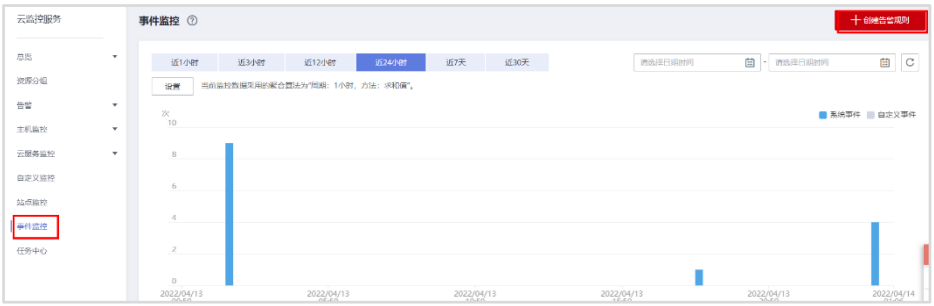


图8-28

步骤 3 根据页面提示配置告警规则名称、告警策略、告警通知等信息。

- 名称：alarm-test
- 事件类型：系统事件
- 事件来源：弹性云服务器
- 监控范围：全部资源
- 选择类型：自定义创建
- 告警策略：默认配置

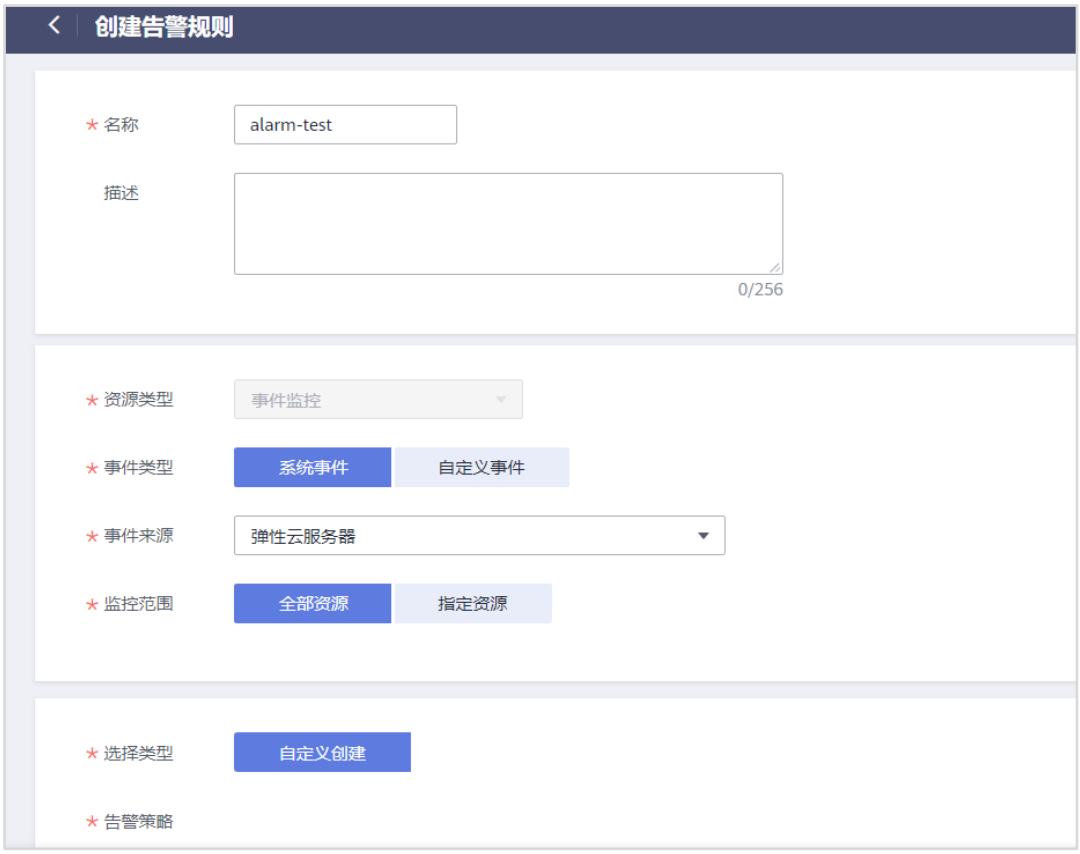


图8-29

- 通知对象：abc（选择资源准备步骤中创建的 SMN 主题）
- 其他配置：默认配置

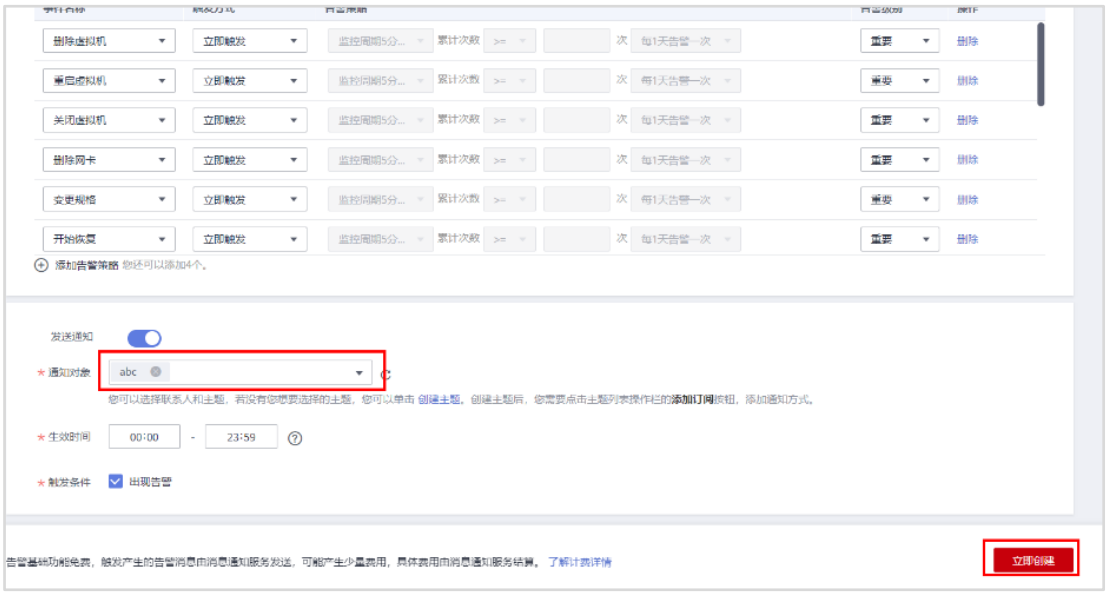


图8-30

说明：告警规则创建完成后，当事件监控指标触发设定的告警策略时，云监控服务会在第一时间通过消息通知服务告知用户云上资源异常，以免因此造成业务损失。

步骤 4 创建完成后，如下图所示，告警规则列表中显示状态为“已启用”，证明告警规则创建成功。

图8-31

8.2.3 应用运维管理 AOM

应用运维管理（Application Operations Management，简称 AOM）是云上应用的一站式立体化运维管理平台，实时监控用户的应用及相关云资源，分析应用健康状态，提供灵活丰富的数据可视化功能，帮助用户及时发现故障，全面掌握应用、资源及业务的实时运行状况。

在用户业务场景中，通过 AOM 主机告警监控的配置，用户可以及时了解主机的资源使用情况、趋势和告警，使用这些信息，用户管理员可以快速响应，保证主机流畅运行。

同时 AOM 提供强大的日志管理能力，日志检索功能可帮助用户快速在海量日志中查询到所需的日志，日志转储帮助用户实现长期存储，通过创建日志统计规则实现关键词周期性统计，并生成指标数据，帮助用户实时了解系统性能及业务等信息。

8.2.3.1 主机告警监控

步骤 1 在服务列表中选择“应用运维管理 AOM”。

图8-32

步骤 2 在应用运维管理界面左侧页签中选择“配置管理”，点击“Agent 管理”，在右侧点击“安装 Agent”选项。

说明：ICAgent 用于采集指标、日志和应用性能数据。对于在 ECS、BMS 控制台直接购买的主机，我们需手动安装 ICAgent。

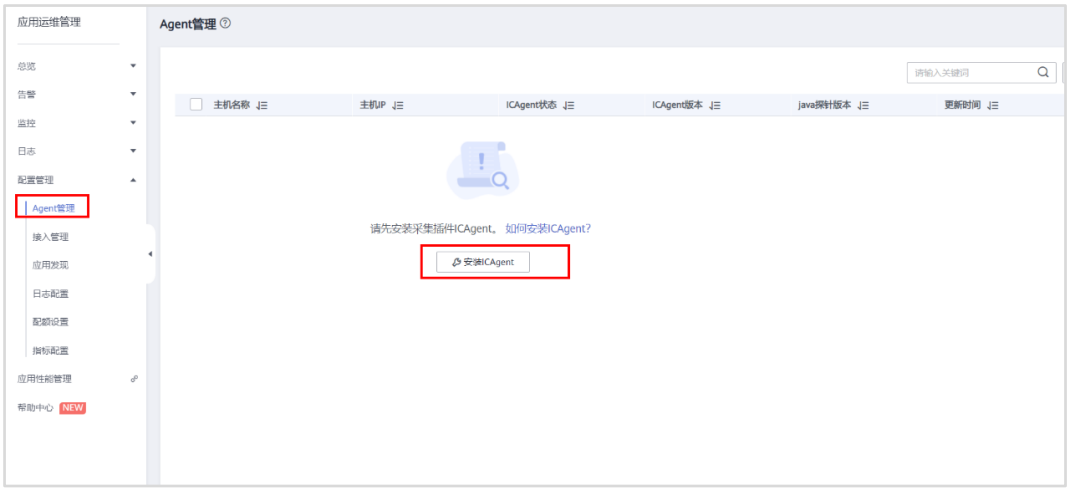


图8-33

步骤 3 在右侧弹出的页面中填入之前 5.2.7 步骤中下载好的 AK/SK，并复制安装命令。

图8-34

步骤 4 登录云主机 test，使用上一步中复制的命令进行 Agent 安装，如下图所示，当看到“ICAgent install success”字样时证明安装完成。

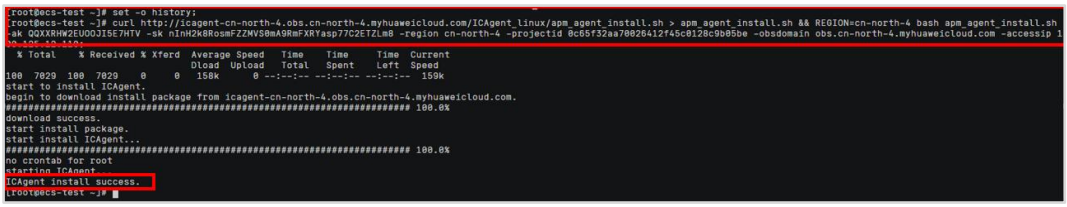


图8-35

步骤 5 此时返回华为云 Agent 管理界面，刷新页面后可查看当前云主机 test 的 ICAgent 状态为“运行”，证明 ICAgent 安装成功。

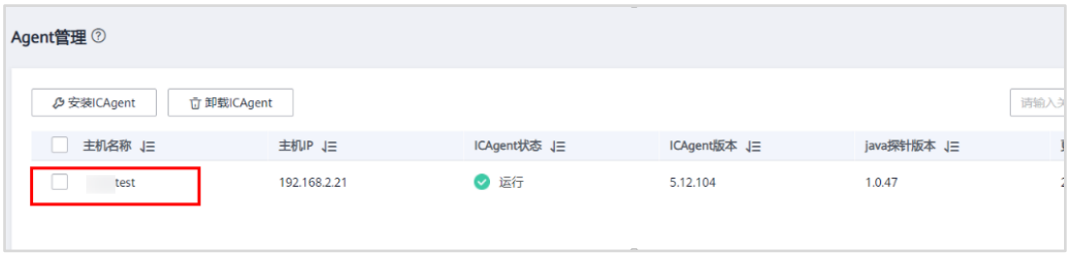


图8-36

步骤 6 在应用运维管理左侧选择“告警”页签，点击其中的“告警规则”，点击右上角“添加告警”。

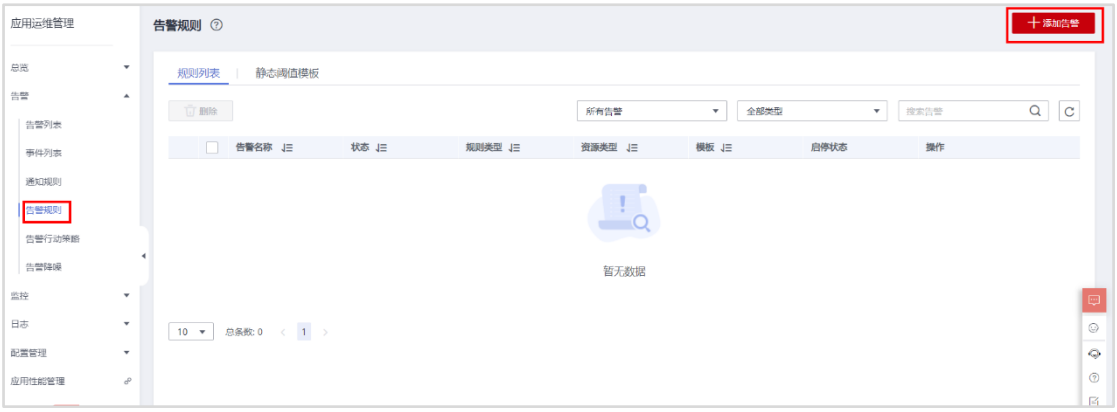


图8-37

步骤 7 按照以下配置添加告警规则。

- 规则名称：cpu-usage

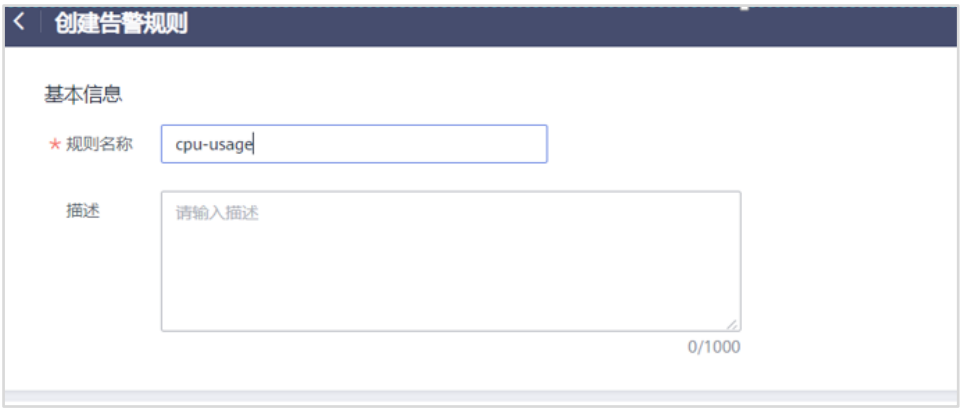


图8-38

- 规则类型：阈值规则
- 监控对象：选择资源对象
- 点击“选择资源对象”按钮

图8-39

- 添加方式：按资源添加
- 指标名称：主机/主机/CPU 使用率（这里以该指标为例，学员可根据实际情况选择相应指标，刚部署的 ECS 主机，可能要等一会才能发现）
- 选择指标维度：test

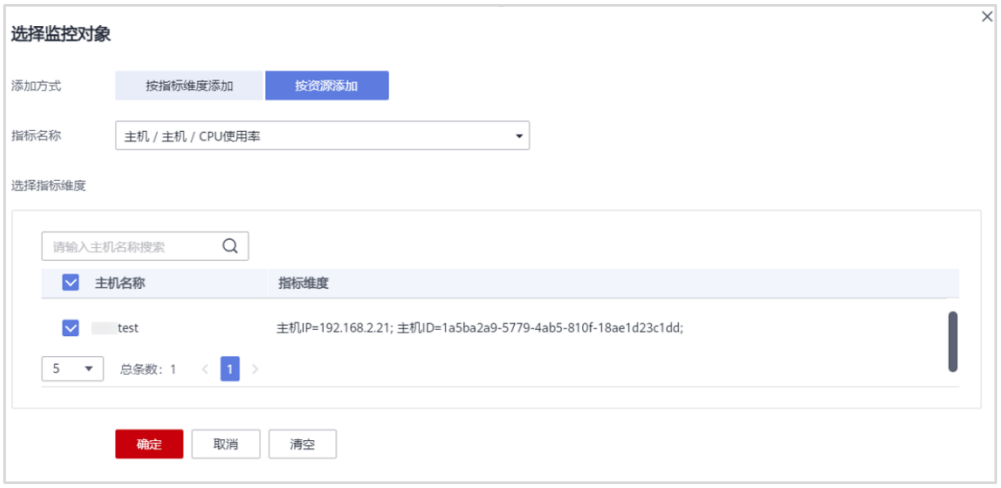


图8-40

- 告警条件：自定义创建

- 触发条件：2 个 | 2 个 | 平均值 | >= | 80 | 重要（这里仅以该条件为例，学员可根据实际需求配置触发条件）

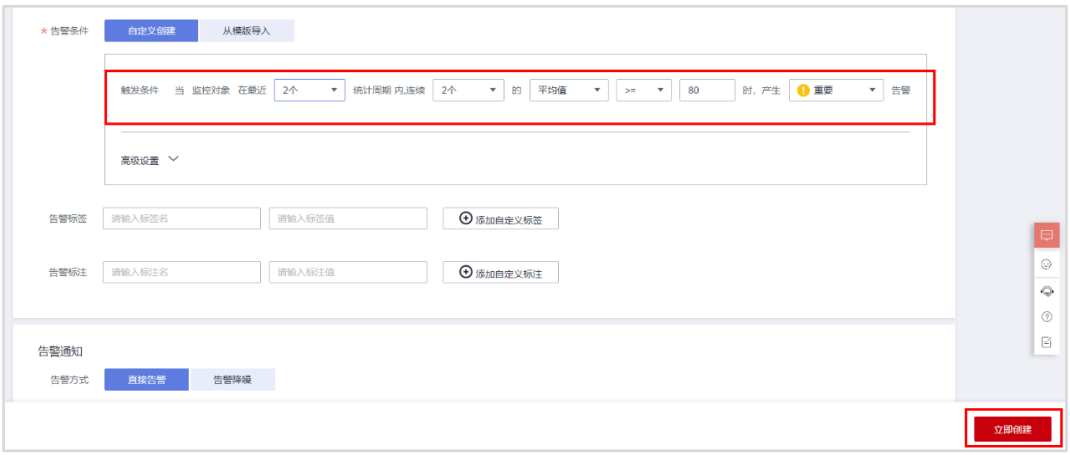


图8-41

步骤 8 创建完毕后在规则列表可查看当前创建的规则状态为“启用”，证明该告警规则配置完成。

图8-42

步骤 9 在应用运维管理左侧的页签中选择“总览”，点击“监控概览”进入监控概览页面，在此页面中可查看对当前接入资源的基础设施监控信息。

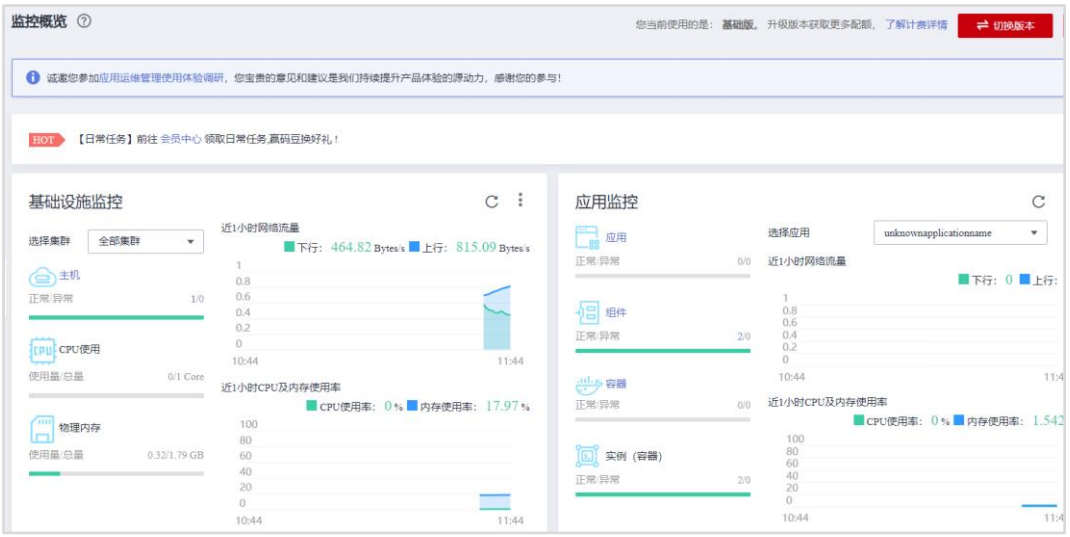


图8-43

8.2.3.2 日志采集

说明：主机系统异常时，日志中的 error 会比较多。此时如果想要第一时间知道异常的发生，可以通过统计日志中 error 的数量并设置阈值告警来进行主动通知。

步骤 1 选择应用运维管理左侧页签中的“日志>日志转储”，点击右上角“添加日志转储”。

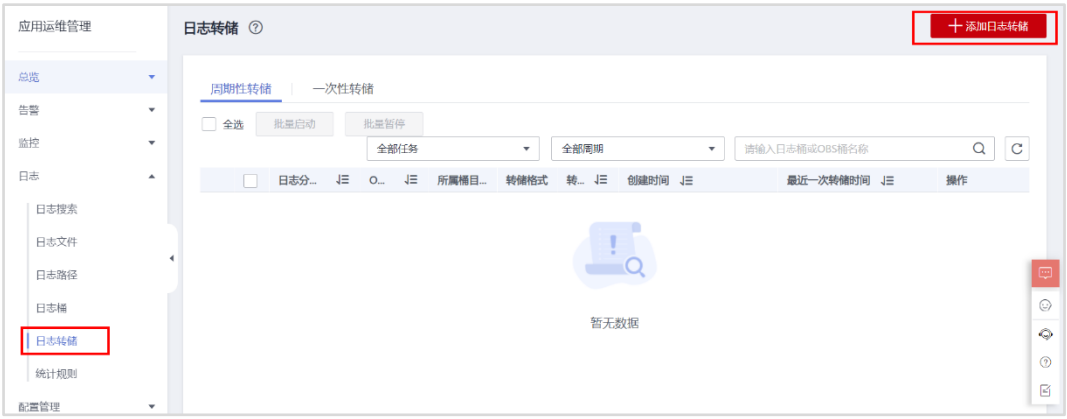


图8-44

步骤 2 按照以下配置完成日志转储添加。

- 转储文件形式：自定义文件
- 转储方式：周期性转储
- 日志类型：系统
- 集群名称：自定义集群
- 主机：192.168.3.219（云主机 test 的私网 IP 地址）
- 日志分组名称：systlog
- 目标 OBS 桶：test-aom-hcip（选择资源准备步骤中创建的桶）

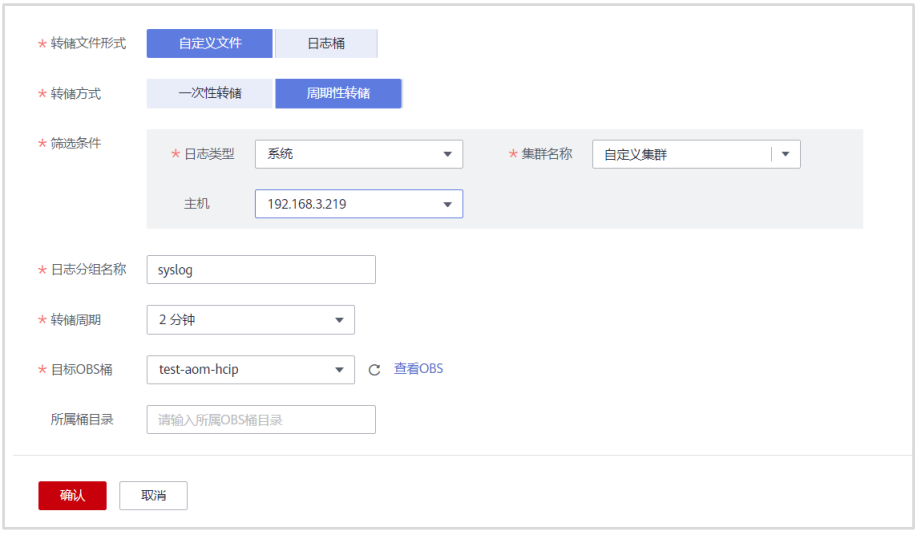


图8-45

步骤 3 配置完成后，在日志转储界面上可以看到创建时间和最近一次转储时间。

图8-46

步骤 4 在应用运维管理左侧页签中选择“日志>日志桶”，点击“添加日志桶”。

说明：后续创建统计规则时需要调用该日志桶。

图8-47

步骤 5 按照以下配置添加日志桶。

- 日志桶名称：syslog
- 日志文件：系统|集群 自定义集群|192.168.3.219|syslog

说明：192.168.3.219 为云主机 test 的私网 IP 地址。

图8-48

步骤 6 在应用运维管理左侧页签中选择“日志>统计规则”，点击右上角“创建统计规则”。

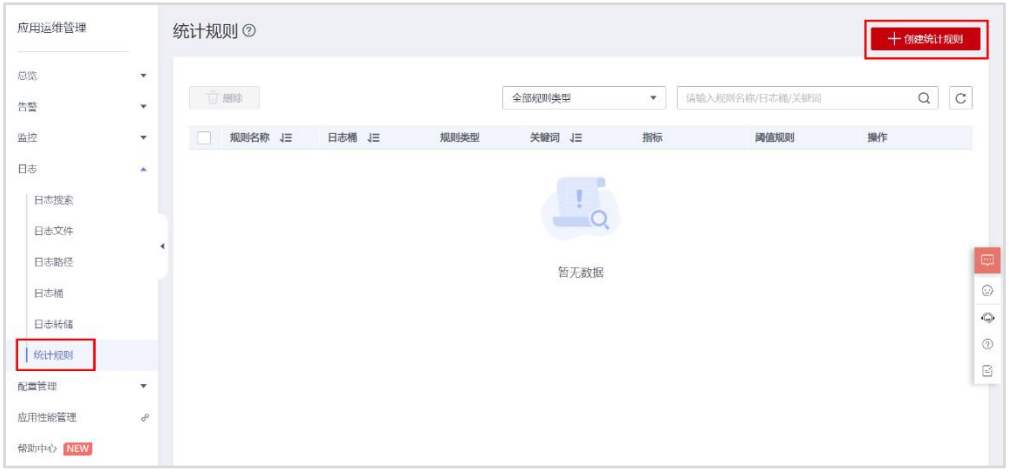


图8-49

步骤 7 按照以下配置创建统计规则，点击“确定”。

- 规则类型：关键词规则
- 规则名称：count-error
- 关键词：error
- 日志桶：syslog

图8-50

步骤 8 创建完成后点击操作栏中的“添加阈值规则”。

图8-51

步骤 9 按照以下配置完成阈值规则创建，点击“添加”。

- 告警名称：count-error
- 统计方式：平均值
- 统计周期：1 分钟
- 阈值条件：>= | 3
- 连续周期：1
- 告警级别：次要
- 是否发送通知：是
- 选择主题：abc
- 触发场景：超限阈值

图8-52

图8-53

说明：创建完成后，若统计结果超限了，就会第一时间发送短信和邮件通知该阈值已超限，服务可能发生异常。收到通知后就可以及时进行定位恢复。

8.2.3.3 CCE 监控

步骤 1 按照以下配置，创建 CCE 集群。具体操作方法可参照 CCE 相关章节。

说明：后续实验中需要使用 AOM 服务对该 CCE 集群进行监控。

图8-54

创建集群：

- 区域：华北-北京四
- 计费模式：按需计费
- 集群名称：cluster-cce（学员自定义）
- 版本：v1.19
- 集群管理规模：50 节点
- 高可用：否
- 网络模型：VPC 网络
- 虚拟私有云：vpc-3（学员可复用已创建的 VPC 或自定义）

- 控制节点子网：vpc-3-subnet（学员可复用已创建的 VPC 或自定义）

创建节点：

- 计费模式：按需计费
- 可用区：随机分配
- 节点类型：弹性云服务器-虚拟机
- 容器引擎：docker
- 节点规格：4 核|8 GB
- 操作系统：公共镜像|默认配置
- 节点名称：学员自定义或默认配置
- 登录方式：密码
- 密码：用户自定义
- 系统盘：默认配置
- 数据盘：默认配置
- 所在子网：vpc-3-subnet（学员可复用已创建的子网）
- 节点 IP：随机分配
- 弹性公网 IP：暂不使用

步骤 2 在服务列表中选择“应用运维管理 AOM”，在左侧页签中选择“总览-监控概览”查看监控信息，本页面提供了资源、应用、应用用户体验的全链路、多层次、一站式运维界面。可查看 CCE 集群的运行情况。

图8-55

步骤 3 在左侧页签中选择“监控-主机监控”，查看主机监控信息，可监控 CCE 集群的主机资源占用与健康状态，监控主机的磁盘、CPU 等常用系统设备使用情况。

图8-56

步骤 4 在左侧页签中选择“监控-容器监控”，可查看 CCE 集群中插件及容器的相关监控信息。

图8-57

8.2.4 应用性能监控 APM

华为云应用性能管理服务（Application Performance Management，简称 APM）可以帮助运维人员快速发现应用的性能瓶颈，以及故障根源的快速定位，同时 APM 应用指标监控可以度量应用的整体健康状况。APM Agent 会采集 Java 应用的 JVM，GC，服务调用，异常，外部调用，数据库访问以及其他中间件的指标数据，在实际业务场景中帮助用户全面掌握应用的运行情况。

步骤 1 创建安全组 sg-apm。

- 在服务列表中选择“虚拟私有云 VPC”，在该网络控制台中选择“访问控制”，点击“安全组”，点击右上角“创建安全组”，按照以下配置完成安全组创建及规则创建。

说明：该安全组供后续部署应用的 ECS 使用。

图8-58

- 名称：sg-apm
- 模板：自定义

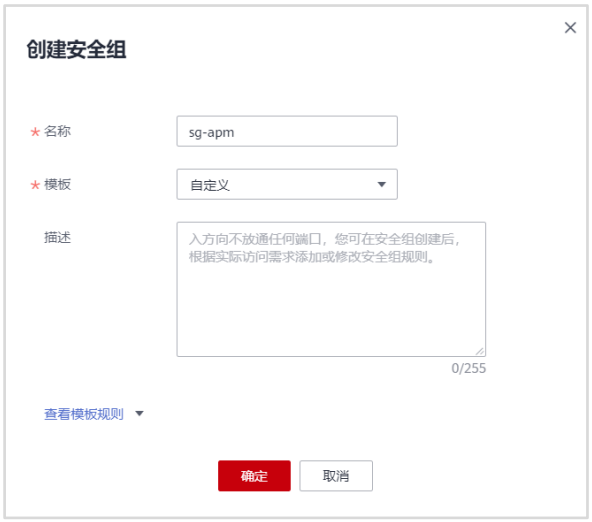


图8-59

- 优先级：1
- 策略：允许
- 协议端口：ICMP|全部
- 类型：IPv4
- 源地址：IP 地址|0.0.0.0/0

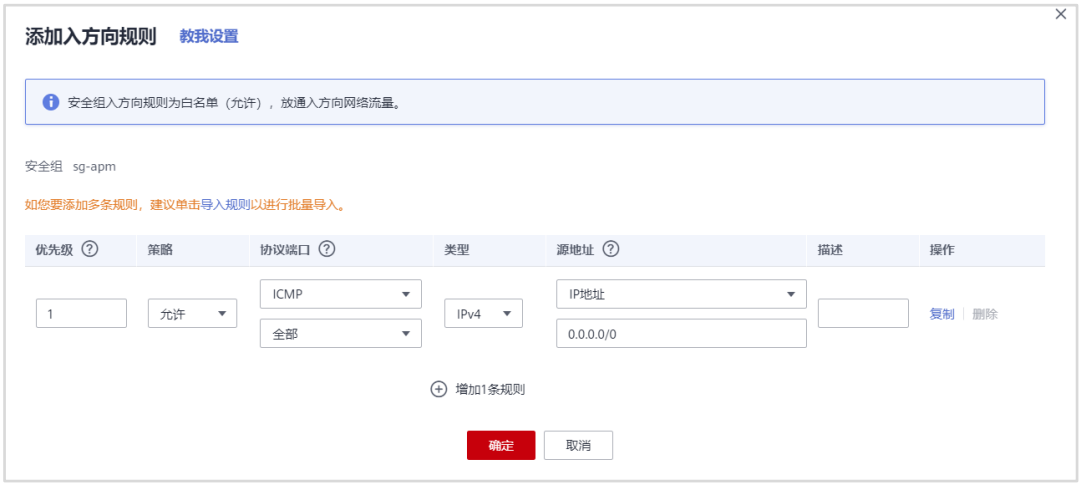


图8-60

- 优先级：1
- 策略：允许
- 协议端口：TCP|8080
- 类型：IPv4
- 源地址：IP 地址|0.0.0.0/0

图8-61

步骤 2 参照之前实验步骤创建 VPC（后续资源将在该 VPC 内创建）。

VPC 配置：

- 区域：华北-北京四
- 名称：vpc-2
- IPv4 网段：192.168.0.0/16

默认子网：

- 可用区：可用区 2
- 名称：vpc-2-subnet
- 子网 IPv4 网段：192.168.2.0/24

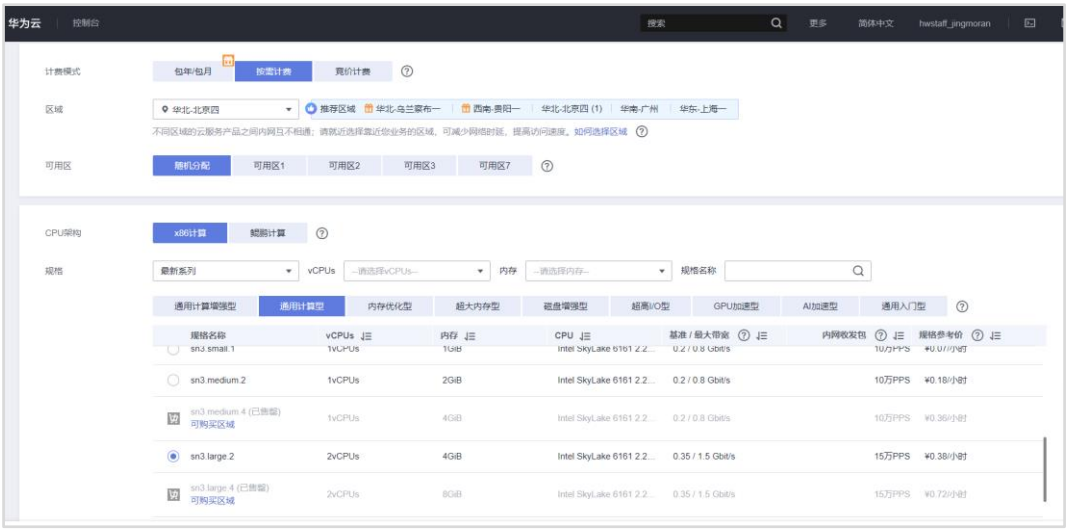
步骤 3 按照以下配置购买弹性云服务器。

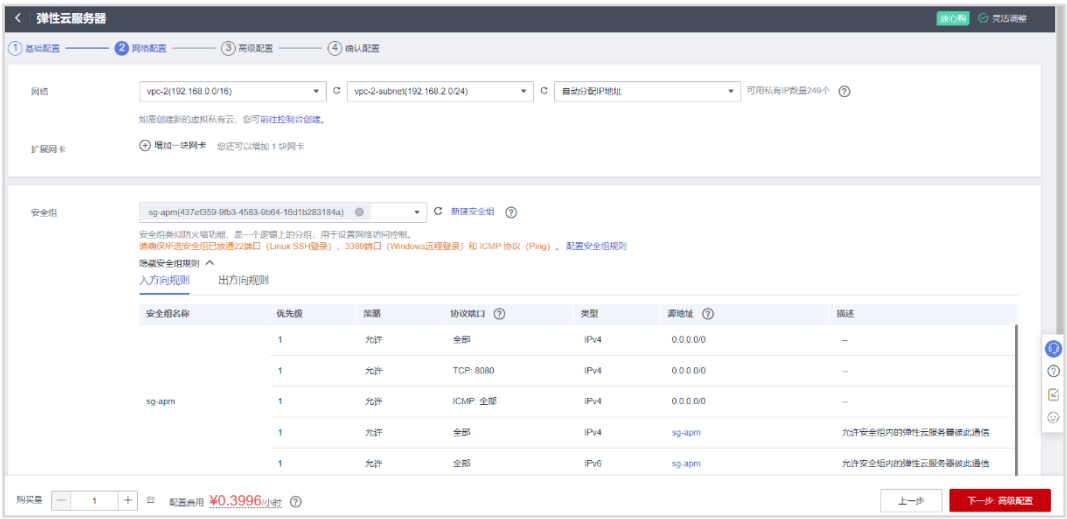
说明：该云服务器用于部署应用。

云主机“ecs-apm”配置：

- 计费模式：按需计费
- 区域：华北-北京四
- 可用区：随机分配
- CPU 架构：x86 计算
- 规格：2 vCPUs | 4 GiB
- 镜像：公共镜像 | CentOS 7.8 64 bit
- 主机安全：开通主机安全（基础版）
- 网络：vpc-2 | vpc-2-subnet | 自动分配 IP 地址
- 安全组：sg-apm
- 弹性公网 IP：现在购买

- 线路：全动态 BGP
- 公网带宽：按流量计费
- 带宽大小：10 Mbit/s
- 系统盘：高 IO | 40 GiB
- 云服务器名称：ecs-apm
- root 密码：自定义





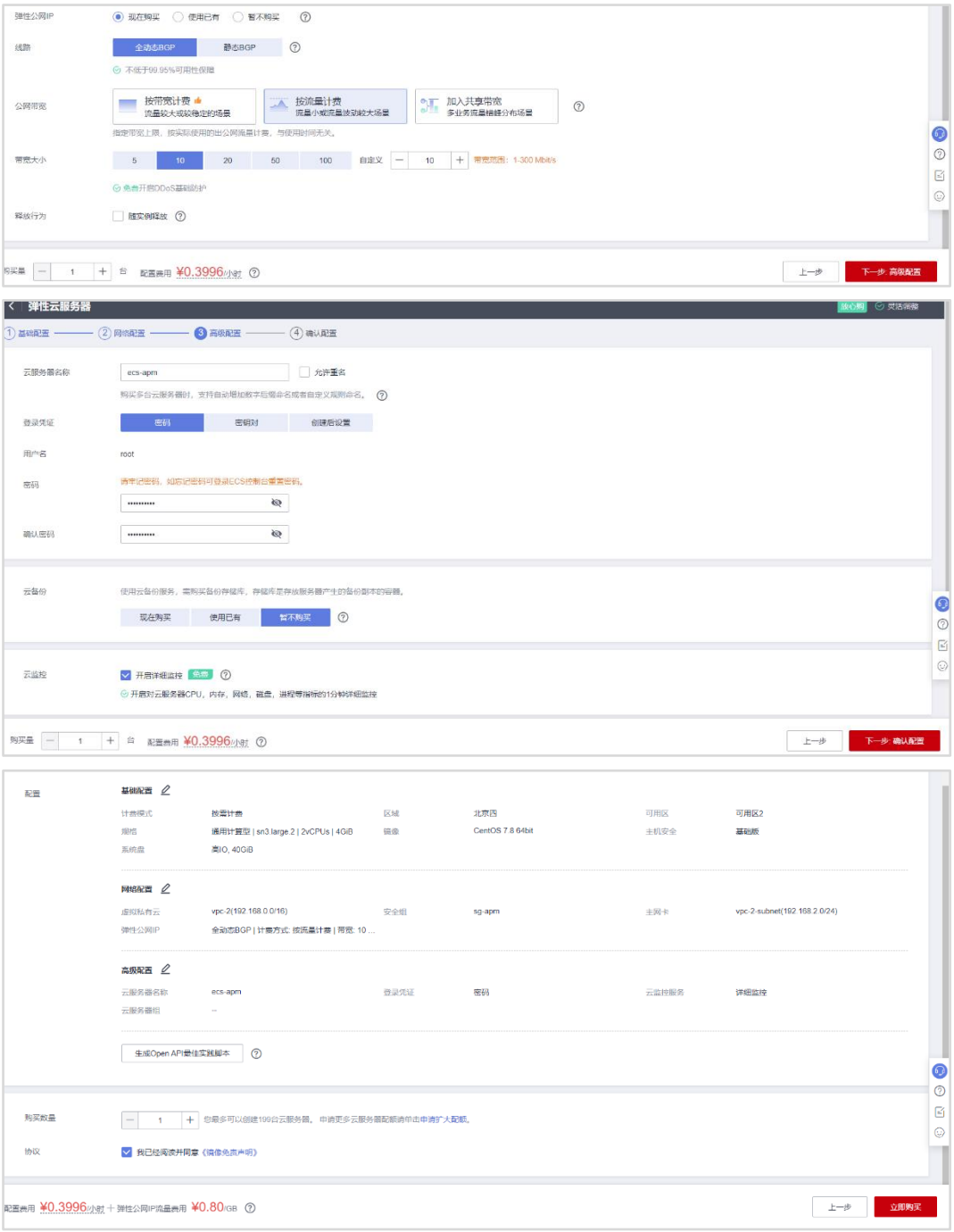


图8-62

步骤 4 登录云主机，下载 jdk 和 tomcat 安装包。

- 使用华为云 CloudShell 登录云主机。

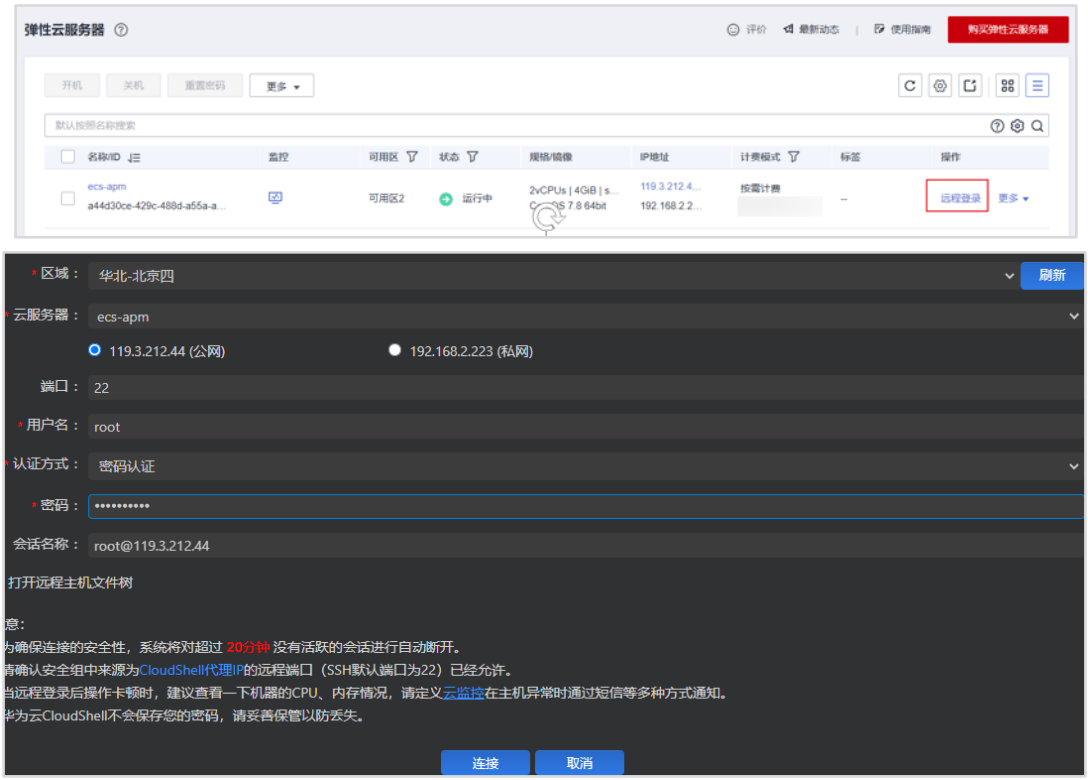


图8-63

- 使用如下命令创建相应文件夹。

```
[root@ecs-apm ~]# cd /home/
[root@ecs-apm home]# mkdir webDemo
[root@ecs-apm home]# cd webDemo/
[root@ecs-apm webDemo]# mkdir jdk
[root@ecs-apm webDemo]# mkdir tomcat
```

图8-64

- 使用如下命令下载 jdk 安装包。

```
[root@ecs-apm webDemo]# cd jdk
[root@ecs-apm jdk]# wget https://cloudservice-v3.obs.cn-east-3.myhuaweicloud.com/jdk-18_linux-x64_bin.tar.gz
```

图8-65

- 使用如下命令下载 tomcat 安装包。

```
[root@ecs-apm jdk]# cd /home/webDemo/tomcat/
[root@ecs-apm tomcat]# wget https://cloudservice-v3.obs.cn-east-3.myhuaweicloud.com/apache-tomcat-8.5.78.tar.gz
```

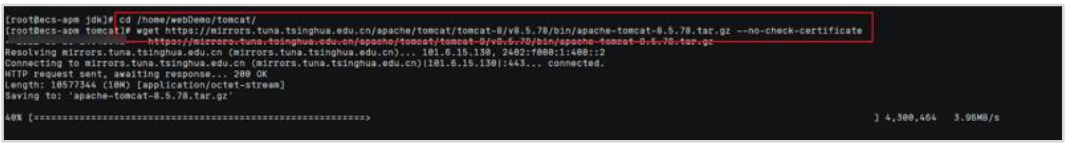


图8-66

步骤 5 安装 jdk。

- 执行如下命令，进入 jdk 目录并解压安装包。

```
[root@ecs-apm tomcat]# cd /home/webDemo/jdk/
[root@ecs-apm jdk]# ls
jdk-18_linux-x64_bin.tar.gz
[root@ecs-apm jdk]# tar -xvf jdk-18_linux-x64_bin.tar.gz
```

图8-67

```
[root@ecs-apm jdk]# vi /etc/profile
```

- 在文件末尾添加如下内容。

```
#set java environment
JAVA_HOME=/home/webDemo/jdk/jdk-18.0.1.1
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
```

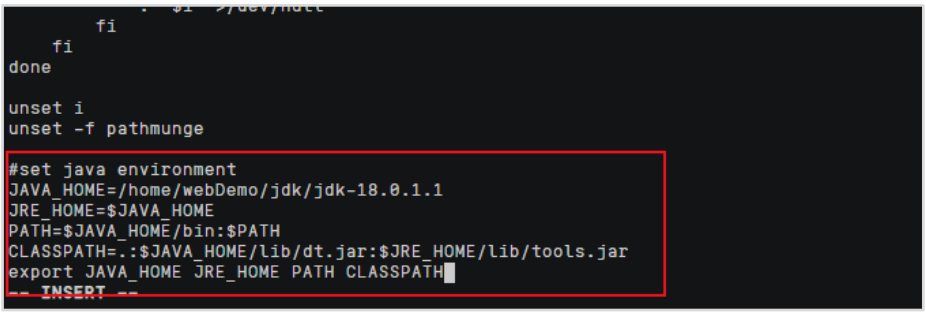


图8-68

- 执行如下命令使得/etc/profile 里的配置生效。

```
[root@ecs-apm jdk]# source /etc/profile
```

```
[root@ecs-apm jdk]# source /etc/profile
[root@ecs-apm jdk]#
```

图8-69

- 执行如下命令验证安装，如下图所示，证明安装完成。

```
[root@ecs-apm jdk]# java -version
```

```
[root@ecs-apm jdk]# java -version
java version "18.0.1.1"
Java(TM) SE Runtime Environment (build 18.0.1.1+2-6)
Java HotSpot(TM) 64-Bit Server VM (build 18.0.1.1+2-6, mixed mode, sharing)
[root@ecs-apm jdk]#
```

图8-70

步骤 6 安装 tomcat。

- 执行如下命令进入 tomcat 目录。

```
[root@ecs-apm ~]# cd /home/webDemo/tomcat/
```

- 执行如下命令解压 tomcat 安装包。

```
[root@ecs-apm tomcat]# tar -xvf apache-tomcat-8.5.78.tar.gz
```

```
[root@ecs-apm tomcat]# tar -xvf apache-tomcat-8.5.78.tar.gz
apache-tomcat-8.5.78/conf/
apache-tomcat-8.5.78/conf/catalina.policy
apache-tomcat-8.5.78/conf/catalina.properties
apache-tomcat-8.5.78/conf/context.xml
apache-tomcat-8.5.78/conf/jaspic-providers.xml
apache-tomcat-8.5.78/conf/jaspic-providers.xsd
apache-tomcat-8.5.78/conf/logging.properties
apache-tomcat-8.5.78/conf/server.xml
apache-tomcat-8.5.78/conf/tomcat-users.xml
apache-tomcat-8.5.78/conf/tomcat-users.xsd
apache-tomcat-8.5.78/conf/web.xml
apache-tomcat-8.5.78/bin/
apache-tomcat-8.5.78/lib/
```

图8-71

- 进入 tomcat 的 bin 目录，执行以下命令安装 tomcat。

```
[root@ecs-apm tomcat]# cd /home/webDemo/tomcat/apache-tomcat-8.5.78/bin/
```

```
[root@ecs-apm tomcat]# cd /home/webDemo/tomcat/apache-tomcat-8.5.78/bin/
[root@ecs-apm bin]#
```

图8-72

- 执行如下命令编辑 setclasspath.sh 脚本。

```
[root@ecs-apm bin]# vi setclasspath.sh
```

- 在 setclasspath.sh 脚本底部添加如下内容。

```
export JAVA_HOME=/home/webDemo/jdk/jdk-18.0.1.1
export JRE_HOME=$JAVA_HOME
```

```
# Set standard commands for invoking Java, if not already set.
if [ -z "$_RUNJAVA" ]; then
  _RUNJAVA="$JRE_HOME"/bin/java
fi
if [ "$os400" != "true" ]; then
  if [ -z "$_RUNJDB" ]; then
    _RUNJDB="$JAVA_HOME"/bin/jdb
  fi
fi

export JAVA_HOME=/home/webDemo/jdk/jdk-18.0.1.1
export JRE_HOME=$JAVA_HOME

-- INSERT --
```

图8-73

- 执行“wq”保存退出。
- 执行以下命令启动 tomcat。

```
[root@ecs-apm bin]# ./startup.sh
```

```
[root@ecs-apm bin]# vi setclasspath.sh
[root@ecs-apm bin]# ./startup.sh
Using CATALINA_BASE:   /home/webDemo/tomcat/apache-tomcat-8.5.78
Using CATALINA_HOME:   /home/webDemo/tomcat/apache-tomcat-8.5.78
Using CATALINA_TMPDIR: /home/webDemo/tomcat/apache-tomcat-8.5.78/temp
Using JRE_HOME:        /home/webDemo/jdk/jdk-18.0.1.1
Using CLASSPATH:       /home/webDemo/tomcat/apache-tomcat-8.5.78/bin/bootstrap.jar:/home/webDemo/tomcat/apache-tomcat-8.5.78/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
[root@ecs-apm bin]#
```

图8-74

- 执行如下命令查看 tomcat 进程，如下图所示，证明 tomcat 启动完成。

```
[root@ecs-apm bin]# ps -ef | grep tomcat
```

```
[root@ecs-apm bin]# ps -ef | grep tomcat
root     18231     1  5 15:22 pts/0    00:00:02 /home/webDemo/jdk/jdk-18.0.1.1/bin/java -Djava.util.logging.config.file=/home/webDemo/tomcat/apache-tomcat-8.5.78/conf/logging.properties -D
java.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djdk.tls.ephemeralDHKeySize=2048 -Djava.protocol.handler.pkgs=org.apache.catalina.webresources -Dorg.apache.catalina.securi
ty.SecurityListener.UMASK=0027 -Dignore.endorsed.dirs= -classpath /home/webDemo/tomcat/apache-tomcat-8.5.78/bin/bootstrap.jar:/home/webDemo/tomcat/apache-tomcat-8.5.78/bin/tomcat-juli.jar
-Dcatalina.base=/home/webDemo/tomcat/apache-tomcat-8.5.78 -Dcatalina.home=/home/webDemo/tomcat/apache-tomcat-8.5.78 -Djava.io.tmpdir=/home/webDemo/tomcat/apache-tomcat-8.5.78/temp org.apac
he.catalina.startup.Bootstrap start
root     18272  8018  0 15:23 pts/0    00:00:00 grep --color=auto tomcat
[root@ecs-apm bin]#
```

图8-75

步骤 7 验证 Java Web 环境搭建完成。

- 在浏览器输入如下内容：http://119.3.212.44（云服务器 ecs-apm 的弹性公网 IP）:8080，如下图所示，证明 Java Web 环境搭建成功。

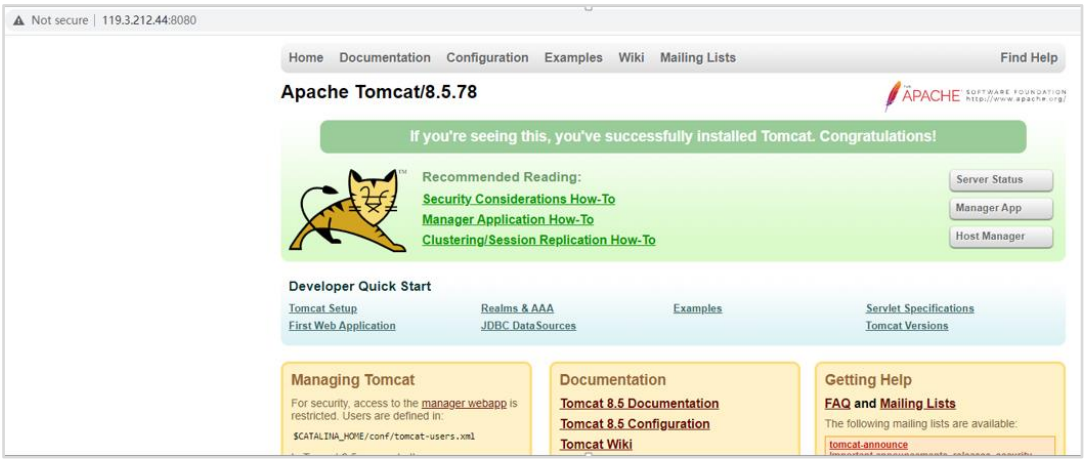


图8-76

步骤 8 APM 接入应用。

- 在服务列表中选择“应用性能管理 APM”。

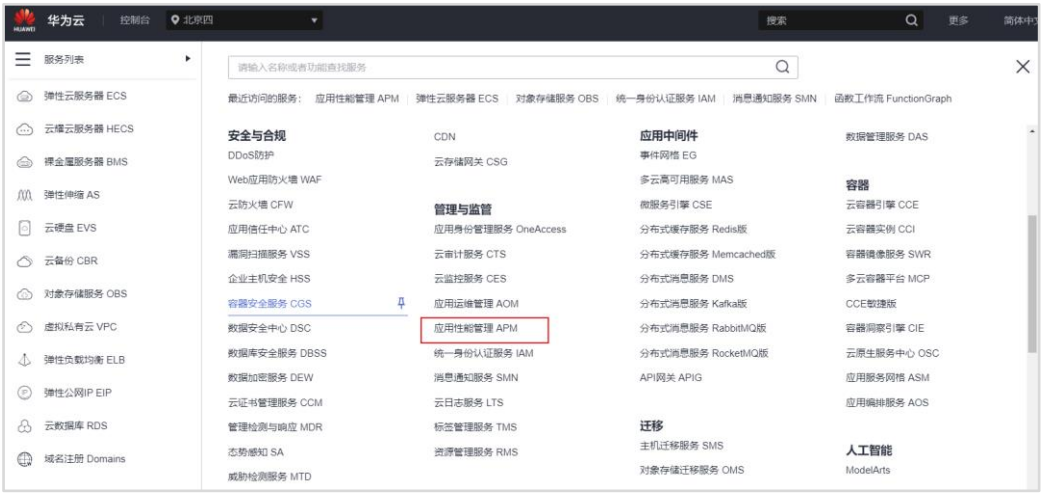


图8-77

- 在“应用列表”中点击“免费体验应用性能管理”。

说明：使用“APM2.0”版本。

图8-78

- 点击“立即体验”。

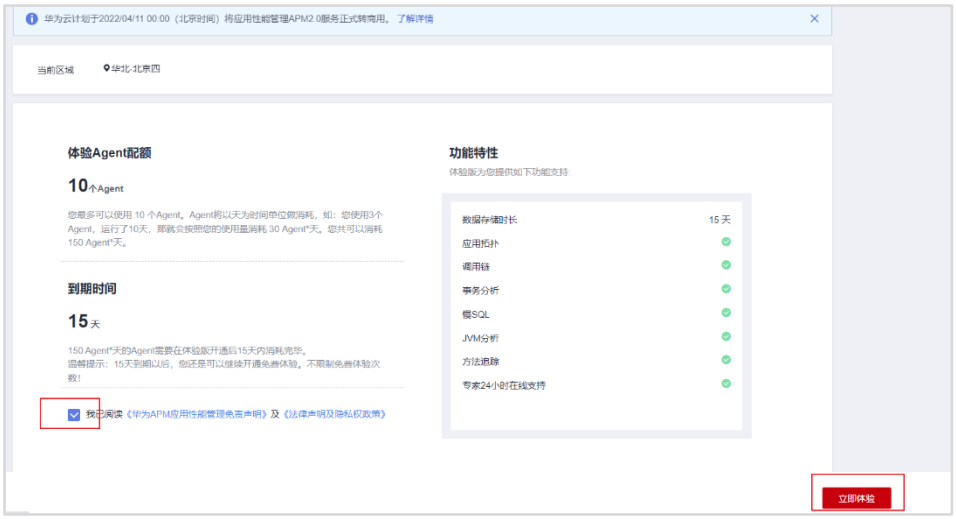


图8-79

- 选择“点击接入应用”。

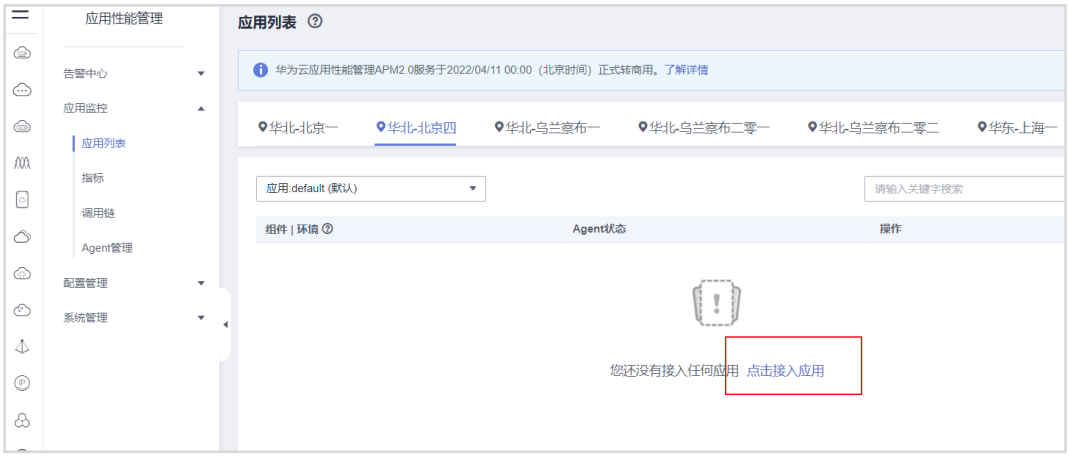


图8-80

- 点击“复制命令”。

图8-81

- 登录云主机，进入/root 目录。

```
[root@ecs-apm ~]# cd /root/
```

- 使用之前复制的命令安装 Agent，如下图所示，当看到“install APM agent success”字样时，证明 Agent 安装成功。

说明：以下命令仅作参考，请使用之前步骤中实际复制的命令替换。

```
[root@ecs-apm ~]# curl -k https://apm2-javaagent-cn-north-4.obs.cn-north-4.myhuaweicloud.com/apm_agent_install.sh -o apm_agent_install.sh && bash apm_agent_install.sh -ak jt8RxdG3u3JRGi3i -sk IojAHgN2b2nJcrnk9awmp2AJyYXwmEn46rY5jpLDFuBu3RujM6Af3jZx7aCRujR2V3amw38P5Ou8pelCuEKWQAIfZ6Kdeb6j5Cg1fsy86P2lQeTzyCGbAWg2ydAb6bxLeh1Kc8njegrdObY40IyFuuHNHFe4eCf71dC6XhSTUpYC6JvKJaiJSsHzy1iEtEl24kT7JUsLruQKQRqG4ZbptEbse21LvMfLu2nCgxfu73FCPxEr51eExtPM1z9x3XY9 -masteraddress https://100.125.12.108:41333 -obsaddress https://apm2-javaagent-cn-north-4.obs.cn-north-4.myhuaweicloud.com -version latest
```

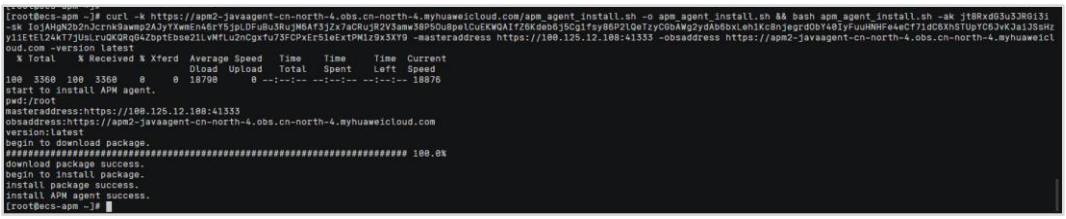


图8-82

- 执行如下命令进入 tomcat 的 bin 目录中。

```
[root@ecs-apm ~]# cd /home/webDemo/tomcat/apache-tomcat-8.5.78/bin/
```

- 执行如下命令修改 catalina.sh 文件。

```
[root@ecs-apm bin]# vi catalina.sh
```

- 将如下字符写入该文件。

```
CATALINA_OPTS="-javaagent:/root/apm-javaagent/apm-javaagent.jar=appName=Tomcat"
```

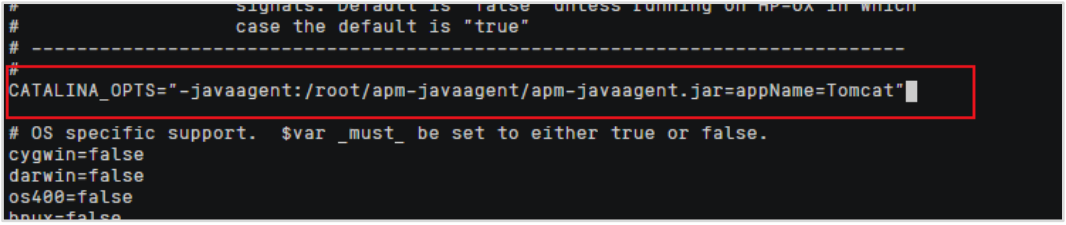


图8-83

- 执行“wq”保存退出。
- 在当前目录下执行如下命令，重新启动 tomcat。

```
[root@ecs-apm bin]# ./shutdown.sh
[root@ecs-apm bin]# ./startup.sh
```

- 启动后刷新几次 tomcat 页面，确认状态，待 1 分钟后返回应用性能管理控制台。

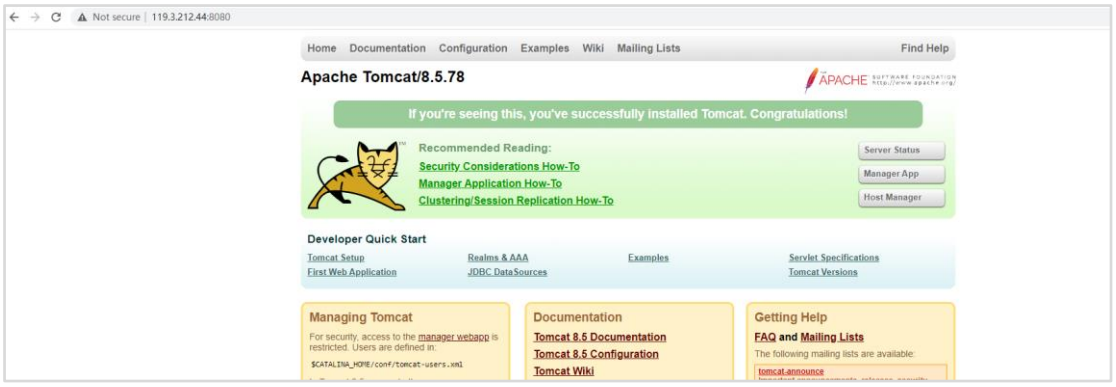


图8-84

- 返回应用性能管理控制台，在“Agent 管理”页签中刷新页面，查看当前 Agent，如下图所示，证明 Agent 已成功接入。

图8-85

- 在“应用列表”页签中查看当前接入应用，如下图所示，证明应用已成功接入 APM。

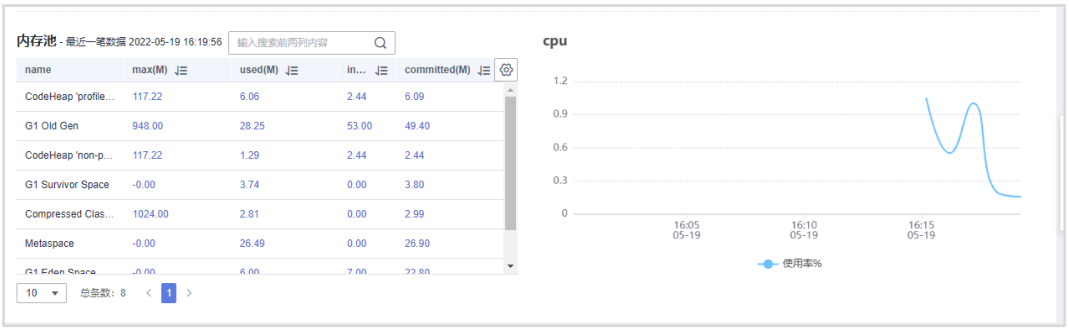
图8-86

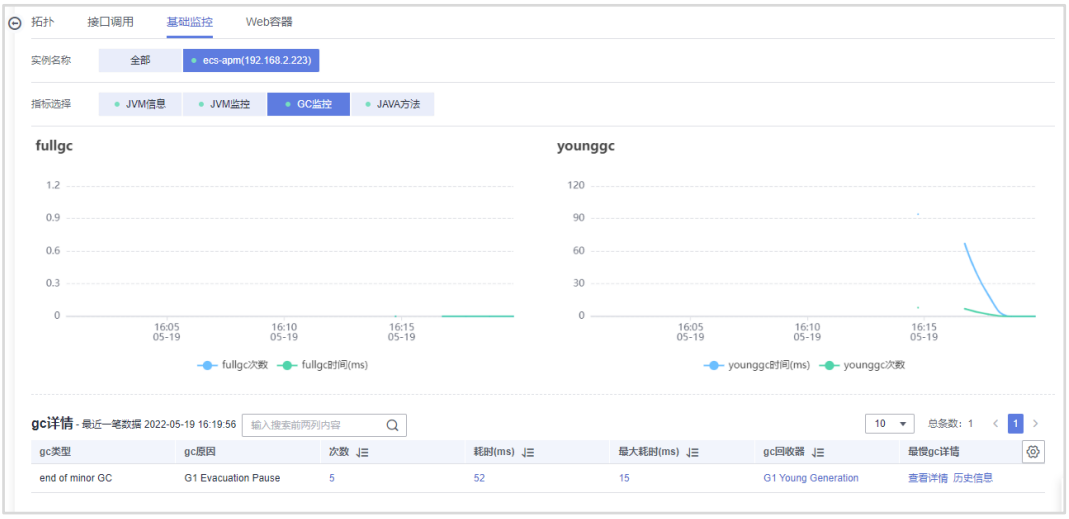
步骤 9 查看应用监控信息。

- 点击应用名称“Tomcat”，查看监控项相关信息。

说明：APM Agent 会周期性采集性能指标数据，用来衡量应用的总体健康状况。可以采集 JVM、GC、服务调用、异常、外部调用、数据库访问以及其他中间件的指标调用等数据，每一种采集的数据类型对应一个采集器，采集器被部署到环境后形成监控项，在数据采集的时候监控项决定了采集的数据结构和采集行为，通过以下界面可以查看相关监控项。


拓扑
接口调用
基础监控
Web容器
实例名称
全部
ecs-apm(192.168.2.223)
指标选择
JVM信息
JVM监控
GC监控
JAVA方法
线程
线程状态
内存
类加载
当前线程数
死锁线程数
守护线程数
所有启动线程数
峰值线程数
WAITING状态线程数
TERMINATED状态线程数
RUNNABLE状态线程数
非堆内存使用(M)
堆内存使用(M)
直接内存使用(M)
总共加载类个数
当前类个数
卸载的类个数


内存池 - 最近一笔数据 2022-05-19 16:19:56
输入搜索前两列内容
name
max(M)
used(M)
committed(M)
CodeHeap 'profile...
117.22
6.06
6.09
G1 Old Gen
948.00
28.25
53.00
49.40
CodeHeap 'non-p...
117.22
1.29
2.44
2.44
G1 Survivor Space
-0.00
3.74
0.00
3.80
Compressed Clas...
1024.00
2.81
0.00
2.99
Metaspace
-0.00
26.49
0.00
26.90
总条数：8
cpu
使用率%


拓扑
接口调用
基础监控
Web容器
实例名称
全部
ecs-apm(192.168.2.223)
指标选择
JVM信息
JVM监控
GC监控
JAVA方法
fullgc
younggc
fullgc次数
fullgc时间(ms)
younggc时间(ms)
younggc次数
gc详情 - 最近一笔数据 2022-05-19 16:19:56
输入搜索前两列内容
总条数：1
gc类型
gc原因
次数
耗时(ms)
最大耗时(ms)
gc回收器
最慢gc详情
end of minor GC
G1 Evacuation Pause
5
52
15
G1 Young Generation
查看详情 历史信息

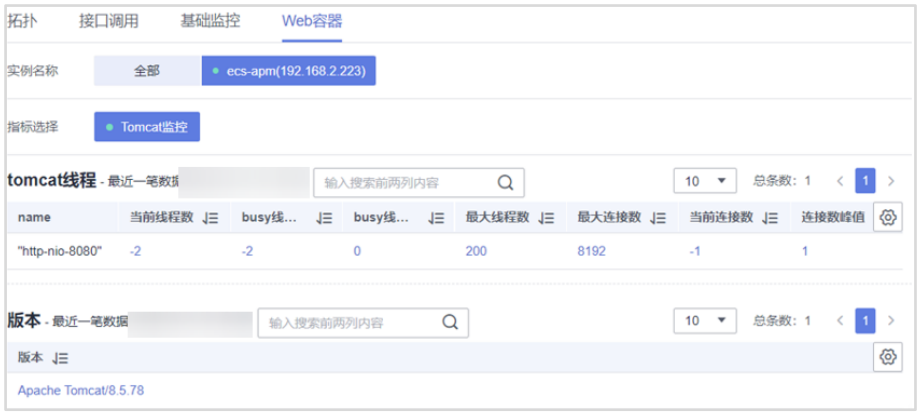


图8-87

8.3 实验恢复

步骤 1 删除 SMN。

- 在服务列表中选择“消息通知服务 SMN”，在左侧页签中选择“主题管理>主题”，在右侧列表中找到本实验创建的主题，点击操作栏中的“更多>删除”

步骤 2 删除 AOM 告警规则。

- 在应用运维管理控制台左侧选择“告警”页签 ，点击其中的“告警规则”，找到本实验创建的告警规则，点击操作栏中的“删除”。

步骤 3 删除 AOM 日志规则。

- 在应用运维管理控制台左侧页签中选择“日志>统计规则”，找到本实验创建的统计规则，选择操作栏中的“删除”。

步骤 4 删除 AOM 日志桶。

- 在应用运维管理控制台左侧页签中选择“日志>日志桶”，找到本实验创建的日志桶，选择操作栏中的“删除”。

步骤 5 删除日志转储。

- 选择应用运维管理控制台左侧页签中的“日志>日志转储”，找到本实验创建的转储规则，选择操作栏中的“删除”。

步骤 6 删除 CES 站点监控。

- 在服务列表中选择“云监控服务 CES”，选择左侧页签中的“站点监控”，进入“站点监控”页面。
- 在右侧列表中找到本实验创建的站点监控，点击操作栏中的“更多>删除”。

步骤 7 删除 ECS。

- 在服务列表中选择“云服务器 ECS”，找到本实验创建的云服务器，点击操作栏中的“更多>删除”。
- 在弹出的对话框中勾选下图中选项，点击“是”。

图8-88

步骤 8 删除安全组。

- 在服务列表中选择“虚拟私有云 VPC”，在“访问控制>安全组”中找到本实验创建的安全组，点击操作栏的“更多>删除”。

步骤 9 删除 VPC。

- 在服务列表中选择“虚拟私有云 VPC”，点击“子网”页签，在列表中找到本实验创建的子网，点击操作栏中的“删除”。
- 点击“虚拟私有云”页签，找到本实验创建的 VPC，点击操作栏中的“删除”删除 ECS，删除安全组，删除 VPC。

8.4 思考题

问题：AOM 服务的 Agent 管理页面中用户自定义接入主机的 IP 是如何获取的?

参考答案：AOM 会默认遍历虚机上的所有网卡设备，按照以太网卡、Bond 网卡、无线网卡等优先级顺序获取 IP，如果获取到的不是期望的地址，可以在启动 ICAgent 时设置进程的环境变量 IC_NET_CARD=网卡名，获取指定网卡 IP。

9 华为云 EI 实验（选做）

9.1 实验介绍

9.1.1 关于本实验

在企业智能（Enterprise Intelligence，简称 EI）实验中，将通过华为云 ModelArts 服务进行图像识别相关实验操作。

本实验指导用户在华为云 ModelArts 平台使用 flowers 数据集对预置的模型进行训练，快速构建花卉图像分类应用。

实验内容为沙箱实验，通过华为云沙箱进行实验操作。

9.1.2 实验目的

使用户掌握如何使用 ModelArts 服务进行数据集创建，预置模型选择，模型训练、部署并最终建立在线预测作业。

9.2 实验配置

9.2.1 实验环境信息

浏览器输入地址：https://lab.huaweicloud.com/testdetail_287；点击“开始实验”，参照沙箱中的实验手册，完成相关实验操作。

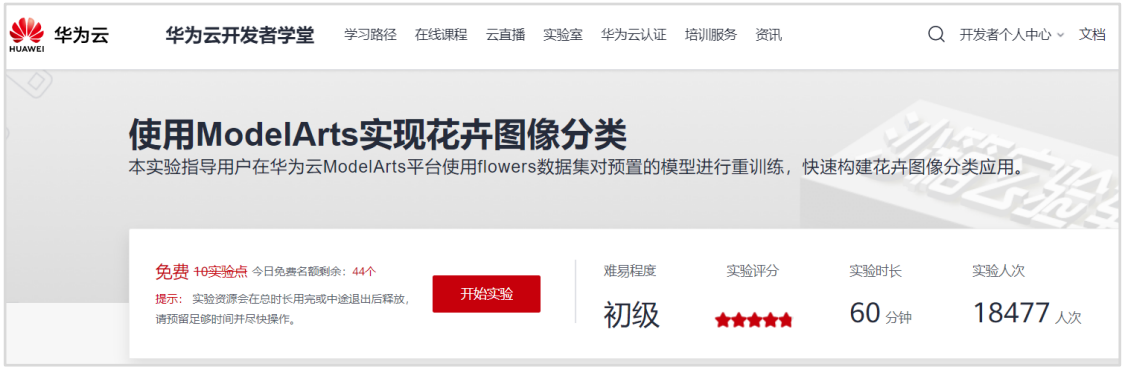


图9-1