Huawei Cloud Service Certification Training

HCIP-Cloud Service Solutions Architect

Lab Guide

ISSUE: 3.0

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base Bantian, Longgang Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

Huawei Certification System

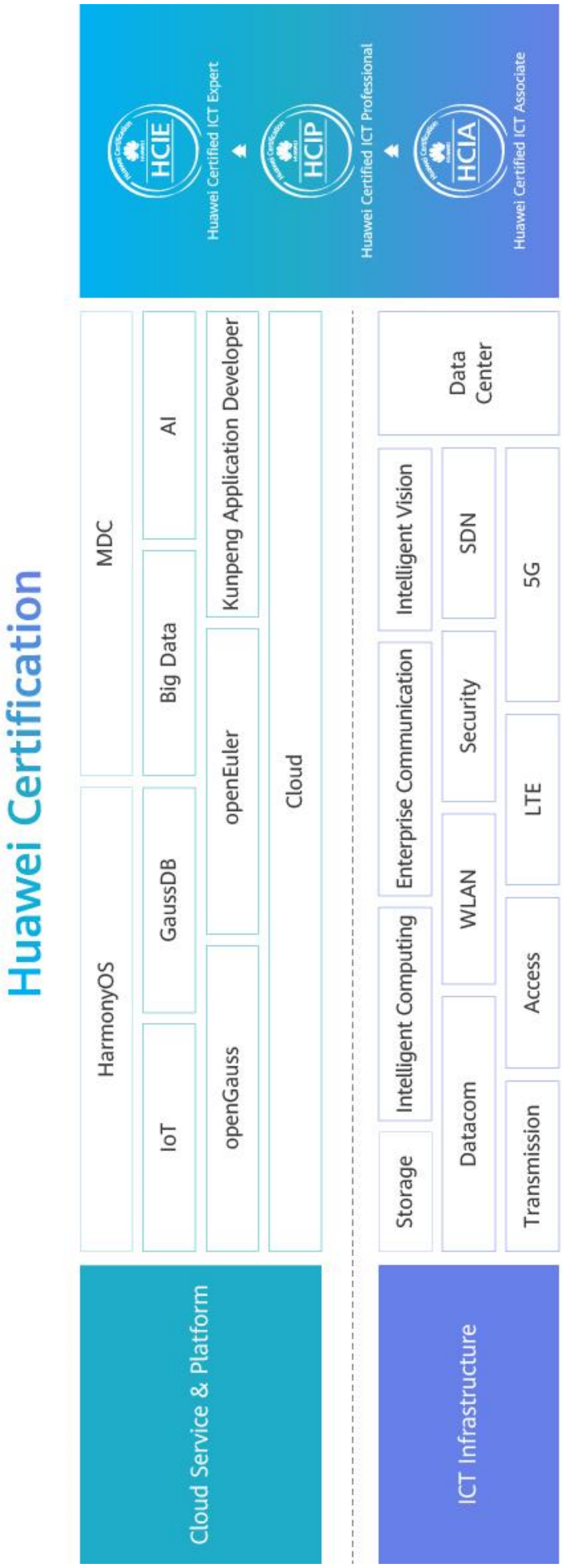
Huawei Certification is an integral part of the company's "Platform + Ecosystem" strategy, and it supports the ICT infrastructure featuring "Cloud-Pipe-Device". It evolves to reflect the latest trends of ICT development. Huawei Certification consists of two categories: ICT Infrastructure Certification, and Cloud Service & Platform Certification, making it the most extensive technical certification program in the industry.

Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE).

Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

The courses of the HCIP-Cloud Service Solutions Architect V3.0 describe the evolution of enterprise IT, cloud-based architecture of traditional applications, cloud native application architecture, and Huawei Cloud innovations and solutions, etc.

Huawei certification helps you unlock opportunities to advance your career and take one more step towards the top of the industry.


Huawei Certification
Cloud Service & Platform
HarmonyOS
MDC
IoT
GaussDB
Big Data
AI
openGauss
openEuler
Kunpeng Application Developer
Cloud
ICT Infrastructure
Storage
Intelligent Computing
Enterprise Communication
Intelligent Vision
Datacom
WLAN
Security
SDN
Data Center
Transmission
Access
LTE
5G
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate

About This Document

Introduction

This document is intended for readers who are preparing for the HCIP-Cloud Service Solutions Architect exam or interested in the basics of the HCIP-Cloud Service Solutions Architect courses, including the evolution of enterprise IT, cloud-based architecture of traditional applications, solution design of cloud-based compute, storage, network, database, and security, containers and cloud native, and Huawei Cloud O&M.

About the Exercises

This document includes eight exercises: compute architecture design, network architecture design, storage architecture design, database architecture design, security architecture design, containerized application deployment, microservice application deployment, and cloud O&M.

- Exercise 1 is about compute architecture design. This exercise will guide you through creating a WordPress website and configuring high availability (HA). This experiment also provides guidance on configuring text injection in AS to facilitate resource configuration management.
- Exercise 2 is about network architecture design. This exercise uses Huawei Cloud resources in different regions to represent on-premises and cloud resources, describes how on-premises resources can communicate with cloud resources and manage cloud resources for O&M, and how cloud resources can communicate with each other and access the internet. This exercise helps you deeply understand the Huawei Cloud network architecture and usage principles.
- Exercise 3 is about storage architecture design. This exercise aims to help you understand the architecture and principles of Huawei Cloud storage services by setting up an environment to run video streaming services.
- Exercise 4 is about database architecture design. This exercise describes how to set up a website using ECSs and cloud database instances and to configure a Redis instance for it, helping you understand architectures and usage of Huawei cloud databases.
- Exercise 5 is about security architecture design. This exercise describes host security, two-factor authentication (2FA), address group, and key hosting on Data Encryption Workshop (DEW). It helps you deeply understand the security architecture of Huawei Cloud and how it works.
- Exercise 6 is about containerized application deployment. In this exercise, image is created and pushed to Huawei SoftWare Repository for Container (SWR) for deploying a container on Cloud Container Engine (CCE). In this way, you will understand how to use the Dockerfile to build images and CCE, retain the latest

three object versions in the OBS bucket using FunctionGraph, and use and configure FunctionGraph.

- Exercise 7 is about microservice application deployment, including microservice deployment and weathermap microservice building through ServiceStage, helping you understand the methods and principles of building ServiceStage microservices.
- Exercise 8 is about cloud O&M, including Cloud Eye and Application Operations Management (AOM), helping you understand their architectures, principles, and usage.

Knowledge Background

This document is part of the Huawei certification courses. Before reading this document, readers should understand:

- Basics of the HCIA-Cloud Service courses and cloud computing
- Basics of Linux

Lab Environment

The lab environment of these exercises is Huawei Cloud (https://www.huaweicloud.com/intl/en-us/). You do not need to purchase any equipment and all the operations described in this document are performed in this environment. Log in to Huawei Cloud Help Center (https://support.huaweicloud.com/intl/en-us/) if you need technical help.

Contents

1 Compute Architecture Design

1.1 Introduction

1.1.1 About This Exercise

In this exercise, you will be guided on how to create a WordPress website using Elastic Cloud Server (ECS) and Relational Database Service (RDS) in Virtual Private Cloud (VPC) on Huawei Cloud. In the cloud architecture, Elastic Load Balance (ELB) will be used to distribute traffic and improve fault tolerance of the website. Auto Scaling (AS) will be used to ensure high service quality and compute resource utilization. Text injection will be used to keep the address of the backend database connected to ECSs created by AS unchanged during resource scaling. After completing this exercise, you will understand how to use Huawei Cloud compute services.

1.1.2 Objectives

Understand how to use cloud services in the cloud computing architecture design.

Master the methods for designing the availability, scalability, and performance of cloud resources.

1.1.3 Related Software

WordPress is a free open-source project and a blog software. You can use WordPress to set up your own websites on servers that support PHP and MySQL databases.

1.1.4 Networking

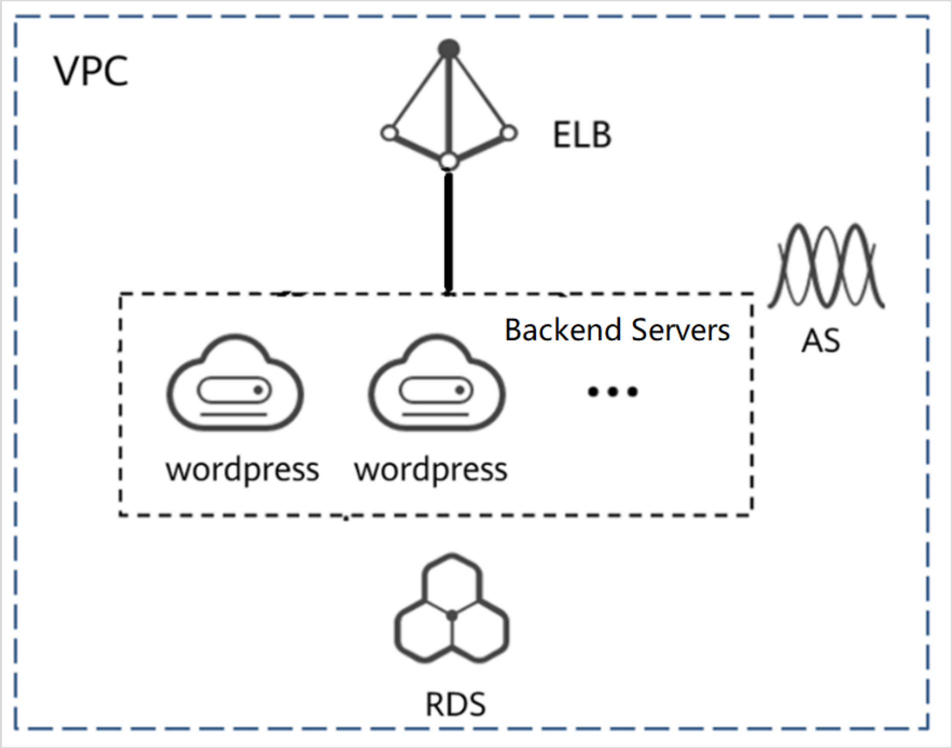


Figure 1-1

1.2 Procedure

1.2.1 Creating VPCs and Security Groups

Step 1 Visit https://intl.huaweicloud.com/en-us/ and log in using your Huawei Cloud account. Select **CN-Hong Kong** region (The **CN-Hong Kong** region is used as an example in this exercise), and choose **Networking** > **Virtual Private Cloud** in the service list.

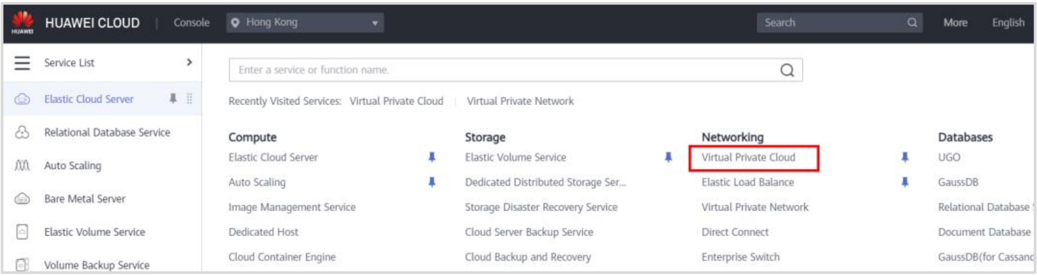


Figure 1-2

Step 2 Click **Create VPC**. (Resources in this exercise will be created in this VPC.)

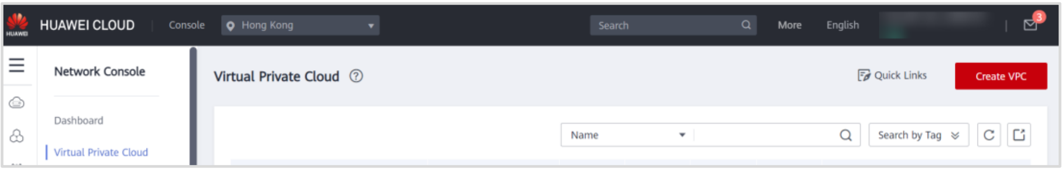


Figure 1-3

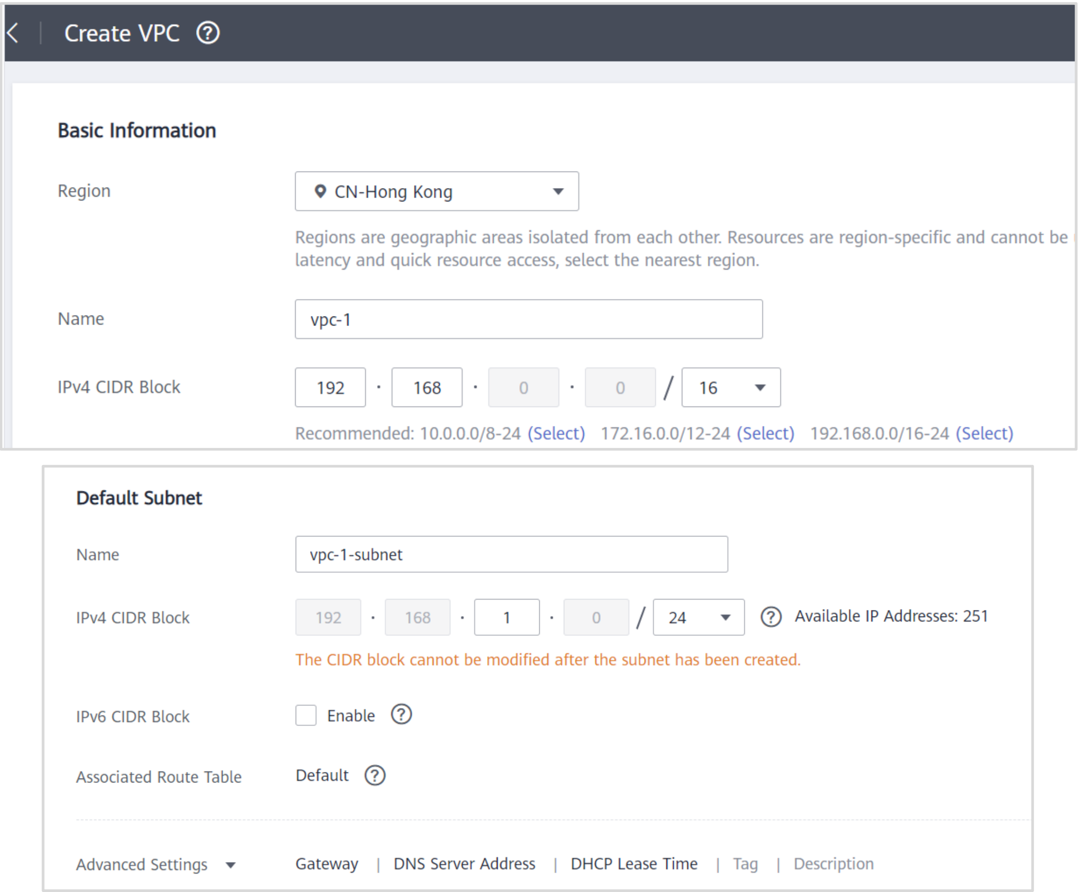
Step 3 Configure the following parameters and click **Create Now**.

Basic Information

- **Region**: **CN-Hong Kong** (The **CN-Hong Kong** region is used as an example in this exercise.)
- **Name**: **vpc-1**
- **IPv4 CIDR Block**: **192.168.0.0/16**

Default Subnet

- **AZ**: **AZ3** (**AZ3** is used as an example in this exercise.)
- **Name**: **vpc-1-subnet**
- **IPv4 CIDR Block**: **192.168.1.0/24**



Create VPC

Basic Information

Region: CN-Hong Kong

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be latency and quick resource access, select the nearest region.

Name: vpc-1

IPv4 CIDR Block: 192 . 168 . 0 . 0 / 16

Recommended: 10.0.0.0/8-24 (Select) 172.16.0.0/12-24 (Select) 192.168.0.0/16-24 (Select)

Default Subnet

Name: vpc-1-subnet

IPv4 CIDR Block: 192 . 168 . 1 . 0 / 24 Available IP Addresses: 251

The CIDR block cannot be modified after the subnet has been created.

IPv6 CIDR Block: □ Enable

Associated Route Table: Default

Advanced Settings: Gateway | DNS Server Address | DHCP Lease Time | Tag | Description

Figure 1-4

Step 4 On the Network Console, choose Access Control > Security Groups, and click Create Security Group in the upper right corner.

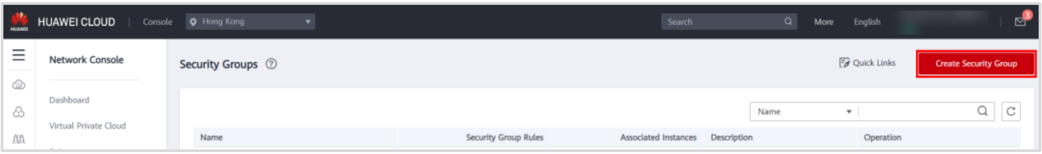
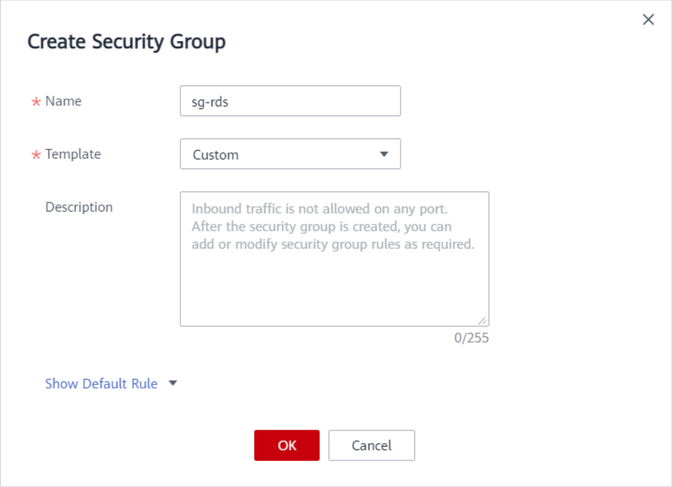


Figure 1-5

Step 5 Create a security group. (This security group is used by the RDS service and traffic should be allowed on port 3306.)

- **Name**: **sg-rds**
- **Template**: Select a required one.


Create Security Group

* Name: sg-rds

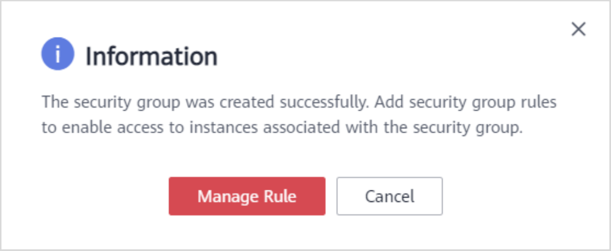
* Template: Custom

Description: Inbound traffic is not allowed on any port. After the security group is created, you can add or modify security group rules as required.

0/255

Figure 1-6

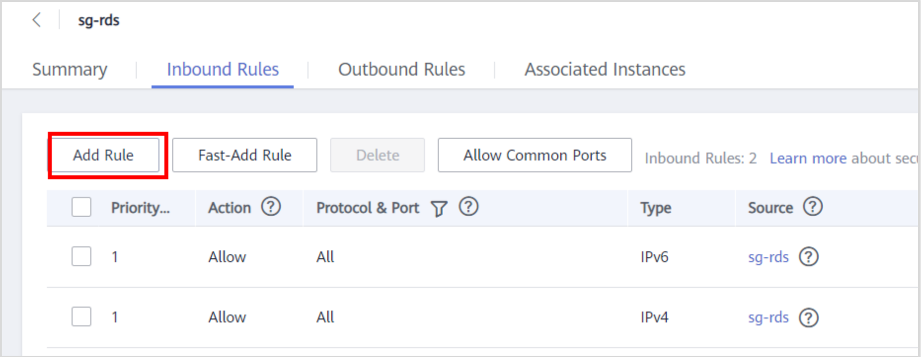
Step 6 In the dialog box displayed, click **Manage Rule**.


Information

The security group was created successfully. Add security group rules to enable access to instances associated with the security group.

Figure 1-7

Step 7 Click the **Inbound Rules** tab, and then click **Add Rule**.

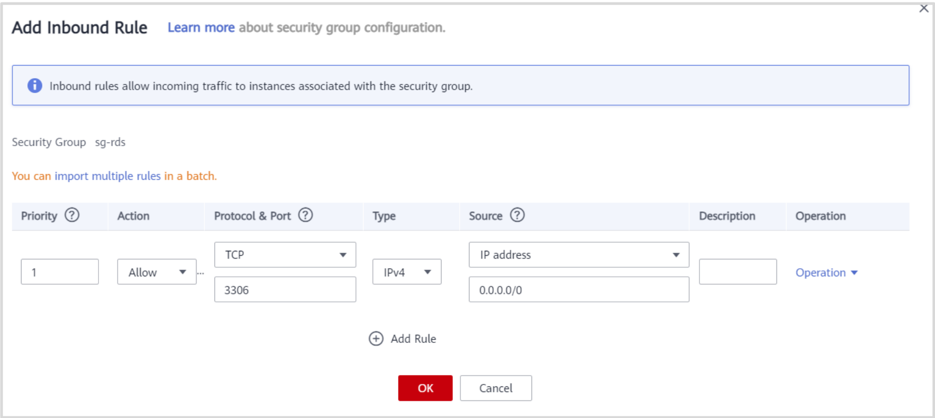


	Priority...	Action	Protocol & Port	Type	Source
□	1	Allow	All	IPv6	sg-rds
□	1	Allow	All	IPv4	sg-rds

Figure 1-8

Step 8 Add a rule as follows:

- **Priority**: **1**
- **Action**: **Allow**
- **Protocol**: **TCP**
- **Port**: **3306**
- **Source**: **IP address** and **0.0.0.0**



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

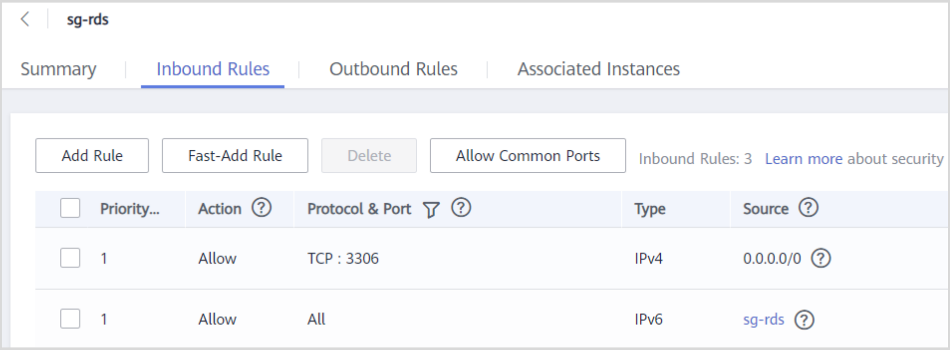
Security Group sg-rds

You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Source	Description	Operation
1	Allow	TCP 3306	IPv4	IP address 0.0.0.0/0		Operation

Figure 1-9

Step 9 Click **OK**.



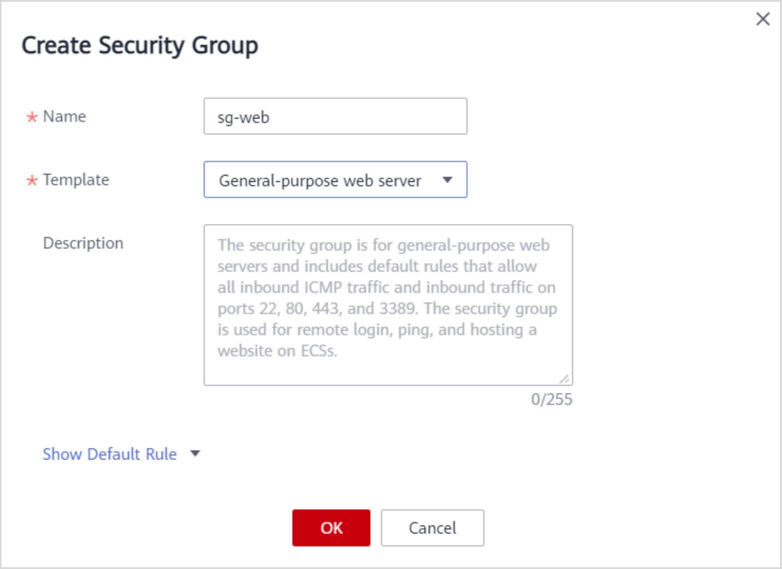
sg-rds

Inbound Rules: 3 Learn more about security

	Priority...	Action	Protocol & Port	Type	Source
□	1	Allow	TCP : 3306	IPv4	0.0.0.0/0
□	1	Allow	All	IPv6	sg-rds

Figure 1-10

Step 10 Create the security group **sg-web** and select **General-purpose web server** as its template. (This security group is used by the ECS in this exercise.)



Create Security Group

* Name: sg-web

* Template: General-purpose web server

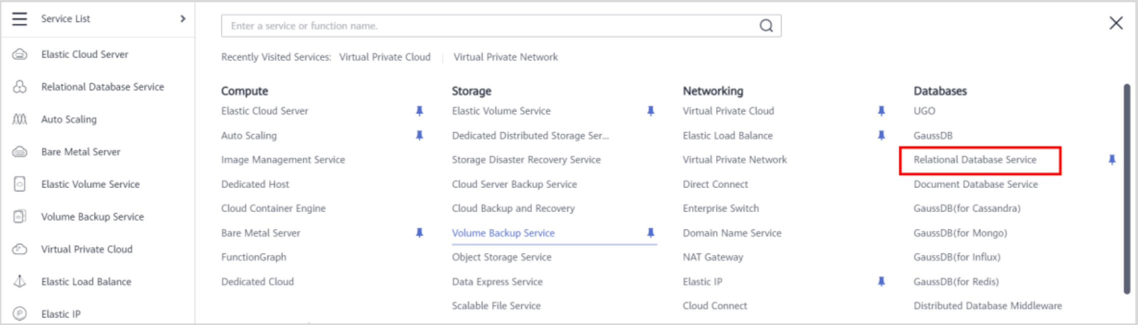
Description: The security group is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and inbound traffic on ports 22, 80, 443, and 3389. The security group is used for remote login, ping, and hosting a website on ECSs.

0/255

Figure 1-11

1.2.2 Creating an RDS Instance

Step 1 In the service list, choose **Relational Database Service**.



Recently Visited Services: Virtual Private Cloud | Virtual Private Network

Compute: Elastic Cloud Server, Auto Scaling, Image Management Service, Dedicated Host, Cloud Container Engine, Bare Metal Server, FunctionGraph, Dedicated Cloud

Storage: Elastic Volume Service, Dedicated Distributed Storage Ser..., Storage Disaster Recovery Service, Cloud Server Backup Service, Cloud Backup and Recovery, Volume Backup Service, Object Storage Service, Data Express Service, Scalable File Service

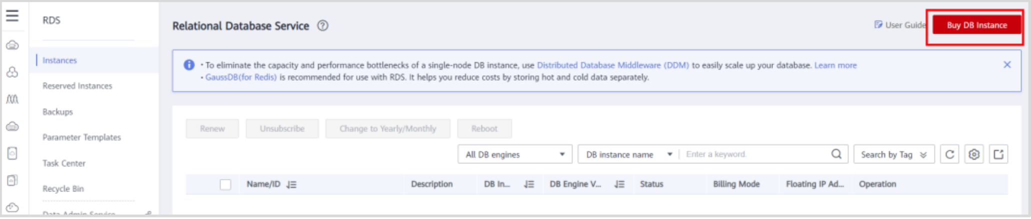
Networking: Virtual Private Cloud, Elastic Load Balance, Virtual Private Network, Direct Connect, Enterprise Switch, Domain Name Service, NAT Gateway, Elastic IP, Cloud Connect

Databases: UGO, GaussDB, Relational Database Service, Document Database Service, GaussDB(for Cassandra), GaussDB(for Mongo), GaussDB(for Influx), GaussDB(for Redis), Distributed Database Middleware

Figure 1-12

Step 2 Click **Buy DB Instance** in the upper right corner.

Note: In this DB instance, a database will be created to interconnect with WordPress.



• To eliminate the capacity and performance bottlenecks of a single-node DB instance, use Distributed Database Middleware (DDM) to easily scale up your database. Learn more
• GaussDB(for Redis) is recommended for use with RDS. It helps you reduce costs by storing hot and cold data separately.

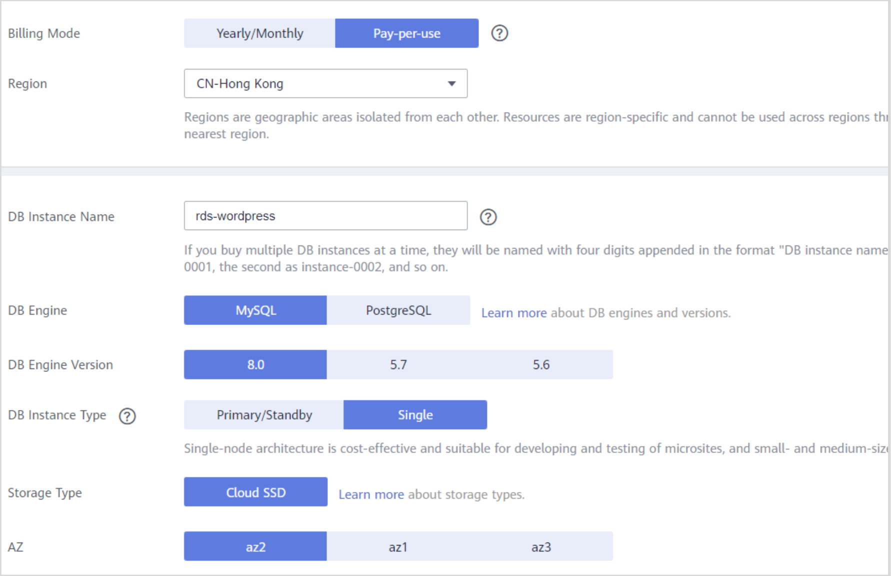
Name/ID	Description	DB In...	DB Engine V...	Status	Billing Mode	Floating IP Ad...	Operation

Figure 1-13

Step 3 Configure parameters as follows:

- **Billing Mode**: **Pay-per-use**
- **Region**: **CN-Hong Kong** (The **CN-Hong Kong** region is used as an example in this exercise.)

- DB Instance Name: rds-wordpress
- DB Engine: MySQL
- DB Engine Version: 8.0
- DB Instance Type: Single
- AZ: az2 (az2 is used as an example in this exercise.)
- Instance Class: 2 vCPUs | 4 GB
- Storage Space (GB): 40
- Disk Encryption: Disable



Billing Mode: Yearly/Monthly | **Pay-per-use**

Region: CN-Hong Kong

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions th nearest region.

DB Instance Name: rds-wordpress

If you buy multiple DB instances at a time, they will be named with four digits appended in the format "DB instance name 0001, the second as instance-0002, and so on.

DB Engine: **MySQL** | PostgreSQL — Learn more about DB engines and versions.

DB Engine Version: **8.0** | 5.7 | 5.6

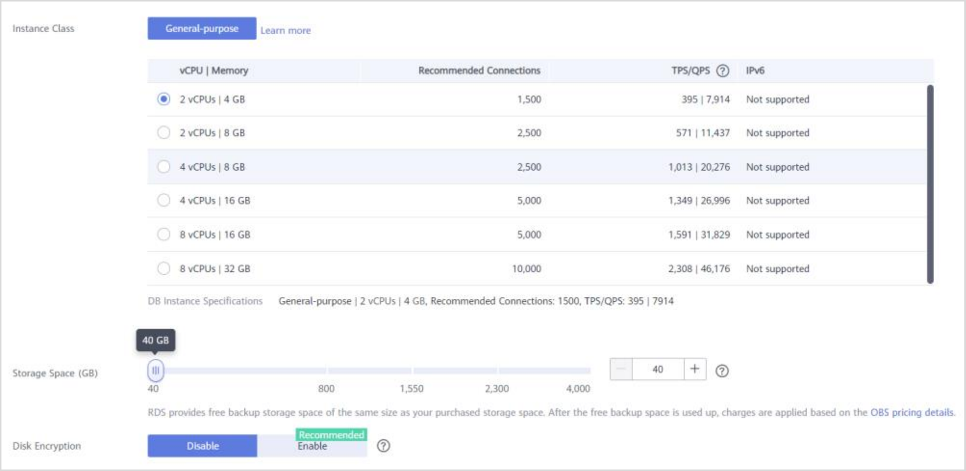
DB Instance Type: Primary/Standby | **Single**

Single-node architecture is cost-effective and suitable for developing and testing of microsites, and small- and medium-siz

Storage Type: **Cloud SSD** — Learn more about storage types.

AZ: **az2** | az1 | az3

Figure 1-14



Instance Class: **General-purpose** Learn more

	vCPU | Memory	Recommended Connections	TPS/QPS	IPv6
●	2 vCPUs | 4 GB	1,500	395 | 7,914	Not supported
○	2 vCPUs | 8 GB	2,500	571 | 11,437	Not supported
○	4 vCPUs | 8 GB	2,500	1,013 | 20,276	Not supported
○	4 vCPUs | 16 GB	5,000	1,349 | 26,996	Not supported
○	8 vCPUs | 16 GB	5,000	1,591 | 31,829	Not supported
○	8 vCPUs | 32 GB	10,000	2,308 | 46,176	Not supported

DB Instance Specifications: General-purpose | 2 vCPUs | 4 GB, Recommended Connections: 1500, TPS/QPS: 395 | 7914

Storage Space (GB): 40 GB

40

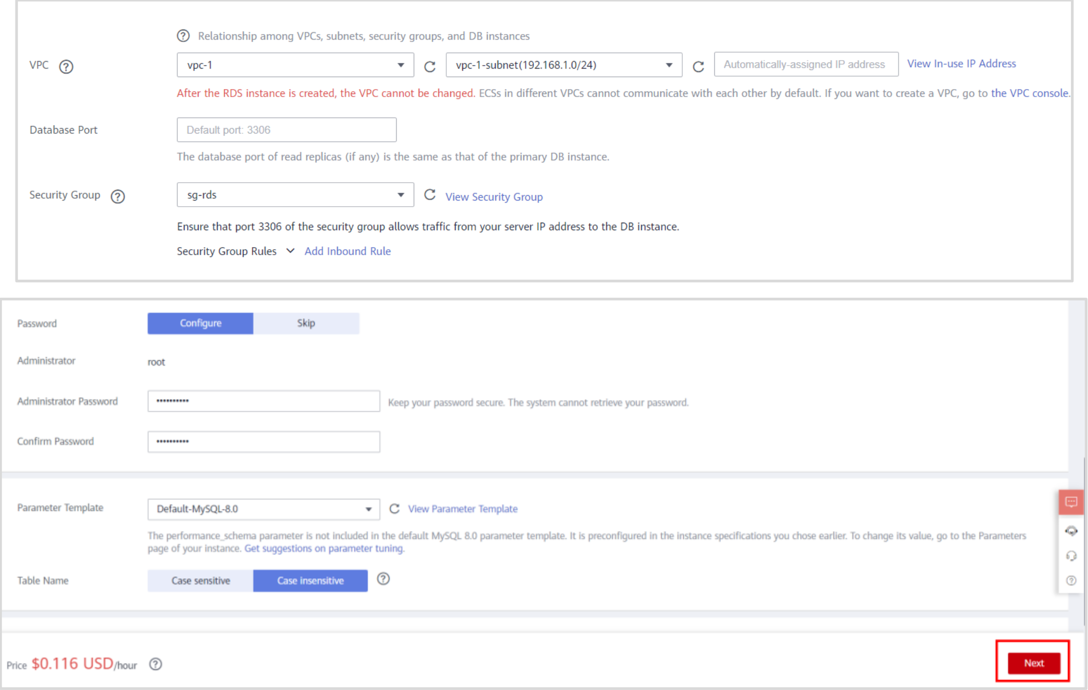
RDS provides free backup storage space of the same size as your purchased storage space. After the free backup space is used up, charges are applied based on the OBS pricing details.

Disk Encryption: **Disable** | Enable (Recommended)

Figure 1-15

- VPC: vpc-1
- Subnet: vpc-1-subnet
- Security Group: sg-rds
- Administrator Password: User-defined

- Retain the default values for other parameters.



Relationship among VPCs, subnets, security groups, and DB instances

VPC: vpc-1 | vpc-1-subnet(192.168.1.0/24) | Automatically-assigned IP address

After the RDS instance is created, the VPC cannot be changed. ECSs in different VPCs cannot communicate with each other by default. If you want to create a VPC, go to the VPC console.

Database Port: Default port: 3306

The database port of read replicas (if any) is the same as that of the primary DB instance.

Security Group: sg-rds

Ensure that port 3306 of the security group allows traffic from your server IP address to the DB instance.

Password: Configure

Administrator: root

Administrator Password: ••••••••••

Keep your password secure. The system cannot retrieve your password.

Confirm Password: ••••••••••

Parameter Template: Default-MySQL-8.0

The performance_schema parameter is not included in the default MySQL 8.0 parameter template. It is preconfigured in the instance specifications you chose earlier. To change its value, go to the Parameters page of your instance. Get suggestions on parameter tuning.

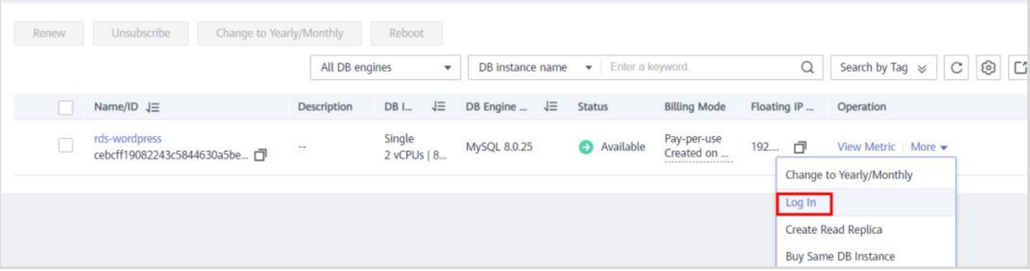
Table Name: Case insensitive

Price $0.116 USD/hour

Figure 1-16

Step 4 Click **Next**. Confirm the configurations and click **Submit**.

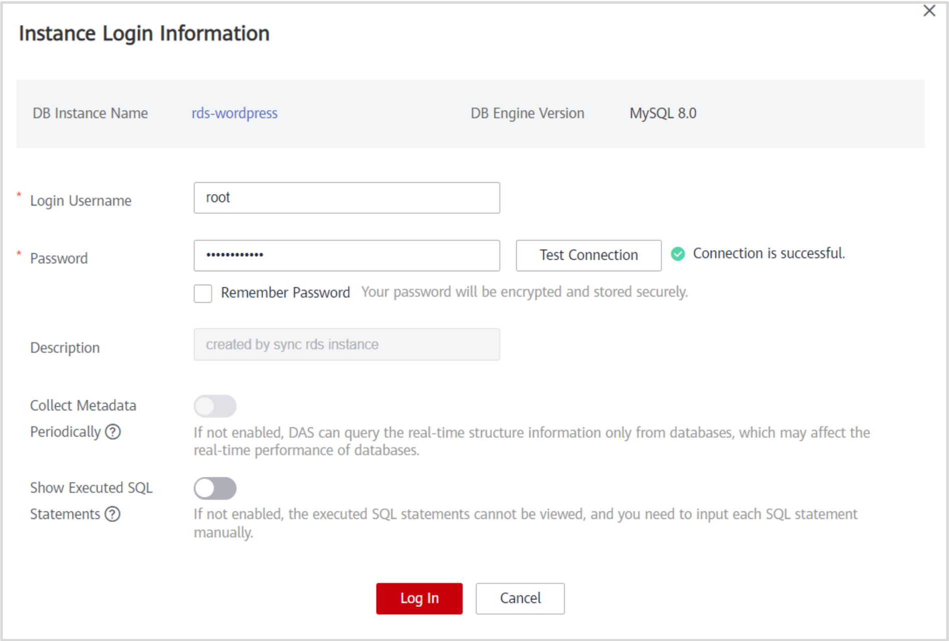
Step 5 On the **Instances** page, locate the instance and choose **More** > **Log In** in the **Operation** column.



	Name/ID	Description	DB I...	DB Engine ...	Status	Billing Mode	Floating IP ...	Operation
□	rds-wordpress cebcff19082243c5844630a5be...	--	Single 2 vCPUs | 8...	MySQL 8.0.25	Available	Pay-per-use Created on ...	192....	View Metric More

Figure 1-17

Step 6 Enter the username and password, click **Test Connection**, and then click **Log In**.



Instance Login Information

DB Instance Name: rds-wordpress

DB Engine Version: MySQL 8.0

* Login Username: root

* Password: ••••••••••• Test Connection ✓ Connection is successful.

□ Remember Password Your password will be encrypted and stored securely.

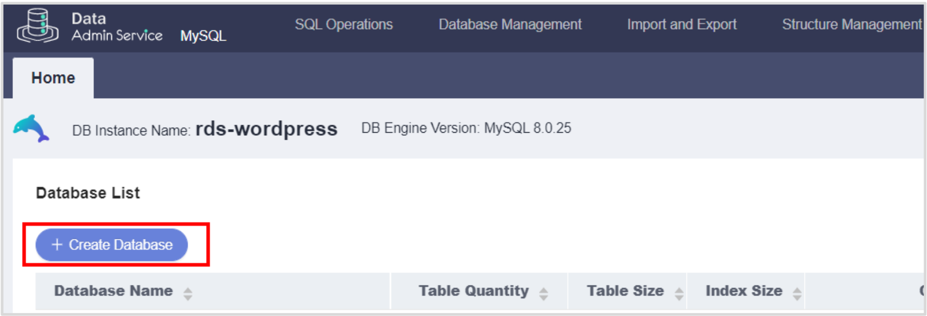
Description: created by sync rds instance

Collect Metadata Periodically: If not enabled, DAS can query the real-time structure information only from databases, which may affect the real-time performance of databases.

Show Executed SQL Statements: If not enabled, the executed SQL statements cannot be viewed, and you need to input each SQL statement manually.

Figure 1-18

Step 7 On the displayed page, click **Create Database**. The created database will be used to interconnect with WordPress.



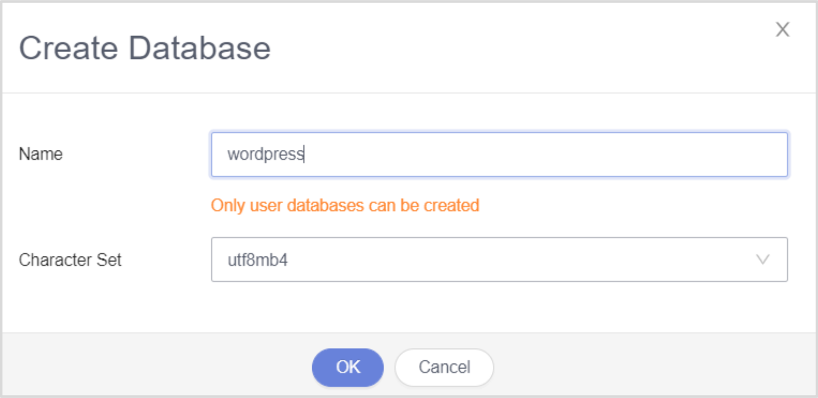
DB Instance Name: rds-wordpress DB Engine Version: MySQL 8.0.25

Database List

Database Name	Table Quantity	Table Size	Index Size

Figure 1-19

Step 8 Enter **wordpress** for **Name**, retain the default character set, and click **OK**.



Create Database

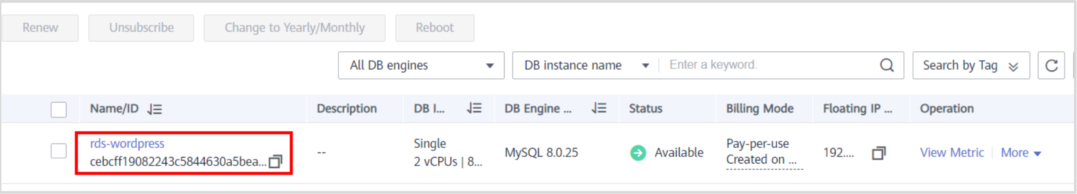
Name: wordpress

Only user databases can be created

Character Set: utf8mb4

Figure 1-20

Step 9 Switch back to the RDS console. On the **Instances** page, click the instance name to go to the **Basic Information** page.

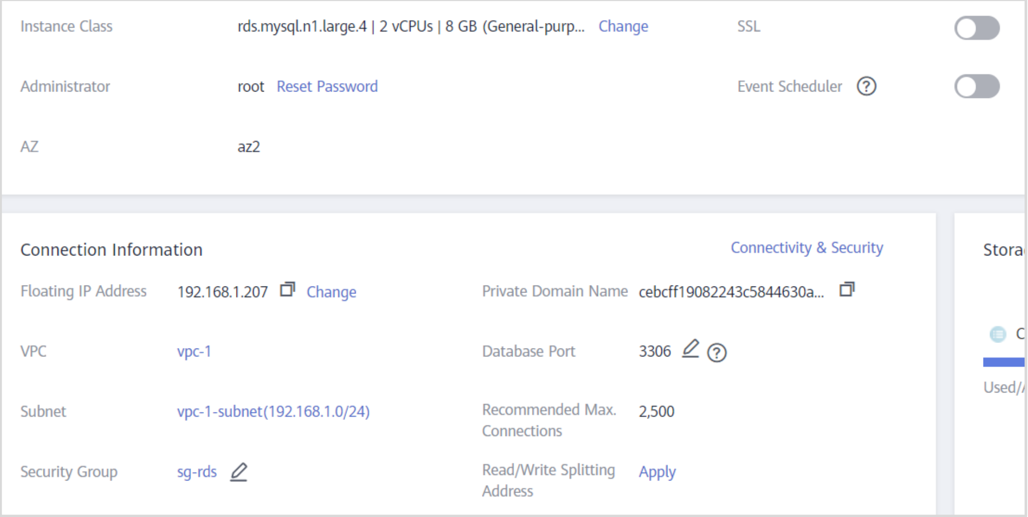


	Name/ID	Description	DB I...	DB Engine ...	Status	Billing Mode	Floating IP ...	Operation
□	rds-wordpress cebcff19082243c5844630a5bea...	--	Single 2 vCPUs | 8...	MySQL 8.0.25	Available	Pay-per-use Created on ...	192....	View Metric | More

Figure 1-21

Step 10 Record the floating IP address and port number of the instance for future use.

Note: When configuring WordPress, you need to enter such information in the configuration file.



Instance Class	rds.mysql.n1.large.4 | 2 vCPUs | 8 GB (General-purp... Change	SSL	
Administrator	root Reset Password	Event Scheduler	
AZ	az2		

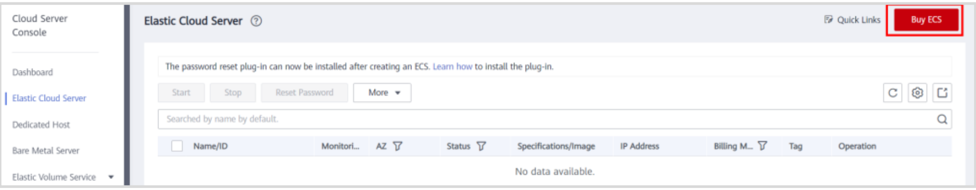
Connection Information

Floating IP Address	192.168.1.207 Change	Private Domain Name	cebcff19082243c5844630a...
VPC	vpc-1	Database Port	3306
Subnet	vpc-1-subnet(192.168.1.0/24)	Recommended Max. Connections	2,500
Security Group	sg-rds	Read/Write Splitting Address	Apply

Figure 1-22

1.2.3 Creating an ECS

Step 1 In the service list, choose **Compute** > **Elastic Cloud Server**, and click **Buy ECS** in the upper right corner.



The password reset plug-in can now be installed after creating an ECS. Learn how to install the plug-in.

□	Name/ID	Monitori...	AZ	Status	Specifications/Image	IP Address	Billing M...	Tag	Operation

No data available.

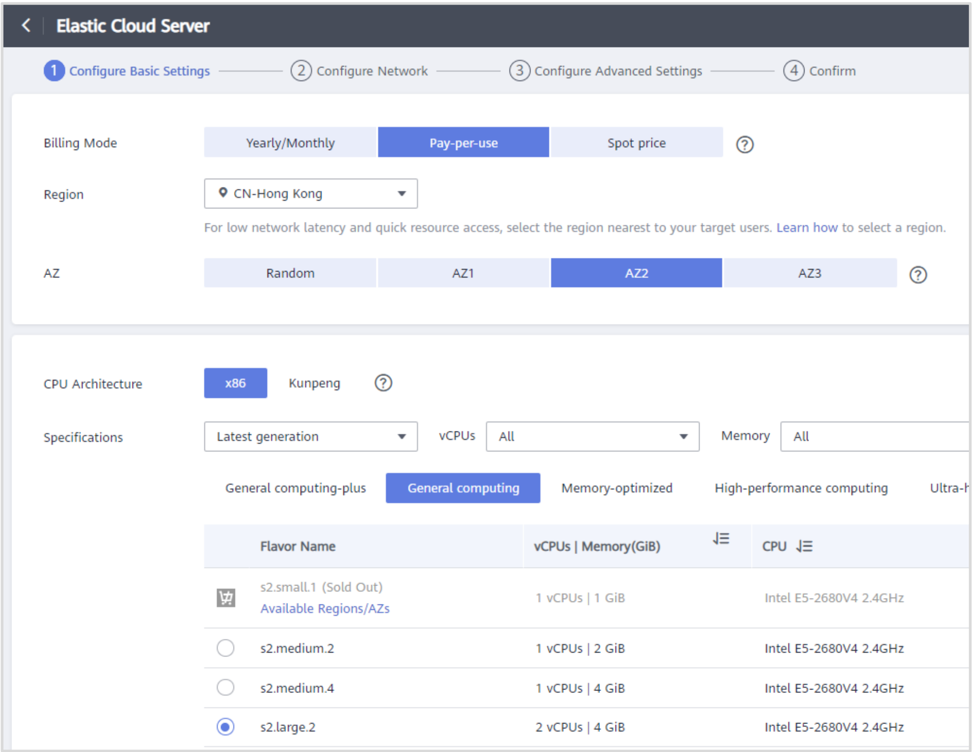
Figure 1-23

Step 2 Configure settings for the ECS.

The following uses **ecs-wordpress** as an example.

- **Billing Mode**: **Pay-per-use**

- **Region**: **CN-Hong Kong** (The **CN-Hong Kong** region is used as an example in this exercise.)
- **AZ**: **AZ 2** (**AZ 2** is used as an example in this exercise.)
- **CPU Architecture**: **x86**
- **Specifications**: **2 vCPUs | 4 GiB**
- **Image**: **Public image** | **CentOS 7.6 64bit(40GB)**
- **Host Security**: **Enable** (Basic)
- **Network**: **vpc-1** | **vpc-1-subnet** | **Automatically assign IP address**
- **Security Group**: **sg-web**
- **EIP**: **Auto assign**
- **EIP Type**: **Premium BGP**
- **Billed By**: **Traffic**
- **Bandwidth Size**: **10 Mbit/s**
- **System Disk**: **High I/O** | **40 GiB**
- **ECS Name**: **ecs-wordpress**
- **Password**: User-defined (with the username of **root**)



Elastic Cloud Server

1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

Billing Mode: Yearly/Monthly | **Pay-per-use** | Spot price

Region: CN-Hong Kong

For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

AZ: Random | AZ1 | **AZ2** | AZ3

CPU Architecture: **x86** | Kunpeng

Specifications: Latest generation | vCPUs: All | Memory: All

General computing-plus | **General computing** | Memory-optimized | High-performance computing | Ultra-

	Flavor Name	vCPUs | Memory(GiB)	CPU
	s2.small.1 (Sold Out) Available Regions/AZs	1 vCPUs | 1 GiB	Intel E5-2680V4 2.4GHz
○	s2.medium.2	1 vCPUs | 2 GiB	Intel E5-2680V4 2.4GHz
○	s2.medium.4	1 vCPUs | 4 GiB	Intel E5-2680V4 2.4GHz
●	s2.large.2	2 vCPUs | 4 GiB	Intel E5-2680V4 2.4GHz

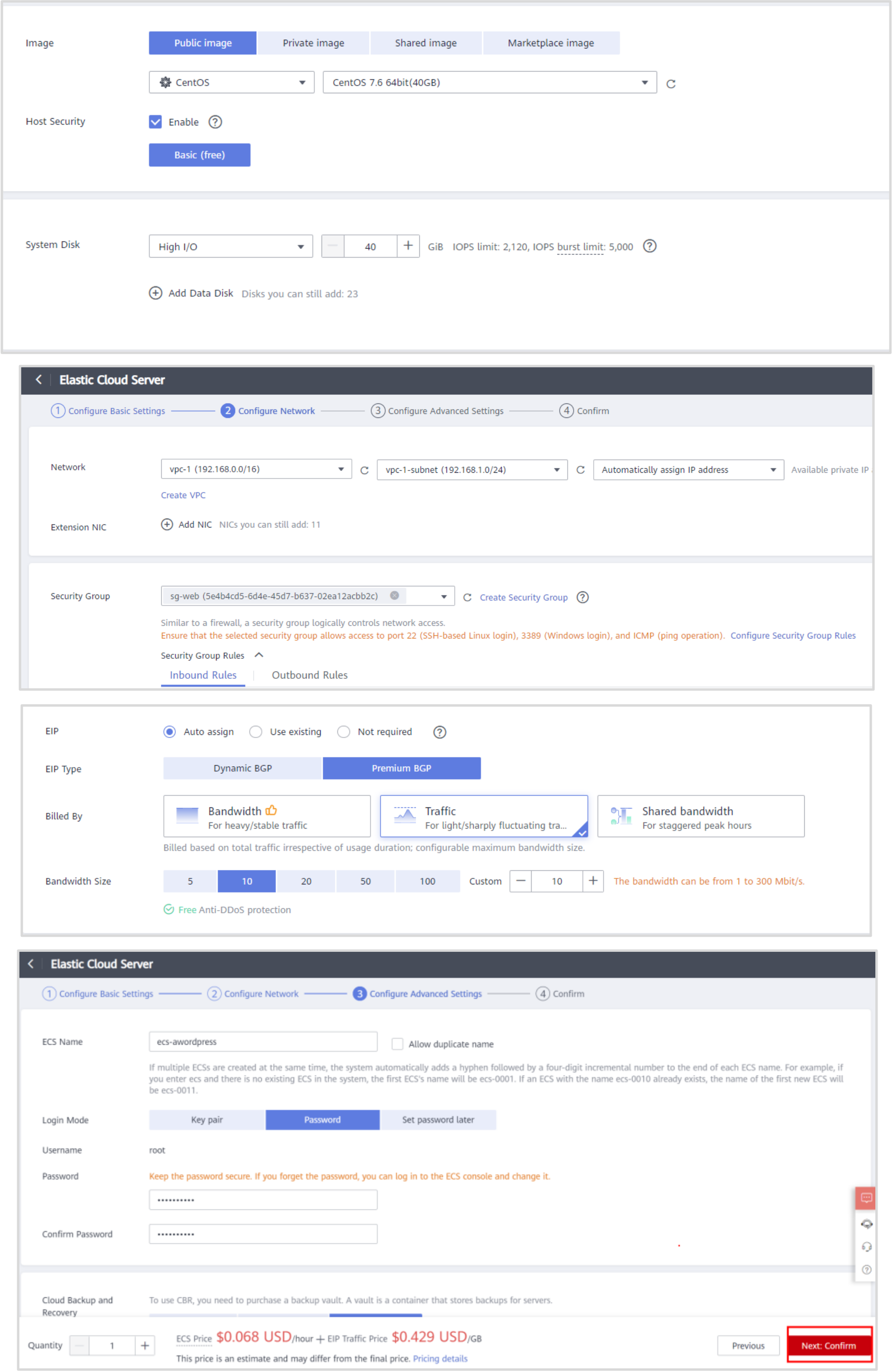


Image: Public image | Private image | Shared image | Marketplace image

CentOS | CentOS 7.6 64bit(40GB)

Host Security: ☑ Enable

Basic (free)

System Disk: High I/O | 40 GiB | IOPS limit: 2,120, IOPS burst limit: 5,000

Add Data Disk Disks you can still add: 23

Elastic Cloud Server

(1) Configure Basic Settings — (2) Configure Network — (3) Configure Advanced Settings — (4) Confirm

Network: vpc-1 (192.168.0.0/16) | vpc-1-subnet (192.168.1.0/24) | Automatically assign IP address | Available private IP

Create VPC

Extension NIC: Add NIC NICs you can still add: 11

Security Group: sg-web (5e4b4cd5-6d4e-45d7-b637-02ea12acbb2c) | Create Security Group

Similar to a firewall, a security group logically controls network access.

Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

Security Group Rules

Inbound Rules | Outbound Rules

EIP: ● Auto assign ○ Use existing ○ Not required

EIP Type: Dynamic BGP | Premium BGP

Billed By: Bandwidth — For heavy/stable traffic | Traffic — For light/sharply fluctuating tra... | Shared bandwidth — For staggered peak hours

Billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size.

Bandwidth Size: 5 | 10 | 20 | 50 | 100 | Custom 10 | The bandwidth can be from 1 to 300 Mbit/s.

Free Anti-DDoS protection

Elastic Cloud Server

(1) Configure Basic Settings — (2) Configure Network — (3) Configure Advanced Settings — (4) Confirm

ECS Name: ecs-awordpress □ Allow duplicate name

If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a four-digit incremental number to the end of each ECS name. For example, if you enter ecs and there is no existing ECS in the system, the first ECS's name will be ecs-0001. If an ECS with the name ecs-0010 already exists, the name of the first new ECS will be ecs-0011.

Login Mode: Key pair | Password | Set password later

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.

••••••••••

Confirm Password: ••••••••••

Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.

Quantity: 1 | ECS Price $0.068 USD/hour + EIP Traffic Price $0.429 USD/GB

This price is an estimate and may differ from the final price. Pricing details

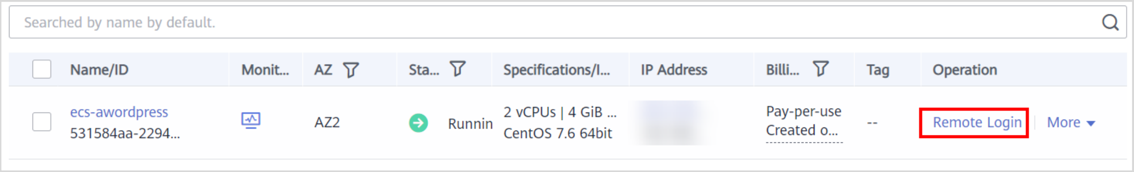
Previous | Next: Confirm

Figure 1-24

Step 3 Confirm the configurations and click **Submit**.

1.2.4 Installing WordPress

Step 1 Locate the newly purchased ECS in the ECS list and click **Remote Login** in the **Operation** column.



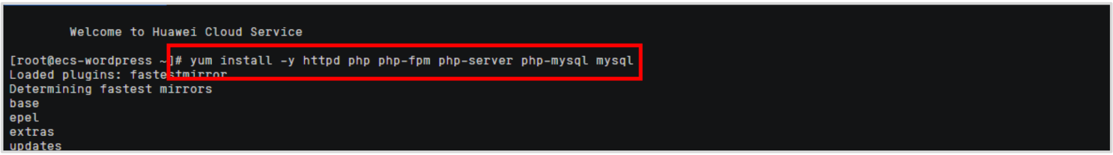
Searched by name by default.

□	Name/ID	Monit...	AZ	Sta...	Specifications/I...	IP Address	Billi...	Tag	Operation
□	ecs-awordpress 531584aa-2294...		AZ2	Runnin	2 vCPUs | 4 GiB ... CentOS 7.6 64bit	[redacted]	Pay-per-use Created o...	--	Remote Login More ▾

Figure 1-25

Step 2 Install Linux, Apache, MySQL, PHP/Perl/Python (LAMP) and start related services.

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



```
         Welcome to Huawei Cloud Service

[root@ecs-wordpress ~]# yum install -y httpd php php-fpm php-server php-mysql mysql
Loaded plugins: fastestmirror
Determining fastest mirrors
base
epel
extras
updates
```

Figure 1-26

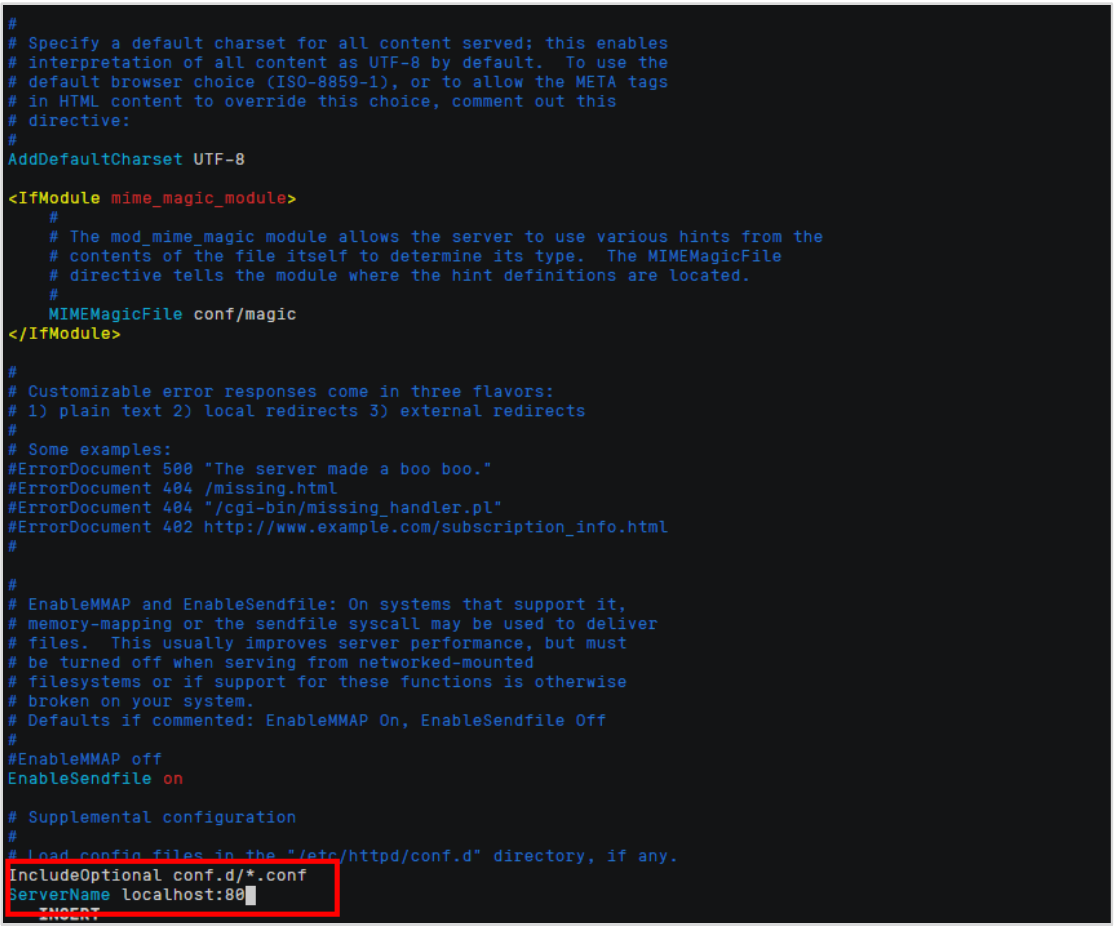
Step 3 Configure httpd.

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

Step 4 In the configuration file, press **Shift+G** to go to the last line of the configuration file, press **I** to enter the editing mode, move the cursor to the end of the configuration file, and press **Enter**. Then copy and paste the following code.

Note: This step is used to set the host name and port number for the server. To enhance reliability and predictability, use the host name and port number specified by **ServerName**.

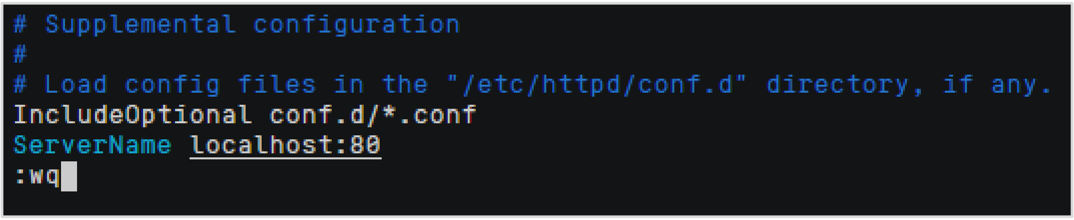
```
ServerName localhost:80
```



```
#
# 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
 INSERT
```

Figure 1-27

Step 5 Press **Esc** to exit the editing mode, enter **:wq**, and press **Enter** to save and exit the configuration file.

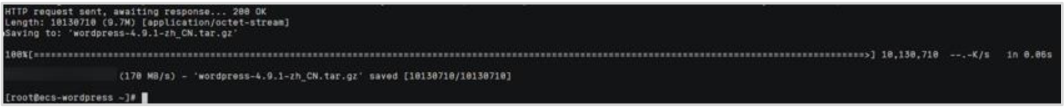


```
# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ServerName localhost:80
:wq
```

Figure 1-28

Step 6 Download the WordPress installation package.

```
[root@ecs-wordpress ~]# wget -c https://cloudservice-v3.obs.cn-east-3.myhuaweicloud.com/wordpress-4.9.10_en.tar.gz
```



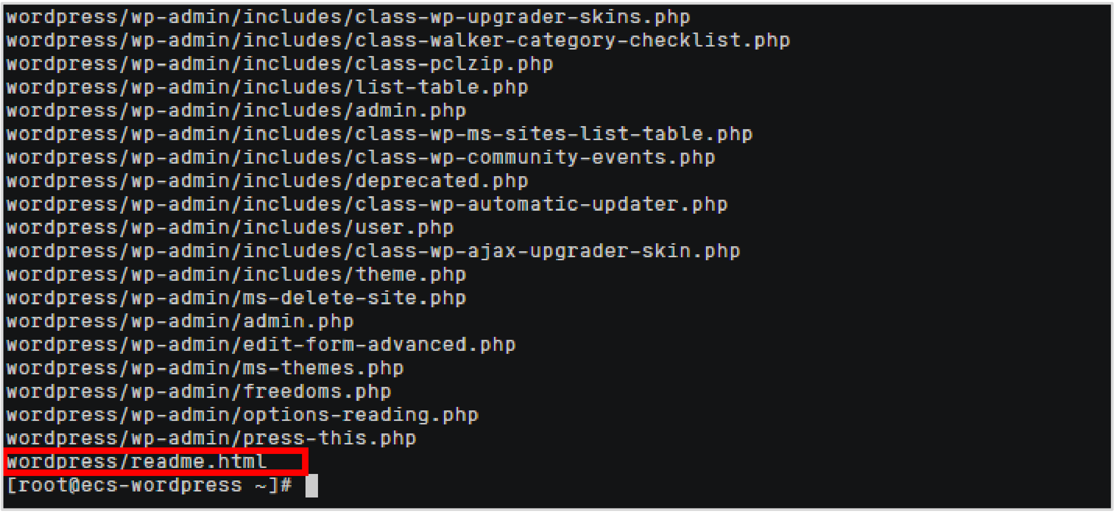
```
HTTP request sent, awaiting response... 200 OK
Length: 10130710 (9.7M) [application/octet-stream]
Saving to: 'wordpress-4.9.1-zh_CN.tar.gz'

100%[========================================================================================>] 10,130,710  --.-K/s   in 0.06s

                (170 MB/s) - 'wordpress-4.9.1-zh_CN.tar.gz' saved [10130710/10130710]

[root@ecs-wordpress ~]# 
```

Figure 1-29

Step 7 Decompress the WordPress installation package to **/var/www/html**.

```
[root@ecs-wordpress ~]# tar -zxvf wordpress-4.9.10_en.tar.gz -C /var/www/html/
```

The decompression is complete when **wordpress/readme.html** is displayed.

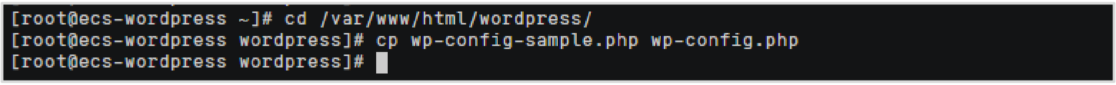


```
wordpress/wp-admin/includes/class-wp-upgrader-skins.php
wordpress/wp-admin/includes/class-walker-category-checklist.php
wordpress/wp-admin/includes/class-pclzip.php
wordpress/wp-admin/includes/list-table.php
wordpress/wp-admin/includes/admin.php
wordpress/wp-admin/includes/class-wp-ms-sites-list-table.php
wordpress/wp-admin/includes/class-wp-community-events.php
wordpress/wp-admin/includes/deprecated.php
wordpress/wp-admin/includes/class-wp-automatic-updater.php
wordpress/wp-admin/includes/user.php
wordpress/wp-admin/includes/class-wp-ajax-upgrader-skin.php
wordpress/wp-admin/includes/theme.php
wordpress/wp-admin/ms-delete-site.php
wordpress/wp-admin/admin.php
wordpress/wp-admin/edit-form-advanced.php
wordpress/wp-admin/ms-themes.php
wordpress/wp-admin/freedoms.php
wordpress/wp-admin/options-reading.php
wordpress/wp-admin/press-this.php
wordpress/readme.html
[root@ecs-wordpress ~]#
```

Figure 1-30

Step 8 Create a **wp-config.php** file.

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



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

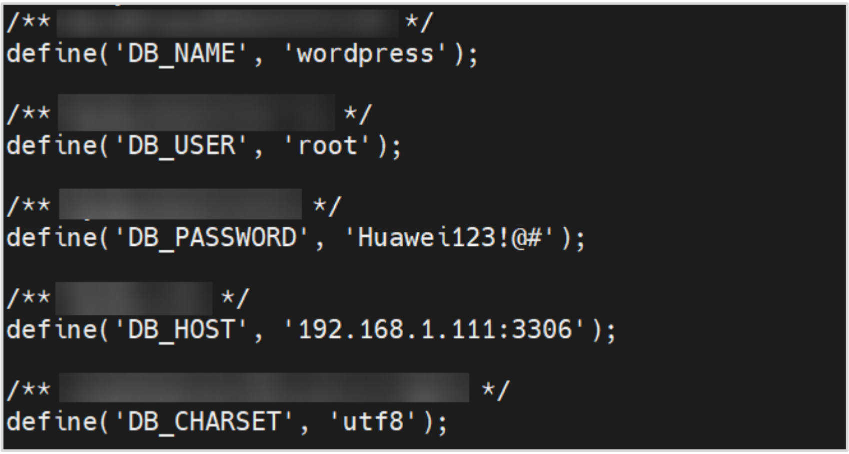
Figure 1-31

Step 9 Configure database parameters in the **wp-config.php** file to interconnect with the **wordpress** database.

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

Configure database parameters as follows:

- DB_NAME: **wordpress**
- DB_USER: **root**
- DB_PASSWORD: user-defined
- DB_HOST: *Private IP address of the RDS instance*:*Port number* (3306 by default)

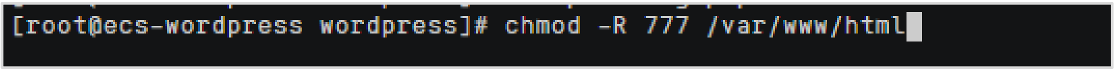


```
/** [redacted] */
define('DB_NAME', 'wordpress');

/** [redacted] */
define('DB_USER', 'root');

/** [redacted] */
define('DB_PASSWORD', 'Huawei123!@#');

/** [redacted] */
define('DB_HOST', '192.168.1.111:3306');

/** [redacted] */
define('DB_CHARSET', 'utf8');
```

Figure 1-32

Step 10 Grant read and write permissions to the directory where the package is decompressed.

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



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

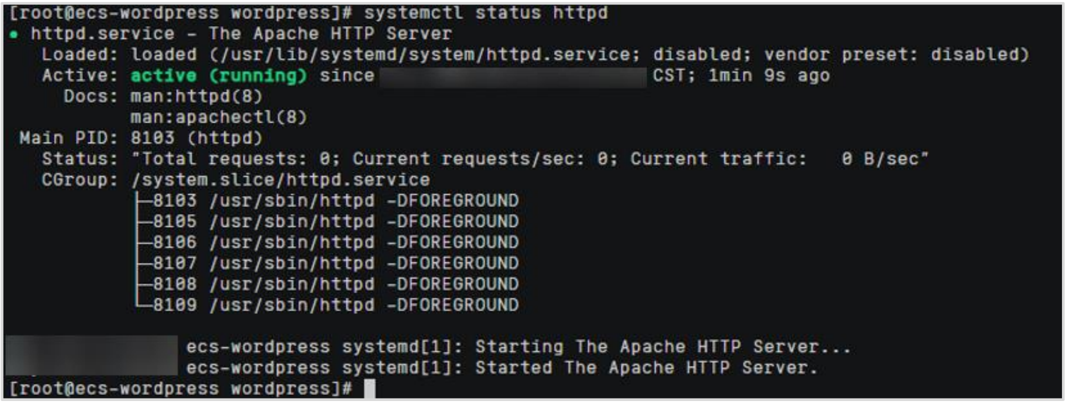
Figure 1-33

Step 11 Enable httpd and php-fpm.

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

Step 12 Check the httpd service status. The status **active (running)** indicates that the httpd service has been enabled.

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

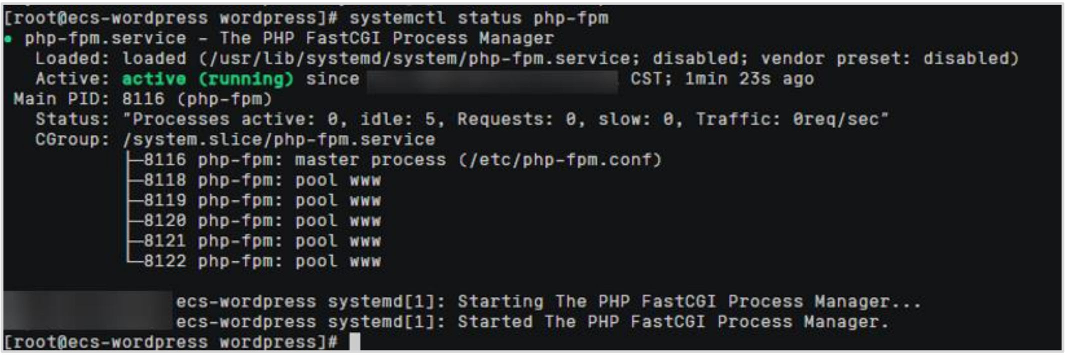


```
[root@ecs-wordpress wordpress]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since [redacted] CST; 1min 9s ago
     Docs: man:httpd(8)
           man:apachectl(8)
 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...
           ecs-wordpress systemd[1]: Started The Apache HTTP Server.
[root@ecs-wordpress wordpress]#
```

Figure 1-34

Step 13 Check the php-fpm service status. The status **active (running)** indicates that the php-fpm service has been enabled.

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

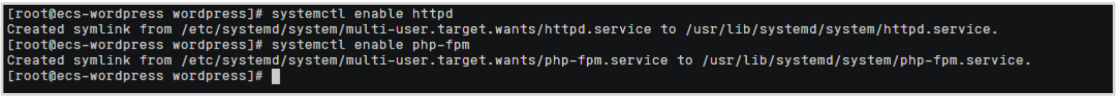


```
[root@ecs-wordpress wordpress]# systemctl status php-fpm
● php-fpm.service - The PHP FastCGI Process Manager
   Loaded: loaded (/usr/lib/systemd/system/php-fpm.service; disabled; vendor preset: disabled)
   Active: active (running) since [redacted] CST; 1min 23s ago
 Main PID: 8116 (php-fpm)
   Status: "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]#
```

Figure 1-35

Step 14 Set httpd and php-fpm to automatically start upon system startup.

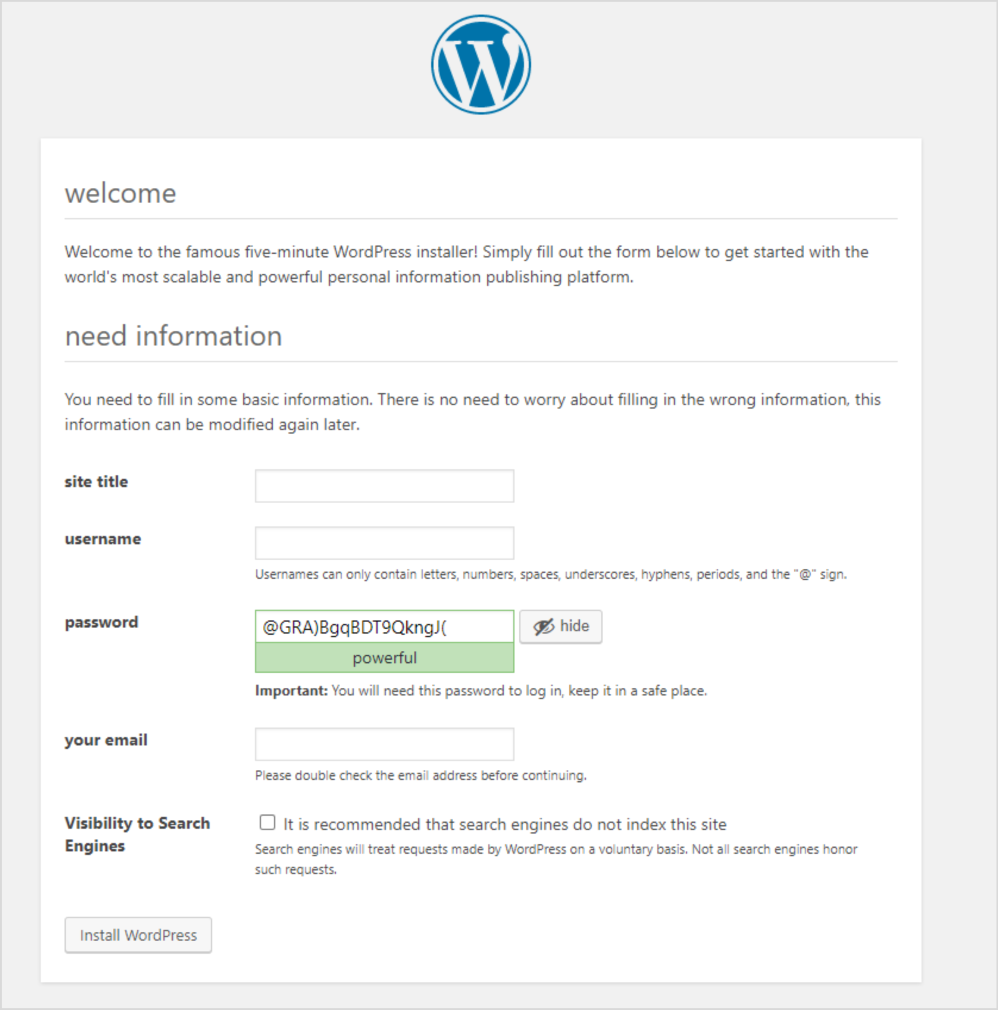
```
[root@ecs-wordpress wordpress]# systemctl enable httpd
[root@ecs-wordpress wordpress]# systemctl enable php-fpm
```



```
[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]#
```

Figure 1-36

Step 15 Open a browser and enter **http://*External IP address of ECS-WordPress*/wordpress/index.php** in the address bar (in this exercise, enter **http://119.3.199.107/wordpress/index.php**). If the information shown in the following figure is displayed, the ECS is successfully interconnected with the database.



welcome

Welcome to the famous five-minute WordPress installer! Simply fill out the form below to get started with the world's most scalable and powerful personal information publishing platform.

need information

You need to fill in some basic information. There is no need to worry about filling in the wrong information, this information can be modified again later.

site title

username

Usernames can only contain letters, numbers, spaces, underscores, hyphens, periods, and the "@" sign.

password: @GRA)BgqBDT9QkngJ(hide

powerful

Important: You will need this password to log in, keep it in a safe place.

your email

Please double check the email address before continuing.

Visibility to Search Engines: □ It is recommended that search engines do not index this site

Search engines will treat requests made by WordPress on a voluntary basis. Not all search engines honor such requests.

Install WordPress

Figure 1-37

1.2.5 Creating an Image and Applying for an ECS

Step 1 Select **Image Management Service** from the service list.

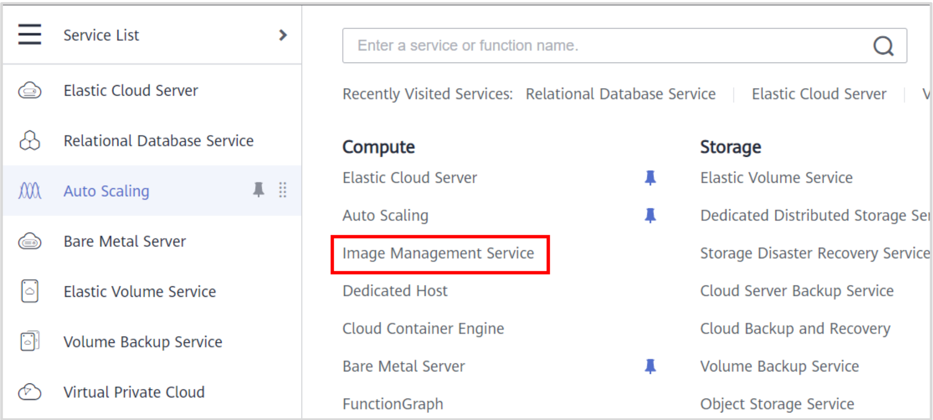


Figure 1-38

Step 2 In the upper right corner, click **Create Image**.

This image will be used by Auto Scaling to provision ECSs.

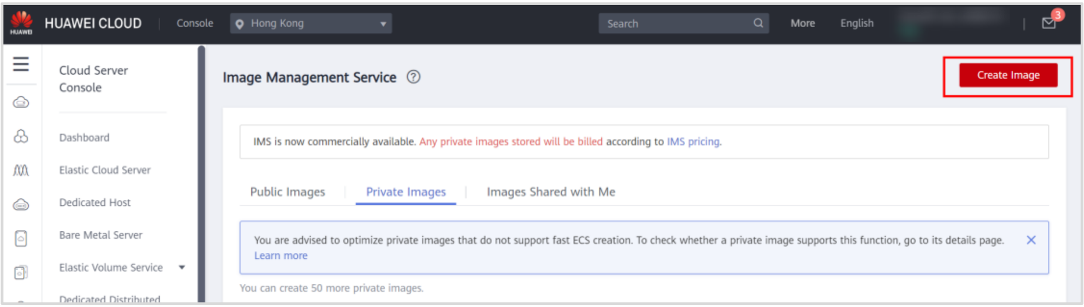


Image Management Service

IMS is now commercially available. Any private images stored will be billed according to IMS pricing.

You are advised to optimize private images that do not support fast ECS creation. To check whether a private image supports this function, go to its details page. Learn more

You can create 50 more private images.

Figure 1-39

Step 3 Configure the following parameters and click **Next**.

- **Region**: **CN-Hong Kong** (The **CN-Hong Kong** region is used as an example in this exercise.)
- **Type**: **System Disk Image**
- **Source**: **ECS** (Select **ecs-wordpress** you created.)
- **Name**: **wordpress**

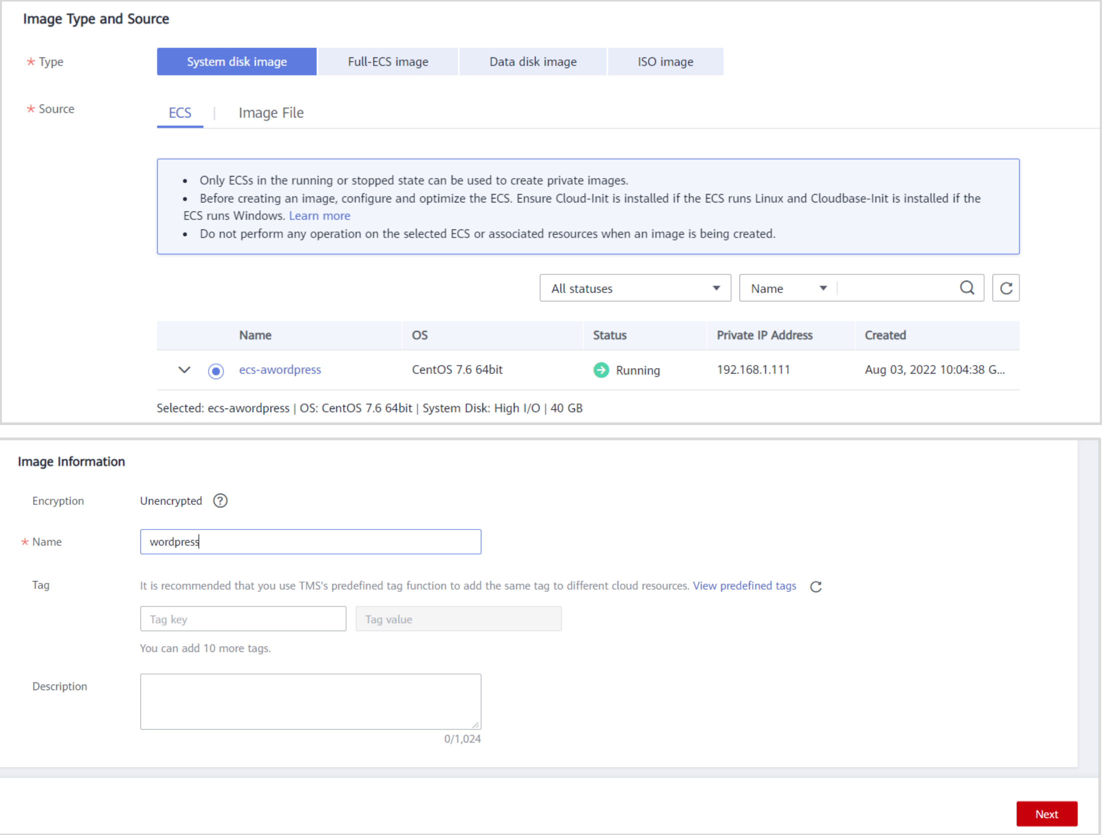


Image Type and Source

* Type: System disk image

* Source: ECS

- Only ECSs in the running or stopped state can be used to create private images.
- Before creating an image, configure and optimize the ECS. Ensure Cloud-Init is installed if the ECS runs Linux and Cloudbase-Init is installed if the ECS runs Windows. Learn more
- Do not perform any operation on the selected ECS or associated resources when an image is being created.

Name	OS	Status	Private IP Address	Created
● ecs-awordpress	CentOS 7.6 64bit	Running	192.168.1.111	Aug 03, 2022 10:04:38 G...

Selected: ecs-awordpress | OS: CentOS 7.6 64bit | System Disk: High I/O | 40 GB

Image Information

Encryption: Unencrypted

* Name: wordpress

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

Tag key | Tag value

You can add 10 more tags.

Description:

0/1,024

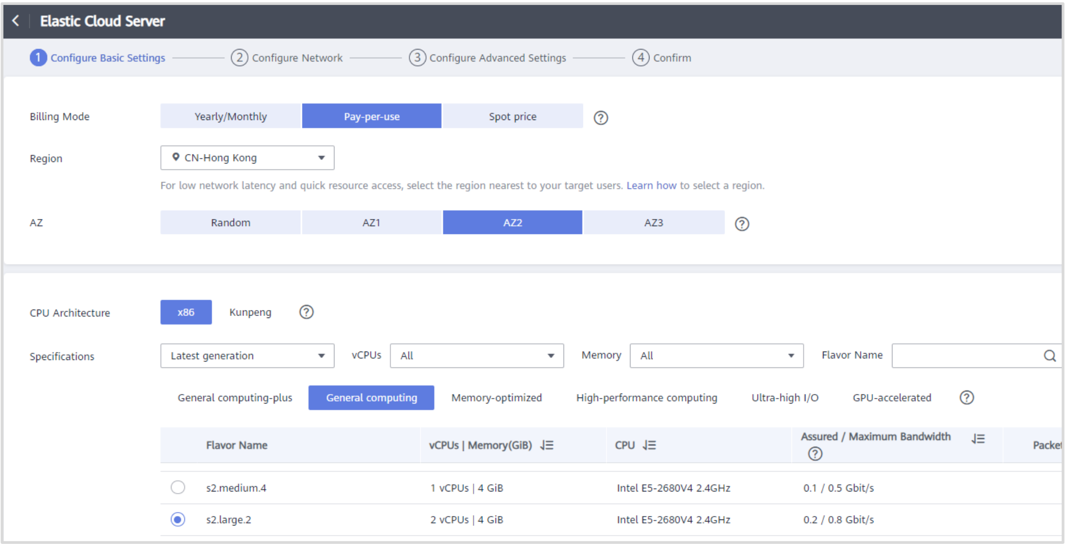
Figure 1-40

Step 4 Locate **wordpress** in the image list and click **Apply for Server** in the **Operation** column.

The ECSs created here and **ecs-wordpress** created previously will be added to a backend server group of Elastic Load Balance (ELB).

Step 5 Configure the following parameters to apply for ECSs.

- **Billing Mode: Pay-per-use**
- **Region: CN-Hong Kong** (The **CN-Hong Kong** region is used as an example in this exercise.)
- **AZ: AZ 2** (**AZ 2** is used as an example in this exercise.)
- **CPU Architecture: x86**
- **Specifications: 2 vCPUs | 4 GiB**
- **Image: Private image | wordpress**
- **Network: vpc-1 | vpc-1-subnet | Automatically assign IP address**
- **Security Group: sg-web**
- **EIP: Not required**
- **System Disk: High I/O | 40 GiB**
- **ECS Name: ecs-awordpress**
- **Password**: Set a password (or use the image password).



Elastic Cloud Server

1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

Billing Mode: Yearly/Monthly | **Pay-per-use** | Spot price

Region: CN-Hong Kong

For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

AZ: Random | AZ1 | **AZ2** | AZ3

CPU Architecture: **x86** | Kunpeng

Specifications: Latest generation | vCPUs: All | Memory: All | Flavor Name

General computing-plus | **General computing** | Memory-optimized | High-performance computing | Ultra-high I/O | GPU-accelerated

	Flavor Name	vCPUs | Memory(GiB)	CPU	Assured / Maximum Bandwidth	Packe
○	s2.medium.4	1 vCPUs | 4 GiB	Intel E5-2680V4 2.4GHz	0.1 / 0.5 Gbit/s	
●	s2.large.2	2 vCPUs | 4 GiB	Intel E5-2680V4 2.4GHz	0.2 / 0.8 Gbit/s	

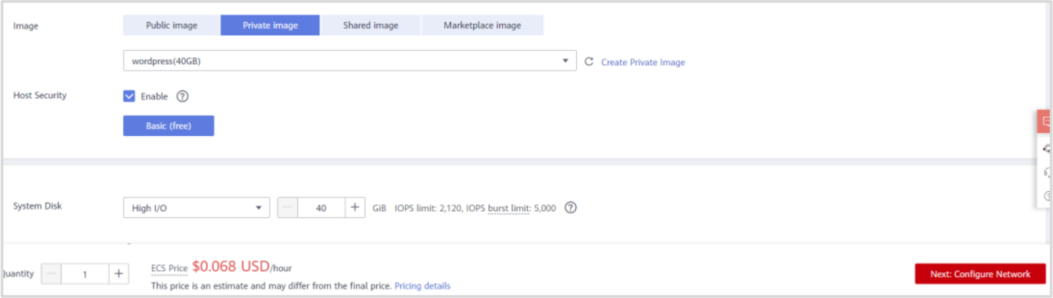


Image: Public image | **Private image** | Shared image | Marketplace image

wordpress(40GB) — Create Private Image

Host Security: ☑ Enable — Basic (free)

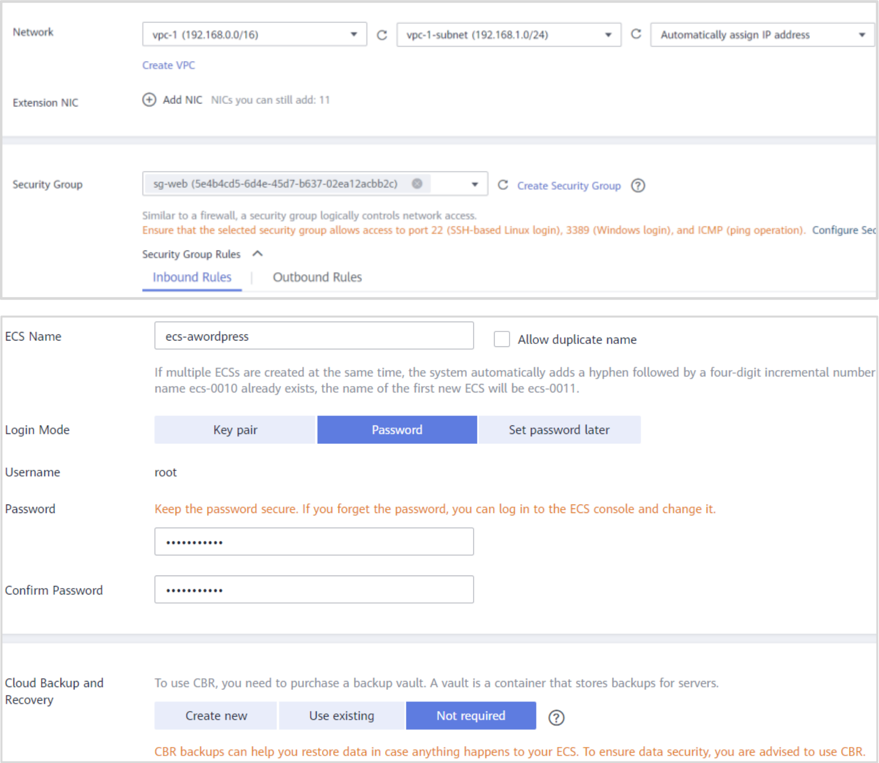
System Disk: High I/O | 40 GiB IOPS limit: 2,120, IOPS burst limit: 5,000

Quantity: 1

ECS Price $0.068 USD/hour

This price is an estimate and may differ from the final price. Pricing details

Next: Configure Network



Network: vpc-1 (192.168.0.0/16) | vpc-1-subnet (192.168.1.0/24) | Automatically assign IP address

Create VPC

Extension NIC: Add NIC NICs you can still add: 11

Security Group: sg-web (5e4b4cd5-6d4e-45d7-b637-02ea12acbb2c) Create Security Group

Similar to a firewall, a security group logically controls network access.
Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Sec

Security Group Rules
Inbound Rules | Outbound Rules

ECS Name: ecs-awordpress □ Allow duplicate name

If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a four-digit incremental number name ecs-0010 already exists, the name of the first new ECS will be ecs-0011.

Login Mode: Key pair | **Password** | Set password later

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.
•••••••••••

Confirm Password: •••••••••••

Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.
Create new | Use existing | **Not required**

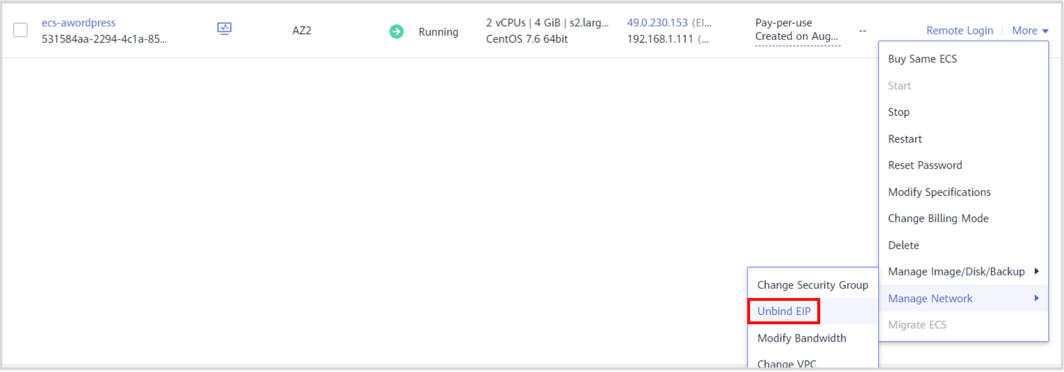
CBR backups can help you restore data in case anything happens to your ECS. To ensure data security, you are advised to use CBR.

Figure 1-41

1.2.6 Buying Load Balancers

Step 1 Unbind the EIP from the ECS **ecs-wordpress**.

Note: The EIP will be bound to the load balancer in the follow-up exercise.



ecs-awordpress 531584aa-2294-4c1a-85...	AZ2	Running	2 vCPUs | 4 GiB | s2.larg... CentOS 7.6 64bit	49.0.230.153 (EI... 192.168.1.111 (...	Pay-per-use Created on Aug...	--	Remote Login	More

Figure 1-42

Step 2 In the service list, choose **Networking** > **Elastic Load Balance**.

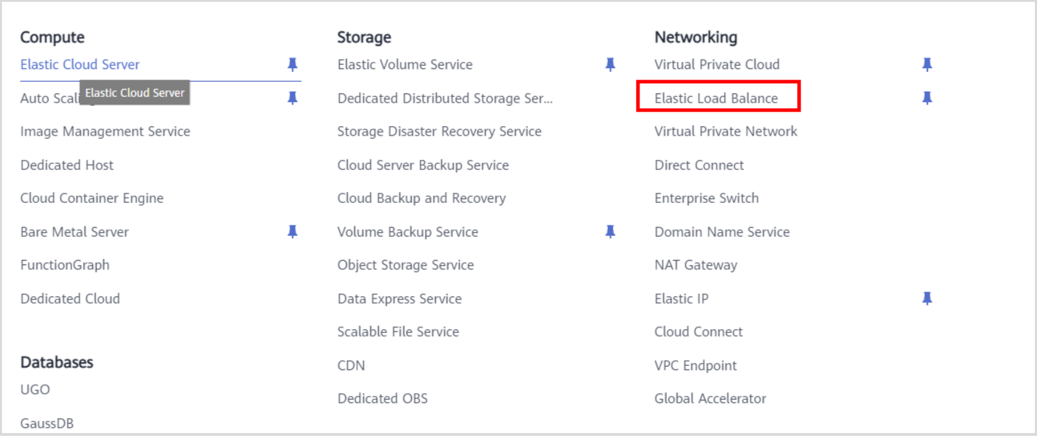
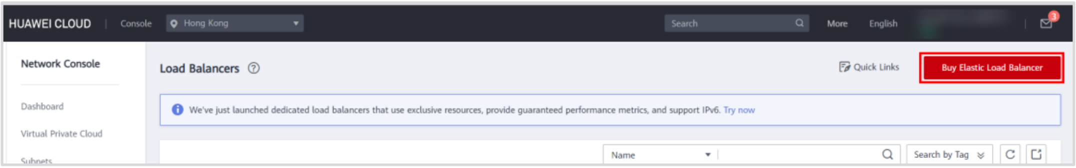


Figure 1-43

Step 3 Click **Buy Elastic Load Balancer** in the upper right corner.

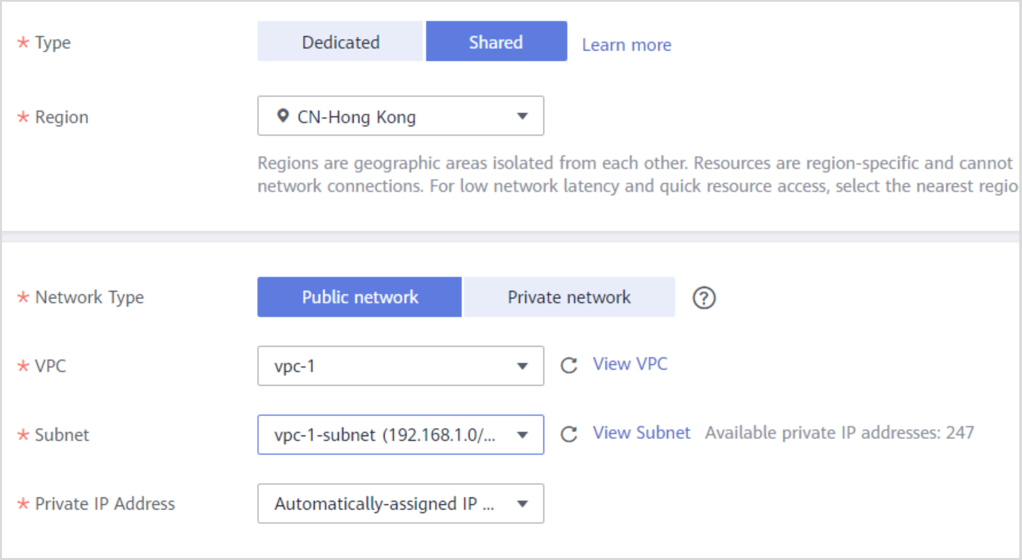


We've just launched dedicated load balancers that use exclusive resources, provide guaranteed performance metrics, and support IPv6. Try now

Figure 1-44

Step 4 Configure the parameters as follows:

- Type: Shared
- Region: CN-Hong Kong (The **CN-Hong Kong** region is used as an example in this exercise.)
- Network Type: Public network
- VPC: vpc-1
- Subnet: vpc-1-subnet
- Private IP Address: Automatically-assigned IP address



* Type: Shared

* Region: CN-Hong Kong

Regions are geographic areas isolated from each other. Resources are region-specific and cannot network connections. For low network latency and quick resource access, select the nearest regio

* Network Type: Public network

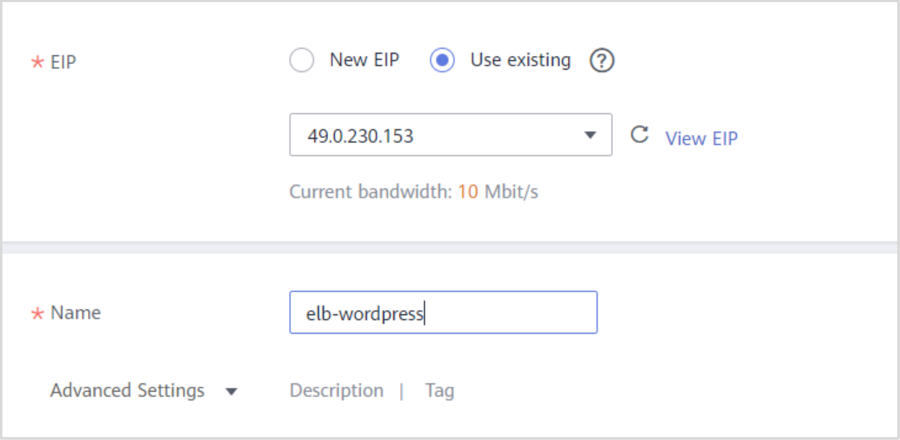
* VPC: vpc-1

* Subnet: vpc-1-subnet (192.168.1.0/... Available private IP addresses: 247

* Private IP Address: Automatically-assigned IP ...

Figure 1-45

- **EIP**: **Use existing** (Assign the above unbound EIP to this load balancer.)
- **Name: elb-wordpress**



* EIP ○ New EIP ● Use existing ?

49.0.230.153 ▾ View EIP

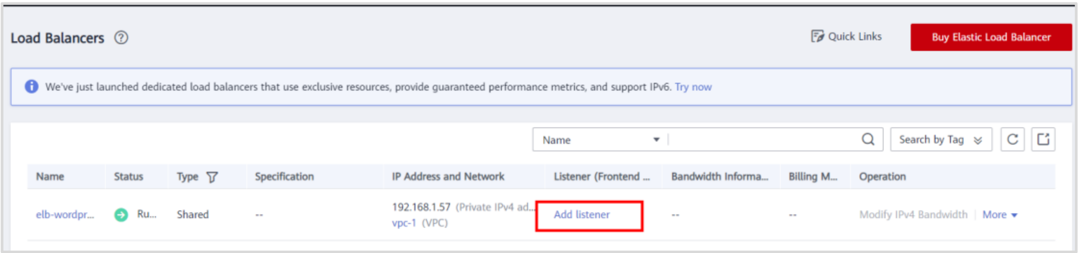
Current bandwidth: 10 Mbit/s

* Name: elb-wordpress

Advanced Settings ▾ Description | Tag

Figure 1-46

Step 5 Locate the **elb-wordpress** in the load balancer list and click **Add listener**.



Load Balancers ? Quick Links Buy Elastic Load Balancer

We've just launched dedicated load balancers that use exclusive resources, provide guaranteed performance metrics, and support IPv6. Try now

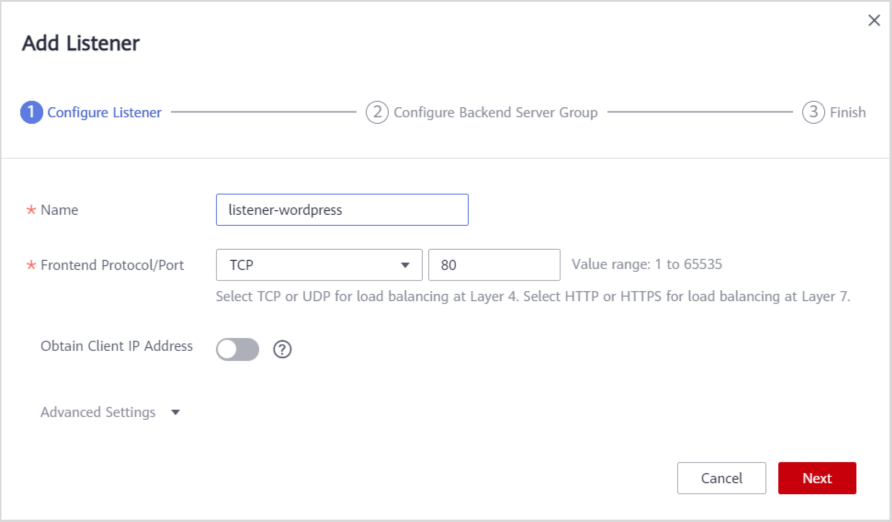
Name ▾ Search by Tag

Name	Status	Type	Specification	IP Address and Network	Listener (Frontend ...	Bandwidth Informa...	Billing M...	Operation
elb-wordpr...	Ru...	Shared	--	192.168.1.57 (Private IPv4 ad... vpc-1 (VPC)	Add listener	--	--	Modify IPv4 Bandwidth | More ▾

Figure 1-47

Step 6 Configure the parameters as follows:

- **Name: listener-wordpress**
- **Frontend Protocol: TCP**
- **Frontend Port: 80** (Used by this load balancer to receive requests from clients.)



Add Listener

1 Configure Listener — 2 Configure Backend Server Group — 3 Finish

* Name: listener-wordpress

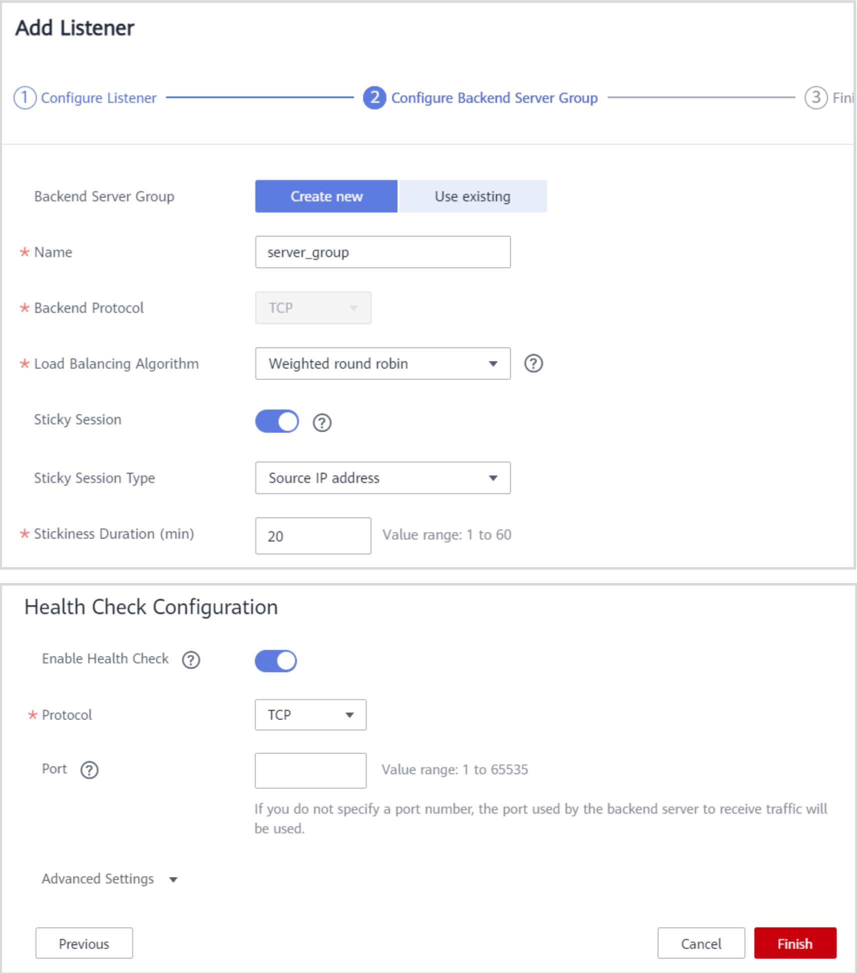
* Frontend Protocol/Port: TCP 80 Value range: 1 to 65535

Select TCP or UDP for load balancing at Layer 4. Select HTTP or HTTPS for load balancing at Layer 7.

Obtain Client IP Address: ○

Figure 1-48

- Enable **Sticky Session** to ensure that requests from a client always are routed to the same server before a session ends. Use the default values for other parameters and click **Next: Add Backend Server**.



Add Listener

1 Configure Listener — 2 Configure Backend Server Group — 3 Fini

Backend Server Group: Create new | Use existing

* Name: server_group

* Backend Protocol: TCP

* Load Balancing Algorithm: Weighted round robin

Sticky Session: ●

Sticky Session Type: Source IP address

* Stickiness Duration (min): 20 Value range: 1 to 60

Health Check Configuration

Enable Health Check: ●

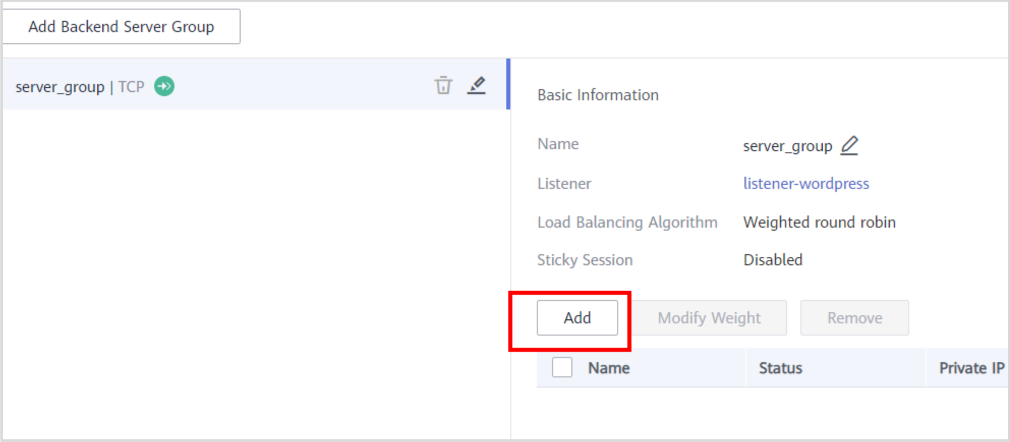
* Protocol: TCP

Port: Value range: 1 to 65535

If you do not specify a port number, the port used by the backend server to receive traffic will be used.

Figure 1-49

- Click **Add**.



Add Backend Server Group

server_group | TCP

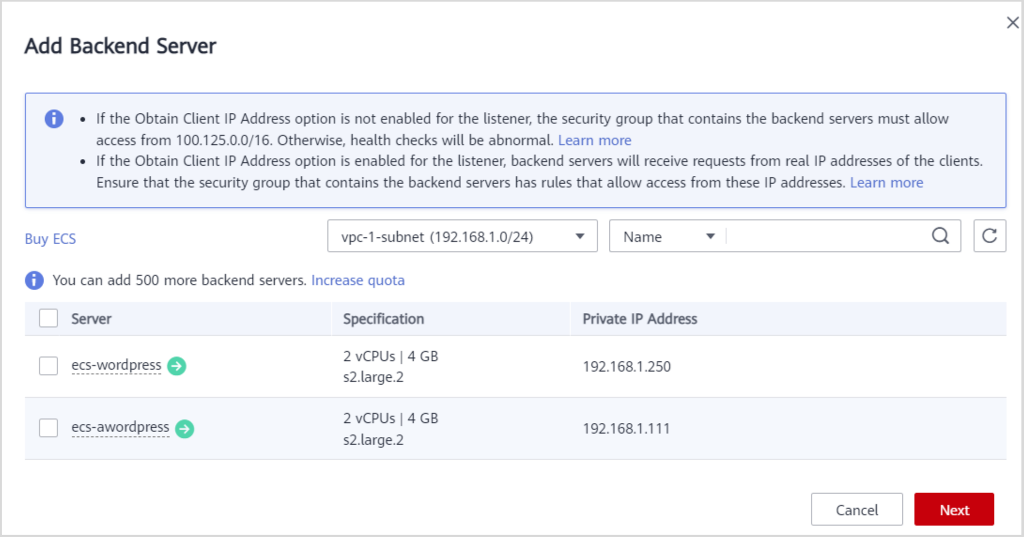
Basic Information

Name	server_group
Listener	listener-wordpress
Load Balancing Algorithm	Weighted round robin
Sticky Session	Disabled

Add | Modify Weight | Remove

□ Name	Status	Private IP

- Select ECS **ecs-wordpress** and the ECS **ecs-wordpress-0001** created using the image.



Add Backend Server

- If the Obtain Client IP Address option is not enabled for the listener, the security group that contains the backend servers must allow access from 100.125.0.0/16. Otherwise, health checks will be abnormal. Learn more
- If the Obtain Client IP Address option is enabled for the listener, backend servers will receive requests from real IP addresses of the clients. Ensure that the security group that contains the backend servers has rules that allow access from these IP addresses. Learn more

Buy ECS | vpc-1-subnet (192.168.1.0/24) | Name

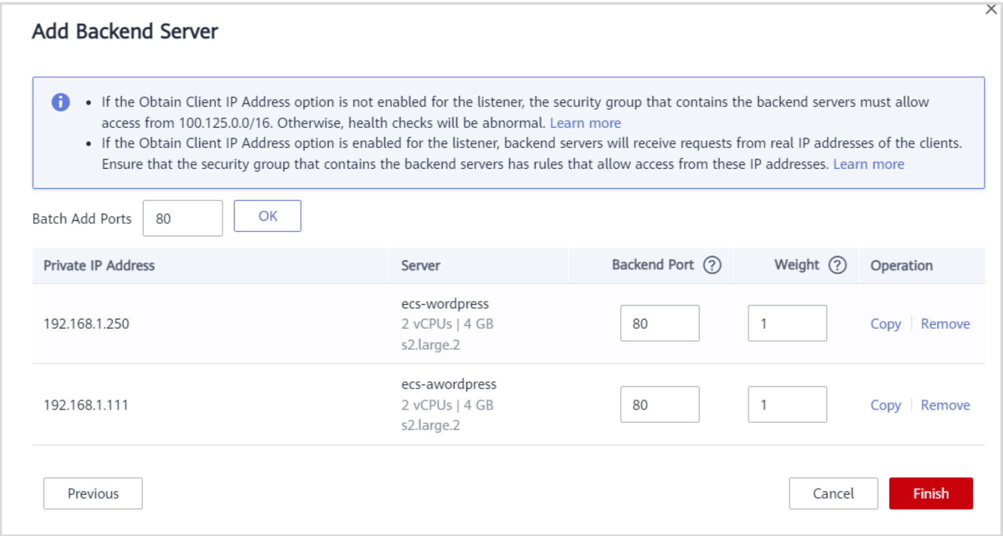
You can add 500 more backend servers. Increase quota

□ Server	Specification	Private IP Address
□ ecs-wordpress	2 vCPUs | 4 GB s2.large.2	192.168.1.250
□ ecs-awordpress	2 vCPUs | 4 GB s2.large.2	192.168.1.111

Cancel | Next

Figure 1-50

- Set **Batch Add Ports** to **80** (used by backend servers to receive requests from this load balancer). Use the default values for other parameters, and click **Finish**.



Add Backend Server

- If the Obtain Client IP Address option is not enabled for the listener, the security group that contains the backend servers must allow access from 100.125.0.0/16. Otherwise, health checks will be abnormal. Learn more
- If the Obtain Client IP Address option is enabled for the listener, backend servers will receive requests from real IP addresses of the clients. Ensure that the security group that contains the backend servers has rules that allow access from these IP addresses. Learn more

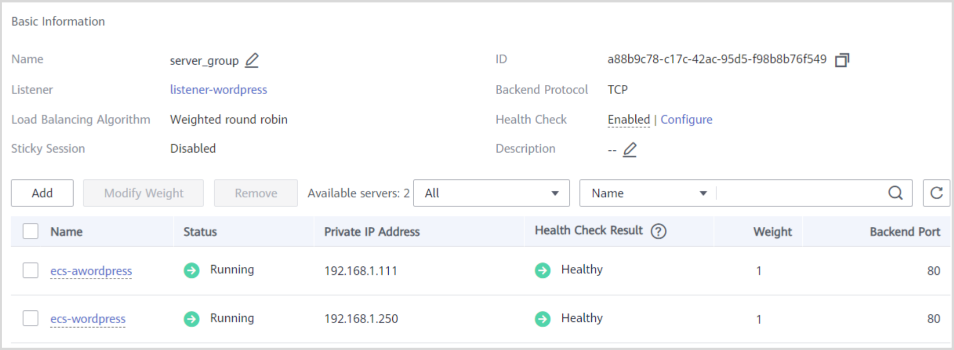
Batch Add Ports 80 OK

Private IP Address	Server	Backend Port	Weight	Operation
192.168.1.250	ecs-wordpress 2 vCPUs | 4 GB s2.large.2	80	1	Copy | Remove
192.168.1.111	ecs-awordpress 2 vCPUs | 4 GB s2.large.2	80	1	Copy | Remove

Previous | Cancel | Finish

Figure 1-51

- After the load balancer is created, choose **Listeners** > **Backend Server Groups** to ensure the health check result is **Healthy**.



Basic Information

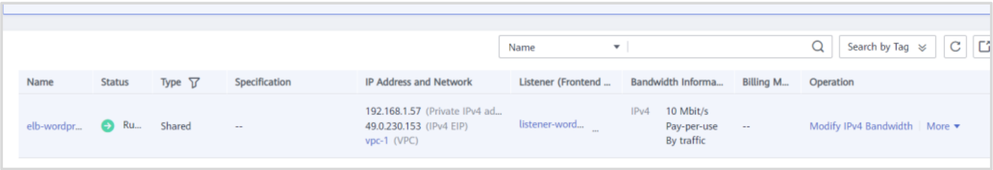
Name	server_group	ID	a88b9c78-c17c-42ac-95d5-f98b8b76f549
Listener	listener-wordpress	Backend Protocol	TCP
Load Balancing Algorithm	Weighted round robin	Health Check	Enabled | Configure
Sticky Session	Disabled	Description	--

Available servers: 2 All Name

Name	Status	Private IP Address	Health Check Result	Weight	Backend Port
ecs-awordpress	Running	192.168.1.111	Healthy	1	80
ecs-wordpress	Running	192.168.1.250	Healthy	1	80

Figure 1-52

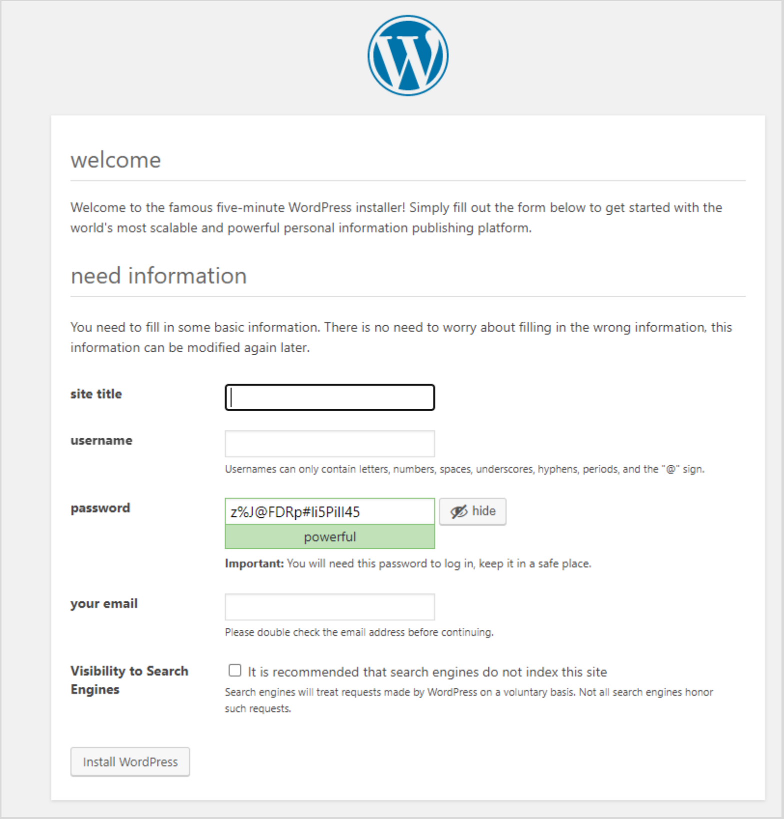
- View the created load balancer on the load balancer page.



Name	Status	Type	Specification	IP Address and Network	Listener (Frontend ...	Bandwidth Informa...	Billing M...	Operation
elb-wordpr...	Ru...	Shared	--	192.168.1.57 (Private IPv4 ad... 49.0.230.153 (IPv4 EIP) vpc-1 (VPC)	listener-word... ...	IPv4 10 Mbit/s Pay-per-use By traffic	--	Modify IPv4 Bandwidth | More

Figure 1-53

Step 7 Log in to http://119.3.199.107 (EIP bound to this load balancer) /wordpress/index.php again. If the following information is displayed, the load balancer is successfully deployed.



welcome

Welcome to the famous five-minute WordPress installer! Simply fill out the form below to get started with the world's most scalable and powerful personal information publishing platform.

need information

You need to fill in some basic information. There is no need to worry about filling in the wrong information, this information can be modified again later.

site title

username

Usernames can only contain letters, numbers, spaces, underscores, hyphens, periods, and the "@" sign.

password z%J@FDRp#li5Pill45 hide

powerful

Important: You will need this password to log in, keep it in a safe place.

your email

Please double check the email address before continuing.

Visibility to Search Engines ☐ It is recommended that search engines do not index this site

Search engines will treat requests made by WordPress on a voluntary basis. Not all search engines honor such requests.

Figure 1-54

1.2.7 Creating an AS Group

Step 1 In the service list, choose **Data Encryption Workshop** under **Security & Compliance**.

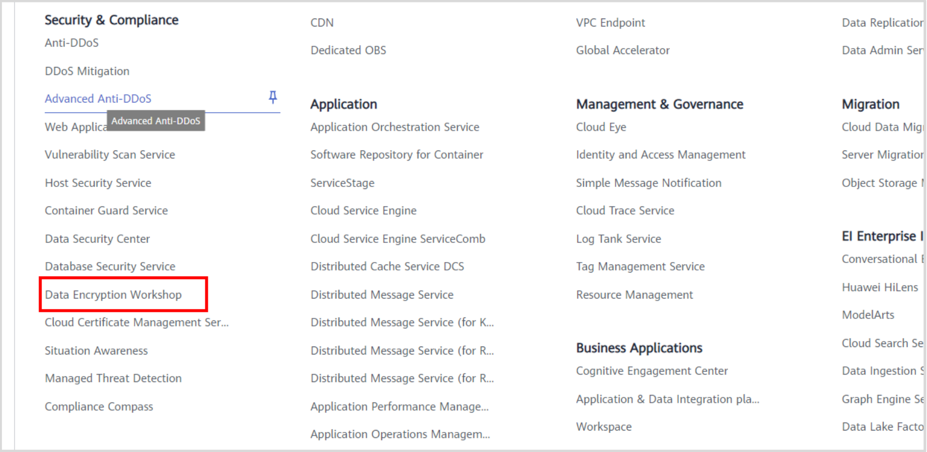
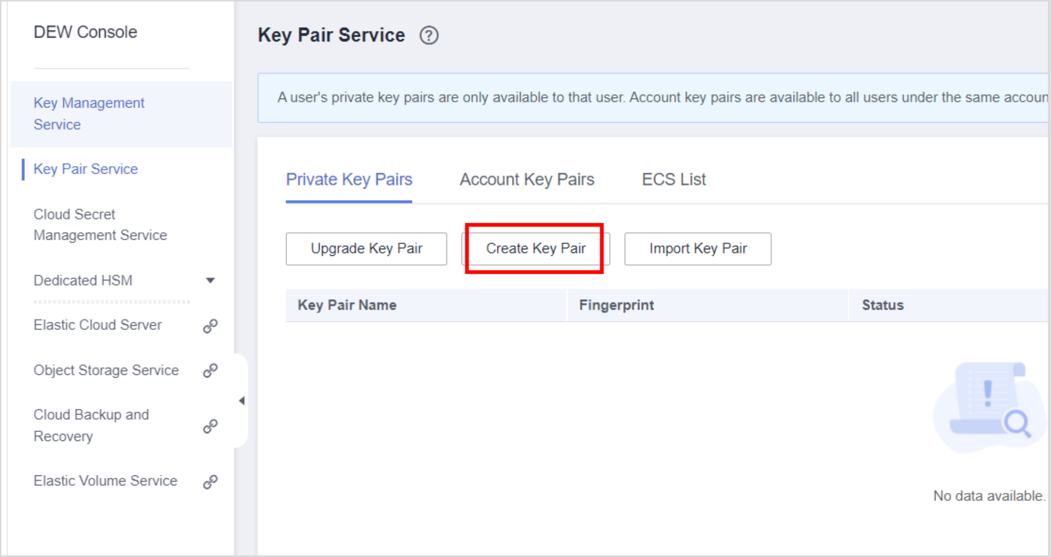


Figure 1-55

Step 2 Choose **Key Pair Service** in the left navigation pane and click **Create Key Pair**.



A user's private key pairs are only available to that user. Account key pairs are available to all users under the same accoun

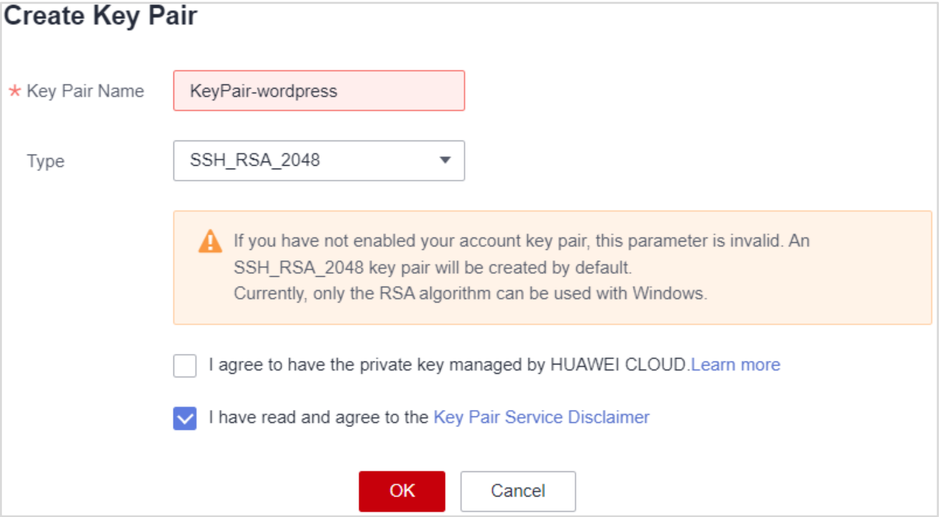
Key Pair Name	Fingerprint	Status

No data available.

Figure 1-56

Set **Key Pair Name to KeyPair-wordpress** and click **OK**.

Note: In this exercise, the key pair is used to create an AS group only.



Create Key Pair

* Key Pair Name: KeyPair-wordpress

Type: SSH_RSA_2048

If you have not enabled your account key pair, this parameter is invalid. An SSH_RSA_2048 key pair will be created by default.
Currently, only the RSA algorithm can be used with Windows.

□ I agree to have the private key managed by HUAWEI CLOUD.Learn more

☑ I have read and agree to the Key Pair Service Disclaimer

Figure 1-57

Step 3 In the service list, choose **Auto Scaling** under **Compute**.

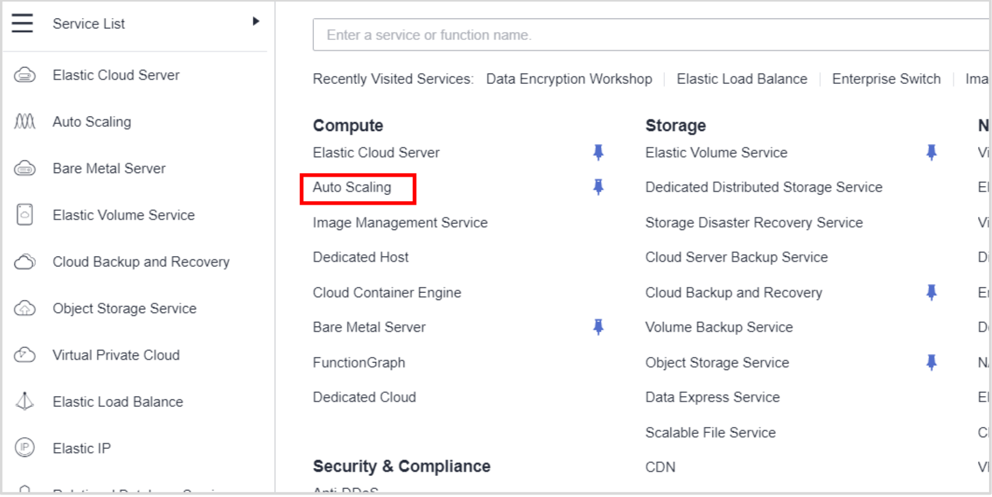
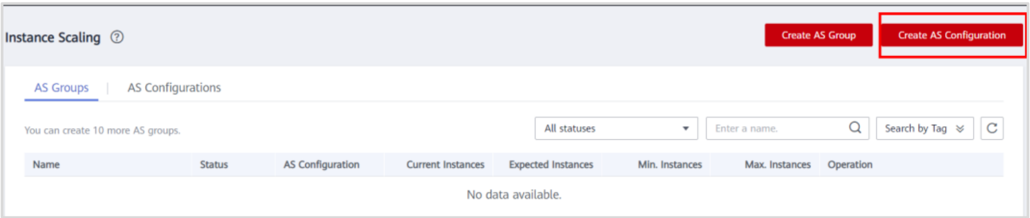


Figure 1-58

Step 4 Click **Create AS Configuration** in the upper right corner.



You can create 10 more AS groups.

Name	Status	AS Configuration	Current Instances	Expected Instances	Min. Instances	Max. Instances	Operation

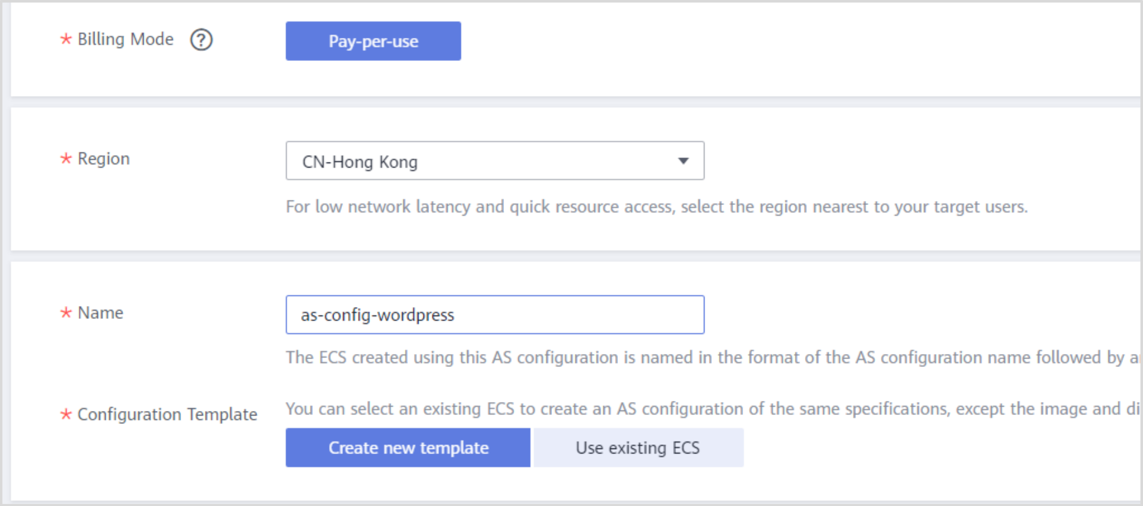
No data available.

Figure 1-59

Step 5 Configure the parameters as follows:

- **Billing Mode**: **Pay-per-use**
- **Region**: **CN-Hong Kong** (The **CN-Hong Kong** region is used as an example in this exercise.)

- Name: as-config-wordpress
- Configuration Template: Create new template



* Billing Mode: Pay-per-use

* Region: CN-Hong Kong

For low network latency and quick resource access, select the region nearest to your target users.

* Name: as-config-wordpress

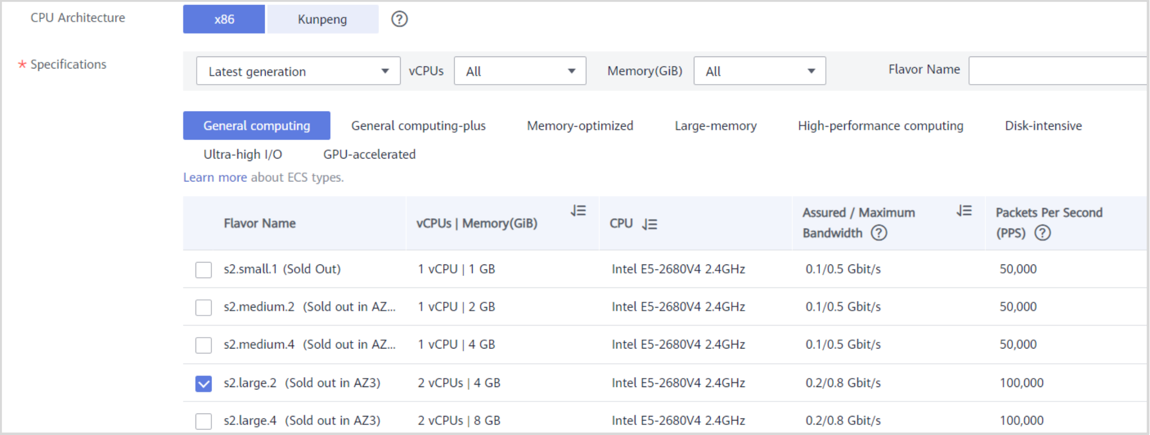
The ECS created using this AS configuration is named in the format of the AS configuration name followed by a

* Configuration Template

You can select an existing ECS to create an AS configuration of the same specifications, except the image and di

Figure 1-60

- Specifications: 2 vCPUs | 4 GiB
- Image: Private image | wordpress
- Disk: EVS | High I/O | 40 GB
- Security Group: sg-web
- EIP: Do not use

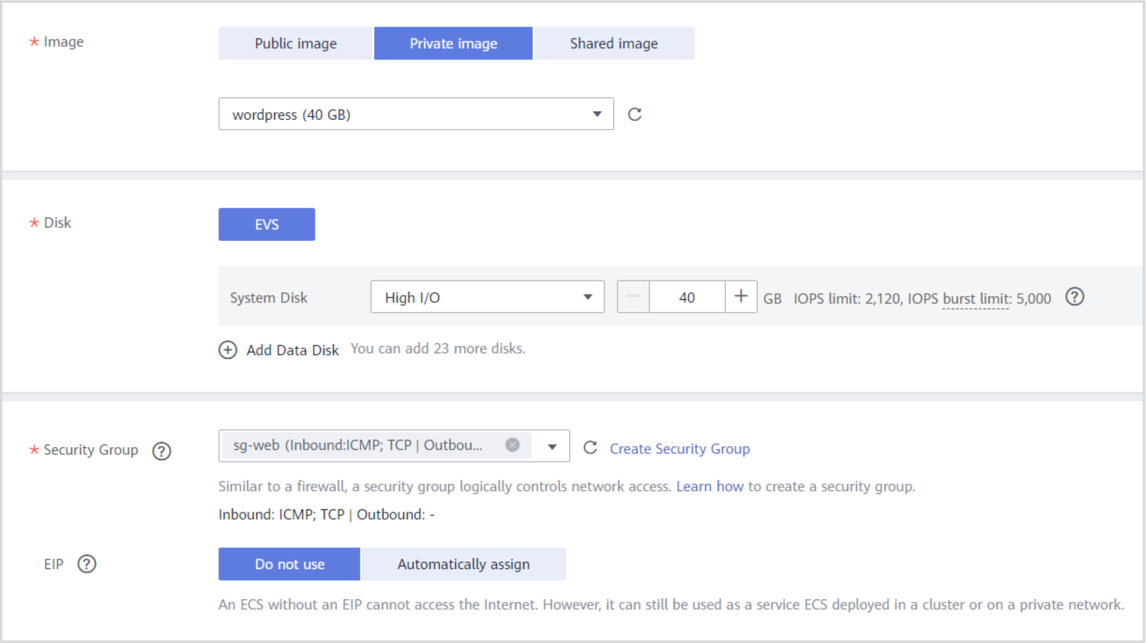


CPU Architecture: x86

* Specifications

Latest generation | vCPUs: All | Memory(GiB): All | Flavor Name:

	Flavor Name	vCPUs | Memory(GiB)	CPU	Assured / Maximum Bandwidth	Packets Per Second (PPS)
☐	s2.small.1 (Sold Out)	1 vCPU | 1 GB	Intel E5-2680V4 2.4GHz	0.1/0.5 Gbit/s	50,000
☐	s2.medium.2 (Sold out in AZ...	1 vCPU | 2 GB	Intel E5-2680V4 2.4GHz	0.1/0.5 Gbit/s	50,000
☐	s2.medium.4 (Sold out in AZ...	1 vCPU | 4 GB	Intel E5-2680V4 2.4GHz	0.1/0.5 Gbit/s	50,000
☑	s2.large.2 (Sold out in AZ3)	2 vCPUs | 4 GB	Intel E5-2680V4 2.4GHz	0.2/0.8 Gbit/s	100,000
☐	s2.large.4 (Sold out in AZ3)	2 vCPUs | 8 GB	Intel E5-2680V4 2.4GHz	0.2/0.8 Gbit/s	100,000



* Image: Public image | **Private image** | Shared image

wordpress (40 GB)

* Disk: **EVS**

System Disk: High I/O — 40 + GB IOPS limit: 2,120, IOPS burst limit: 5,000

Add Data Disk You can add 23 more disks.

* Security Group: sg-web (Inbound:ICMP; TCP | Outbou... Create Security Group

Similar to a firewall, a security group logically controls network access. Learn how to create a security group.

Inbound: ICMP; TCP | Outbound: -

EIP: **Do not use** | Automatically assign

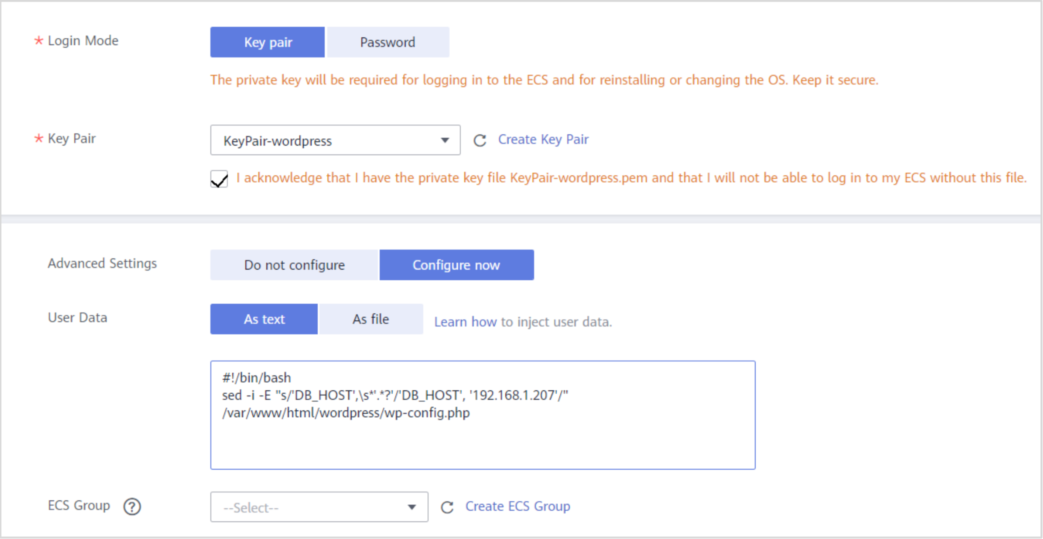
An ECS without an EIP cannot access the Internet. However, it can still be used as a service ECS deployed in a cluster or on a private network.

Figure 1-61

- Select **Key Pair** for **Login Mode** and select the key pair you created from the drop-down list. Select **Configure now** for **Advanced Settings**, leave **User Data** to **As text**, and copy the following content to the box to modify the database address in the **wp-config.php** file in the selected image. (In this exercise, the IP address following **DB_HOST** is changed from **192.168.1.137** to **192.168.1.207**.)

```
#!/bin/bash
sed -i -E "s/'DB_HOST',\s*'.*?'/'DB_HOST', '192.168.1.207'/" /var/www/html/wordpress/wp-config.php
```

Note: 192.168.1.207 is the private IP address of the backend database in this lab. Replace it with the actual IP address.



* Login Mode: **Key pair** | Password

The private key will be required for logging in to the ECS and for reinstalling or changing the OS. Keep it secure.

* Key Pair: KeyPair-wordpress Create Key Pair

☑ I acknowledge that I have the private key file KeyPair-wordpress.pem and that I will not be able to log in to my ECS without this file.

Advanced Settings: Do not configure | **Configure now**

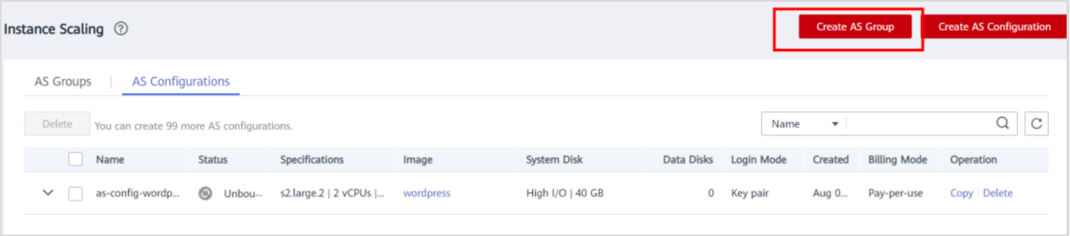
User Data: **As text** | As file Learn how to inject user data.

```
#!/bin/bash
sed -i -E "s/'DB_HOST',\s*'.*?'/'DB_HOST', '192.168.1.207'/"
/var/www/html/wordpress/wp-config.php
```

ECS Group: --Select-- Create ECS Group

Figure 1-62

Step 6 After the AS configuration is created, click **Create AS Group** in the upper right corner.



Instance Scaling ?

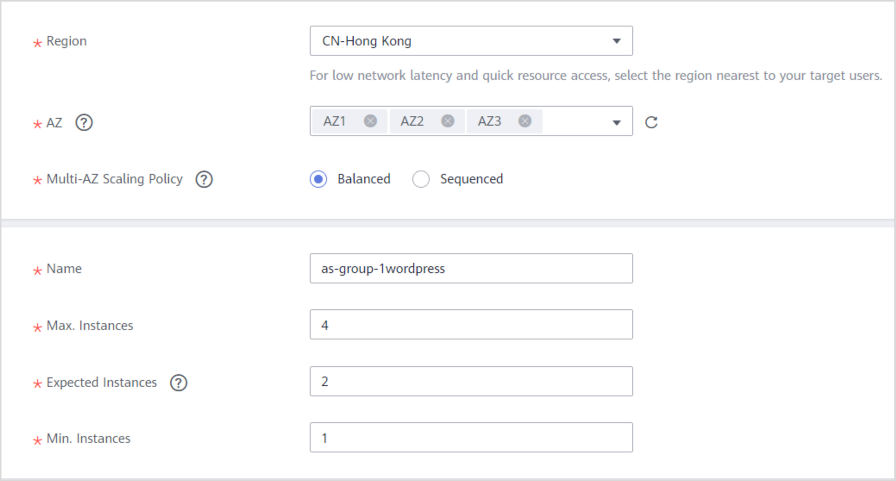
You can create 99 more AS configurations.

	Name	Status	Specifications	Image	System Disk	Data Disks	Login Mode	Created	Billing Mode	Operation
□	as-config-wordp...	Unbou...	s2.large.2 | 2 vCPUs |...	wordpress	High I/O | 40 GB	0	Key pair	Aug 0...	Pay-per-use	Copy | Delete

Figure 1-63

Step 7 Configure the parameters as follows:

- **Region**: **CN-Hong Kong** (The **CN-Hong Kong** region is used as an example in this exercise.)
- **AZ**: Retain the default setting.
- **Multi-AZ Scaling Policy**: **Balanced**
- **Name**: **as-config-wordpress**
- **Max. Instances**: **4**
- **Expected Instances**: **2** (Considering the lab environment capacity, you are advised to set the expected number of instances to 2 in this exercise.)
- **Min. Instances**: **1**
- **AS Configuration**: **as-config-wordpress**
- **VPC**: **vpc-1**
- **Subnet**: **vpc-1-subnet**
- **Load Balancing**: **Elastic load balancer**
- **Load Balancer**: **elb-wordpress** (Select the balancer you created previously.)
- **Backend ECS Group**: Select a backend ECS group bound with load balancer **elb-wordpress**.



* Region: CN-Hong Kong

For low network latency and quick resource access, select the region nearest to your target users.

* AZ ?: AZ1 ⊗ AZ2 ⊗ AZ3 ⊗

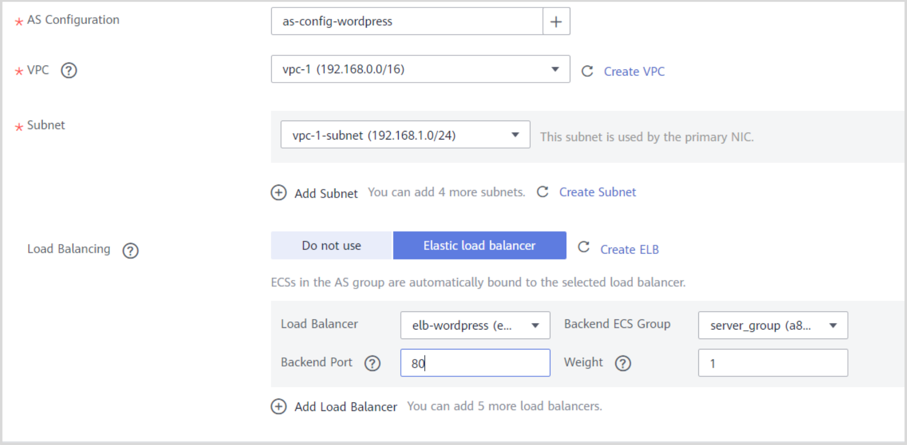
* Multi-AZ Scaling Policy ?: ● Balanced ○ Sequenced

* Name: as-group-1wordpress

* Max. Instances: 4

* Expected Instances ?: 2

* Min. Instances: 1



* AS Configuration: as-config-wordpress

* VPC: vpc-1 (192.168.0.0/16)

* Subnet: vpc-1-subnet (192.168.1.0/24) This subnet is used by the primary NIC.

Add Subnet You can add 4 more subnets. Create Subnet

Load Balancing: Do not use | Elastic load balancer

ECSs in the AS group are automatically bound to the selected load balancer.

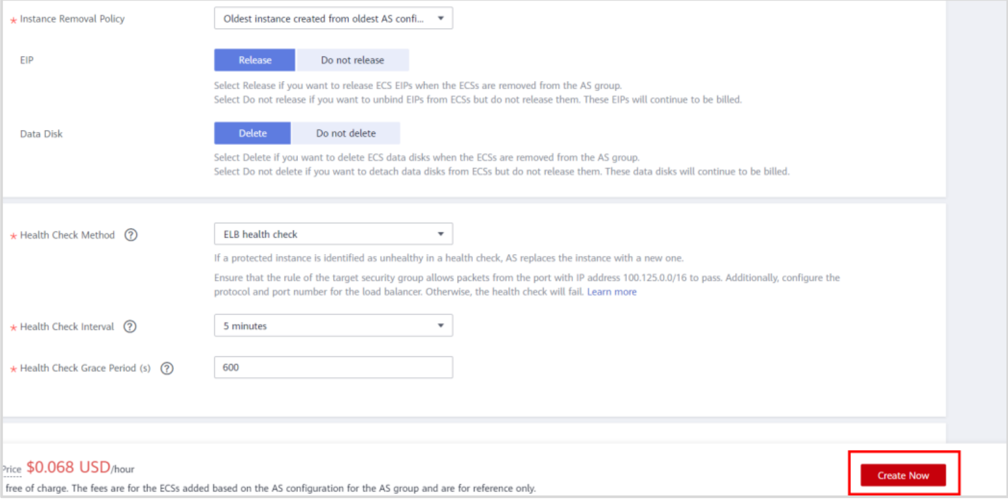
Load Balancer: elb-wordpress (e... Backend ECS Group: server_group (a8...

Backend Port: 80 Weight: 1

Add Load Balancer You can add 5 more load balancers.

Figure 1-64

- Retain the default settings for other parameters and click **Create Now**.



* Instance Removal Policy: Oldest instance created from oldest AS confi...

EIP: Release | Do not release

Select Release if you want to release ECS EIPs when the ECSs are removed from the AS group.
Select Do not release if you want to unbind EIPs from ECSs but do not release them. These EIPs will continue to be billed.

Data Disk: Delete | Do not delete

Select Delete if you want to delete ECS data disks when the ECSs are removed from the AS group.
Select Do not delete if you want to detach data disks from ECSs but do not release them. These data disks will continue to be billed.

* Health Check Method: ELB health check

If a protected instance is identified as unhealthy in a health check, AS replaces the instance with a new one.

Ensure that the rule of the target security group allows packets from the port with IP address 100.125.0.0/16 to pass. Additionally, configure the protocol and port number for the load balancer. Otherwise, the health check will fail. Learn more

* Health Check Interval: 5 minutes

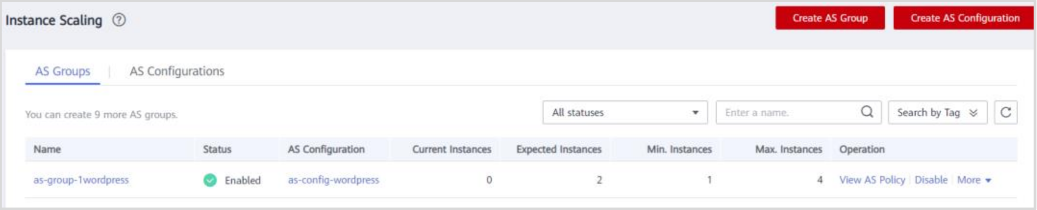
* Health Check Grace Period (s): 600

Price $0.068 USD/hour

free of charge. The fees are for the ECSs added based on the AS configuration for the AS group and are for reference only.

Figure 1-65

Step 8 In the AS group list, check that the created AS group is enabled.



Instance Scaling

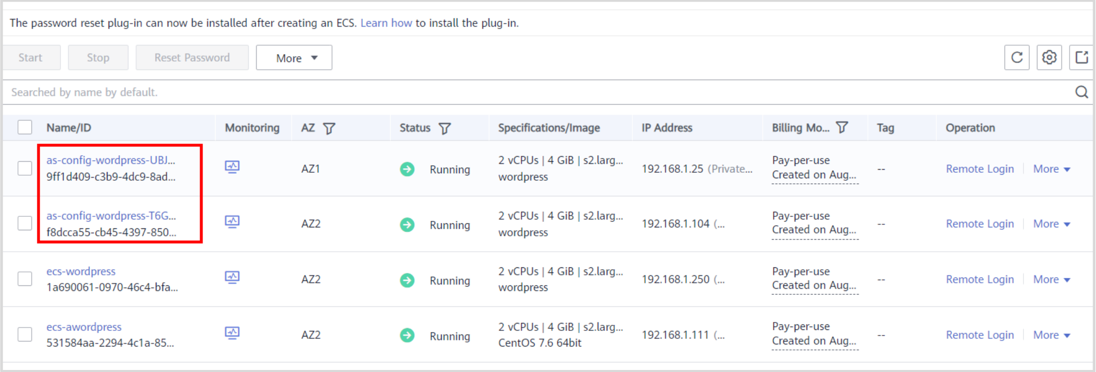
AS Groups | AS Configurations

You can create 9 more AS groups.

Name	Status	AS Configuration	Current Instances	Expected Instances	Min. Instances	Max. Instances	Operation
as-group-1wordpress	Enabled	as-config-wordpress	0	2	1	4	View AS Policy | Disable | More

Figure 1-66

Step 9 Click **Elastic Cloud Server** in the left navigation pane. Check that two ECSs are created by AS and displayed in the ECS list.


The password reset plug-in can now be installed after creating an ECS. Learn how to install the plug-in.

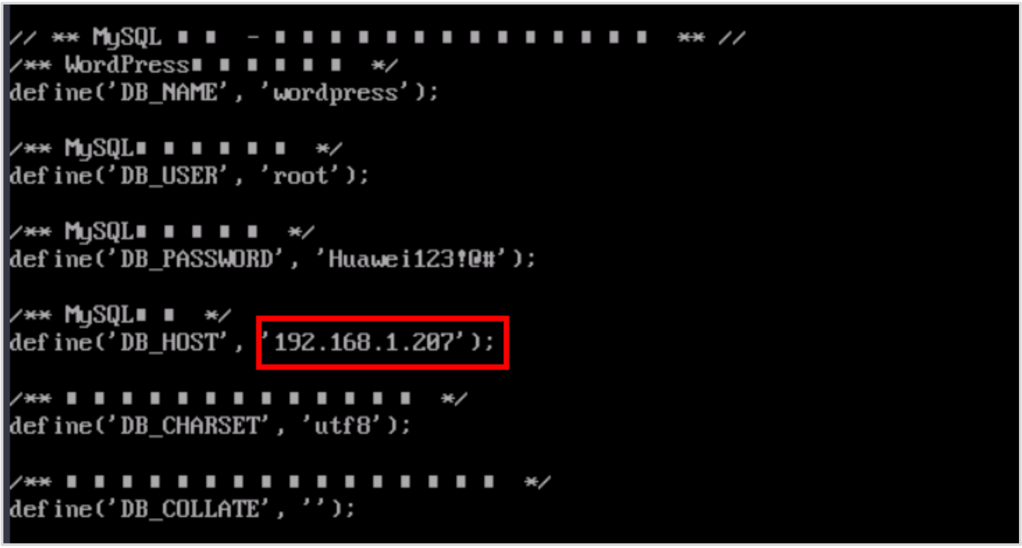
Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mo...	Tag	Operation
as-config-wordpress-UBJ... 9ff1d409-c3b9-4dc9-8ad...		AZ1	Running	2 vCPUs | 4 GiB | s2.larg... wordpress	192.168.1.25 (Private...	Pay-per-use Created on Aug...	--	Remote Login | More
as-config-wordpress-T6G... f8dcca55-cb45-4397-850...		AZ2	Running	2 vCPUs | 4 GiB | s2.larg... wordpress	192.168.1.104 (...	Pay-per-use Created on Aug...	--	Remote Login | More
ecs-wordpress 1a690061-0970-46c4-bfa...		AZ2	Running	2 vCPUs | 4 GiB | s2.larg... wordpress	192.168.1.250 (...	Pay-per-use Created on Aug...	--	Remote Login | More
ecs-awordpress 531584aa-2294-4c1a-85...		AZ2	Running	2 vCPUs | 4 GiB | s2.larg... CentOS 7.6 64bit	192.168.1.111 (...	Pay-per-use Created on Aug...	--	Remote Login | More

Figure 1-67

Step 10 Locate an ECS and click **Remote Login** to log in to the ECS. Then run the following command to view the **wp-config.php** file on the ECS. Check that the value of **DB_HOST** has been changed from **192.168.1.137** to **192.168.1.207**. (This step is performed to verify the text injection is successful and does not affect login.)

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

Note: You can use text injection to easily modify the backend database address. In this way, you can keep services run during resource scaling without the need to create images.

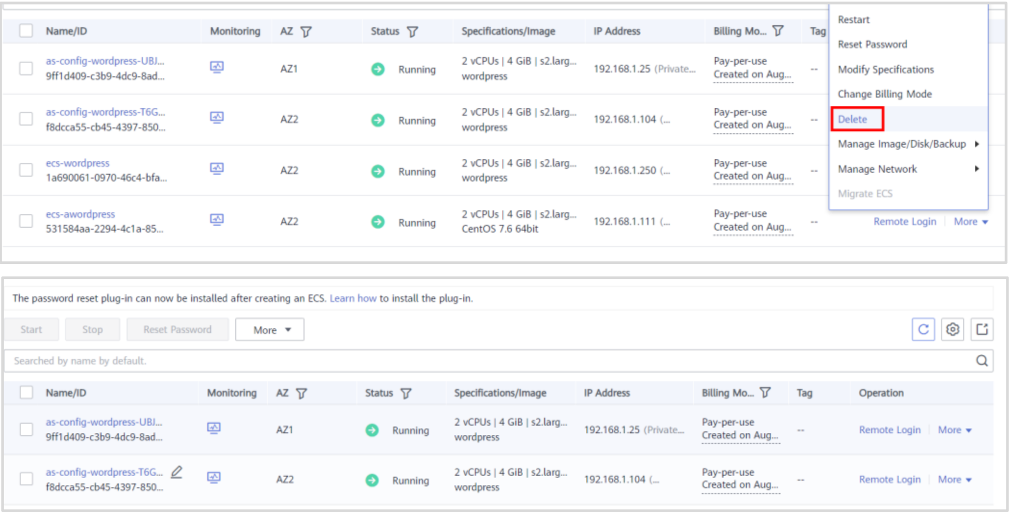


```
// ** MySQL ■ ■  - ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■  ** //
/** WordPress■ ■ ■ ■ ■ ■  */
define('DB_NAME', 'wordpress');

/** MySQL■ ■ ■ ■ ■ ■  */
define('DB_USER', 'root');

/** MySQL■ ■ ■ ■ ■  */
define('DB_PASSWORD', 'Huawei123!@#');

/** MySQL■ ■  */
define('DB_HOST', '192.168.1.207');

/** ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■  */
define('DB_CHARSET', 'utf8');

/** ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■  */
define('DB_COLLATE', '');
```

Figure 1-68

Step 11 Delete the two ECSs named **ecs-wordpress** you created manually in previous sections.

Note: This step is to check whether the ECSs scaled out by AS can provide services properly.



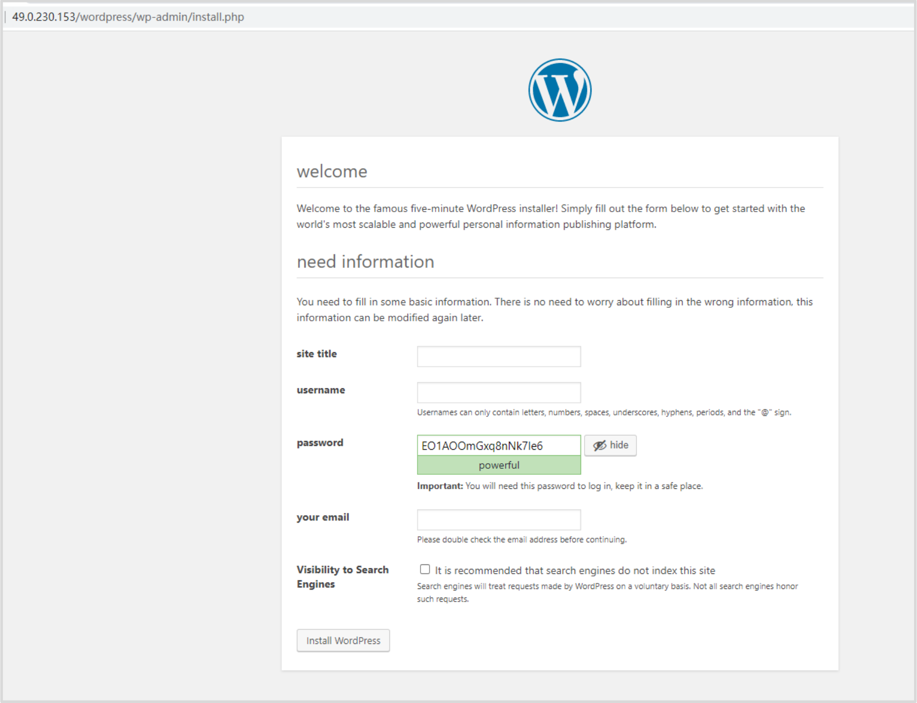
Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mo...	Tag
as-config-wordpress-UBJ... 9ff1d409-c3b9-4dc9-8ad...		AZ1	Running	2 vCPUs | 4 GiB | s2.larg... wordpress	192.168.1.25 (Private...	Pay-per-use Created on Aug...	--
as-config-wordpress-T6G... f8dcca55-cb45-4397-850...		AZ2	Running	2 vCPUs | 4 GiB | s2.larg... wordpress	192.168.1.104 (...	Pay-per-use Created on Aug...	--
ecs-wordpress 1a690061-0970-46c4-bfa...		AZ2	Running	2 vCPUs | 4 GiB | s2.larg... wordpress	192.168.1.250 (...	Pay-per-use Created on Aug...	--
ecs-awordpress 531584aa-2294-4c1a-85...		AZ2	Running	2 vCPUs | 4 GiB | s2.larg... CentOS 7.6 64bit	192.168.1.111 (...	Pay-per-use Created on Aug...	--

The password reset plug-in can now be installed after creating an ECS. Learn how to install the plug-in.

Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mo...	Tag	Operation
as-config-wordpress-UBJ... 9ff1d409-c3b9-4dc9-8ad...		AZ1	Running	2 vCPUs | 4 GiB | s2.larg... wordpress	192.168.1.25 (Private...	Pay-per-use Created on Aug...	--	Remote Login | More
as-config-wordpress-T6G... f8dcca55-cb45-4397-850...		AZ2	Running	2 vCPUs | 4 GiB | s2.larg... wordpress	192.168.1.104 (...	Pay-per-use Created on Aug...	--	Remote Login | More

Figure 1-69

Step 12 Open a browser and enter **http://** *(EIP of the load balancer)***/wordpress/index.php**.



49.0.230.153/wordpress/wp-admin/install.php

welcome

Welcome to the famous five-minute WordPress installer! Simply fill out the form below to get started with the world's most scalable and powerful personal information publishing platform.

need information

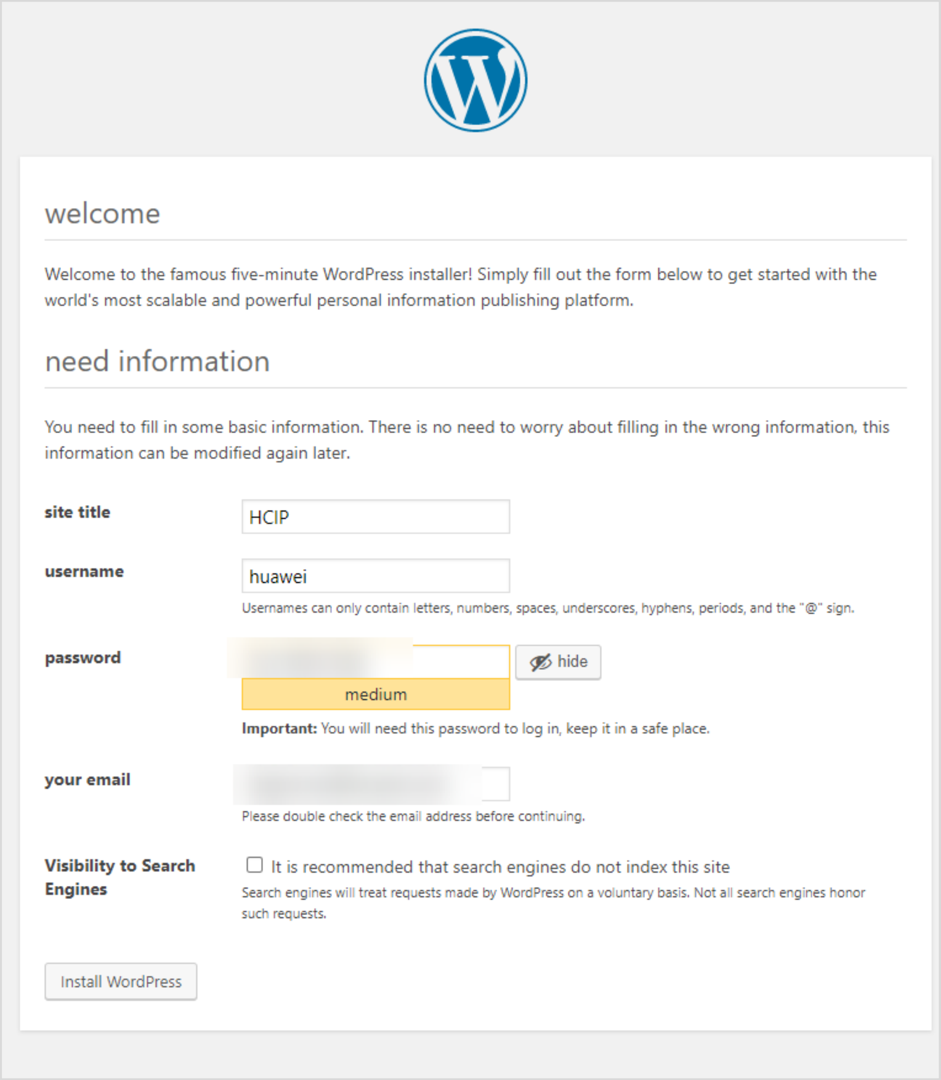
You need to fill in some basic information. There is no need to worry about filling in the wrong information, this information can be modified again later.

site title	
username	Usernames can only contain letters, numbers, spaces, underscores, hyphens, periods, and the "@" sign.
password	EO1AOOmGxq8nNk7le6 hide powerful Important: You will need this password to log in, keep it in a safe place.
your email	Please double check the email address before continuing.
Visibility to Search Engines	□ It is recommended that search engines do not index this site Search engines will treat requests made by WordPress on a voluntary basis. Not all search engines honor such requests.

Figure 1-70

Step 13 Enter the registration information as follows and click **Install WordPress**. After the installation is complete, log in to WordPress. If the login is successful, the ECS created by AS can provide services properly.

- **Site Title**: HCIP
- **Username**: **huawei** (user-defined)
- **Password**: User-defined
- **Your Email**: User-defined



welcome

Welcome to the famous five-minute WordPress installer! Simply fill out the form below to get started with the world's most scalable and powerful personal information publishing platform.

need information

You need to fill in some basic information. There is no need to worry about filling in the wrong information, this information can be modified again later.

site title: HCIP

username: huawei

Usernames can only contain letters, numbers, spaces, underscores, hyphens, periods, and the "@" sign.

password: [redacted] hide

medium

Important: You will need this password to log in, keep it in a safe place.

your email: [redacted]

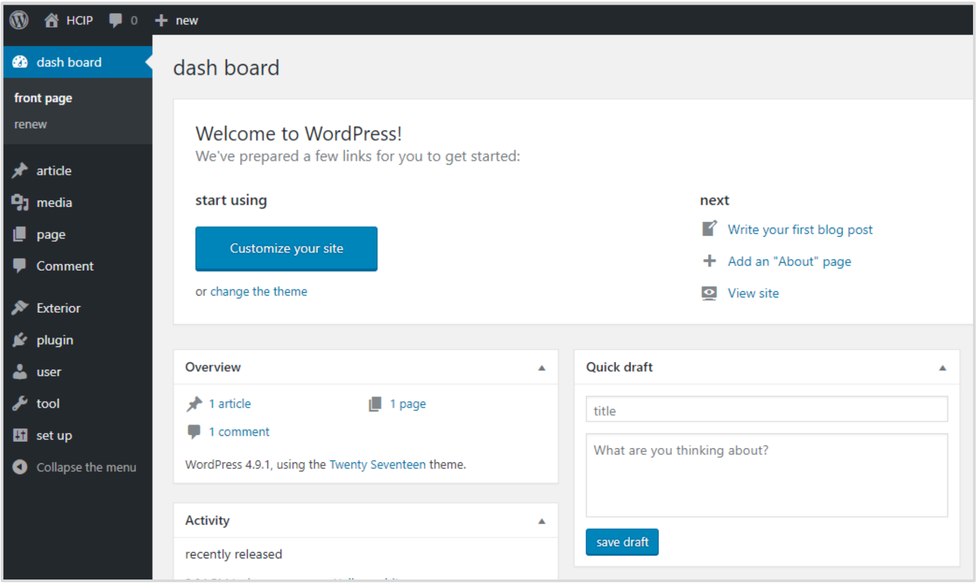
Please double check the email address before continuing.

Visibility to Search Engines: □ It is recommended that search engines do not index this site

Search engines will treat requests made by WordPress on a voluntary basis. Not all search engines honor such requests.

Install WordPress

Figure 1-71



dash board

Welcome to WordPress!

We've prepared a few links for you to get started:

start using

Customize your site

or change the theme

next

Write your first blog post

Add an "About" page

View site

Overview

1 article 1 page

1 comment

WordPress 4.9.1, using the Twenty Seventeen theme.

Activity

recently released

Quick draft

title

What are you thinking about?

save draft

Figure 1-72

1.3 Clearing Resources

Step 1 Delete the AS group. In the service list, choose **Auto Scaling** under **Compute**. In the navigation pane on the left, choose **Instance Scaling**.

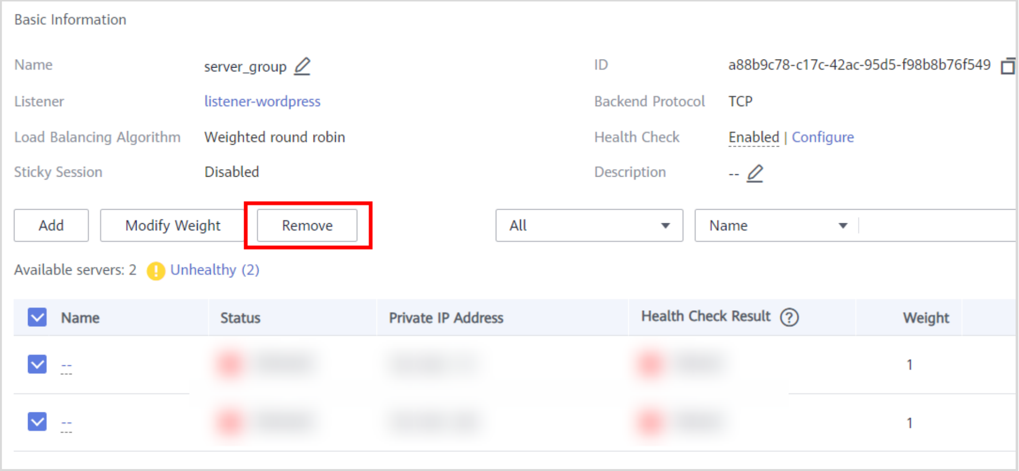
- On the **AS Groups** tab, locate the row containing the AS group to be deleted and choose **More** > **Delete** in the **Operation** column.
- Click the **AS Configurations** tab, locate the row containing the AS configuration to be deleted, and click **Delete** in the **Operation** column.

Step 2 Delete the key pair.

- In the service list, choose **Data Encryption Workshop** under **Security & Compliance**. In the navigation pane on the left, choose **Key Pair Service**.
- On the **Private Key Pairs** tab, locate the row containing the key pair to be deleted and click **Delete** in the **Operation** column.

Step 3 Deleting the load balancer

- In the service list, choose **Elastic Load Balance** under **Networking**. In the load balancer list, click the load balancer purchased in this exercise. On the **Backend Server Groups** tab, in the **Basic Information** area, select all backend servers and click **Remove** above the server list.



Basic Information

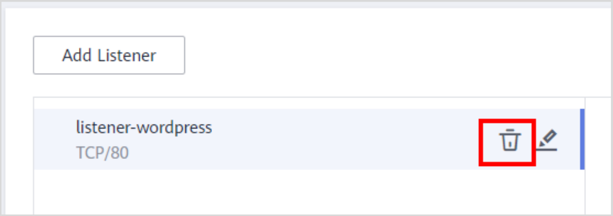
Name server_group
ID a88b9c78-c17c-42ac-95d5-f98b8b76f549
Listener listener-wordpress
Backend Protocol TCP
Load Balancing Algorithm Weighted round robin
Health Check Enabled | Configure
Sticky Session Disabled
Description --

Available servers: 2 ! Unhealthy (2)

☑ Name	Status	Private IP Address	Health Check Result ?	Weight
☑ --	[redacted]	[redacted]	[redacted]	1
☑ --	[redacted]	[redacted]	[redacted]	1

Figure 1-73

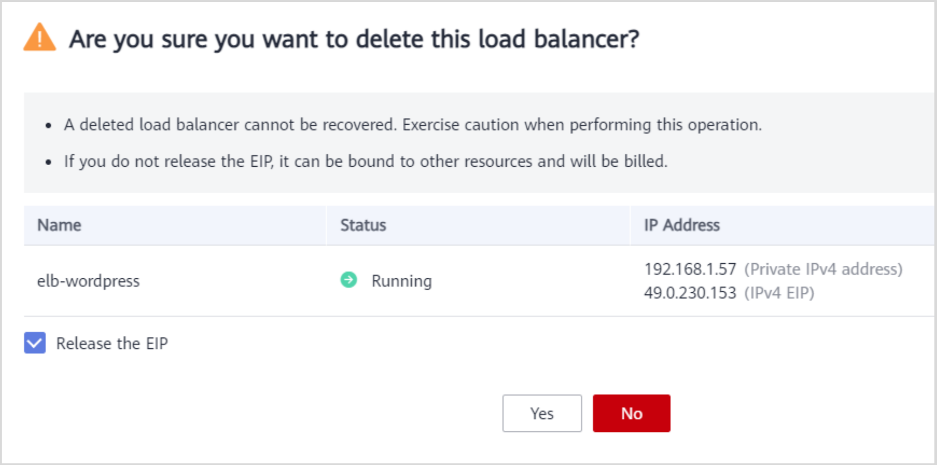
- On the **Listeners** tab, delete the listener purchased in this exercise.



listener-wordpress
TCP/80

Figure 1-74

- Back to the load balancer list and click **Delete** in the **Operation** column to delete the load balancer.
- In the displayed dialog box, select **Release the EIP** and click **Yes**.



Are you sure you want to delete this load balancer?

- A deleted load balancer cannot be recovered. Exercise caution when performing this operation.
- If you do not release the EIP, it can be bound to other resources and will be billed.

Name	Status	IP Address
elb-wordpress	Running	192.168.1.57 (Private IPv4 address) 49.0.230.153 (IPv4 EIP)

☑ Release the EIP

Figure 1-75

Step 4 Delete the image created in this exercise.

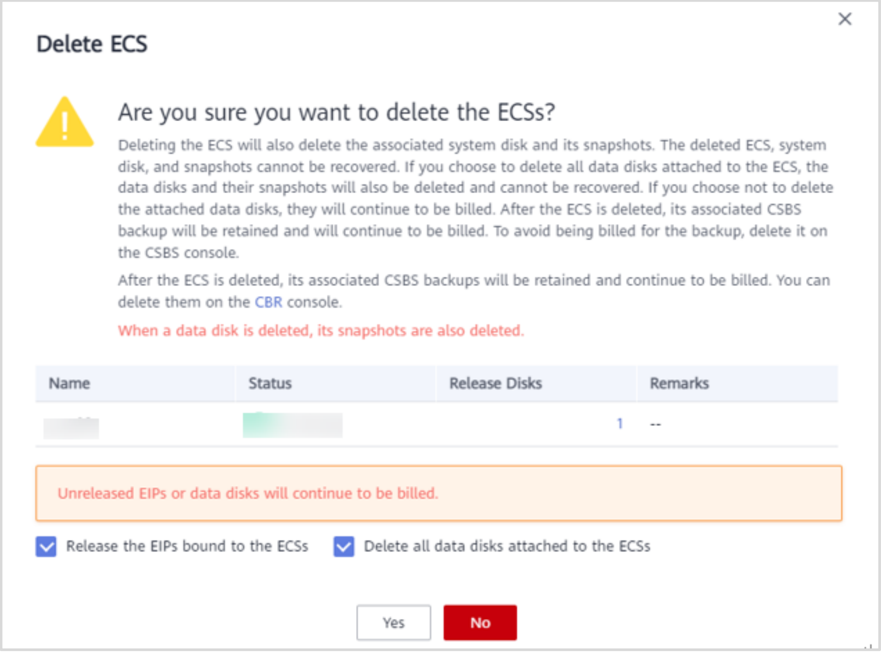
- In the service list, choose **Image Management Service** under **Compute**. In the private image list, locate the image created in this exercise and choose **More** > **Delete** in the **Operation** column.

Step 5 Delete the RDS instance.

- In the service list, choose **Relational Database Service** under **Database**. In the instance list, locate the instance purchased in this exercise and click **Delete** in the **Operation** column.

Step 6 Delete the ECS.

- In the service list, choose **Elastic Cloud Server** under **Compute**. In the ECS list, locate the ECS purchased in this exercise and choose **More** > **Delete** in the **Operation** column.
- In the displayed dialog box, select the check boxes displayed in the following picture and click **Yes**.



Delete ECS

Are you sure you want to delete the ECSs?

Deleting the ECS will also delete the associated system disk and its snapshots. The deleted ECS, system disk, and snapshots cannot be recovered. If you choose to delete all data disks attached to the ECS, the data disks and their snapshots will also be deleted and cannot be recovered. If you choose not to delete the attached data disks, they will continue to be billed. After the ECS is deleted, its associated CSBS backup will be retained and will continue to be billed. To avoid being billed for the backup, delete it on the CSBS console.

After the ECS is deleted, its associated CSBS backups will be retained and continue to be billed. You can delete them on the CBR console.

When a data disk is deleted, its snapshots are also deleted.

Name	Status	Release Disks	Remarks
[redacted]	[redacted]	1	--

Unreleased EIPs or data disks will continue to be billed.

☑ Release the EIPs bound to the ECSs ☑ Delete all data disks attached to the ECSs

Figure 1-76

Step 7 Delete the security group.

- In the service list, choose **Virtual Private Cloud** under **Networking**. In the security group list, locate the security group created in this exercise and click **Delete** in the **Operation** column.

Step 8 Delete the subnet and VPC.

- Choose **Subnets** in the navigation pane on the left. Locate the subnet created in this exercise and click **Delete** in the **Operation** column.
- Choose **My VPCs** in the navigation pane on the left. In the VPC list, locate the VPC created in this exercise and click **Delete** in the **Operation** column.

1.4 Quiz

Question: If health check is enabled without specifying a health check port, how will the health check be performed?

Answer: If you do not specify a health check port, a port of the backend server will be used for health checks by default. If you specify a port, the port will be used for health checks.

2 Network Architecture Design

2.1 Introduction

2.1.1 About This Exercise

This exercise uses Huawei Cloud resources in different regions to represent on-premises and cloud resources, describes how on-premises resources can communicate with cloud resources and manage cloud resources for O&M, and how cloud resources can communicate with each other and access the internet.

VPC 1 in the CN-Hong Kong region represents an on-premises network, and its ECS represents an on-premises server used for O&M. VPC 2, VPC 3, and their ECSs in the AP-Singapore region represent cloud resources.

To enable ECSs in VPC 2 and VPC 3 in the AP-Singapore region to communicate with each other, a VPC peering connection is required. To enable the on-premises ECS used for O&M in the CN-Hong Kong region to manage cloud resources in AP-Singapore region, Virtual Private Network (VPN) and VPC peering connections are required. To enable internet access, a NAT gateway is deployed in VPC 2 in the AP-Singapore region so that ECSs in VPC 3 and VPC 2 can access the internet through the NAT gateway.

This exercise uses regions CN-Hong Kong and AP-Singapore as an example. Trainees can select regions based on their own needs.

2.1.2 Objectives

Understand how to use the cloud services involved in the cloud network architecture.

Understand how to design cloud networks with scalability, manage cloud and on-premises resources in unified manner, and allow cloud and on-premises communications.

2.1.3 Networking

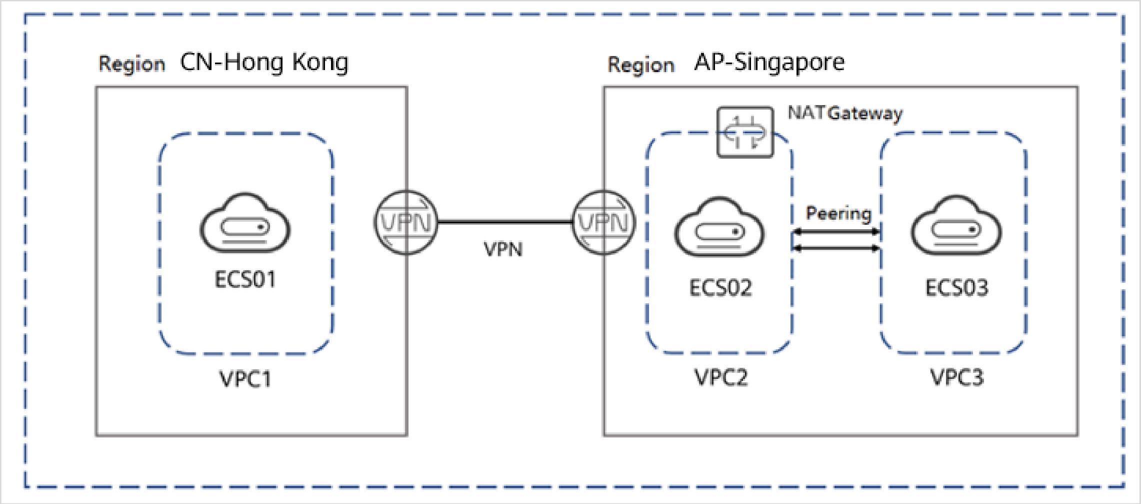


Figure 2-1

2.2 Procedure

2.2.1 Creating VPCs

Step 1 Visit https://intl.huaweicloud.com/en-us/ and log in using your Huawei Cloud account. If you are an IAM user, log in as an IAM user.

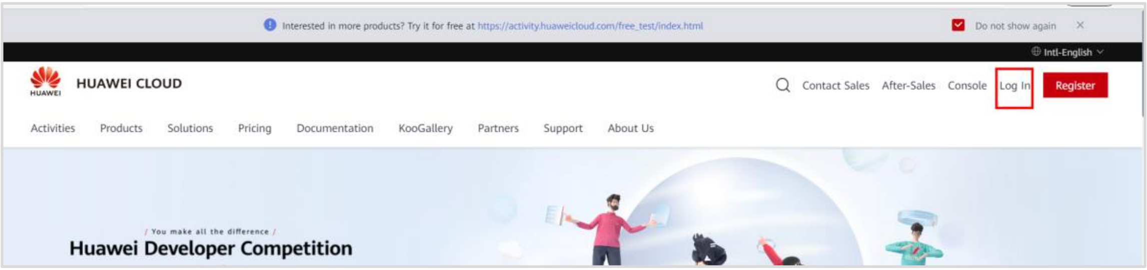

Interested in more products? Try it for free at https://activity.huaweicloud.com/free_test/index.html

Figure 2-2

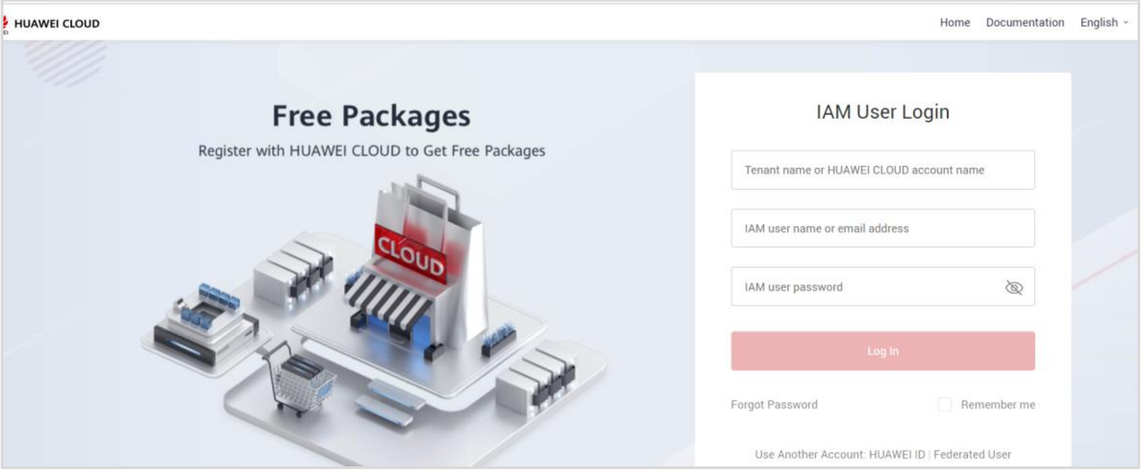

HUAWEI CLOUD
Home
Documentation
English
Free Packages
Register with HUAWEI CLOUD to Get Free Packages
CLOUD
IAM User Login
Tenant name or HUAWEI CLOUD account name
IAM user name or email address
IAM user password
Log In
Forgot Password
Remember me
Use Another Account: HUAWEI ID | Federated User

Figure 2-3

Step 2 Click **Console** and select **CN-Hong Kong**.

Step 3 In the service list, choose **Networking** > **Virtual Private Cloud**.

Step 4 Click **Create VPC** in the upper right corner.

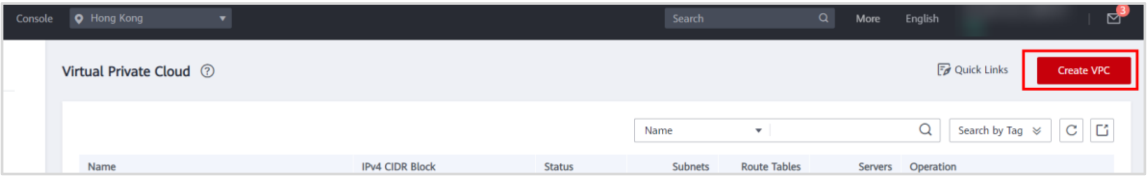


Figure 2-4

Step 5 Configure the following parameters and click **Create Now**.

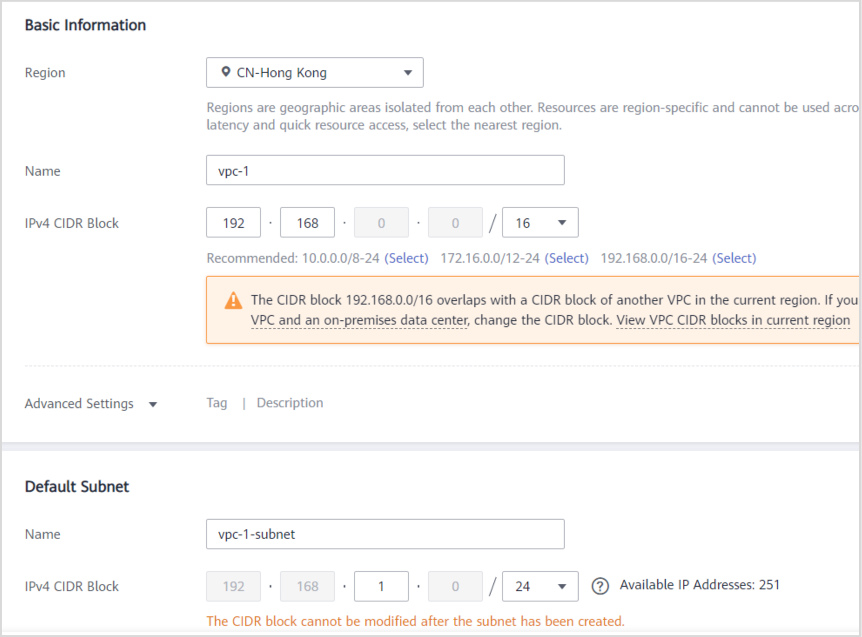
Note: In this exercise, this VPC represents an on-premises network.

Basic Information

- **Region**: **CN-Hong Kong**
- **Name**: **vpc-1**
- **IPv4 CIDR Block**: **192.168.0.0/16**

Default Subnet

- **Name**: **vpc-1-subnet**
- **IPv4 CIDR Block**: **192.168.1.0/24**



Basic Information

Region: CN-Hong Kong

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used acro latency and quick resource access, select the nearest region.

Name: vpc-1

IPv4 CIDR Block: 192 . 168 . 0 . 0 / 16

Recommended: 10.0.0.0/8-24 (Select) 172.16.0.0/12-24 (Select) 192.168.0.0/16-24 (Select)

The CIDR block 192.168.0.0/16 overlaps with a CIDR block of another VPC in the current region. If you VPC and an on-premises data center, change the CIDR block. View VPC CIDR blocks in current region

Advanced Settings Tag | Description

Default Subnet

Name: vpc-1-subnet

IPv4 CIDR Block: 192 . 168 . 1 . 0 / 24 Available IP Addresses: 251

The CIDR block cannot be modified after the subnet has been created.

Figure 2-5

Step 6 Repeat the preceding steps to create VPC 2 and VPC 3 as follows.

Note: VPC 2 and VPC 3 represent cloud networks.

Basic Information

- **Region: AP-Singapore**
- **Name: vpc-2**
- **IPv4 CIDR Block: 192.168.0.0/16**

Default Subnet

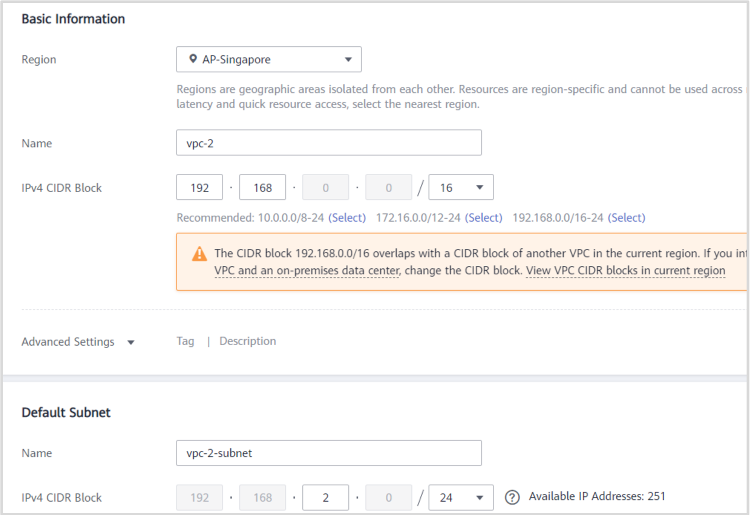
- **AZ: AZ1**
- **Name: vpc-2-subnet**
- **IPv4 CIDR Block: 192.168.2.0/24**

Basic Information

- **Region: AP-Singapore**
- **Name: vpc-3**
- **IPv4 CIDR Block: 192.168.0.0/16**

Default Subnet

- **AZ: AZ1**
- **Name: vpc-3-subnet**
- **IPv4 CIDR Block: 192.168.3.0/24**



Basic Information

Region: AP-Singapore

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across latency and quick resource access, select the nearest region.

Name: vpc-2

IPv4 CIDR Block: 192 . 168 . 0 . 0 / 16

Recommended: 10.0.0.0/8-24 (Select) 172.16.0.0/12-24 (Select) 192.168.0.0/16-24 (Select)

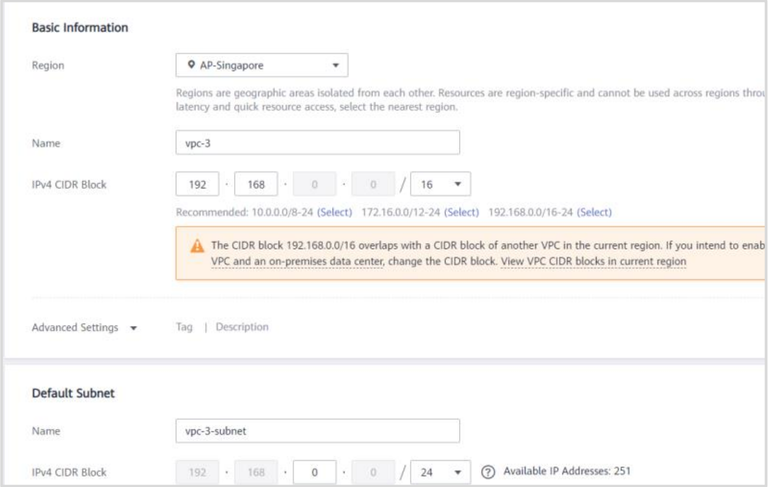
The CIDR block 192.168.0.0/16 overlaps with a CIDR block of another VPC in the current region. If you in VPC and an on-premises data center, change the CIDR block. View VPC CIDR blocks in current region

Advanced Settings Tag | Description

Default Subnet

Name: vpc-2-subnet

IPv4 CIDR Block: 192 . 168 . 2 . 0 / 24 Available IP Addresses: 251



Basic Information

Region: AP-Singapore

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions throu latency and quick resource access, select the nearest region.

Name: vpc-3

IPv4 CIDR Block: 192 . 168 . 0 . 0 / 16

Recommended: 10.0.0.0/8-24 (Select) 172.16.0.0/12-24 (Select) 192.168.0.0/16-24 (Select)

The CIDR block 192.168.0.0/16 overlaps with a CIDR block of another VPC in the current region. If you intend to enab VPC and an on-premises data center, change the CIDR block. View VPC CIDR blocks in current region

Advanced Settings Tag | Description

Default Subnet

Name: vpc-3-subnet

IPv4 CIDR Block: 192 . 168 . 0 . 0 / 24 Available IP Addresses: 251

Figure 2-6

2.2.2 Creating Security Groups

Step 1 In the **CN-Hong Kong** region, choose **Access Control** > **Security Groups** on the network console, and click **Create Security Group** in the upper right corner.

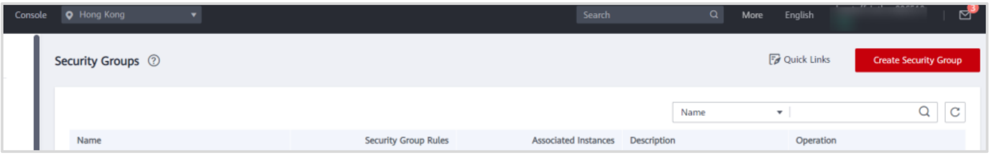
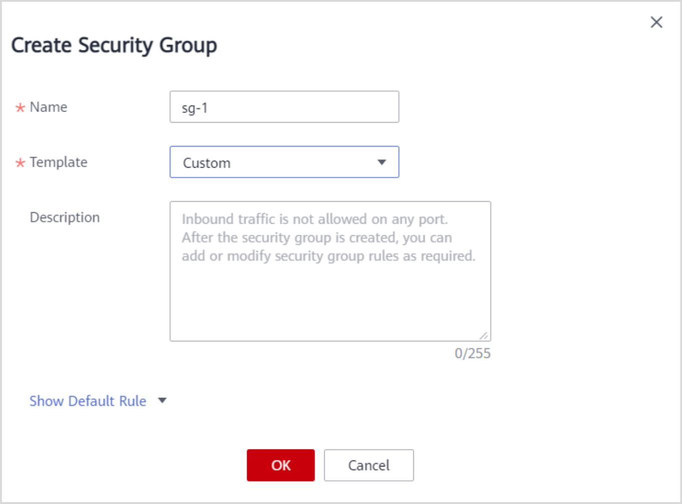


Figure 2-7

Step 2 Configure the parameters as follows and click **OK**.

Note: This security group is used by ECSs in VPC 1. You need to allow all ICMP traffic and traffic on port 22. ICMP is used for connectivity tests, and port 22 is used for SSH login tests.

- **Name**: sg-1
- **Template**: Select a required one.



Create Security Group

* Name: sg-1

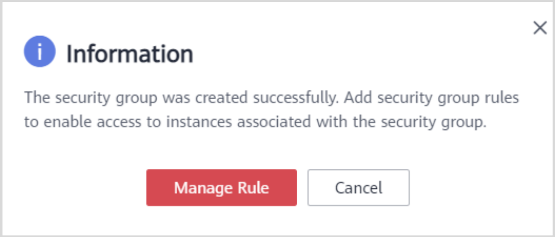
* Template: Custom

Description: Inbound traffic is not allowed on any port. After the security group is created, you can add or modify security group rules as required.

0/255

Figure 2-8

Step 3 In the dialog box displayed, click **Manage Rule**.



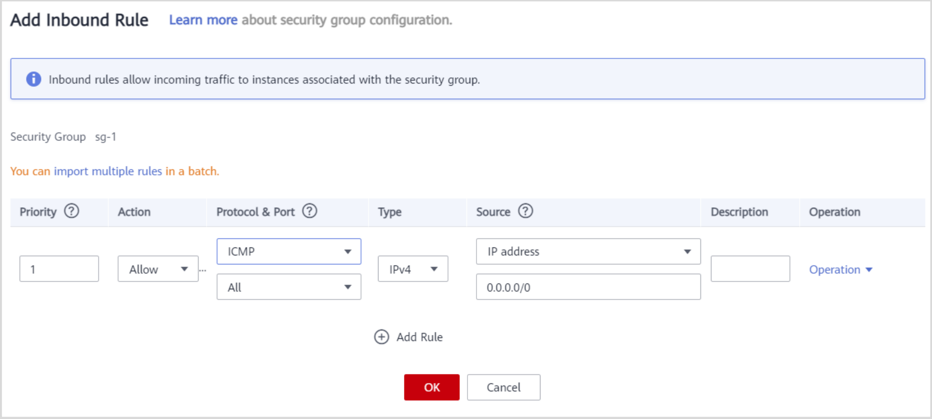
Information

The security group was created successfully. Add security group rules to enable access to instances associated with the security group.

Figure 2-9

Step 4 Add the first inbound rule as follows:

- Priority: 1
- Action: Allow
- Protocol: ICMP
- Port: All
- Source: **IP address** and **0.0.0.0/0**



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group sg-1

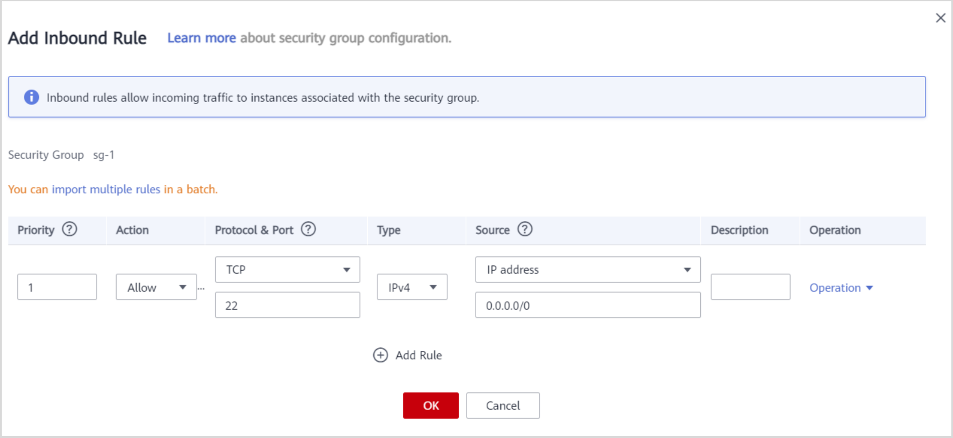
You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Source	Description	Operation
1	Allow	ICMP All	IPv4	IP address 0.0.0.0/0		Operation

Figure 2-10

Step 5 Add the second inbound rule as follows:

- Priority: 1
- Action: Allow
- Protocol: TCP
- Port: 22
- Source: **IP address** and **0.0.0.0/0**



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group sg-1

You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Source	Description	Operation
1	Allow	TCP 22	IPv4	IP address 0.0.0.0/0		Operation

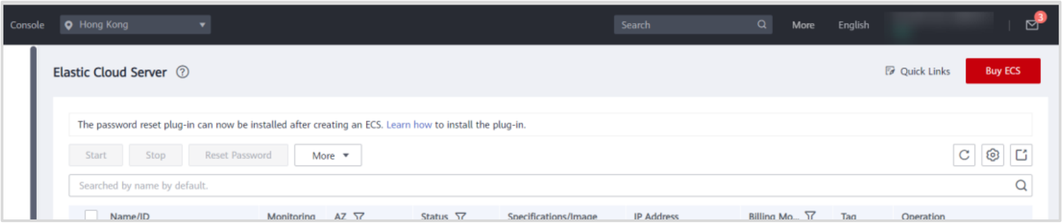
Figure 2-11

Step 6 Repeat the preceding steps to create security group **sg-4** in the AP-Singapore region.

Note: Security group sg-4 is used by ECSs in the AP-Singapore region. You also need to allow all ICMP traffic and traffic on port 22.

2.2.3 Buying ECSs

Step 1 In the **CN-Hong Kong** region, click **Buy ECS** in the upper right corner.



The password reset plug-in can now be installed after creating an ECS. Learn how to install the plug-in.

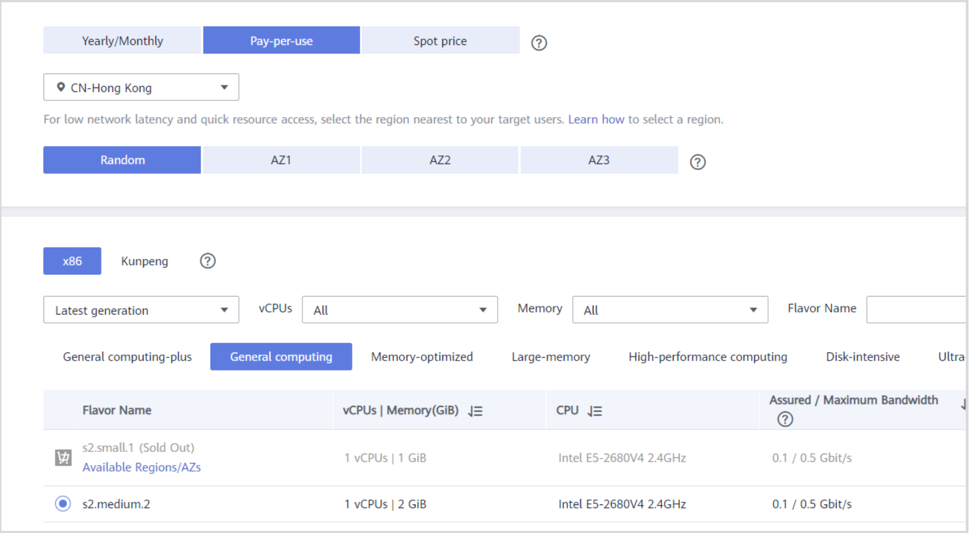
Figure 2-12

Step 2 Configure the parameters as follows.

Note: ecs-01 represents an on-premises server used for O&M.

ecs-01 configuration:

- **Billing Mode: Pay-per-use**
- **Region: CN-Hong Kong**
- **AZ: Random**
- **CPU Architecture: x86**
- **Specifications: 1 vCPUs | 2 GiB**
- **Image: Public image | CentOS 7.6 64bit(40GB)**
- **Host Security: Enable | Basic (free)**
- **Network: vpc-1 | vpc-1-subnet | Automatically assign IP address**
- **Security Group: sg-1**
- **EIP: Not required**
- **System Disk: High I/O | 40 GiB**
- **ECS Name: ecs-01**
- **Password**: User-defined (with the username of **root**)



For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

	Flavor Name	vCPUs | Memory(GiB)	CPU	Assured / Maximum Bandwidth
	s2.small.1 (Sold Out) Available Regions/AZs	1 vCPUs | 1 GiB	Intel E5-2680V4 2.4GHz	0.1 / 0.5 Gbit/s
●	s2.medium.2	1 vCPUs | 2 GiB	Intel E5-2680V4 2.4GHz	0.1 / 0.5 Gbit/s

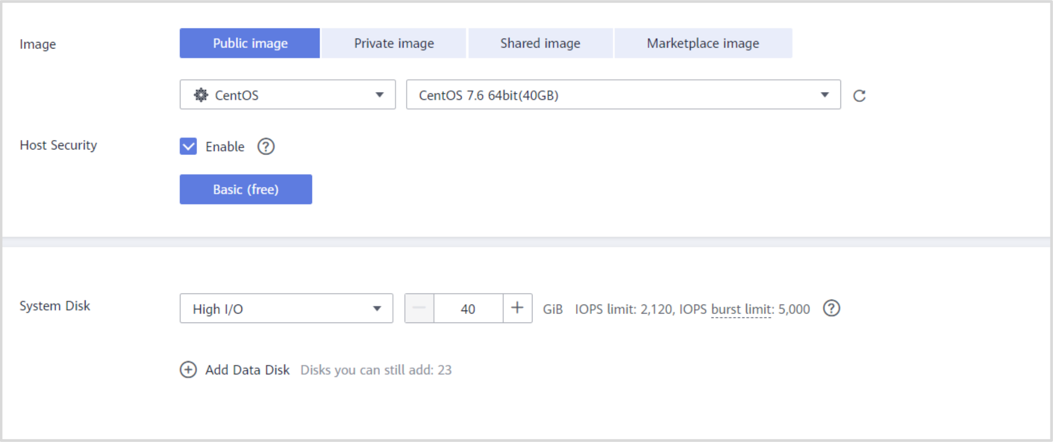


Image: Public image | Private image | Shared image | Marketplace image

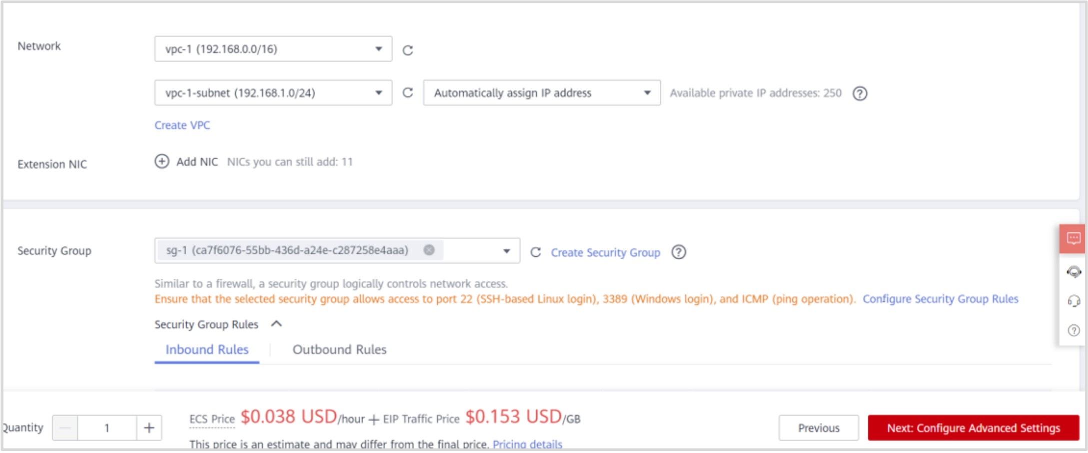
CentOS | CentOS 7.6 64bit(40GB)

Host Security: ☑ Enable

Basic (free)

System Disk: High I/O | 40 GiB | IOPS limit: 2,120, IOPS burst limit: 5,000

Add Data Disk Disks you can still add: 23



Network: vpc-1 (192.168.0.0/16)

vpc-1-subnet (192.168.1.0/24) | Automatically assign IP address | Available private IP addresses: 250

Create VPC

Extension NIC: Add NIC NICs you can still add: 11

Security Group: sg-1 (ca7f6076-55bb-436d-a24e-c287258e4aaa) | Create Security Group

Similar to a firewall, a security group logically controls network access.

Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

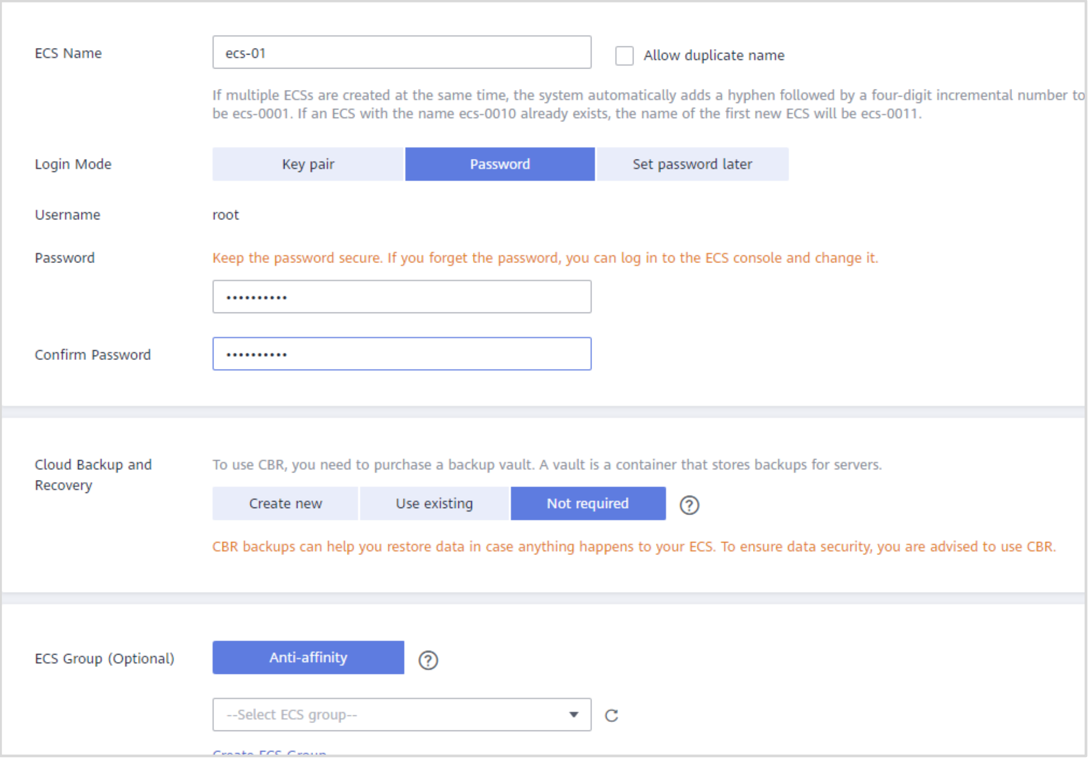
Security Group Rules

Inbound Rules | Outbound Rules

Quantity: 1 | ECS Price $0.038 USD/hour + EIP Traffic Price $0.153 USD/GB

This price is an estimate and may differ from the final price. Pricing details

Previous | Next: Configure Advanced Settings



ECS Name: ecs-01 | □ Allow duplicate name

If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a four-digit incremental number to be ecs-0001. If an ECS with the name ecs-0010 already exists, the name of the first new ECS will be ecs-0011.

Login Mode: Key pair | Password | Set password later

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.

••••••••••

Confirm Password: ••••••••••

Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.

Create new | Use existing | Not required

CBR backups can help you restore data in case anything happens to your ECS. To ensure data security, you are advised to use CBR.

ECS Group (Optional): Anti-affinity

--Select ECS group--

Create ECS Group

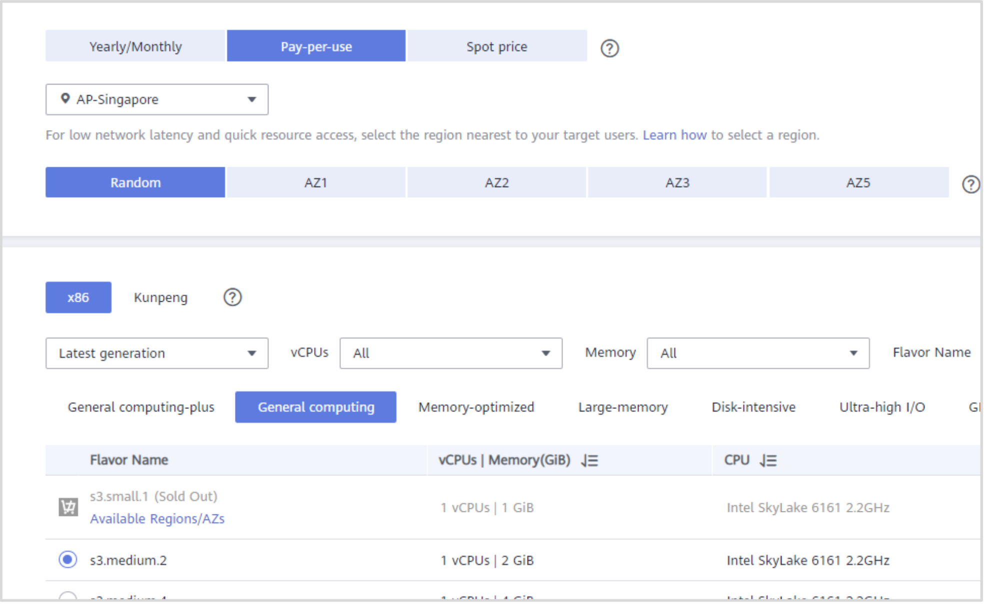
Figure 2-13

Step 3 Repeat the preceding steps to purchase ecs-02 and ecs-03 in the AP-Singapore region.

Note: ecs-02 and ecs-03 represent cloud resources.

ecs-02 configuration:

- Billing Mode: Pay-per-use
- Region: AP-Singapore
- AZ: Random
- CPU Architecture: x86
- Specifications: 1 vCPUs | 2 GiB
- Image: Public image | CentOS 7.6 64bit(40GB)
- Host Security: Enable | Basic (free)
- Network: vpc-2 | vpc-2-subnet | Automatically assign IP address
- Security Group: sg-4
- EIP: Not required
- System Disk: High I/O | 40 GiB
- ECS Name: ecs-02
- **Password**: User-defined (with the username of **root**)



Yearly/Monthly | Pay-per-use | Spot price

AP-Singapore

For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

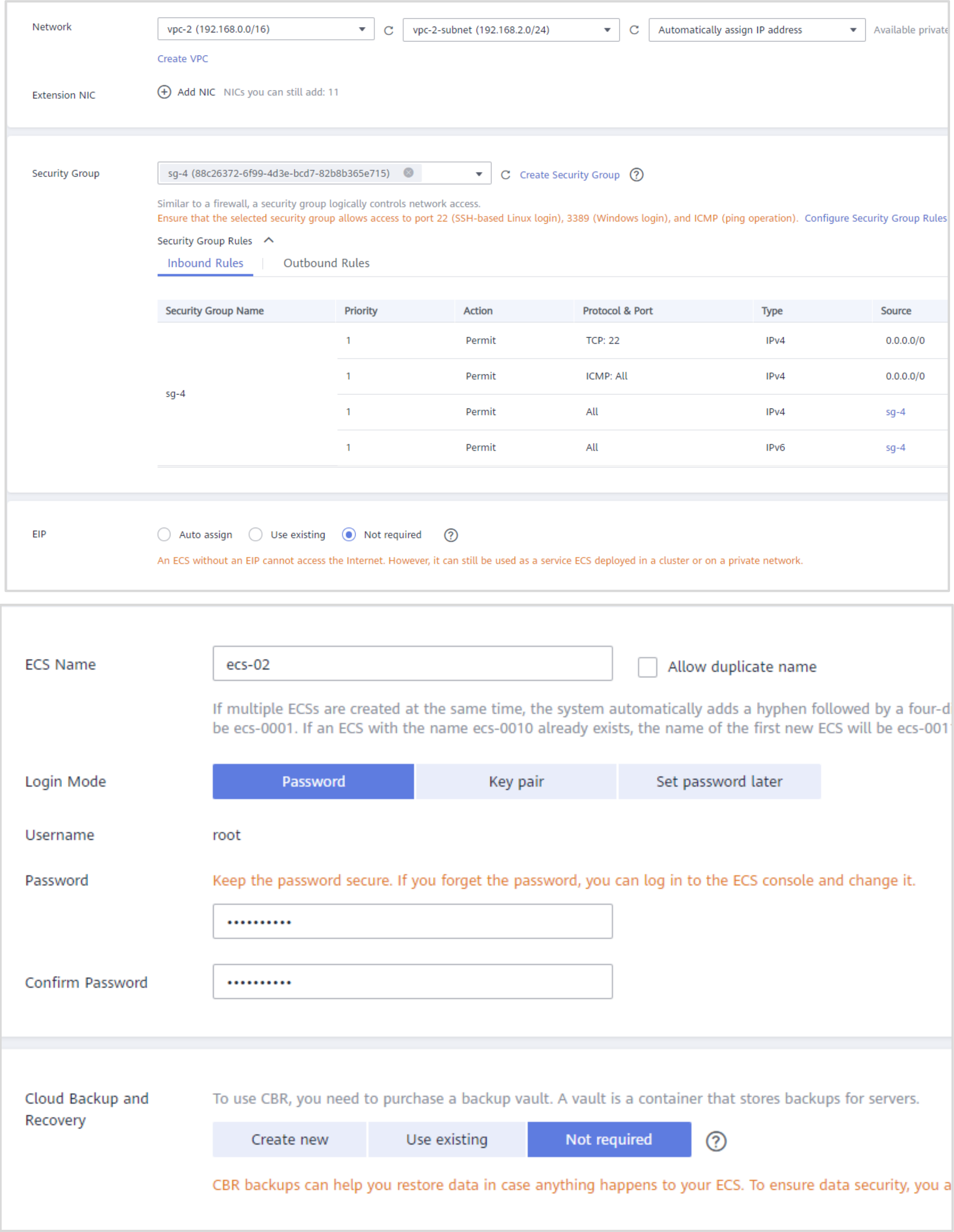
Random | AZ1 | AZ2 | AZ3 | AZ5

x86 | Kunpeng

Latest generation | vCPUs: All | Memory: All | Flavor Name

General computing-plus | General computing | Memory-optimized | Large-memory | Disk-intensive | Ultra-high I/O | Gi

Flavor Name	vCPUs | Memory(GiB)	CPU
s3.small.1 (Sold Out) Available Regions/AZs	1 vCPUs | 1 GiB	Intel SkyLake 6161 2.2GHz
● s3.medium.2	1 vCPUs | 2 GiB	Intel SkyLake 6161 2.2GHz



Network: vpc-2 (192.168.0.0/16) | vpc-2-subnet (192.168.2.0/24) | Automatically assign IP address | Available private

Create VPC

Extension NIC: Add NIC NICs you can still add: 11

Security Group: sg-4 (88c26372-6f99-4d3e-bcd7-82b8b365e715)

Create Security Group

Similar to a firewall, a security group logically controls network access.

Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

Security Group Rules

Inbound Rules | Outbound Rules

Security Group Name	Priority	Action	Protocol & Port	Type	Source
sg-4	1	Permit	TCP: 22	IPv4	0.0.0.0/0
	1	Permit	ICMP: All	IPv4	0.0.0.0/0
	1	Permit	All	IPv4	sg-4
	1	Permit	All	IPv6	sg-4

EIP: ○ Auto assign ○ Use existing ● Not required

An ECS without an EIP cannot access the Internet. However, it can still be used as a service ECS deployed in a cluster or on a private network.

ECS Name: ecs-02

□ Allow duplicate name

If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a four-d be ecs-0001. If an ECS with the name ecs-0010 already exists, the name of the first new ECS will be ecs-001

Login Mode: [✓ Password] Key pair Set password later

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.

••••••••••

Confirm Password: ••••••••••

Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.

Create new Use existing [✓ Not required]

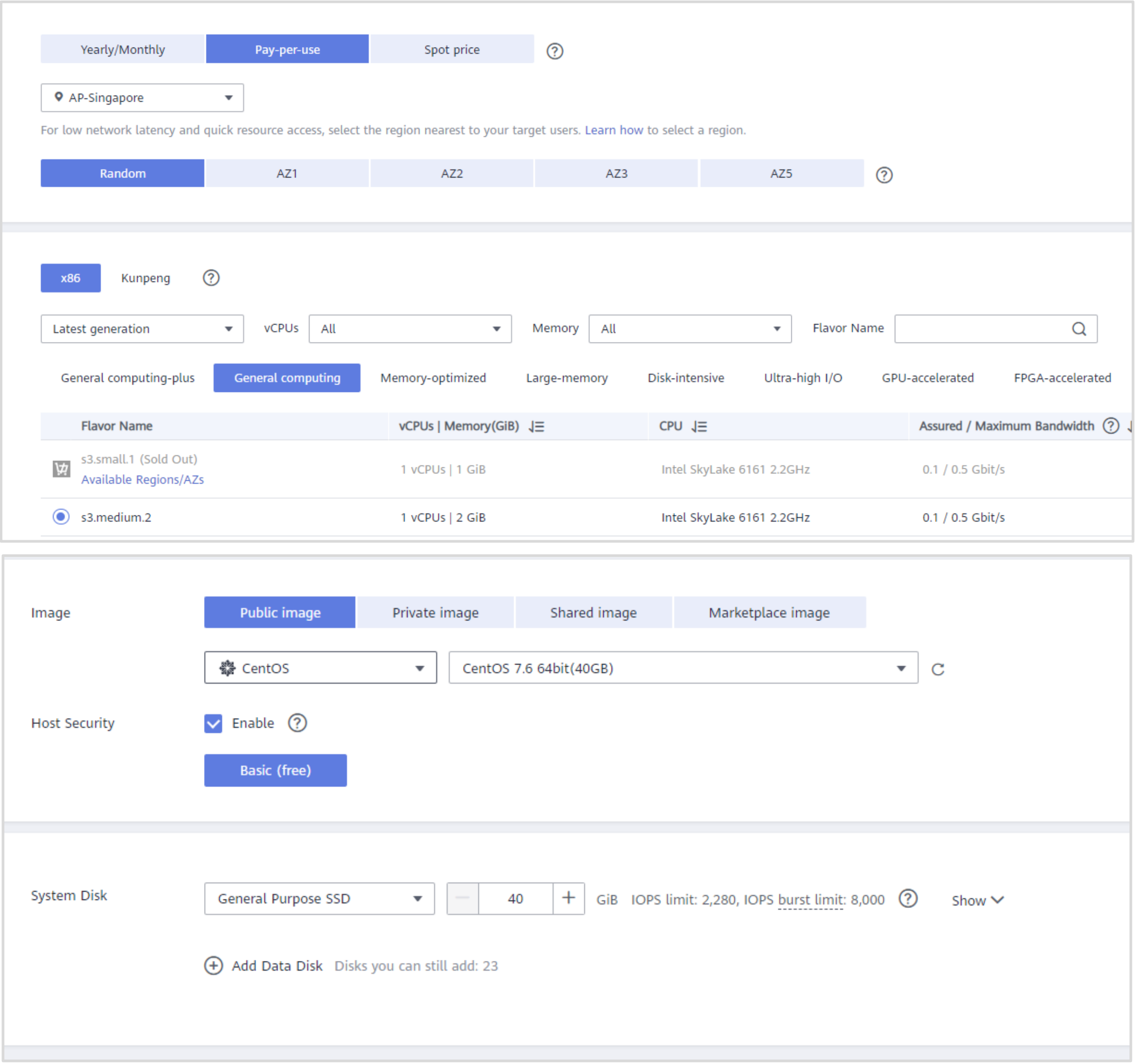
CBR backups can help you restore data in case anything happens to your ECS. To ensure data security, you a

Figure 2-14

ecs-03 configuration:

- Billing Mode: Pay-per-use
- Region: AP-Singapore
- AZ: Random
- CPU Architecture: x86
- Specifications: 1 vCPUs | 2 GiB

- Image: Public image | CentOS 7.6 64bit(40GB)
- Host Security: Enable | Basic (free)
- Network: vpc-3 | vpc-3-subnet | Automatically assign IP address
- Security Group: sg-4
- EIP: Not required
- System Disk: High I/O | 40 GiB
- ECS Name: ecs-03
- Password: User-defined (with the username of **root**)



For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

Flavor Name	vCPUs | Memory(GiB)	CPU	Assured / Maximum Bandwidth
s3.small.1 (Sold Out) Available Regions/AZs	1 vCPUs | 1 GiB	Intel SkyLake 6161 2.2GHz	0.1 / 0.5 Gbit/s
● s3.medium.2	1 vCPUs | 2 GiB	Intel SkyLake 6161 2.2GHz	0.1 / 0.5 Gbit/s

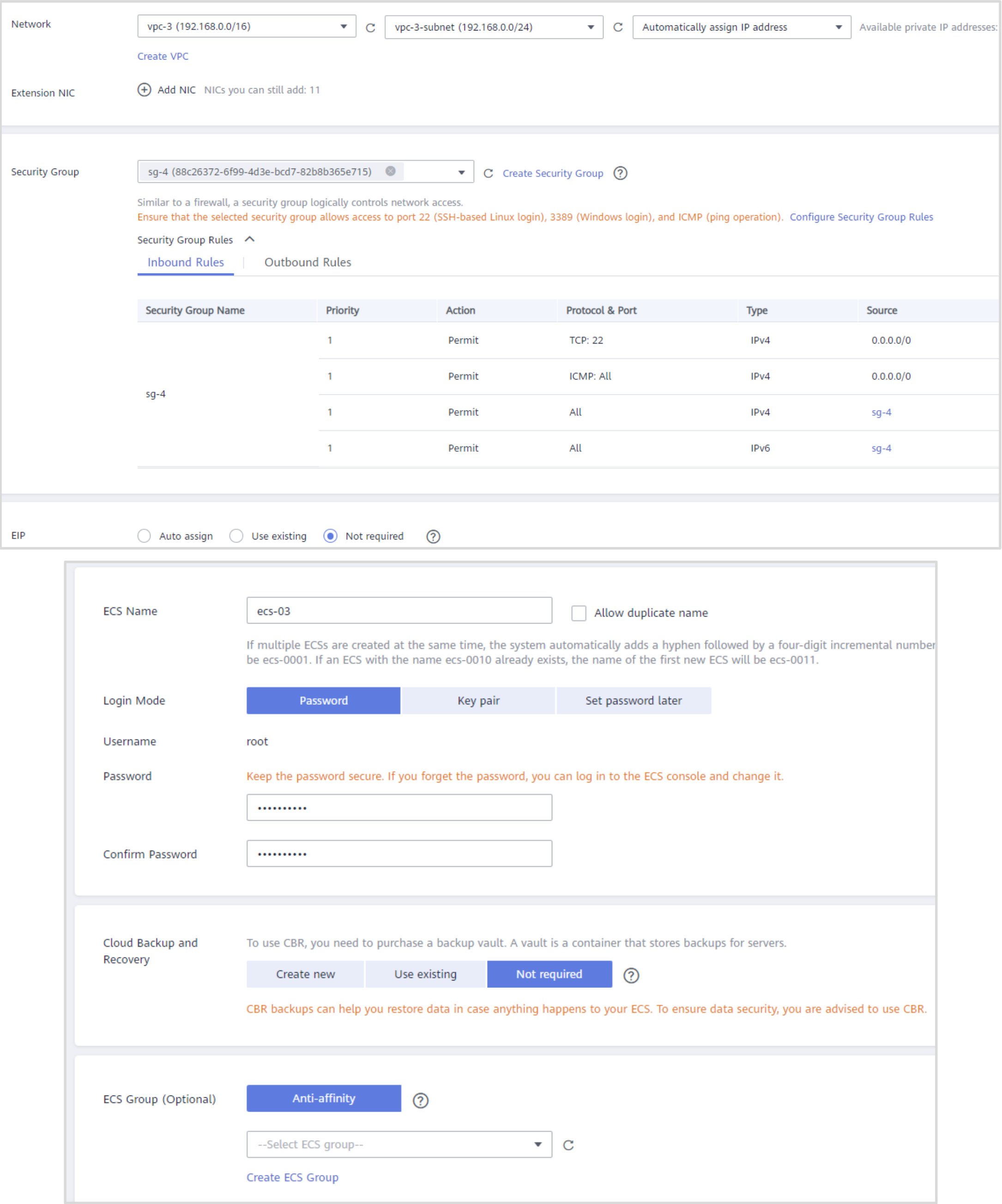
Image: Public image | Private image | Shared image | Marketplace image

CentOS | CentOS 7.6 64bit(40GB)

Host Security: ☑ Enable

Basic (free)

System Disk: General Purpose SSD | 40 GiB IOPS limit: 2,280, IOPS burst limit: 8,000



Network: vpc-3 (192.168.0.0/16) | vpc-3-subnet (192.168.0.0/24) | Automatically assign IP address | Available private IP addresses:

Create VPC

Extension NIC: Add NIC NICs you can still add: 11

Security Group: sg-4 (88c26372-6f99-4d3e-bcd7-82b8b365e715) Create Security Group

Similar to a firewall, a security group logically controls network access.

Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

Security Group Rules

Inbound Rules | Outbound Rules

Security Group Name	Priority	Action	Protocol & Port	Type	Source
sg-4	1	Permit	TCP: 22	IPv4	0.0.0.0/0
	1	Permit	ICMP: All	IPv4	0.0.0.0/0
	1	Permit	All	IPv4	sg-4
	1	Permit	All	IPv6	sg-4

EIP: ○ Auto assign ○ Use existing ● Not required

ECS Name: ecs-03 □ Allow duplicate name

If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a four-digit incremental number be ecs-0001. If an ECS with the name ecs-0010 already exists, the name of the first new ECS will be ecs-0011.

Login Mode: Password | Key pair | Set password later

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.

••••••••••

Confirm Password: ••••••••••

Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.

Create new | Use existing | Not required

CBR backups can help you restore data in case anything happens to your ECS. To ensure data security, you are advised to use CBR.

ECS Group (Optional): Anti-affinity

--Select ECS group--

Create ECS Group

Figure 2-15

2.2.4 Creating a VPC Peering Connection

Step 1 In the **AP-Singapore** region, choose **VPC Peering** on the **Network Console**, and click **Create VPC Peering Connection** in the upper right corner.

Note: This VPC peering connection is used to enable cloud resources in VPC 2 and VPC 3 to communicate.

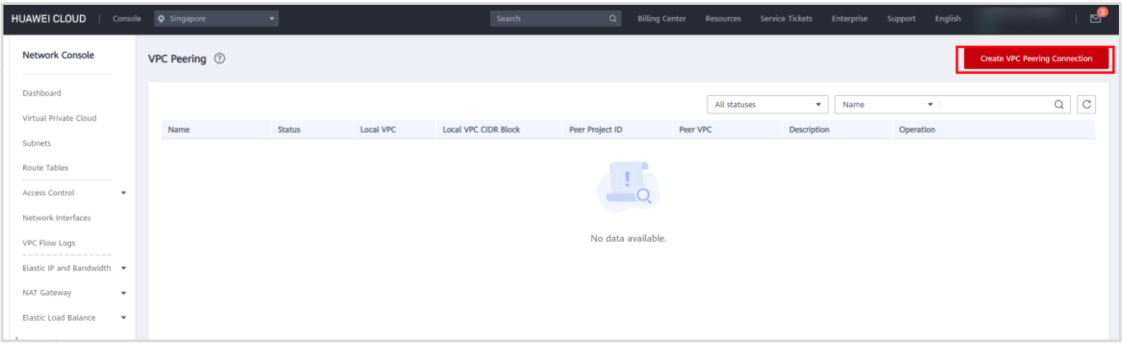
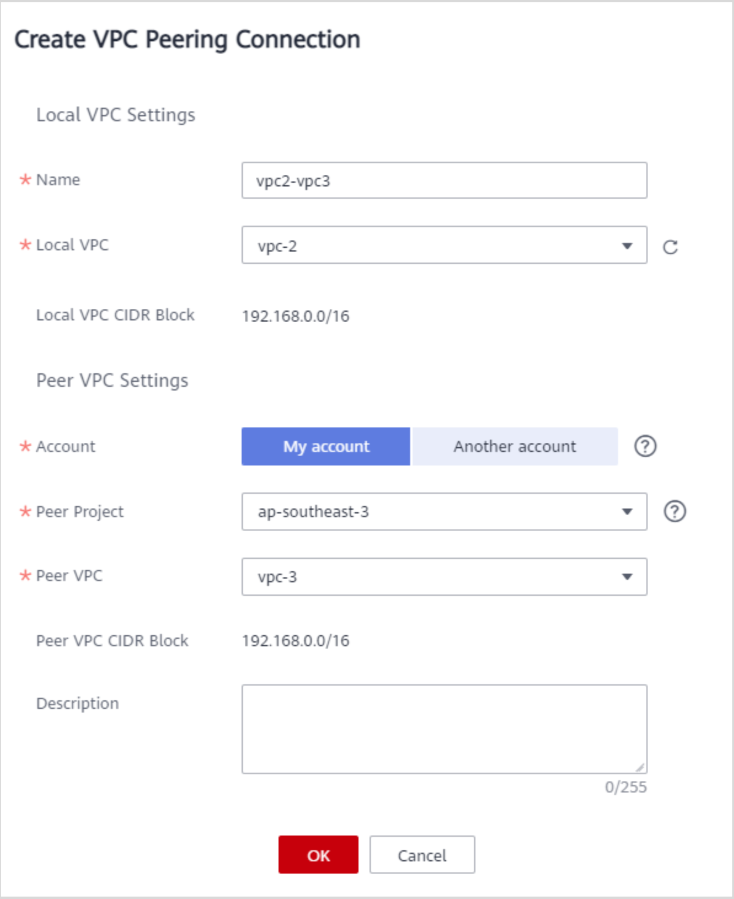


Figure 2-16

Step 2 Configure the parameters as follows:

- **Name: vpc2-vpc3**
- **Local VPC: vpc-2**
- **Account: My account**
- **Peer Project: ap-southeast-3**
- **Peer VPC: vpc-3**


Create VPC Peering Connection

Local VPC Settings

* Name: vpc2-vpc3

* Local VPC: vpc-2

Local VPC CIDR Block: 192.168.0.0/16

Peer VPC Settings

* Account: My account | Another account

* Peer Project: ap-southeast-3

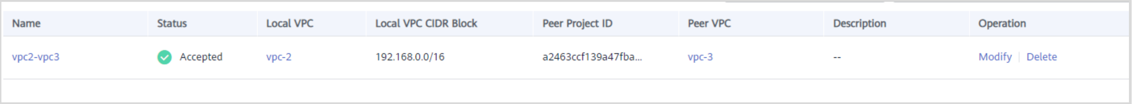
* Peer VPC: vpc-3

Peer VPC CIDR Block: 192.168.0.0/16

Description:

Figure 2-17

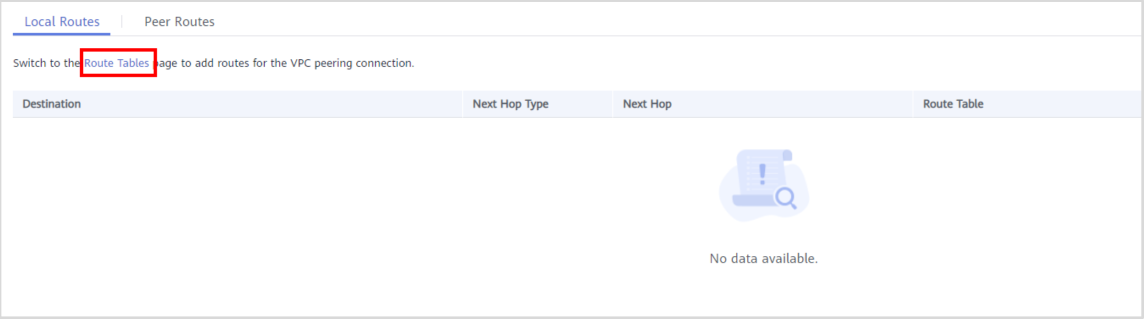
Step 3 Return to the VPC peering connection list, view the created VPC peering connection **vpc2-vpc3**, and click the connection name **vpc2-vpc3**.



Name	Status	Local VPC	Local VPC CIDR Block	Peer Project ID	Peer VPC	Description	Operation
vpc2-vpc3	✓ Accepted	vpc-2	192.168.0.0/16	a2463ccf139a47fba...	vpc-3	--	Modify | Delete

Figure 2-18

Step 4 Click **Route Tables** on the **Local Routes** tab to go to the details page of the **rtb-vpc-2** route table.



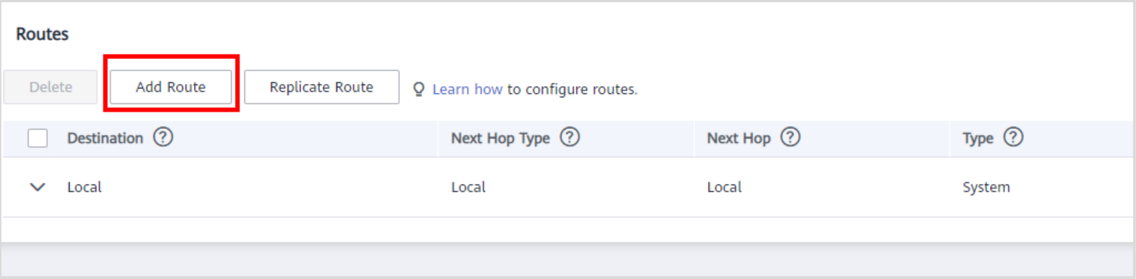
Switch to the Route Tables page to add routes for the VPC peering connection.

Destination	Next Hop Type	Next Hop	Route Table

No data available.

Figure 2-19

Step 5 Click **Add Route**.



Routes

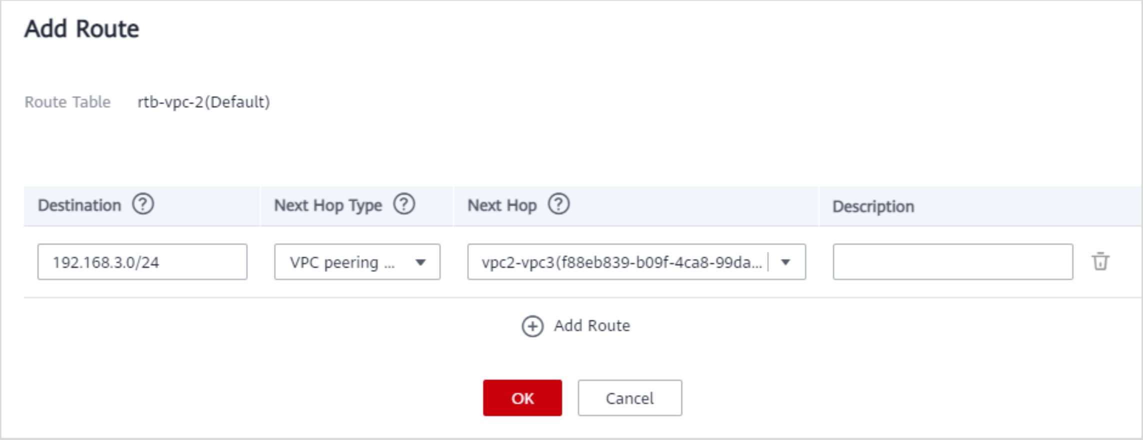
□ Destination ⓘ	Next Hop Type ⓘ	Next Hop ⓘ	Type ⓘ
Local	Local	Local	System

Figure 2-20

Step 6 Configure the parameters as follows and click **OK**.

Note: This route is added to the route table of VPC 2 to forward traffic to the subnet in VPC 3.

- **Destination: 192.168.3.0/24**
- **Next Hop Type: VPC peering connection**
- **Next Hop: vpc2-vpc3**



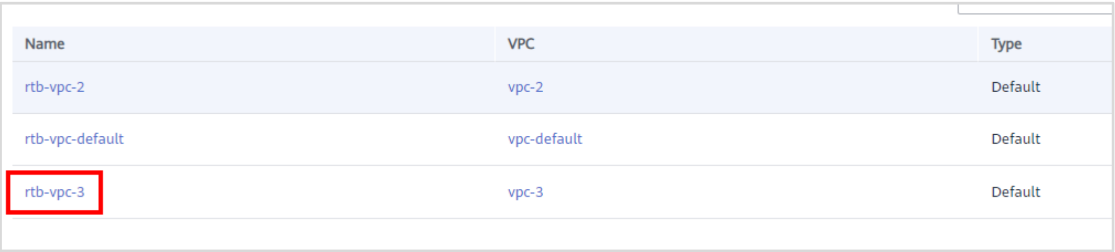
Add Route

Route Table rtb-vpc-2(Default)

Destination	Next Hop Type	Next Hop	Description
192.168.3.0/24	VPC peering ...	vpc2-vpc3(f88eb839-b09f-4ca8-99da...	

Figure 2-21

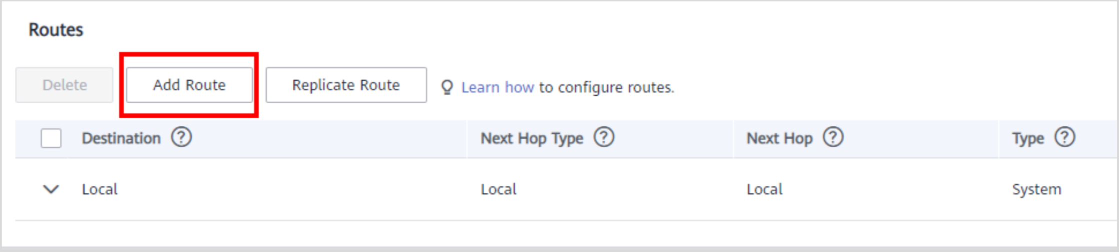
Step 7 In the route table list, click the name of the **rtb-vpc-3** route table to add a peer route.



Name	VPC	Type
rtb-vpc-2	vpc-2	Default
rtb-vpc-default	vpc-default	Default
rtb-vpc-3	vpc-3	Default

Figure 2-22

Step 8 Click **Add Route**.



Routes

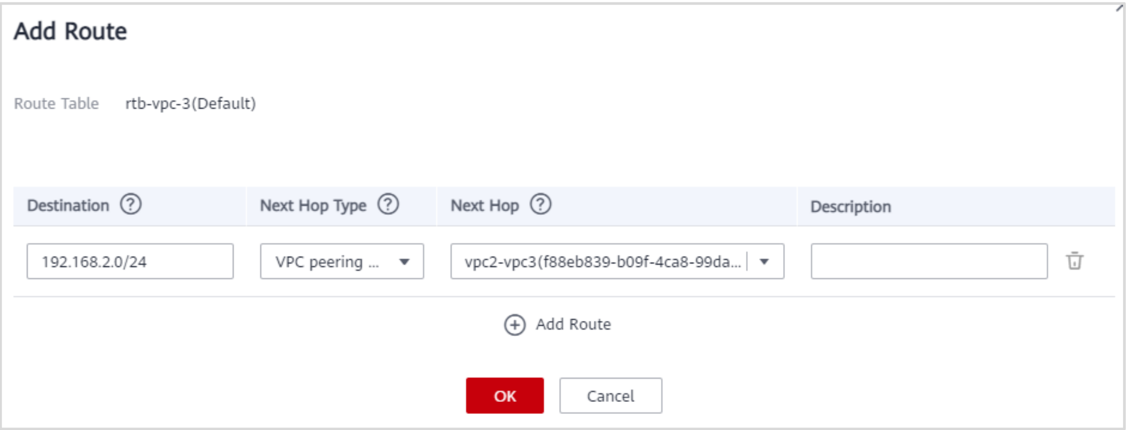
Destination	Next Hop Type	Next Hop	Type
Local	Local	Local	System

Figure 2-23

Step 9 Configure the parameters as follows and click **OK**.

Note: This route is added to the route table of VPC 3 to forward traffic to the subnet in VPC 2.

- **Destination: 192.168.2.0/24**
- **Next Hop Type: VPC peering connection**
- **Next Hop: vpc2-vpc3**



Add Route

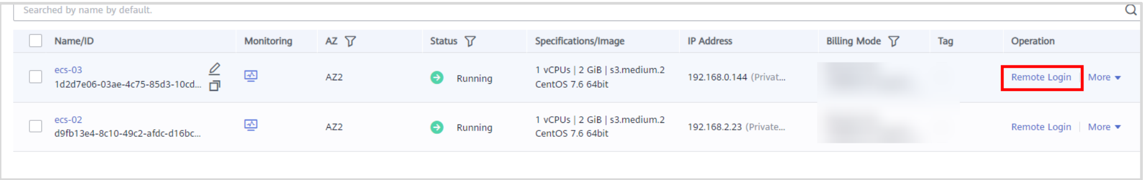
Route Table rtb-vpc-3(Default)

Destination ⓘ	Next Hop Type ⓘ	Next Hop ⓘ	Description
192.168.2.0/24	VPC peering ... ▾	vpc2-vpc3(f88eb839-b09f-4ca8-99da... ▾	

Figure 2-24

Step 10 Log in to ecs-03 and verify the communication between ecs-02 and ecs-03.

- Locate the row that contains ecs-03 and click **Remote Login** in the **Operation** column.

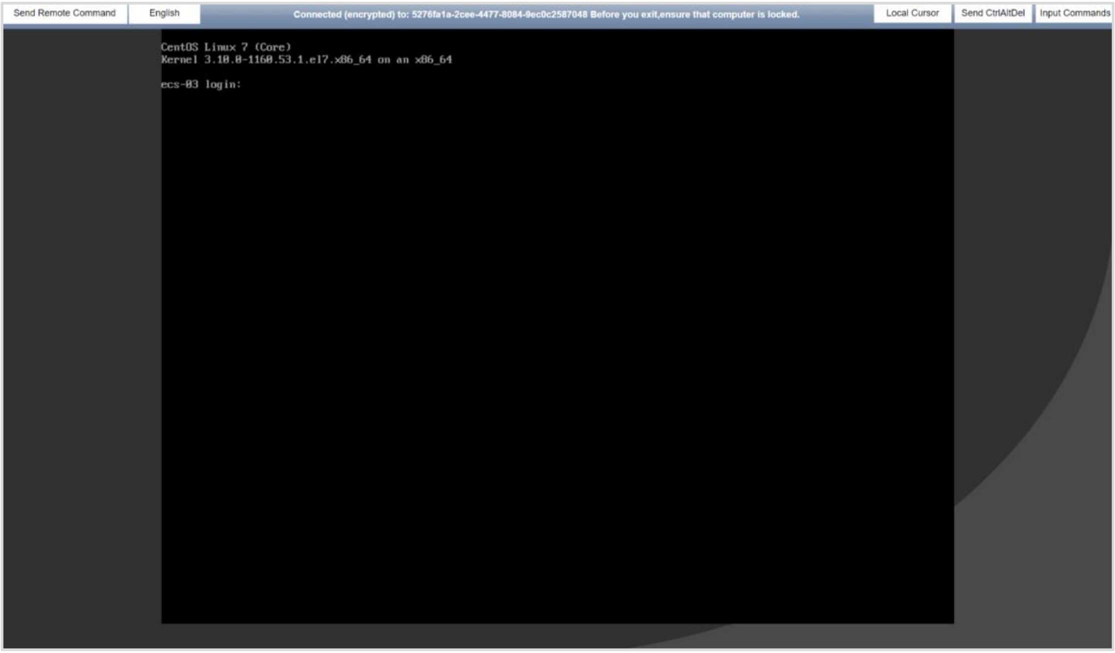


Searched by name by default.

□	Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mode	Tag	Operation
□	ecs-03 1d2d7e06-03ae-4c75-85d3-10cd...		AZ2	Running	1 vCPUs | 2 GiB | s3.medium.2 CentOS 7.6 64bit	192.168.0.144 (Privat...	[redacted]		Remote Login More ▾
□	ecs-02 d9fb13e4-8c10-49c2-afdc-d16bc...		AZ2	Running	1 vCPUs | 2 GiB | s3.medium.2 CentOS 7.6 64bit	192.168.2.23 (Private...	[redacted]		Remote Login | More ▾

Figure 2-25

- Enter the password to log in to ecs-03.



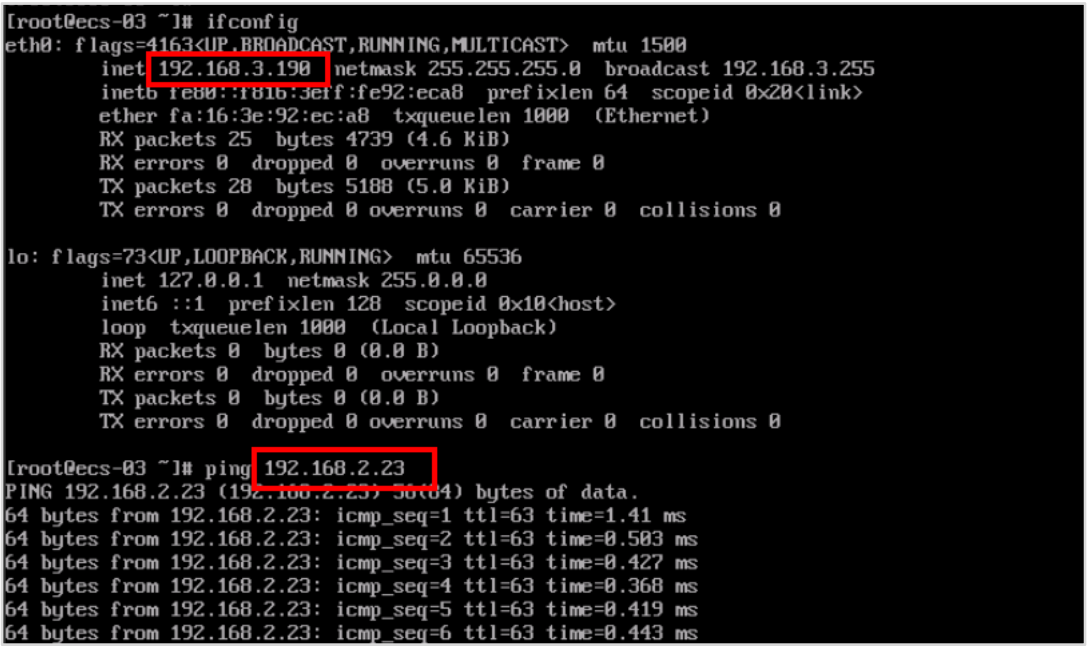
Connected (encrypted) to: 5276fa1a-2cee-4477-8084-9ec0c2587048 Before you exit,ensure that computer is locked.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.53.1.el7.x86_64 on an x86_64

ecs-03 login:
```

Figure 2-26

- Ping ecs-02 from ecs-03 to test the communication between them.

Note: 192.168.2.23 is the private IP address of ecs-02 in the VPC.



```
[root@ecs-03 ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.3.190  netmask 255.255.255.0  broadcast 192.168.3.255
        inet6 fe80::f816:3eff:fe92:eca8  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:92:ec:a8  txqueuelen 1000  (Ethernet)
        RX packets 25  bytes 4739 (4.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 5188 (5.0 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

[root@ecs-03 ~]# ping 192.168.2.23
PING 192.168.2.23 (192.168.2.23) 56(84) bytes of data.
64 bytes from 192.168.2.23: icmp_seq=1 ttl=63 time=1.41 ms
64 bytes from 192.168.2.23: icmp_seq=2 ttl=63 time=0.503 ms
64 bytes from 192.168.2.23: icmp_seq=3 ttl=63 time=0.427 ms
64 bytes from 192.168.2.23: icmp_seq=4 ttl=63 time=0.368 ms
64 bytes from 192.168.2.23: icmp_seq=5 ttl=63 time=0.419 ms
64 bytes from 192.168.2.23: icmp_seq=6 ttl=63 time=0.443 ms
```

Figure 2-27

2.2.5 Configuring a VPN

Step 1 In the **CN-Hong Kong** region, click **Console**, choose **Virtual Private Network** > **VPN Gateway**, and click **Buy VPN Gateway**.

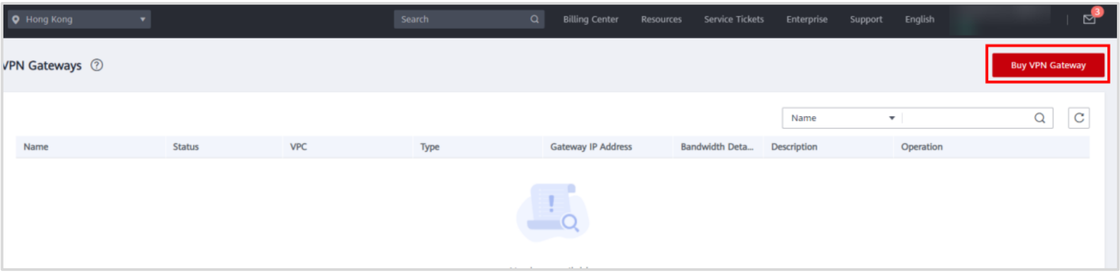
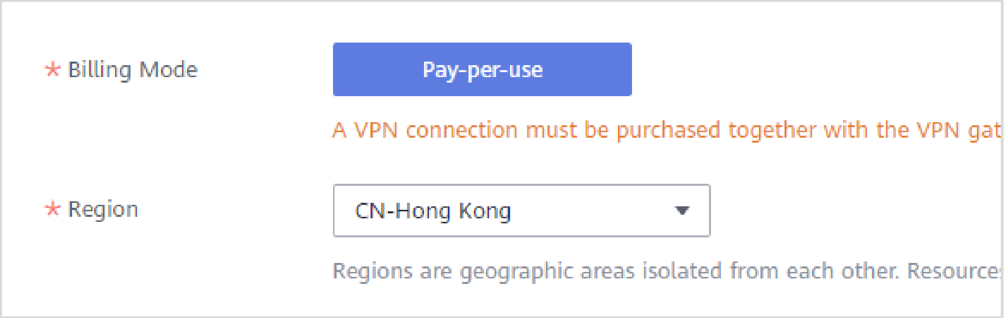


Figure 2-28

Step 2 Set the following parameters to create a VPN gateway.

Note: This VPN gateway connects the on-premises site in the CN-Hong Kong region to cloud resources in the AP-Singapore region.

- **Billing Mode**: **Pay-per-use**
- **Region**: **CN-Hong Kong**



* Billing Mode: Pay-per-use

A VPN connection must be purchased together with the VPN gat

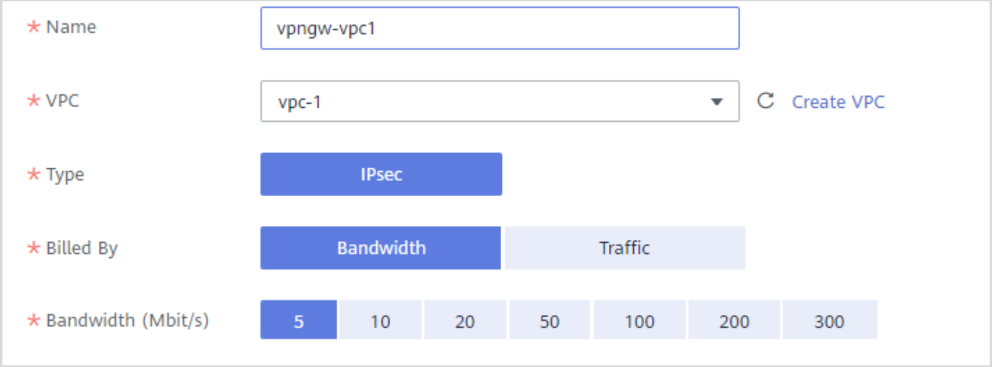
* Region: CN-Hong Kong

Regions are geographic areas isolated from each other. Resource

Figure 2-29

VPN gateway configuration:

- **Name**: **vpngw-vpc1**
- **VPC**: **vpc-1**
- **Type**: **IPsec**
- **Billed By**: **Bandwidth**
- **Bandwidth (Mbit/s)**: **5 Mbit/s**



* Name: vpngw-vpc1

* VPC: vpc-1

* Type: IPsec

* Billed By: Bandwidth | Traffic

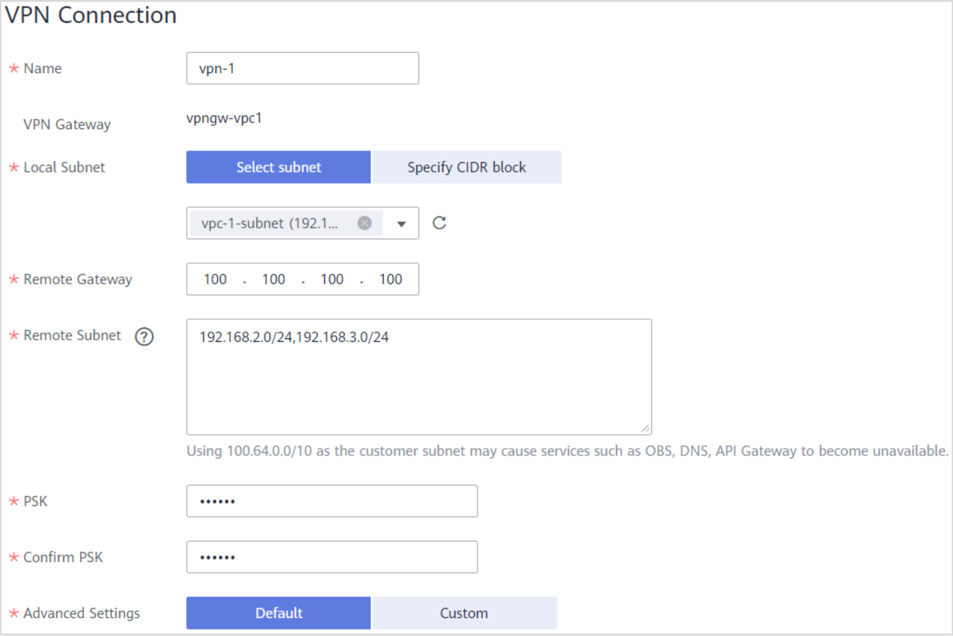
* Bandwidth (Mbit/s): 5 | 10 | 20 | 50 | 100 | 200 | 300

Figure 2-30

VPN connection configuration:

- **Name**: **vpn-1**
- **Local Subnet**: **Select subnet** | **vpc-1-subnet**
- **Remote Gateway**: **100.100.100.100** (Change this IP address to the actual IP address of the remote gateway after you create the remote gateway.)
- **Remote Subnet**: **192.168.2.0/24,192.168.3.0/24**

  Note: Enter the subnets of both VPC 2 and VPC 3. This configuration specifies the traffic of interest in IPsec on the local end. IPsec encapsulation will be performed on the specified traffic.
- **PSK**: User-defined



VPN Connection

* Name: vpn-1

VPN Gateway: vpngw-vpc1

* Local Subnet: [✓ Select subnet] Specify CIDR block

vpc-1-subnet (192.1...

* Remote Gateway: 100 . 100 . 100 . 100

* Remote Subnet: 192.168.2.0/24,192.168.3.0/24

Using 100.64.0.0/10 as the customer subnet may cause services such as OBS, DNS, API Gateway to become unavailable.

* PSK: ••••••

* Confirm PSK: ••••••

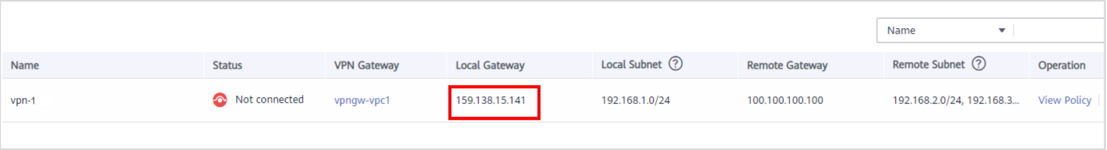
* Advanced Settings: [✓ Default] Custom

Figure 2-31

Step 3 Confirm the configuration and click **Submit**.

Step 4 View the created VPN gateway, and record its IP address (159.138.15.141 in this example).

Note: You need to enter this VPN gateway IP address when creating a remote VPN gateway.



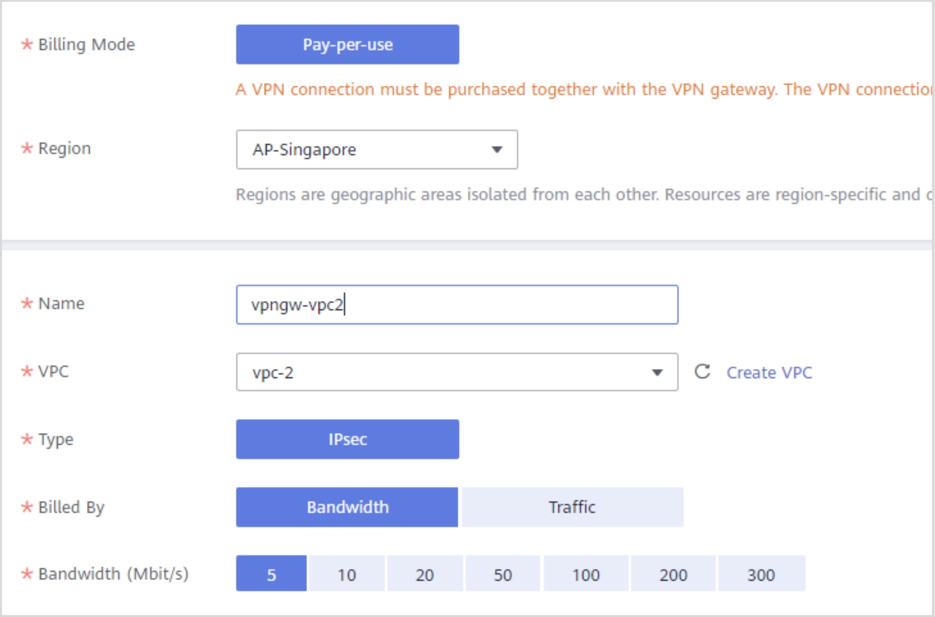
Name	Status	VPN Gateway	Local Gateway	Local Subnet ?	Remote Gateway	Remote Subnet ?	Operation
vpn-1	Not connected	vpngw-vpc1	159.138.15.141	192.168.1.0/24	100.100.100.100	192.168.2.0/24, 192.168.3...	View Policy

Figure 2-32

Step 5 In the **AP-Singapore** region, click **Console**, choose **Virtual Private Network** > **VPN Gateway**, and click **Buy VPN Gateway**. Set parameters as follows to create a VPN gateway:

Note: This VPN gateway is created on the cloud (AP-Singapore region) to connect to the VPN gateway at the on-premises site (CN-Hong Kong region).

- Region: AP-Singapore
- Name: vpngw-vpc2
- VPC: vpc-2
- Type: IPsec
- Billed By: Bandwidth
- Bandwidth (Mbit/s): 5



* Billing Mode: Pay-per-use

A VPN connection must be purchased together with the VPN gateway. The VPN connectio

* Region: AP-Singapore

Regions are geographic areas isolated from each other. Resources are region-specific and c

* Name: vpngw-vpc2

* VPC: vpc-2

* Type: IPsec

* Billed By: Bandwidth | Traffic

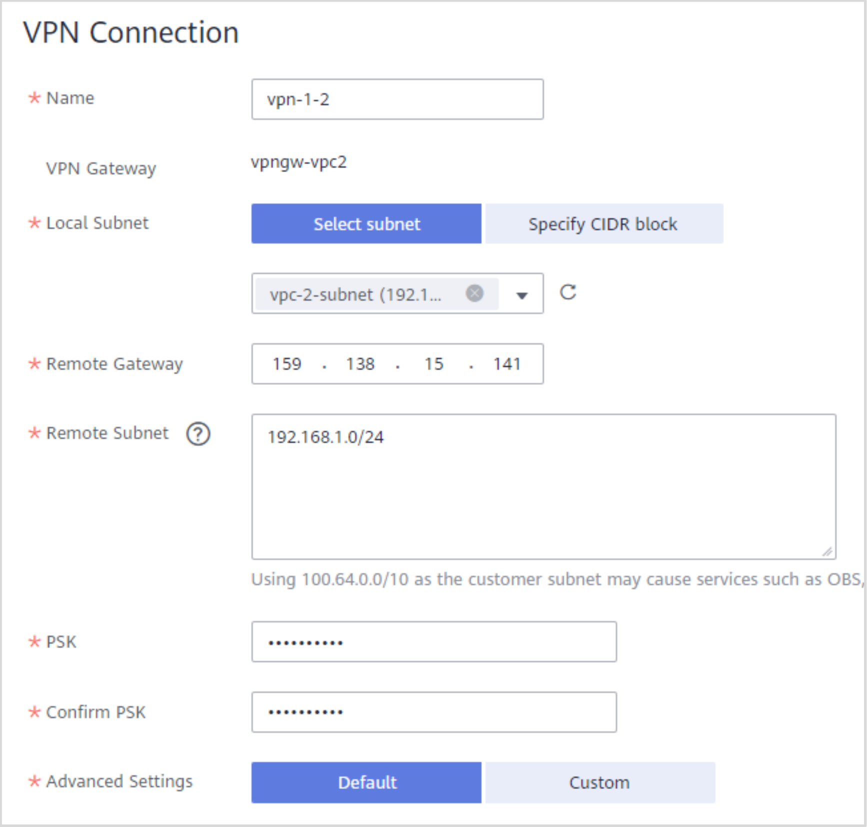
* Bandwidth (Mbit/s): 5 | 10 | 20 | 50 | 100 | 200 | 300

Figure 2-33

Step 6 Set the following parameters to create a VPN connection.

- **Name**: **vpn-1-2**
- **Local Subnet**: **Select subnet** | **vpc-2-subnet**
- **Remote Gateway**: **159.138.15.141** (IP address of the VPN gateway created in Step 2)
- **Remote Subnet**: **192.168.1.0/24**

  Note: Enter the subnet of VPC 1. This configuration specifies the traffic of interest in IPsec on the local end. IPsec encapsulation will be performed on the specified traffic.
- **PSK**: User-defined
- **Advanced Settings**: **Default**



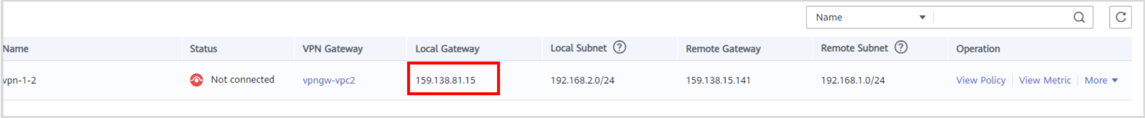
VPN Connection

* Name	vpn-1-2
VPN Gateway	vpngw-vpc2
* Local Subnet	Select subnet / Specify CIDR block vpc-2-subnet (192.1...
* Remote Gateway	159 . 138 . 15 . 141
* Remote Subnet	192.168.1.0/24 Using 100.64.0.0/10 as the customer subnet may cause services such as OBS,
* PSK	••••••••••
* Confirm PSK	••••••••••
* Advanced Settings	Default / Custom

Figure 2-34

Step 7 View the created VPN gateway, and record its IP address (159.138.81.15 in this example).

Note: You need to change the value of **Remote Gateway** to this gateway IP address for the VPN gateway in the CN-Hong Kong region.



Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet	Operation
vpn-1-2	Not connected	vpngw-vpc2	159.138.81.15	192.168.2.0/24	159.138.15.141	192.168.1.0/24	View Policy | View Metric | More

Figure 2-35

Step 8 Switch to the **CN-Hong Kong** region, and choose **Virtual Private Network** > **VPN Connections**.

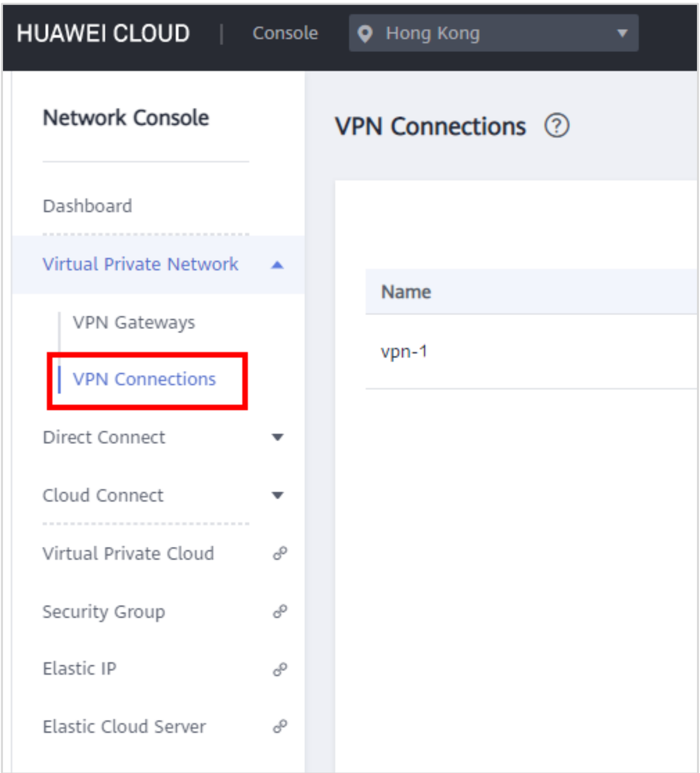
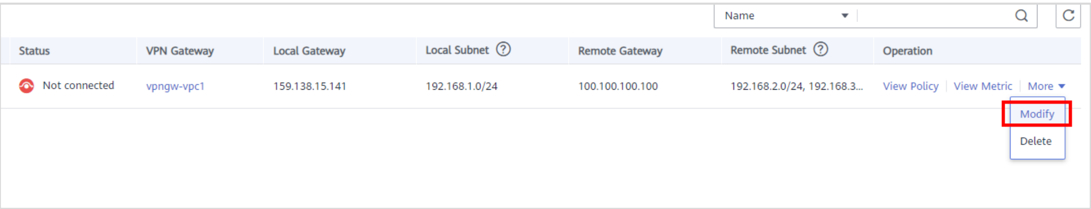


Figure 2-36

Step 9 Choose **More** > **Modify** in the **Operation** column.

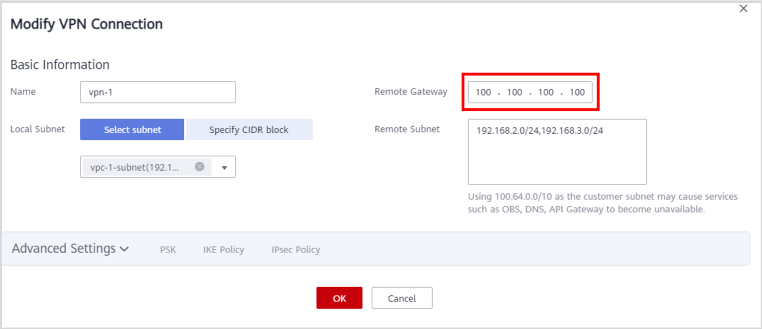


Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet	Operation
Not connected	vpngw-vpc1	159.138.15.141	192.168.1.0/24	100.100.100.100	192.168.2.0/24, 192.168.3...	View Policy | View Metric | More

Figure 2-37

Step 10 Change the value of **Remote Gateway** to 159.138.81.15, and click **OK**.

- Before change



Name: vpn-1

Local Subnet: vpc-1-subnet(192.1...

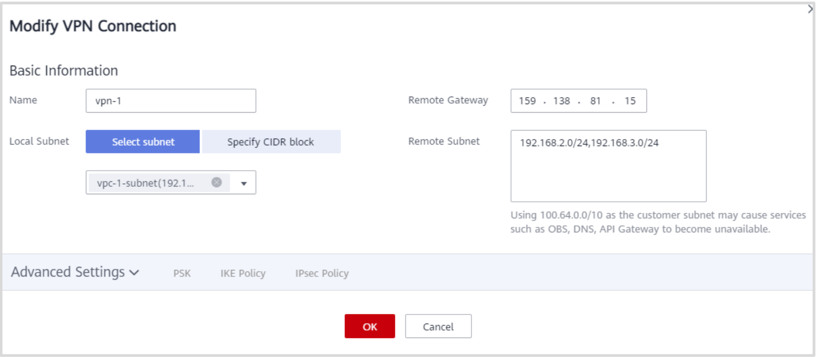
Remote Gateway: 100 . 100 . 100 . 100

Remote Subnet: 192.168.2.0/24,192.168.3.0/24

Using 100.64.0.0/10 as the customer subnet may cause services such as OBS, DNS, API Gateway to become unavailable.

Figure 2-38

- After change



Modify VPN Connection

Basic Information

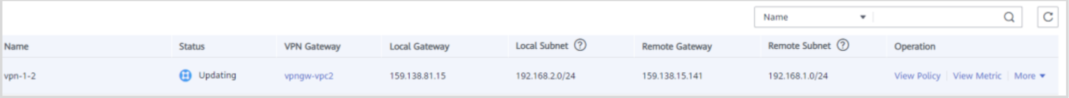
Name	vpn-1	Remote Gateway	159 . 138 . 81 . 15
Local Subnet	Select subnet / Specify CIDR block vpc-1-subnet(192.1...	Remote Subnet	192.168.2.0/24,192.168.3.0/24

Using 100.64.0.0/10 as the customer subnet may cause services such as OBS, DNS, API Gateway to become unavailable.

Figure 2-39

Step 11 Check that the VPN connection status is **Updating**.

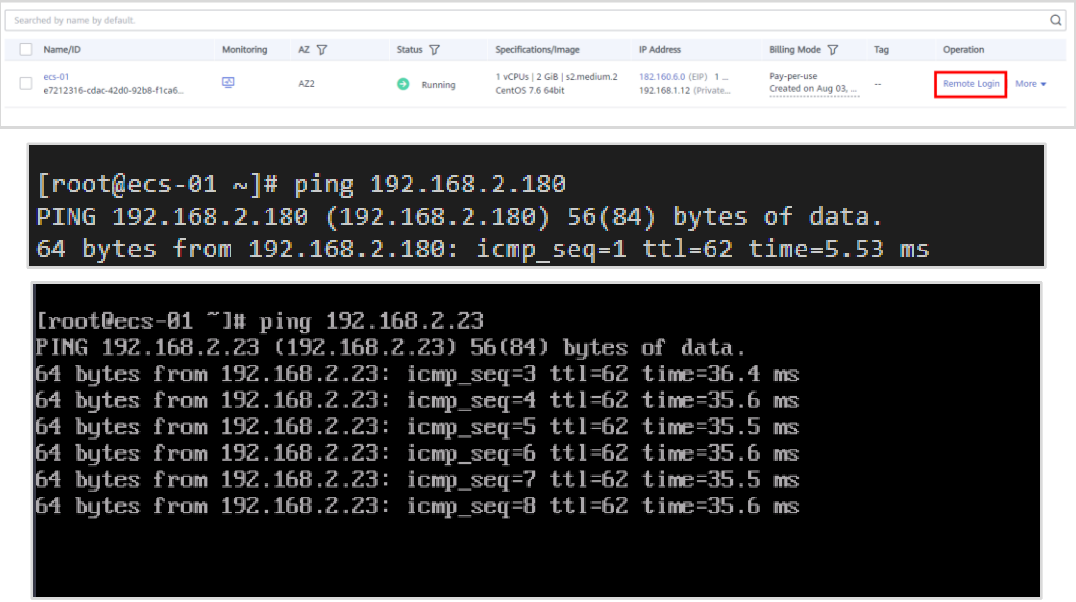
Note: When no traffic triggers IPsec SA negotiation, the VPN connection remains in the Updating state.



Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet	Operation
vpn-1-2	Updating	vpngw-vpc2	159.138.81.15	192.168.2.0/24	159.138.15.141	192.168.1.0/24	View Policy | View Metric | More

Figure 2-40

Step 12 Log in to ECS01, and run the **ping** command to test connectivity with ECS02. Then, traffic of interest in IPsec is sent, which triggers IPsec SA negotiation.



Searched by name by default.

□	Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mode	Tag	Operation
□	ecs-01 e7212316-cdac-42d0-92b8-f1ca6...		AZ2	Running	1 vCPUs | 2 GiB | s2.medium.2 CentOS 7.6 64bit	182.160.6.0 (EIP) 1 ... 192.168.1.12 (Private...	Pay-per-use Created on Aug 03, ...	--	Remote Login More

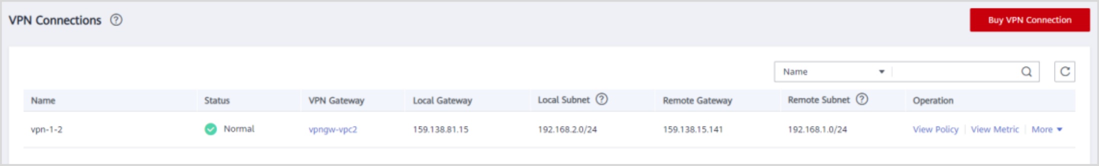
```
[root@ecs-01 ~]# ping 192.168.2.180
PING 192.168.2.180 (192.168.2.180) 56(84) bytes of data.
64 bytes from 192.168.2.180: icmp_seq=1 ttl=62 time=5.53 ms
```

```
[root@ecs-01 ~]# ping 192.168.2.23
PING 192.168.2.23 (192.168.2.23) 56(84) bytes of data.
64 bytes from 192.168.2.23: icmp_seq=3 ttl=62 time=36.4 ms
64 bytes from 192.168.2.23: icmp_seq=4 ttl=62 time=35.6 ms
64 bytes from 192.168.2.23: icmp_seq=5 ttl=62 time=35.5 ms
64 bytes from 192.168.2.23: icmp_seq=6 ttl=62 time=35.6 ms
64 bytes from 192.168.2.23: icmp_seq=7 ttl=62 time=35.5 ms
64 bytes from 192.168.2.23: icmp_seq=8 ttl=62 time=35.6 ms
```

Figure 2-41

Step 13 Refresh the VPN connection page. The VPN connection status is changed to **Normal**.

This means that the VPN connection is successfully established, IPsec SA negotiation is successful, and packets can be properly transmitted.



VPN Connections

Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet	Operation
vpn-1-2	● Normal	vpngw-vpc2	159.138.81.15	192.168.2.0/24	159.138.15.141	192.168.1.0/24	View Policy | View Metric | More

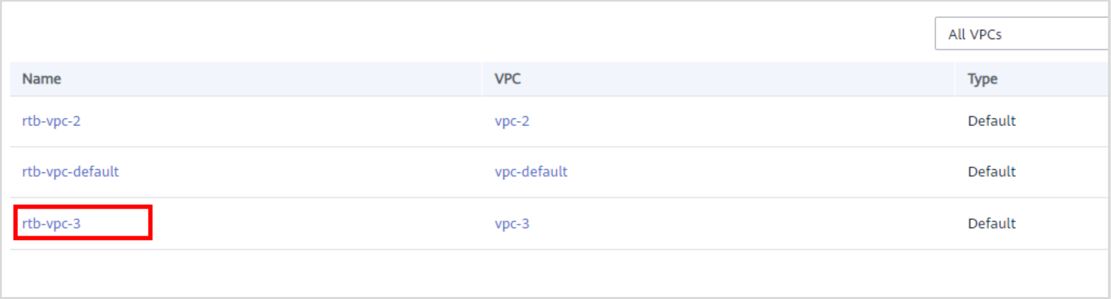
Figure 2-42

2.2.6 Configuring ECS01 to Manage ECS03

When the VPN connection is in normal state, ECS01 and ECS02 can communicate with each other. To use ECS01 to log in to ECS03 for management, perform the following operations:

- Add a route to 192.168.1.0/24 (subnet in VPC 1) to the route table of VPC 3, with the next hop set to the VPC peering connection with VPC 2.
- Change the value of **Local Subnet** to **Specify CIDR block** for the VPN connection of VPC 2, and add the CIDR block 192.168.3.0/24.

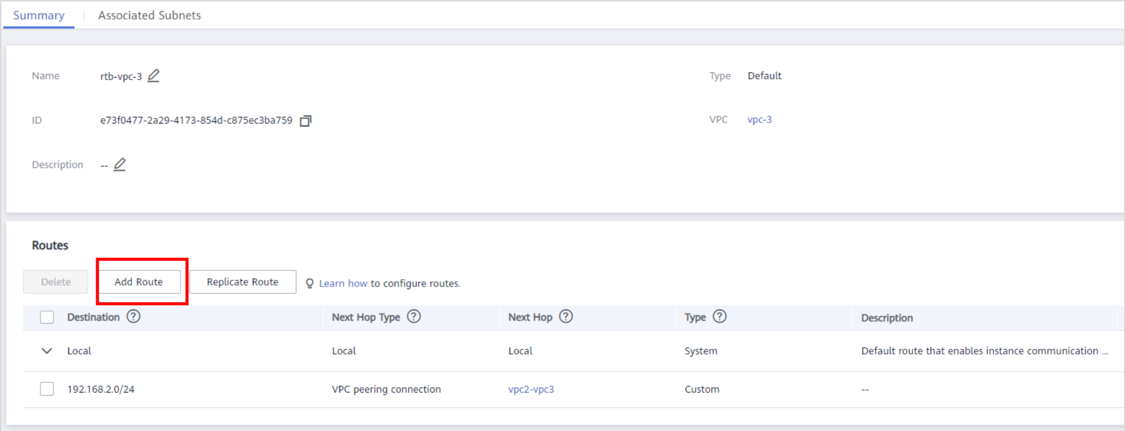
Step 1 Go to the route table management page of the AP-Singapore region, and select the **rtb-vpc-3** route table of VPC 3.



Name	VPC	Type
rtb-vpc-2	vpc-2	Default
rtb-vpc-default	vpc-default	Default
rtb-vpc-3	vpc-3	Default

Figure 2-43

Step 2 Click **Add Route**.



Name rtb-vpc-3

Type Default

ID e73f0477-2a29-4173-854d-c875ec3ba759

VPC vpc-3

Description --

Routes

Learn how to configure routes.

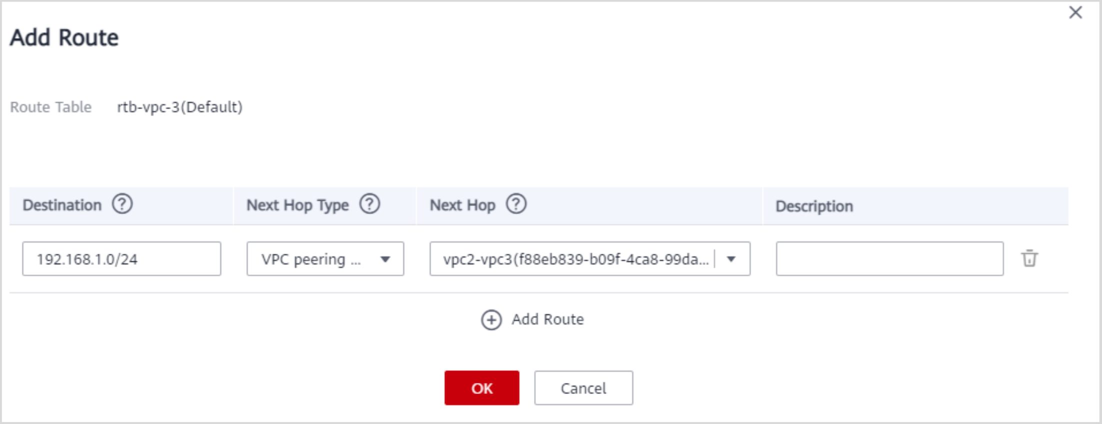
□ Destination	Next Hop Type	Next Hop	Type	Description
Local	Local	Local	System	Default route that enables instance communication ...
□ 192.168.2.0/24	VPC peering connection	vpc2-vpc3	Custom	--

Figure 2-44

Step 3 Add a route to 192.168.1.0/24, with the next hop set to a VPC peering connection. Then, click **Confirm**.

Note: This configuration adds a route destined for VPC 1 to the route table of VPC 3.

- **Destination: 192.168.1.0/24**
- **Next Hop Type: VPC peering connection**
- **Next Hop: vpc2-vpc3**



Add Route

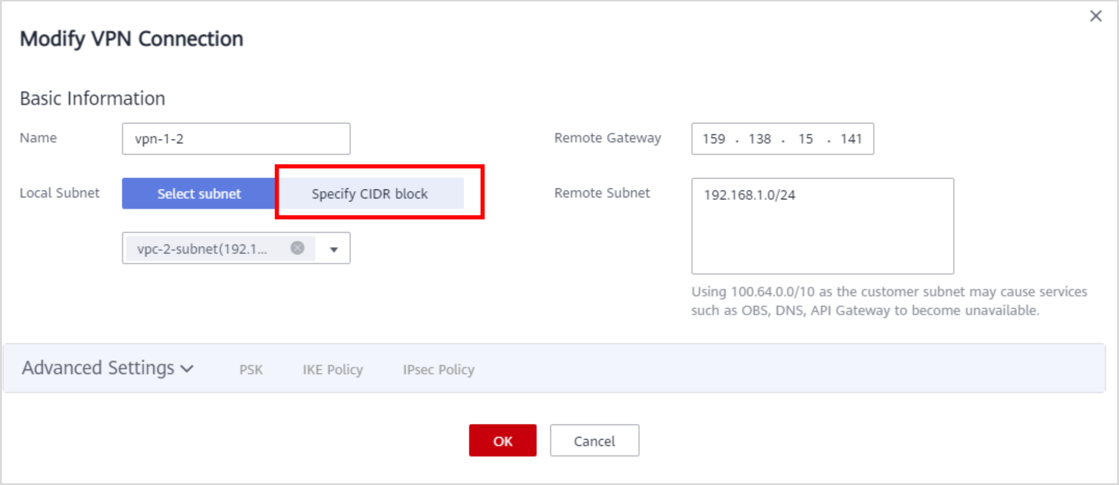
Route Table rtb-vpc-3(Default)

Destination	Next Hop Type	Next Hop	Description
192.168.1.0/24	VPC peering ...	vpc2-vpc3(f88eb839-b09f-4ca8-99da...	

Figure 2-45

Step 4 In the AP-Singapore region, click **Console**, and choose **Virtual Private Network** > **VPN Connections**. Change the value of **Local Subnet** to **Specify CIDR block** for the VPN connection **vpn-1-2**, and add the CIDR block 192.168.3.0/24.

- Before change



Modify VPN Connection

Basic Information

Name: vpn-1-2

Remote Gateway: 159 . 138 . 15 . 141

Local Subnet: Select subnet | Specify CIDR block

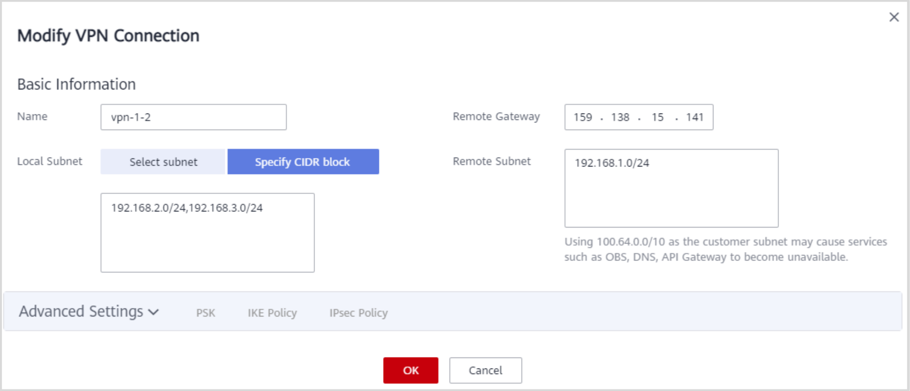
vpc-2-subnet(192.1...

Remote Subnet: 192.168.1.0/24

Using 100.64.0.0/10 as the customer subnet may cause services such as OBS, DNS, API Gateway to become unavailable.

Figure 2-46

- After change



Modify VPN Connection

Basic Information

Name: vpn-1-2

Remote Gateway: 159 . 138 . 15 . 141

Local Subnet: Select subnet / Specify CIDR block

192.168.2.0/24,192.168.3.0/24

Remote Subnet: 192.168.1.0/24

Using 100.64.0.0/10 as the customer subnet may cause services such as OBS, DNS, API Gateway to become unavailable.

Figure 2-47

Note: After the modification, VPC 3 has a route to 192.168.1.0/24, and the local subnet of the VPN connection in the AP-Singapore region contains the CIDR block 192.168.3.0/24. When packets on 192.168.3.0/24 reach VPC 2, IPsec encapsulation is triggered for the packets.

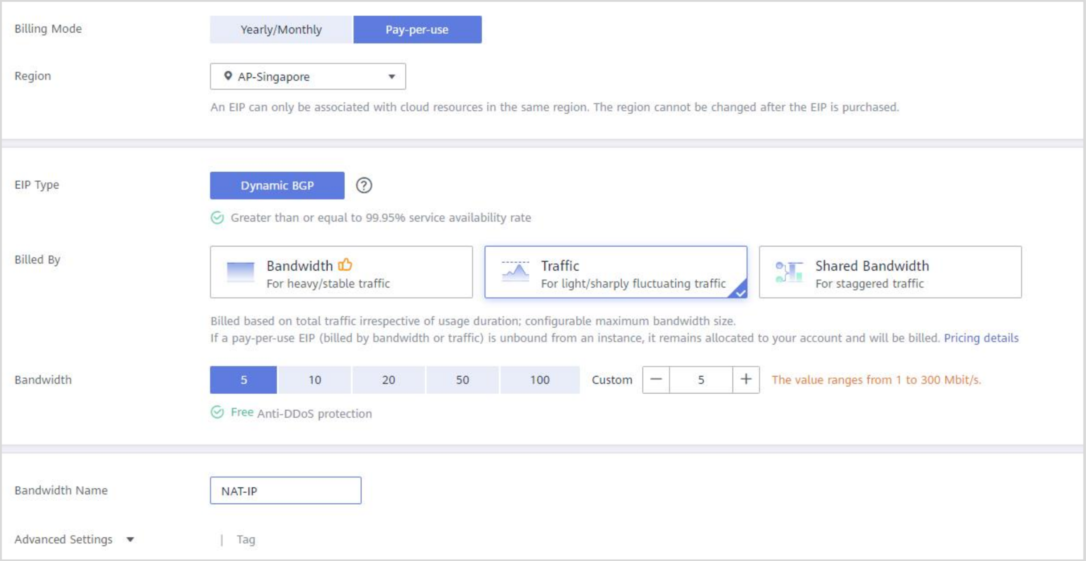
2.2.7 Creating a NAT Gateway

Step 1 In the **AP-Singapore** region, choose **Virtual Private Cloud** under **Networking**. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **EIPs**, click **Buy EIP** in the upper right corner, set the following parameters, and click **Next**.

This NAT gateway is created in vpc-2 to enable Internet access for resources in **vpc-2** and **vpc-3**.

- **Billing Mode**: **Pay-per-use**
- **Region**: **AP-Singapore**
- **EIP Type**: **Dynamic BGP**
- **Billed By**: **Traffic**
- **Bandwidth (Mbit/s)**: **5**
- **Bandwidth Name**: **NAT-IP**

Retain the default settings for other parameters.



Billing Mode: Yearly/Monthly | Pay-per-use

Region: AP-Singapore

An EIP can only be associated with cloud resources in the same region. The region cannot be changed after the EIP is purchased.

EIP Type: Dynamic BGP

Greater than or equal to 99.95% service availability rate

Billed By: Bandwidth (For heavy/stable traffic) | Traffic (For light/sharply fluctuating traffic) | Shared Bandwidth (For staggered traffic)

Billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size.
If a pay-per-use EIP (billed by bandwidth or traffic) is unbound from an instance, it remains allocated to your account and will be billed. Pricing details

Bandwidth: 5 | 10 | 20 | 50 | 100 | Custom — 5 + The value ranges from 1 to 300 Mbit/s.

Free Anti-DDoS protection

Bandwidth Name: NAT-IP

Advanced Settings | Tag

Figure 2-48

Step 2 In the **AP-Singapore** region, choose **NAT Gateway** under **Networking**. On the displayed **Public NAT Gateway** page, and click **Buy Public NAT Gateway** in the upper right corner.

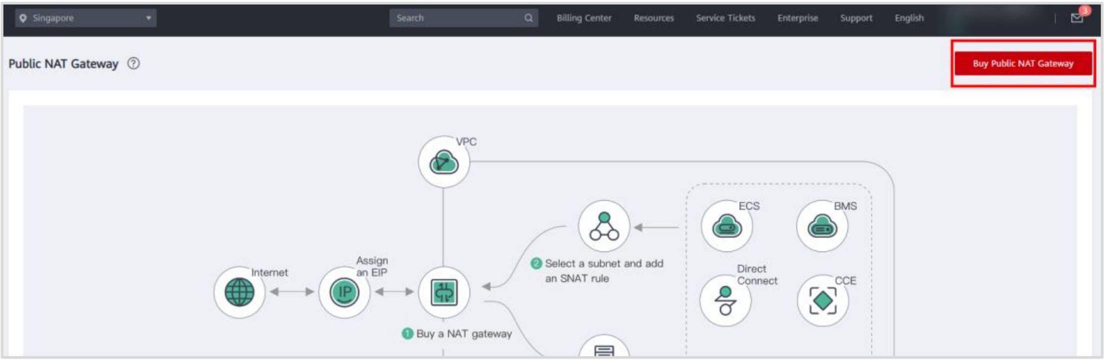
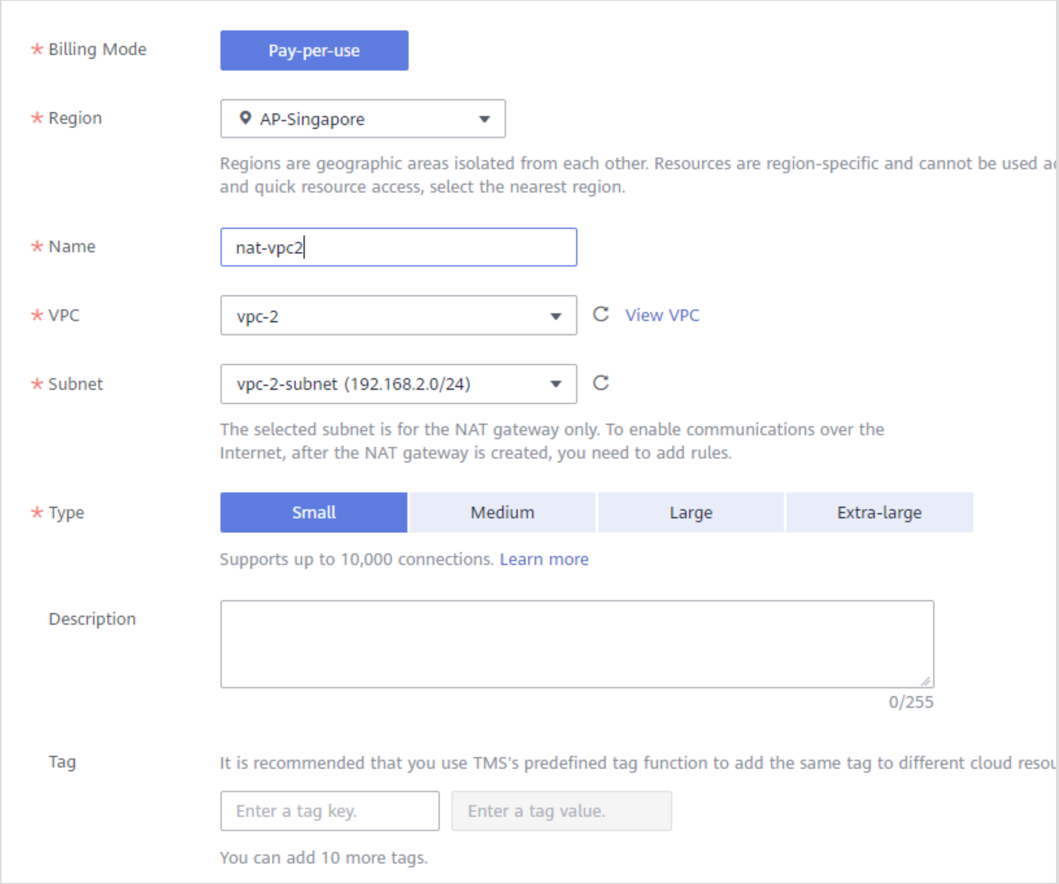


Figure 2-49

Step 3 Configure required parameters.

- **Billing Mode: Pay-per-use**
- **Region: AP-Singapore**
- **Name: nat-vpc2**
- **VPC: vpc-2**
- **Subnet: vpc-2-subnet**
- **Specifications : Small**



* Billing Mode: Pay-per-use

* Region: AP-Singapore

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used a and quick resource access, select the nearest region.

* Name: nat-vpc2

* VPC: vpc-2

* Subnet: vpc-2-subnet (192.168.2.0/24)

The selected subnet is for the NAT gateway only. To enable communications over the Internet, after the NAT gateway is created, you need to add rules.

* Type: Small | Medium | Large | Extra-large

Supports up to 10,000 connections. Learn more

Description

0/255

Tag

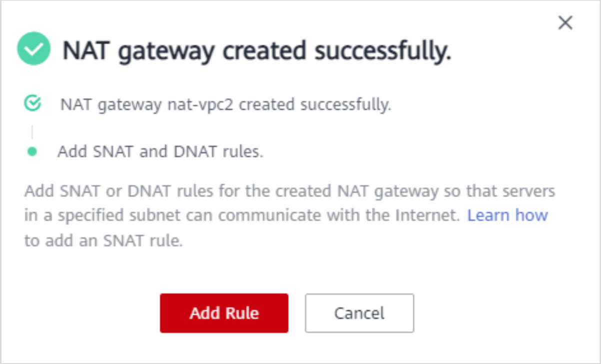
It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resou

Enter a tag key. Enter a tag value.

You can add 10 more tags.

Figure 2-50

Step 4 In the displayed dialog box, click **Add Rule**.



NAT gateway created successfully.

NAT gateway nat-vpc2 created successfully.

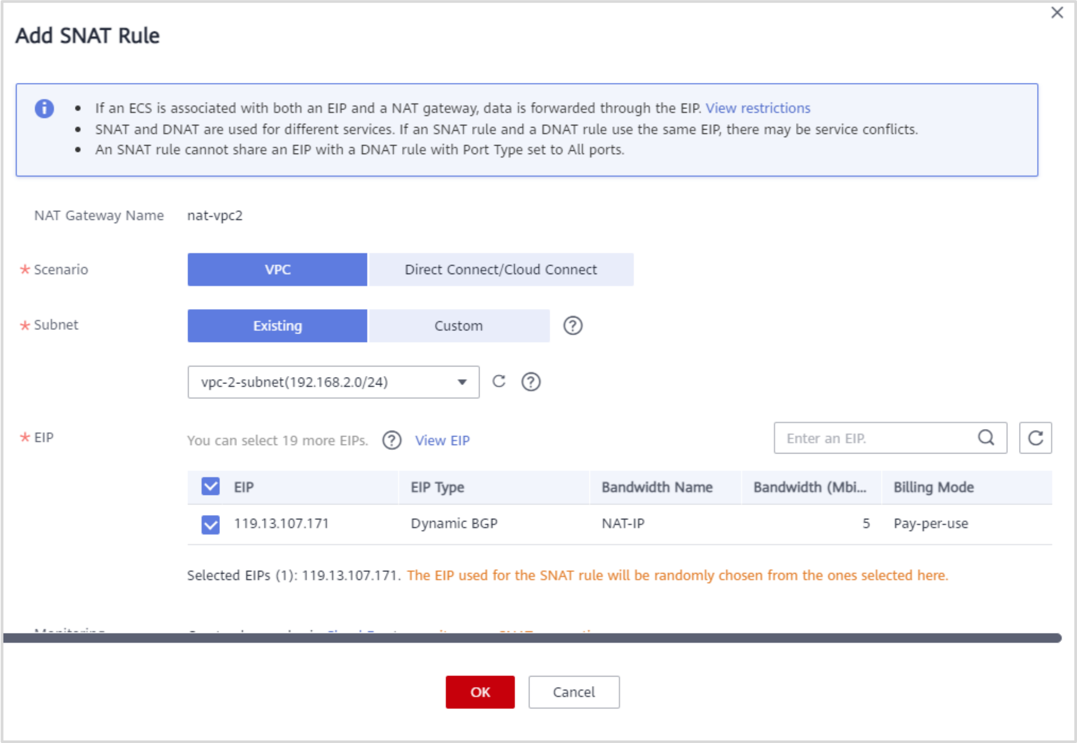
Add SNAT and DNAT rules.

Add SNAT or DNAT rules for the created NAT gateway so that servers in a specified subnet can communicate with the Internet. Learn how to add an SNAT rule.

Figure 2-51

Step 5 Add the first SNAT rule to enable servers in 192.168.2.0/24 of **vpc-2** to access the Internet.

- **Scenario**: **VPC**
- **Subnet**: **Existing** | **vpc-2-subnet**
- **EIP**: **121.36.79.241** (Select the newly created EIP.)



Add SNAT Rule

- If an ECS is associated with both an EIP and a NAT gateway, data is forwarded through the EIP. View restrictions
- SNAT and DNAT are used for different services. If an SNAT rule and a DNAT rule use the same EIP, there may be service conflicts.
- An SNAT rule cannot share an EIP with a DNAT rule with Port Type set to All ports.

NAT Gateway Name nat-vpc2

* Scenario: VPC | Direct Connect/Cloud Connect

* Subnet: Existing | Custom

vpc-2-subnet(192.168.2.0/24)

* EIP: You can select 19 more EIPs. View EIP

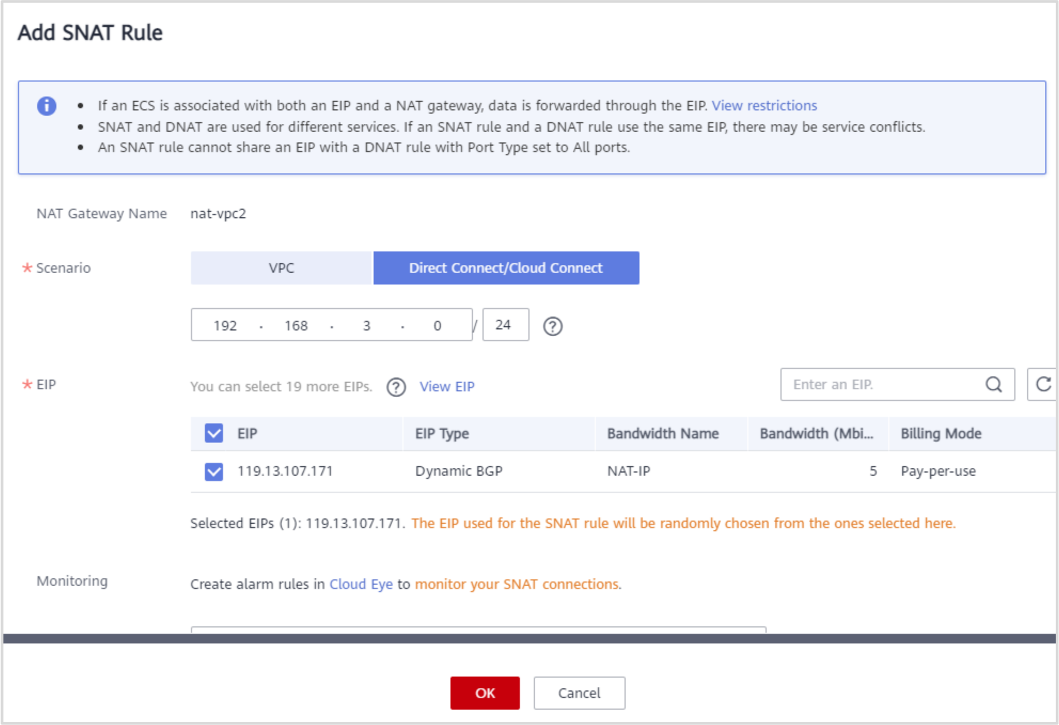
☑ EIP	EIP Type	Bandwidth Name	Bandwidth (Mbi...	Billing Mode
☑ 119.13.107.171	Dynamic BGP	NAT-IP	5	Pay-per-use

Selected EIPs (1): 119.13.107.171. The EIP used for the SNAT rule will be randomly chosen from the ones selected here.

Figure 2-52

Step 6 Add the second SNAT rule to enable servers in 192.168.3.0/24 of **vpc-3** to access the Internet.

- **Scenario: Direct Connect/Cloud Connect | 192.168.3.0/24**
- **EIP: 121.36.79.241** (Select the newly created EIP.)



Add SNAT Rule

- If an ECS is associated with both an EIP and a NAT gateway, data is forwarded through the EIP. View restrictions
- SNAT and DNAT are used for different services. If an SNAT rule and a DNAT rule use the same EIP, there may be service conflicts.
- An SNAT rule cannot share an EIP with a DNAT rule with Port Type set to All ports.

NAT Gateway Name nat-vpc2

* Scenario: VPC | Direct Connect/Cloud Connect

192 . 168 . 3 . 0 / 24

* EIP: You can select 19 more EIPs. View EIP

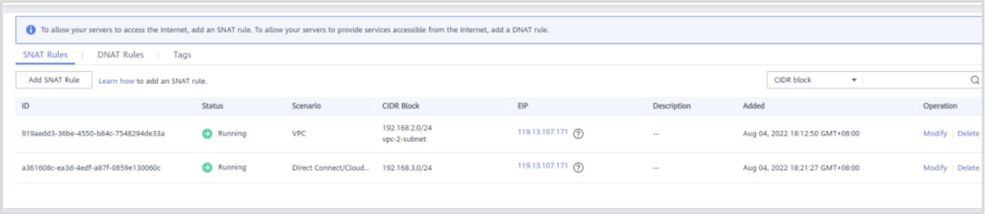
☑ EIP	EIP Type	Bandwidth Name	Bandwidth (Mbi...	Billing Mode
☑ 119.13.107.171	Dynamic BGP	NAT-IP	5	Pay-per-use

Selected EIPs (1): 119.13.107.171. The EIP used for the SNAT rule will be randomly chosen from the ones selected here.

Monitoring: Create alarm rules in Cloud Eye to monitor your SNAT connections.

Figure 2-53

Step 7 View the SNAT rule list. Check whether the SNAT rules you added are displayed in the SNAT rule list.

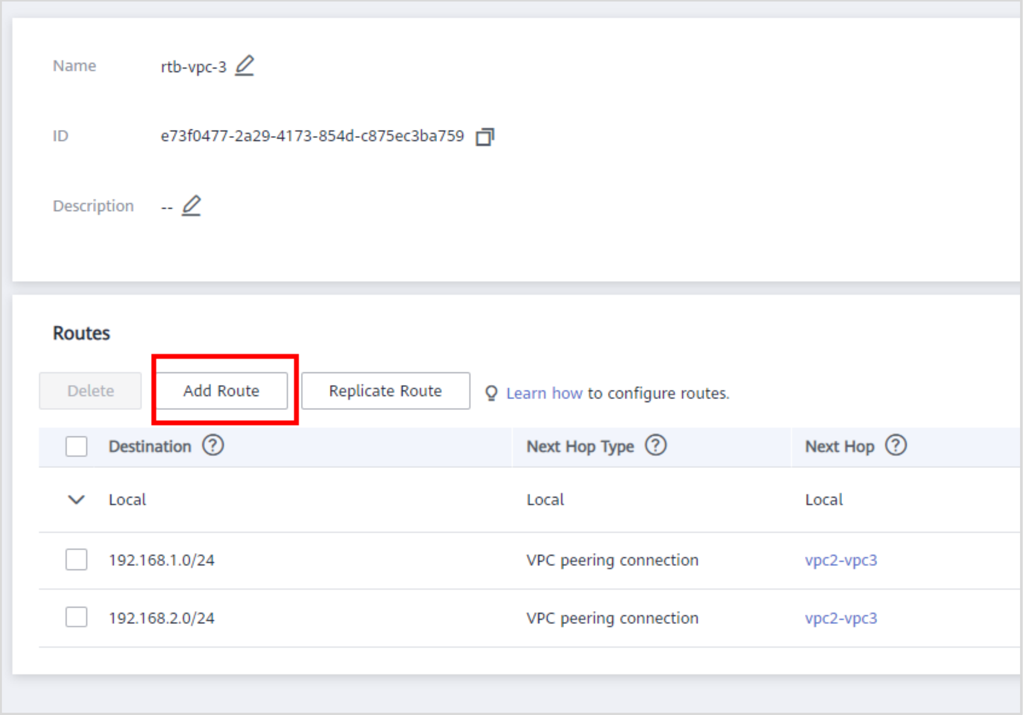


To allow your servers to access the Internet, add an SNAT rule. To allow your servers to provide services accessible from the Internet, add a DNAT rule.

ID	Status	Scenario	CIDR Block	EIP	Description	Added	Operation
919aedd3-36be-4550-b84c-7548294de33a	Running	VPC	192.168.2.0/24 vpc-2-subnet	119.13.107.171	--	Aug 04, 2022 18:12:50 GMT+08:00	Modify | Delete
a361608c-ea3d-4edf-a87f-0859e130060c	Running	Direct Connect/Cloud...	192.168.3.0/24	119.13.107.171	--	Aug 04, 2022 18:21:27 GMT+08:00	Modify | Delete

Figure 2-54

Step 8 In route table **rtb-vpc-3** of **vpc-3**, click **Add Route**.



Name rtb-vpc-3

ID e73f0477-2a29-4173-854d-c875ec3ba759

Description --

Routes

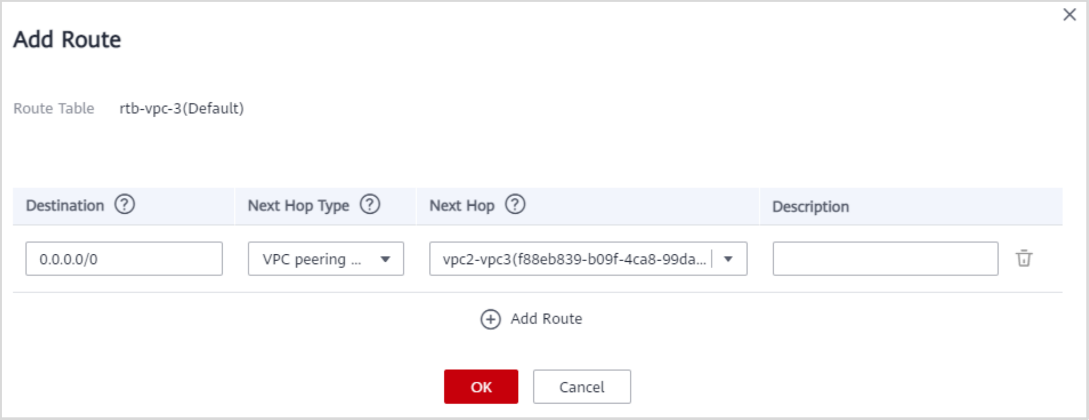
Destination	Next Hop Type	Next Hop
Local	Local	Local
192.168.1.0/24	VPC peering connection	vpc2-vpc3
192.168.2.0/24	VPC peering connection	vpc2-vpc3

Figure 2-55

Step 9 Add a default route pointing to the VPC peering connection and click **OK**.

The default route is used to divert Internet access traffic generated from **vpc-3** to **vpc-2** through a VPC peering connection. Then servers in **vpc-3** can use the SNAT rule added in **vpc-2** to access the Internet.

- **Destination**: **0.0.0.0/0**
- **Next Hop Type**: **VPC peering connection**
- **Next Hop**: **vpc2-vpc3**



Route Table rtb-vpc-3(Default)

Destination	Next Hop Type	Next Hop	Description
0.0.0.0/0	VPC peering ...	vpc2-vpc3(f88eb839-b09f-4ca8-99da...	

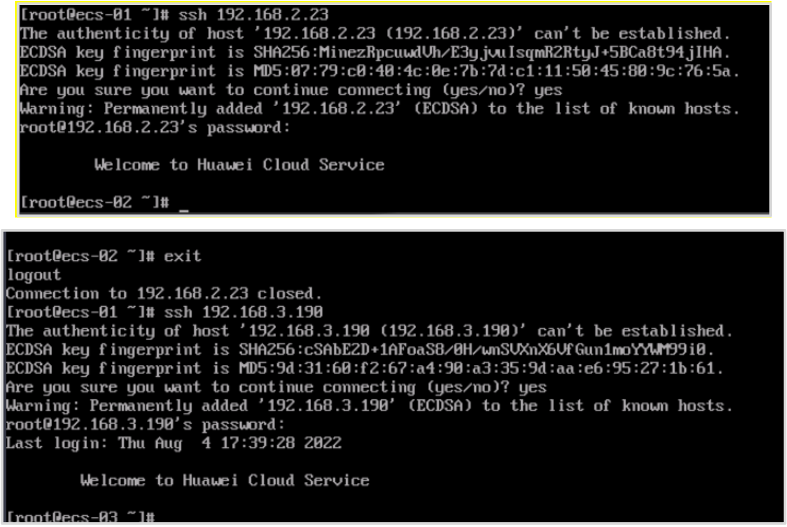
Figure 2-56

2.3 Verifying the Result

2.3.1 Logging In to a Remote Resource from an O&M Host

Step 1 Log in to **ECS01** in the **CN-Hong Kong** region and log in to **ECS02** and **ECS03** in SSH mode from **ECS01**, respectively.

```
[root@ecs-01 ~]# ssh 192.168.2.23
[root@ecs-02 ~]# exit
[root@ecs-01 ~]# ssh 192.168.3.190
[root@ecs-03 ~]
```



```
[root@ecs-01 ~]# ssh 192.168.2.23
The authenticity of host '192.168.2.23 (192.168.2.23)' can't be established.
ECDSA key fingerprint is SHA256:MinezRpcuwdVh/E3yjvuIsqmR2RtyJ+5BCa8t94jIHA.
ECDSA key fingerprint is MD5:07:79:c0:40:4c:0e:7b:7d:c1:11:50:45:80:9c:76:5a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.23' (ECDSA) to the list of known hosts.
root@192.168.2.23's password:

        Welcome to Huawei Cloud Service

[root@ecs-02 ~]# _
```

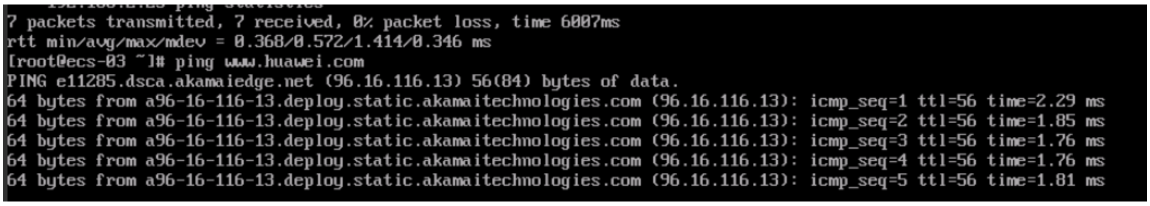
```
[root@ecs-02 ~]# exit
logout
Connection to 192.168.2.23 closed.
[root@ecs-01 ~]# ssh 192.168.3.190
The authenticity of host '192.168.3.190 (192.168.3.190)' can't be established.
ECDSA key fingerprint is SHA256:cSAbE2D+1AFoaS8/0H/wmSVXnX6VfGun1moYYWM99i0.
ECDSA key fingerprint is MD5:9d:31:60:f2:67:a4:90:a3:35:9d:aa:e6:95:27:1b:61.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.3.190' (ECDSA) to the list of known hosts.
root@192.168.3.190's password:
Last login: Thu Aug  4 17:39:28 2022

        Welcome to Huawei Cloud Service

[root@ecs-03 ~]#
```

Figure 2-57

The preceding information indicates that you can log in to **ECS02** and **ECS03** using SSH from **ECS01**, and the on-premises O&M host (**ECS01**) can perform remote O&M on cloud resources.

2.3.2 Cloud Resources Accessing the Internet Through a Public NAT Gateway

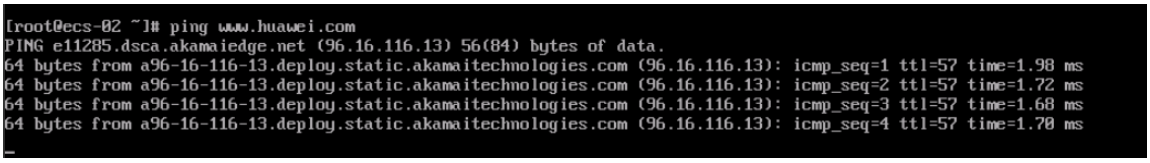
Step 1 In the **AP-Singapore** region, Log in to **ECS03** and ping a public IP address.



```
7 packets transmitted, 7 received, 0% packet loss, time 6007ms
rtt min/avg/max/mdev = 0.368/0.572/1.414/0.346 ms
[root@ecs-03 ~]# ping www.huawei.com
PING e11285.dsca.akamaiedge.net (96.16.116.13) 56(84) bytes of data.
64 bytes from a96-16-116-13.deploy.static.akamaitechnologies.com (96.16.116.13): icmp_seq=1 ttl=56 time=2.29 ms
64 bytes from a96-16-116-13.deploy.static.akamaitechnologies.com (96.16.116.13): icmp_seq=2 ttl=56 time=1.85 ms
64 bytes from a96-16-116-13.deploy.static.akamaitechnologies.com (96.16.116.13): icmp_seq=3 ttl=56 time=1.76 ms
64 bytes from a96-16-116-13.deploy.static.akamaitechnologies.com (96.16.116.13): icmp_seq=4 ttl=56 time=1.76 ms
64 bytes from a96-16-116-13.deploy.static.akamaitechnologies.com (96.16.116.13): icmp_seq=5 ttl=56 time=1.81 ms
```

Figure 2-58

Step 2 In the **AP-Singapore** region, Log in to **ECS02** and ping a public IP address.



```
[root@ecs-02 ~]# ping www.huawei.com
PING e11285.dsca.akamaiedge.net (96.16.116.13) 56(84) bytes of data.
64 bytes from a96-16-116-13.deploy.static.akamaitechnologies.com (96.16.116.13): icmp_seq=1 ttl=57 time=1.98 ms
64 bytes from a96-16-116-13.deploy.static.akamaitechnologies.com (96.16.116.13): icmp_seq=2 ttl=57 time=1.72 ms
64 bytes from a96-16-116-13.deploy.static.akamaitechnologies.com (96.16.116.13): icmp_seq=3 ttl=57 time=1.68 ms
64 bytes from a96-16-116-13.deploy.static.akamaitechnologies.com (96.16.116.13): icmp_seq=4 ttl=57 time=1.70 ms
_
```

Figure 2-59

The preceding command output indicates that servers in **vpc-2** and **vpc-3** can access the Internet through the public NAT gateway in **vpc-2**.

2.4 Clearing Resources

Step 1 Delete the public NAT gateway.

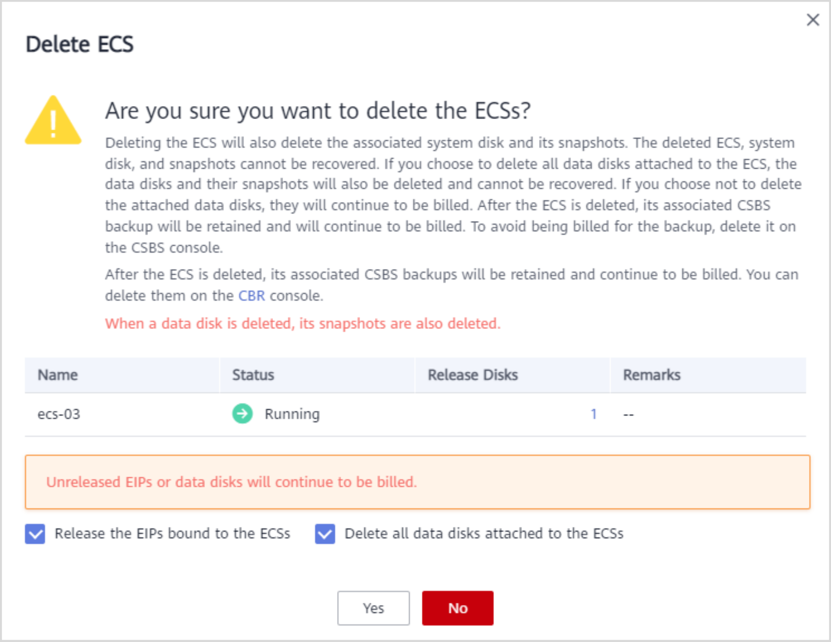
Choose **NAT Gateway** from the service list. Locate the public NAT gateway created in this experiment and choose **More** > **Delete** in the **Operation** column.

Step 2 Delete the VPN gateway.

- Choose **Virtual Private Network** from the service list. On the displayed page, locate the VPN connection created in this experiment in the list, and choose **More** > **Delete** in the **Operation** column.
- In the navigation pane on the left, choose V**PN Gateways**, locate the VPN gateway created in this experiment in the list, and choose **More** > **Delete** in the **Operation** column.

Step 3 Delete the ECSs.

- In the service list, choose **Elastic Cloud Server** under **Compute**. In the ECS list, locate the ECSs created in this exercise and choose **More** > **Delete** in the **Operation** column to delete them one by one.
- In the displayed dialog box, select the check boxes displayed in the following picture and click **Yes**.



Delete ECS

Are you sure you want to delete the ECSs?

Deleting the ECS will also delete the associated system disk and its snapshots. The deleted ECS, system disk, and snapshots cannot be recovered. If you choose to delete all data disks attached to the ECS, the data disks and their snapshots will also be deleted and cannot be recovered. If you choose not to delete the attached data disks, they will continue to be billed. After the ECS is deleted, its associated CSBS backup will be retained and will continue to be billed. To avoid being billed for the backup, delete it on the CSBS console.

After the ECS is deleted, its associated CSBS backups will be retained and continue to be billed. You can delete them on the CBR console.

When a data disk is deleted, its snapshots are also deleted.

Name	Status	Release Disks	Remarks
ecs-03	Running	1	--

Unreleased EIPs or data disks will continue to be billed.

☑ Release the EIPs bound to the ECSs ☑ Delete all data disks attached to the ECSs

Figure 2-60

Step 4 Delete the VPC peering connection.

In the service list, choose **Virtual Private Cloud** under **Networking**. On the network console, choose **VPC Peering**, locate the VPC peering connection created in this experiment and click **Delete** in the **Operation** column.

Step 5 Delete the security group.

In the service list, choose **Virtual Private Cloud** under **Networking**. On the network console, choose **Access Control** > **Security Groups**. In the security group list, locate the security group created in this exercise and choose **More** > **Delete** in the **Operation** column.

Step 6 Delete the VPCs.

- In the service list, choose **Virtual Private Cloud** under **Networking**. On the network console, choose **Subnets**. In the subnet list, locate the subnet created in this exercise and click **Delete** in the **Operation** column.
- Choose **Virtual Private Cloud** in the navigation pane on the left. In the VPC list, locate the VPCs created in this exercise and click **Delete** in the **Operation** column to delete them one by one.

2.5 Quiz

Question: In the VPN connection configuration, how do I configure **Local Subnet** and **Remote Subnet**?

Answer: Set **Local Subnet** to a VPC subnet that needs to access an on-premises network through VPN. Set **Remote Subnet** to an on-premises subnet that needs to access a VPC through VPN.

3 Storage Architecture Design

3.1 Introduction

3.1.1 About This Exercise

In this exercise, you will establish an environment on Huawei Cloud to run video streaming services. Initially, Huawei Cloud ECS, Elastic Volume Service (EVS), Scalable File Service (SFS), and Object Storage Service (OBS) will be used to set up a video website. Then, ELB will be used for distributing requests to different AZs for HA deployment.

This exercise uses region CN-Hong Kong as an example. You can use any region they want.

3.1.2 Objectives

Acquire the operation principles and configuration methods of storage services.

Understand the service scenarios of cloud data management and configuration.

3.1.3 Networking

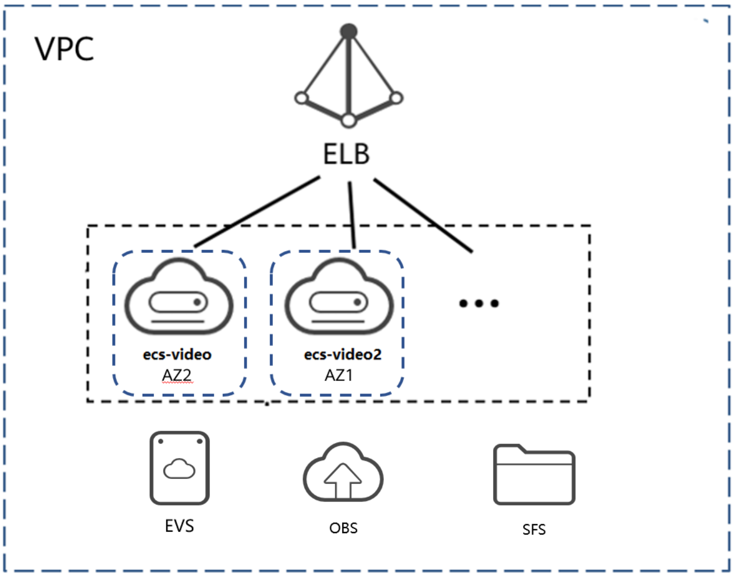


Figure 3-1

3.1.4 Related Software

Nginx is a lightweight web server that can act as a reverse proxy or mail (IMAP/POP3) proxy, and released under the BSD-like protocol. It provides high concurrency with a low memory footprint.

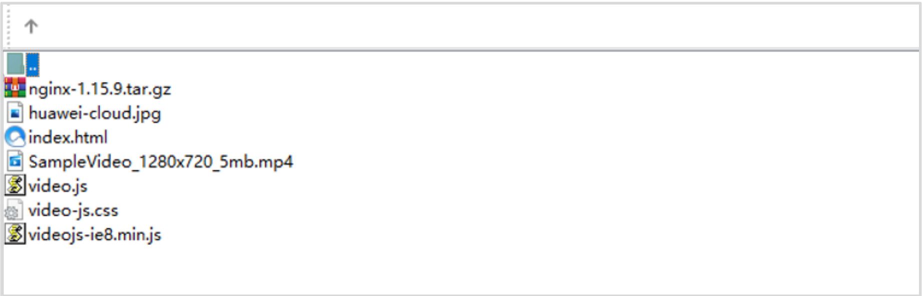
3.2 Procedure

3.2.1 Preparations

Step 1 Download video files.

- Open a browser on the local PC, enter https://cloudservice-v3.obs.cn-east-3.myhuaweicloud.com/video_en.zip in the address box, and press Enter to download the exercise files.
- Obtain the exercise files shown in the following figure:

huawei-cloud.jpg, index.html, nginx-1.15.9.tar.gz, SampleVideo_1280x720_5mb.mp4, video.js, and more



..
nginx-1.15.9.tar.gz
huawei-cloud.jpg
index.html
SampleVideo_1280x720_5mb.mp4
video.js
video-js.css
videojs-ie8.min.js

Figure 3-2

3.2.2 Creating a VPC

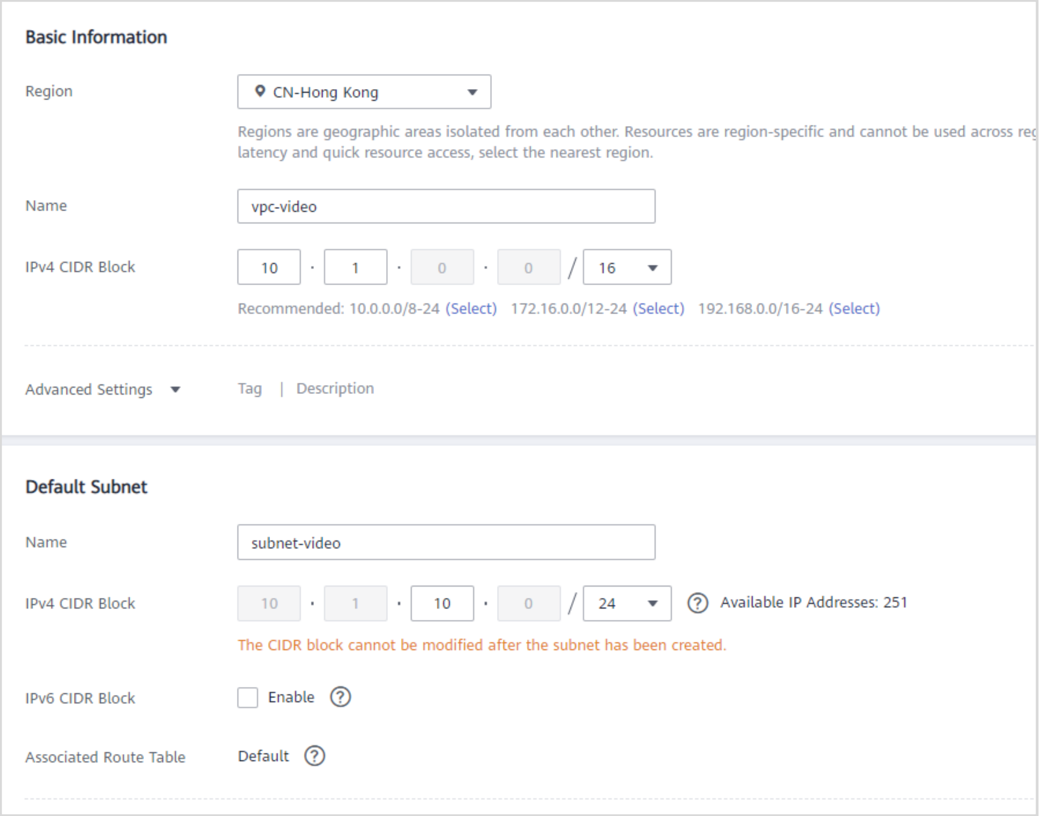
Step 1 In the CN-Hong Kong region, configure the parameters as follows to create a VPC: (Resources in this exercise will be created in this VPC.)

Basic Information

- **Region: CN-Hong Kong**
- **Name: vpc-video**
- **IPv4 CIDR Block: 10.1.0.0/16**

Default Subnet

- **Name: subnet-video**
- **IPv4 CIDR Block: 10.1.10.0/24**



Basic Information

Region: CN-Hong Kong

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across reg latency and quick resource access, select the nearest region.

Name: vpc-video

IPv4 CIDR Block: 10 . 1 . 0 . 0 / 16

Recommended: 10.0.0.0/8-24 (Select) 172.16.0.0/12-24 (Select) 192.168.0.0/16-24 (Select)

Advanced Settings ▾ Tag | Description

Default Subnet

Name: subnet-video

IPv4 CIDR Block: 10 . 1 . 10 . 0 / 24 ⓘ Available IP Addresses: 251

The CIDR block cannot be modified after the subnet has been created.

IPv6 CIDR Block: □ Enable ⓘ

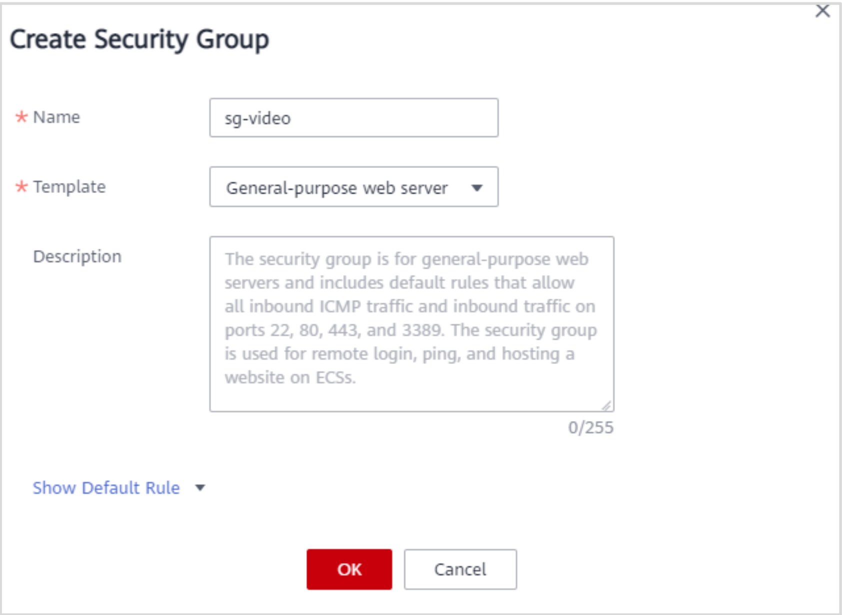
Associated Route Table: Default ⓘ

Figure 3-3

3.2.3 Creating a Security Group

Step 1 In the CN-Hong Kong region, configure the parameters as follows to create a security group: (Servers running the video streaming service in this exercise will use this security group.)

- **Name: sg-video**
- **Template: General-purpose web server**



Create Security Group

* Name: sg-video

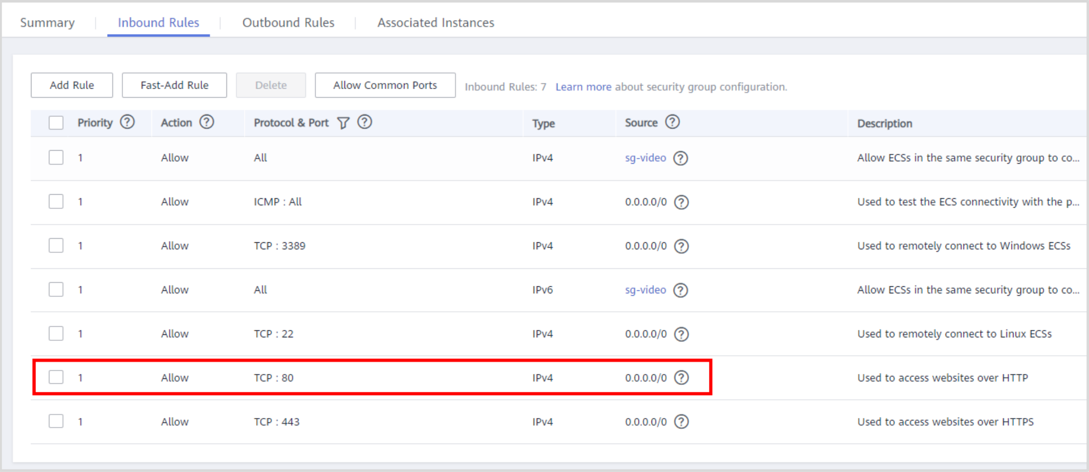
* Template: General-purpose web server

Description: The security group is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and inbound traffic on ports 22, 80, 443, and 3389. The security group is used for remote login, ping, and hosting a website on ECSs.

0/255

Figure 3-4

Step 2 View the security group rules. You can see that there is an inbound rule that allows traffic on port 80.



Inbound Rules: 7 Learn more about security group configuration.

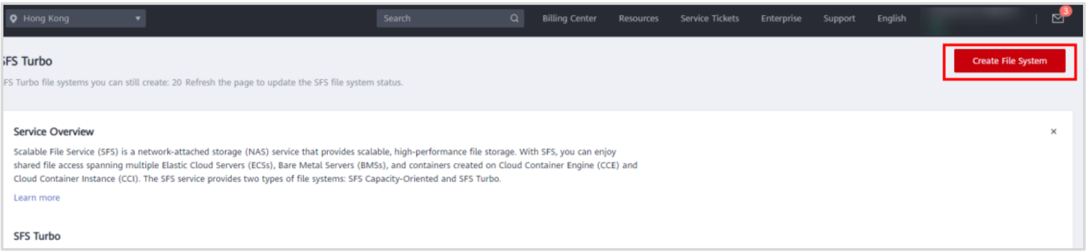
□	Priority	Action	Protocol & Port	Type	Source	Description
□	1	Allow	All	IPv4	sg-video	Allow ECSs in the same security group to co...
□	1	Allow	ICMP : All	IPv4	0.0.0.0/0	Used to test the ECS connectivity with the p...
□	1	Allow	TCP : 3389	IPv4	0.0.0.0/0	Used to remotely connect to Windows ECSs
□	1	Allow	All	IPv6	sg-video	Allow ECSs in the same security group to co...
□	1	Allow	TCP : 22	IPv4	0.0.0.0/0	Used to remotely connect to Linux ECSs
□	1	Allow	TCP : 80	IPv4	0.0.0.0/0	Used to access websites over HTTP
□	1	Allow	TCP : 443	IPv4	0.0.0.0/0	Used to access websites over HTTPS

Figure 3-5

3.2.4 Creating an SFS File System

Step 1 In the CN-Hong Kong region, choose **Scalable File Service** > **SFS Turbo** and click **Create File System** in the upper right corner.

Note: The file system created in this step will be mounted to the ECSs.



ﾐFS Turbo

FS Turbo file systems you can still create: 20 Refresh the page to update the SFS file system status.

Service Overview

Scalable File Service (SFS) is a network-attached storage (NAS) service that provides scalable, high-performance file storage. With SFS, you can enjoy shared file access spanning multiple Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), and containers created on Cloud Container Engine (CCE) and Cloud Container Instance (CCI). The SFS service provides two types of file systems: SFS Capacity-Oriented and SFS Turbo.

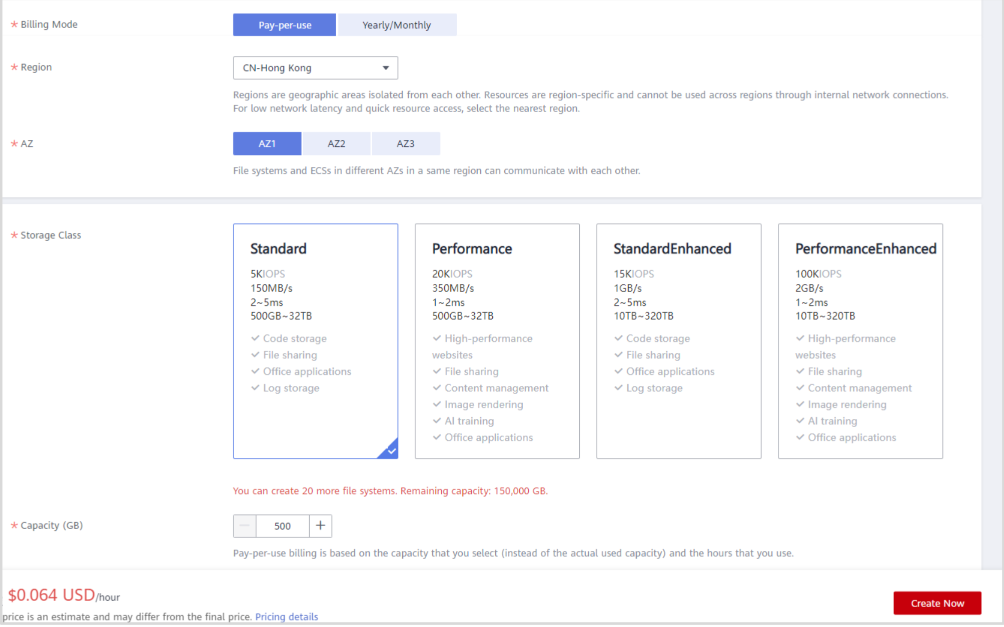
Learn more

SFS Turbo

Figure 3-6

Step 2 Configure the parameters as follows, confirm the configuration, and click **Create Now**.

- Billing Mode: Pay-per-use
- Region: CN-Hong Kong
- AZ: AZ1
- Storage Class: Standard
- Capacity (GB): 500
- Protocol Type: NFS



* Billing Mode: Pay-per-use | Yearly/Monthly

* Region: CN-Hong Kong

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

* AZ: AZ1 | AZ2 | AZ3

File systems and ECSs in different AZs in a same region can communicate with each other.

* Storage Class

Standard	Performance	StandardEnhanced	PerformanceEnhanced
5KIOPS 150MB/s 2~5ms 500GB~32TB	20KIOPS 350MB/s 1~2ms 500GB~32TB	15KIOPS 1GB/s 2~5ms 10TB~320TB	100KIOPS 2GB/s 1~2ms 10TB~320TB
✓ Code storage ✓ File sharing ✓ Office applications ✓ Log storage	✓ High-performance websites ✓ File sharing ✓ Content management ✓ Image rendering ✓ AI training ✓ Office applications	✓ Code storage ✓ File sharing ✓ Office applications ✓ Log storage	✓ High-performance websites ✓ File sharing ✓ Content management ✓ Image rendering ✓ AI training ✓ Office applications

You can create 20 more file systems. Remaining capacity: 150,000 GB.

* Capacity (GB): 500

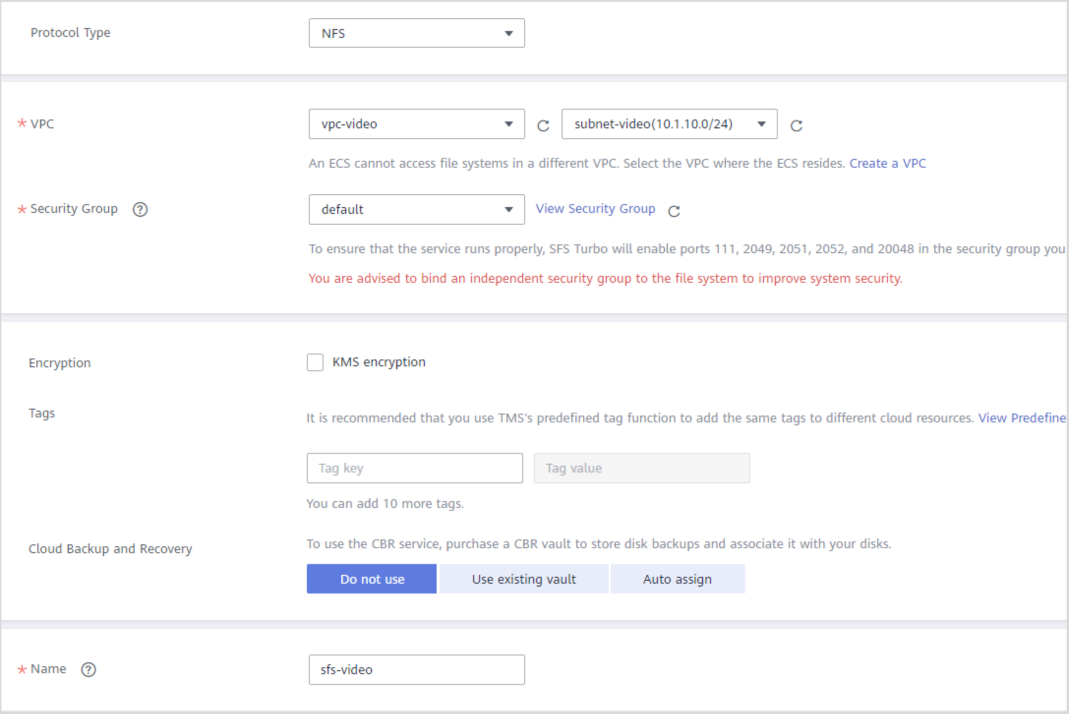
Pay-per-use billing is based on the capacity that you select (instead of the actual used capacity) and the hours that you use.

$0.064 USD/hour

price is an estimate and may differ from the final price. Pricing details

Figure 3-7

- VPC: vpc-video | subnet-video
- Security Group: sg-video
- Name: sfs-video
- Retain the default settings for other parameters.



Protocol Type: NFS

* VPC: vpc-video | subnet-video(10.1.10.0/24)

An ECS cannot access file systems in a different VPC. Select the VPC where the ECS resides. Create a VPC

* Security Group: default | View Security Group

To ensure that the service runs properly, SFS Turbo will enable ports 111, 2049, 2051, 2052, and 20048 in the security group you

You are advised to bind an independent security group to the file system to improve system security.

Encryption: □ KMS encryption

Tags: It is recommended that you use TMS's predefined tag function to add the same tags to different cloud resources. View Predefine

You can add 10 more tags.

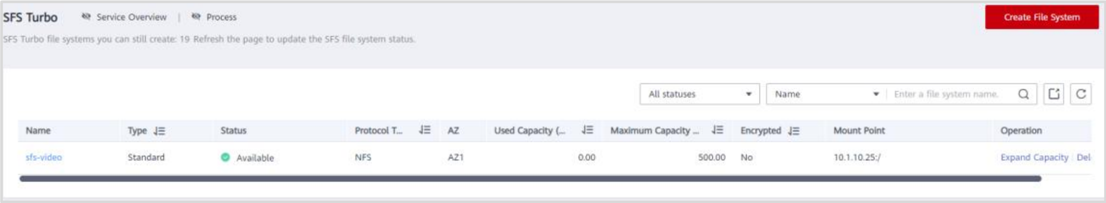
Cloud Backup and Recovery: To use the CBR service, purchase a CBR vault to store disk backups and associate it with your disks.

* Name: sfs-video

Figure 3-8

Step 3 View the created SFS file system.

Step 4 The file system status is **Available**.



SFS Turbo file systems you can still create: 19 Refresh the page to update the SFS file system status.

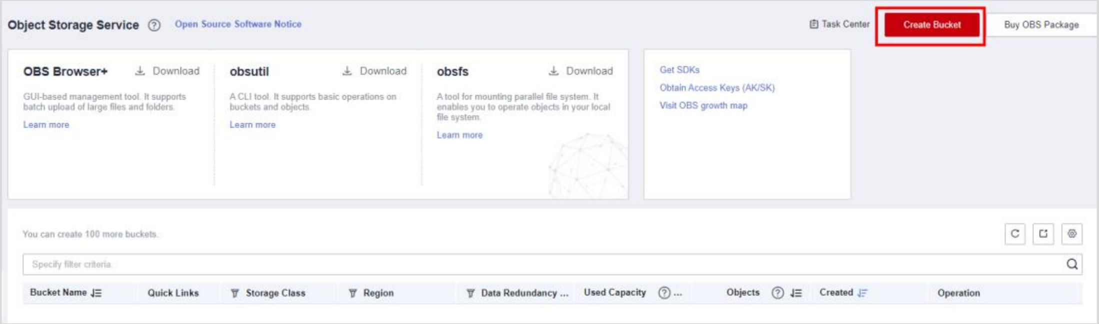
Name	Type	Status	Protocol T...	AZ	Used Capacity (...	Maximum Capacity ...	Encrypted	Mount Point	Operation
sfs-video	Standard	● Available	NFS	AZ1	0.00	500.00	No	10.1.10.25:/	Expand Capacity Del

Figure 3-9

3.2.5 Creating an OBS Bucket

Step 1 In the CN-Hong Kong region, choose **Object Storage Service** > **Object Storage** and click **Create Bucket** in the upper right corner.

Note: The **video.zip** file downloaded during preparations needs to be uploaded to the bucket created in this step.



OBS Browser+: GUI-based management tool. It supports batch upload of large files and folders. Learn more

obsutil: A CLI tool. It supports basic operations on buckets and objects. Learn more

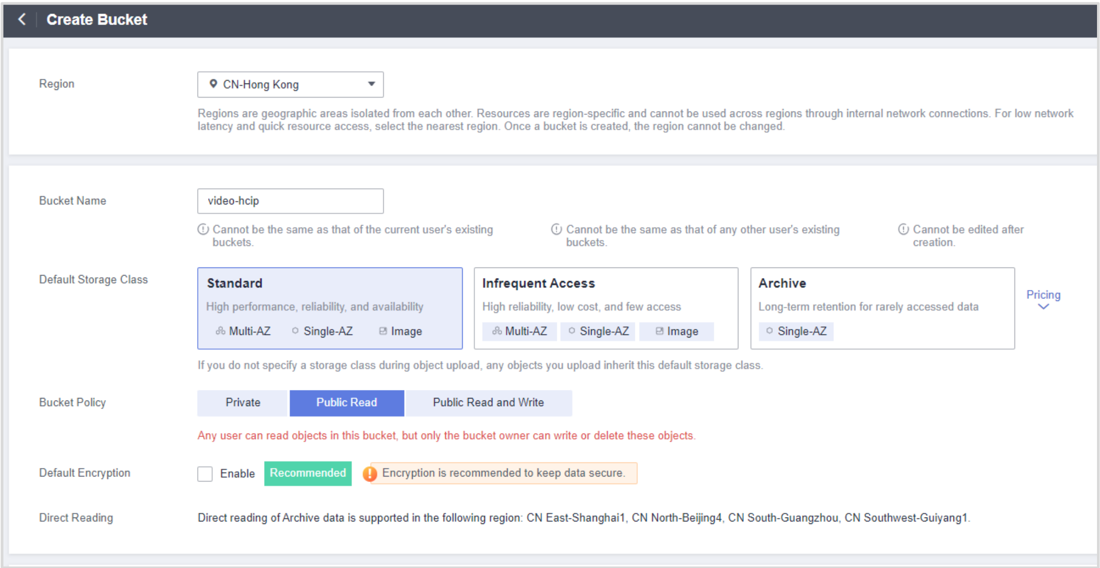
obsfs: A tool for mounting parallel file system. It enables you to operate objects in your local file system. Learn more

You can create 100 more buckets.

Figure 3-10

Step 2 Configure the parameters as follows, confirm the configuration, and click **Create Now**.

- Region: CN-Hong Kong
- Bucket Name: video-hcip
- Default Storage Class: Standard
- Bucket Policy: Public Read
- Direct Reading: Disable



Create Bucket

Region: CN-Hong Kong

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region. Once a bucket is created, the region cannot be changed.

Bucket Name: video-hcip

Cannot be the same as that of the current user's existing buckets. Cannot be the same as that of any other user's existing buckets. Cannot be edited after creation.

Default Storage Class:
- Standard: High performance, reliability, and availability. Multi-AZ, Single-AZ, Image
- Infrequent Access: High reliability, low cost, and few access. Multi-AZ, Single-AZ, Image
- Archive: Long-term retention for rarely accessed data. Single-AZ

If you do not specify a storage class during object upload, any objects you upload inherit this default storage class.

Bucket Policy: Private | **Public Read** | Public Read and Write

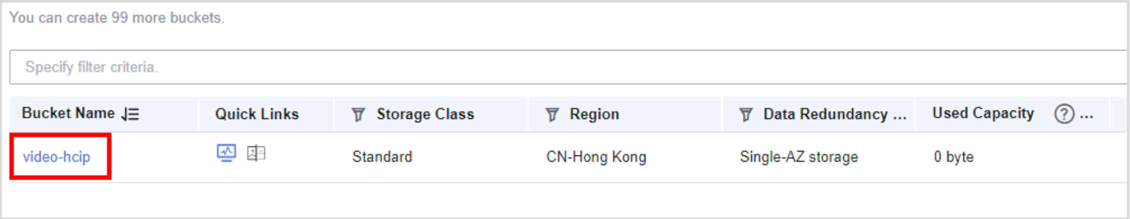
Any user can read objects in this bucket, but only the bucket owner can write or delete these objects.

Default Encryption: □ Enable Encryption is recommended to keep data secure.

Direct Reading: Direct reading of Archive data is supported in the following region: CN East-Shanghai1, CN North-Beijing4, CN South-Guangzhou, CN Southwest-Guiyang1.

Figure 3-11

Step 3 Click the name of the created OBS bucket to go to the bucket management page.



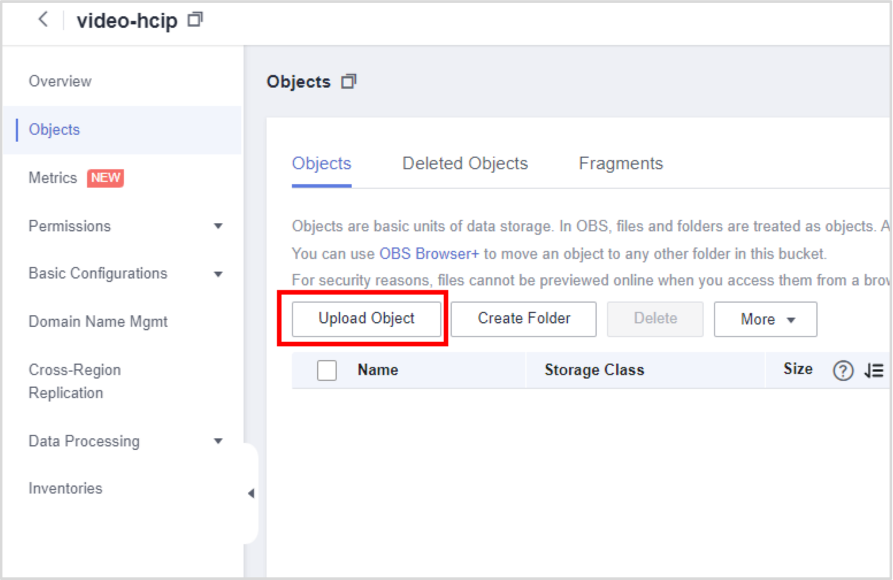
You can create 99 more buckets.

Specify filter criteria.

Bucket Name	Quick Links	Storage Class	Region	Data Redundancy ...	Used Capacity
video-hcip		Standard	CN-Hong Kong	Single-AZ storage	0 byte

Figure 3-12

Step 4 Choose **Objects** > **Upload Object**.



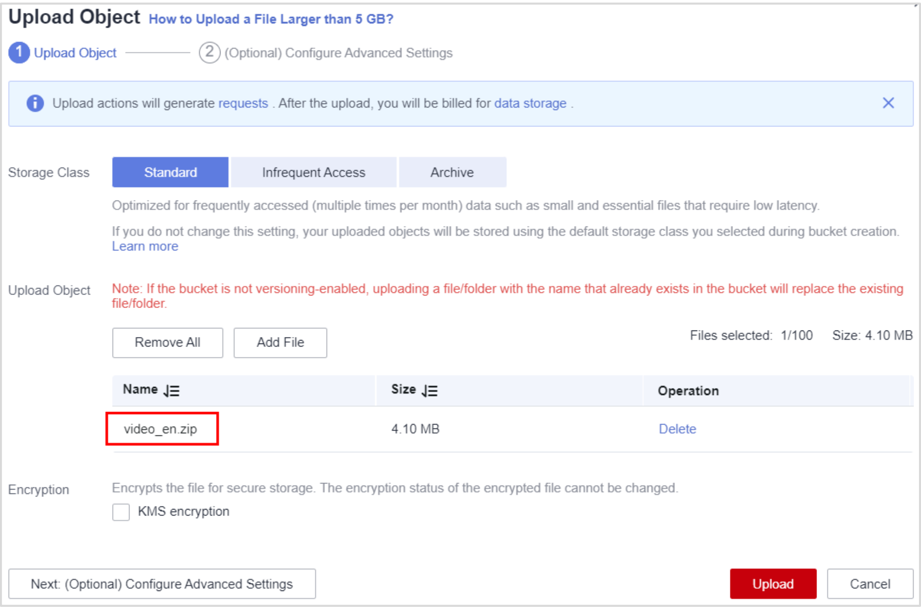
Objects are basic units of data storage. In OBS, files and folders are treated as objects. A

You can use OBS Browser+ to move an object to any other folder in this bucket.

For security reasons, files cannot be previewed online when you access them from a brow

Figure 3-13

Step 5 Click **add file**, find the **video_en.zip** file in the local directory, and click **Upload**.



Upload actions will generate requests . After the upload, you will be billed for data storage .

Storage Class: Standard

Optimized for frequently accessed (multiple times per month) data such as small and essential files that require low latency.

If you do not change this setting, your uploaded objects will be stored using the default storage class you selected during bucket creation.

Upload Object: Note: If the bucket is not versioning-enabled, uploading a file/folder with the name that already exists in the bucket will replace the existing file/folder.

Files selected: 1/100 Size: 4.10 MB

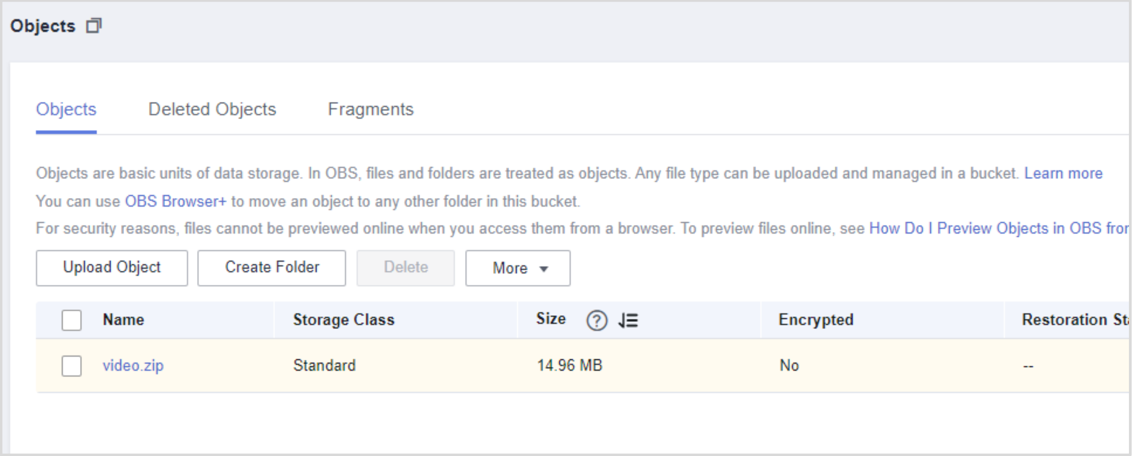
Name	Size	Operation
video_en.zip	4.10 MB	Delete

Encryption: Encrypts the file for secure storage. The encryption status of the encrypted file cannot be changed.

□ KMS encryption

Figure 3-14

Step 6 In the object list, view the uploaded file.



Objects

Objects | Deleted Objects | Fragments

Objects are basic units of data storage. In OBS, files and folders are treated as objects. Any file type can be uploaded and managed in a bucket. Learn more

You can use OBS Browser+ to move an object to any other folder in this bucket.

For security reasons, files cannot be previewed online when you access them from a browser. To preview files online, see How Do I Preview Objects in OBS fror

Upload Object | Create Folder | Delete | More

	Name	Storage Class	Size	Encrypted	Restoration St
□	video.zip	Standard	14.96 MB	No	--

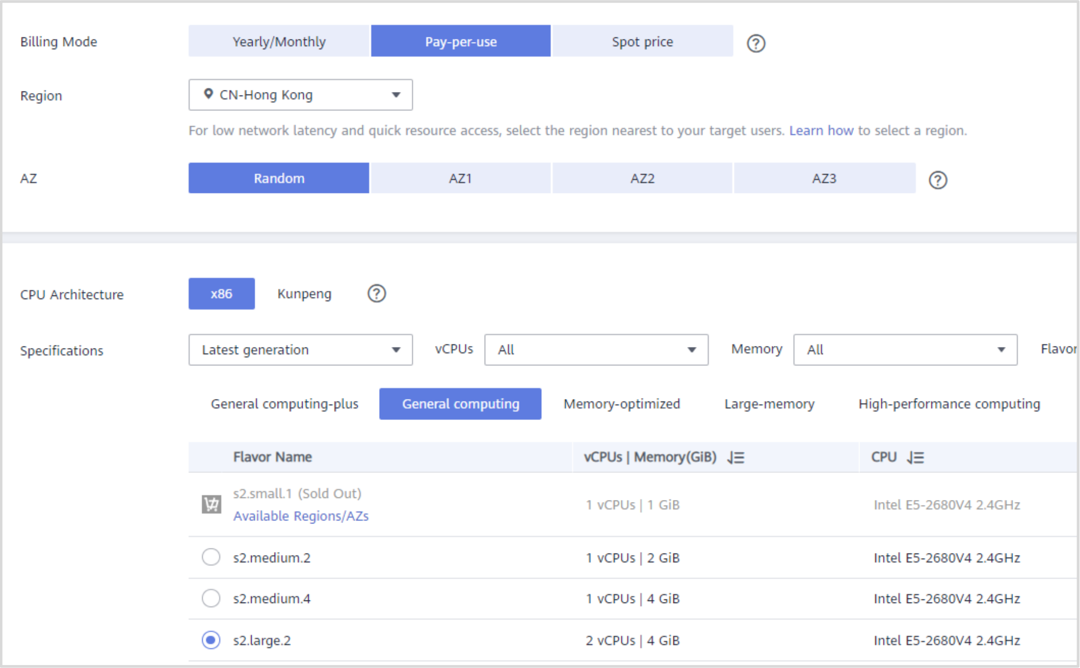
Figure 3-15

3.2.6 Creating an ECS

Step 1 In the CN-Hong Kong region, configure the parameters as follows to create an ECS. Confirm the configuration and click **Next**.

Note: This ECS will be used to deploy the video streaming service.

- **Billing Mode**: **Pay-per-use**
- **Region**: **CN-Hong Kong**
- **AZ**: Random
- **Specifications**: **2 vCPUs | 4 GiB**
- **Image**: **Public image | CentOS 7.6 64 bit(40 GB)**
- **Host Security**: **Basic (free)**
- **System Disk**: **High I/O | 40 GiB**
- **Network**: **vpc-video | subnet-video | Automatically assign IP address**
- **Security Group**: **sg-video**
- **EIP**: **Auto assign**
- **EIP Type**: **Premium BGP**
- **Billed By**: **Traffic**
- **Bandwidth Size**: **10 Mbit/s**
- **ECS Name**: **ecs-video**
- **Password**: User-defined (with the username of **root**)



Billing Mode: Yearly/Monthly | **Pay-per-use** | Spot price

Region: CN-Hong Kong

For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

AZ: **Random** | AZ1 | AZ2 | AZ3

CPU Architecture: **x86** | Kunpeng

Specifications: Latest generation | vCPUs: All | Memory: All | Flavor

General computing-plus | **General computing** | Memory-optimized | Large-memory | High-performance computing

	Flavor Name	vCPUs | Memory(GiB)	CPU
	s2.small.1 (Sold Out) Available Regions/AZs	1 vCPUs | 1 GiB	Intel E5-2680V4 2.4GHz
○	s2.medium.2	1 vCPUs | 2 GiB	Intel E5-2680V4 2.4GHz
○	s2.medium.4	1 vCPUs | 4 GiB	Intel E5-2680V4 2.4GHz
●	s2.large.2	2 vCPUs | 4 GiB	Intel E5-2680V4 2.4GHz

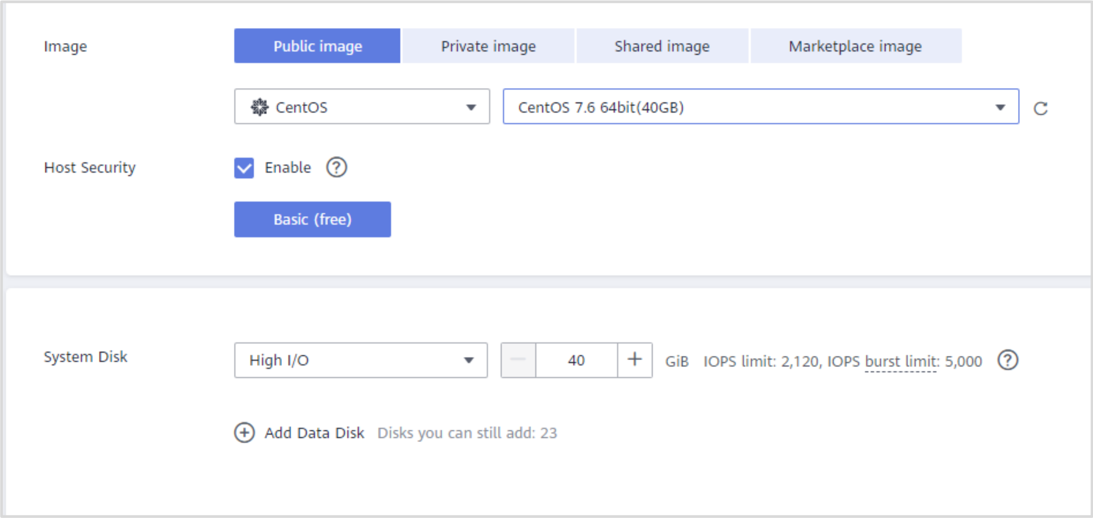


Image: **Public image** | Private image | Shared image | Marketplace image

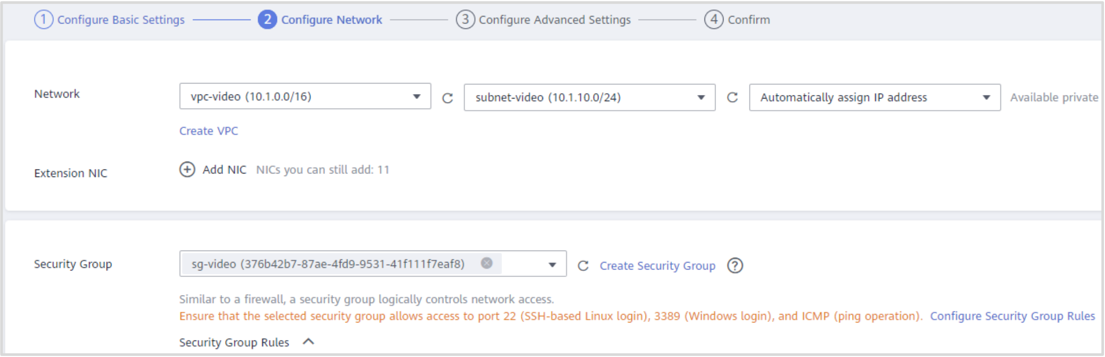
CentOS | CentOS 7.6 64bit(40GB)

Host Security: ☑ Enable

Basic (free)

System Disk: High I/O | 40 GiB | IOPS limit: 2,120, IOPS burst limit: 5,000

Add Data Disk Disks you can still add: 23



1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

Network: vpc-video (10.1.0.0/16) | subnet-video (10.1.10.0/24) | Automatically assign IP address | Available private

Create VPC

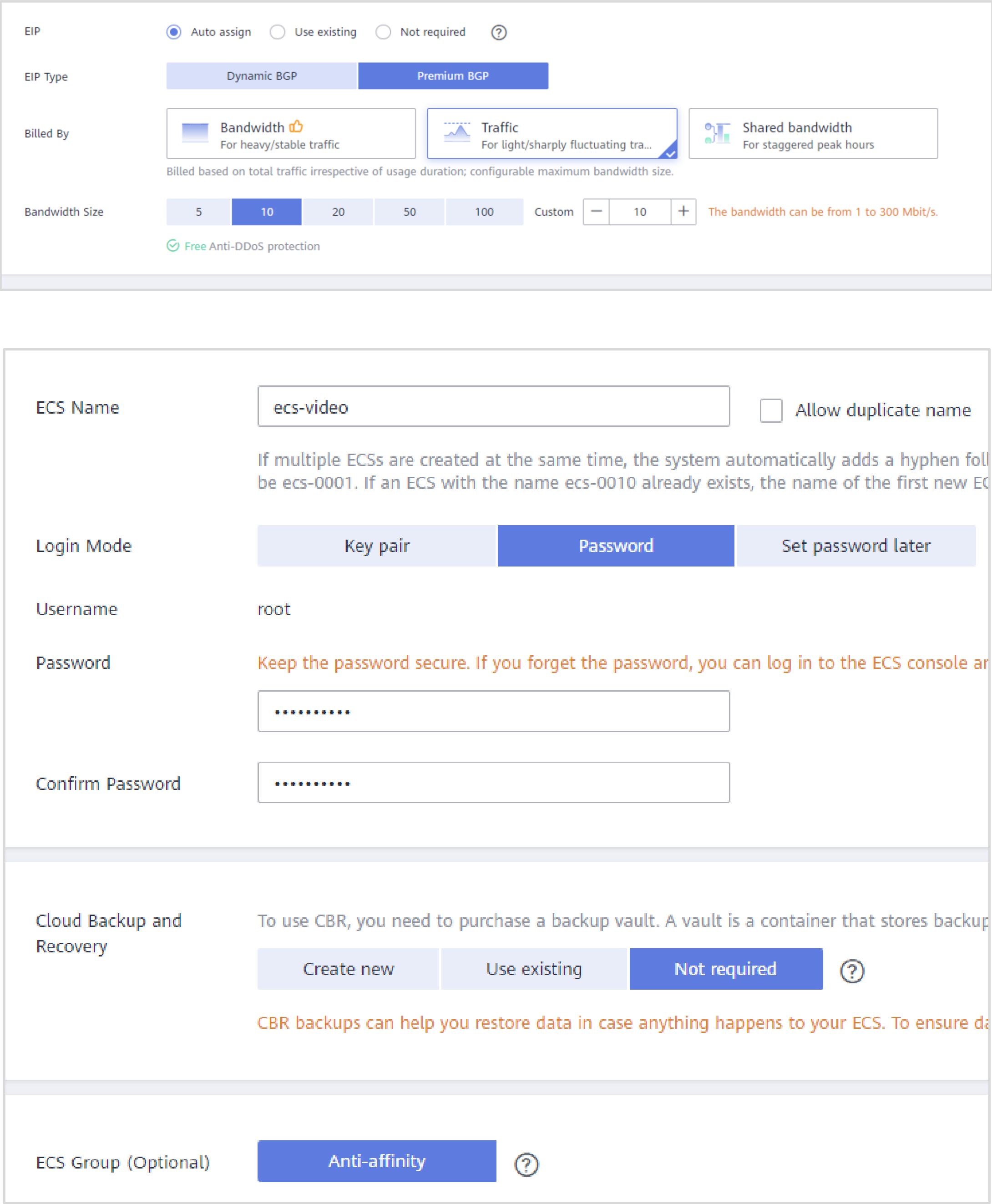
Extension NIC: Add NIC NICs you can still add: 11

Security Group: sg-video (376b42b7-87ae-4fd9-9531-41f111f7eaf8) Create Security Group

Similar to a firewall, a security group logically controls network access.

Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

Security Group Rules



EIP: ● Auto assign ○ Use existing ○ Not required

EIP Type: Dynamic BGP | **Premium BGP**

Billed By: Bandwidth (For heavy/stable traffic) | **Traffic** (For light/sharply fluctuating tra...) | Shared bandwidth (For staggered peak hours)

Billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size.

Bandwidth Size: 5 | **10** | 20 | 50 | 100 | Custom − 10 +

The bandwidth can be from 1 to 300 Mbit/s.

Free Anti-DDoS protection

ECS Name: ecs-video

□ Allow duplicate name

If multiple ECSs are created at the same time, the system automatically adds a hyphen foll
be ecs-0001. If an ECS with the name ecs-0010 already exists, the name of the first new EC

Login Mode: Key pair | **Password** | Set password later

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console ar

••••••••••

Confirm Password: ••••••••••

Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backup

Create new | Use existing | **Not required**

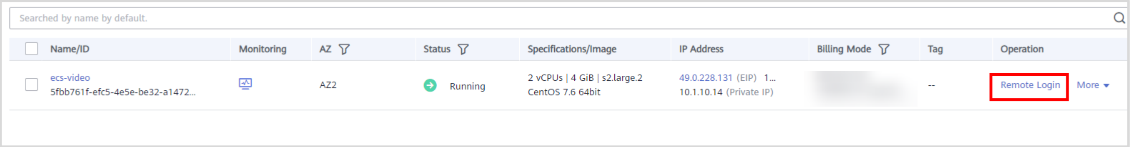
CBR backups can help you restore data in case anything happens to your ECS. To ensure da

ECS Group (Optional): Anti-affinity

Figure 3-16

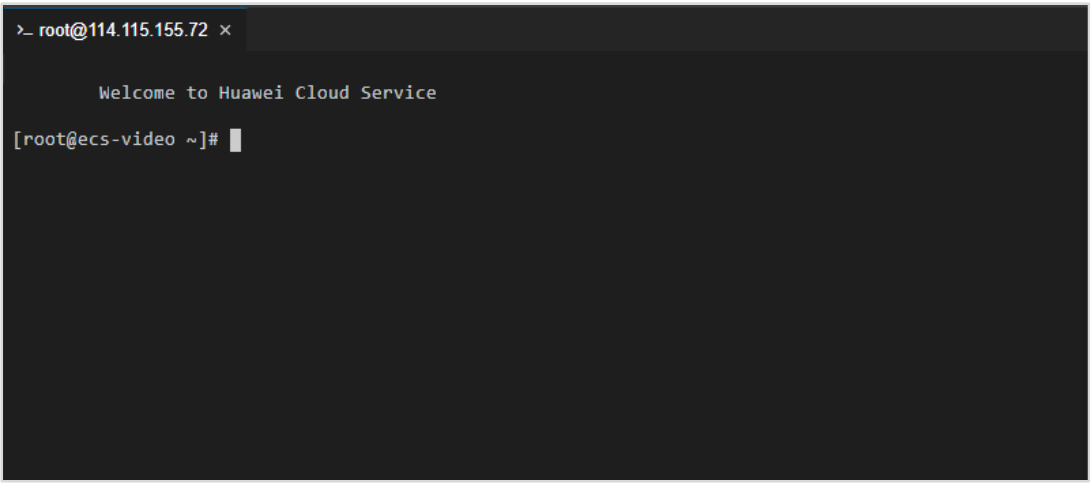
3.2.7 Mounting the SFS File System

Step 1 In the ECS list, locate the created ECS and click **Remote Login** to log in to **ecs-video** using CloudShell.



Searched by name by default.

□	Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mode	Tag	Operation
□	ecs-video 5fbb761f-efc5-4e5e-be32-a1472...		AZ2	Running	2 vCPUs | 4 GiB | s2.large.2 CentOS 7.6 64bit	49.0.228.131 (EIP) 1... 10.1.10.14 (Private IP)	[redacted]	--	Remote Login More

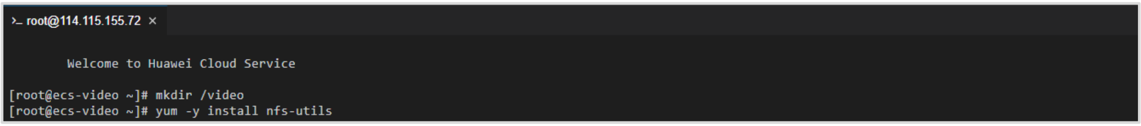


```
        Welcome to Huawei Cloud Service

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

Figure 3-17

Step 2 Run the following commands to create the **video** folder and install the NFS client:

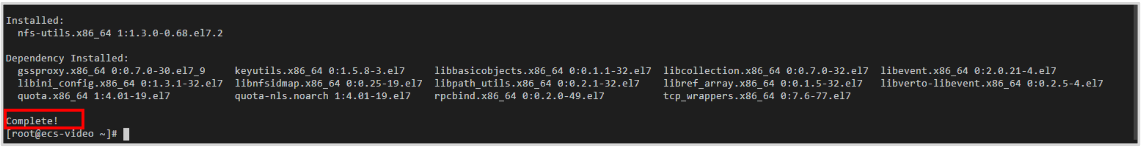
```
[root@ecs-video ~]# mkdir /video
[root@ecs-video ~]# yum -y install nfs-utils
```



```
        Welcome to Huawei Cloud Service

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

Figure 3-18

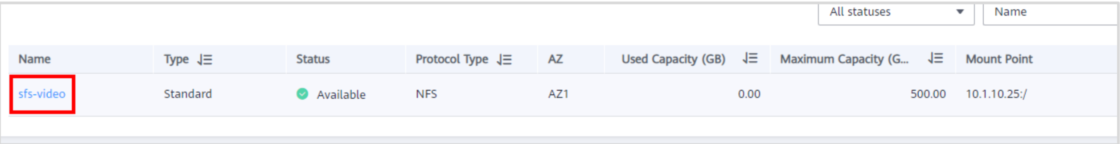
If **Complete** is displayed, the NFS client has been installed:



```
Installed:
  nfs-utils.x86_64 1:1.3.0-0.68.el7.2

Dependency Installed:
  gssproxy.x86_64 0:0.7.0-30.el7_9      keyutils.x86_64 0:1.5.8-3.el7     libbasicobjects.x86_64 0:0.1.1-32.el7  libcollection.x86_64 0:0.7.0-32.el7  libevent.x86_64 0:2.0.21-4.el7
  libini_config.x86_64 0:1.3.1-32.el7  libnfsidmap.x86_64 0:0.25-19.el7  libpath_utils.x86_64 0:0.2.1-32.el7    libref_array.x86_64 0:0.1.5-32.el7   libverto-libevent.x86_64 0:0.2.5-4.el7
  quota.x86_64 1:4.01-19.el7           quota-nls.noarch 1:4.01-19.el7    rpcbind.x86_64 0:0.2.0-49.el7          tcp_wrappers.x86_64 0:7.6-77.el7

Complete!
[root@ecs-video ~]#
```

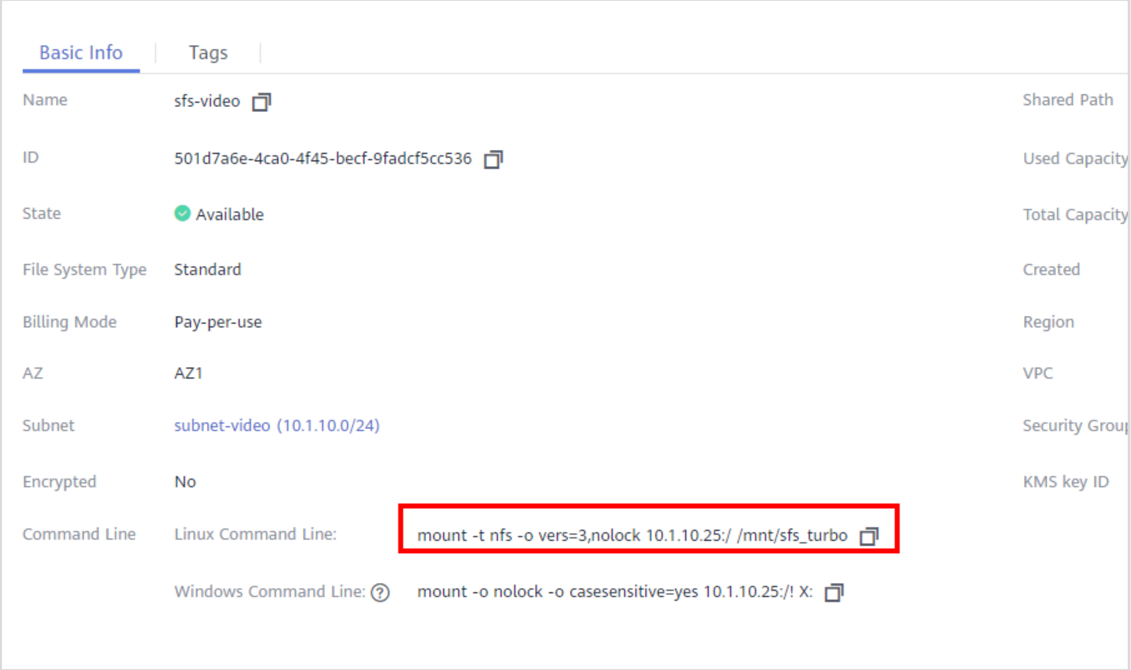
Figure 3-19

Step 3 Go back to the Huawei Cloud console, choose **Scalable File Service** > **SFS Turbo**, and click the name of the created SFS file system to go to the details page.



Name	Type	Status	Protocol Type	AZ	Used Capacity (GB)	Maximum Capacity (G...	Mount Point
sfs-video	Standard	Available	NFS	AZ1	0.00	500.00	10.1.10.25:/

Step 4 Take note of the mount command.



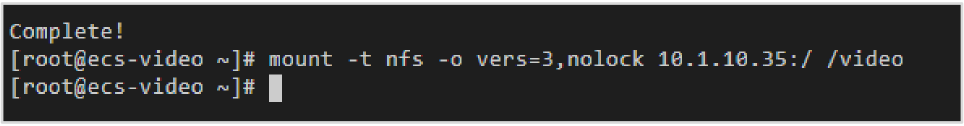
Name	sfs-video	Shared Path
ID	501d7a6e-4ca0-4f45-becf-9fadcf5cc536	Used Capacity
State	Available	Total Capacity
File System Type	Standard	Created
Billing Mode	Pay-per-use	Region
AZ	AZ1	VPC
Subnet	subnet-video (10.1.10.0/24)	Security Grou
Encrypted	No	KMS key ID
Command Line	Linux Command Line: mount -t nfs -o vers=3,nolock 10.1.10.25:/ /mnt/sfs_turbo Windows Command Line: mount -o nolock -o casesensitive=yes 10.1.10.25:/! X:	

Figure 3-20

Step 5 Log in to **esc-video** and run the following command to mount the SFS file system:

```
[root@ecs-video ~]# mount -t nfs -o vers=3,nolock 10.1.10.25:/ /video
```

Note: Replace the "mount -t nfs -o vers=3,nolock 10.1.10.25:/" part in the preceding command with what you have taken note of in the last step.



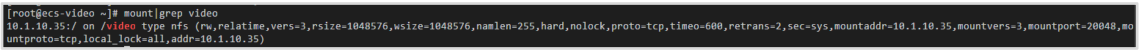
```
Complete!
[root@ecs-video ~]# mount -t nfs -o vers=3,nolock 10.1.10.35:/ /video
[root@ecs-video ~]#
```

Figure 3-21

Step 6 Run the following command to verify the mounting:

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

If the following information is displayed, the file system has been mounted.



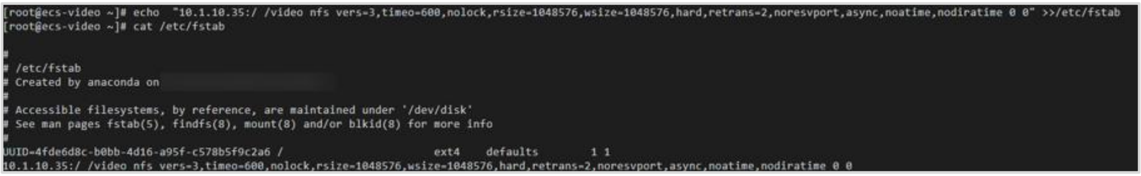
```
[root@ecs-video ~]# mount|grep video
10.1.10.35:/ on /video type nfs (rw,relatime,vers=3,rsize=1048576,wsize=1048576,namlen=255,hard,nolock,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=10.1.10.35,mountvers=3,mountport=20048,mo
untproto=tcp,local_lock=all,addr=10.1.10.35)
```

Figure 3-22

Step 7 Run the following command to configure automatic mounting at system start:

```
[root@ecs-video ~]#echo "10.1.10.25:/ /video nfs
vers=3,timeo=600,nolock,rsize=1048576,wsize=1048576,hard,retrans=2,noresvport,async,noatime,nodi
ratime 0 0" >>/etc/fstab
```

Note: The IP address in the command varies with the file system. Use the actual IP address of the file system.



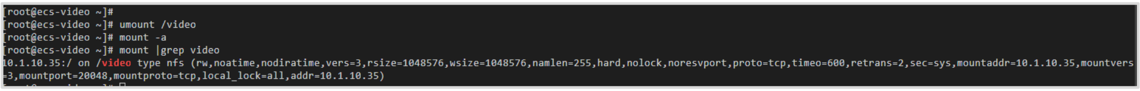
```
[root@ecs-video ~]# echo  "10.1.10.35:/ /video nfs vers=3,timeo=600,nolock,rsize=1048576,wsize=1048576,hard,retrans=2,noresvport,async,noatime,nodiratime 0 0" >>/etc/fstab
[root@ecs-video ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on [redacted]
#
# 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
```

Figure 3-23

Step 8 Run the following commands to verify automatic mounting:

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

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

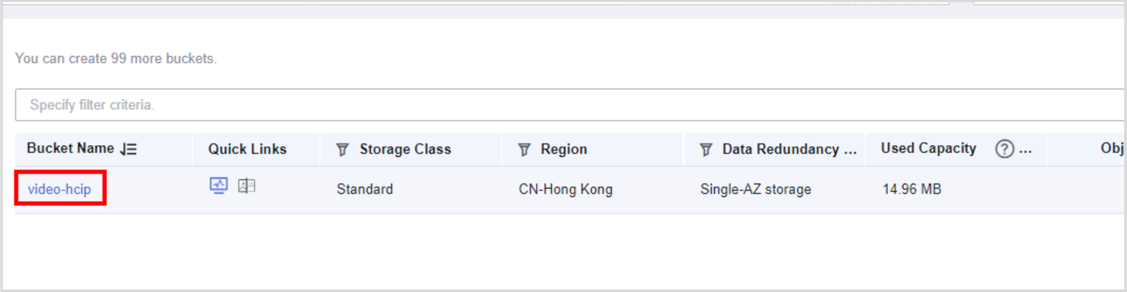


```
[root@ecs-video ~]#
[root@ecs-video ~]# umount /video
[root@ecs-video ~]# mount -a
[root@ecs-video ~]# mount |grep video
10.1.10.35:/ on /video type nfs (rw,noatime,nodiratime,vers=3,rsize=1048576,wsize=1048576,namlen=255,hard,nolock,noresvport,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=10.1.10.35,mountvers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

Figure 3-24

3.2.8 Downloading the Object File

Step 1 In the CN-Hong Kong region, choose **Object Storage Service** > **Object Storage**. In the bucket list, click the name of the created bucket **video-hcip** to go to the configuration page.



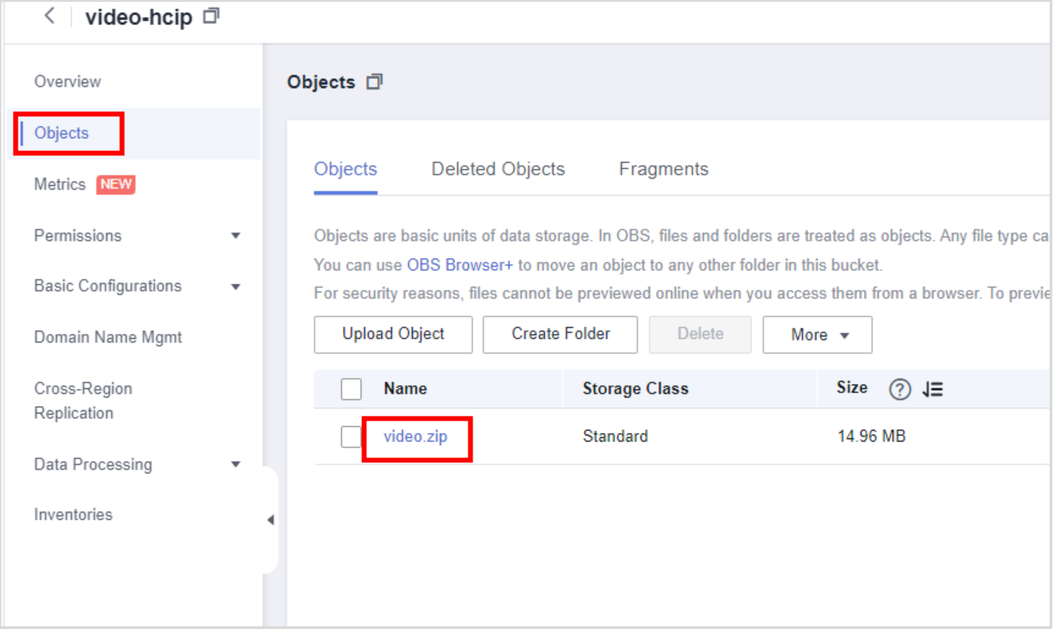
You can create 99 more buckets.

Specify filter criteria.

Bucket Name	Quick Links	Storage Class	Region	Data Redundancy ...	Used Capacity	...	Obj
video-hcip		Standard	CN-Hong Kong	Single-AZ storage	14.96 MB		

Figure 3-25

Step 2 On the **Objects** page, click the name of **video.zip** in the object list.



video-hcip

Overview
Objects
Metrics NEW
Permissions
Basic Configurations
Domain Name Mgmt
Cross-Region Replication
Data Processing
Inventories

Objects

Objects | Deleted Objects | Fragments

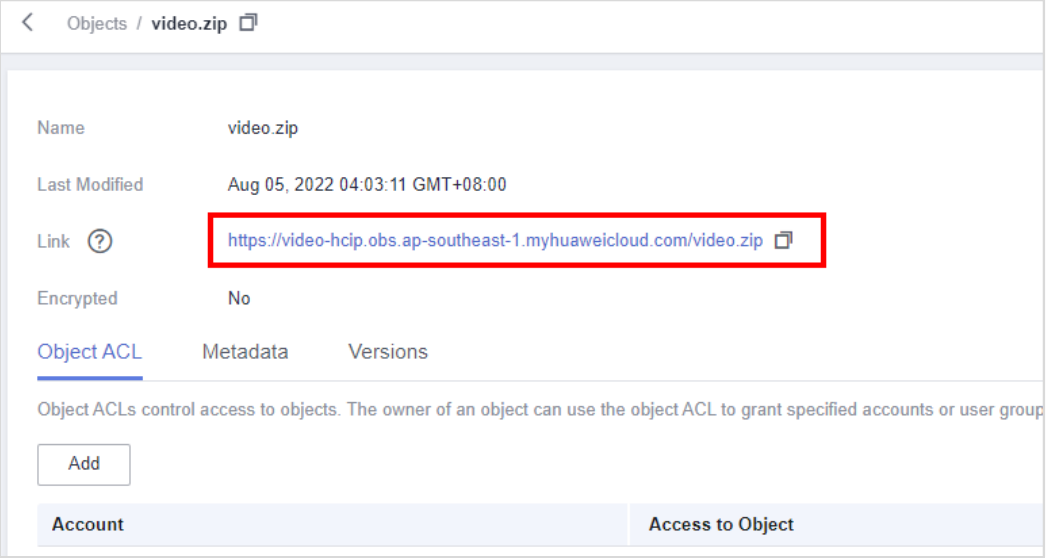
Objects are basic units of data storage. In OBS, files and folders are treated as objects. Any file type ca
You can use OBS Browser+ to move an object to any other folder in this bucket.
For security reasons, files cannot be previewed online when you access them from a browser. To previe

Upload Object | Create Folder | Delete | More

□	Name	Storage Class	Size
□	video.zip	Standard	14.96 MB

Figure 3-26

Step 3 View and take note of the object link.



Objects / video.zip

Name video.zip

Last Modified Aug 05, 2022 04:03:11 GMT+08:00

Link https://video-hcip.obs.ap-southeast-1.myhuaweicloud.com/video.zip

Encrypted No

Object ACL | Metadata | Versions

Object ACLs control access to objects. The owner of an object can use the object ACL to grant specified accounts or user group

Add

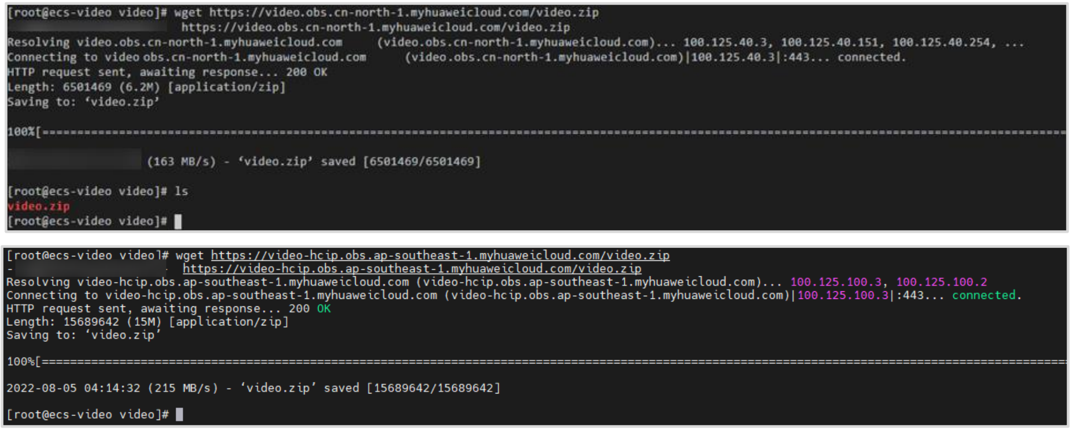
Account	Access to Object

Figure 3-27

Step 4 Log in to **esc-video** and run the following commands to download the object file:

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

Note: The object link in the command varies with the object. Use the one you have taken note of in the last step.



```
[root@ecs-video video]# wget https://video.obs.cn-north-1.myhuaweicloud.com/video.zip
[redacted]                 https://video.obs.cn-north-1.myhuaweicloud.com/video.zip
Resolving video.obs.cn-north-1.myhuaweicloud.com    (video.obs.cn-north-1.myhuaweicloud.com)... 100.125.40.3, 100.125.40.151, 100.125.40.254, ...
Connecting to video obs.cn-north-1.myhuaweicloud.com     (video.obs.cn-north-1.myhuaweicloud.com)|100.125.40.3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6501469 (6.2M) [application/zip]
Saving to: ‘video.zip’

100%[==================================================================================================================================]

[redacted]          (163 MB/s) - ‘video.zip’ saved [6501469/6501469]

[root@ecs-video video]# ls
video.zip
[root@ecs-video video]# █
```

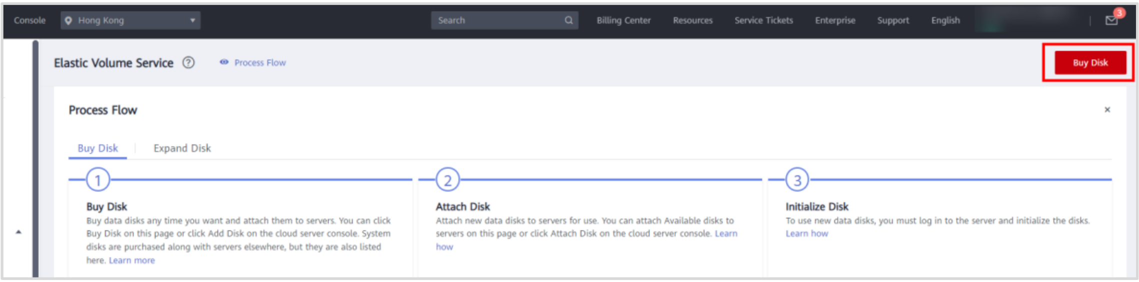
```
[root@ecs-video video]# wget https://video-hcip.obs.ap-southeast-1.myhuaweicloud.com/video.zip
- [redacted]            https://video-hcip.obs.ap-southeast-1.myhuaweicloud.com/video.zip
Resolving video-hcip.obs.ap-southeast-1.myhuaweicloud.com (video-hcip.obs.ap-southeast-1.myhuaweicloud.com)... 100.125.100.3, 100.125.100.2
Connecting to video-hcip.obs.ap-southeast-1.myhuaweicloud.com (video-hcip.obs.ap-southeast-1.myhuaweicloud.com)|100.125.100.3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15689642 (15M) [application/zip]
Saving to: ‘video.zip’

100%[==================================================================================================================================]

2022-08-05 04:14:32 (215 MB/s) - ‘video.zip’ saved [15689642/15689642]

[root@ecs-video video]# █
```

Figure 3-28

3.2.9 Attaching an EVS Disk

Step 1 In the CN-Hong Kong region, choose **Elastic Volume Service** > **Disks** and click **Buy Disk** in the upper right corner.

Note: This disk will be attached to **ecs-video**, and Nginx will be installed on this disk.



Buy Disk
Buy data disks any time you want and attach them to servers. You can click Buy Disk on this page or click Add Disk on the cloud server console. System disks are purchased along with servers elsewhere, but they are also listed here. Learn more

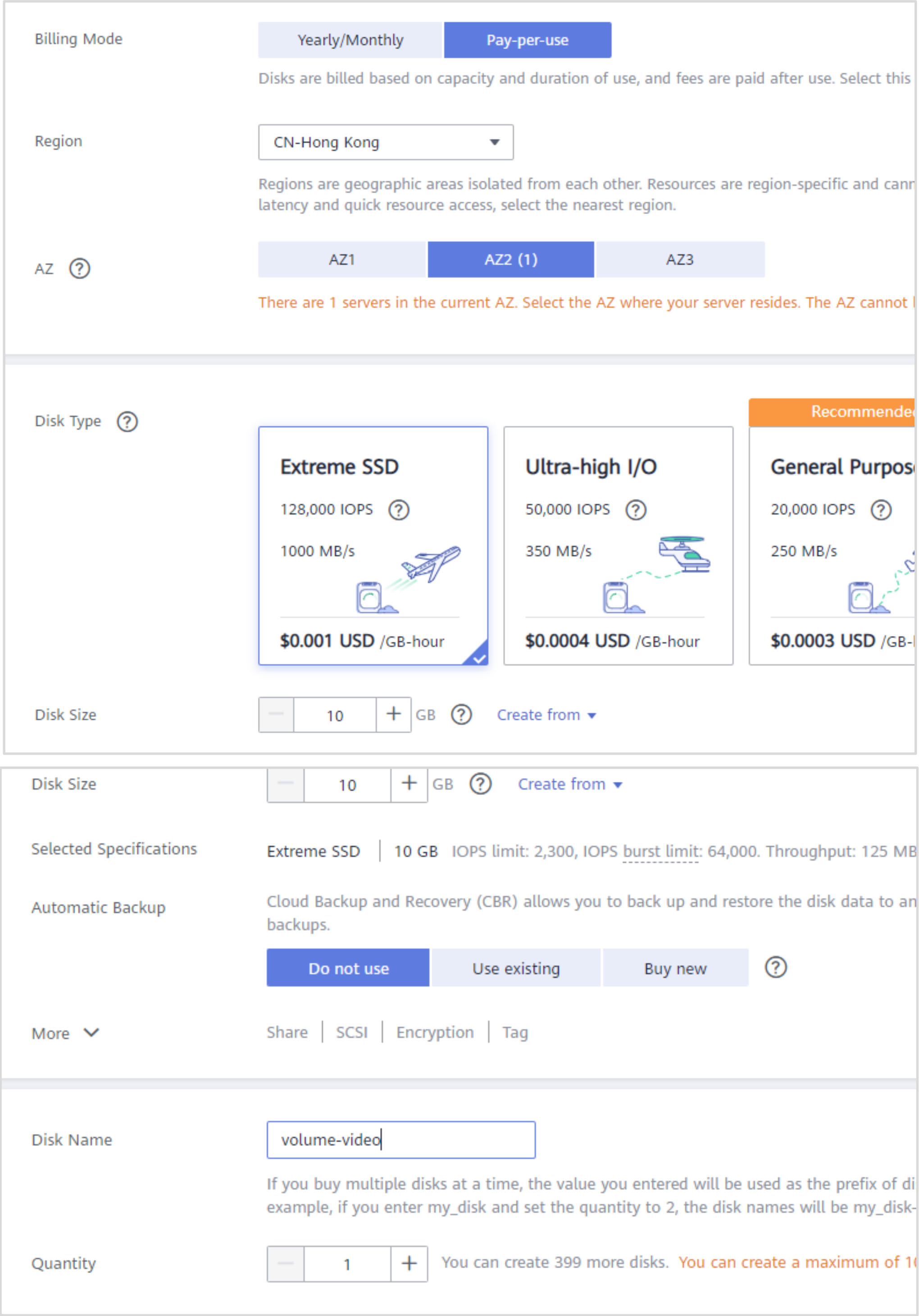
Attach Disk
Attach new data disks to servers for use. You can attach Available disks to servers on this page or click Attach Disk on the cloud server console. Learn how

Initialize Disk
To use new data disks, you must log in to the server and initialize the disks. Learn how

Figure 3-29

Step 2 Configure the parameters as follows, confirm the configuration, and click **Next**.

- Billing Mode: Pay-per-use
- Region: CN-Hong Kong
- AZ: AZ2
- Disk Type: Ultra-high I/O
- Disk Size: 10 GB
- Automatic Backup: Do not use
- Disk Name: volume-video



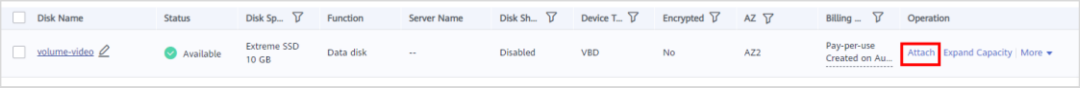
Billing Mode	Yearly/Monthly [✓ Pay-per-use] Disks are billed based on capacity and duration of use, and fees are paid after use. Select this
Region	CN-Hong Kong ▾ Regions are geographic areas isolated from each other. Resources are region-specific and cann latency and quick resource access, select the nearest region.
AZ ⓘ	AZ1 [✓ AZ2 (1)] AZ3 There are 1 servers in the current AZ. Select the AZ where your server resides. The AZ cannot
Disk Type ⓘ	[✓ Extreme SSD 128,000 IOPS 1000 MB/s $0.001 USD /GB-hour] | Ultra-high I/O 50,000 IOPS 350 MB/s $0.0004 USD /GB-hour | Recommende General Purpos 20,000 IOPS 250 MB/s $0.0003 USD /GB-
Disk Size	— 10 + GB ⓘ Create from ▾

Disk Size — 10 + GB ⓘ Create from ▾

Selected Specifications	Extreme SSD | 10 GB IOPS limit: 2,300, IOPS burst limit: 64,000. Throughput: 125 MB
Automatic Backup	Cloud Backup and Recovery (CBR) allows you to back up and restore the disk data to an backups. [✓ Do not use] Use existing Buy new ⓘ
More ⌄	Share | SCSI | Encryption | Tag
Disk Name	volume-video If you buy multiple disks at a time, the value you entered will be used as the prefix of di example, if you enter my_disk and set the quantity to 2, the disk names will be my_disk-
Quantity	— 1 + You can create 399 more disks. You can create a maximum of 1

Figure 3-30

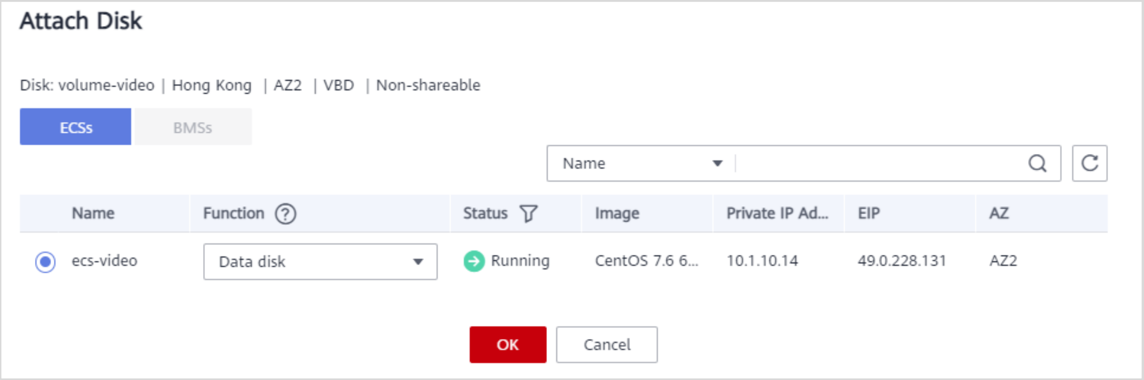
Step 3 In the EVS disk list, view the created **ecs-video** disk and click **Attach**.



□ Disk Name	Status	Disk Sp...	Function	Server Name	Disk Sh...	Device T...	Encrypted	AZ	Billing ...	Operation
□ volume-video	Available	Extreme SSD 10 GB	Data disk	--	Disabled	VBD	No	AZ2	Pay-per-use Created on Au...	Attach Expand Capacity | More ▾

Figure 3-31

Step 4 In the displayed dialog box, select **ECSs**, select **ecs-video**, and click **OK**.



Attach Disk

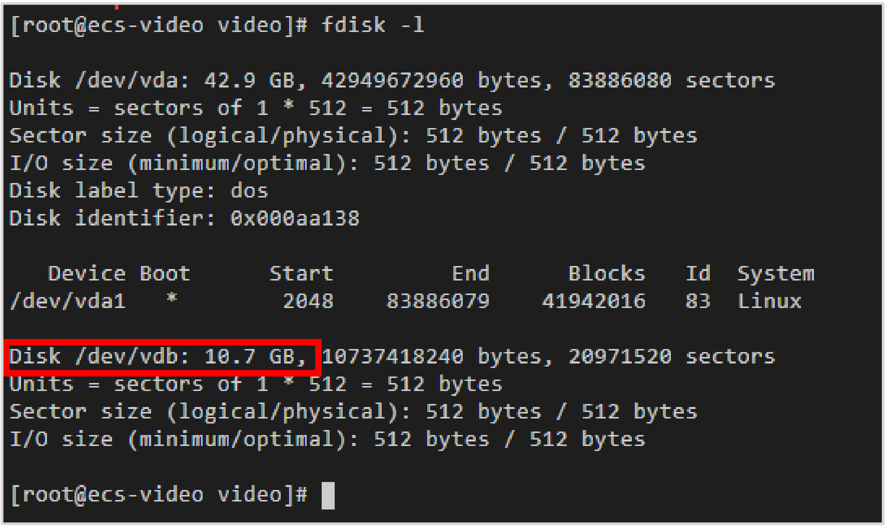
Disk: volume-video | Hong Kong | AZ2 | VBD | Non-shareable

	Name	Function	Status	Image	Private IP Ad...	EIP	AZ
●	ecs-video	Data disk	Running	CentOS 7.6 6...	10.1.10.14	49.0.228.131	AZ2

Figure 3-32

Step 5 Log in to **ecs-video** and run the following command to view the disk information:

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

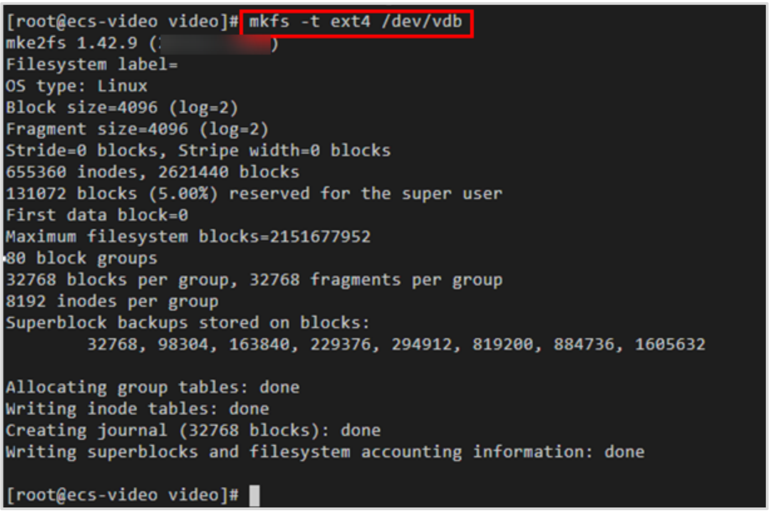


```
[root@ecs-video video]# fdisk -l

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]#
```

Figure 3-33

Step 6 Run the following command to create a file system for the disk: (Use the device name you have obtained in the last step.

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

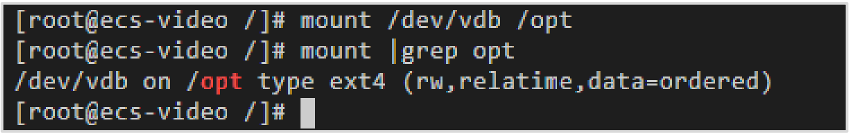


```
[root@ecs-video video]# mkfs -t ext4 /dev/vdb
mke2fs 1.42.9 ([redacted])
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
655360 inodes, 2621440 blocks
131072 blocks (5.00%) reserved for the super user
First data block=0
Maximum 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]#
```

Figure 3-34

Step 7 Run the following commands to mount the disk on **/opt** and check whether the mounting is successful:

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

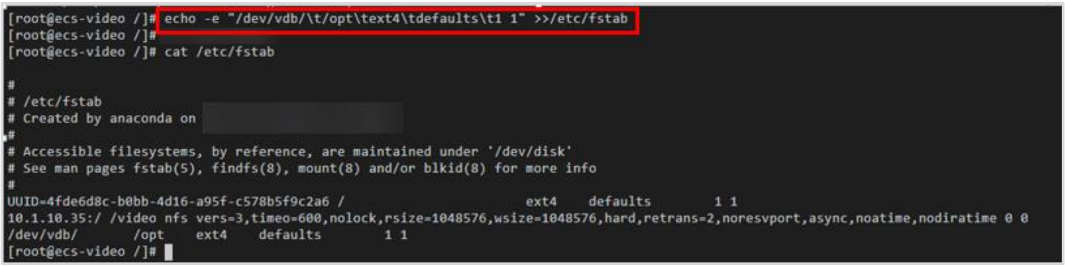


```
[root@ecs-video /]# mount /dev/vdb /opt
[root@ecs-video /]# mount |grep opt
/dev/vdb on /opt type ext4 (rw,relatime,data=ordered)
[root@ecs-video /]#
```

Figure 3-35

Step 8 Run the following command to configure automatic mounting at system start:

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

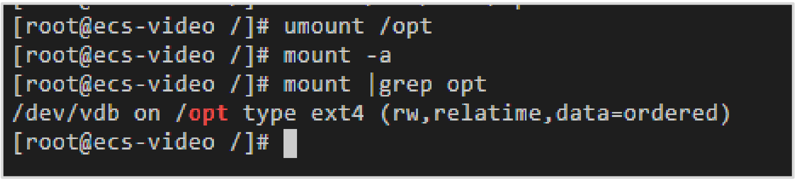


```
[root@ecs-video /]# echo -e "/dev/vdb/\t/opt\text4\tdefaults\t1 1" >>/etc/fstab
[root@ecs-video /]#
[root@ecs-video /]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on [redacted]
#
# 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 /]#
```

Figure 3-36

Step 9 Run the following commands to verify automatic mounting:

```
[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 /]#
```

Figure 3-37

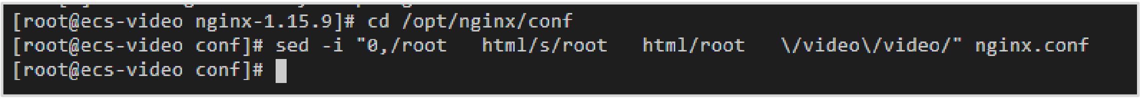
3.2.10 Compiling and Installing Nginx

Step 1 Log in to **ecs-video** and run the following commands to compile and install Nginx on the attached disk:

```
cd /video
yum install -y unzip
unzip -o video_en.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
```

Step 2 Run the following commands to edit the **nginx.conf** file:

```
[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
```

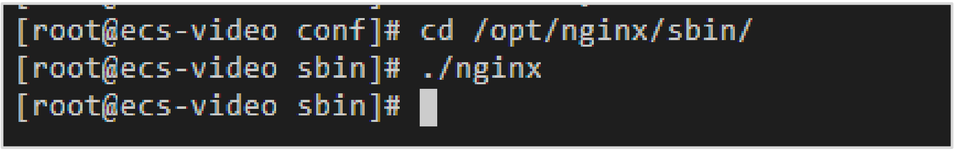


```
[root@ecs-video nginx-1.15.9]# cd /opt/nginx/conf
[root@ecs-video conf]# sed -i "0,/root    html/s/root    html/root    \/video\/video/" nginx.conf
[root@ecs-video conf]#
```

Figure 3-38

Step 3 # Run the following commands to start Nginx:

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

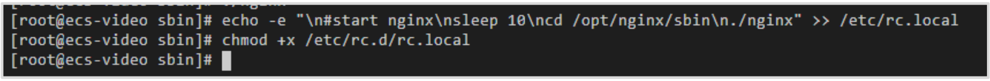


```
[root@ecs-video conf]# cd /opt/nginx/sbin/
[root@ecs-video sbin]# ./nginx
[root@ecs-video sbin]#
```

Figure 3-39

Step 4 Run the following commands to configure automatic startup:

```
[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
```



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

Figure 3-40

Step 5 Use a browser on the local PC to log in to **ecs-video** using the public IP address and verify that the video can be played. If the following figure shows up, the video can be played, indicating that the video streaming service has been set up.

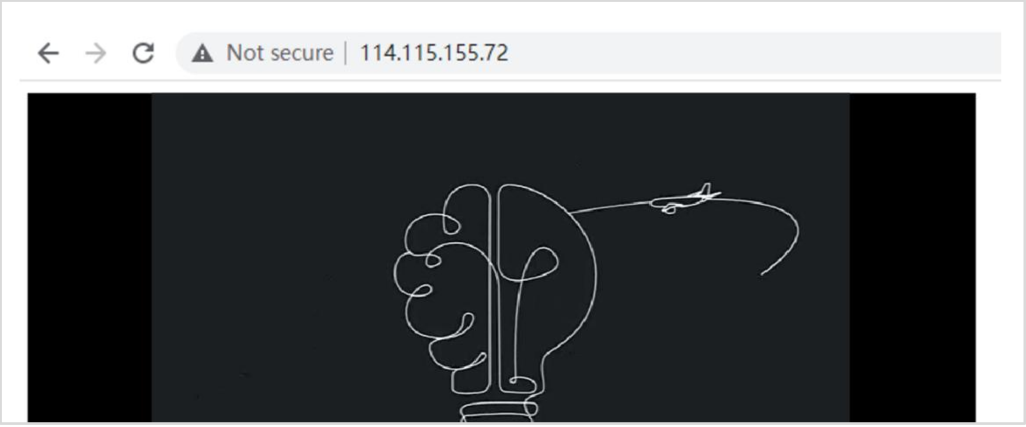


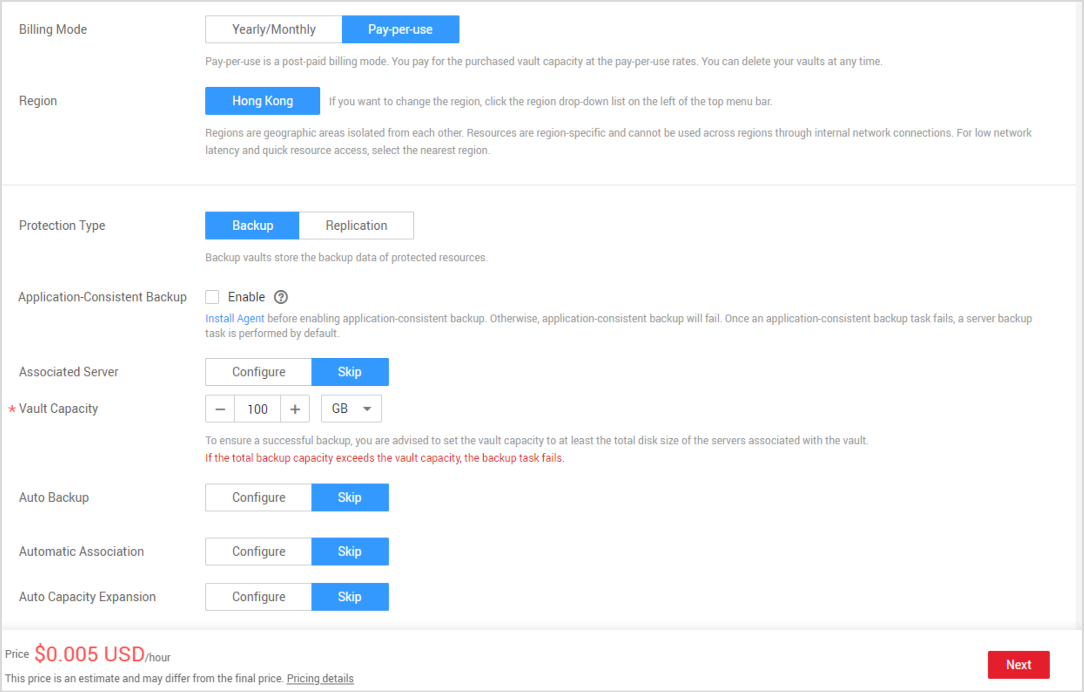
Figure 3-41

3.2.11 Configuring HA

Step 1 In the CN-Hong Kong region, choose **Storage** > **Cloud Backup and Recovery** > **Cloud Backup Backups** and click **Buy Server Backup Vault** in the upper right corner. Configure the parameters as follows to create a server backup vault.

Note: A full-ECS image will be created in this exercise, so a cloud server backup vault needs to be purchased in the first place.

- **Billing Mode**: **Pay-per-use**
- **Region**: CN-**Hong Kong**
- **Protection Type**: **Backup**
- **Associated Server**: **Skip**
- **Vault Capacity**: **100 GB**
- **Auto Backup**: **Skip**
- Retain the default settings for other parameters.



Billing Mode: Yearly/Monthly | Pay-per-use

Pay-per-use is a post-paid billing mode. You pay for the purchased vault capacity at the pay-per-use rates. You can delete your vaults at any time.

Region: Hong Kong — If you want to change the region, click the region drop-down list on the left of the top menu bar.

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

Protection Type: Backup | Replication

Backup vaults store the backup data of protected resources.

Application-Consistent Backup: □ Enable

Install Agent before enabling application-consistent backup. Otherwise, application-consistent backup will fail. Once an application-consistent backup task fails, a server backup task is performed by default.

Associated Server: Configure | Skip

* Vault Capacity: − 100 + GB

To ensure a successful backup, you are advised to set the vault capacity to at least the total disk size of the servers associated with the vault.

If the total backup capacity exceeds the vault capacity, the backup task fails.

Auto Backup: Configure | Skip

Automatic Association: Configure | Skip

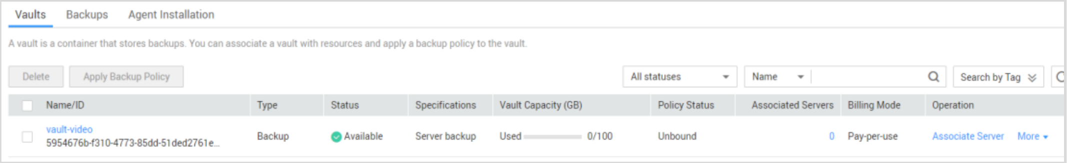
Auto Capacity Expansion: Configure | Skip

Price $0.005 USD/hour

This price is an estimate and may differ from the final price. Pricing details

Figure 3-42

Step 2 View the server backup vault you have created.



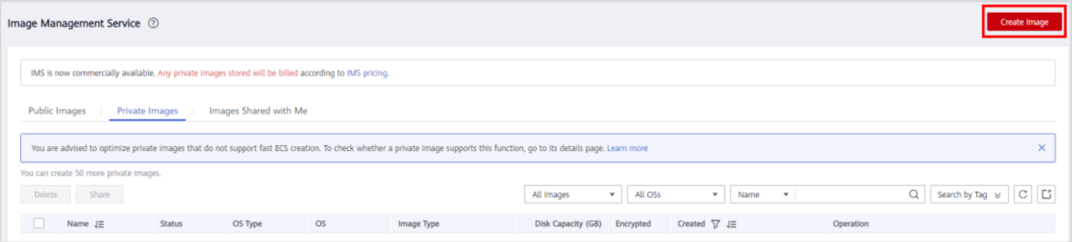
A vault is a container that stores backups. You can associate a vault with resources and apply a backup policy to the vault.

□	Name/ID	Type	Status	Specifications	Vault Capacity (GB)	Policy Status	Associated Servers	Billing Mode	Operation
□	vault-video 5954676b-f310-4773-85dd-51ded2761e...	Backup	● Available	Server backup	Used 0/100	Unbound	0	Pay-per-use	Associate Server More

Figure 3-43

Step 3 In the CN-Hong Kong region, choose **Image Management Service** and click **Create Image** in the upper right corner.

Note: An ECS will be provisioned using the full-ECS image. The new ECS and **ecs-video** will then be used as the ELB backend servers.



IMS is now commercially available. Any private images stored will be billed according to IMS pricing.

You are advised to optimize private images that do not support fast ECS creation. To check whether a private image supports this function, go to its details page. Learn more

You can create 50 more private images.

□	Name	Status	OS Type	OS	Image Type	Disk Capacity (GB)	Encrypted	Created	Operation

Figure 3-44

Step 4 Configure the parameters as follows, confirm the configuration, and click **Next**.

- **Region: CN-Hong Kong**
- **Type: Full-ECS image**
- **Source: ECS | ecs-video**

- **Server Backup Vault: vault-video**
- **Name: ecs-video**

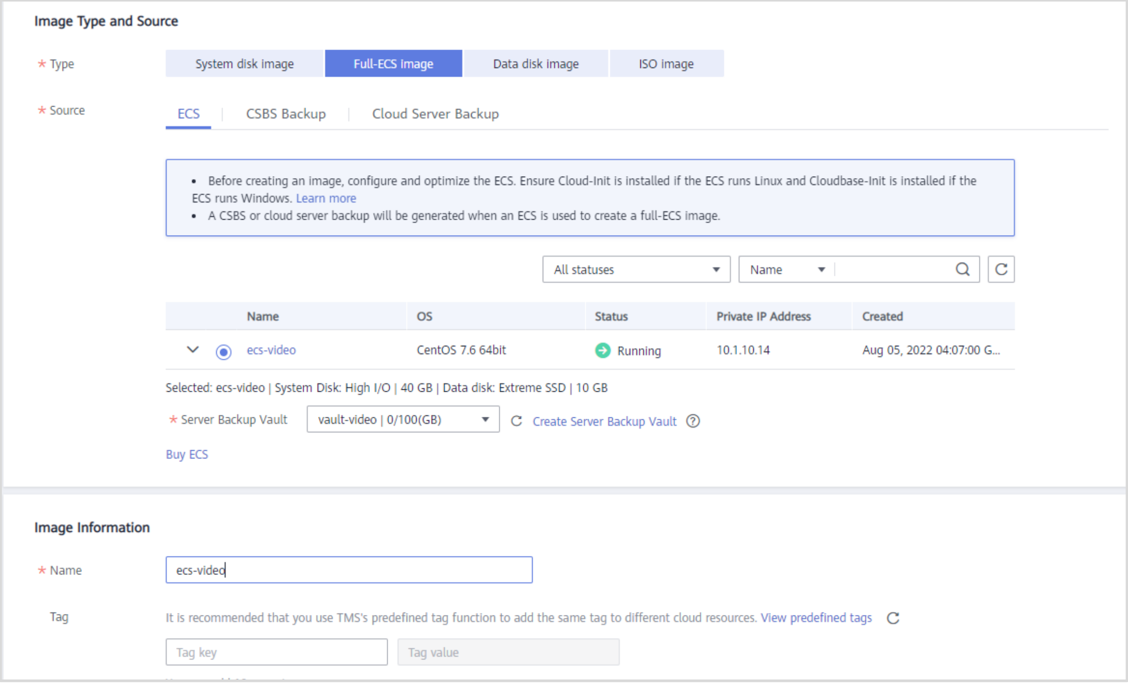


Image Type and Source

* Type: System disk image | **Full-ECS Image** | Data disk image | ISO image

* Source: **ECS** | CSBS Backup | Cloud Server Backup

- Before creating an image, configure and optimize the ECS. Ensure Cloud-Init is installed if the ECS runs Linux and Cloudbase-Init is installed if the ECS runs Windows. Learn more
- A CSBS or cloud server backup will be generated when an ECS is used to create a full-ECS image.

All statuses | Name

	Name	OS	Status	Private IP Address	Created
●	ecs-video	CentOS 7.6 64bit	Running	10.1.10.14	Aug 05, 2022 04:07:00 G...

Selected: ecs-video | System Disk: High I/O | 40 GB | Data disk: Extreme SSD | 10 GB

* Server Backup Vault: vault-video | 0/100(GB) Create Server Backup Vault

Buy ECS

Image Information

* Name: ecs-video

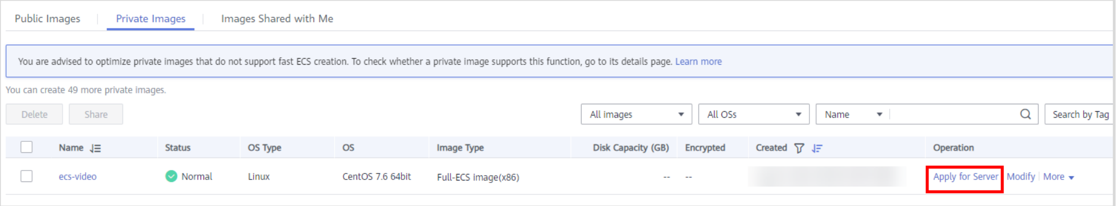
Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

Tag key | Tag value

Figure 3-45

Step 5 Click **Apply for Server** to create **ecs-video2** in AZ1 using the created image. (**ecs-video** resides in AZ2.)

Note: To ensure HA, **ecs-video** and **ecs-video2** are deployed in different AZs. You can select the AZs based on site requirements.



Public Images | **Private Images** | Images Shared with Me

You are advised to optimize private images that do not support fast ECS creation. To check whether a private image supports this function, go to its details page. Learn more

You can create 49 more private images.

Delete | Share | All images | All OSs | Name | Search by Tag

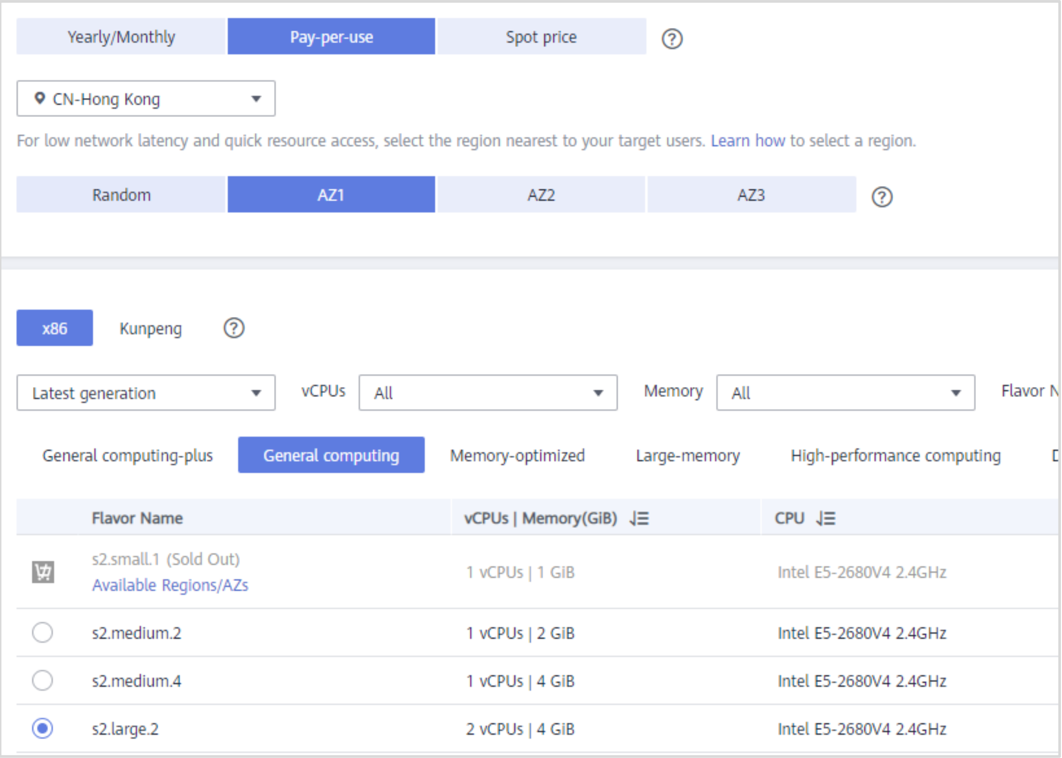
□	Name	Status	OS Type	OS	Image Type	Disk Capacity (GB)	Encrypted	Created	Operation
□	ecs-video	Normal	Linux	CentOS 7.6 64bit	Full-ECS image(x86)	--	--	[redacted]	Apply for Server Modify More

Figure 3-46

Step 6 Configure the parameters as follows:

- **Billing Mode: Pay-per-use**
- **Region: CN-Hong Kong**
- **AZ: AZ1**
- **Specifications: 2 vCPUs | 4 GiB**
- **Image: Private image | ecs-video**
- **System Disk: High I/O | 40 GiB**
- **Data Disk: Extreme SSD | 10 GB**
- **Network: vpc-video | subnet-video**

- **Security Group: sg-video**
- **EIP: Not required**
- **ECS Name: ecs-video2**
- **Password**: User-defined (with the username of **root**)



For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

	Flavor Name	vCPUs | Memory(GiB)	CPU
	s2.small.1 (Sold Out) Available Regions/AZs	1 vCPUs | 1 GiB	Intel E5-2680V4 2.4GHz
○	s2.medium.2	1 vCPUs | 2 GiB	Intel E5-2680V4 2.4GHz
○	s2.medium.4	1 vCPUs | 4 GiB	Intel E5-2680V4 2.4GHz
●	s2.large.2	2 vCPUs | 4 GiB	Intel E5-2680V4 2.4GHz

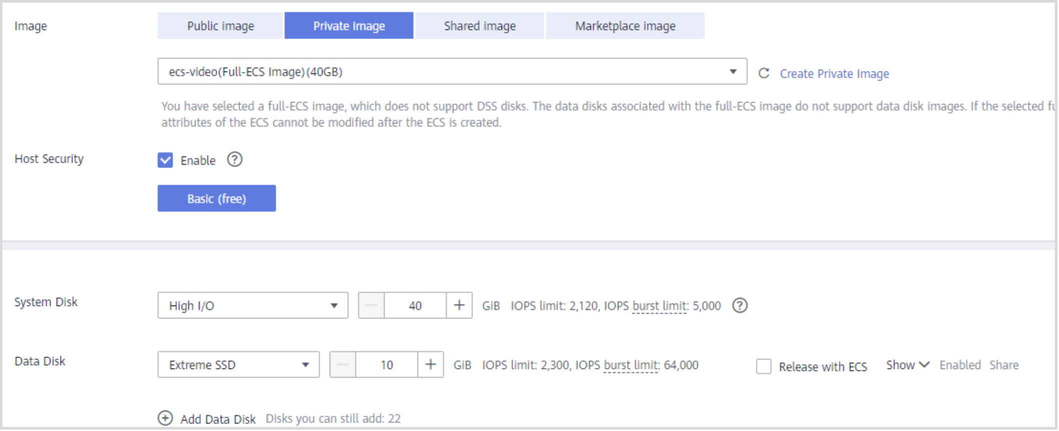


Image: Private image — ecs-video(Full-ECS Image)(40GB)

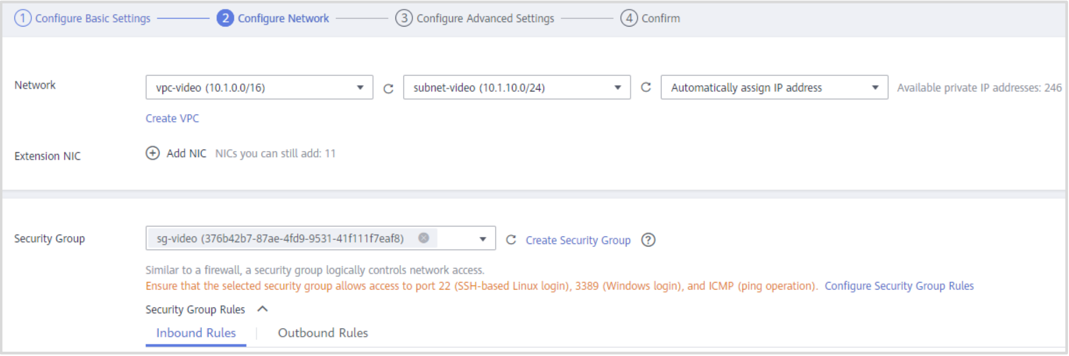
You have selected a full-ECS image, which does not support DSS disks. The data disks associated with the full-ECS image do not support data disk images. If the selected fu attributes of the ECS cannot be modified after the ECS is created.

Host Security: ☑ Enable

System Disk: High I/O 40 GiB IOPS limit: 2,120, IOPS burst limit: 5,000

Data Disk: Extreme SSD 10 GiB IOPS limit: 2,300, IOPS burst limit: 64,000 □ Release with ECS Show Enabled Share

Add Data Disk Disks you can still add: 22



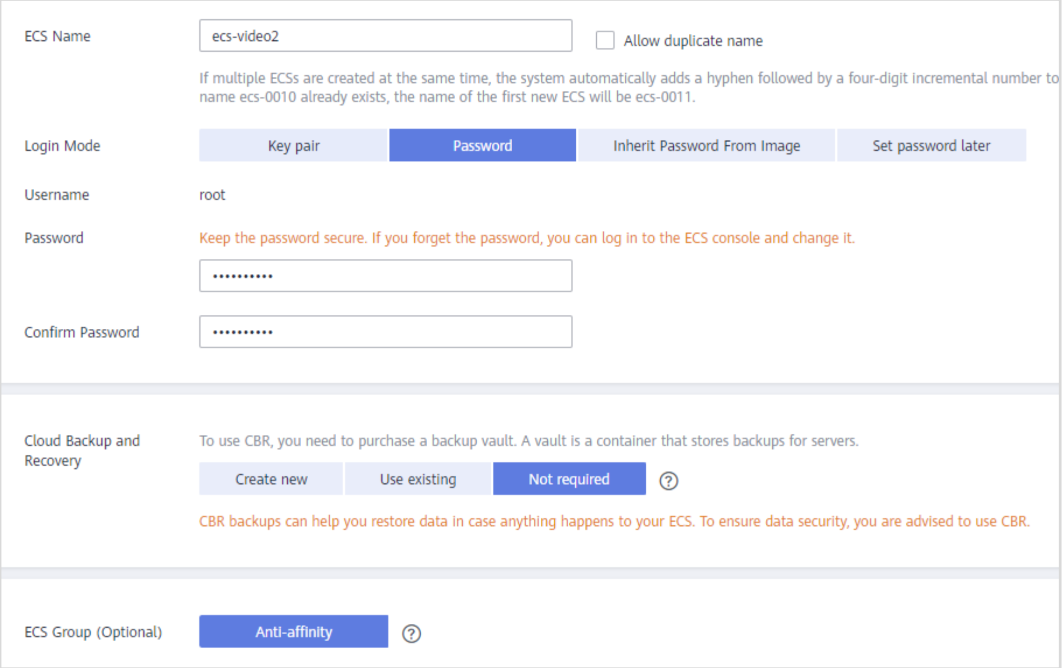
Network: vpc-video (10.1.0.0/16) subnet-video (10.1.10.0/24) Automatically assign IP address Available private IP addresses: 246

Extension NIC: Add NIC NICs you can still add: 11

Security Group: sg-video (376b42b7-87ae-4fd9-9531-41f111f7eaf8)

Similar to a firewall, a security group logically controls network access.
Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation).

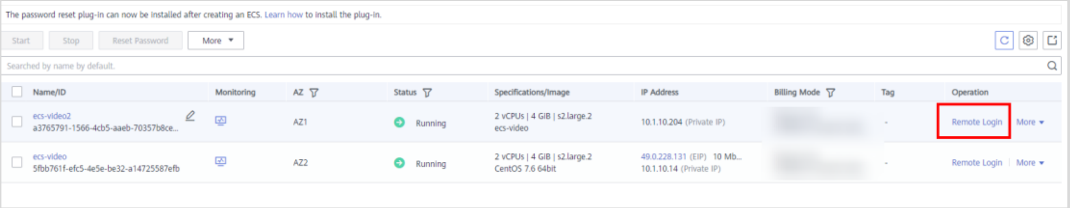
Security Group Rules



ECS Name	ecs-video2 □ Allow duplicate name If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a four-digit incremental number to name ecs-0010 already exists, the name of the first new ECS will be ecs-0011.
Login Mode	Key pair | **Password** | Inherit Password From Image | Set password later
Username	root
Password	Keep the password secure. If you forget the password, you can log in to the ECS console and change it. ••••••••••
Confirm Password	••••••••••
Cloud Backup and Recovery	To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers. Create new | Use existing | **Not required** CBR backups can help you restore data in case anything happens to your ECS. To ensure data security, you are advised to use CBR.
ECS Group (Optional)	Anti-affinity

Figure 3-47

Step 7 In the ECS list, locate the created **esc-video2** and click **Remote Login** to log in to the ECS using CloudShell.



The password reset plug-in can now be installed after creating an ECS. Learn how to install the plug-in.
Start
Stop
Reset Password
More
Searched by name by default.

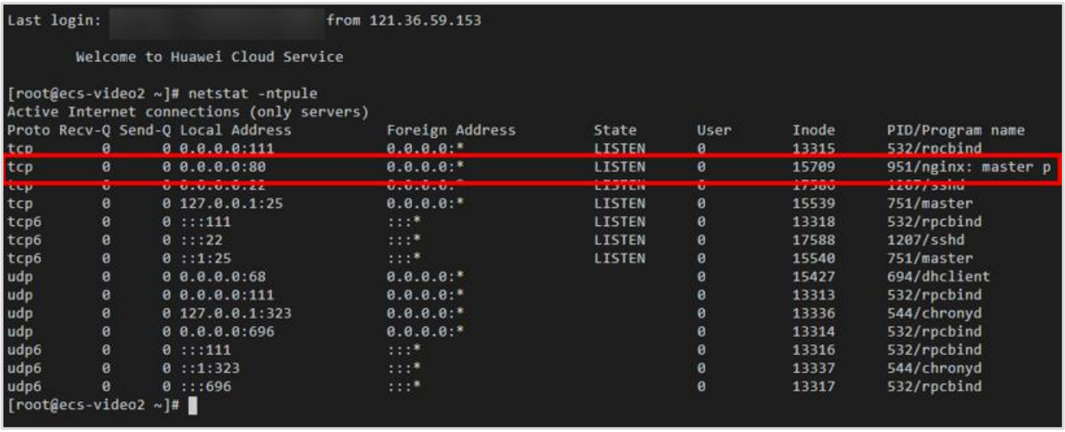
Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mode	Tag	Operation
ecs-video2 a3765791-1566-4cb5-aaeb-70357b8ce...		AZ1	Running	2 vCPUs | 4 GiB | s2.large.2 ecs-video	10.1.10.204 (Private IP)	[redacted]	-	Remote Login More
ecs-video 5fbb761f-efc5-4e5e-be32-a14725587efb		AZ2	Running	2 vCPUs | 4 GiB | s2.large.2 CentOS 7.6 64bit	49.0.228.131 (EIP) 10 Mb... 10.1.10.14 (Private IP)	[redacted]	-	Remote Login More

Figure 3-48

Step 8 Run the following command to check the service status:

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

If the following information is displayed, the Nginx service has been enabled.

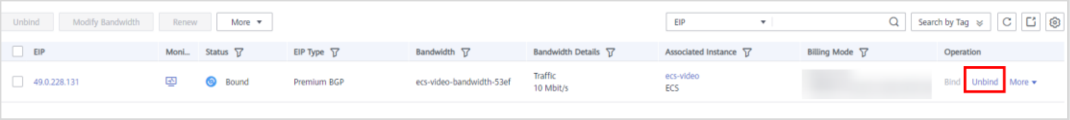


```
Last login: [redacted] from 121.36.59.153

        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          17580      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 ~]#
```

Figure 3-49

Step 9 In the service list, choose **Elastic IP**. In the EIP list, locate the EIP bound to **ecs-video** and click **Unbind** to unbind the EIP from **ecs-video**.

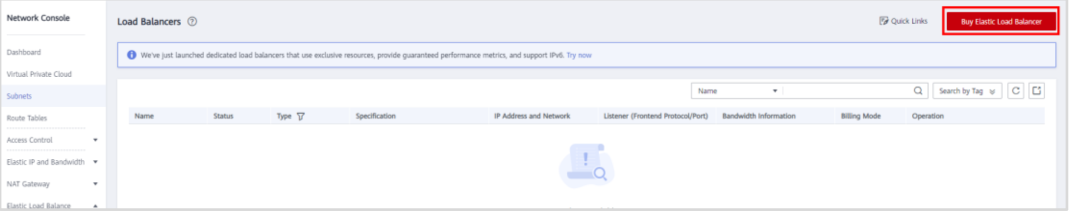
Note: This EIP will then be bound to the load balancer.



EIP	Moni...	Status	EIP Type	Bandwidth	Bandwidth Details	Associated Instance	Billing Mode	Operation
49.0.228.131		Bound	Premium BGP	ecs-video-bandwidth-53ef	Traffic 10 Mbit/s	ecs-video ECS	[redacted]	Bind Unbind More

Figure 3-50

Step 10 In the CN-Hong Kong region, choose **Elastic Load Balance** and click **Buy Elastic Load Balancer** in the upper right corner.



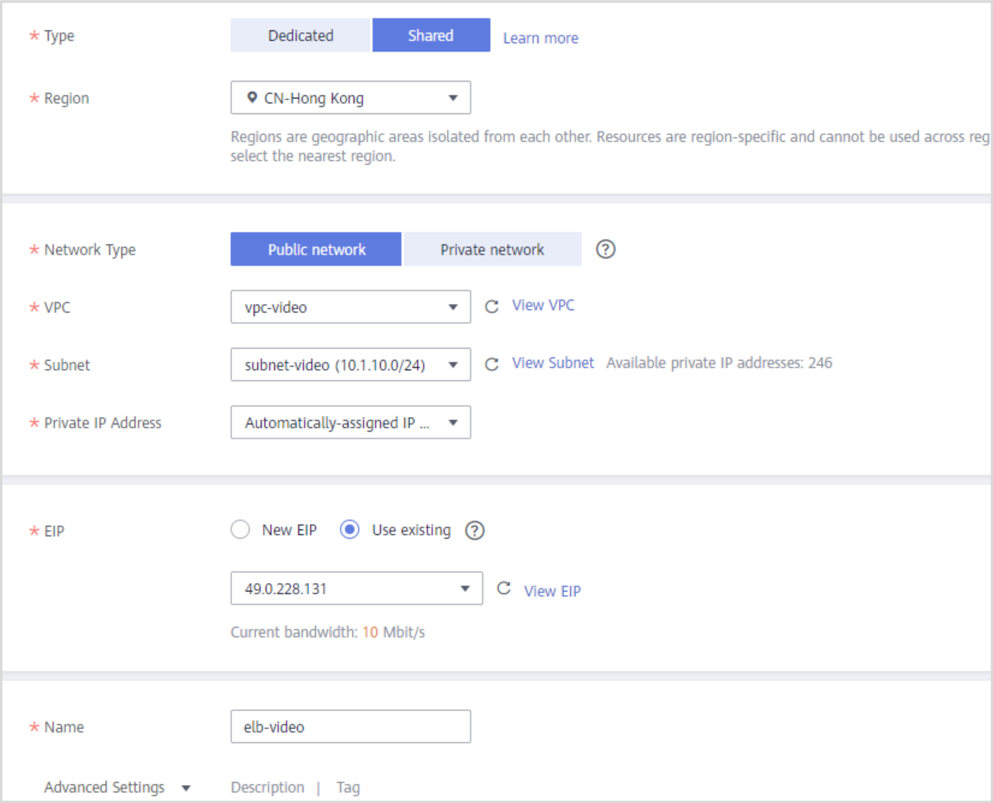
We've just launched dedicated load balancers that use exclusive resources, provide guaranteed performance metrics, and support IPv6. Try now

Name	Status	Type	Specification	IP Address and Network	Listener (Frontend Protocol/Port)	Bandwidth Information	Billing Mode	Operation

Figure 3-51

Step 11 Configure the parameters as follows:

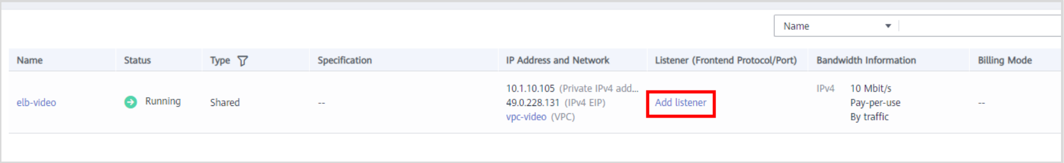
- Type: Shared
- Region: CN-Hong Kong
- Network Type: Public network
- VPC: vpc-video
- Subnet: subnet-video
- Private IP Address: Automatically-assigned IP address
- EIP: Use existing | *114.115.155.72* (select the EIP unbound from the ECS in step 9).
- Name: elb-video



* Type	Dedicated / **Shared** · Learn more
* Region	CN-Hong Kong Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across reg select the nearest region.
* Network Type	**Public network** / Private network
* VPC	vpc-video · View VPC
* Subnet	subnet-video (10.1.10.0/24) · View Subnet · Available private IP addresses: 246
* Private IP Address	Automatically-assigned IP ...
* EIP	○ New EIP ● Use existing 49.0.228.131 · View EIP Current bandwidth: 10 Mbit/s
* Name	elb-video
Advanced Settings	Description | Tag

Figure 3-52

Step 12 View the purchased load balancer and click **Add listener**.



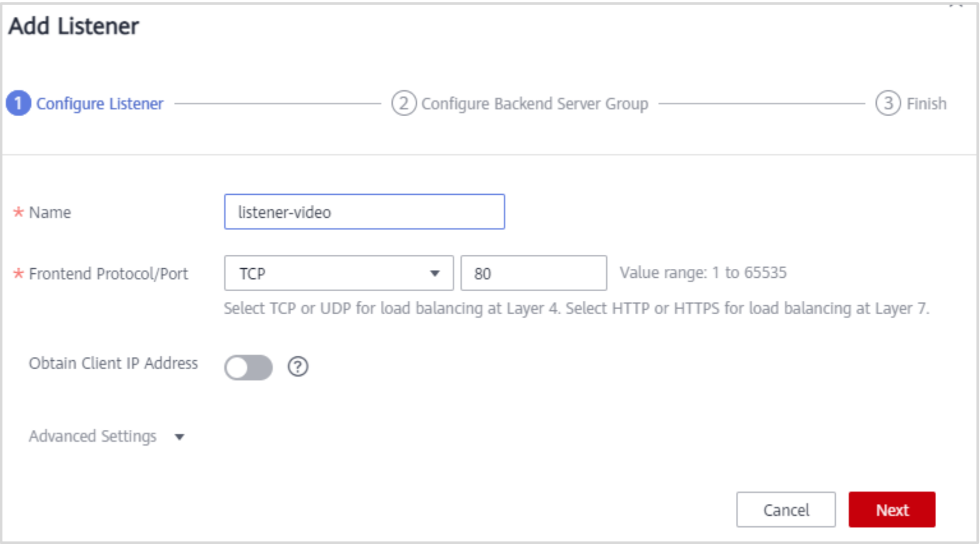
Name

Name	Status	Type	Specification	IP Address and Network	Listener (Frontend Protocol/Port)	Bandwidth Information	Billing Mode
elb-video	Running	Shared	--	10.1.10.105 (Private IPv4 add... 49.0.228.131 (IPv4 EIP) vpc-video (VPC)	Add listener	IPv4 10 Mbit/s Pay-per-use By traffic	--

Figure 3-53

Step 13 Configure the parameters as follows to create a listener:

- **Name**: **listener-video** (can be customized)
- **Frontend Protocol**: **TCP**
- **Frontend Port**: **80** (Used by this load balancer to receive requests from clients.)
- Retain the default settings for other parameters.



Add Listener

1 Configure Listener — 2 Configure Backend Server Group — 3 Finish

* Name: listener-video

* Frontend Protocol/Port: TCP 80 Value range: 1 to 65535

Select TCP or UDP for load balancing at Layer 4. Select HTTP or HTTPS for load balancing at Layer 7.

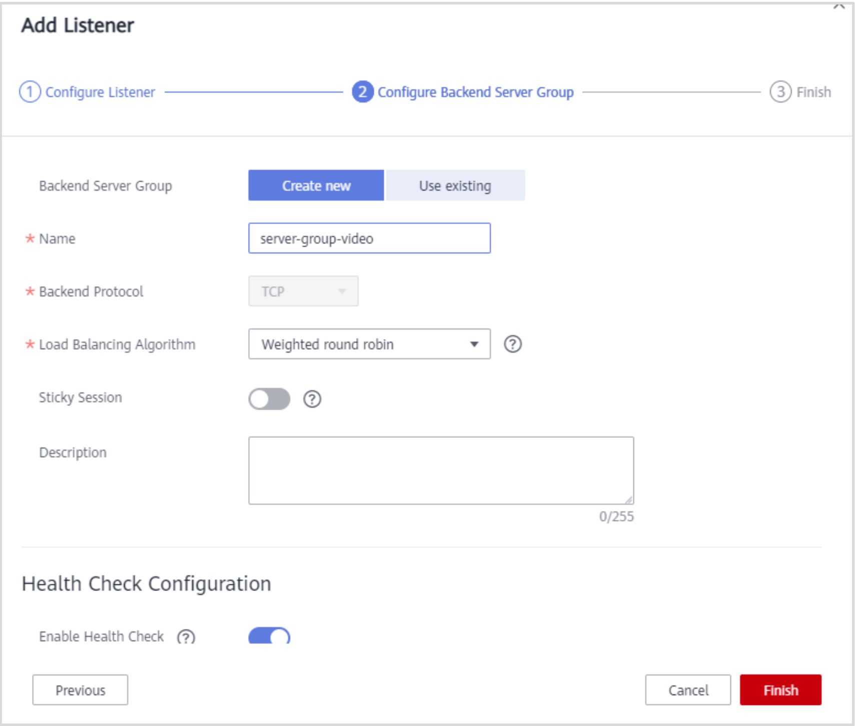
Obtain Client IP Address

Advanced Settings

Figure 3-54

Step 14 Configure a backend routing policy:

- **Name**: **server-group-video** (can be customized)
- **Backend Protocol**: **TCP**
- **Load Balancing Algorithm**: **Weighted round robin**
- Retain the default settings for other parameters.



Add Listener

1 Configure Listener — 2 Configure Backend Server Group — 3 Finish

Backend Server Group: Create new | Use existing

* Name: server-group-video

* Backend Protocol: TCP

* Load Balancing Algorithm: Weighted round robin

Sticky Session

Description

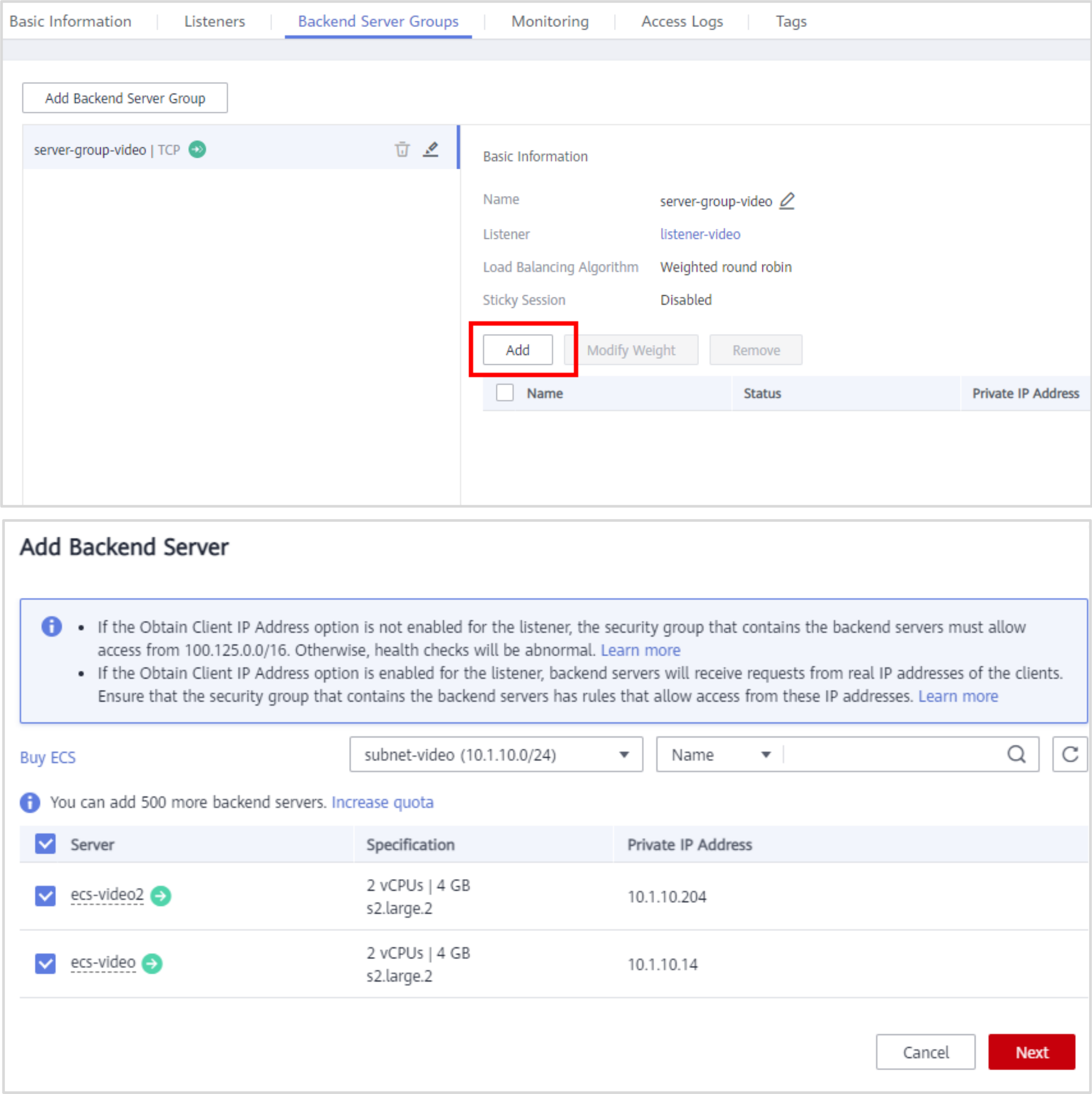
0/255

Health Check Configuration

Enable Health Check

Figure 3-55

Step 15 Click **Add**. On the displayed page, select the two video servers and click **Next**.



Basic Information | Listeners | Backend Server Groups | Monitoring | Access Logs | Tags

Add Backend Server Group

server-group-video | TCP

Basic Information

Name	server-group-video
Listener	listener-video
Load Balancing Algorithm	Weighted round robin
Sticky Session	Disabled

Add | Modify Weight | Remove

☐ Name	Status	Private IP Address

Add Backend Server

- If the Obtain Client IP Address option is not enabled for the listener, the security group that contains the backend servers must allow access from 100.125.0.0/16. Otherwise, health checks will be abnormal. Learn more
- If the Obtain Client IP Address option is enabled for the listener, backend servers will receive requests from real IP addresses of the clients. Ensure that the security group that contains the backend servers has rules that allow access from these IP addresses. Learn more

Buy ECS | subnet-video (10.1.10.0/24) | Name

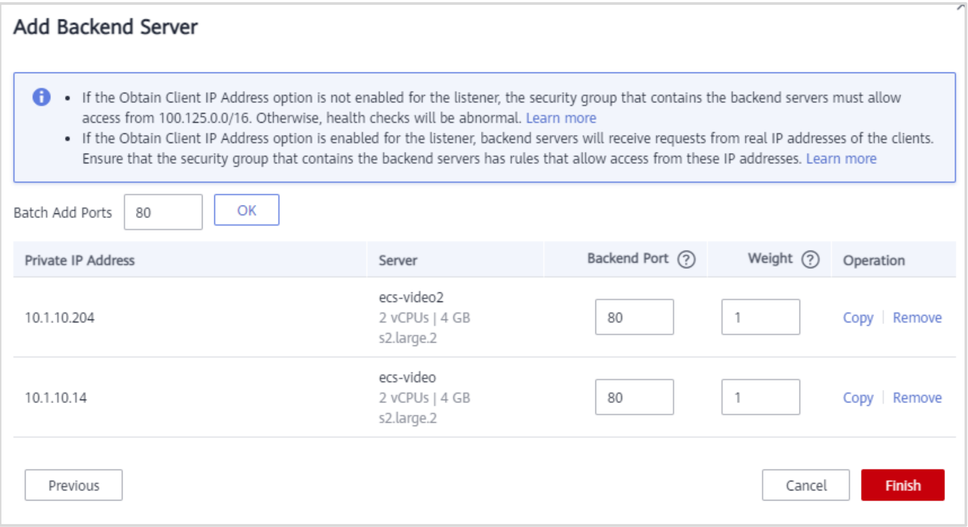
You can add 500 more backend servers. Increase quota

☑ Server	Specification	Private IP Address
☑ ecs-video2	2 vCPUs | 4 GB s2.large.2	10.1.10.204
☑ ecs-video	2 vCPUs | 4 GB s2.large.2	10.1.10.14

Cancel | Next

Figure 3-56

Step 16 Set **Batch Add Ports** to **80**. (This port is used by backend servers to provide network services.)



Add Backend Server

- If the Obtain Client IP Address option is not enabled for the listener, the security group that contains the backend servers must allow access from 100.125.0.0/16. Otherwise, health checks will be abnormal. Learn more
- If the Obtain Client IP Address option is enabled for the listener, backend servers will receive requests from real IP addresses of the clients. Ensure that the security group that contains the backend servers has rules that allow access from these IP addresses. Learn more

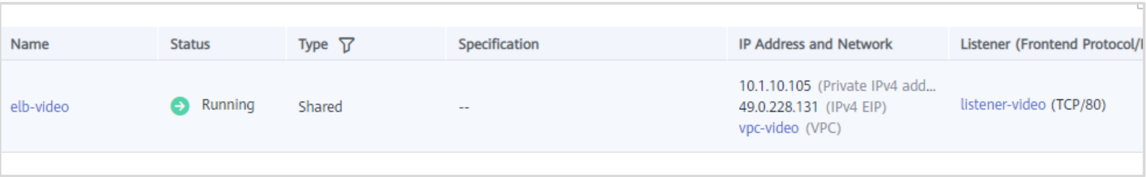
Batch Add Ports 80 OK

Private IP Address	Server	Backend Port	Weight	Operation
10.1.10.204	ecs-video2 2 vCPUs | 4 GB s2.large.2	80	1	Copy | Remove
10.1.10.14	ecs-video 2 vCPUs | 4 GB s2.large.2	80	1	Copy | Remove

Figure 3-57

Step 17 Confirm the configuration and click **Submit**.

Step 18 View the created load balancer and take note of the EIP for future use.



Name	Status	Type	Specification	IP Address and Network	Listener (Frontend Protocol/I
elb-video	Running	Shared	--	10.1.10.105 (Private IPv4 add... 49.0.228.131 (IPv4 EIP) vpc-video (VPC)	listener-video (TCP/80)

Figure 3-58

3.3 Verifying the Result

Step 1 Use the browser on the local PC to log in to **elb-video** using the EIP recorded in the last step and verify that the video can be played. If the following figure shows up, the video can be played, indicating that the video streaming service has been set up and ELB is working properly.

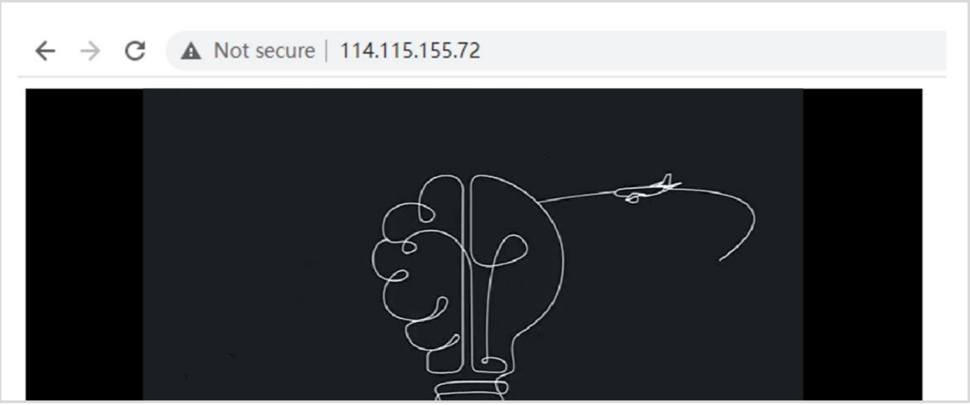
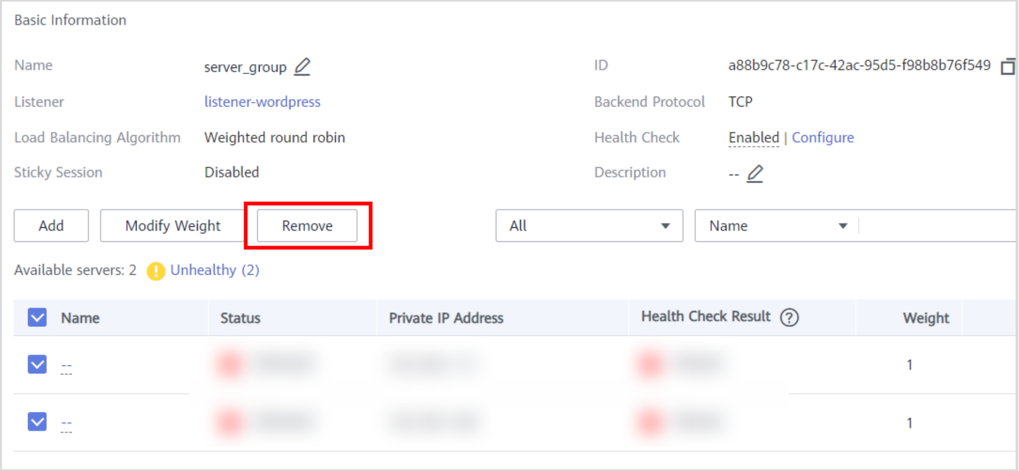


Figure 3-59

3.4 Clearing Resources

Step 1 Delete the load balancer.

- In the service list, choose **Networking** > **Elastic Load Balance**. In the load balancer list, click the load balancer purchased in this exercise. On the **Backend Server Groups** tab, in the **Basic Information** area, select all backend servers and click **Remove** above the server list.



Basic Information

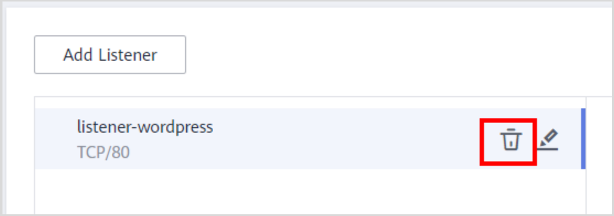
Name: server_group
Listener: listener-wordpress
Load Balancing Algorithm: Weighted round robin
Sticky Session: Disabled
ID: a88b9c78-c17c-42ac-95d5-f98b8b76f549
Backend Protocol: TCP
Health Check: Enabled | Configure
Description: --

Available servers: 2 Unhealthy (2)

☑ Name	Status	Private IP Address	Health Check Result	Weight
☑ --	[redacted]	[redacted]	[redacted]	1
☑ --	[redacted]	[redacted]	[redacted]	1

Figure 3-60

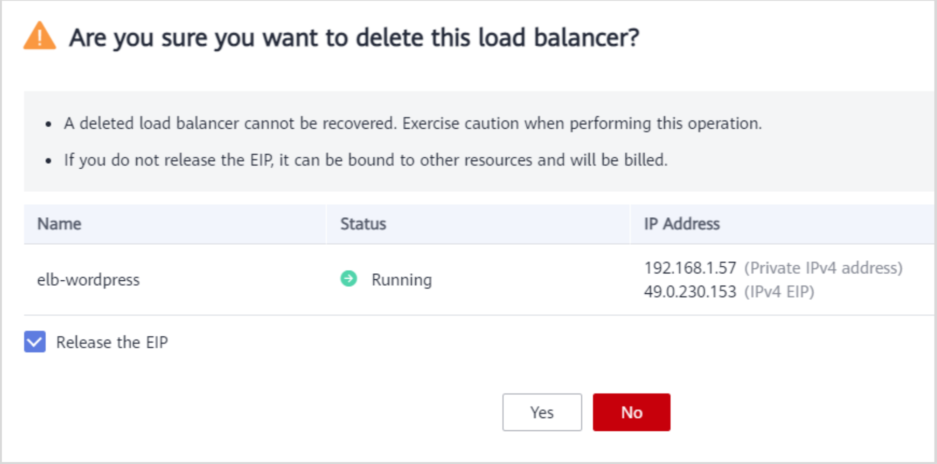
- On the **Listeners** tab, delete the listener purchased in this exercise.



listener-wordpress
TCP/80

Figure 3-61

- Back to the load balancer list and click **Delete** in the **Operation** column to delete the load balancer.
- In the displayed dialog box, select **Release the EIP** and click **Yes**.



Are you sure you want to delete this load balancer?

- A deleted load balancer cannot be recovered. Exercise caution when performing this operation.
- If you do not release the EIP, it can be bound to other resources and will be billed.

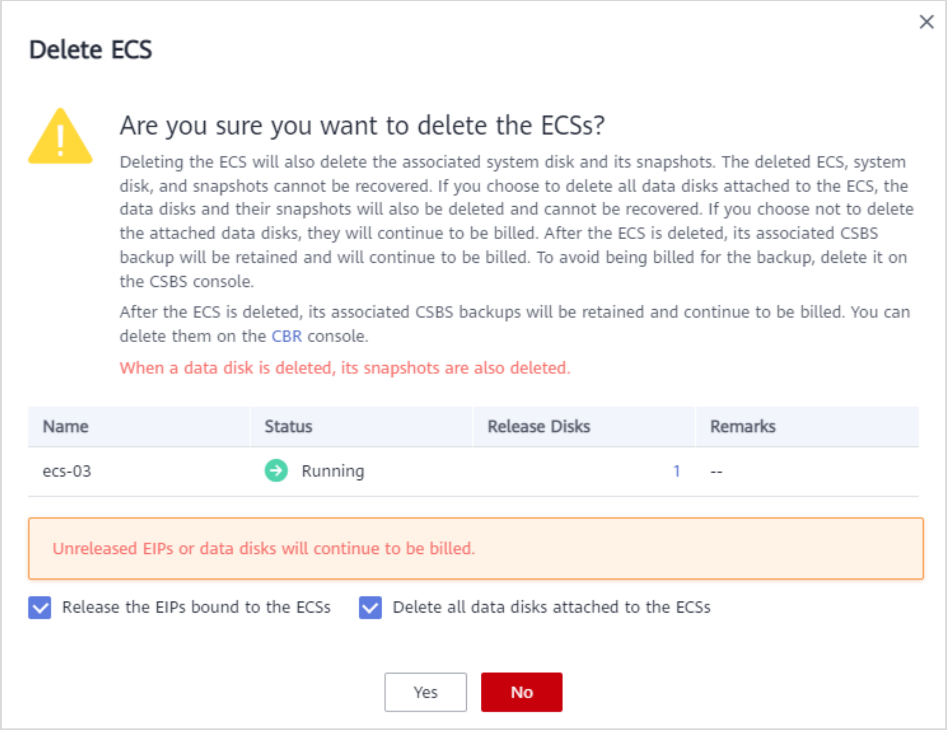
Name	Status	IP Address
elb-wordpress	Running	192.168.1.57 (Private IPv4 address) 49.0.230.153 (IPv4 EIP)

☑ Release the EIP

Figure 3-62

Step 2 Delete the ECSs.

- In the service list, choose **Elastic Cloud Server**. In the ECS list, locate the ECS purchased in this exercise and choose **More** > **Delete** in the **Operation** column.
- In the displayed dialog box, select the check boxes displayed in the following picture and click **Yes**.



Delete ECS

Are you sure you want to delete the ECSs?

Deleting the ECS will also delete the associated system disk and its snapshots. The deleted ECS, system disk, and snapshots cannot be recovered. If you choose to delete all data disks attached to the ECS, the data disks and their snapshots will also be deleted and cannot be recovered. If you choose not to delete the attached data disks, they will continue to be billed. After the ECS is deleted, its associated CSBS backup will be retained and will continue to be billed. To avoid being billed for the backup, delete it on the CSBS console.

After the ECS is deleted, its associated CSBS backups will be retained and continue to be billed. You can delete them on the CBR console.

When a data disk is deleted, its snapshots are also deleted.

Name	Status	Release Disks	Remarks
ecs-03	Running	1	--

Unreleased EIPs or data disks will continue to be billed.

☑ Release the EIPs bound to the ECSs ☑ Delete all data disks attached to the ECSs

Figure 3-63

Step 3 Delete the SFS file system.

In the service list, choose **Scalable File Service**. In the file system list, locate the file system purchased in this exercise and choose **More** > **Delete** in the **Operation** column.

Step 4 Delete the OBS bucket.

In the service list, choose **Object Storage Service**. In the bucket list, locate the bucket purchased in this exercise and click **Delete** in the **Operation** column.

Step 5 Delete the security group.

In the service list, choose **Virtual Private Cloud**. On the network console, choose **Access Control** > **Security Groups**. In the security group list, locate the security group created in this exercise and click **Delete** in the **Operation** column.

Step 6 Delete the subnet and VPC.

- In the service list, choose **Virtual Private Cloud**. On the network console, choose **Subnets**. In the subnet list, locate the subnet created in this exercise and click **Delete** in the **Operation** column.
- Choose **Virtual Private Cloud** in the navigation pane on the left. In the VPC list, locate the VPC created in this exercise and click **Delete** in the **Operation** column.

3.5 Quiz

Question: In this exercise, when HA is configured, a full-ECS image is used to provision an ECS. Why a system disk image is not used instead?

Answer: In this exercise, an EVS disk was attached to **ecs-video**. So a full-ECS image is required to create the image, in which the OS data, application data, and service data are all included.

4 Database Architecture Design

4.1 Introduction

4.1.1 About This Exercise

This exercise describes how to set up a WordPress website using an ECS and RDS for MySQL instance on Huawei Cloud and how to deploy a DCS instance to speed up access to the WordPress website.

This exercise uses region CN-Hong Kong as an example. Trainees can select regions based on their own needs.

4.1.2 Objectives

Understand how to use the cloud services involved in the cloud database architecture.

Understand how to manage cloud databases and keep them available.

4.1.3 Networking

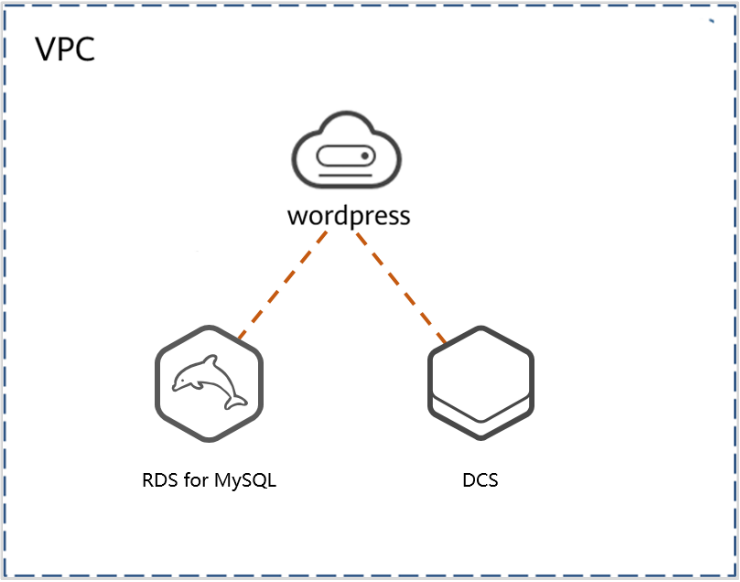


Figure 4-1

4.1.4 Related Software

Redis, which stands for Remote Dictionary Server, is an open source log-based, key-value database written in ANSI C language. Redis supports both in-memory and persistent storage, network connections, and APIs in multiple different languages.

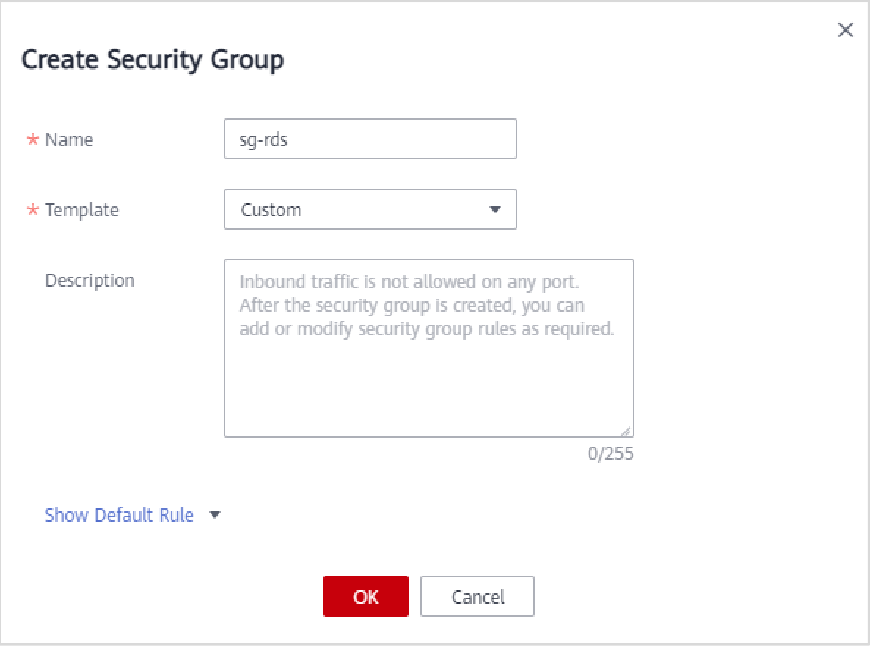
4.2 Procedure

4.2.1 Creating a Security Group

Step 1 Log in to the Huawei Cloud console and select region **CN-Hong Kong**. Then choose **Networking** > **Virtual Private Cloud**. On the network console, choose **Access Control** > **Security Groups**, click **Create Security Group**, and configure parameters as follows to create security group **sg-rds**.

Note: This security group is for a RDS database instance, so port 3306 has to be enabled.

- **Name**: **sg-rds**
- **Template**: **Custom**



Create Security Group

* Name: sg-rds

* Template: Custom

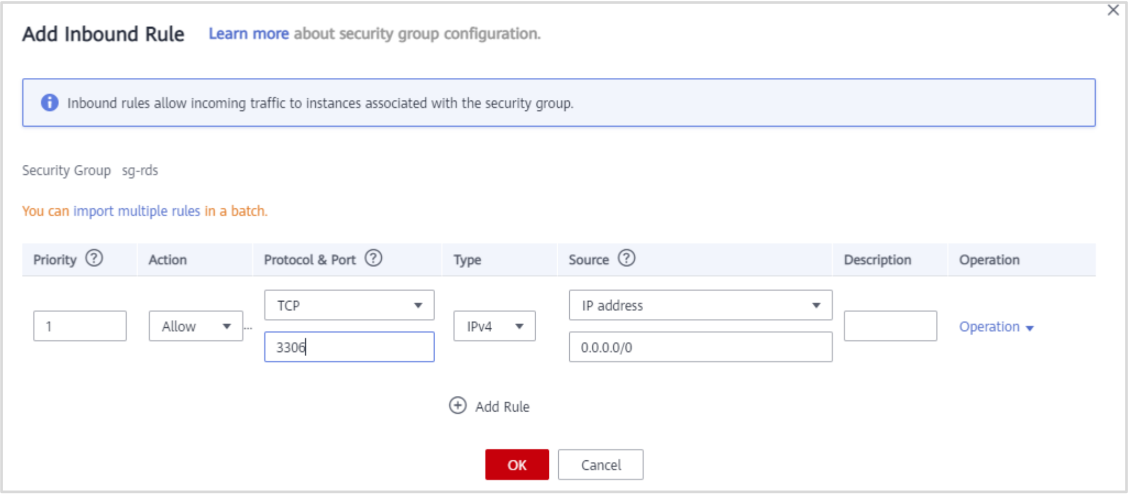
Description: Inbound traffic is not allowed on any port. After the security group is created, you can add or modify security group rules as required.

0/255

Figure 4-2

Step 2 Add an inbound rule to allow access to database port **3306**.

- **Priority**: **1**
- **Action**: **Allow**
- **Protocol & Port**: **TCP** and **3306**
- **Type**: **IPv4**
- **Source**: **IP address** and **0.0.0.0/0**



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group sg-rds

You can import multiple rules in a batch.

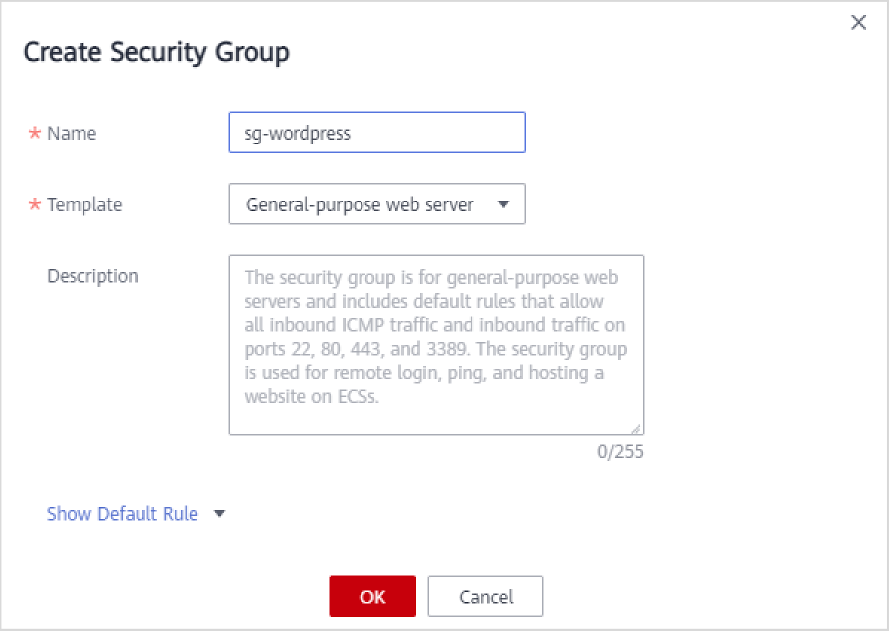
Priority	Action	Protocol & Port	Type	Source	Description	Operation
1	Allow	TCP 3306	IPv4	IP address 0.0.0.0/0		Operation

Figure 4-3

Step 3 Create security group **sg-wordpress**.

Note: This security group is for the ECSs used to set up WordPress. A general-purpose web server template is required.

- **Name: sg-wordpress**
- **Template: General-purpose web server**



Create Security Group

* Name: sg-wordpress

* Template: General-purpose web server

Description: The security group is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and inbound traffic on ports 22, 80, 443, and 3389. The security group is used for remote login, ping, and hosting a website on ECSs.

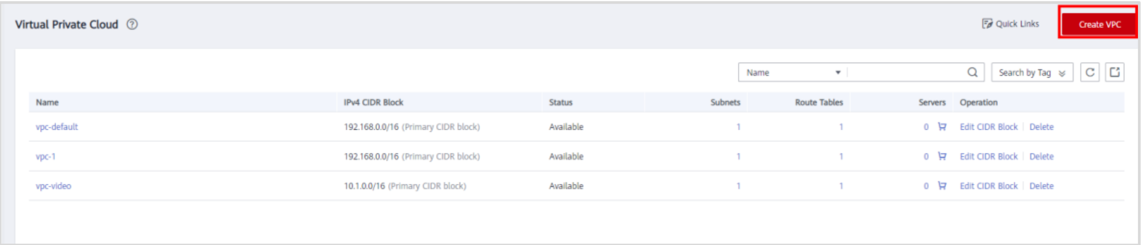
0/255

Figure 4-4

4.2.2 Creating a VPC

Step 1 In the service list, choose **Virtual Private Cloud**. On the displayed page, click **Create VPC**.

Note: Resources required in this exercise will be created in this VPC.



Name	IPv4 CIDR Block	Status	Subnets	Route Tables	Servers	Operation
vpc-default	192.168.0.0/16 (Primary CIDR block)	Available	1	1	0	Edit CIDR Block | Delete
vpc-1	192.168.0.0/16 (Primary CIDR block)	Available	1	1	0	Edit CIDR Block | Delete
vpc-video	10.1.0.0/16 (Primary CIDR block)	Available	1	1	0	Edit CIDR Block | Delete

Figure 4-5

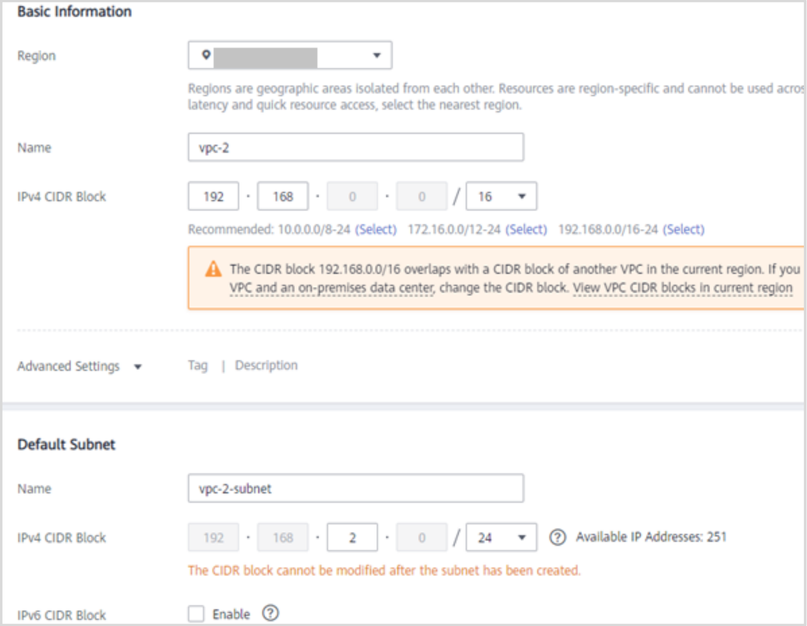
Step 2 Configure the required parameters to create VPC **vpc-2**.

Basic Information

- **Region: CN-Hong Kong**
- **Name: vpc-2**
- **IPv4 CIDR Block: 192.168.0.0/16**

Default Subnet

- **AZ: AZ1** (This exercise uses AZ1 as an example. Trainees can select AZs based on their needs. This note is valid for all similar resources and will not be described later.)
- **Name: vpc-2-subnet**
- **IPv4 CIDR Block: 192.168.2.0/24**



Basic Information

Region: [redacted] ▾

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used acros
latency and quick resource access, select the nearest region.

Name: vpc-2

IPv4 CIDR Block: 192 . 168 . 0 . 0 / 16 ▾

Recommended: 10.0.0.0/8-24 (Select) 172.16.0.0/12-24 (Select) 192.168.0.0/16-24 (Select)

The CIDR block 192.168.0.0/16 overlaps with a CIDR block of another VPC in the current region. If you
VPC and an on-premises data center, change the CIDR block. View VPC CIDR blocks in current region

Advanced Settings ▾ Tag | Description

Default Subnet

Name: vpc-2-subnet

IPv4 CIDR Block: 192 . 168 . 2 . 0 / 24 ▾ ⓘ Available IP Addresses: 251

The CIDR block cannot be modified after the subnet has been created.

IPv6 CIDR Block: □ Enable ⓘ

Figure 4-6

4.2.3 Buying a Cloud Database Instance

Step 1 On the management console, select region **CN-Hong Kong**, click **Service List**, and choose **RDS** under **Databases**.

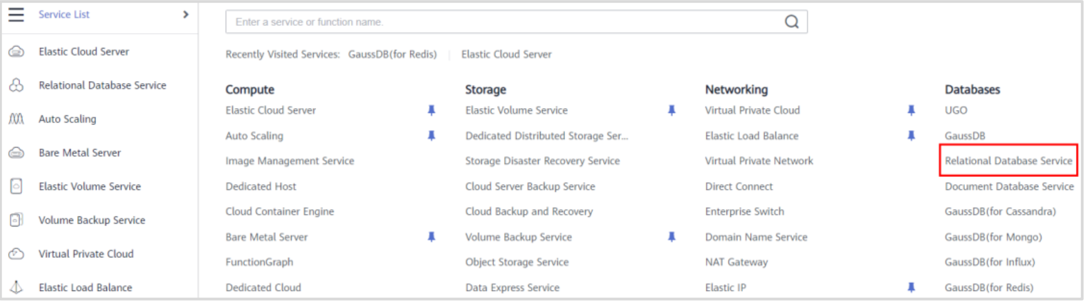
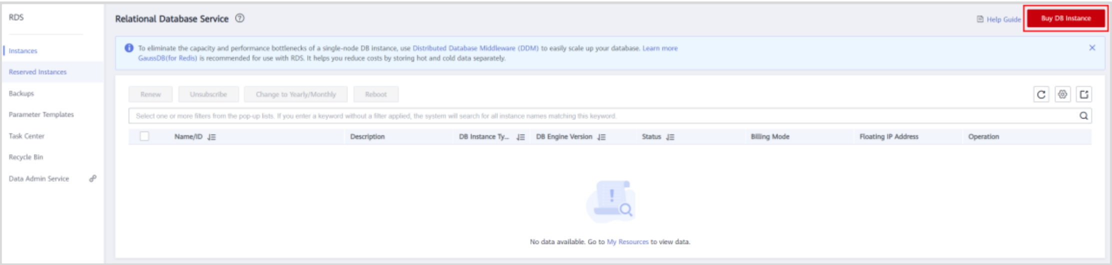


Figure 4-7

Step 2 Click **Buy DB Instance** in the upper right corner.

Note: In this DB instance, a database will be created to interconnect with WordPress.



To eliminate the capacity and performance bottlenecks of a single-node DB instance, use Distributed Database Middleware (DDM) to easily scale up your database. Learn more GaussDB(for Redis) is recommended for use with RDS. It helps you reduce costs by storing hot and cold data separately.

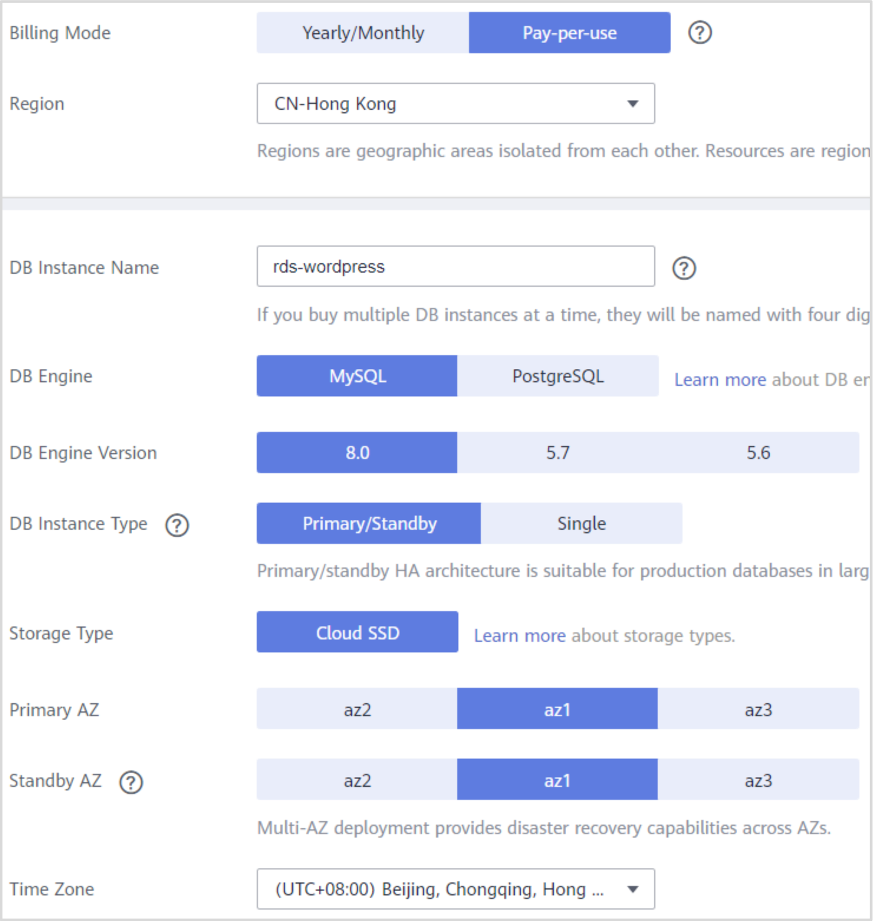
Select one or more filters from the pop-up lists. If you enter a keyword without a filter applied, the system will search for all instance names matching this keyword.

No data available. Go to My Resources to view data.

Figure 4-8

Step 3 Configure the following parameters and click **Next**.

- Billing Mode: Pay-per-use
- Region: CN-Hong Kong
- DB Instance Name: rds-wordpress
- DB Engine: RDS for MySQL
- DB Engine Version: MySQL 8.0
- DB Instance Primary/Standby
- AZ: AZ1
- Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
- Instance Class: Dedicated Edition | 4 vCPUs | 16 GB
- VPC: vpc-2 | vpc-2-subnet | Automatically-assigned IP
- Security Group: sg-rds
- Administrator Password: User-defined
- Parameter Template: Default-MySQL-8.0
- Quantity: 1



Billing Mode: Yearly/Monthly [✓ Pay-per-use]

Region: CN-Hong Kong

Regions are geographic areas isolated from each other. Resources are region

DB Instance Name: rds-wordpress

If you buy multiple DB instances at a time, they will be named with four dig

DB Engine: [✓ MySQL] PostgreSQL Learn more about DB er

DB Engine Version: [✓ 8.0] 5.7 5.6

DB Instance Type: [✓ Primary/Standby] Single

Primary/standby HA architecture is suitable for production databases in larg

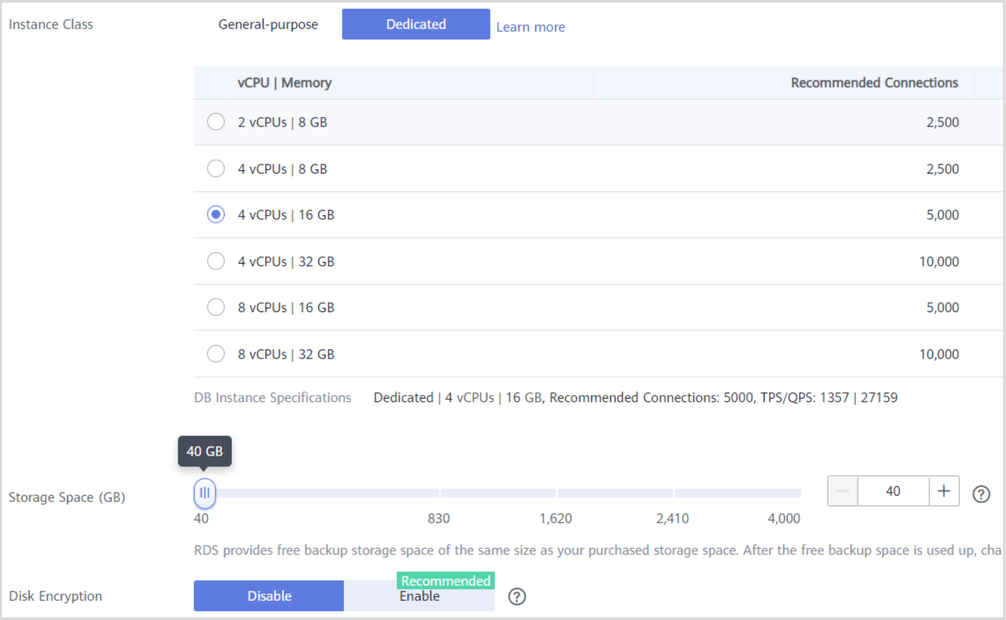
Storage Type: [✓ Cloud SSD] Learn more about storage types.

Primary AZ: az2 [✓ az1] az3

Standby AZ: az2 [✓ az1] az3

Multi-AZ deployment provides disaster recovery capabilities across AZs.

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong ...



Instance Class: General-purpose [✓ Dedicated] Learn more

	vCPU | Memory	Recommended Connections
○	2 vCPUs | 8 GB	2,500
○	4 vCPUs | 8 GB	2,500
●	4 vCPUs | 16 GB	5,000
○	4 vCPUs | 32 GB	10,000
○	8 vCPUs | 16 GB	5,000
○	8 vCPUs | 32 GB	10,000

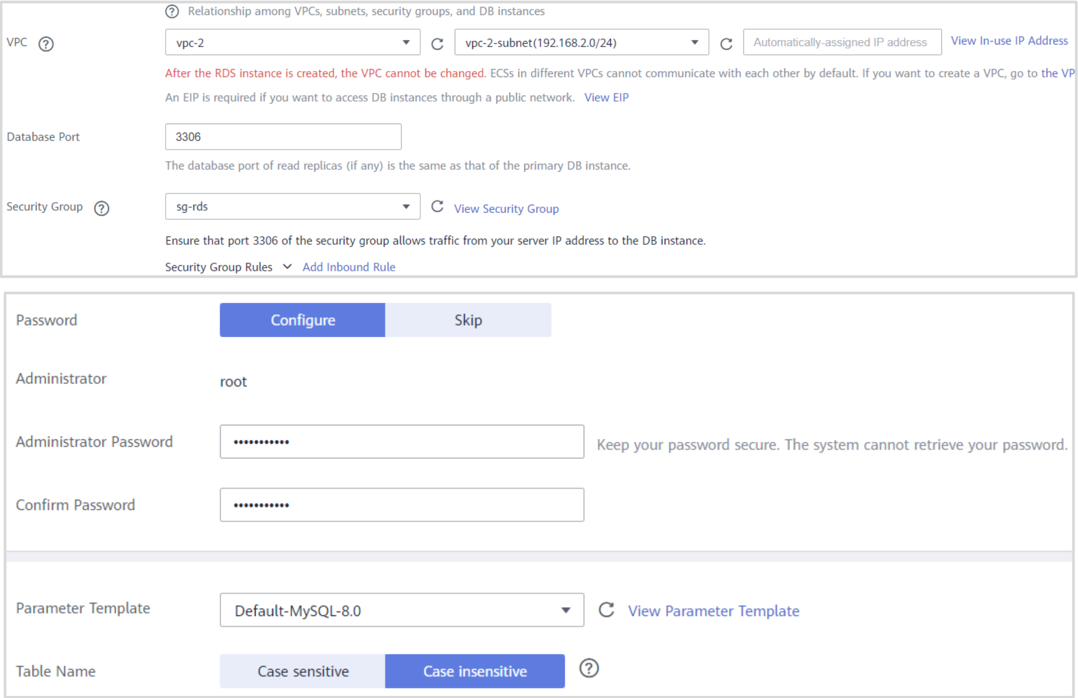
DB Instance Specifications: Dedicated | 4 vCPUs | 16 GB, Recommended Connections: 5000, TPS/QPS: 1357 | 27159

Storage Space (GB): 40 GB

40

RDS provides free backup storage space of the same size as your purchased storage space. After the free backup space is used up, cha

Disk Encryption: [✓ Disable] Enable Recommended



Relationship among VPCs, subnets, security groups, and DB instances

VPC: vpc-2 | vpc-2-subnet(192.168.2.0/24) | Automatically-assigned IP address | View In-use IP Address

After the RDS instance is created, the VPC cannot be changed. ECSs in different VPCs cannot communicate with each other by default. If you want to create a VPC, go to the VP

An EIP is required if you want to access DB instances through a public network. View EIP

Database Port: 3306

The database port of read replicas (if any) is the same as that of the primary DB instance.

Security Group: sg-rds | View Security Group

Ensure that port 3306 of the security group allows traffic from your server IP address to the DB instance.

Security Group Rules | Add Inbound Rule

Password: Configure | Skip

Administrator: root

Administrator Password: ••••••••••• Keep your password secure. The system cannot retrieve your password.

Confirm Password: •••••••••••

Parameter Template: Default-MySQL-8.0 | View Parameter Template

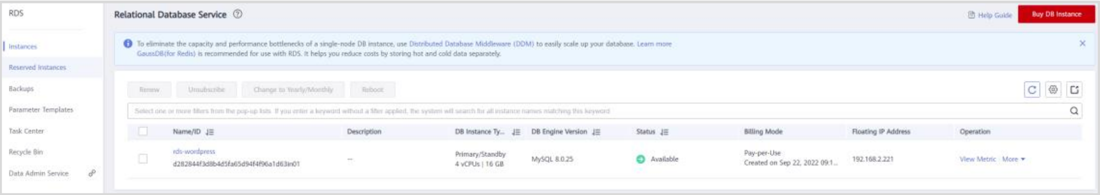
Table Name: Case sensitive | Case insensitive

Figure 4-9

Step 4 Confirm configurations, click **Submit**, and wait for 5 to 10 minutes until the instance is created.

4.2.4 Creating a Database for WordPress

Step 1 On the **Instances** page, locate the created instance, record its private IP address, and click **Log In** in the **Operation** column.



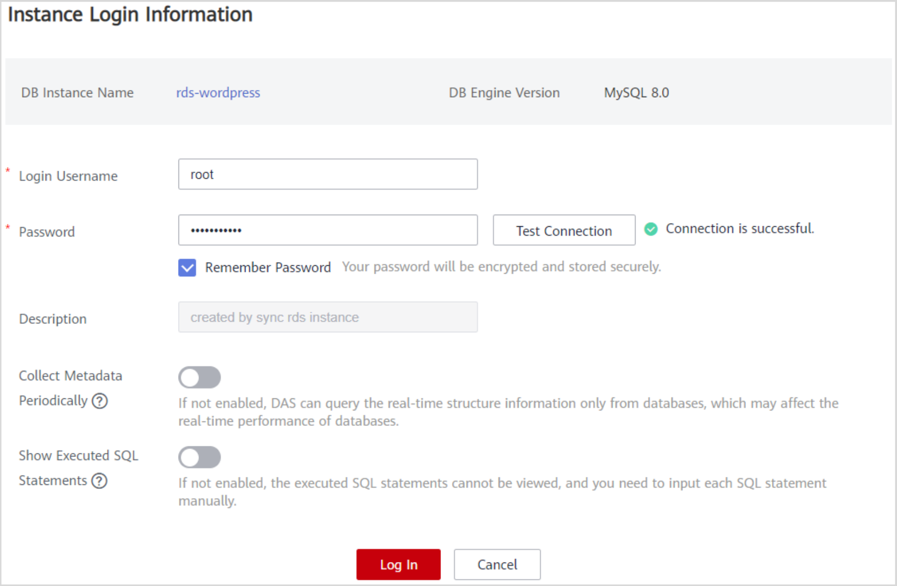
To eliminate the capacity and performance bottlenecks of a single-node DB instance, use Distributed Database Middleware (DDM) to easily scale up your database. Learn more
GaussDB(for Redis) is recommended for use with RDS. It helps you reduce costs by storing hot and cold data separately.

Select one or more filters from the pop-up lists. If you enter a keyword without a filter applied, the system will search for all instance names matching this keyword

Name/ID	Description	DB Instance Ty...	DB Engine Version	Status	Billing Mode	Floating IP Address	Operation
rds-wordpress d282844f3d8b4d5fa65d94f4f96a1d63in01	--	Primary/Standby 4 vCPUs | 16 GB	MySQL 8.0.25	Available	Pay-per-Use Created on Sep 22, 2022 09:1...	192.168.2.221	View Metric More

Figure 4-10

Step 2 In the displayed window, enter the instance login username and password and click **Test Connection**. After a successful connection message is displayed, click **Log In**.



Instance Login Information

DB Instance Name rds-wordpress DB Engine Version MySQL 8.0

* Login Username root

* Password ••••••••••• Connection is successful.

☑ Remember Password Your password will be encrypted and stored securely.

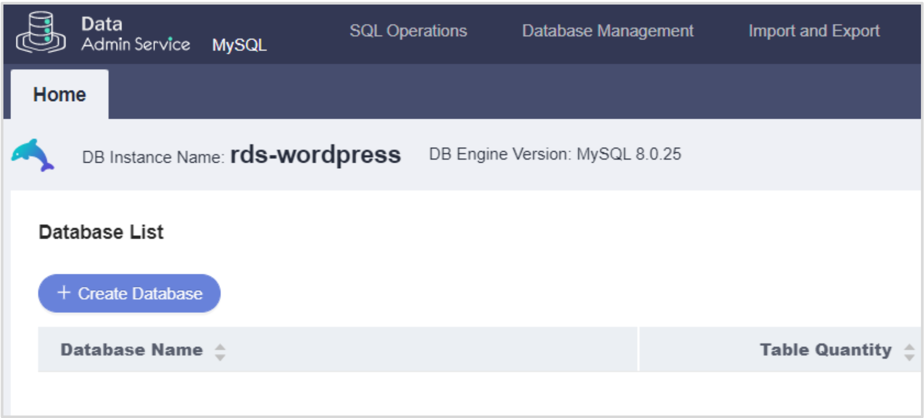
Description created by sync rds instance

Collect Metadata Periodically: off — If not enabled, DAS can query the real-time structure information only from databases, which may affect the real-time performance of databases.

Show Executed SQL Statements: off — If not enabled, the executed SQL statements cannot be viewed, and you need to input each SQL statement manually.

Figure 4-11

Step 3 On the home page, click **Create Database**. The created database will be used to interconnect with WordPress.



DB Instance Name: **rds-wordpress** DB Engine Version: MySQL 8.0.25

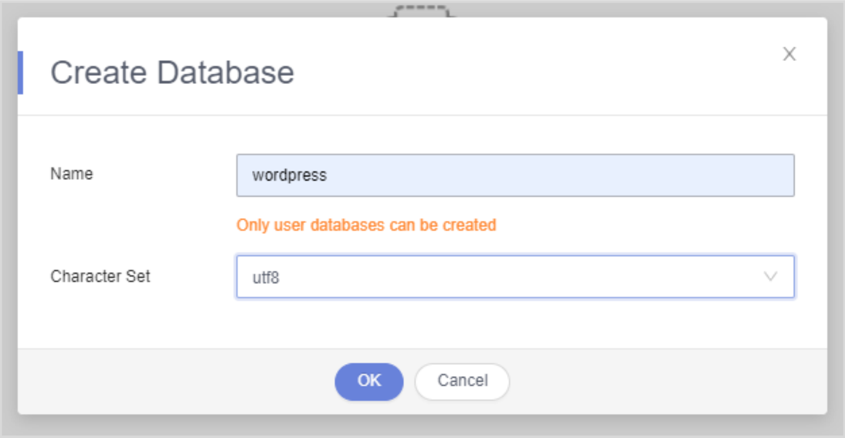
Database List

Database Name	Table Quantity

Figure 4-12

Step 4 In the displayed dialog box, enter a database name and specify a character set as follows and click **OK**.

- **Name**: **wordpress**
- **Character Set**: **utf8** (default setting)

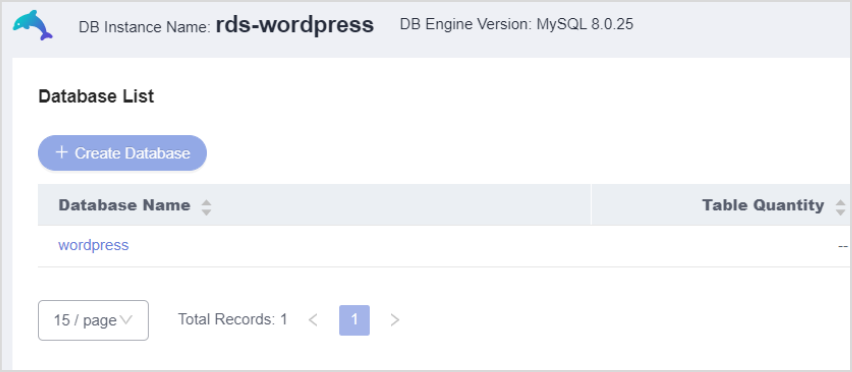


Name: wordpress

Only user databases can be created

Character Set: utf8

Step 5 View the created database in the database list.



DB Instance Name: rds-wordpress DB Engine Version: MySQL 8.0.25

Database List

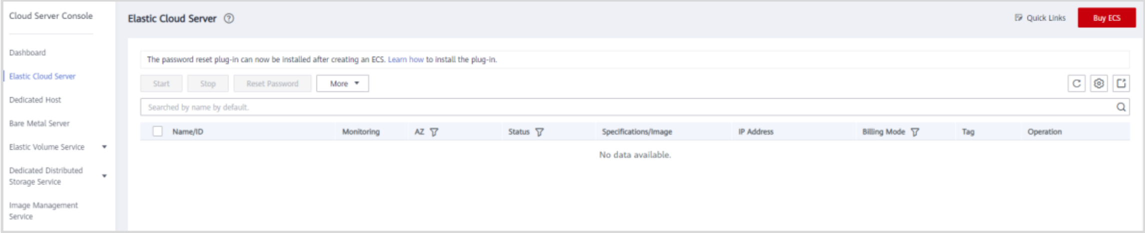
Database Name	Table Quantity
wordpress	--

Figure 4-13

4.2.5 Deploying WordPress

Step 1 In the service list, choose **Compute** > **Elastic Cloud Server**, and click **Buy ECS** in the upper right corner.

Note: The created ECS will be used to deploy WordPress.



The password reset plug-in can now be installed after creating an ECS. Learn how to install the plug-in.

Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mode	Tag	Operation

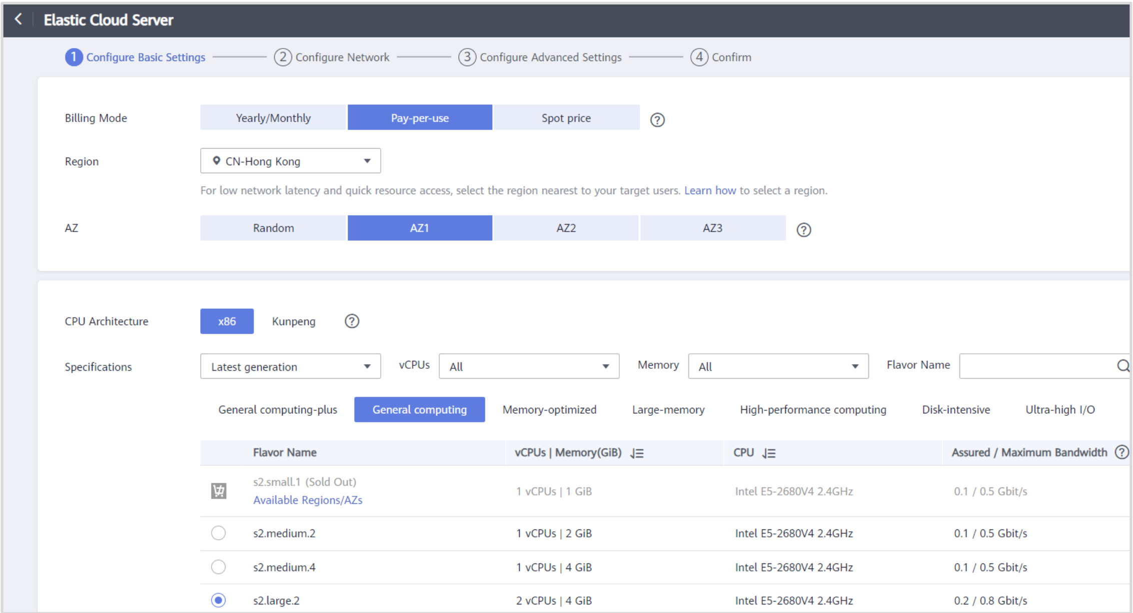
No data available.

Figure 4-14

Step 2 Configure parameters as follows to create an ECS:

- **Billing Mode: Pay-per-use**
- **Region: CN-Hong Kong**
- **AZ: AZ1**
- **Specifications: 2 vCPUs | 4 GiB**

- Image: Public image|CentOS 7.6 64bit(40GB)
- Host Security: Basic (free)
- System Disk: High I/O | 40 GiB
- Network: vpc-2 | vpc-2-subnet | Automatically-assigned IP
- Security Group: sg-wordpress
- EIP: Auto assign
- EIP Type: Dynamic BGP
- Billed By: Traffic
- Bandwidth Size: 10 Mbit/s
- ECS Name: ecs-wordpress
- Password: User-defined (for username **root**)



Elastic Cloud Server

1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

Billing Mode: Yearly/Monthly | **Pay-per-use** | Spot price

Region: CN-Hong Kong

For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

AZ: Random | **AZ1** | AZ2 | AZ3

CPU Architecture: **x86** | Kunpeng

Specifications: Latest generation vCPUs: All Memory: All Flavor Name:

General computing-plus | **General computing** | Memory-optimized | Large-memory | High-performance computing | Disk-intensive | Ultra-high I/O

	Flavor Name	vCPUs | Memory(GiB)	CPU	Assured / Maximum Bandwidth
	s2.small.1 (Sold Out) Available Regions/AZs	1 vCPUs | 1 GiB	Intel E5-2680V4 2.4GHz	0.1 / 0.5 Gbit/s
○	s2.medium.2	1 vCPUs | 2 GiB	Intel E5-2680V4 2.4GHz	0.1 / 0.5 Gbit/s
○	s2.medium.4	1 vCPUs | 4 GiB	Intel E5-2680V4 2.4GHz	0.1 / 0.5 Gbit/s
●	s2.large.2	2 vCPUs | 4 GiB	Intel E5-2680V4 2.4GHz	0.2 / 0.8 Gbit/s

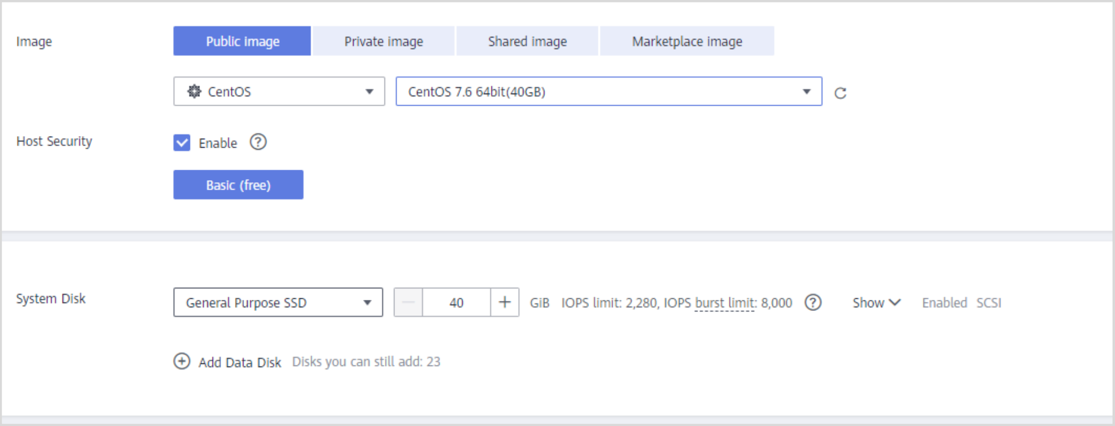


Image: **Public image** | Private image | Shared image | Marketplace image

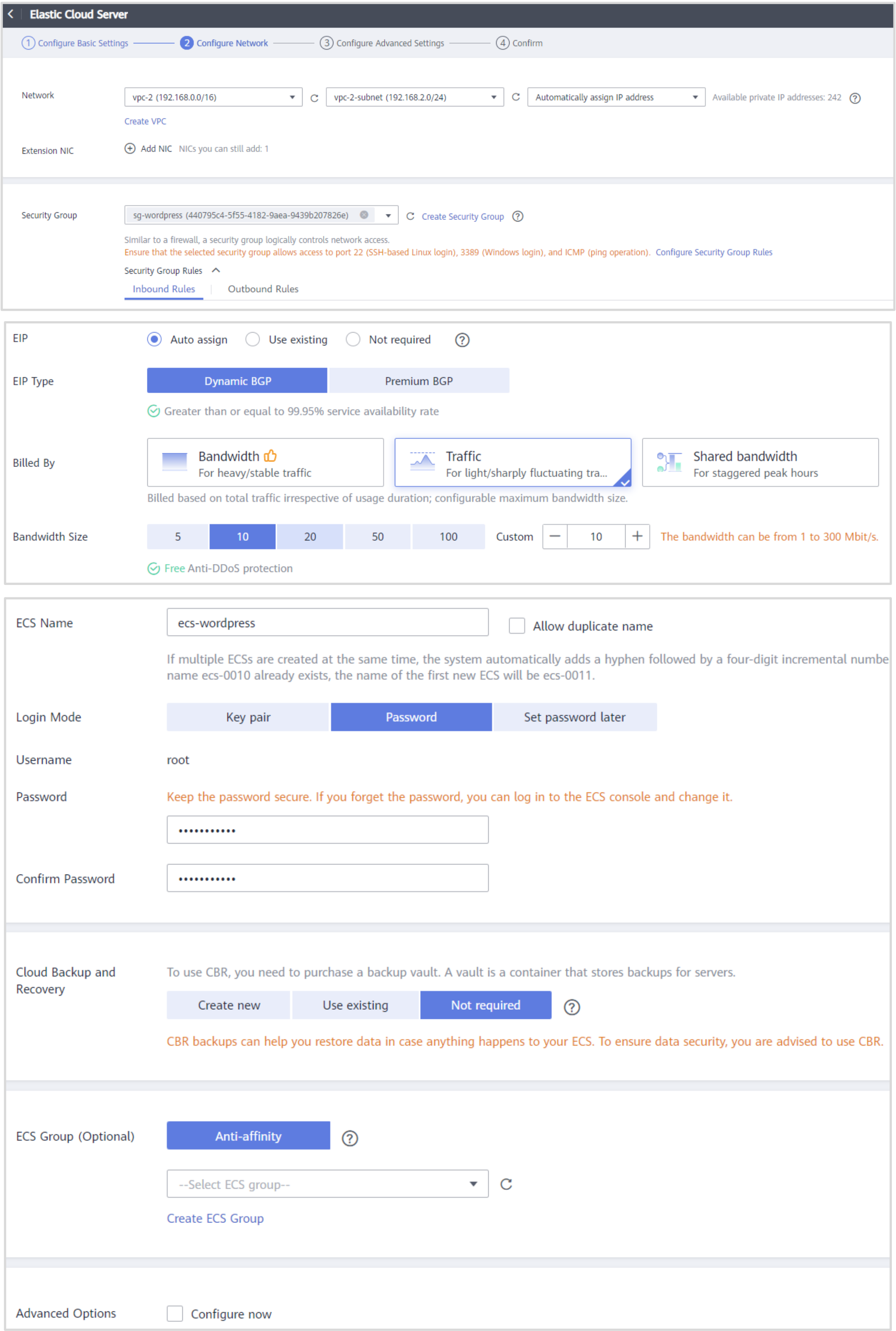
CentOS | CentOS 7.6 64bit(40GB)

Host Security: ☑ Enable

Basic (free)

System Disk: General Purpose SSD | 40 GiB IOPS limit: 2,280, IOPS burst limit: 8,000 Show Enabled SCSI

Add Data Disk Disks you can still add: 23



Elastic Cloud Server

(1) Configure Basic Settings — (2) Configure Network — (3) Configure Advanced Settings — (4) Confirm

Network: vpc-2 (192.168.0.0/16) | vpc-2-subnet (192.168.2.0/24) | Automatically assign IP address | Available private IP addresses: 242

Create VPC

Extension NIC: Add NIC NICs you can still add: 1

Security Group: sg-wordpress (440795c4-5f55-4182-9aea-9439b207826e) Create Security Group

Similar to a firewall, a security group logically controls network access.

Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

Security Group Rules

Inbound Rules | Outbound Rules

EIP: ● Auto assign ○ Use existing ○ Not required

EIP Type: Dynamic BGP | Premium BGP

Greater than or equal to 99.95% service availability rate

Billed By: Bandwidth (For heavy/stable traffic) | Traffic (For light/sharply fluctuating tra...) | Shared bandwidth (For staggered peak hours)

Billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size.

Bandwidth Size: 5 | 10 | 20 | 50 | 100 | Custom — 10 + The bandwidth can be from 1 to 300 Mbit/s.

Free Anti-DDoS protection

ECS Name: ecs-wordpress □ Allow duplicate name

If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a four-digit incremental numbe name ecs-0010 already exists, the name of the first new ECS will be ecs-0011.

Login Mode: Key pair | Password | Set password later

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.

•••••••••••

Confirm Password: •••••••••••

Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.

Create new | Use existing | Not required

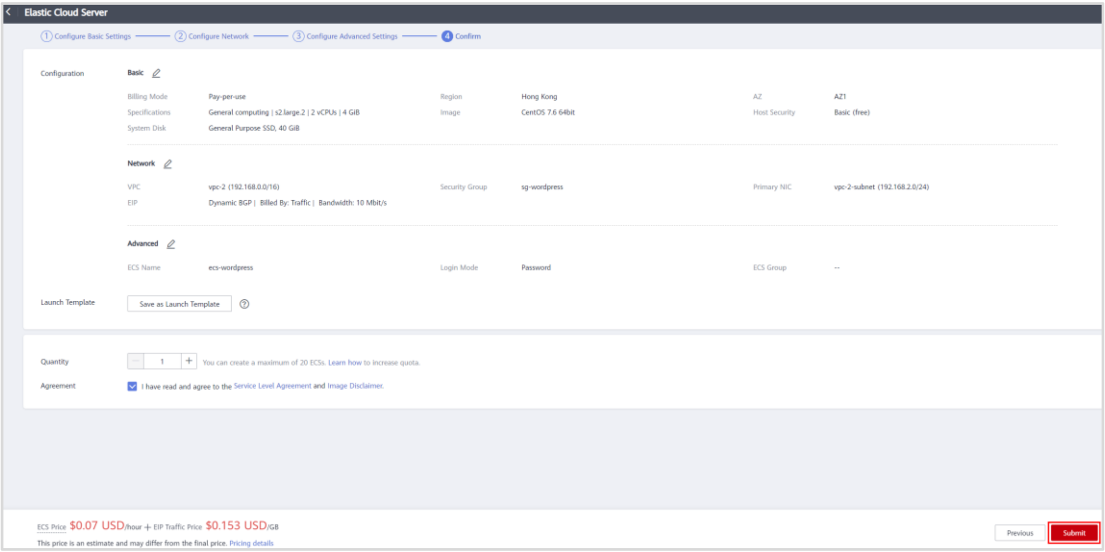
CBR backups can help you restore data in case anything happens to your ECS. To ensure data security, you are advised to use CBR.

ECS Group (Optional): Anti-affinity

--Select ECS group--

Create ECS Group

Advanced Options: □ Configure now



Elastic Cloud Server

① Configure Basic Settings — ② Configure Network — ③ Configure Advanced Settings — ④ Confirm

Configuration

Basic

Billing Mode	Pay-per-use	Region	Hong Kong	AZ	AZ1
Specifications	General computing | s2.large.2 | 2 vCPUs | 4 GiB	Image	CentOS 7.6 64bit	Host Security	Basic (free)
System Disk	General Purpose SSD, 40 GiB				

Network

VPC	vpc-2 (192.168.0.0/16)	Security Group	sg-wordpress	Primary NIC	vpc-2-subnet (192.168.2.0/24)
EIP	Dynamic BGP | Billed By: Traffic | Bandwidth: 10 Mbit/s				

Advanced

ECS Name	ecs-wordpress	Login Mode	Password	ECS Group	--

Launch Template: Save as Launch Template

Quantity: 1 You can create a maximum of 20 ECSs. Learn how to increase quota.

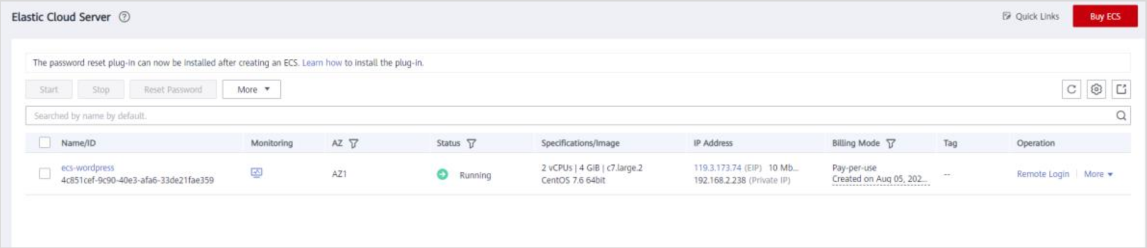
Agreement: ☑ I have read and agree to the Service Level Agreement and Image Disclaimer.

ECS Price $0.07 USD/hour + EIP Traffic Price $0.153 USD/GB

This price is an estimate and may differ from the final price. Pricing details

Figure 4-15

Step 3 In the ECS list, locate the created ECS and click **Remote Login** to log in to ECS **esc-wordpress** using Remote Login.



Elastic Cloud Server

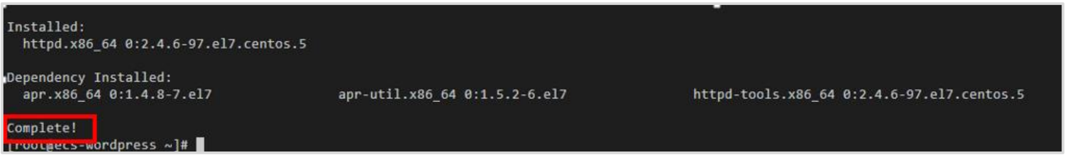
The password reset plug-in can now be installed after creating an ECS. Learn how to install the plug-in.

Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mode	Tag	Operation
ecs-wordpress 4c851cef-9c90-40e3-afa6-33de21fae359		AZ1	Running	2 vCPUs | 4 GiB | c7.large.2 CentOS 7.6 64bit	119.3.173.74 (EIP) 10 Mb... 192.168.2.238 (Private IP)	Pay-per-use Created on Aug 05, 202...	--	Remote Login | More

Figure 4-16

Step 4 Run the following command to install Apache:

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

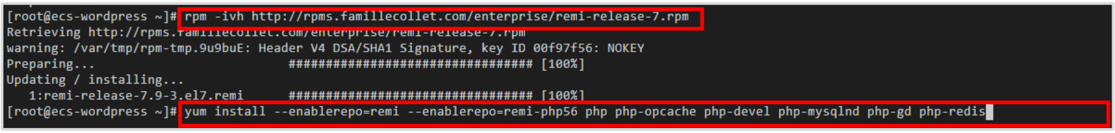


```
Installed:
  httpd.x86_64 0:2.4.6-97.el7.centos.5

Dependency Installed:
  apr.x86_64 0:1.4.8-7.el7                    apr-util.x86_64 0:1.5.2-6.el7                    httpd-tools.x86_64 0:2.4.6-97.el7.centos.5

Complete!
[root@ecs-wordpress ~]#
```

Figure 4-17

Step 5 Run the following command to install PHP:

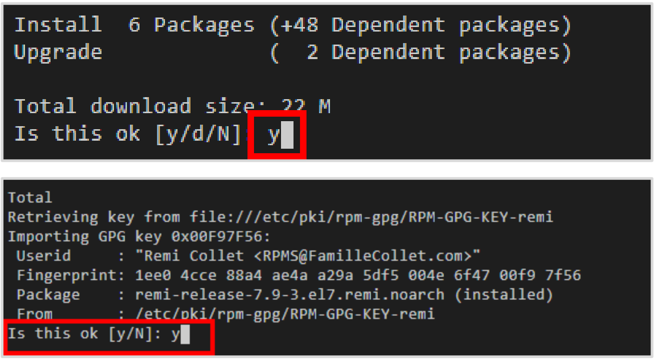
```
[root@ecs-wordpress ~]# rpm -ivh http://rpms.famillecollet.com/enterprise/remi-release-7.rpm
[root@ecs-wordpress ~]# yum install --enablerepo=remi --enablerepo=remi-php72 php php-opcache
php-devel php-mysqlnd php-gd php-redis
```



```
[root@ecs-wordpress ~]# rpm -ivh http://rpms.famillecollet.com/enterprise/remi-release-7.rpm
Retrieving http://rpms.famillecollet.com/enterprise/remi-release-7.rpm
warning: /var/tmp/rpm-tmp.9u9buE: Header V4 DSA/SHA1 Signature, key ID 00f97f56: NOKEY
Preparing...                          ################################# [100%]
Updating / installing...
   1:remi-release-7.9-3.el7.remi      ################################# [100%]
[root@ecs-wordpress ~]# yum install --enablerepo=remi --enablerepo=remi-php56 php php-opcache php-devel php-mysqlnd php-gd php-redis
```

Figure 4-18

Step 6 Enter **y** twice for confirmation.



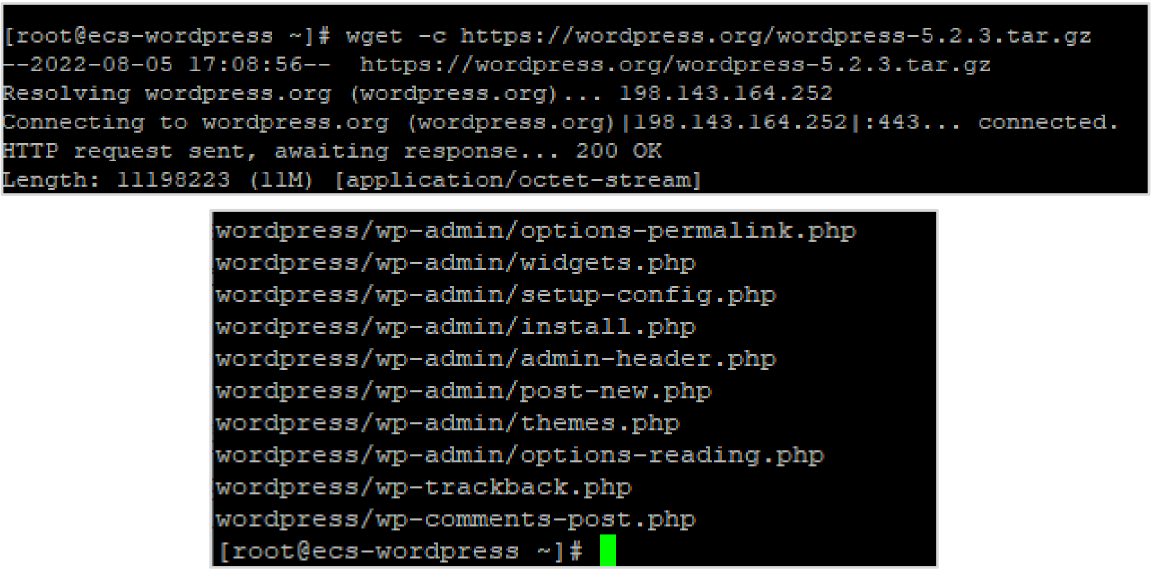
```
Install  6 Packages (+48 Dependent packages)
Upgrade             (  2 Dependent packages)

Total download size: 22 M
Is this ok [y/d/N]: y
```

```
Total
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-remi
Importing GPG key 0x00F97F56:
 Userid     : "Remi Collet <RPMS@FamilleCollet.com>"
 Fingerprint: 1ee0 4cce 88a4 ae4a a29a 5df5 004e 6f47 00f9 7f56
 Package    : remi-release-7.9-3.el7.remi.noarch (installed)
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-remi
Is this ok [y/N]: y
```

Figure 4-19

Step 7 Run the following commands to download the WordPress installation package, decompress the package, and copy the obtained files to Apache directory **/var/www/html**:

```
[root@ecs-wordpress ~]# wget -c https://wordpress.org/wordpress-5.2.3.tar.gz
[root@ecs-wordpress ~]# tar -zxvf wordpress-5.2.3.tar.gz -C /var/www/html
```



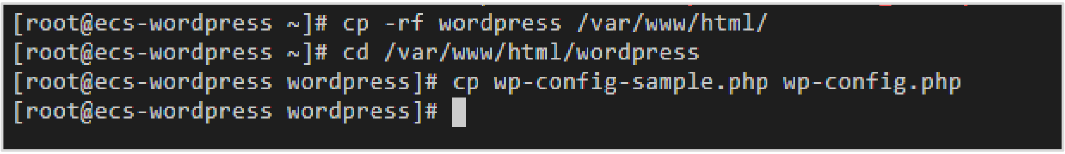
```
[root@ecs-wordpress ~]# wget -c https://wordpress.org/wordpress-5.2.3.tar.gz
--2022-08-05 17:08:56--  https://wordpress.org/wordpress-5.2.3.tar.gz
Resolving wordpress.org (wordpress.org)... 198.143.164.252
Connecting to wordpress.org (wordpress.org)|198.143.164.252|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11198223 (11M) [application/octet-stream]
```

```
wordpress/wp-admin/options-permalink.php
wordpress/wp-admin/widgets.php
wordpress/wp-admin/setup-config.php
wordpress/wp-admin/install.php
wordpress/wp-admin/admin-header.php
wordpress/wp-admin/post-new.php
wordpress/wp-admin/themes.php
wordpress/wp-admin/options-reading.php
wordpress/wp-trackback.php
wordpress/wp-comments-post.php
[root@ecs-wordpress ~]#
```

Figure 4-20

Step 8 Run the following commands to switch to the httpd working directory and copy the configuration file:

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



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

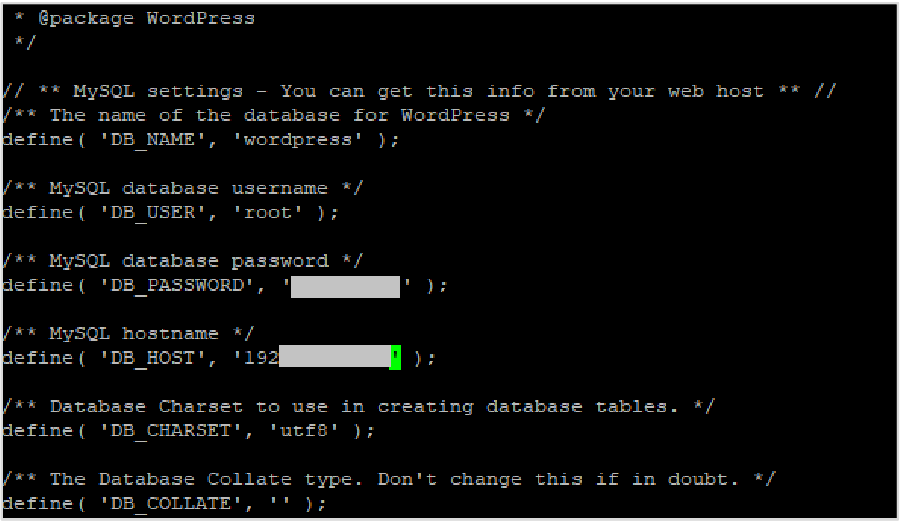
Figure 4-21

Step 9 Run the following command to configure database parameters in the **wp-config.php** file to interconnect with the **wordpress** database:

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

Configure the parameters as follows:

- **DB_NAME**: **wordpress**
- **DB_USER**: **root**
- **DB_PASSWORD**: **Huawei123!@#** (user-defined)
- **DB_HOST**: **192.168.2.40:3306** (private IP address:port number of the DB instance)

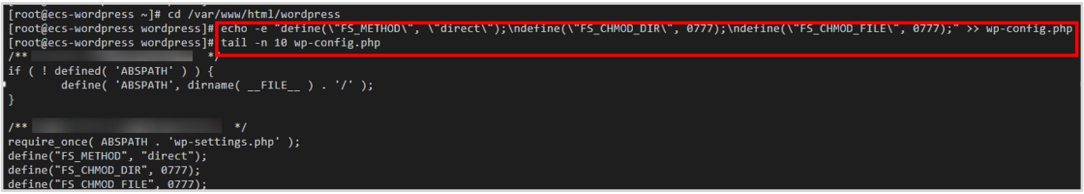


```
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'root' );

/** MySQL database password */
define( 'DB_PASSWORD', '[redacted]' );

/** MySQL hostname */
define( 'DB_HOST', '192[redacted]' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

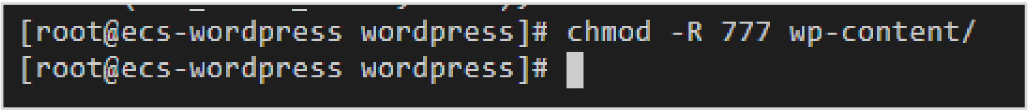
Figure 4-22

Step 10 Run the following commands to configure permissions for the WordPress directory:

```
[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
/** [redacted] */
if ( ! defined( 'ABSPATH' ) ) {
        define( 'ABSPATH', dirname( __FILE__ ) . '/' );
}

/** [redacted] */
require_once( ABSPATH . 'wp-settings.php' );
define("FS_METHOD", "direct");
define("FS_CHMOD_DIR", 0777);
define("FS_CHMOD_FILE", 0777);
```

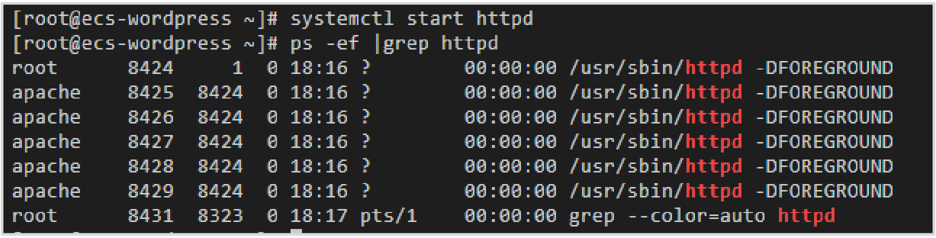


```
[root@ecs-wordpress wordpress]# chmod -R 777 wp-content/
[root@ecs-wordpress wordpress]# 
```

Figure 4-23

Step 11 Run the following commands to enable Apache. If information similar to the following is displayed, Apache is running normally:

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

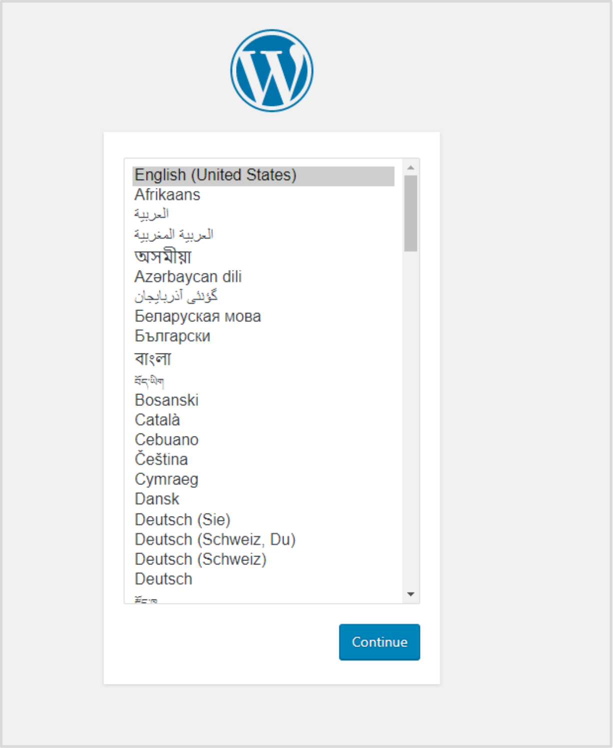


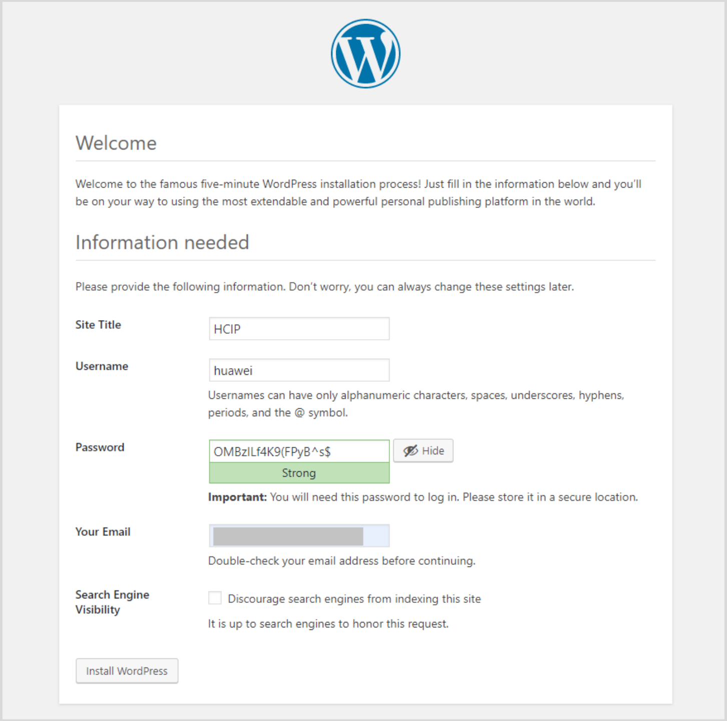
```
[root@ecs-wordpress ~]# systemctl start httpd
[root@ecs-wordpress ~]# ps -ef |grep httpd
root      8424     1  0 18:16 ?        00:00:00 /usr/sbin/httpd -DFOREGROUND
apache    8425  8424  0 18:16 ?        00:00:00 /usr/sbin/httpd -DFOREGROUND
apache    8426  8424  0 18:16 ?        00:00:00 /usr/sbin/httpd -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
```

Figure 4-24

Step 12 Open a browser on your local PC and enter *EIP of ECS-WordPress/wordpress*, for example, enter **121.36.79.241/wordpress/index.php**. After you log in to WordPress, configure parameters as follows and click **Install WordPress**:

- **Site Title**: HCIP
- **Username**: **huawei** (user-defined)
- **Password**: User-defined
- **Your Email**: User-defined





Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Don't worry, you can always change these settings later.

Site Title: HCIP

Username: huawei

Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password: OMBzILf4K9(FPyB^s$

Strong

Important: You will need this password to log in. Please store it in a secure location.

Your Email: [redacted]

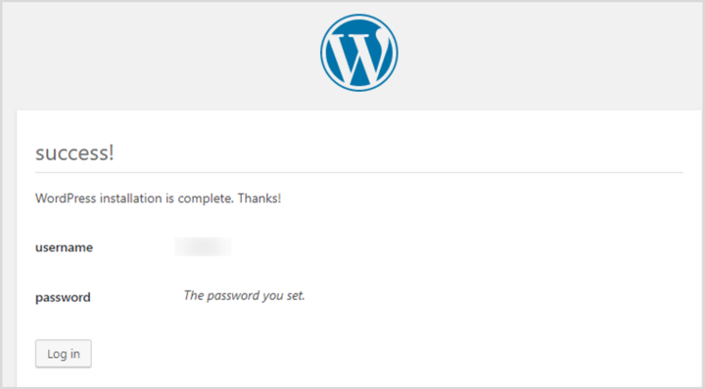
Double-check your email address before continuing.

Search Engine Visibility: □ Discourage search engines from indexing this site

It is up to search engines to honor this request.

Figure 4-25

Step 13 Click **Log in**.



success!

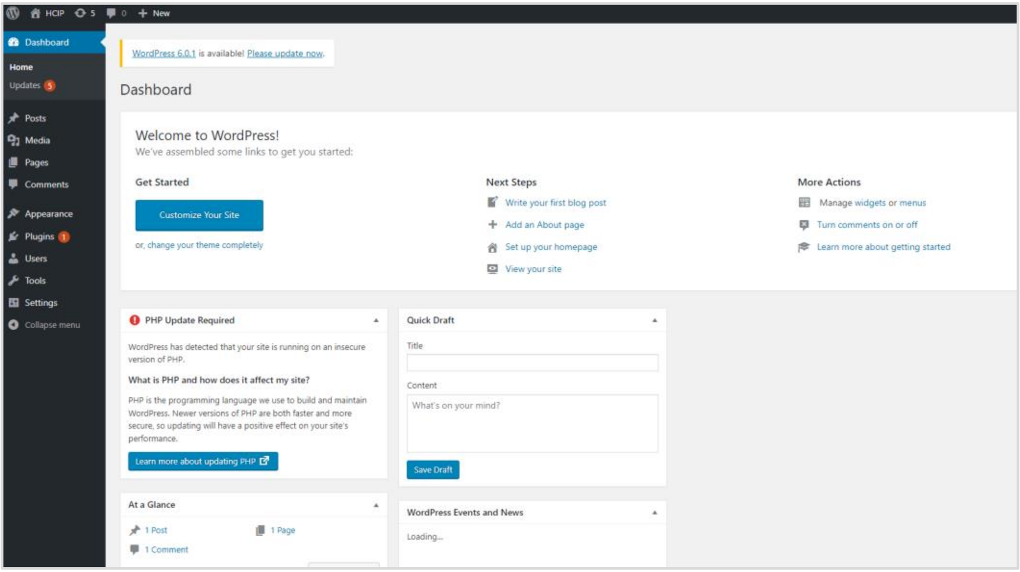
WordPress installation is complete. Thanks!

username [redacted]

password *The password you set.*

Figure 4-26

Step 14 Enter the username and password configured in the previous step to log in to WordPress. If the following page is displayed, WordPress is set up:



WordPress 6.0.1 is available! Please update now.

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

Get Started

or, change your theme completely

Next Steps

- Write your first blog post
- Add an About page
- Set up your homepage
- View your site

More Actions

- Manage widgets or menus
- Turn comments on or off
- Learn more about getting started

PHP Update Required

WordPress has detected that your site is running on an insecure version of PHP.

What is PHP and how does it affect my site?

PHP is the programming language we use to build and maintain WordPress. Newer versions of PHP are both faster and more secure, so updating will have a positive effect on your site's performance.

Quick Draft

Title:

Content: What's on your mind?

At a Glance

1 Post 1 Page

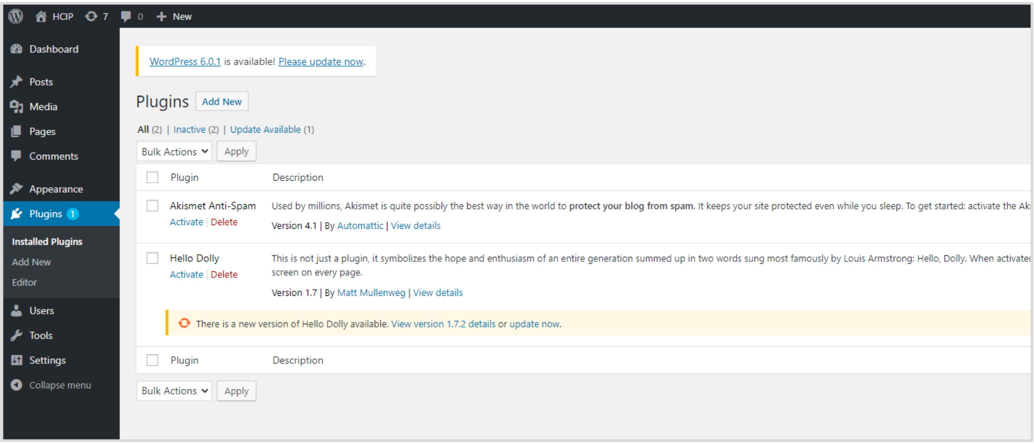
1 Comment

WordPress Events and News

Loading...

Figure 4-27

Step 15 In the navigation pane on the left, choose **Plugins** and then click **Add New**.



WordPress 6.0.1 is available! Please update now.

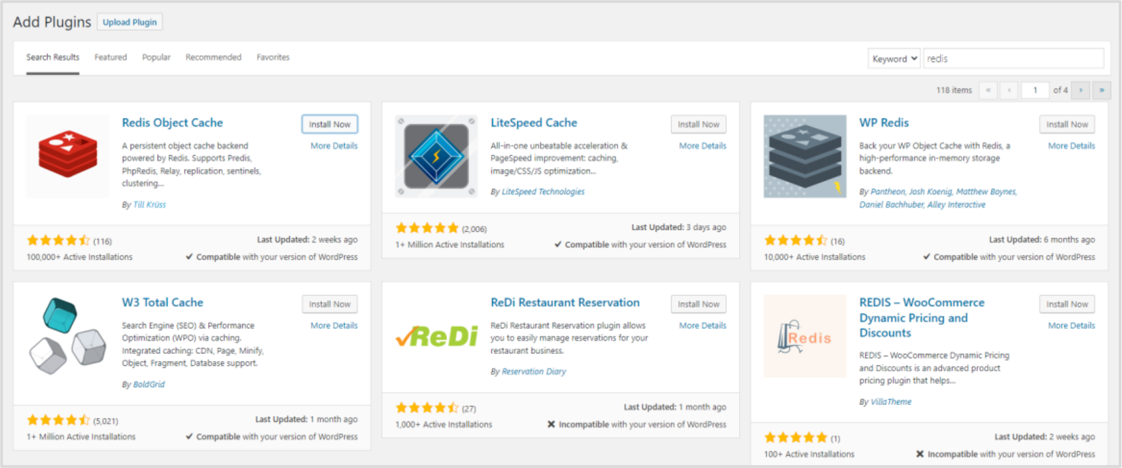
Plugins

All (2) | Inactive (2) | Update Available (1)

□ Plugin	Description
□ Akismet Anti-Spam Activate | Delete	Used by millions, Akismet is quite possibly the best way in the world to **protect your blog from spam.** It keeps your site protected even while you sleep. To get started: activate the Ak Version 4.1 | By Automattic | View details
□ Hello Dolly Activate | Delete	This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated screen on every page. Version 1.7 | By Matt Mullenweg | View details
	There is a new version of Hello Dolly available. View version 1.7.2 details or update now.
□ Plugin	Description

Figure 4-28

Step 16 Enter **redis** in the search box on the right, locate **Redis Object Cache**, and click **Install Now**.



Keyword: redis

Redis Object Cache
A persistent object cache backend powered by Redis. Supports Predis, PhpRedis, Relay, replication, sentinels, clustering...
By Till Krüss
(116) Last Updated: 2 weeks ago
100,000+ Active Installations ✓ Compatible with your version of WordPress

LiteSpeed Cache
All-in-one unbeatable acceleration & PageSpeed improvement: caching, image/CSS/JS optimization...
By LiteSpeed Technologies
(2,006) Last Updated: 3 days ago
1+ Million Active Installations ✓ Compatible with your version of WordPress

WP Redis
Back your WP Object Cache with Redis, a high-performance in-memory storage backend.
By Pantheon, Josh Koenig, Matthew Boynes, Daniel Bachhuber, Alley Interactive
(16) Last Updated: 6 months ago
10,000+ Active Installations ✓ Compatible with your version of WordPress

W3 Total Cache
Search Engine (SEO) & Performance Optimization (WPO) via caching. Integrated caching: CDN, Page, Minify, Object, Fragment, Database support.
By BoldGrid
(5,021) Last Updated: 1 month ago
1+ Million Active Installations ✓ Compatible with your version of WordPress

ReDi Restaurant Reservation
ReDi Restaurant Reservation plugin allows you to easily manage reservations for your restaurant business.
By Reservation Diary
(27) Last Updated: 1 month ago
1,000+ Active Installations ✕ Incompatible with your version of WordPress

REDIS – WooCommerce Dynamic Pricing and Discounts
REDIS – WooCommerce Dynamic Pricing and Discounts is an advanced product pricing plugin that helps...
By VillaTheme
(1) Last Updated: 2 weeks ago
100+ Active Installations ✕ Incompatible with your version of WordPress

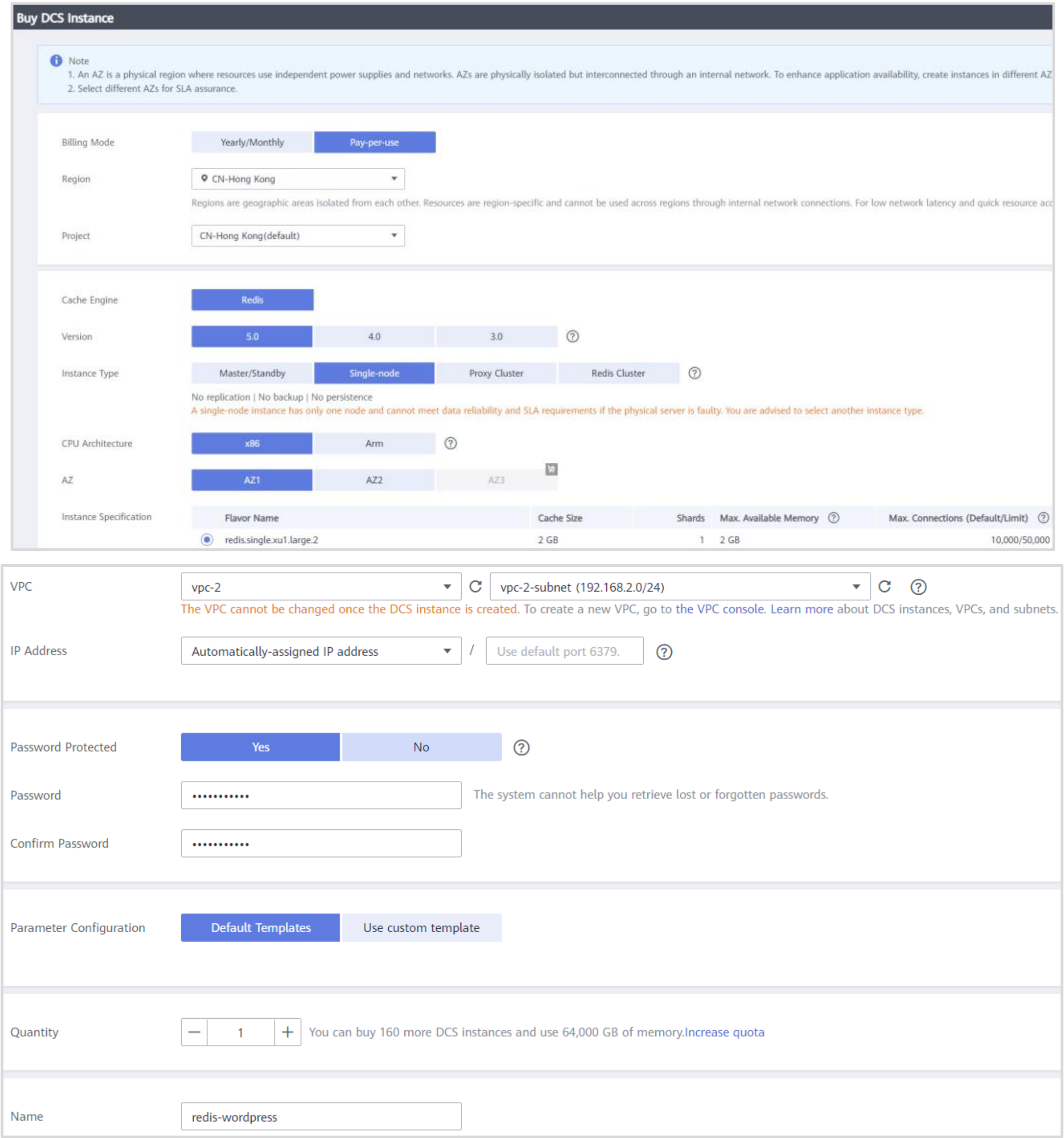
Figure 4-29

4.2.6 Creating a DCS Instance

Step 1 Select region **CN-Hong Kong**, choose **Service List** > **DCS**, click **Buy DCS Instance**, and configure parameters as follows to buy a **DCS** instance:

Note: This exercise uses the **DCS** instance to provide Redis services for WordPress.

- **Billing Mode: Pay-per-use**
- **Region: CN-Hong Kong**
- **Project: CN-Hong Kong (default)**
- **Cache Engine: Redis**
- **Version: 5.0**
- **Instance Type: Single-node**
- **Replicas: 2**
- **AZ: AZ1**
- **Instance Specifications: redis.single.xu1.large.2**
- **VPC: vpc-2**
- **Subnet: vpc-2-subnet**
- **Administrator Password: user-defined**
- **Quantity: 1**
- **Name: redis-wordpress**



Buy DCS Instance

Note
1. An AZ is a physical region where resources use independent power supplies and networks. AZs are physically isolated but interconnected through an internal network. To enhance application availability, create instances in different AZ
2. Select different AZs for SLA assurance.

Billing Mode: Yearly/Monthly | **Pay-per-use**

Region: CN-Hong Kong
Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource acc

Project: CN-Hong Kong(default)

Cache Engine: **Redis**

Version: **5.0** | 4.0 | 3.0

Instance Type: Master/Standby | **Single-node** | Proxy Cluster | Redis Cluster
No replication | No backup | No persistence
A single-node instance has only one node and cannot meet data reliability and SLA requirements if the physical server is faulty. You are advised to select another instance type.

CPU Architecture: **x86** | Arm

AZ: **AZ1** | AZ2 | AZ3

Instance Specification

	Flavor Name	Cache Size	Shards	Max. Available Memory	Max. Connections (Default/Limit)
●	redis.single.xu1.large.2	2 GB	1	2 GB	10,000/50,000

VPC: vpc-2 | vpc-2-subnet (192.168.2.0/24)
The VPC cannot be changed once the DCS instance is created. To create a new VPC, go to the VPC console. Learn more about DCS instances, VPCs, and subnets.

IP Address: Automatically-assigned IP address / Use default port 6379.

Password Protected: **Yes** | No

Password: ••••••••••• The system cannot help you retrieve lost or forgotten passwords.

Confirm Password: •••••••••••

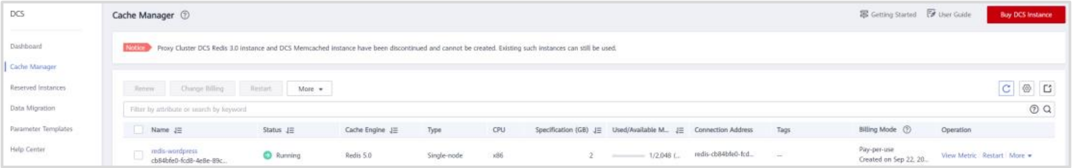
Parameter Configuration: **Default Templates** | Use custom template

Quantity: 1 You can buy 160 more DCS instances and use 64,000 GB of memory.Increase quota

Name: redis-wordpress

Figure 4-30

Step 2 In the instance list, locate the instance that you bought and click its name.

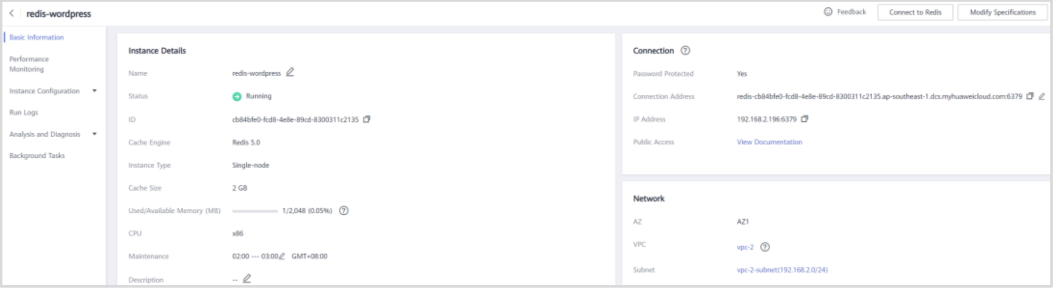


Notice Proxy Cluster DCS Redis 3.0 instance and DCS Memcached instance have been discontinued and cannot be created. Existing such instances can still be used.

Name	Status	Cache Engine	Type	CPU	Specification (GB)	Used/Available M...	Connection Address	Tags	Billing Mode	Operation
redis-wordpress cb84bfe0-fcd8-4e8e-89c...	Running	Redis 5.0	Single-node	x86	2	1/2,048 (...	redis-cb84bfe0-fcd...	--	Pay-per-use Created on Sep 22, 20...	View Metric Restart More

Figure 4-31

Step 3 On the **Connection** page, view and write down the administrator, IP address, port number.



Instance Details

Name	redis-wordpress
Status	Running
ID	cb84bfe0-fcd8-4e8e-89cd-8300311c2135
Cache Engine	Redis 5.0
Instance Type	Single-node
Cache Size	2 GB
Used/Available Memory (MB)	1/2,048 (0.05%)
CPU	x86
Maintenance	02:00 --- 03:00 GMT+08:00
Description	--

Connection

Password Protected	Yes
Connection Address	redis-cb84bfe0-fcd8-4e8e-89cd-8300311c2135.ap-southeast-1.dcs.myhuaweicloud.com:6379
IP Address	192.168.2.196:6379
Public Access	View Documentation

Network

AZ	AZ1
VPC	vpc-2
Subnet	vpc-2-subnet(192.168.2.0/24)

Figure 4-32

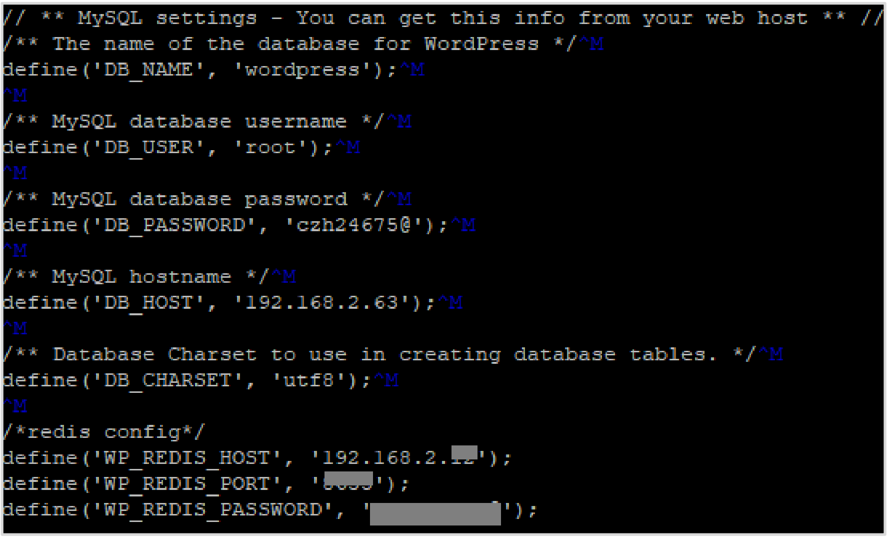
Step 4 Log in to ECS **ecs-wordpress** and run the following commands to modify its configuration file:

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

Add the following information to the file to interconnect with the DCS instance:

```
/*redis config*/
define('WP_REDIS_HOST', '192.168.2.IP');
define('WP_REDIS_PORT', '6379');
define('WP_REDIS_PASSWORD', 'DCS PASSWORD');
```

Note: **192.168.2.IP** is the IP address of the DCS instance recorded in step 3. Configure the IP address based on service requirements. **DCS PASSWORD** is the password of the DCS instance set in step 1. Enter the required password.



```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */^M
define('DB_NAME', 'wordpress');^M
^M
/** MySQL database username */^M
define('DB_USER', 'root');^M
^M
/** MySQL database password */^M
define('DB_PASSWORD', 'czh24675@');^M
^M
/** MySQL hostname */^M
define('DB_HOST', '192.168.2.63');^M
^M
/** Database Charset to use in creating database tables. */^M
define('DB_CHARSET', 'utf8');^M
^M
/*redis config*/
define('WP_REDIS_HOST', '192.168.2.[redacted]');
define('WP_REDIS_PORT', '[redacted]');
define('WP_REDIS_PASSWORD', '[redacted]');
```

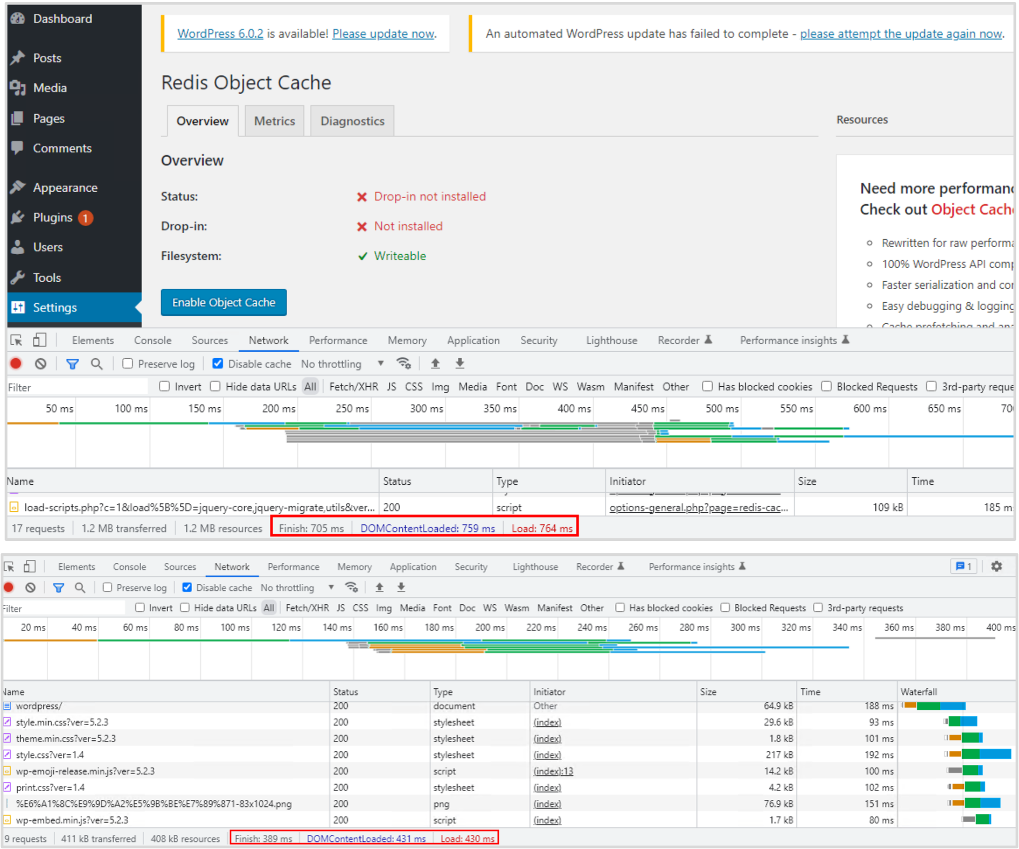
Figure 4-33

Step 5 Run the following command to exit:

```
:wq
```

4.2.7 Enabling Redis Object Cache

Step 1 Before enabling Redis Object Cache, Please post a blog with text and pictures, then open a browser, press **F12**, select **Disable cache**, and view the time required for loading. Refresh the WordPress page and find that the time for loading content is 430ms.



WordPress 6.0.2 is available! Please update now.

An automated WordPress update has failed to complete - please attempt the update again now.

Redis Object Cache

Overview

Status: ✕ Drop-in not installed

Drop-in: ✕ Not installed

Filesystem: ✓ Writeable

Need more performanc
Check out Object Cach

- Rewritten for raw performa
- 100% WordPress API comp
- Faster serialization and co
- Easy debugging & logging
- Cache prefetching and an

Name	Status	Type	Initiator	Size	Time
load-scripts.php?c=1&load%5B%5D=jquery-core,jquery-migrate,utils&ver...	200	script	options-general.php?page=redis-cac...	109 kB	185 m

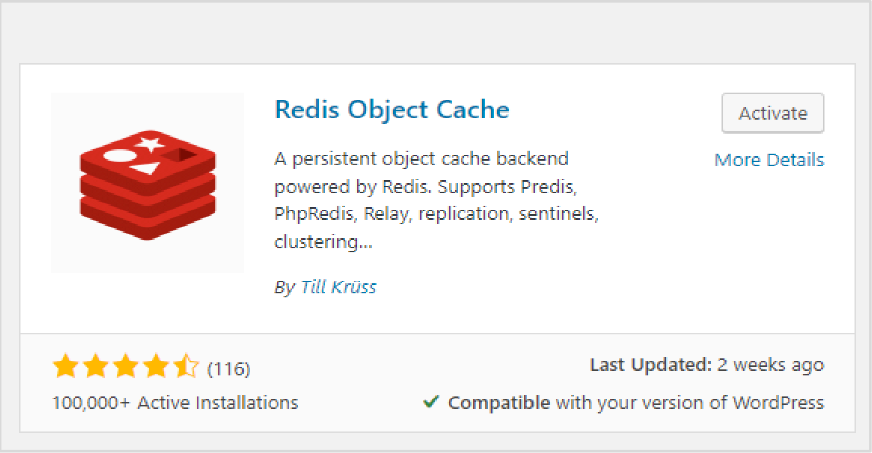
17 requests | 1.2 MB transferred | 1.2 MB resources | Finish: 705 ms | DOMContentLoaded: 759 ms | Load: 764 ms

Name	Status	Type	Initiator	Size	Time	Waterfall
wordpress/	200	document	Other	64.9 kB	188 ms	
style.min.css?ver=5.2.3	200	stylesheet	(index)	29.6 kB	93 ms	
theme.min.css?ver=5.2.3	200	stylesheet	(index)	1.8 kB	101 ms	
style.css?ver=1.4	200	stylesheet	(index)	217 kB	192 ms	
wp-emoji-release.min.js?ver=5.2.3	200	script	(index):13	14.2 kB	100 ms	
print.css?ver=1.4	200	stylesheet	(index)	4.2 kB	102 ms	
%E6%A1%8C%E9%9D%A2%E5%9B%BE%E7%89%871-83x1024.png	200	png	(index)	76.9 kB	151 ms	
wp-embed.min.js?ver=5.2.3	200	script	(index)	1.7 kB	80 ms	

9 requests | 411 kB transferred | 408 kB resources | Finish: 389 ms | DOMContentLoaded: 431 ms | Load: 430 ms

Figure 4-34

Step 2 Log in to WordPress on your local PC, choose **Plugins** > **Installed Plugins**, locate **Redis Object Cache**, and click **Activate**.



Redis Object Cache

A persistent object cache backend powered by Redis. Supports Predis, PhpRedis, Relay, replication, sentinels, clustering...

By Till Krüss

★★★★☆ (116)

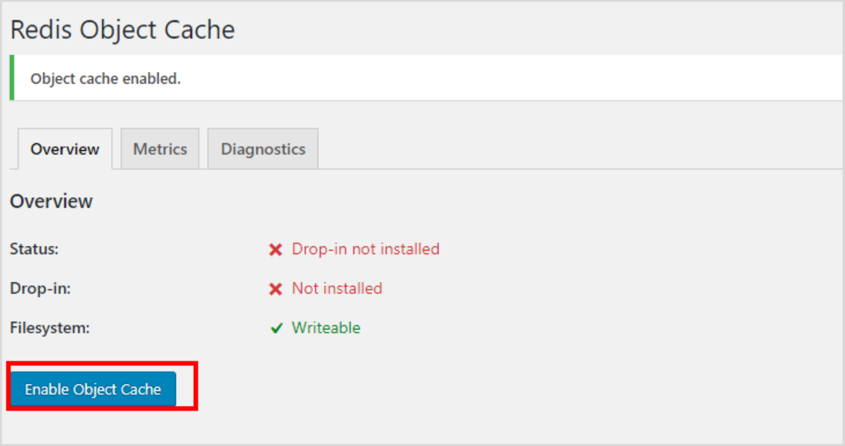
100,000+ Active Installations

Last Updated: 2 weeks ago

✓ Compatible with your version of WordPress

Figure 4-35

Step 3 On the displayed page, click the **Overview** tab and click **Enable Object Cache**.



Redis Object Cache

Object cache enabled.

Overview

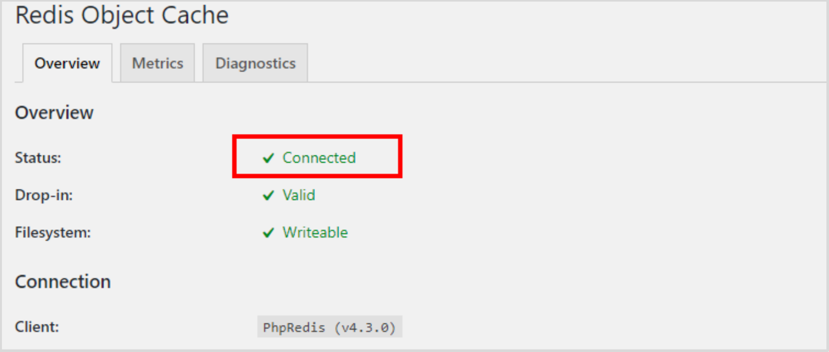
Status: ✗ Drop-in not installed

Drop-in: ✗ Not installed

Filesystem: ✓ Writeable

Figure 4-36

Step 4 Check whether the status is **Connected**. If yes, Redis Object Cache is enabled.



Redis Object Cache

Overview

Status: ✓ Connected

Drop-in: ✓ Valid

Filesystem: ✓ Writeable

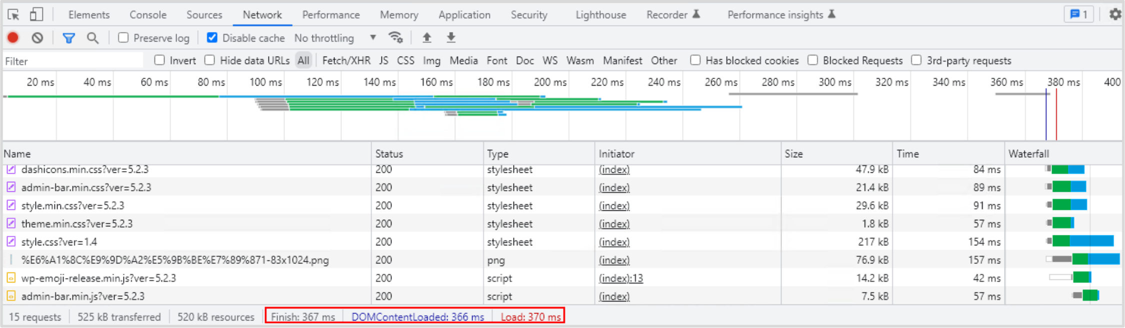
Connection

Client: `PhpRedis (v4.3.0)`

Figure 4-37

4.3 Verifying the Result

Step 1 Open a browser, press **F12**, select **Disable cache**, and view the time required for page loading. Refresh the page. If the time for loading is 370ms, less than 430ms required before Redis Object Cache is enabled, the website response is speed up. This exercise is successful.



□ Preserve log ☑ Disable cache No throttling

Name	Status	Type	Initiator	Size	Time	Waterfall
dashicons.min.css?ver=5.2.3	200	stylesheet	(index)	47.9 kB	84 ms	
admin-bar.min.css?ver=5.2.3	200	stylesheet	(index)	21.4 kB	89 ms	
style.min.css?ver=5.2.3	200	stylesheet	(index)	29.6 kB	91 ms	
theme.min.css?ver=5.2.3	200	stylesheet	(index)	1.8 kB	57 ms	
style.css?ver=1.4	200	stylesheet	(index)	217 kB	154 ms	
%E6%A1%8C%E9%9D%A2%E5%9B%BE%E7%89%871-83x1024.png	200	png	(index)	76.9 kB	157 ms	
wp-emoji-release.min.js?ver=5.2.3	200	script	(index):13	14.2 kB	42 ms	
admin-bar.min.js?ver=5.2.3	200	script	(index)	7.5 kB	57 ms	

15 requests | 525 kB transferred | 520 kB resources | Finish: 367 ms | DOMContentLoaded: 366 ms | Load: 370 ms

Figure 4-38

4.4 Clearing Resources

Step 1 Delete the DCS instance.

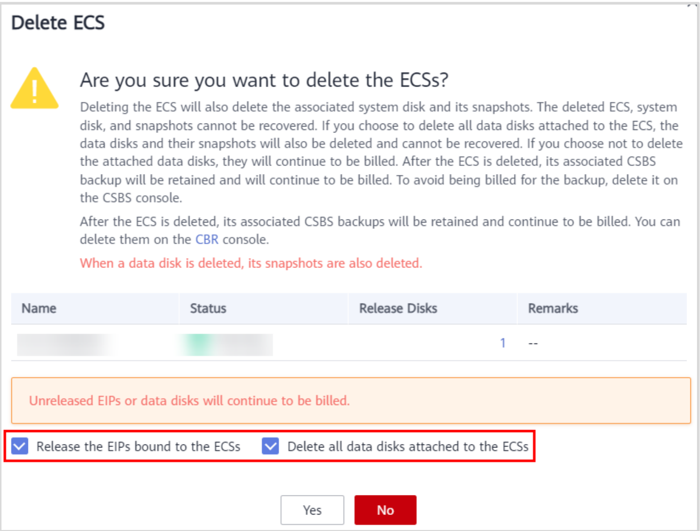
Choose **Service List** > **DCS**. In the instance list, locate the DB instance that you bought in this exercise and click **Delete** in the **Operation** column.

Step 2 Delete the RDS for MySQL instance.

Choose **Service List** > **RDS**. In the instance list, locate the DB instance that you bought in this exercise and click **Delete** in the **Operation** column.

Step 3 Delete the ECS.

- Choose **Service List** > **Elastic Cloud Server**. In the ECS list, locate the ECS that you created in this exercise and click **Delete** in the **Operation** column.
- In the displayed dialog box, select the options displayed in the following picture and click **Yes**.



Delete ECS

Are you sure you want to delete the ECSs?

Deleting the ECS will also delete the associated system disk and its snapshots. The deleted ECS, system disk, and snapshots cannot be recovered. If you choose to delete all data disks attached to the ECS, the data disks and their snapshots will also be deleted and cannot be recovered. If you choose not to delete the attached data disks, they will continue to be billed. After the ECS is deleted, its associated CSBS backup will be retained and will continue to be billed. To avoid being billed for the backup, delete it on the CSBS console.

After the ECS is deleted, its associated CSBS backups will be retained and continue to be billed. You can delete them on the CBR console.

When a data disk is deleted, its snapshots are also deleted.

Name	Status	Release Disks	Remarks
[redacted]	[redacted]	1	--

Unreleased EIPs or data disks will continue to be billed.

☑ Release the EIPs bound to the ECSs ☑ Delete all data disks attached to the ECSs

Figure 4-39 Deleting the ECS

Step 4 Delete the security groups.

Choose **Service List** > **Virtual Private Cloud** > **Access Control** > **Security Groups**. In the security group list, locate the security group that you created in this exercise and click **Delete** in the **Operation** column.

Step 5 Delete the subnet and VPC.

- Choose **Service List** > **Virtual Private Cloud** > **Subnets**. In the subnet list, locate the subnet that you created in this exercise and click **Delete** in the **Operation** column.
- Choose **My VPCs** in the navigation pane on the left. In the VPC list, locate the VPC that you created in this exercise and click **Delete** in the **Operation** column.

4.5 Quiz

Question: What Service Can I Use If I Want to Improve Database Storage and Performance by Configuring Multiple Database Instances?

Answer: You can use Huawei Cloud Distributed Database Middleware (DDM). It can scale out your compute and storage resources linearly, helping you handle high concurrency and real-time interactions

5 Security Architecture Design

5.1 Introduction

5.1.1 About This Exercise

This exercise involves the following operations:

- Damn Vulnerable Web Application (DVWA) server deployment: Deploy a DVWA server on ECS to provide an exercise environment, and perform subsequent security operations on the server.
- Host Security Service (HSS): Purchase HSS for the DVWA server. Obtain server status and check server risks on the HSS console. Improve server security management capabilities.
- Two-factor authentication: Configure two-factor authentication for the DVWA server, and log in to the server through two-factor authentication. Learn the basic functions of two-factor authentication.
- Host security group: Verify the access control function of the host security group by deleting and adding port 8080 to the security group.
- IP address group: Verify how to configure the address group and security group and learn how they work. Add a test cloud server address to an address group, and add the address group to the deny rule of a security group.
- Data Encryption Workshop (DEW): In this exercise, create a key on the DEW console, create an agency on the IAM page, and install the KooCLI client on the ECS. With these configurations, the KooCLI client can obtain information about the keys managed in DEW.

5.1.2 Objectives

To understand how HSS works.

To learn how to configure and use two-factor authentication, security groups, and address groups.

To learn how to configure and use Web Application Firewall (WAF).

To learn how to use ECS to obtain the keys managed in DEW.

5.1.3 Networking

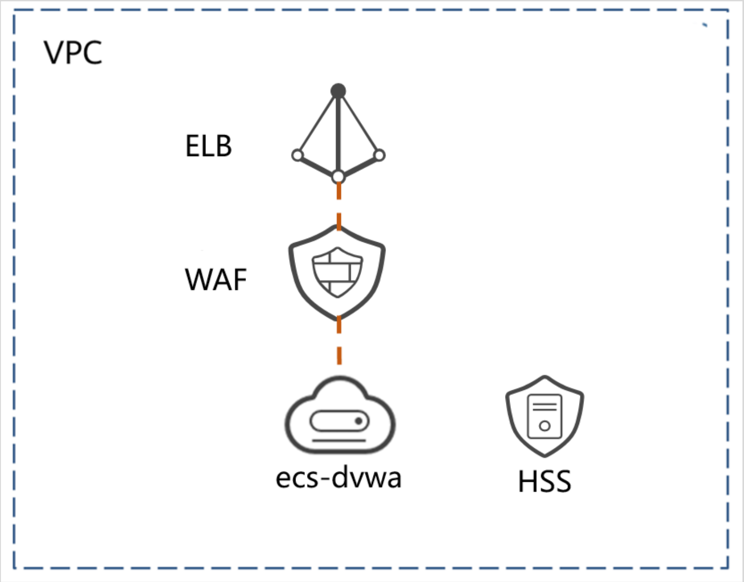


Figure 5-1

5.1.4 Related Software

- Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is highly vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment. DVWA contains common vulnerabilities that can be exploited by SQL injection, XSS, and blind injection.
- XAMPP is a completely free, easy to install Apache distribution containing MySQL, PHP, and Perl. The XAMPP open source package has been set up to be incredibly easy to install and to use. It can help you easily set up a web server.
- Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.
- KooCLI is a Huawei Cloud Command Line Interface, a tool for managing cloud service APIs released on API Explorer. With this tool, you can call open APIs of cloud services to manage and use your cloud resources.

5.2 Procedure

5.2.1 Deploying DVWA

Step 1 In the **CN-Hong Kong** region, choose **Networking** > **Virtual Private Cloud** in the service list.

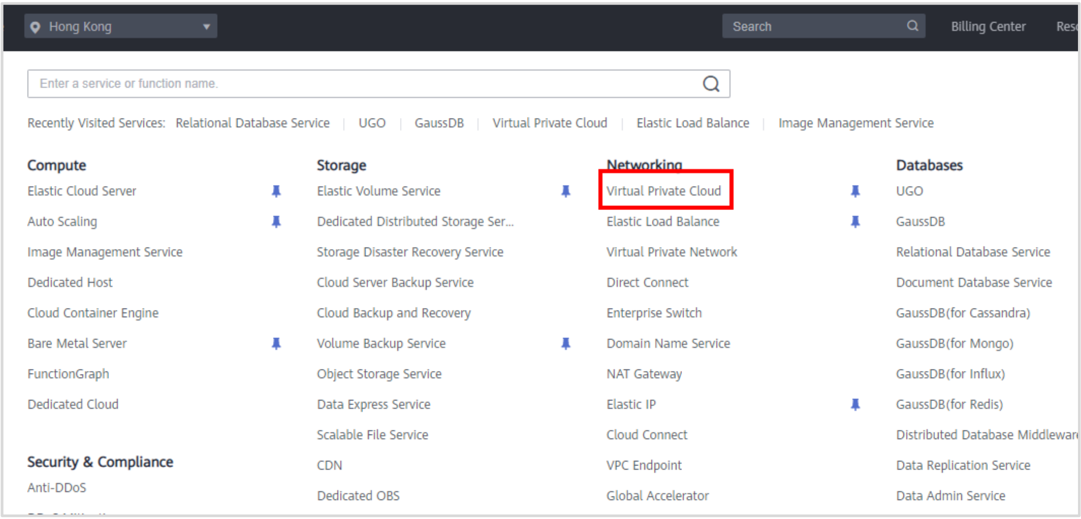
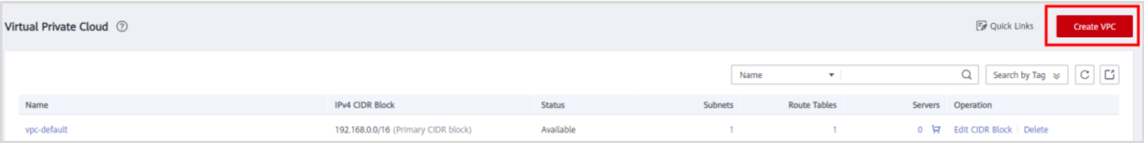


Figure 5-2

Step 2 Click **Create VPC** in the upper right corner. (Resources in this exercise will be created in this VPC.)



Name	IPv4 CIDR Block	Status	Subnets	Route Tables	Servers	Operation
vpc-default	192.168.0.0/16 (Primary CIDR block)	Available	1	1	0	Edit CIDR Block | Delete

Figure 5-3

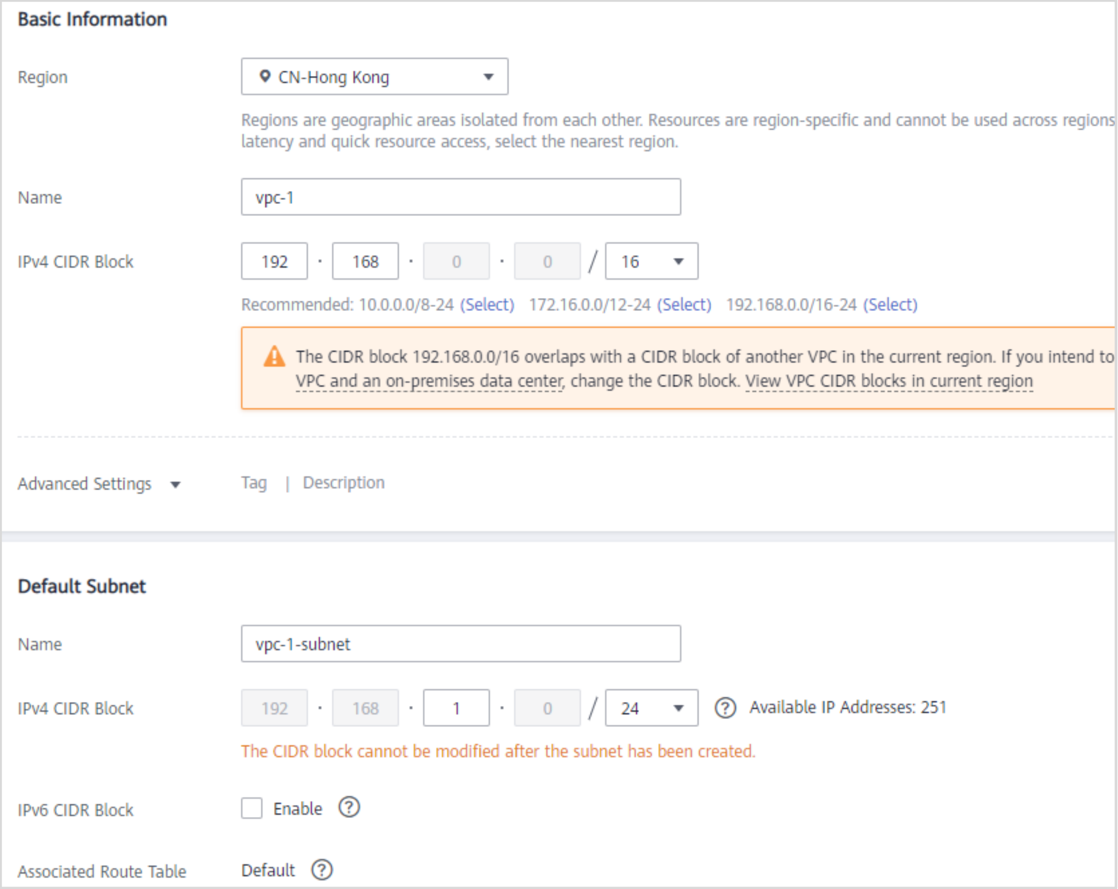
Step 3 Configure the following parameters and click **Create Now**.

Basic Information

- **Region: CN-Hong Kong**
- **Name: vpc-1**
- **IPv4 CIDR Block: 192.168.0.0/16**

Default Subnet

- **AZ: AZ1**
- **Name: subnet-20**
- **IPv4 CIDR Block: 192.168.20.0/24**



Basic Information

Region: CN-Hong Kong

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions latency and quick resource access, select the nearest region.

Name: vpc-1

IPv4 CIDR Block: 192 . 168 . 0 . 0 / 16

Recommended: 10.0.0.0/8-24 (Select) 172.16.0.0/12-24 (Select) 192.168.0.0/16-24 (Select)

The CIDR block 192.168.0.0/16 overlaps with a CIDR block of another VPC in the current region. If you intend to VPC and an on-premises data center, change the CIDR block. View VPC CIDR blocks in current region

Advanced Settings ▾ Tag | Description

Default Subnet

Name: vpc-1-subnet

IPv4 CIDR Block: 192 . 168 . 1 . 0 / 24 Available IP Addresses: 251

The CIDR block cannot be modified after the subnet has been created.

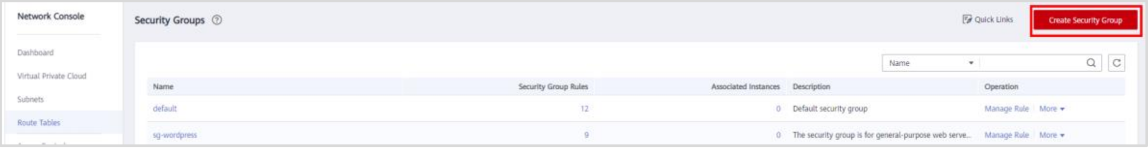
IPv6 CIDR Block: □ Enable

Associated Route Table: Default

Figure 5-4

Step 4 In the navigation pane on the left, choose **Access Control** > **Security Groups**, and click **Create Security Group** in the upper right corner.

Note: This security group is used by DVWA ECSs and should allow all ICMP traffic and traffic on ports 22, 443, 80, and 8080.

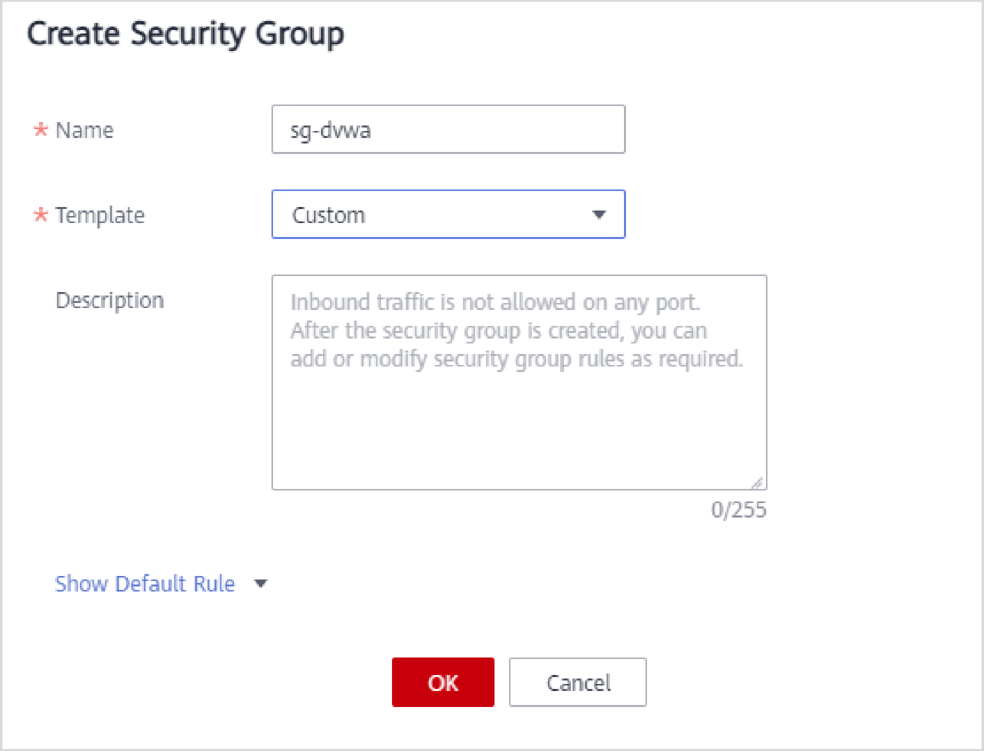


Name	Security Group Rules	Associated Instances	Description	Operation
default	12	0	Default security group	Manage Rule More ▾
sg-wordpress	9	0	The security group is for general-purpose web serve...	Manage Rule More ▾

Figure 5-5

Step 5 Configure the parameters as follows and click **OK**.

- **Name**: **sg-dvwa**
- **Template**: Select a required one.



Create Security Group

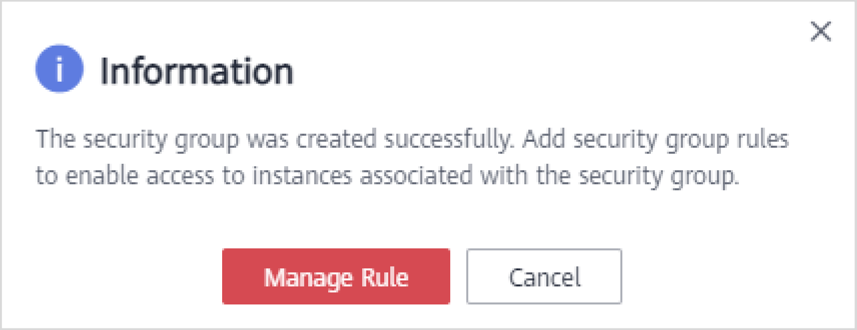
* Name: sg-dwva

* Template: Custom

Description: Inbound traffic is not allowed on any port. After the security group is created, you can add or modify security group rules as required.

Figure 5-6

Step 6 In the dialog box displayed, click **Manage Rule**.



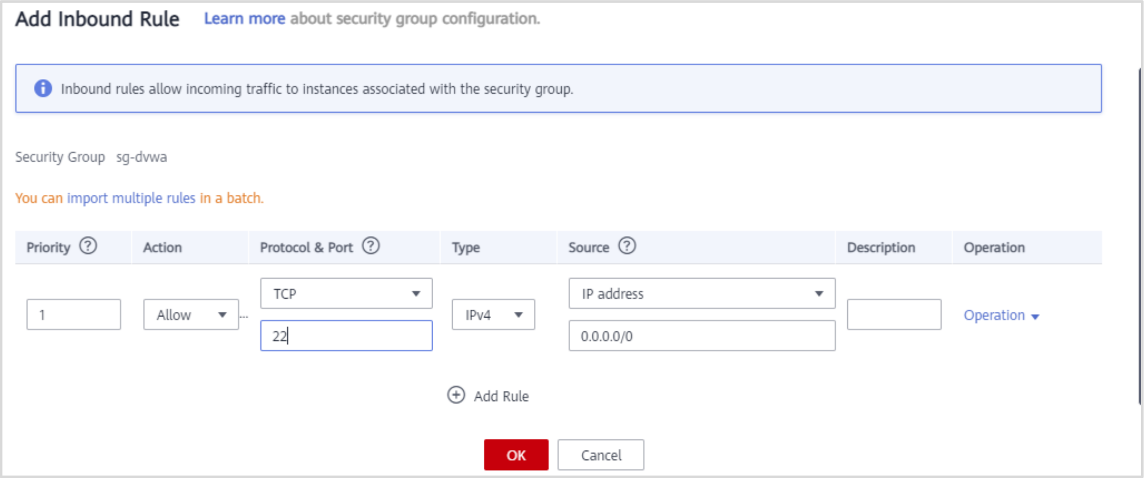
Information

The security group was created successfully. Add security group rules to enable access to instances associated with the security group.

Figure 5-7

Step 7 On the **Inbound Rules** tab, add the following inbound rules.

- **Priority**: **1**
- **Action**: **Allow**
- **Protocol & Port**: **TCP** | **22**
- **Type**: **IPv4**
- **Source**: **IP address** | **0.0.0.0/0**



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

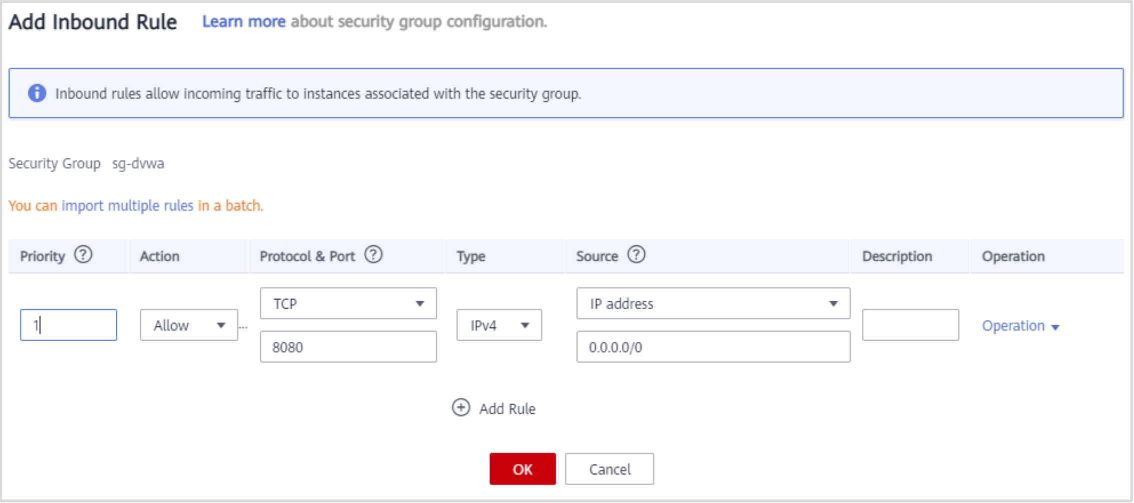
Security Group sg-dvwa

You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Source	Description	Operation
1	Allow	TCP 22	IPv4	IP address 0.0.0.0/0		Operation

Figure 5-8

- Priority: 1
- Action: Allow
- Protocol & Port: TCP | 8080
- Type: IPv4
- Source: IP address | 0.0.0.0/0



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

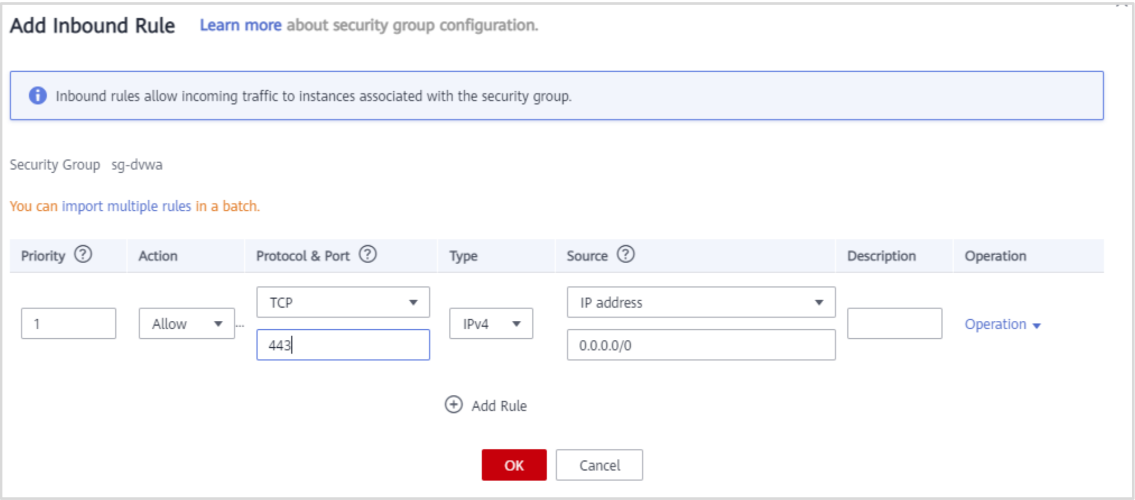
Security Group sg-dvwa

You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Source	Description	Operation
1	Allow	TCP 8080	IPv4	IP address 0.0.0.0/0		Operation

Figure 5-9

- Priority: 1
- Action: Allow
- Protocol & Port: TCP | 443
- Type: IPv4
- Source: IP address | 0.0.0.0/0



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

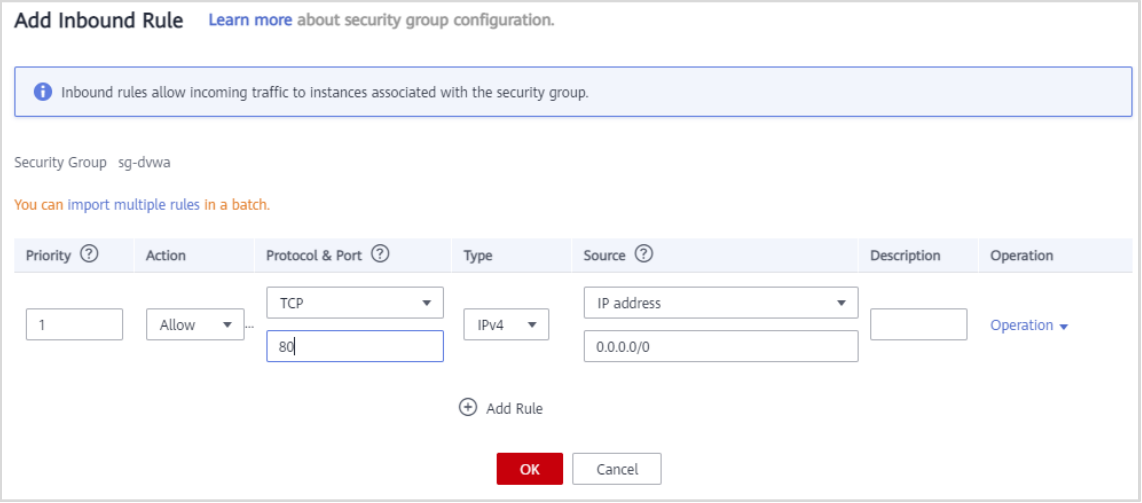
Security Group sg-dvwa

You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Source	Description	Operation
1	Allow	TCP 443	IPv4	IP address 0.0.0.0/0		Operation

Figure 5-10

- Priority: 1
- Action: Allow
- Protocol & Port: TCP | 80
- Type: IPv4
- Source: IP address | 0.0.0.0/0



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

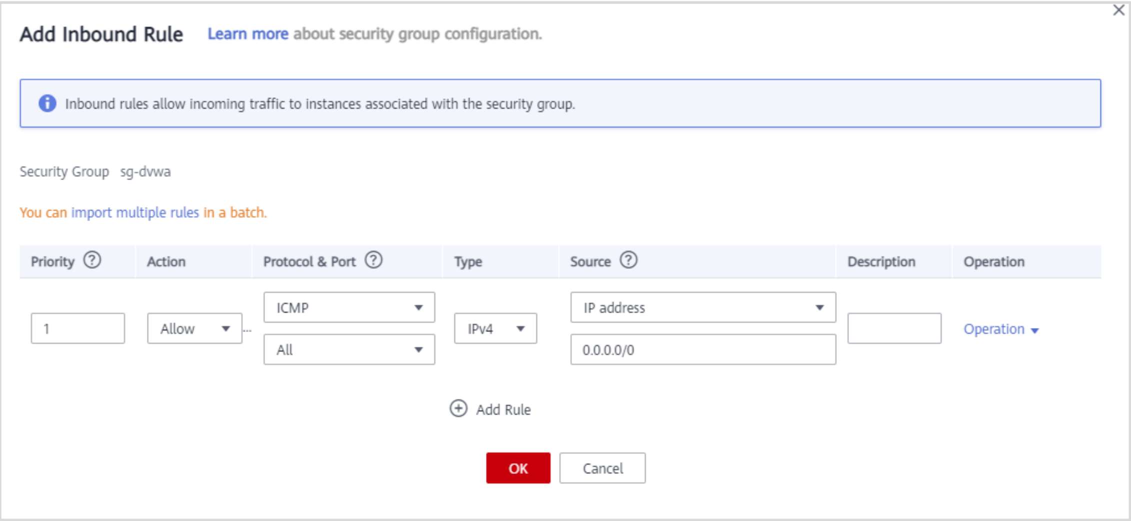
Security Group sg-dvwa

You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Source	Description	Operation
1	Allow	TCP 80	IPv4	IP address 0.0.0.0/0		Operation

Figure 5-11

- Priority: 1
- Action: Allow
- Protocol & Port: ICMP | All
- Type: IPv4
- Source: IP address | 0.0.0.0/0



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group sg-dvwa

You can import multiple rules in a batch.

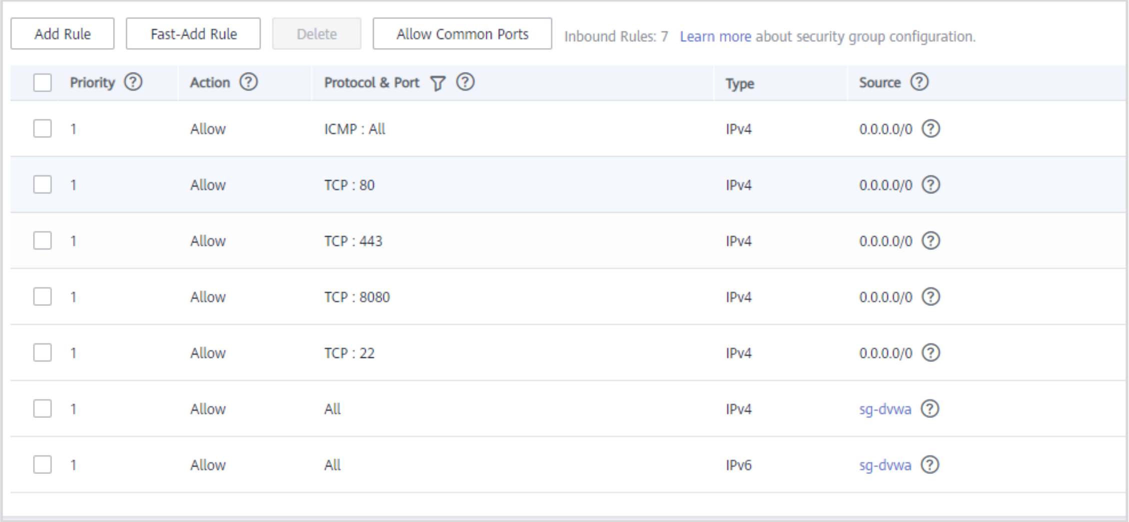
Priority	Action	Protocol & Port	Type	Source	Description	Operation
1	Allow	ICMP All	IPv4	IP address 0.0.0.0/0		Operation

Add Rule

OK Cancel

Figure 5-12

Step 8 Check the added inbound rules. There are inbound rules that allow ICMP traffic and traffic on ports 80, 22, 8080, and 443.

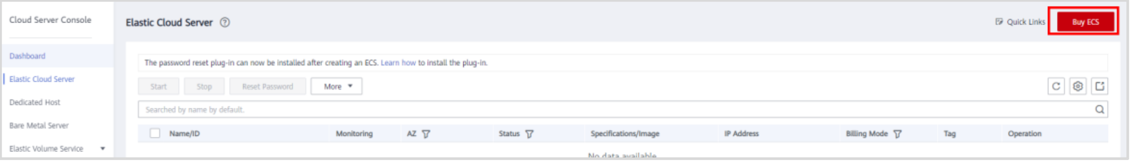


Add Rule Fast-Add Rule Delete Allow Common Ports Inbound Rules: 7 Learn more about security group configuration.

□	Priority	Action	Protocol & Port	Type	Source
□	1	Allow	ICMP : All	IPv4	0.0.0.0/0
□	1	Allow	TCP : 80	IPv4	0.0.0.0/0
□	1	Allow	TCP : 443	IPv4	0.0.0.0/0
□	1	Allow	TCP : 8080	IPv4	0.0.0.0/0
□	1	Allow	TCP : 22	IPv4	0.0.0.0/0
□	1	Allow	All	IPv4	sg-dvwa
□	1	Allow	All	IPv6	sg-dvwa

Figure 5-13

Step 9 In the service list, choose **Elastic Cloud Server** under **Compute**. On the displayed page, click **Buy ECS** in the upper right corner.



The password reset plug-in can now be installed after creating an ECS. Learn how to install the plug-in.

Searched by name by default.

□	Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mode	Tag	Operation

No data available

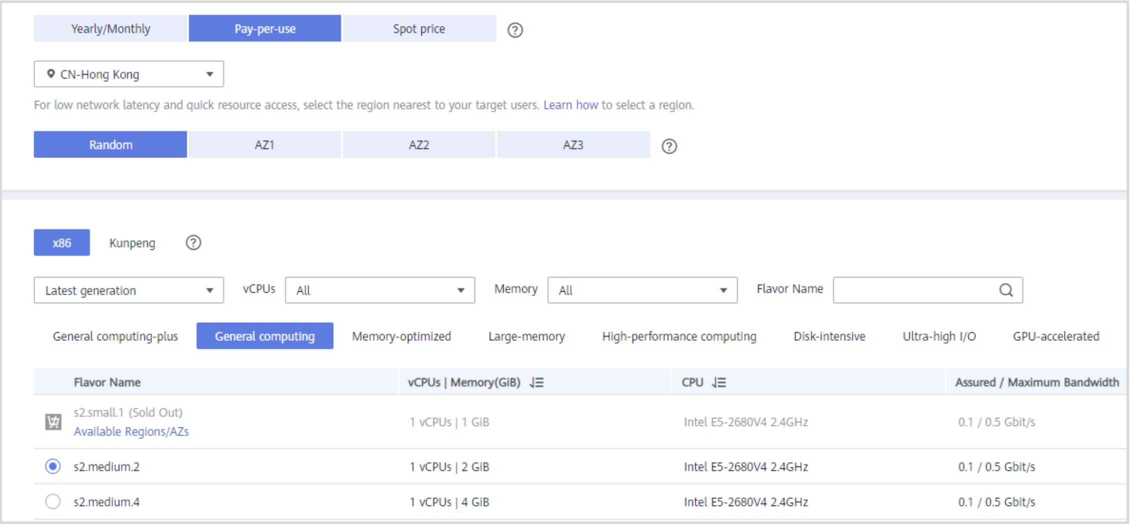
Figure 5-14

Step 10 Configure settings for the ECS.

Note: This ECS will be used to deploy DVWA.

The following uses **ecs-dvwa** as an example.

- Billing Mode: Pay-per-use
- Region: CN-Hong Kong
- AZ: Random
- CPU Architecture: x86
- Specifications: 1 vCPUs | 2 GiB
- Image: Public image | CentOS 7.6 64bit(40GB)
- Host Security: Enable (Basic)
- Network: vpc-1 | subnet-20 | Automatically assign IP address
- Security Group: sg-dvwa
- EIP: Auto assign
- EIP Type: Premium BGP
- Billed By: Traffic
- Bandwidth Size: 10 Mbit/s
- System Disk: High I/O | 40 GiB
- ECS Name: ecs-dvwa
- **Password**: User-defined (with the username of **root**)



For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

	Flavor Name	vCPUs | Memory(GiB)	CPU	Assured / Maximum Bandwidth
	s2.small.1 (Sold Out) Available Regions/AZs	1 vCPUs | 1 GiB	Intel E5-2680V4 2.4GHz	0.1 / 0.5 Gbit/s
●	s2.medium.2	1 vCPUs | 2 GiB	Intel E5-2680V4 2.4GHz	0.1 / 0.5 Gbit/s
○	s2.medium.4	1 vCPUs | 4 GiB	Intel E5-2680V4 2.4GHz	0.1 / 0.5 Gbit/s

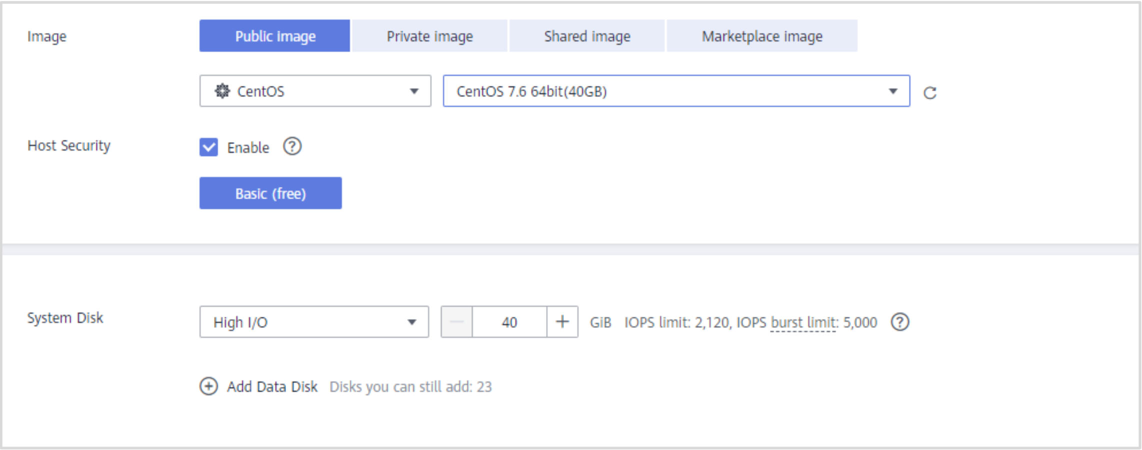
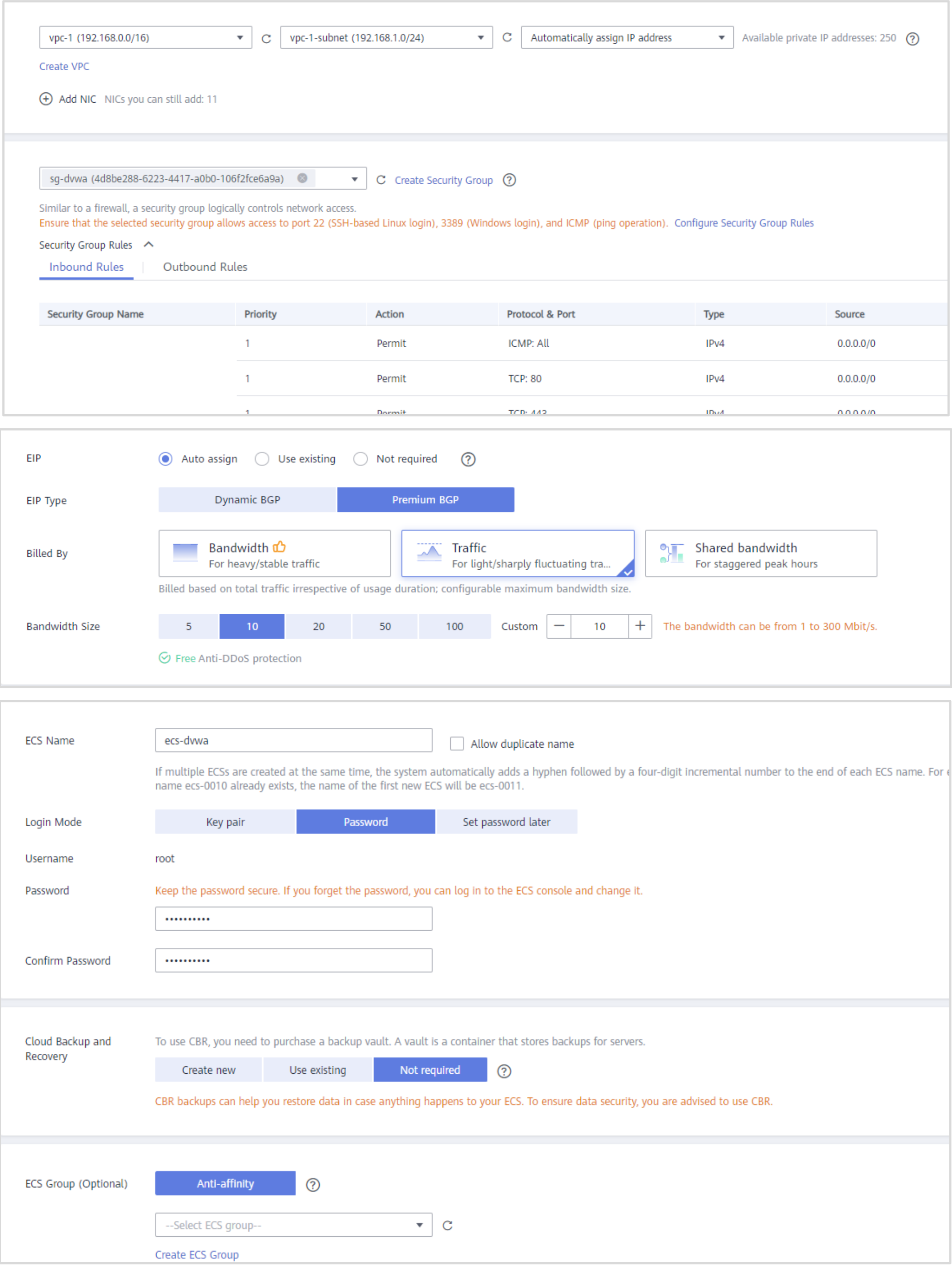


Image: CentOS | CentOS 7.6 64bit(40GB)

Host Security: ☑ Enable

System Disk: High I/O | 40 GiB IOPS limit: 2,120, IOPS burst limit: 5,000

Disks you can still add: 23



vpc-1 (192.168.0.0/16) ▾ | vpc-1-subnet (192.168.1.0/24) ▾ | Automatically assign IP address ▾ | Available private IP addresses: 250

Create VPC

⊕ Add NIC NICs you can still add: 11

sg-dvwa (4d8be288-6223-4417-a0b0-106f2fce6a9a) ▾ Create Security Group

Similar to a firewall, a security group logically controls network access.
Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

Security Group Rules

Inbound Rules | Outbound Rules

Security Group Name	Priority	Action	Protocol & Port	Type	Source
	1	Permit	ICMP: All	IPv4	0.0.0.0/0
	1	Permit	TCP: 80	IPv4	0.0.0.0/0
	1	Permit	TCP: 443	IPv4	0.0.0.0/0

EIP: ● Auto assign ○ Use existing ○ Not required

EIP Type: Dynamic BGP | **Premium BGP**

Billed By: Bandwidth (For heavy/stable traffic) | **Traffic** (For light/sharply fluctuating tra...) | Shared bandwidth (For staggered peak hours)

Billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size.

Bandwidth Size: 5 | **10** | 20 | 50 | 100 | Custom — 10 + The bandwidth can be from 1 to 300 Mbit/s.

✓ Free Anti-DDoS protection

ECS Name: ecs-dvwa □ Allow duplicate name

If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a four-digit incremental number to the end of each ECS name. For e name ecs-0010 already exists, the name of the first new ECS will be ecs-0011.

Login Mode: Key pair | **Password** | Set password later

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.
••••••••••

Confirm Password: ••••••••••

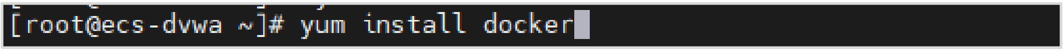
Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.
Create new | Use existing | **Not required**
CBR backups can help you restore data in case anything happens to your ECS. To ensure data security, you are advised to use CBR.

ECS Group (Optional): **Anti-affinity**
--Select ECS group-- ▾
Create ECS Group

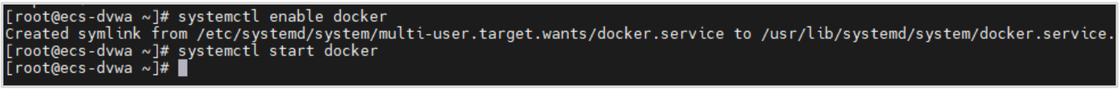
Figure 5-15

Step 11 Log in to the ECS and install Docker.

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



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

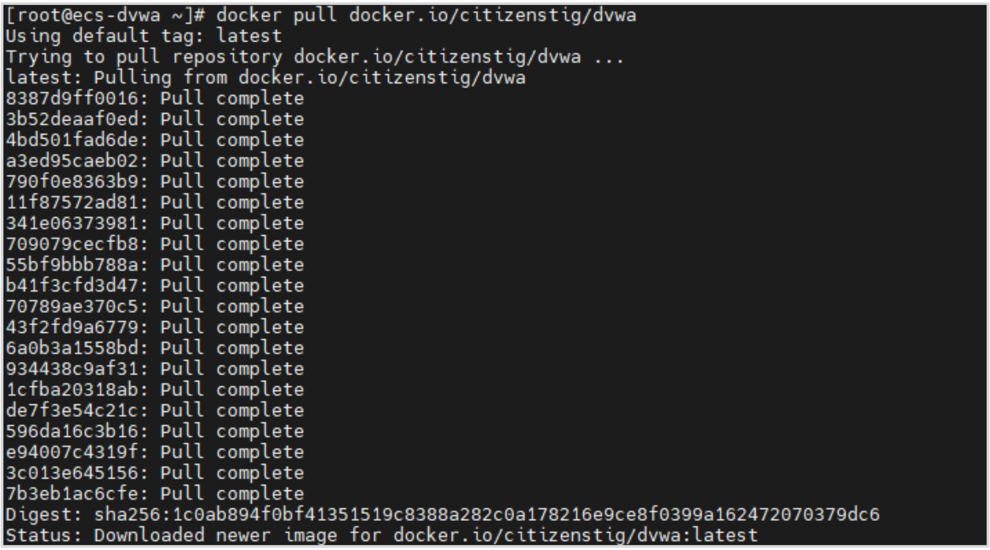


```
[root@ecs-dvwa ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multi-user.target.wants/docker.service to /usr/lib/systemd/system/docker.service.
[root@ecs-dvwa ~]# systemctl start docker
[root@ecs-dvwa ~]#
```

Figure 5-16

Step 12 Download the DVWA container image.

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

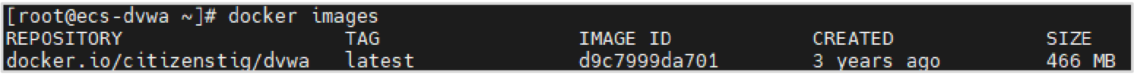


```
[root@ecs-dvwa ~]# docker pull docker.io/citizenstig/dvwa
Using default tag: latest
Trying to pull repository docker.io/citizenstig/dvwa ...
latest: Pulling from docker.io/citizenstig/dvwa
8387d9ff0016: Pull complete
3b52deaaf0ed: Pull complete
4bd501fad6de: Pull complete
a3ed95caeb02: Pull complete
790f0e8363b9: Pull complete
11f87572ad81: Pull complete
341e06373981: Pull complete
709079cecfb8: Pull complete
55bf9bbb788a: Pull complete
b41f3cfd3d47: Pull complete
70789ae370c5: Pull complete
43f2fd9a6779: Pull complete
6a0b3a1558bd: Pull complete
934438c9af31: Pull complete
1cfba20318ab: Pull complete
de7f3e54c21c: Pull complete
596da16c3b16: Pull complete
e94007c4319f: Pull complete
3c013e645156: Pull complete
7b3eb1ac6cfe: Pull complete
Digest: sha256:1c0ab894f0bf41351519c8388a282c0a178216e9ce8f0399a162472070379dc6
Status: Downloaded newer image for docker.io/citizenstig/dvwa:latest
```

Figure 5-17

Step 13 View the current image.

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

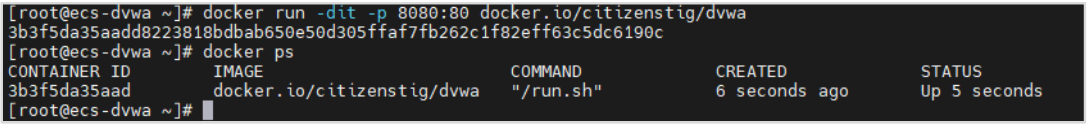


```
[root@ecs-dvwa ~]# docker images
REPOSITORY                  TAG                 IMAGE ID            CREATED             SIZE
docker.io/citizenstig/dvwa   latest              d9c7999da701        3 years ago         466 MB
```

Figure 5-18

Step 14 Run the image as a container and map the container service port 80 to port 8080.

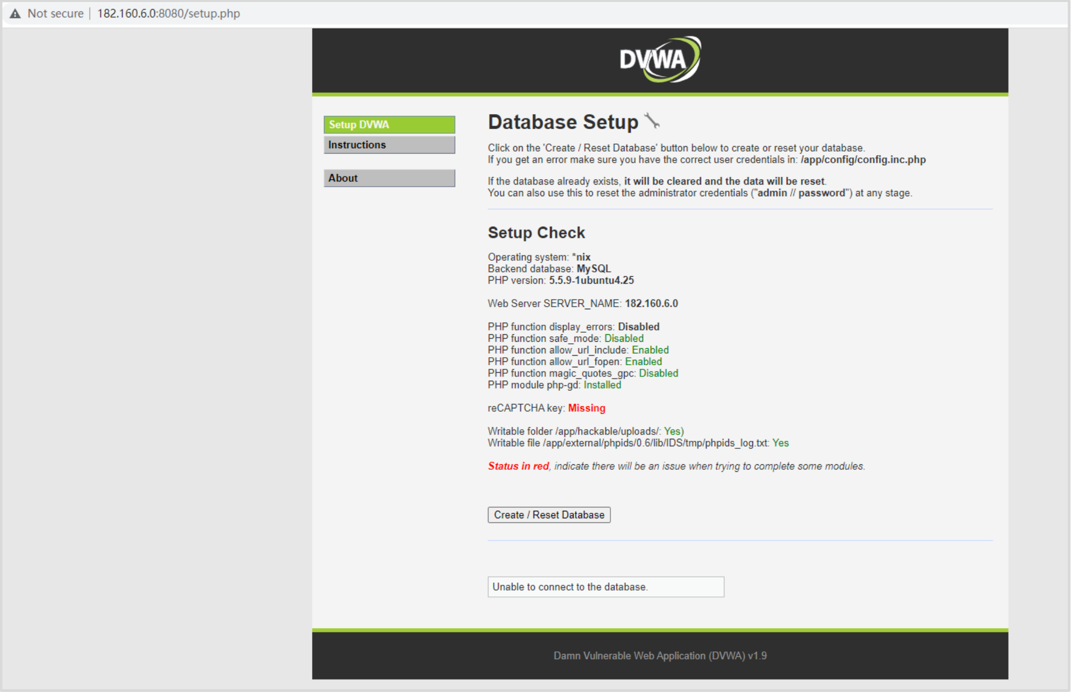
```
[root@ecs-dvwa ~]# docker run -dit -p 8080:80 docker.io/citizenstig/dvwa
3b3f5da35aadd8223818bdbab650e50d305ffaf7fb262c1f82eff63c5dc6190c
[root@ecs-dvwa ~]# docker ps
```



```
[root@ecs-dvwa ~]# docker run -dit -p 8080:80 docker.io/citizenstig/dvwa
3b3f5da35aadd8223818bdbab650e50d305ffaf7fb262c1f82eff63c5dc6190c
[root@ecs-dvwa ~]# docker ps
CONTAINER ID        IMAGE                        COMMAND             CREATED             STATUS
3b3f5da35aad        docker.io/citizenstig/dvwa   "/run.sh"           6 seconds ago       Up 5 seconds
[root@ecs-dvwa ~]#
```

Figure 5-19

Step 15 Open a local browser, enter *http://182.160.6.0:8080* in the address bar to open the DVWA web page and click **Create/Reset Database**. (182.160.6.0 is the EIP bound to the ECS **ecs-dvwa**.)



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/app/config/config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Operating system: ***nix**
Backend database: **MySQL**
PHP version: **5.5.9-1ubuntu4.25**

Web Server SERVER_NAME: **182.160.6.0**

PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module php-gd: Installed

reCAPTCHA key: **Missing**

Writable folder /app/hackable/uploads/: Yes)
Writable file /app/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes

Status in red*, indicate there will be an issue when trying to complete some modules.*

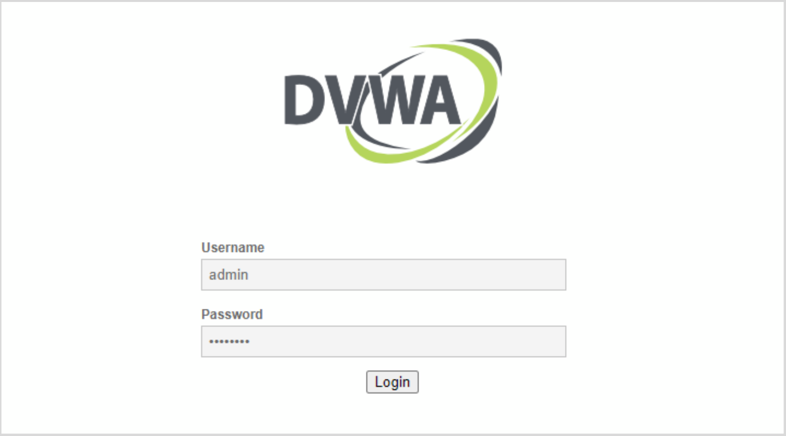
Unable to connect to the database.

Damn Vulnerable Web Application (DVWA) v1.9

Figure 5-20

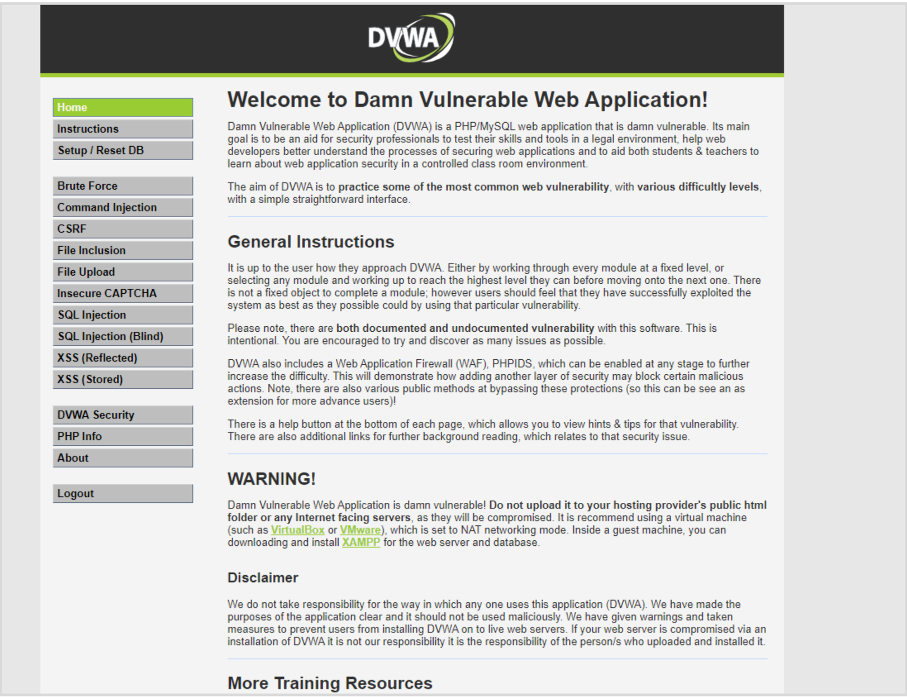
Step 16 After the initialization is complete, the login page is displayed. Enter the username and password for logging in to DVWA. If the following information is displayed, the DVWA host is successfully deployed.

Note: The user name is **admin** and the password is **password**.



Username: admin

Password: ••••••••



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerability**, with **various difficultly levels**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be see an as extension for more advance users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can downloading and install XAMPP for the web server and database.

Disclaimer

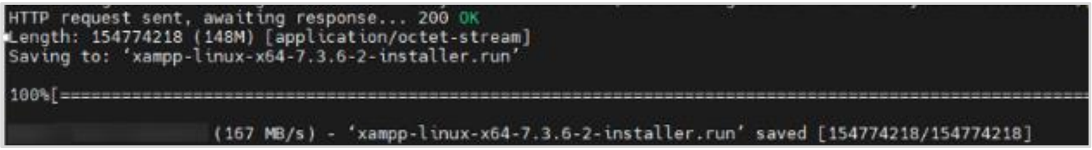
We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

Figure 5-21

Step 17 Log in to the ECS and download XAMPP.

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



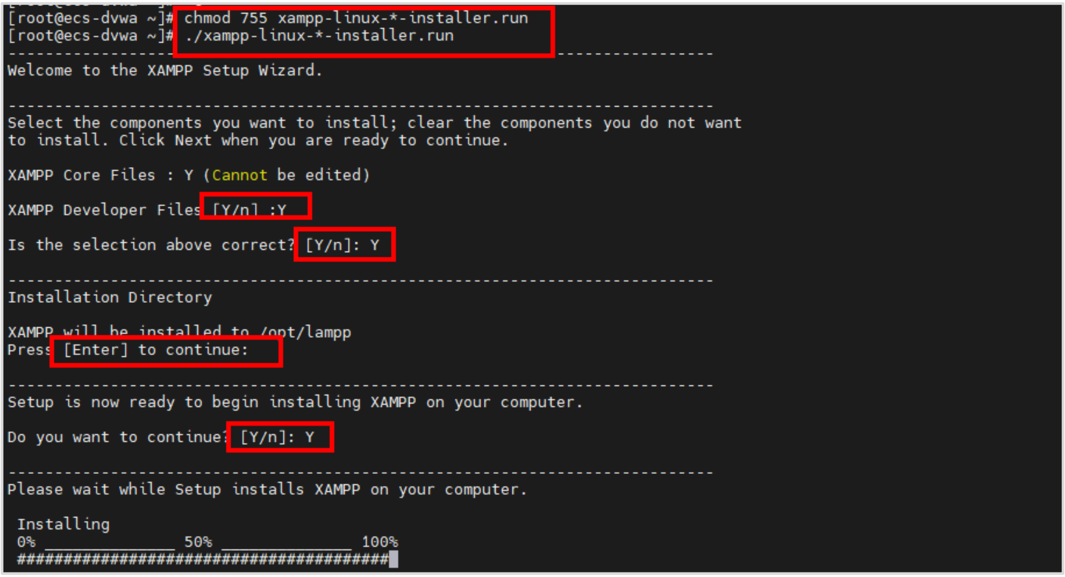
```
HTTP request sent, awaiting response... 200 OK
Length: 154774218 (148M) [application/octet-stream]
Saving to: 'xampp-linux-x64-7.3.6-2-installer.run'

100%[==========================================================================================

[redacted] (167 MB/s) - 'xampp-linux-x64-7.3.6-2-installer.run' saved [154774218/154774218]
```

Figure 5-22

Modify permissions and install XAMPP.

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

Note: After running the command, perform operations as instructed in the following figure to complete the installation.

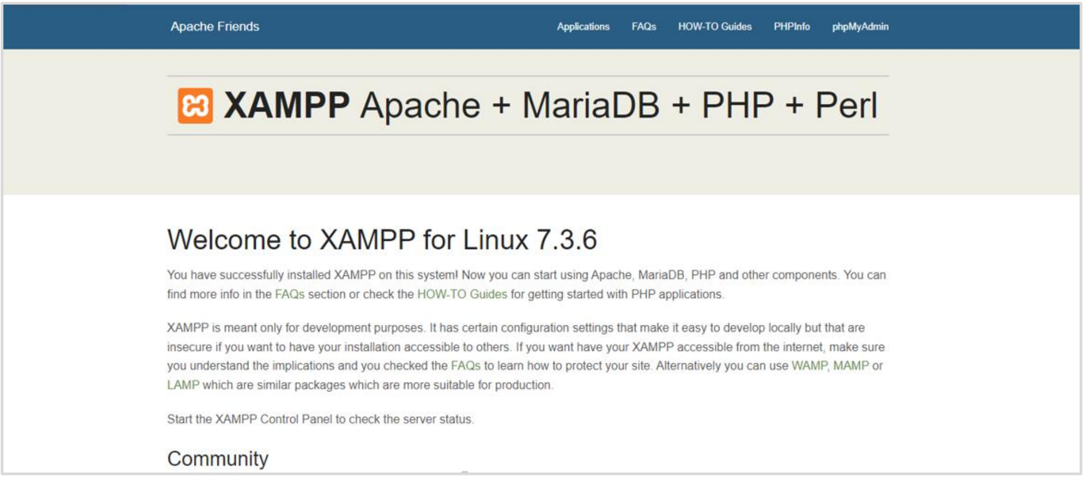


```
[root@ecs-dvwa ~]# chmod 755 xampp-linux-*-installer.run
[root@ecs-dvwa ~]# ./xampp-linux-*-installer.run
----------------------------------------------------------------------------
Welcome to the XAMPP Setup Wizard.

----------------------------------------------------------------------------
Select the components you want to install; clear the components you do not want
to install. Click Next when you are ready to continue.

XAMPP Core Files : Y (Cannot be edited)

XAMPP Developer Files [Y/n] :Y

Is the selection above correct? [Y/n]: Y

----------------------------------------------------------------------------
Installation Directory

XAMPP will be installed to /opt/lampp
Press [Enter] to continue:

----------------------------------------------------------------------------
Setup is now ready to begin installing XAMPP on your computer.

Do you want to continue? [Y/n]: Y

----------------------------------------------------------------------------
Please wait while Setup installs XAMPP on your computer.

 Installing
 0% ______________ 50% ______________ 100%
 ########################################
```

Figure 5-23

Step 18 In the local browser, enter http://182.160.6.0 in the address bar. If you can access XAMPP, the installation is successful.

Note: In this exercise, 182.160.6.0 is the EIP bound to the ECS **ecs-dvwa**. Replace it with the actual value.



XAMPP Apache + MariaDB + PHP + Perl

Welcome to XAMPP for Linux 7.3.6

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure you understand the implications and you checked the FAQs to learn how to protect your site. Alternatively you can use WAMP, MAMP or LAMP which are similar packages which are more suitable for production.

Start the XAMPP Control Panel to check the server status.

Community

Figure 5-24

5.2.2 Enabling HSS

Step 1 On the **Service List** page, select **Host Security Service** under **Security & Compliance**.

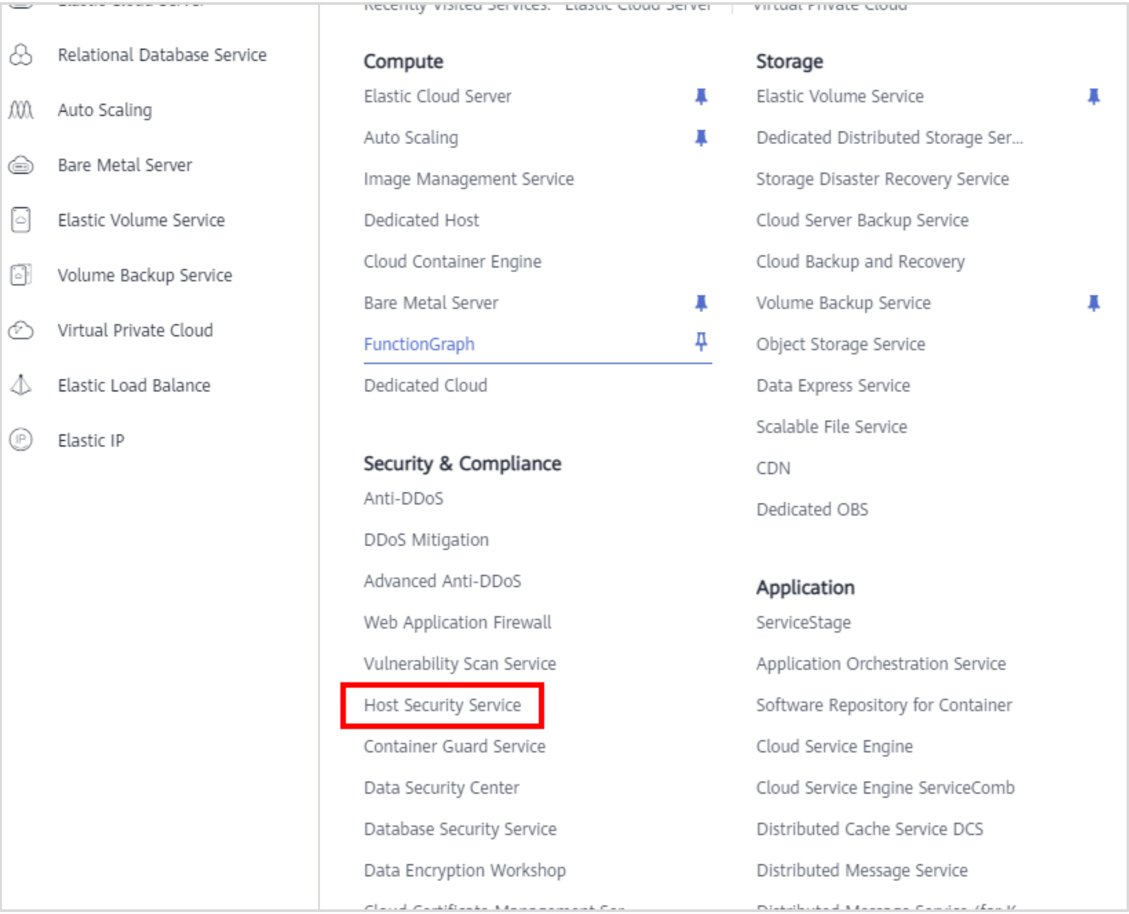


Figure 5-25

Step 2 Click **Buy HSS** in the upper right corner.

Notes: HSS provides asset management, vulnerability management, baseline check, intrusion detection, application recognition service (ARS), file integrity check, secure operations, and web tamper protection functions, helping you identify and manage data assets on your servers, scan for risks in real time, and block intrusions.

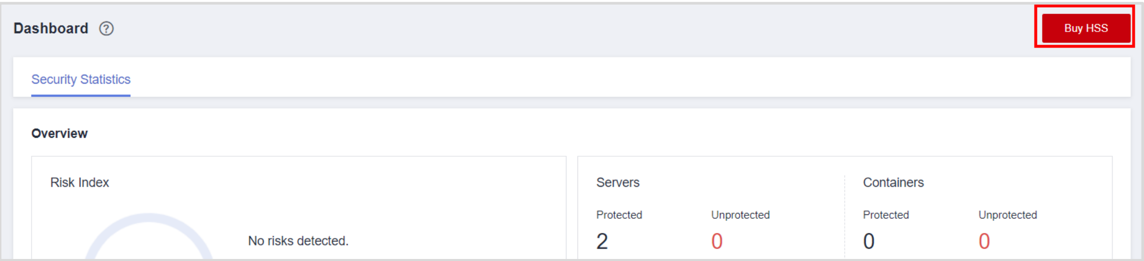
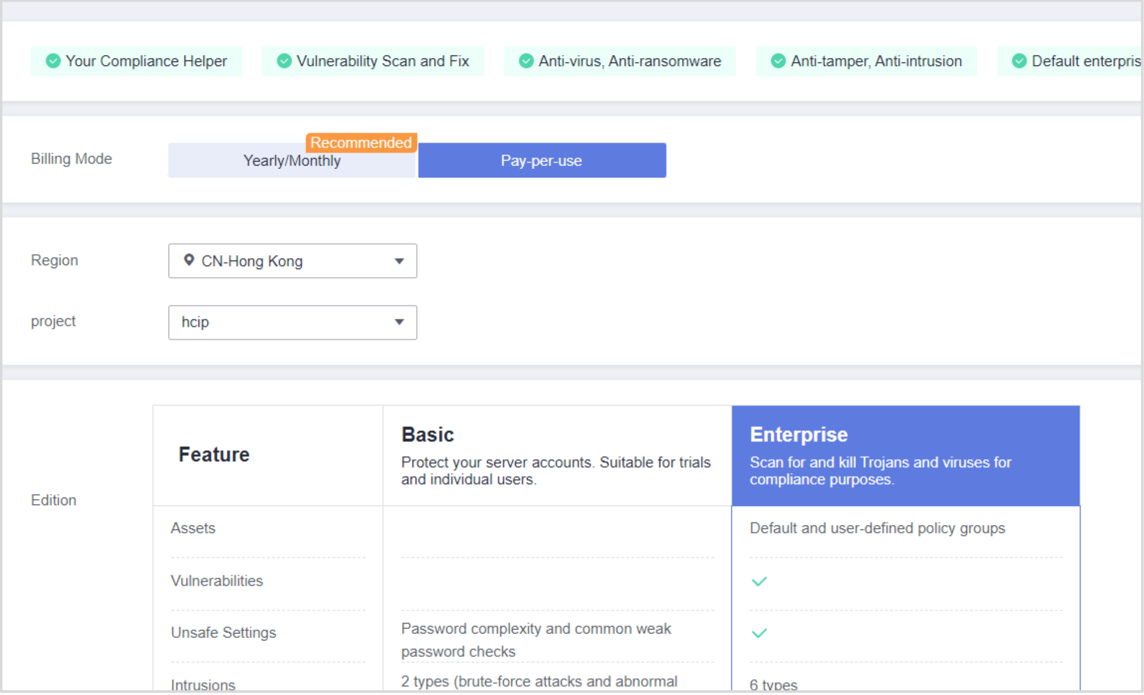


Figure 5-26

Step 3 Configure HSS parameters, as shown in the following figure. Click **Pay Now**.

- Billing mode: Pay-per-use
- **Region: Hong Kong**
- **Edition: Enterprise**



✓ Your Compliance Helper ✓ Vulnerability Scan and Fix ✓ Anti-virus, Anti-ransomware ✓ Anti-tamper, Anti-intrusion ✓ Default enterpris

Billing Mode: Yearly/Monthly (Recommended) | Pay-per-use

Region: CN-Hong Kong

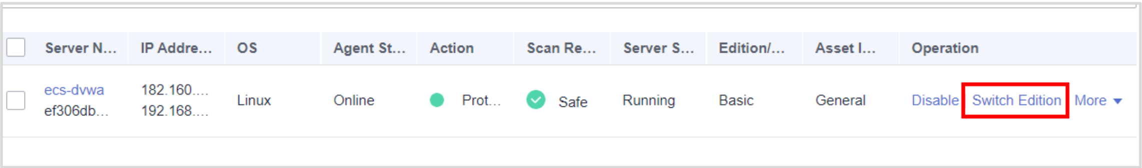
project: hcip

Edition

Feature	Basic Protect your server accounts. Suitable for trials and individual users.	Enterprise Scan for and kill Trojans and viruses for compliance purposes.
Assets		Default and user-defined policy groups
Vulnerabilities		✓
Unsafe Settings	Password complexity and common weak password checks	✓
Intrusions	2 types (brute-force attacks and abnormal	6 types

Figure 5-27

Step 4 After you are directed to the server list, click **Switch Edition**.



□	Server N...	IP Addre...	OS	Agent St...	Action	Scan Re...	Server S...	Edition/...	Asset I...	Operation
□	ecs-dvwa ef306db...	182.160.... 192.168....	Linux	Online	● Prot...	✓ Safe	Running	Basic	General	Disable Switch Edition More ▾

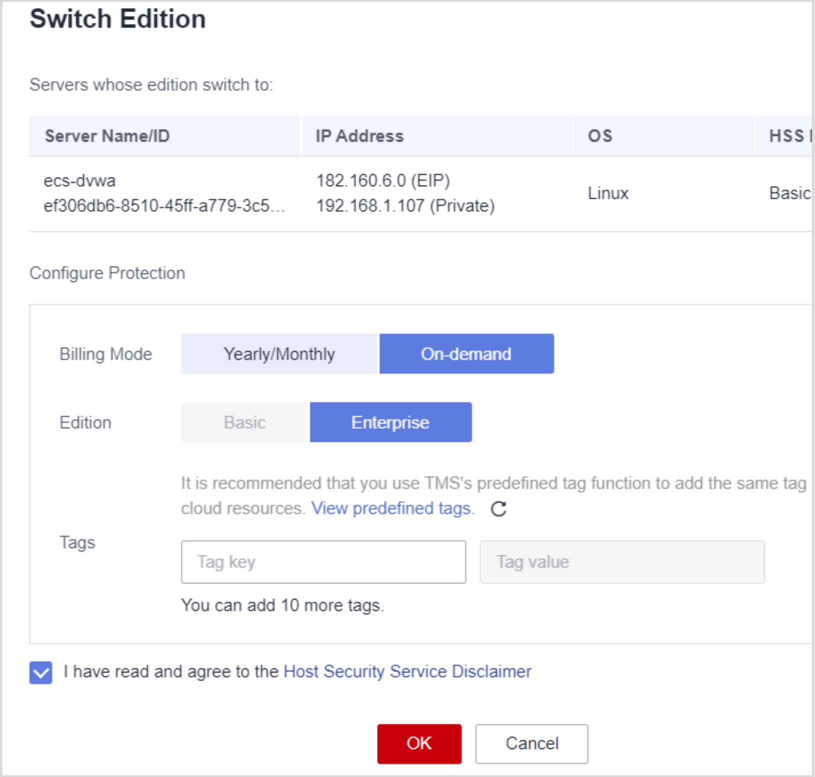
Figure 5-28

Step 5 Configure edition parameters, as shown in the following figure. Read the disclaimer, select **I have read and agree to the Host Security Service Disclaimer**, and click **OK**.

Note: The basic edition is free of charge and provides only part of HSS functions. It does not provide protection capabilities or support for DJCP MLPS compliance.

The enterprise edition supports DJCP MLPS L2 compliance, virus and Trojan scan and removal, one-click vulnerability fix, and intrusion detection.

- **Billing Mode: On-demand**
- **Edition: Enterprise**



Switch Edition

Servers whose edition switch to:

Server Name/ID	IP Address	OS	HSS I
ecs-dvwa ef306db6-8510-45ff-a779-3c5…	182.160.6.0 (EIP) 192.168.1.107 (Private)	Linux	Basic

Configure Protection

Billing Mode: Yearly/Monthly | **On-demand**

Edition: Basic | **Enterprise**

Tags: It is recommended that you use TMS's predefined tag function to add the same tag cloud resources. View predefined tags.

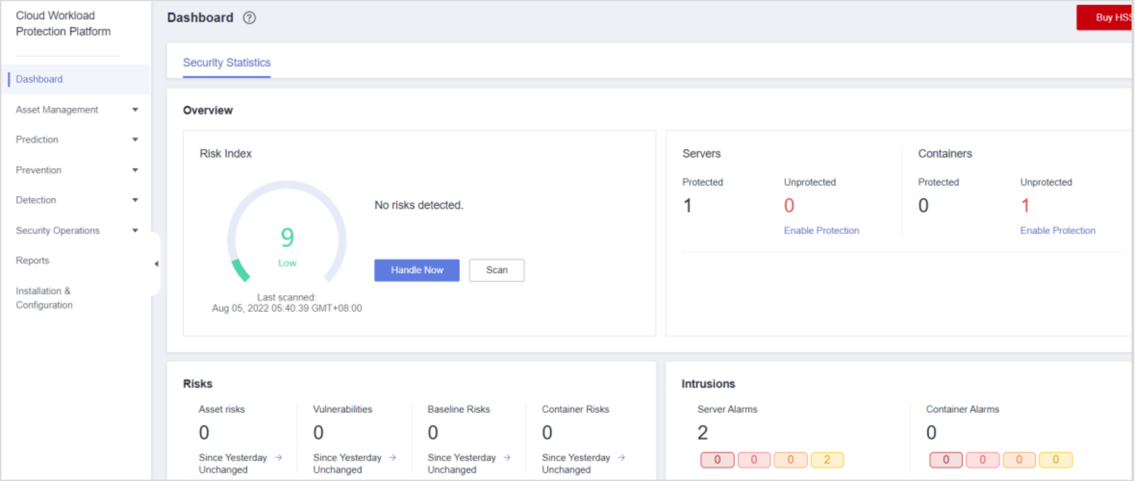
Tag key | Tag value

You can add 10 more tags.

☑ I have read and agree to the Host Security Service Disclaimer

Figure 5-29

Step 6 Return to the Host Security Service home page. Click **Dashboard** to check the server risk and protection statistics.



Dashboard

Security Statistics

Overview

Risk Index: 9 Low

No risks detected.

Last scanned: Aug 05, 2022 05:40:39 GMT+08:00

Servers: Protected 1; Unprotected 0 (Enable Protection)

Containers: Protected 0; Unprotected 1 (Enable Protection)

Risks

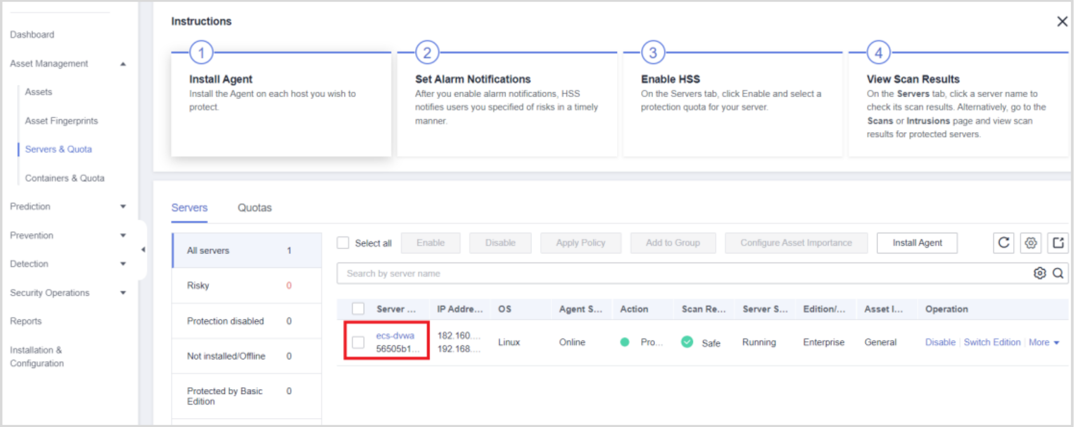
Asset risks	Vulnerabilities	Baseline Risks	Container Risks
0	0	0	0
Since Yesterday → Unchanged	Since Yesterday → Unchanged	Since Yesterday → Unchanged	Since Yesterday → Unchanged

Intrusions

Server Alarms	Container Alarms
2	0
0 0 0 2	0 0 0 0

Figure 5-30

Step 7 Click the **Asset Management > Servers & Quota** tab, click the server’s name.



Instructions

1 **Install Agent** Install the Agent on each host you wish to protect.

2 **Set Alarm Notifications** After you enable alarm notifications, HSS notifies users you specified of risks in a timely manner.

3 **Enable HSS** On the Servers tab, click Enable and select a protection quota for your server.

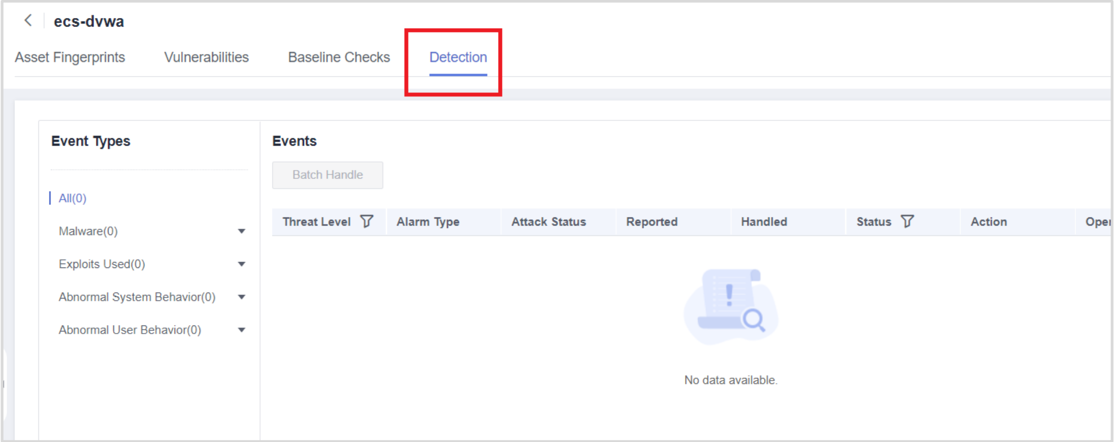
4 **View Scan Results** On the **Servers** tab, click a server name to check its scan results. Alternatively, go to the **Scans** or **Intrusions** page and view scan results for protected servers.

All servers	1
Risky	0
Protection disabled	0
Not installed/Offline	0
Protected by Basic Edition	0

Server ...	IP Addre...	OS	Agent S...	Action	Scan Re...	Server S...	Edition/...	Asset I...	Operation
ecs-dvwa 56505b1...	182.160.... 192.168....	Linux	Online	● Pro...	✓ Safe	Running	Enterprise	General	Disable | Switch Edition | More ▾

Figure 5-31

Step 8 Click the **Intrusions** tab and check intrusions.



Event Types

- All(0)
- Malware(0)
- Exploits Used(0)
- Abnormal System Behavior(0)
- Abnormal User Behavior(0)

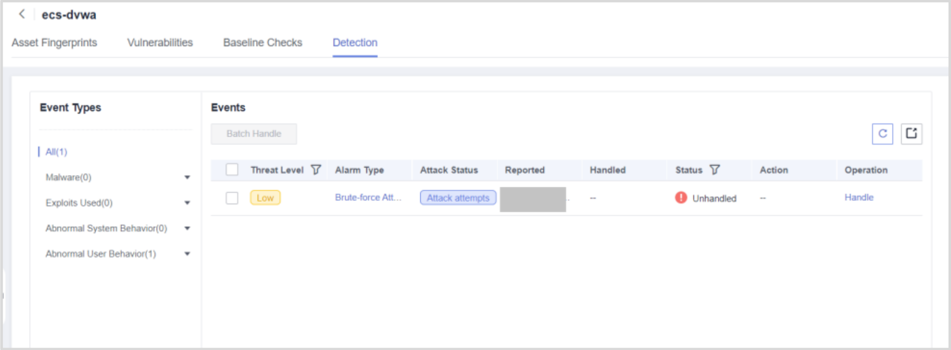
Events

Threat Level	Alarm Type	Attack Status	Reported	Handled	Status	Action	Oper

No data available.

Note: The HSS the enterprise edition provides the intrusion detection function. It can identify and block intrusions in real time, detect internal risks, and detect and remove malicious programs.

You can log in to the ECS by tools like PUTTY but keep entering incorrect passwords to simulate brute force attack.Then Haddle it by **Add to Login Whitelist.**

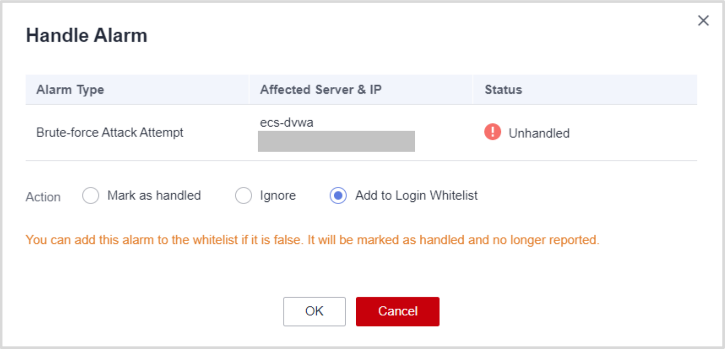


Event Types

- All(1)
- Malware(0)
- Exploits Used(0)
- Abnormal System Behavior(0)
- Abnormal User Behavior(1)

Events

□	Threat Level	Alarm Type	Attack Status	Reported	Handled	Status	Action	Operation
□	Low	Brute-force Att...	Attack attempts	[redacted]	--	● Unhandled	--	Handle



Handle Alarm

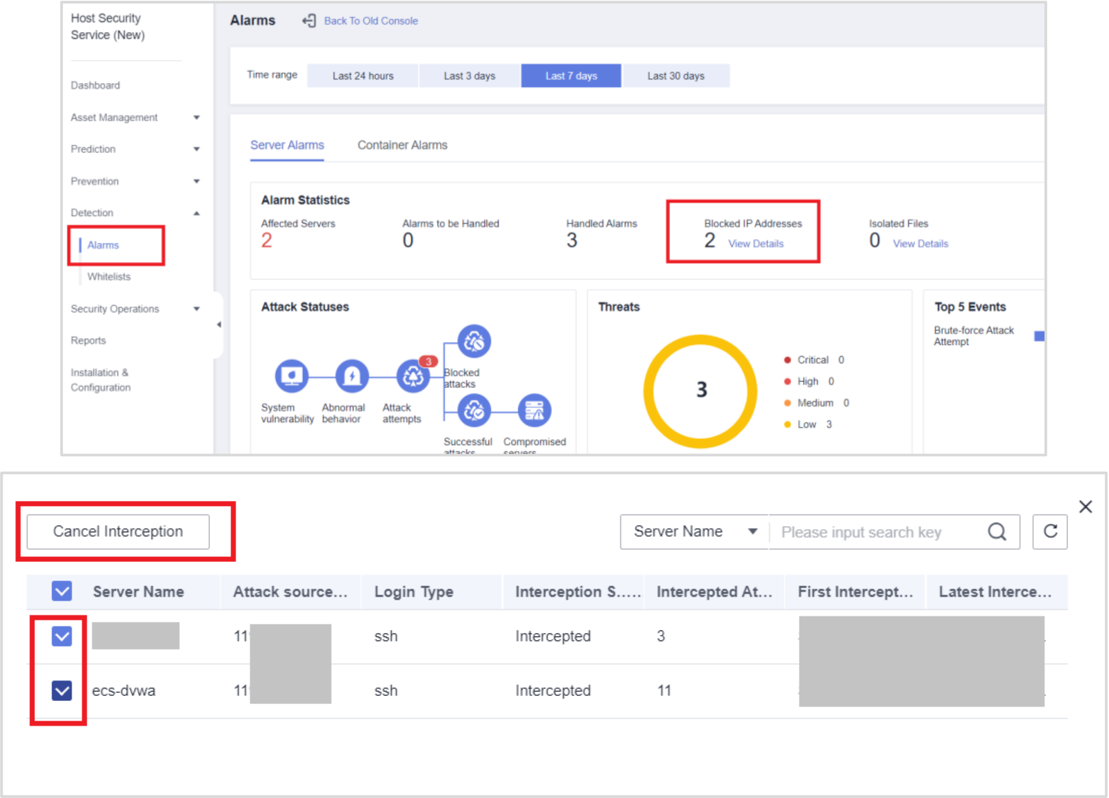
Alarm Type	Affected Server & IP	Status
Brute-force Attack Attempt	ecs-dvwa [redacted]	Unhandled

Action ○ Mark as handled ○ Ignore ● Add to Login Whitelist

You can add this alarm to the whitelist if it is false. It will be marked as handled and no longer reported.

Figure 5-32

Step 9 Click the **Detection > Alarms** to view blocked IP addresses and click **cancel interception.**



Alarm Statistics

Affected Servers	Alarms to be Handled	Handled Alarms	Blocked IP Addresses	Isolated Files
2	0	3	2 View Details	0 View Details

☑	Server Name	Attack source...	Login Type	Interception S.....	Intercepted At...	First Intercept...	Latest Interce...
☑	[redacted]	11[redacted]	ssh	Intercepted	3	[redacted]	[redacted]
☑	ecs-dvwa	11[redacted]	ssh	Intercepted	11	[redacted]	[redacted]

Figure 5-33

5.2.3 Configuring Two-Factor Authentication

In practice, some service hosts or O&M hosts have high requirements on access security. Authentication based only on usernames and passwords is considered insecure. In this case, you can configure two-factor authentication to meet multi-dimensional authentication requirements for host login.

Step 1 Create topics and add subscriptions on the Simple Message Notification (SMN) console.

Note: The SMN configuration is used for subsequent two-factor authentication.

- On the **Service List** page, select **Simple Message Notification** under **Management & Governance**.

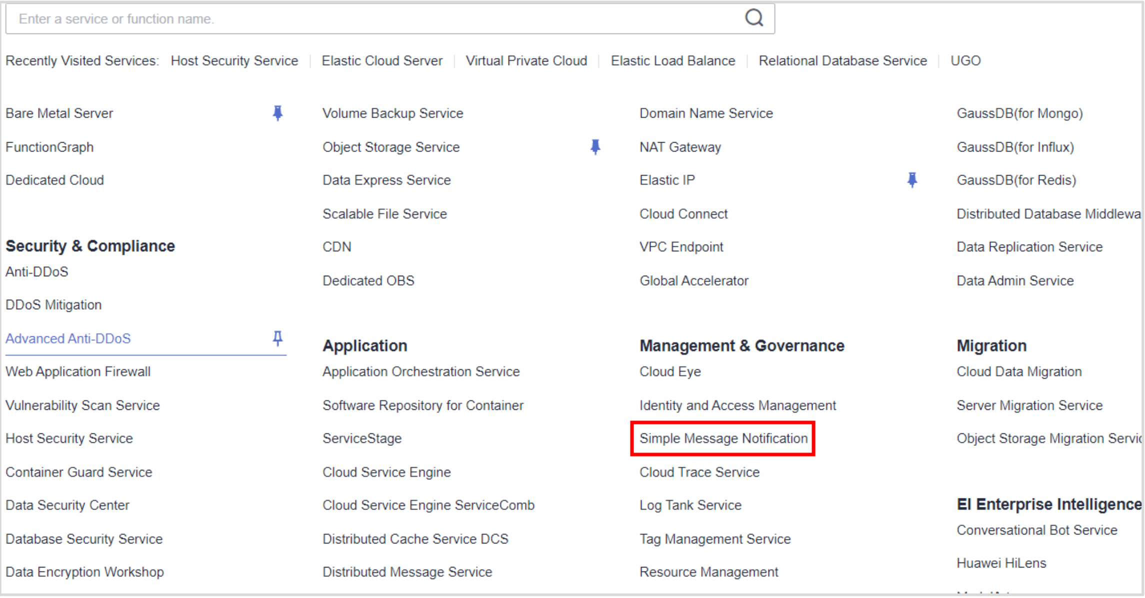


Figure 5-34

- On the **Dashboard** page, click **Topics** under **My Resources**.

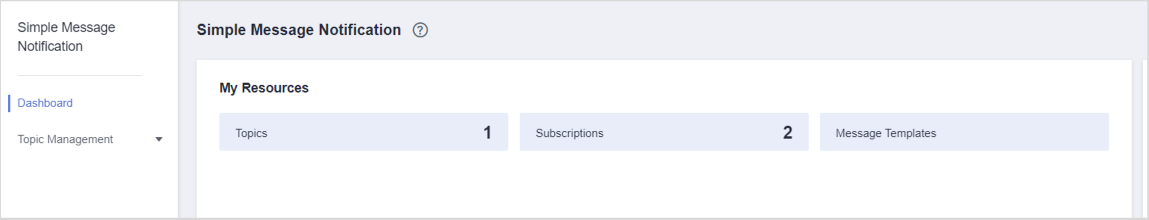
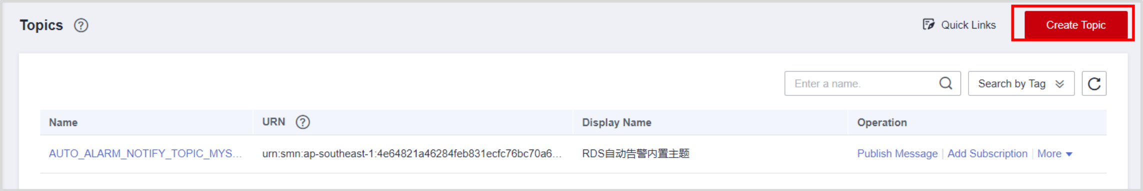


Figure 5-35

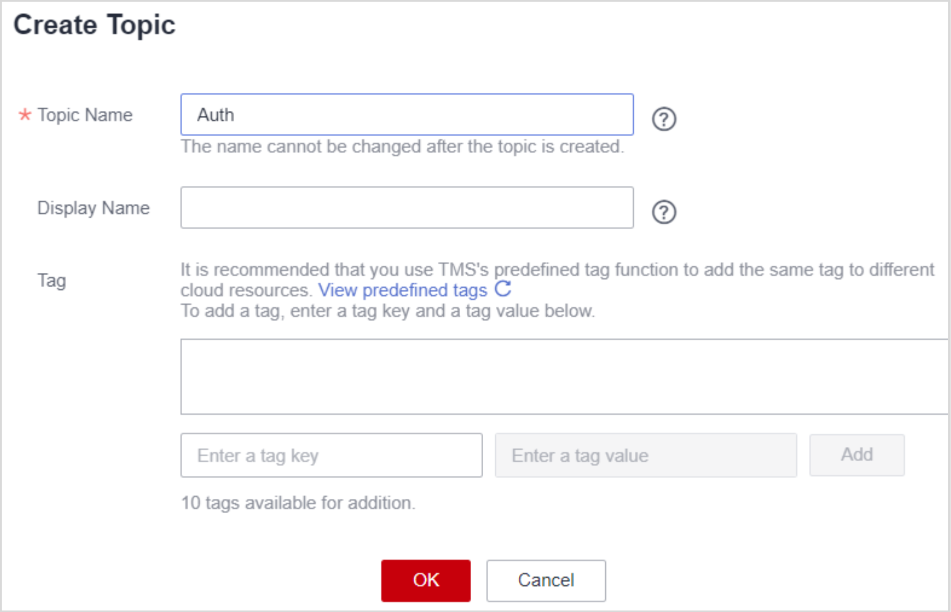
- In the upper right corner, click **Create Topic**.



Name	URN	Display Name	Operation
AUTO_ALARM_NOTIFY_TOPIC_MYS...	urn:smn:ap-southeast-1:4e64821a46284feb831ecfc76bc70a6...	RDS自动告警内置主题	Publish Message | Add Subscription | More

Figure 5-36

- Set **Topic Name** to **Auth** and click **OK**.

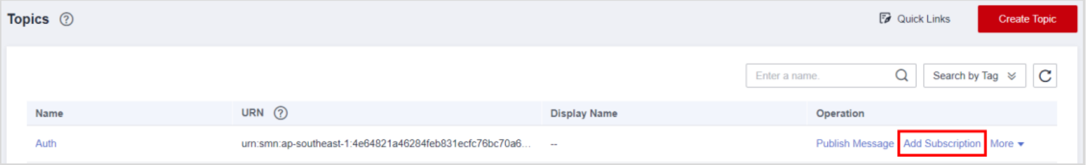


Create Topic

* Topic Name	Auth The name cannot be changed after the topic is created.
Display Name	
Tag	It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags To add a tag, enter a tag key and a tag value below. 10 tags available for addition.

Figure 5-37

- In the **Operation** column of the topic, click **Add Subscription**.



Topics

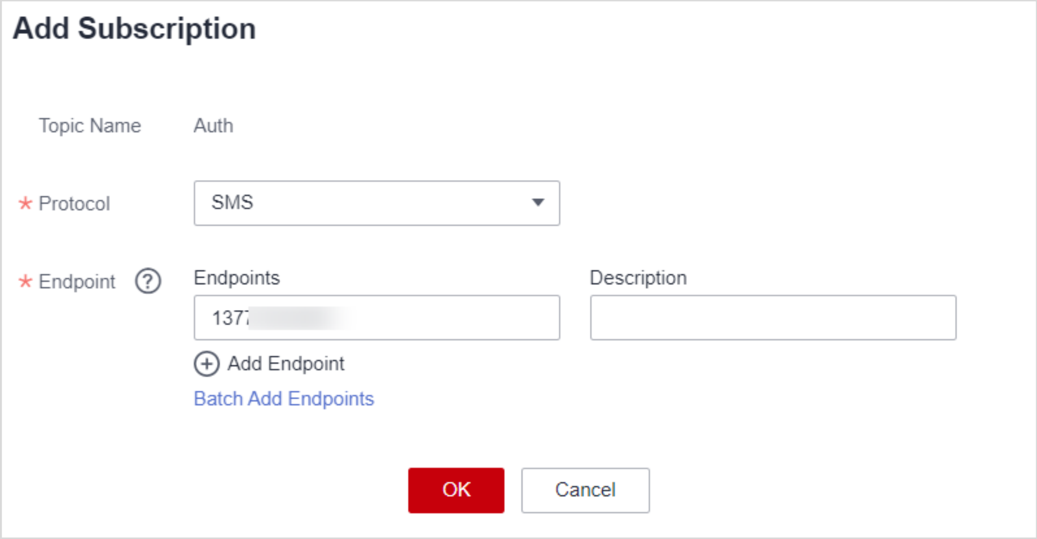
Name	URN	Display Name	Operation
Auth	urn:smn:ap-southeast-1:4e64821a46284feb831ecfc76bc70a6...	--	Publish Message Add Subscription More

Figure 5-38

- Configure the following parameters:

  Protocol: **SMS**

  Endpoint: personal mobile number (customized by trainees)



Add Subscription

Topic Name	Auth	
* Protocol	SMS	
* Endpoint	Endpoints	Description
	137[redacted]	

Figure 5-39

- Confirm the subscription on your mobile phone (SMS message) to make the subscription take effect.

Step 2 Create two-factor authentication.

- On the **Service List** page, select **Host Security Service** under **Security & Compliance**.

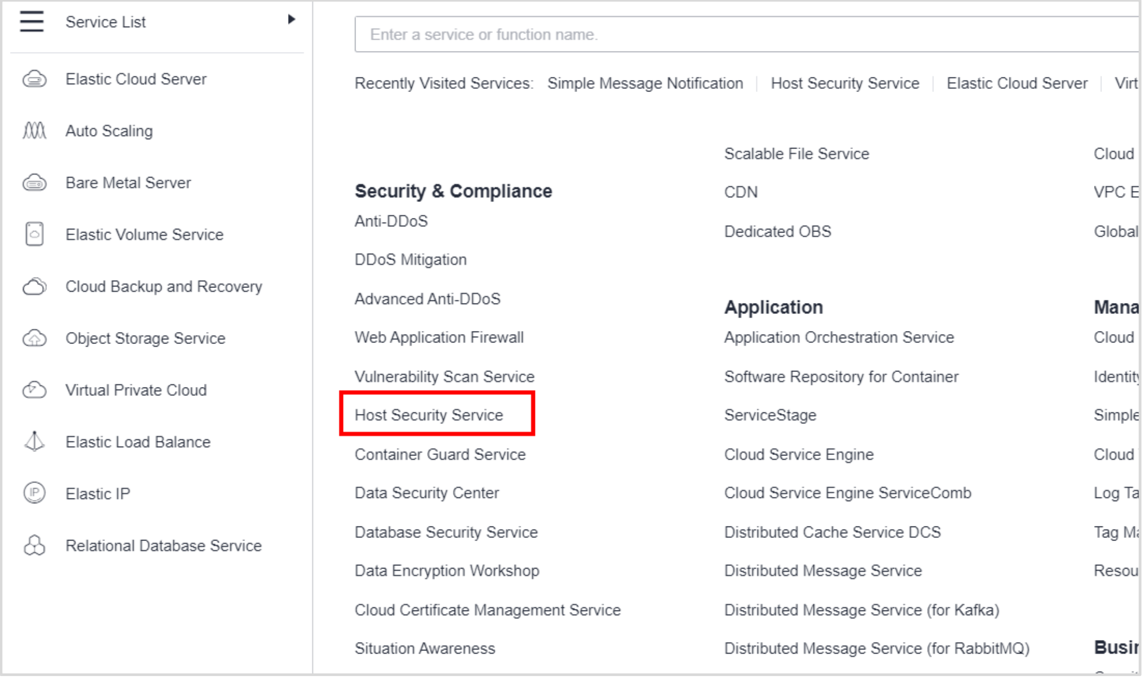
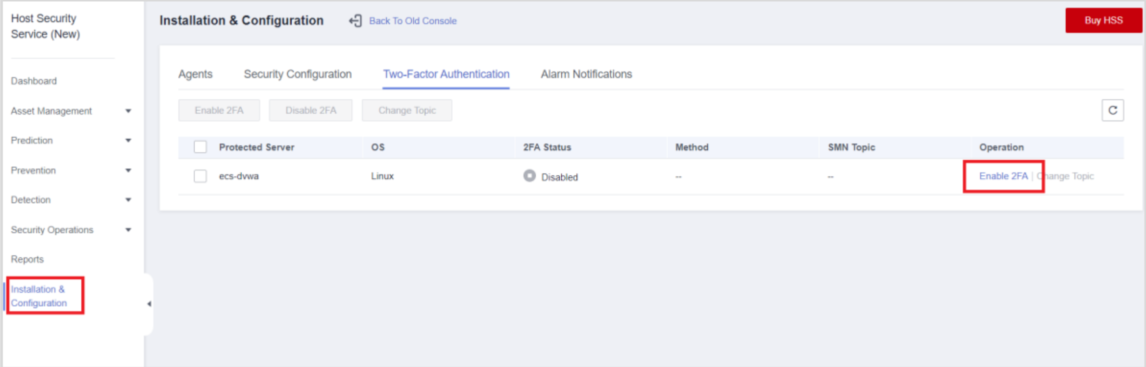

Service List
Elastic Cloud Server
Auto Scaling
Bare Metal Server
Elastic Volume Service
Cloud Backup and Recovery
Object Storage Service
Virtual Private Cloud
Elastic Load Balance
Elastic IP
Relational Database Service
Enter a service or function name.
Recently Visited Services: Simple Message Notification | Host Security Service | Elastic Cloud Server | Virt
Security & Compliance
Anti-DDoS
DDoS Mitigation
Advanced Anti-DDoS
Web Application Firewall
Vulnerability Scan Service
Host Security Service
Container Guard Service
Data Security Center
Database Security Service
Data Encryption Workshop
Cloud Certificate Management Service
Situation Awareness
Scalable File Service
CDN
Dedicated OBS
Application
Application Orchestration Service
Software Repository for Container
ServiceStage
Cloud Service Engine
Cloud Service Engine ServiceComb
Distributed Cache Service DCS
Distributed Message Service
Distributed Message Service (for Kafka)
Distributed Message Service (for RabbitMQ)
Cloud
VPC E
Global
Mana
Cloud
Identity
Simple
Cloud
Log Ta
Tag Ma
Resou
Busir

Figure 5-40

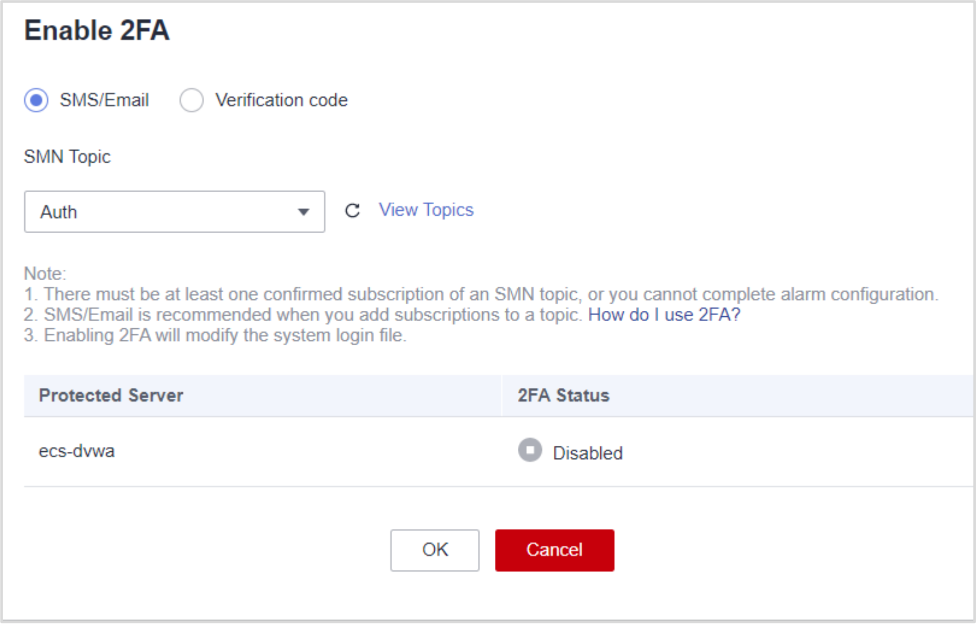
- On the displayed page, in the navigation pane on the left, choose **Installation & Configuration**. Choose the **Two-Factor Authentication** tab, locate the protected server, and click **Enable 2FA** in the **Operation** column.



Protected Server	OS	2FA Status	Method	SMN Topic	Operation
ecs-dvwa	Linux	○ Disabled	--	--	Enable 2FA | Change Topic

Figure 5-41

- Select the newly created SMN topic **Auth** and click **OK**.



Enable 2FA

● SMS/Email ○ Verification code

SMN Topic

Auth

View Topics

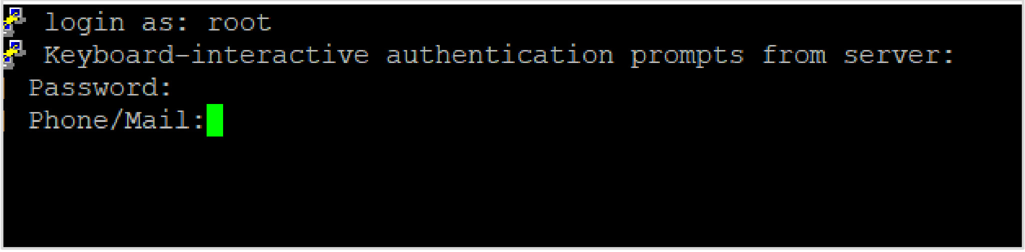
Note:
1. There must be at least one confirmed subscription of an SMN topic, or you cannot complete alarm configuration.
2. SMS/Email is recommended when you add subscriptions to a topic. How do I use 2FA?
3. Enabling 2FA will modify the system login file.

Protected Server	2FA Status
ecs-dvwa	Disabled

Figure 5-42

- Use PUTTY to Log in to the DVWA host.

Enter the username and password, enter the mobile number in the subscription, and enter the received SMS verification code to log in to the host. If the login is successful, the two-factor authentication configuration is successful. This section describes how to verify the basic functions and usage of two-factor authentication.

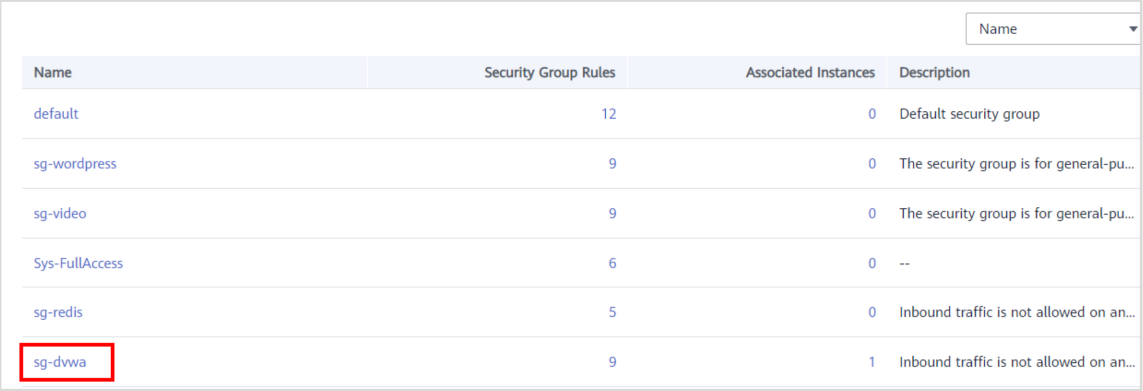


```
login as: root
Keyboard-interactive authentication prompts from server:
Password:
Phone/Mail:
```

Figure 5-43

5.2.4 Configuring a Security Group

Step 1 In the service list, choose **Networking** > **Virtual Private Cloud**. On the network console, choose **Access Control** > **Security Groups**. In the security group list, click the security group name **sg-dvwa**.



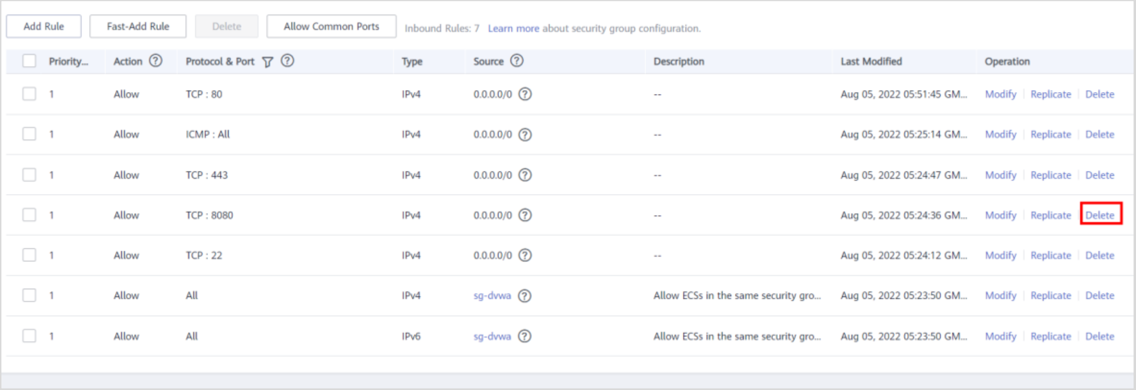
Name ▾

Name	Security Group Rules	Associated Instances	Description
default	12	0	Default security group
sg-wordpress	9	0	The security group is for general-pu...
sg-video	9	0	The security group is for general-pu...
Sys-FullAccess	6	0	--
sg-redis	5	0	Inbound traffic is not allowed on an...
sg-dvwa	9	1	Inbound traffic is not allowed on an...

Figure 5-44

Step 2 Click the **Inbound Rules** tab and delete the rule whose **Protocol & Port** is **TCP: 8080**.

Note: This rule is deleted to reject traffic on port 8080 and then we can verify the access control function of the security group.

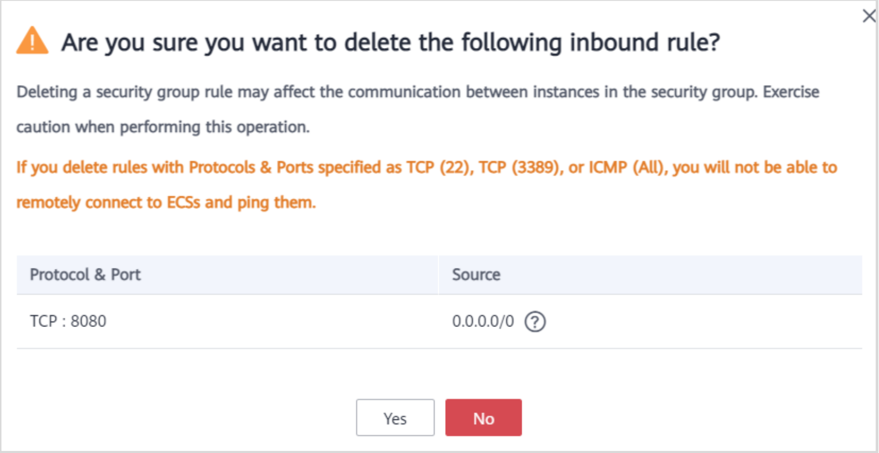


Inbound Rules: 7 Learn more about security group configuration.

□	Priority...	Action	Protocol & Port	Type	Source	Description	Last Modified	Operation
□	1	Allow	TCP : 80	IPv4	0.0.0.0/0	--	Aug 05, 2022 05:51:45 GM...	Modify | Replicate | Delete
□	1	Allow	ICMP : All	IPv4	0.0.0.0/0	--	Aug 05, 2022 05:25:14 GM...	Modify | Replicate | Delete
□	1	Allow	TCP : 443	IPv4	0.0.0.0/0	--	Aug 05, 2022 05:24:47 GM...	Modify | Replicate | Delete
□	1	Allow	TCP : 8080	IPv4	0.0.0.0/0	--	Aug 05, 2022 05:24:36 GM...	Modify | Replicate | Delete
□	1	Allow	TCP : 22	IPv4	0.0.0.0/0	--	Aug 05, 2022 05:24:12 GM...	Modify | Replicate | Delete
□	1	Allow	All	IPv4	sg-dvwa	Allow ECSs in the same security gro...	Aug 05, 2022 05:23:50 GM...	Modify | Replicate | Delete
□	1	Allow	All	IPv6	sg-dvwa	Allow ECSs in the same security gro...	Aug 05, 2022 05:23:50 GM...	Modify | Replicate | Delete

Figure 5-45

Step 3 In the displayed dialog box, click **Yes**.



Are you sure you want to delete the following inbound rule?

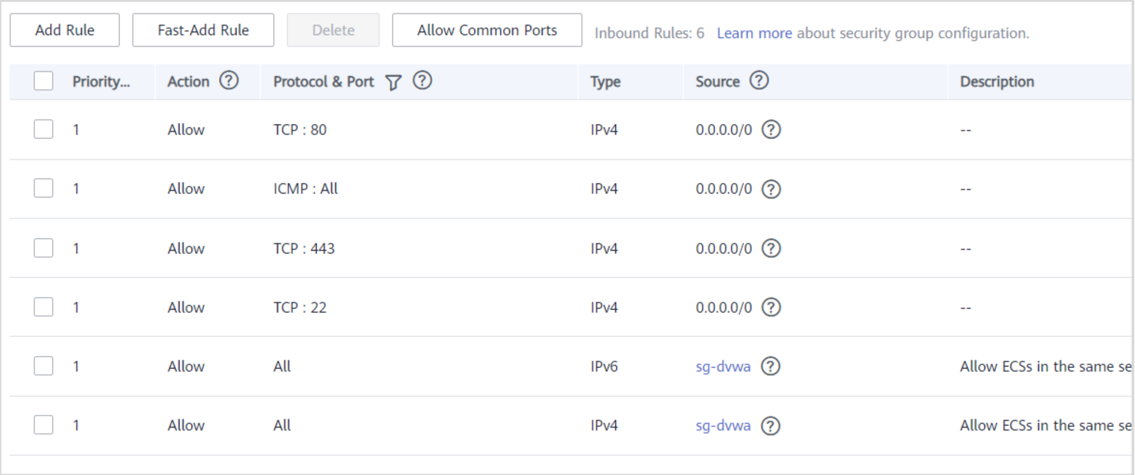
Deleting a security group rule may affect the communication between instances in the security group. Exercise caution when performing this operation.

If you delete rules with Protocols & Ports specified as TCP (22), TCP (3389), or ICMP (All), you will not be able to remotely connect to ECSs and ping them.

Protocol & Port	Source
TCP : 8080	0.0.0.0/0

Figure 5-46

Step 4 Check the inbound rule list. The rule that allows traffic on port 8080 does not exist.

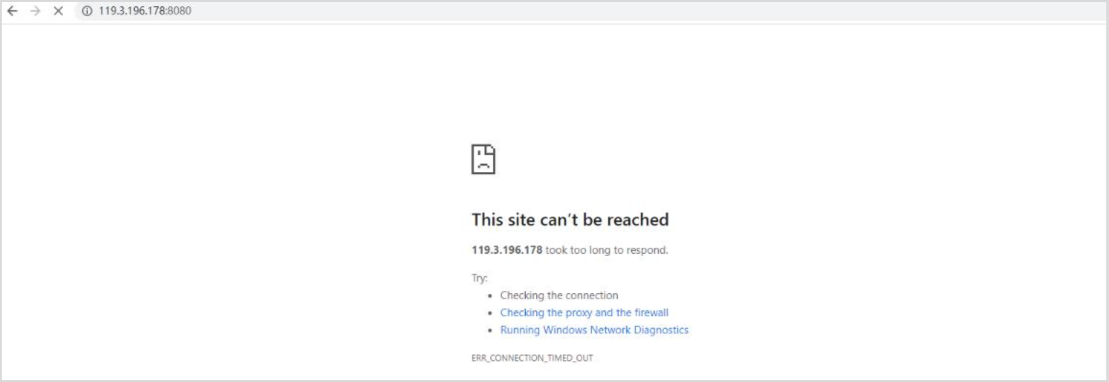


Inbound Rules: 6 Learn more about security group configuration.

Priority...	Action	Protocol & Port	Type	Source	Description
1	Allow	TCP : 80	IPv4	0.0.0.0/0	--
1	Allow	ICMP : All	IPv4	0.0.0.0/0	--
1	Allow	TCP : 443	IPv4	0.0.0.0/0	--
1	Allow	TCP : 22	IPv4	0.0.0.0/0	--
1	Allow	All	IPv6	sg-dvwa	Allow ECSs in the same se
1	Allow	All	IPv4	sg-dvwa	Allow ECSs in the same se

Figure 5-47

Step 5 Visit http://119.3.196.178 (EIP address of the DVWA ECS):8080. Refresh the page and find that the login fails. This indicates that the security group **sg-dvwa** blocks traffic on port 8080.



This site can't be reached

119.3.196.178 took too long to respond.

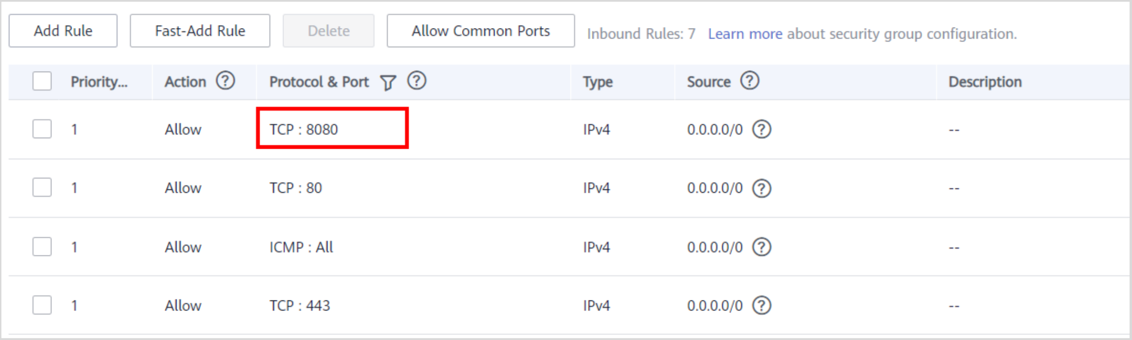
Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Figure 5-48

Step 6 Add an inbound rule to allow traffic on port 8080 again.

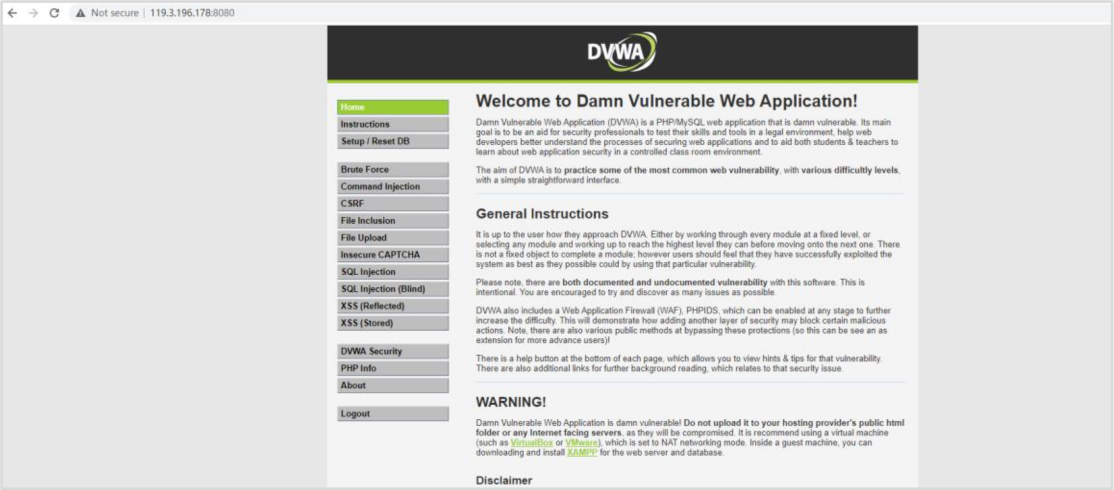


Inbound Rules: 7 Learn more about security group configuration.

Priority...	Action	Protocol & Port	Type	Source	Description
1	Allow	TCP : 8080	IPv4	0.0.0.0/0	--
1	Allow	TCP : 80	IPv4	0.0.0.0/0	--
1	Allow	ICMP : All	IPv4	0.0.0.0/0	--
1	Allow	TCP : 443	IPv4	0.0.0.0/0	--

Figure 5-49

Step 7 Refresh the page. The login is successful. This indicates that the security group **sg-dvwa** allows traffic on port 8080. The above operations exercise the basic functions of security groups.



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerability**, with **various difficultly levels**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be see an as extension for more advance users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can downloading and install XAMPP for the web server and database.

Disclaimer

Figure 5-50

5.2.5 Configuring an IP Address Group

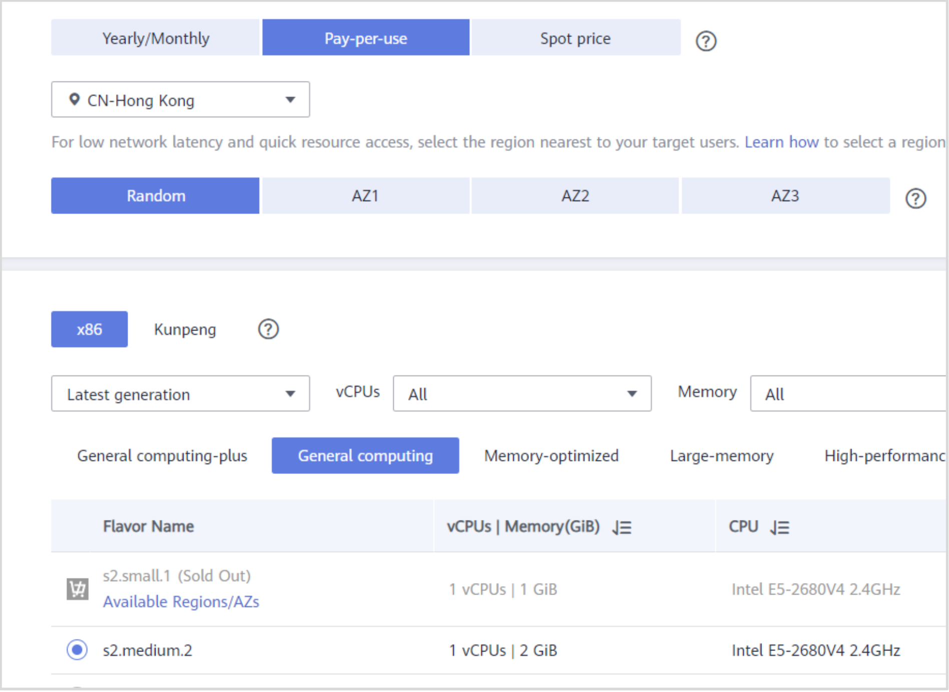
If multiple IP addresses can use the same security group, you can add these IP addresses to an IP address group.

Step 1 Create a test ECS in the VPC subnet created in **错误!未找到引用源。** in "DVWA Deployment".

Note: This ECS is used only for connectivity test and verification and is not used for application deployment.

Configure the ECS **test** as follows:

- **Billing Mode**: **Pay-per-use**
- **Region**: **CN-Hong Kong**
- **AZ**: **Random**
- **CPU Architecture**: **x86**
- **Specifications**: **1 vCPUs | 2 GiB**
- **Image**: **Public image** | **CentOS 7.6 64bit(40GB)**
- **Host Security**: **Enable** | **Basic (free)**
- **Network**: **vpc-1** | **subnet-20** | **Automatically assign IP address** (Same network configuration as **ecs-dvwa**)
- **Security Group**: **default** (Select a security group different from that of **ecs-dvwa**.)
- **EIP**: **Not required**
- **System Disk**: **High I/O** | **40 GiB**
- **ECS Name**: **test**
- **Password**: User-defined (with the username of **root**)



Yearly/Monthly | Pay-per-use | Spot price

CN-Hong Kong

For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region

Random | AZ1 | AZ2 | AZ3

x86 | Kunpeng

Latest generation vCPUs All Memory All

General computing-plus | General computing | Memory-optimized | Large-memory | High-performanc

	Flavor Name	vCPUs | Memory(GiB)	CPU
	s2.small.1 (Sold Out) Available Regions/AZs	1 vCPUs | 1 GiB	Intel E5-2680V4 2.4GHz
●	s2.medium.2	1 vCPUs | 2 GiB	Intel E5-2680V4 2.4GHz

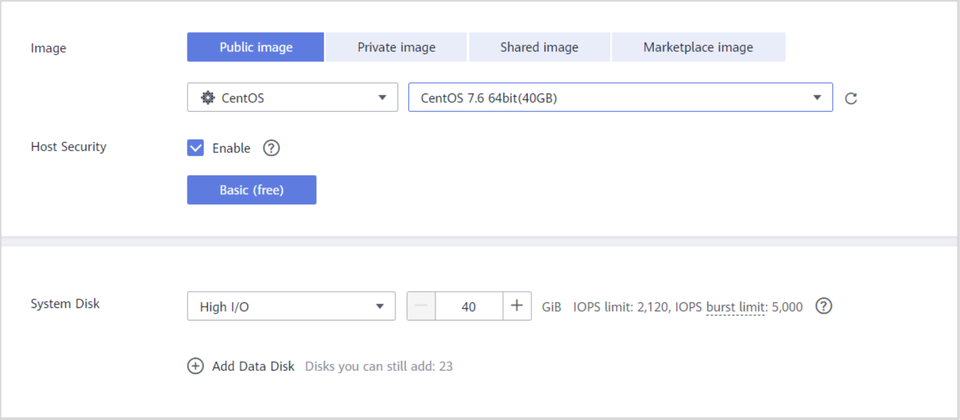


Image: Public image | Private image | Shared image | Marketplace image

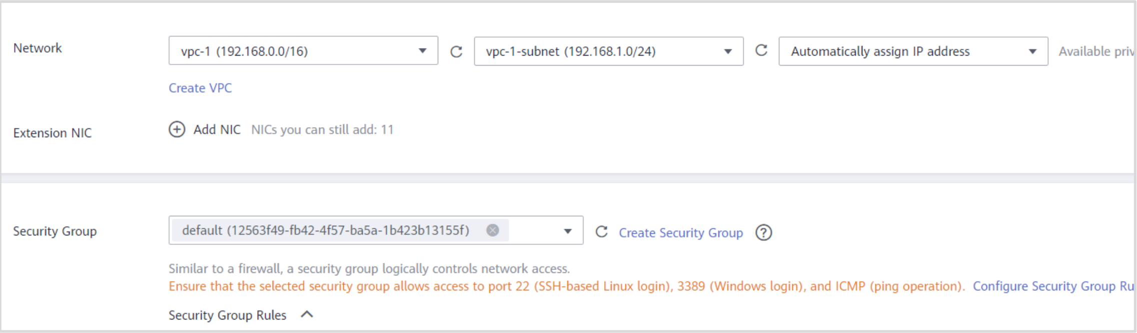
CentOS | CentOS 7.6 64bit(40GB)

Host Security: ☑ Enable

Basic (free)

System Disk: High I/O | 40 GiB IOPS limit: 2,120, IOPS burst limit: 5,000

Add Data Disk Disks you can still add: 23



Network: vpc-1 (192.168.0.0/16) | vpc-1-subnet (192.168.1.0/24) | Automatically assign IP address | Available priv

Create VPC

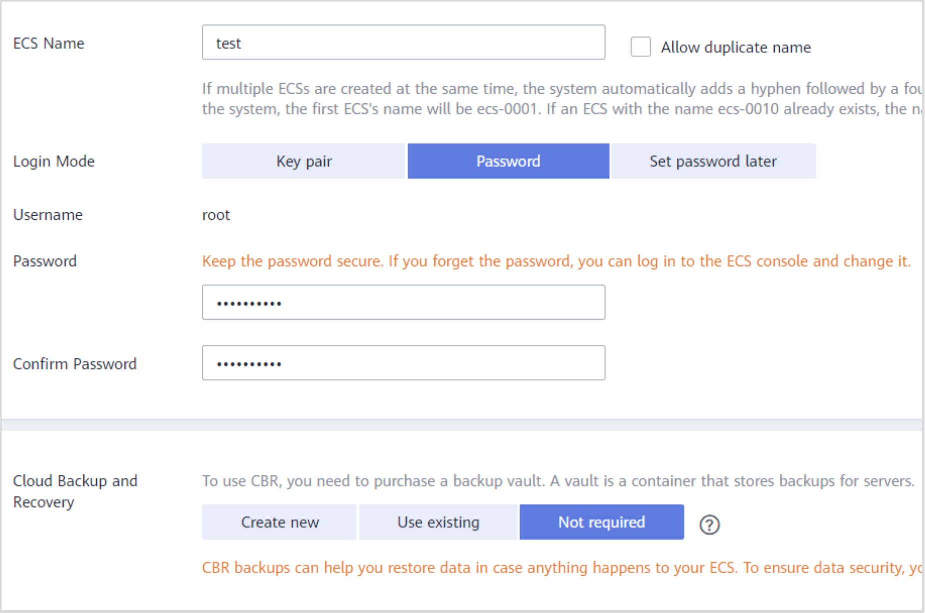
Extension NIC: Add NIC NICs you can still add: 11

Security Group: default (12563f49-fb42-4f57-ba5a-1b423b13155f) | Create Security Group

Similar to a firewall, a security group logically controls network access.

Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Ru

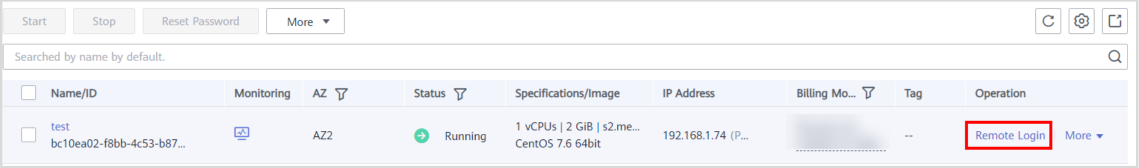
Security Group Rules



ECS Name	test ☐ Allow duplicate name If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a fou the system, the first ECS's name will be ecs-0001. If an ECS with the name ecs-0010 already exists, the n
Login Mode	Key pair | **Password** | Set password later
Username	root
Password	Keep the password secure. If you forget the password, you can log in to the ECS console and change it. ••••••••••
Confirm Password	••••••••••
Cloud Backup and Recovery	To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers. Create new | Use existing | **Not required** ⓘ CBR backups can help you restore data in case anything happens to your ECS. To ensure data security, yo

Figure 5-51

Step 2 Log in to the test ECS.



Start | Stop | Reset Password | More ▾

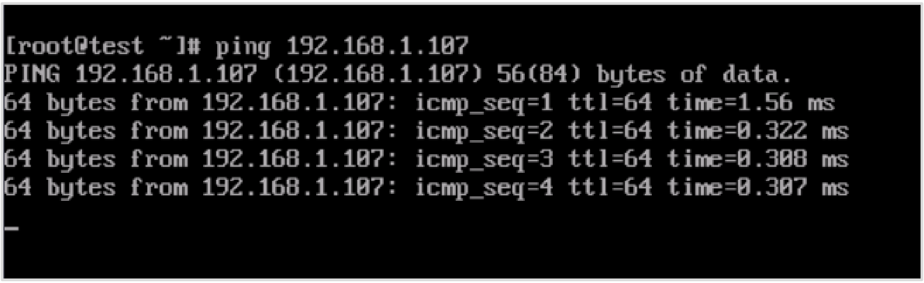
Searched by name by default.

☐	Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mo...	Tag	Operation
☐	test bc10ea02-f8bb-4c53-b87...		AZ2	Running	1 vCPUs | 2 GiB | s2.me... CentOS 7.6 64bit	192.168.1.74 (P...	[redacted]	--	Remote Login More ▾

Figure 5-52

Step 3 Ping the DVWA ECS from the test ECS to verify the connectivity between them.

Note: Before configuring an IP address group, ensure that the two ECSs can communicate with each other.

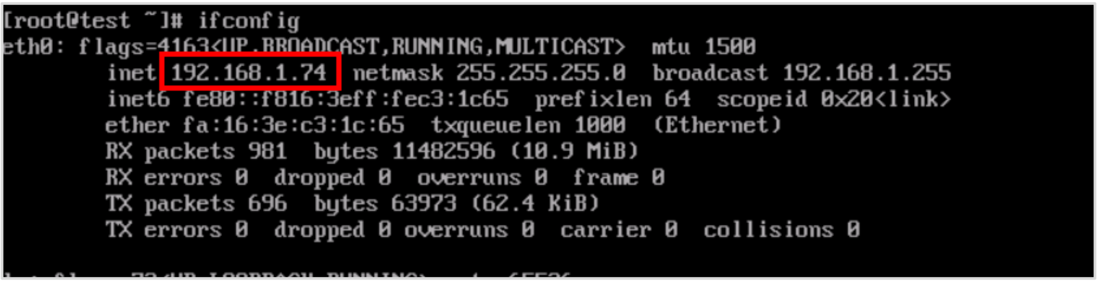


```
[root@test ~]# ping 192.168.1.107
PING 192.168.1.107 (192.168.1.107) 56(84) bytes of data.
64 bytes from 192.168.1.107: icmp_seq=1 ttl=64 time=1.56 ms
64 bytes from 192.168.1.107: icmp_seq=2 ttl=64 time=0.322 ms
64 bytes from 192.168.1.107: icmp_seq=3 ttl=64 time=0.308 ms
64 bytes from 192.168.1.107: icmp_seq=4 ttl=64 time=0.307 ms
_
```

Figure 5-53

Step 4 Use the **ifconfig** command to query the IP address of the test ECS and make a note of the IP address.

Note: The IP address will be added to the IP address group later.



```
[root@test ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.74  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f816:3eff:fec3:1c65  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:c3:1c:65  txqueuelen 1000  (Ethernet)
        RX packets 981  bytes 11482596 (10.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 696  bytes 63973 (62.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 5-54

Step 5 On the **Network Console**, choose **Access Control** > **IP Address Groups** and click **Create IP Address Group** in the upper right corner.

Note: This IP address group will be configured in the security group for traffic blocking tests.

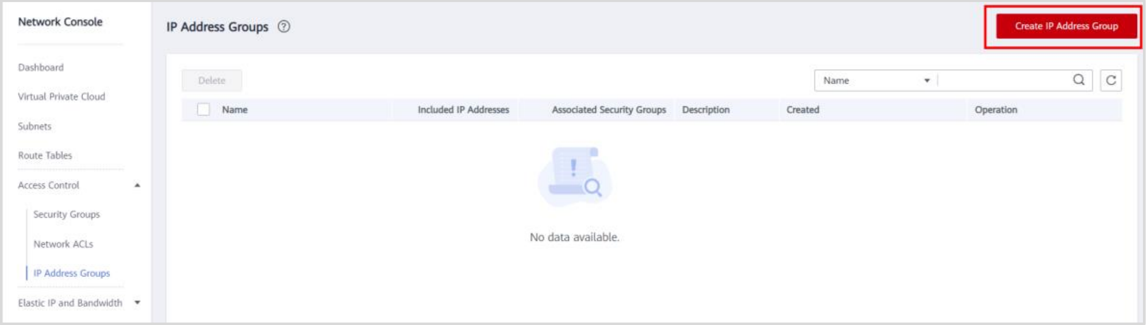
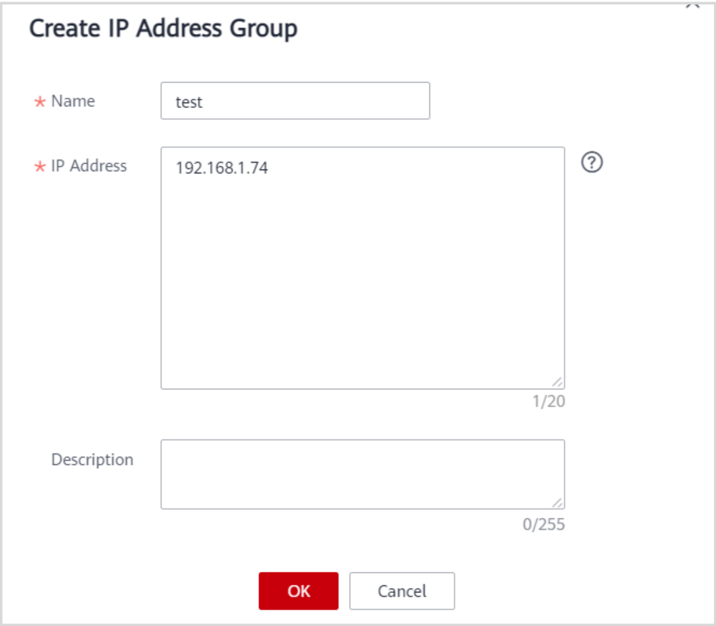


Figure 5-55

Step 6 Configure the parameters as follows and click **OK**.

- **Name: test**
- **IP Address**: Enter the private IP address of the test ECS.



Create IP Address Group

* Name: test

* IP Address: 192.168.1.74

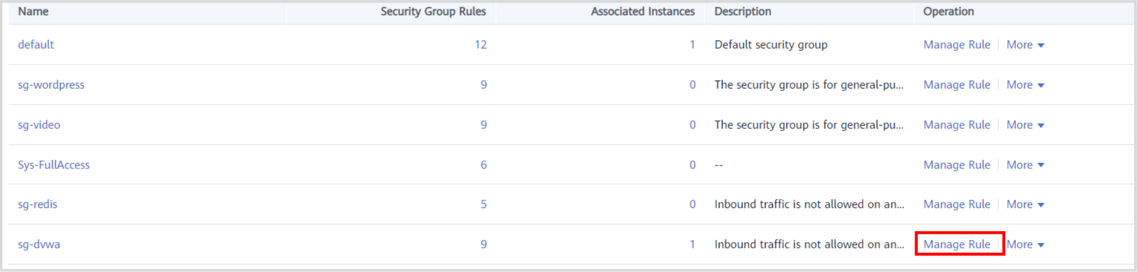
1/20

Description:

0/255

Figure 5-56

Step 7 In the security group list, locate the row that contains the security group **sg-dvwa** and click **Manage Rule** in the **Operation** column.

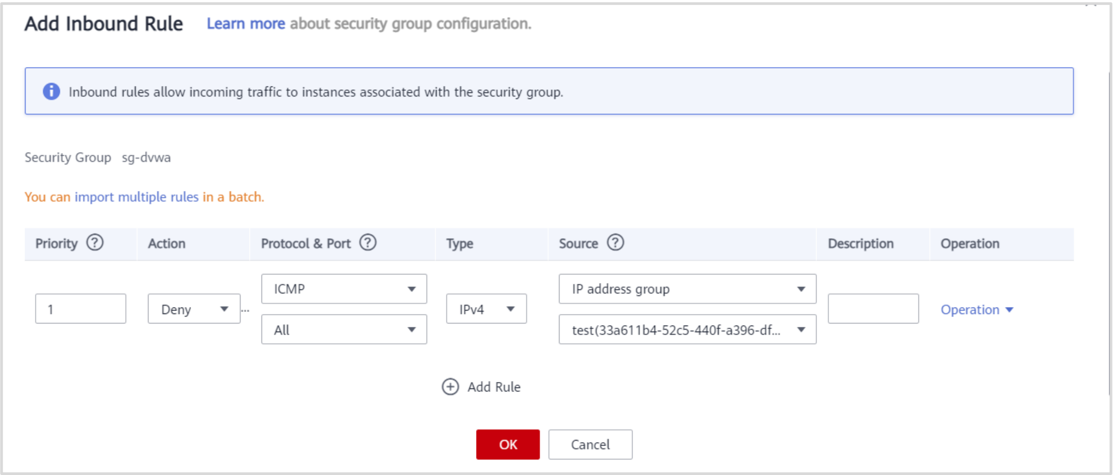


Name	Security Group Rules	Associated Instances	Description	Operation
default	12	1	Default security group	Manage Rule | More ▾
sg-wordpress	9	0	The security group is for general-pu...	Manage Rule | More ▾
sg-video	9	0	The security group is for general-pu...	Manage Rule | More ▾
Sys-FullAccess	6	0	--	Manage Rule | More ▾
sg-redis	5	0	Inbound traffic is not allowed on an...	Manage Rule | More ▾
sg-dvwa	9	1	Inbound traffic is not allowed on an...	Manage Rule | More ▾

Figure 5-57

Step 8 Click the **Inbound Rules** tab and then click **Add Rule**.

- **Priority**: **1**
- **Action**: **Deny**
- **Protocol & Port**: **ICMP** | **All**
- **Source**: **IP address group** | **test**



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group sg-dvwa

You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Source	Description	Operation
1	Deny	ICMP All	IPv4	IP address group test(33a611b4-52c5-440f-a396-df...		Operation ▾

Figure 5-58

Step 9 Log in to the test ECS again and check the connectivity between the test ECS and the DVWA ECS. The communication fails. The security group with the IP address group configured takes effect and blocks the corresponding traffic. This indicates that IP address groups can work together with security groups.

5.2.6 Hosting a Key on DEW

5.2.6.1 Obtaining an AK/SK

Note: The AK/SK obtained in this section will be used in subsequent KooCLI initialization.

Step 1 Click the username in the upper right corner and choose **My Credentials**.

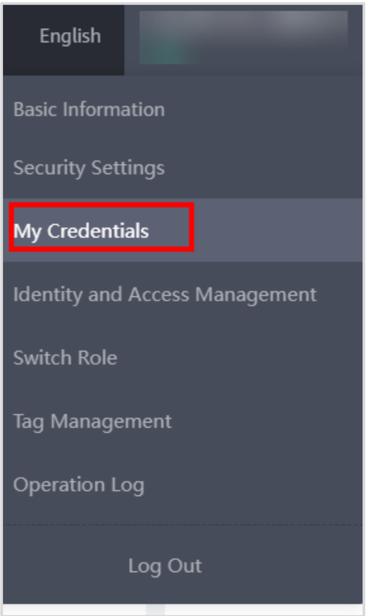
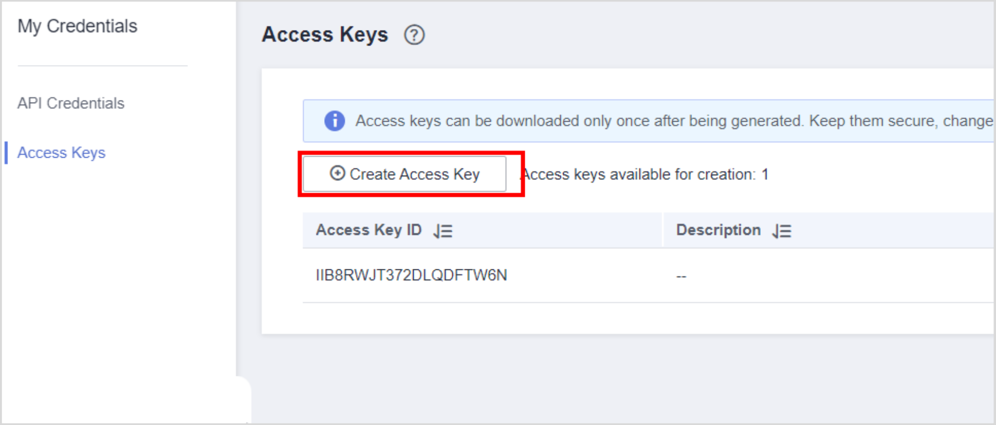


Figure 5-59

Step 2 On the **Access Keys** page, click **Create Access Key**.



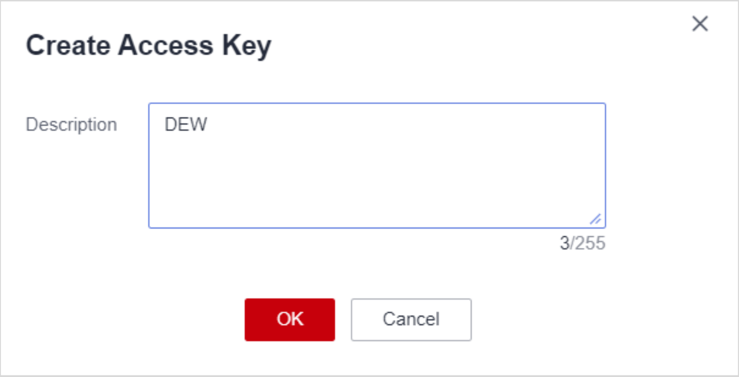
Access keys can be downloaded only once after being generated. Keep them secure, change

Access keys available for creation: 1

Access Key ID	Description
IIB8RWJT372DLQDFTW6N	--

Figure 5-60

Step 3 Enter a description as needed and click **OK**.

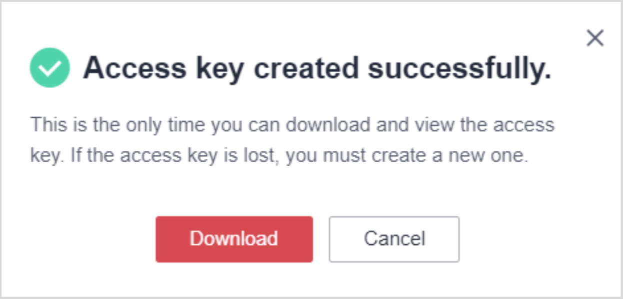


Description: DEW

3/255

Figure 5-61

Step 4 Wait until the creation is successful, and click **Download**.

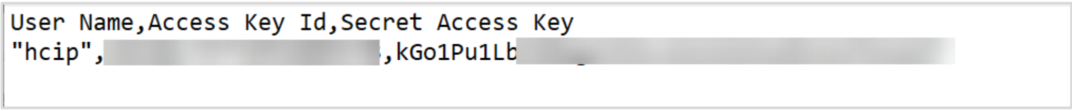


Access key created successfully.

This is the only time you can download and view the access key. If the access key is lost, you must create a new one.

Figure 5-62

Step 5 Properly save the AK/SK on your local PC for later use.



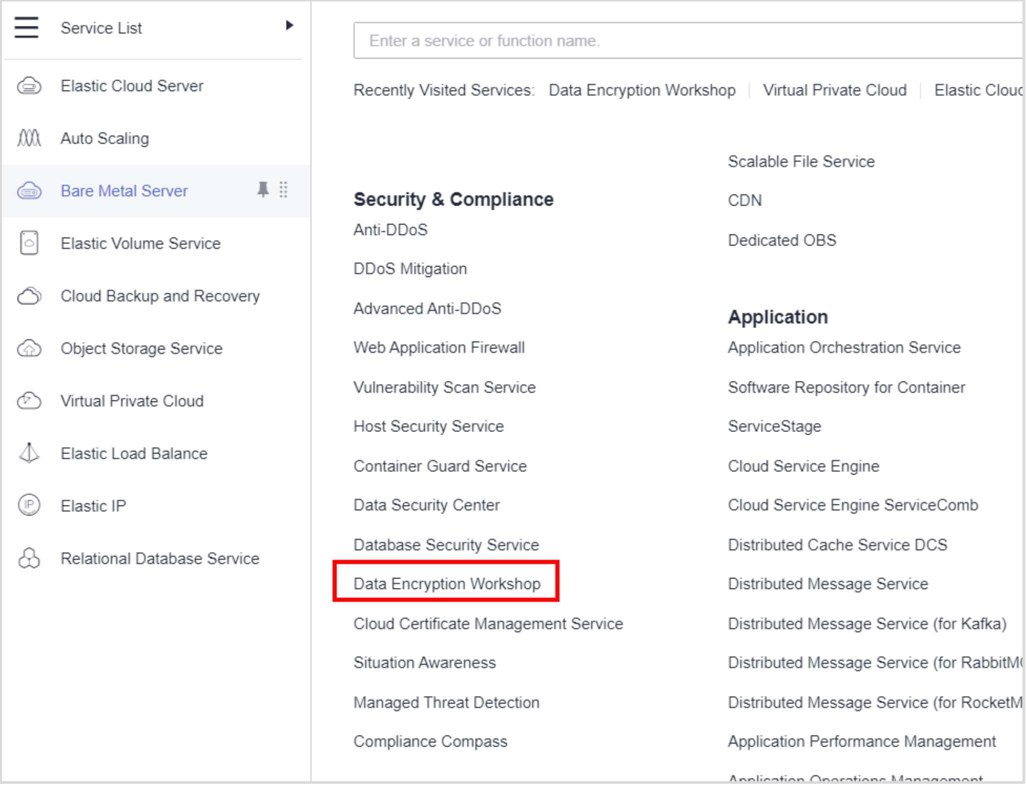
```
User Name,Access Key Id,Secret Access Key
"hcip",[redacted],kGo1Pu1Lb[redacted]
```

Figure 5-63

5.2.6.2 Creating a Secret

Note: The secret is hosted in DEW and will be obtained by ECS through the KooCLI client.

Step 1 In the service list, choose **Data Encryption Workshop** under **Security & Compliance**.



Service List
Elastic Cloud Server
Auto Scaling
Bare Metal Server
Elastic Volume Service
Cloud Backup and Recovery
Object Storage Service
Virtual Private Cloud
Elastic Load Balance
Elastic IP
Relational Database Service
Enter a service or function name.
Recently Visited Services: Data Encryption Workshop | Virtual Private Cloud | Elastic Clouc
Security & Compliance
Anti-DDoS
DDoS Mitigation
Advanced Anti-DDoS
Web Application Firewall
Vulnerability Scan Service
Host Security Service
Container Guard Service
Data Security Center
Database Security Service
Data Encryption Workshop
Cloud Certificate Management Service
Situation Awareness
Managed Threat Detection
Compliance Compass
Scalable File Service
CDN
Dedicated OBS
Application
Application Orchestration Service
Software Repository for Container
ServiceStage
Cloud Service Engine
Cloud Service Engine ServiceComb
Distributed Cache Service DCS
Distributed Message Service
Distributed Message Service (for Kafka)
Distributed Message Service (for RabbitM
Distributed Message Service (for RocketM
Application Performance Management

Figure 5-64

Step 2 On the **Cloud Secret Management Service** page, click **Create Secret**.

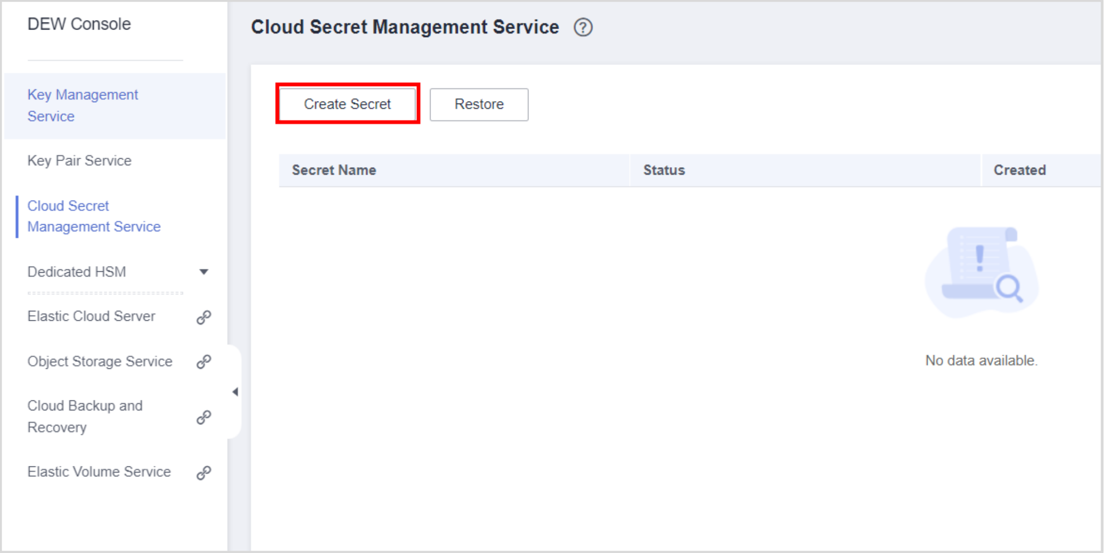
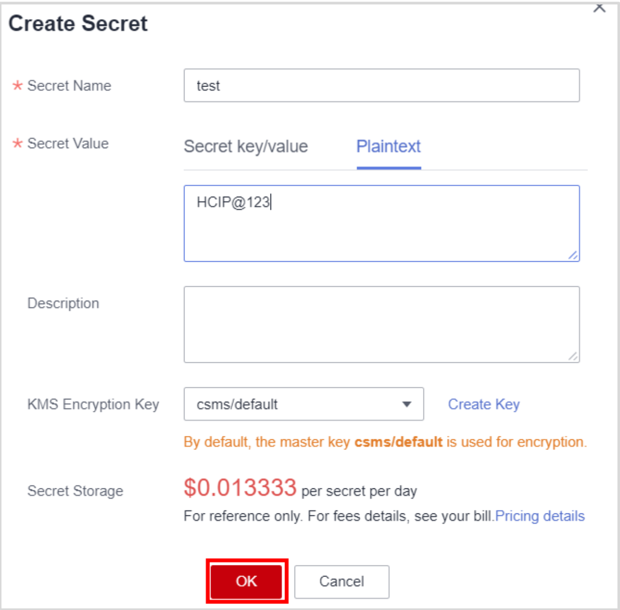


Figure 5-65

Step 3 Configure secret parameters, as shown in the following figure.

- **Secret Name: test**
- **Secret Value**: Set a value as needed. Example: **HCIP@123**

Retain the default settings for other parameters.



Create Secret

* Secret Name: test

* Secret Value: Secret key/value | Plaintext

HCIP@123

Description:

KMS Encryption Key: csms/default Create Key

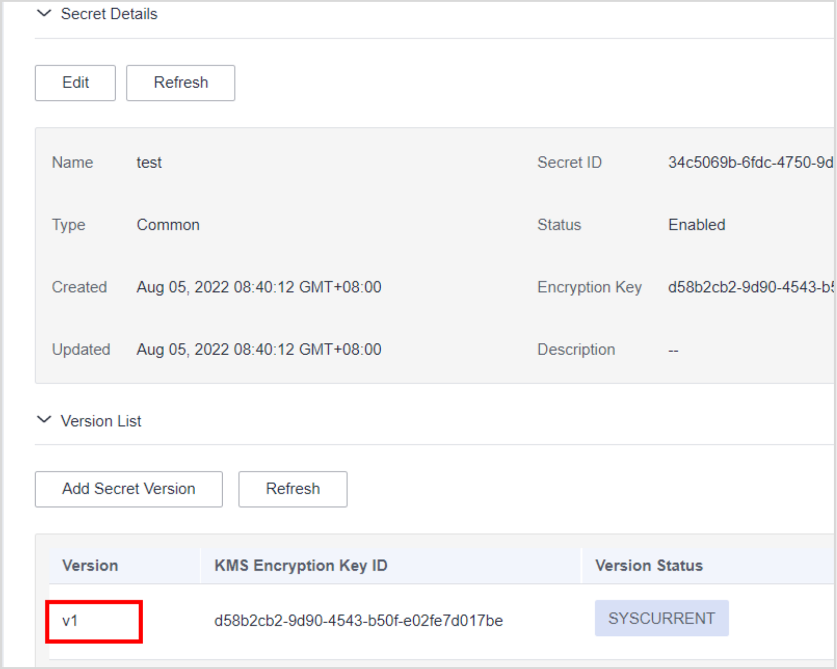
By default, the master key **csms/default** is used for encryption.

Secret Storage: $0.013333 per secret per day

For reference only. For fees details, see your bill.Pricing details

Figure 5-66

Step 4 Click the secret name to view details. The current version is **v1**.



Name	test	Secret ID	34c5069b-6fdc-4750-9d
Type	Common	Status	Enabled
Created	Aug 05, 2022 08:40:12 GMT+08:00	Encryption Key	d58b2cb2-9d90-4543-b5
Updated	Aug 05, 2022 08:40:12 GMT+08:00	Description	--

Version	KMS Encryption Key ID	Version Status
v1	d58b2cb2-9d90-4543-b50f-e02fe7d017be	SYSCURRENT

Figure 5-67

5.2.6.3 Creating an Agency

Note: The agency is used to delegate permissions to the ECS so that the ECS can obtain DEW-managed keys through KooCLI.

Step 1 In the upper right corner of the page, hover the mouse over the username and select **Identity and Access Management**.

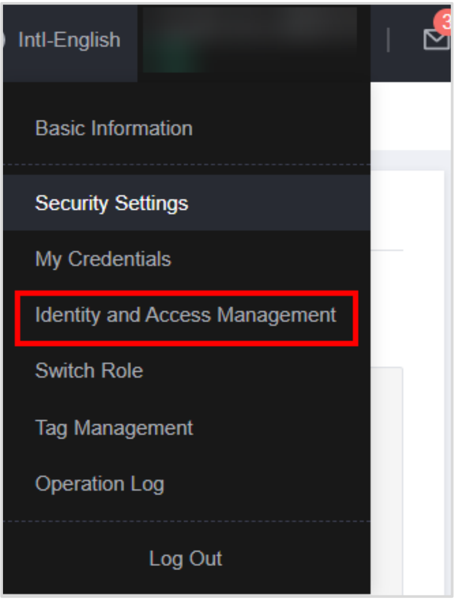
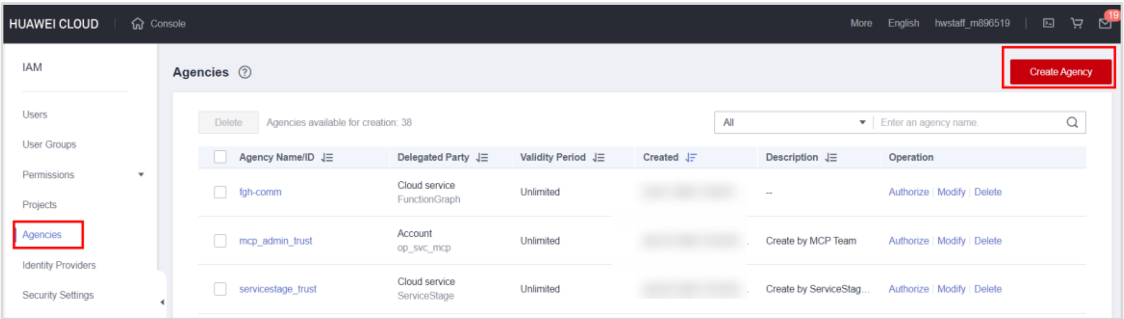


Figure 5-68

Step 2 Choose **Agencies** in the navigation pane on the left and click **Create Agency**.



Agencies

Agencies available for creation: 38

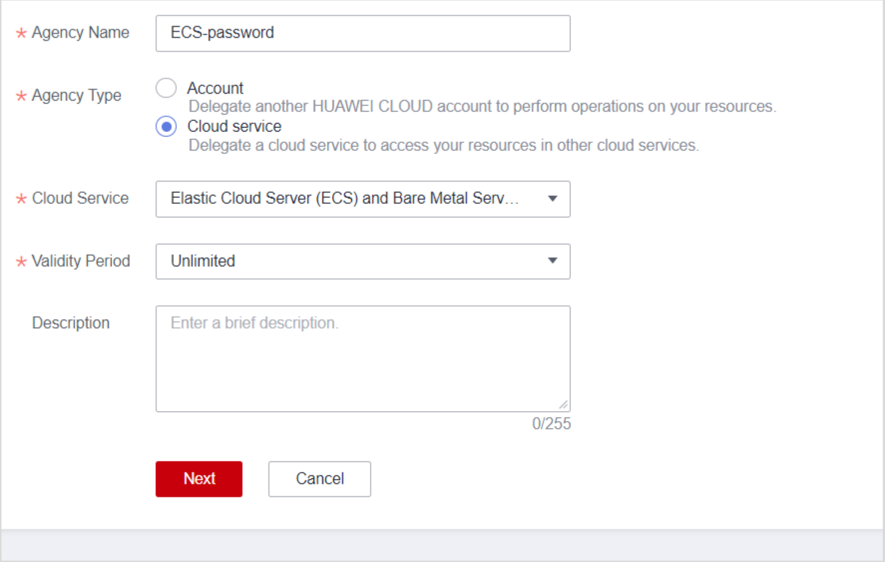
All | Enter an agency name.

	Agency Name/ID	Delegated Party	Validity Period	Created	Description	Operation
□	fgh-comm	Cloud service FunctionGraph	Unlimited	[redacted]	--	Authorize | Modify | Delete
□	mcp_admin_trust	Account op_svc_mcp	Unlimited	[redacted]	Create by MCP Team	Authorize | Modify | Delete
□	servicestage_trust	Cloud service ServiceStage	Unlimited	[redacted]	Create by ServiceStag...	Authorize | Modify | Delete

Figure 5-69

Step 3 Configure the agency and click **Next**.

- **Agency Name: ECS-password**
- **Agency Type: Cloud service**
- **Cloud Service: Elastic Cloud Server (ECS) and Bare Metal Server (BMS)**
- **Validity Period: Unlimited**



* Agency Name: ECS-password

* Agency Type:
○ Account
Delegate another HUAWEI CLOUD account to perform operations on your resources.
● Cloud service
Delegate a cloud service to access your resources in other cloud services.

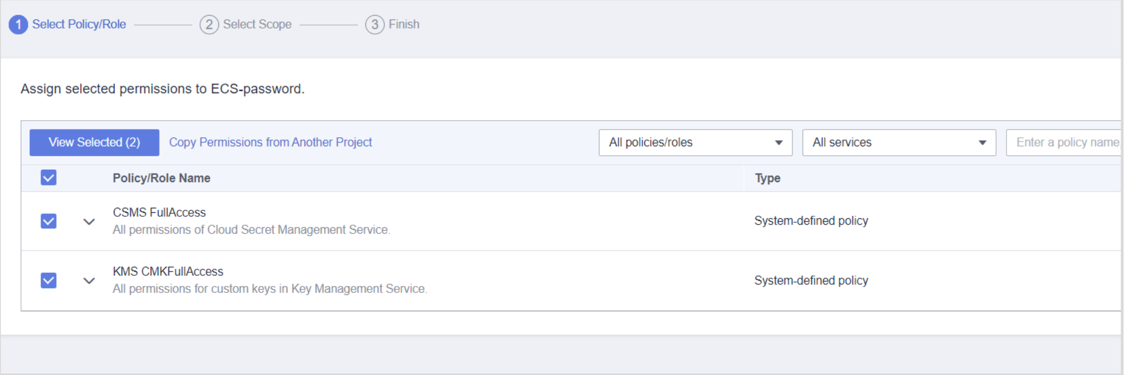
* Cloud Service: Elastic Cloud Server (ECS) and Bare Metal Serv...

* Validity Period: Unlimited

Description: Enter a brief description.
0/255

Figure 5-70

Step 4 Select **CSMS FullAccess** and **KMS CMKFullAccess**.

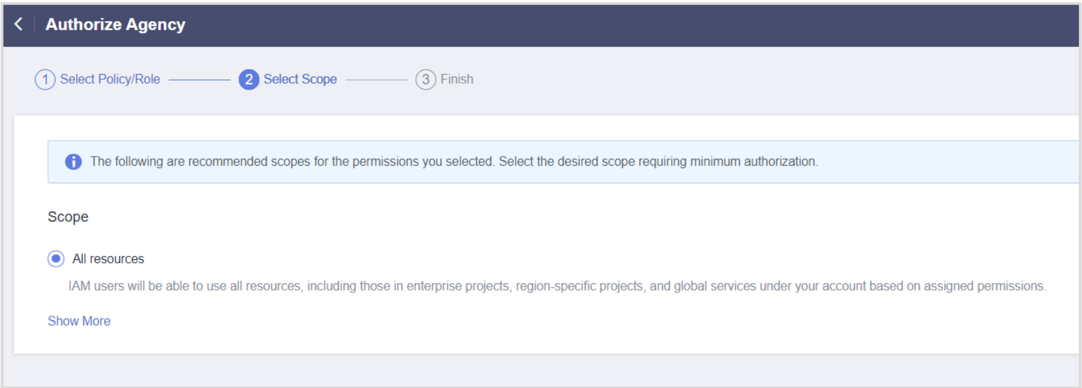


Assign selected permissions to ECS-password.

☑		Policy/Role Name	Type
☑	∨	CSMS FullAccess All permissions of Cloud Secret Management Service.	System-defined policy
☑	∨	KMS CMKFullAccess All permissions for custom keys in Key Management Service.	System-defined policy

Figure 5-71

Step 5 Retain the default authorization scope and click **OK**.



The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

Scope

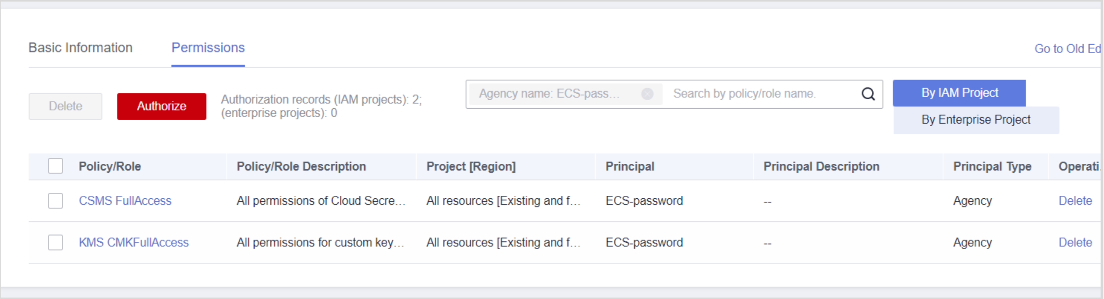
● All resources

IAM users will be able to use all resources, including those in enterprise projects, region-specific projects, and global services under your account based on assigned permissions.

Show More

Figure 5-72

Step 6 After the agency is created, view the assigned permissions on the **Permissions** page.



Authorization records (IAM projects): 2; (enterprise projects): 0

Agency name: ECS-pass... | Search by policy/role name.

□	Policy/Role	Policy/Role Description	Project [Region]	Principal	Principal Description	Principal Type	Operati
□	CSMS FullAccess	All permissions of Cloud Secre...	All resources [Existing and f...	ECS-password	--	Agency	Delete
□	KMS CMKFullAccess	All permissions for custom key...	All resources [Existing and f...	ECS-password	--	Agency	Delete

Figure 5-73

5.2.6.4 Installing KooCLI

Step 1 Create an ECS named **ecs-test** by referring to steps 3 to 4 in DVWA Deployment. (You can use the ECS **test** created in section **错误!未找到引用源。**if it has not been deleted).

Note: This ECS is used only for installing KooCLI and obtaining keys.

Configure the ECS **ecs-test** as follows:

- **Billing Mode: Pay-per-use**
- **Region: CN-Hong Kong**
- **AZ: Random**
- **CPU Architecture: x86**
- **Specifications: 1 vCPUs | 2 GiB**
- **Image: Public image | CentOS 7.6 64bit(40GB)**
- **Host Security: Enable** (Basic)
- **Network: vpc-1 | subnet-20 | Automatically assign IP address**
- **Security Group: default**

- **EIP**: **Auto assign**
- **EIP Type**: **Premium BGP**
- **Billed By**: **Traffic**
- **Bandwidth Size**: **10 Mbit/s**
- **System disk**: **General-purpose SSD | 40 GiB**
- **ECS Name**: **ecs-test**
- **Password**: User-defined (with the username of **root**)

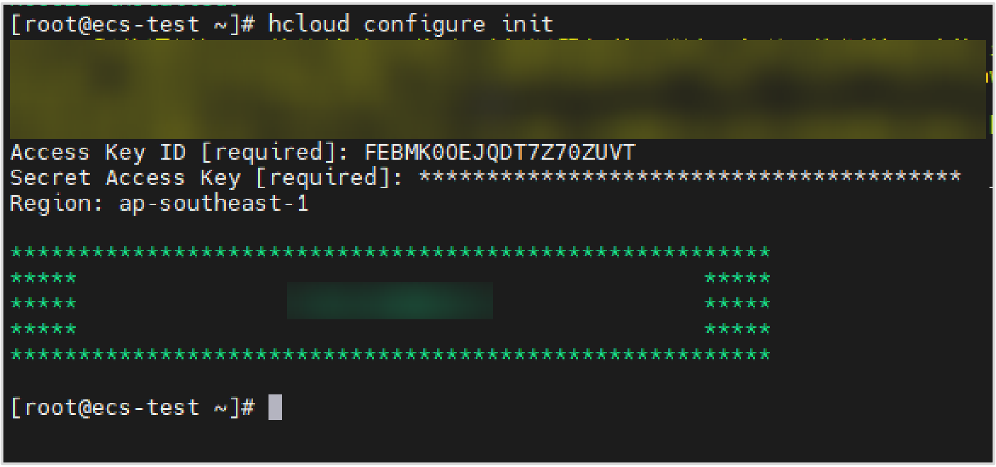
Step 2 Log in to **ecs-test** and install the KooCLI client.

```
[root@ecs-test ~]# curl -sSL https://ap-southeast-3-hwcloudcli.obs.ap-southeast-3.myhuaweicloud.com/cli/latest/hcloud_install.sh -o ./hcloud_install.sh && bash ./hcloud_install.sh -y
```

Step 3 Initialize the ECS. Enter "Y" to agree Privacy Statement at https://www.huaweicloud.com/intl/zh-cn/declaration/sa_prp.html.

The AK/SK obtained in section **错误!未找到引用源。**is required here.

```
[root@ecs-test ~]# hcloud configure init
Access Key ID [required]: Enter the AK.
Secret Access Key [required]: Enter the SK.
Region Name: Enter a region name, for example, ap-southeast-1.
```



```
[root@ecs-test ~]# hcloud configure init
[redacted]
Access Key ID [required]: FEBMK00EJQDT7Z70ZUVT
Secret Access Key [required]: *****************************************
Region: ap-southeast-1

**********************************************************
*****                                                *****
*****              [redacted]                        *****
*****                                                *****
**********************************************************

[root@ecs-test ~]#
```

Figure 5-74

If your current environment language is Chinese. To switch the language, run the **hcloud configure set --cli-lang=en** command.

```
[root@ecs-test ~]# hcloud configure set --cli-lang=en
```

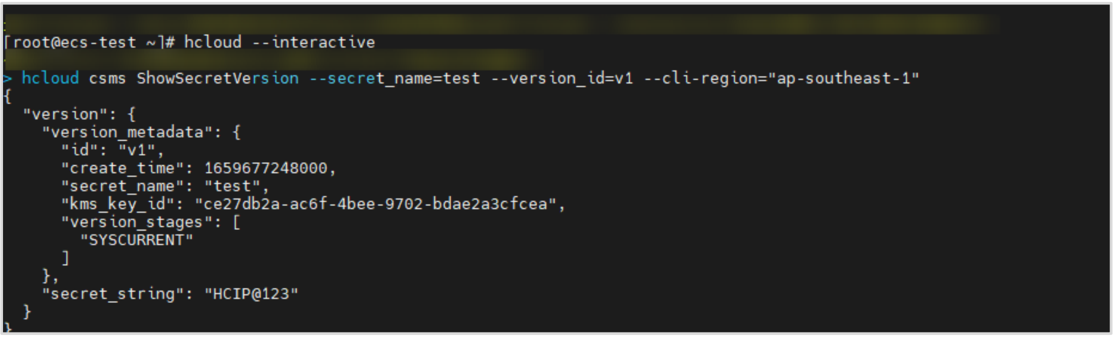
5.2.6.5 Using KooCLI to Obtain the Key

Step 1 Enter the KooCLI interaction mode:

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

Step 2 View information about the key created in DEW. As shown in the following figure, key **HCIP@123** has been obtained, indicating that ECS can obtain the DEW-managed key through the KooCLI client.

```
> hcloud csms ShowSecretVersion --secret_name=test --version_id=v1 --cli-region="ap-southeast-1"
# --secret_name=Key name
# --version_id=Key version
# --cli-region="Current region"
```



```
[redacted]
[root@ecs-test ~]# hcloud --interactive
[redacted]
> hcloud csms ShowSecretVersion --secret_name=test --version_id=v1 --cli-region="ap-southeast-1"
{
  "version": {
    "version_metadata": {
      "id": "v1",
      "create_time": 1659677248000,
      "secret_name": "test",
      "kms_key_id": "ce27db2a-ac6f-4bee-9702-bdae2a3cfcea",
      "version_stages": [
        "SYSCURRENT"
      ]
    },
    "secret_string": "HCIP@123"
  }
}
```

Figure 5-75

5.3 Clearing Resources

Step 1 Delete the agency.

- In the upper right corner of the page, hover the mouse over the username and select **Identity and Access Management**.

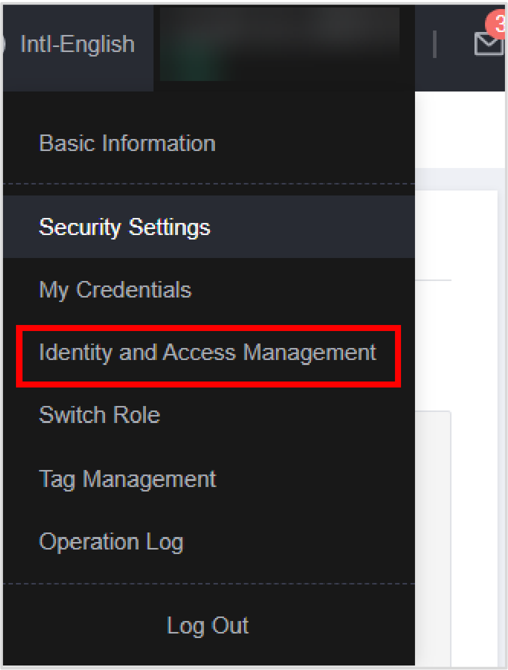


Figure 5-76

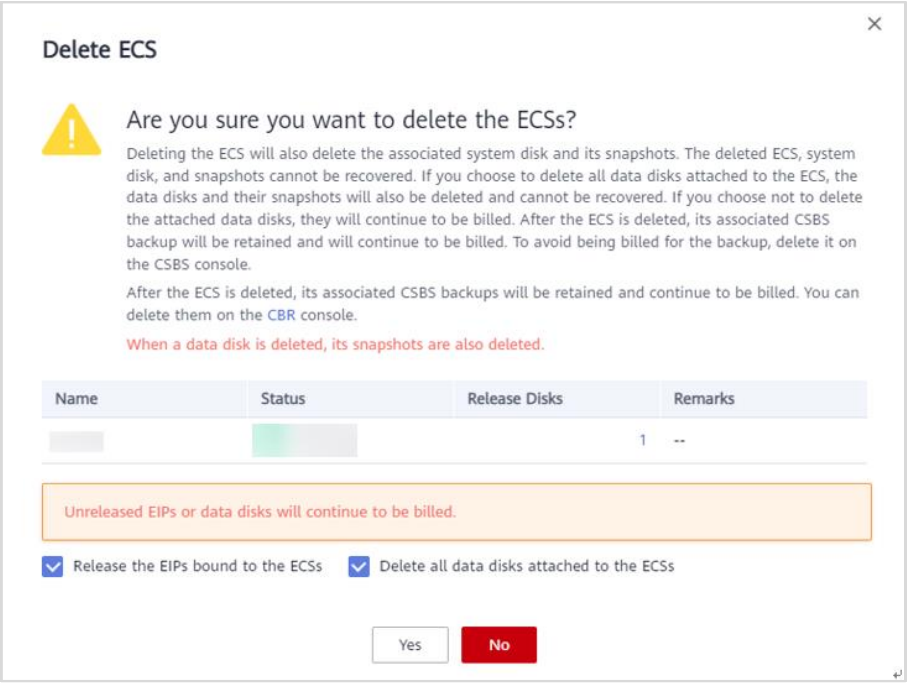
- Choose **Agencies** in the left navigation pane. Locate the row containing the agency created in this exercise click **Delete** in the **Operation** column.

Step 2 Delete the secret.

- In the service list, choose **Data Encryption Workshop** under **Security & Compliance**. In the navigation pane on the left, choose **Cloud Secret Management Service**, locate the row containing the secret created in this exercise and click **Delete** in the **Operation** column.
- In the displayed dialog box, select **Delete now** and click **OK**.

Step 3 Delete the ECS.

- In the service list, choose **Elastic Cloud Server** under **Compute**. In the ECS list, locate the ECS purchased in this exercise and choose **More** > **Delete** in the **Operation** column.
- In the displayed dialog box, select the check boxes displayed in the following picture and click **Yes**.



Delete ECS

Are you sure you want to delete the ECSs?

Deleting the ECS will also delete the associated system disk and its snapshots. The deleted ECS, system disk, and snapshots cannot be recovered. If you choose to delete all data disks attached to the ECS, the data disks and their snapshots will also be deleted and cannot be recovered. If you choose not to delete the attached data disks, they will continue to be billed. After the ECS is deleted, its associated CSBS backup will be retained and will continue to be billed. To avoid being billed for the backup, delete it on the CSBS console.

After the ECS is deleted, its associated CSBS backups will be retained and continue to be billed. You can delete them on the CBR console.

When a data disk is deleted, its snapshots are also deleted.

Name	Status	Release Disks	Remarks
[redacted]	[redacted]	1	--

Unreleased EIPs or data disks will continue to be billed.

☑ Release the EIPs bound to the ECSs ☑ Delete all data disks attached to the ECSs

Figure 5-77

Step 4 Delete two-factor authentication.

On the **Service List** page, select **Host Security Service** under **Security & Compliance**. Choose **Installation & Configuration**, click the **Two-Factor Authentication** tab, and click **Delete** in the **Operation** column of a record.

Step 5 Delete the SMN topic.

In the service list, choose **Simple Message Notification**. In the navigation pane on the left, choose **Topic Management** > **Topics**. In the right pane, locate the topic created in this exercise, choose **More** > **Delete** in the **Operation** column, and click **OK**.

Step 6 Delete the IP address group.

In the service list, choose **Virtual Private Cloud** under **Networking**. On the network console, choose **Access Control** > **IP Address Groups**. In the IP address group list, locate the IP address group created in this exercise and click **Delete** in the **Operation** column.

Step 7 Delete the security group.

In the service list, choose **Virtual Private Cloud** under **Networking**. On the network console, choose **Access Control** > **Security Groups**. In the security group list, locate the security group created in this exercise and click **Delete** in the **Operation** column.

Step 8 Delete the subnet and VPC.

- In the service list, choose **Virtual Private Cloud** under **Networking**. On the network console, choose **Subnets**. In the subnet list, locate the subnet created in this exercise and click **Delete** in the **Operation** column.
- Choose **Virtual Private Cloud** in the navigation pane on the left. In the VPC list, locate the VPC created in this exercise and click **Delete** in the **Operation** column.

5.4 Quiz

Question: Besides real-time intrusion detection, what functions does the HSS enterprise edition provide?

Answer: Virus and Trojan detection and removal, baseline check, one-click vulnerability fix, and security configuration

6 Containerized Application Deployment

6.1 Introduction

6.1.1 About This Exercise

This exercise consists of two parts:

1. Deploy Docker engine and containers on ECSs to provide web services. Use Dockerfiles to build and push images to SoftWare Repository for Container (SWR). To test whether the pushed image is available, use Cloud Container Engine (CCE) to pull and deploy the image. Use a local browser to access the EIP of the CCE node to check whether the web page is normal.
2. Use FunctionGraph to update object versions in an OBS bucket and retain only the latest three versions.

This exercise uses the Hong Kong or Singapore region as an example.

6.1.2 Objectives

Understand how to use and configure Docker engine.

Understand how to use and configure SoftWare Repository for Container (SWR).

Understand how to use and configure Cloud Container Engine (CCE).

Understand how to use and configure FunctionGraph.

6.1.3 Networking

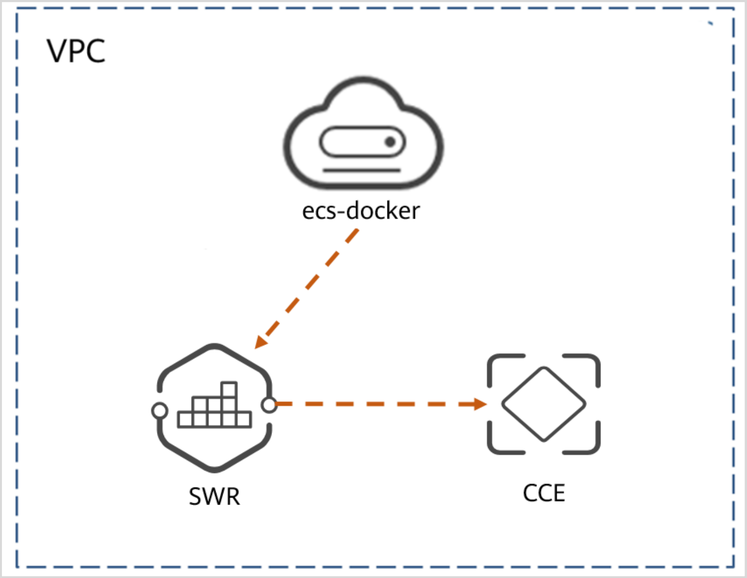


Figure 6-1 Container networking

6.1.4 Related Software

Docker is an open source container engine that allows developers to package applications and dependency packages into a portable image and release the image to any popular Linux or Windows operating system.

httpd is the main program of the Apache Hypertext Transfer Protocol (HTTP) server. It is a backend process that runs independently and creates a pool of subprocesses or threads that process requests.

6.2 Procedure

6.2.1 Deploying Containers & CCE

6.2.1.1 Creating a VPC

Step 1 On the upper area of the console, select **CN-Hong Kong**.

Step 2 In the service list, choose **Networking** > **Virtual Private Cloud**.

Step 3 Click **Create VPC** in the upper right corner. (Subsequent resources will be created in the VPC.)

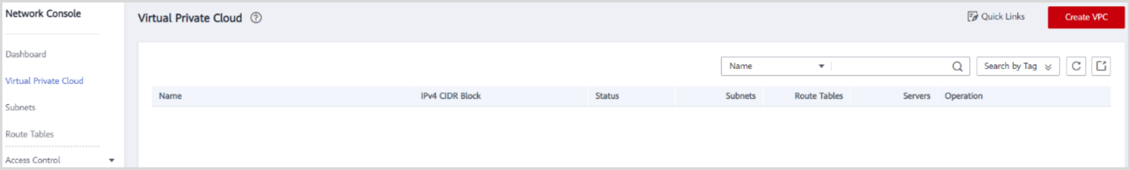


Figure 6-2

Step 4 Configure the following parameters and click **Create Now**.

- **Region**: **CN-Hong Kong**
- **Name**: **vpc-1**
- **IPv4 CIDR Block**: **192.168.0.0/16**

Default Subnet

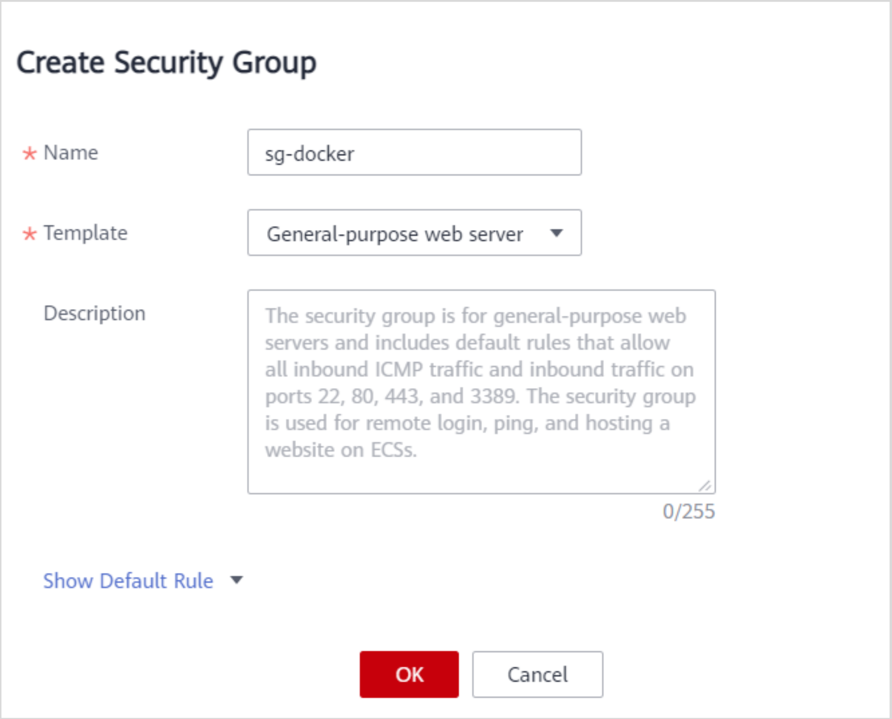
- **Name**: **vpc-1-subnet**
- **IPv4 CIDR Block**: **192.168.1.0/24**

6.2.1.2 Creating a Security Group

Step 1 Create security group **sg-docker** in **CN-Hong Kong** based on the following configurations:

Note: This security group is used by the ECS where the Docker engine will be deployed.

- **Name**: **sg-docker**
- General-purpose web server



Create Security Group

* Name: sg-docker

* Template: General-purpose web server

Description: The security group is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and inbound traffic on ports 22, 80, 443, and 3389. The security group is used for remote login, ping, and hosting a website on ECSs.

Figure 6-3

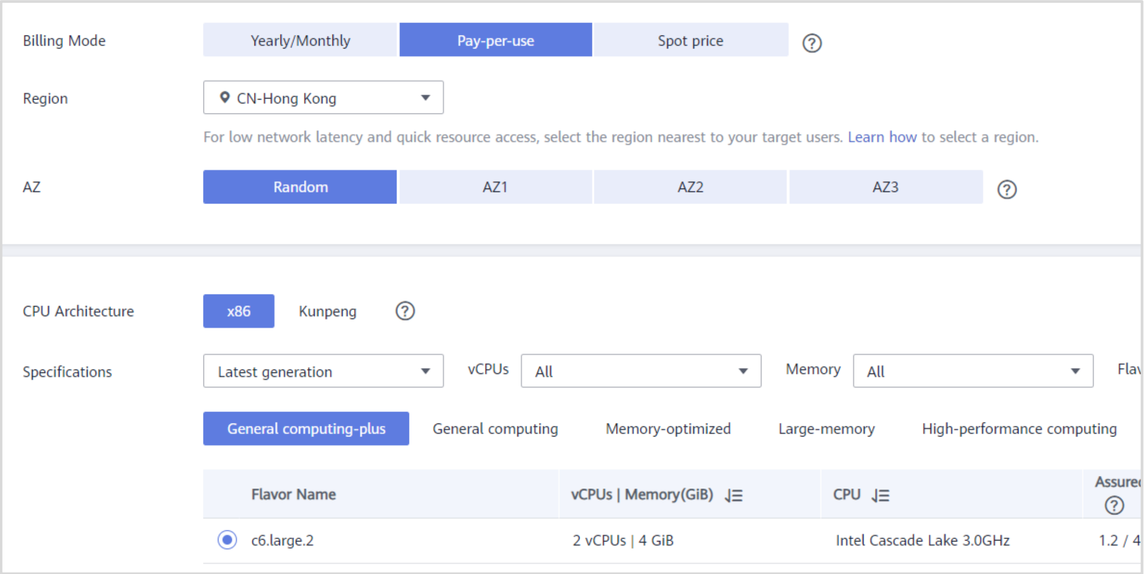
6.2.1.3 Creating an ECS

Step 1 Create an ECS **ecs-docker** based on the following configurations:

Note: This ECS is used to deploy the Docker engine.

Configure the ECS **ecs-docker** as follows:

- Billing Mode: Pay-per-use
- Region: CN-Hong Kong
- AZ: Random
- CPU Architecture: x86
- Specifications: 2 vCPUs | 4 GiB
- Image: Public image | CentOS 7.6 64bit(40GB)
- Host Security: Enable | Basic (free)
- Network: vpc-1 | vpc-1-subnet | Automatically assign IP address
- Security Group: sg-docker
- EIP: Auto assign
- EIP Type: Dynamic BGP
- Billed By: Traffic
- Bandwidth Size: 10 Mbit/s
- System Disk: High I/O | 40 GiB
- ECS Name: ecs-docker
- Login Mode ： Password(User-defined)



Billing Mode: Yearly/Monthly | **Pay-per-use** | Spot price

Region: CN-Hong Kong

For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

AZ: **Random** | AZ1 | AZ2 | AZ3

CPU Architecture: **x86** | Kunpeng

Specifications: Latest generation | vCPUs: All | Memory: All | Flav

General computing-plus | General computing | Memory-optimized | Large-memory | High-performance computing

	Flavor Name	vCPUs | Memory(GiB)	CPU	Assurec
●	c6.large.2	2 vCPUs | 4 GiB	Intel Cascade Lake 3.0GHz	1.2 / 4

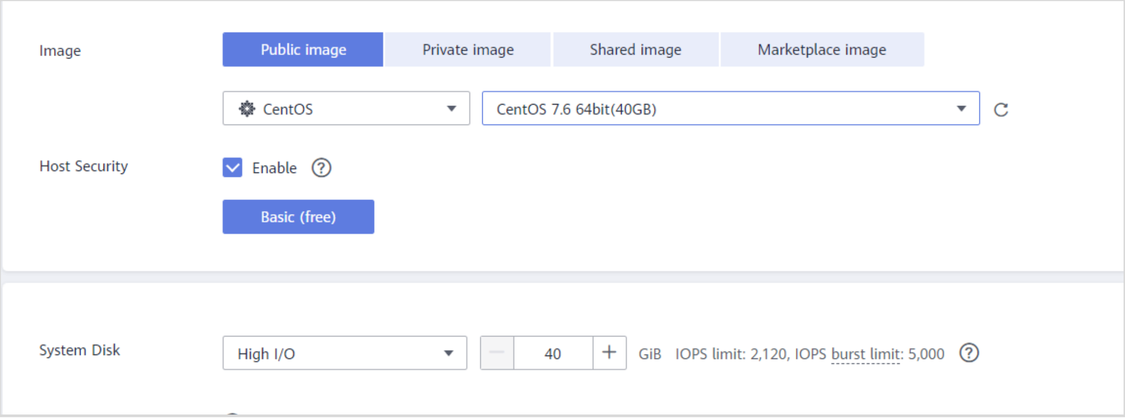


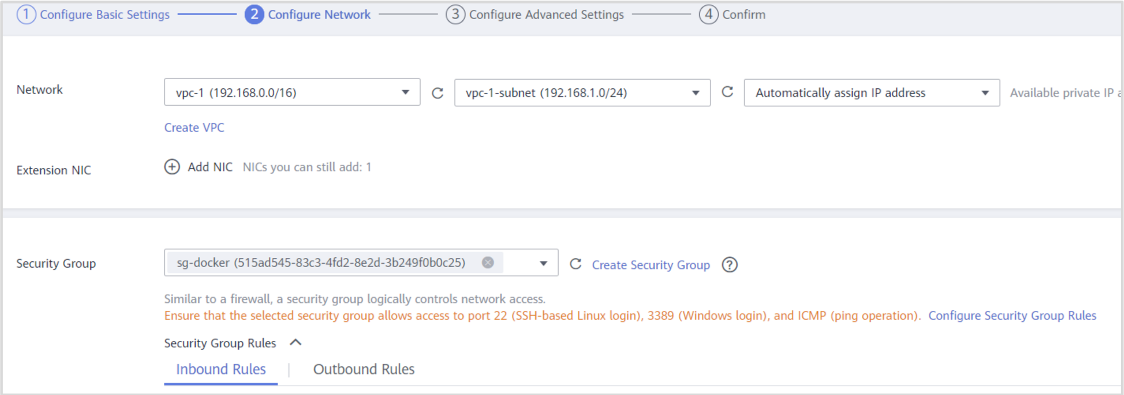
Image: **Public image** | Private image | Shared image | Marketplace image

CentOS | CentOS 7.6 64bit(40GB)

Host Security: ☑ Enable

Basic (free)

System Disk: High I/O | 40 GiB IOPS limit: 2,120, IOPS burst limit: 5,000



Network: vpc-1 (192.168.0.0/16) | vpc-1-subnet (192.168.1.0/24) | Automatically assign IP address | Available private IP a

Create VPC

Extension NIC: ⊕ Add NIC NICs you can still add: 1

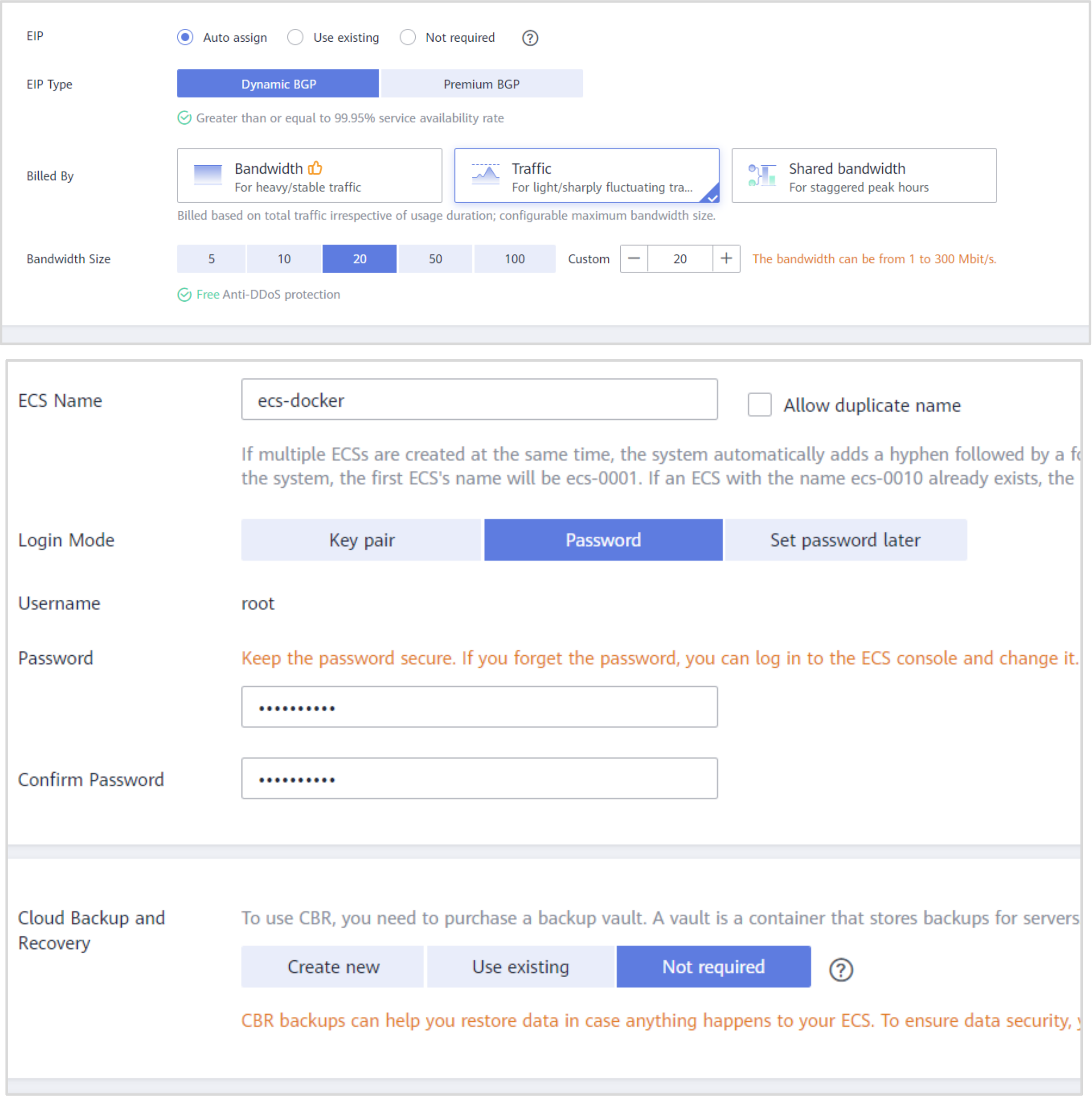
Security Group: sg-docker (515ad545-83c3-4fd2-8e2d-3b249f0b0c25) | Create Security Group

Similar to a firewall, a security group logically controls network access.

Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

Security Group Rules

Inbound Rules | Outbound Rules



EIP ● Auto assign ○ Use existing ○ Not required ⓘ

EIP Type [✓ Dynamic BGP] Premium BGP

✓ Greater than or equal to 99.95% service availability rate

Billed By: Bandwidth — For heavy/stable traffic | [✓ Traffic — For light/sharply fluctuating tra...] | Shared bandwidth — For staggered peak hours

Billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size.

Bandwidth Size: 5 | 10 | [✓ 20] | 50 | 100 | Custom − 20 + The bandwidth can be from 1 to 300 Mbit/s.

✓ Free Anti-DDoS protection

ECS Name: ecs-docker □ Allow duplicate name

If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a f
the system, the first ECS's name will be ecs-0001. If an ECS with the name ecs-0010 already exists, the

Login Mode: Key pair | [✓ Password] | Set password later

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.

••••••••••

Confirm Password: ••••••••••

Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers

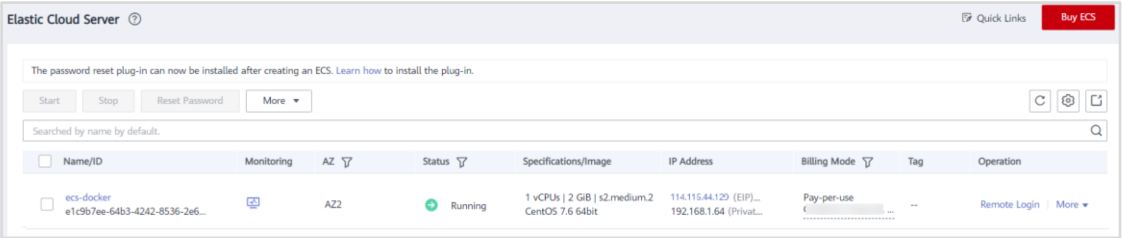
Create new | Use existing | [✓ Not required] ⓘ

CBR backups can help you restore data in case anything happens to your ECS. To ensure data security, y

Figure 6-4

6.2.1.4 Installing and Deploying Docker

Step 1 Use Huawei Cloud CloudShell to log in to ecs-docker.



Elastic Cloud Server ⓘ

The password reset plug-in can now be installed after creating an ECS. Learn how to install the plug-in.

Searched by name by default.

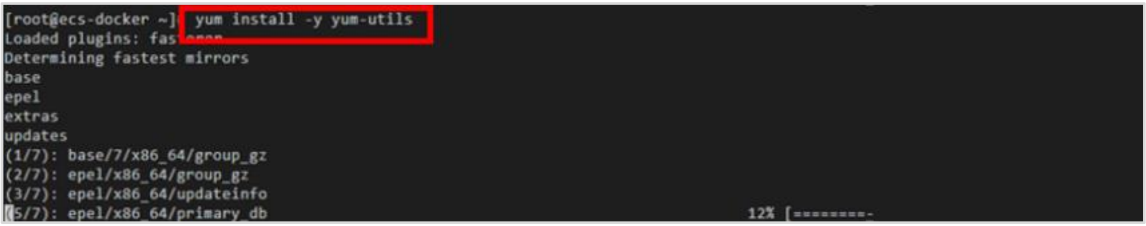
□	Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mode	Tag	Operation
□	ecs-docker e1c9b7ee-64b3-4242-8536-2e6...		AZ2	Running	1 vCPUs | 2 GiB | s2.medium.2 CentOS 7.6 64bit	114.115.44.129 (EIP)... 192.168.1.64 (Privat...	Pay-per-use [redacted]	--	Remote Login | More ▾

Figure 6-5

Step 2 Run the following command to install the yum unit:

Note: If a non-root user is used, **sudo** needs to be added to some commands.

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

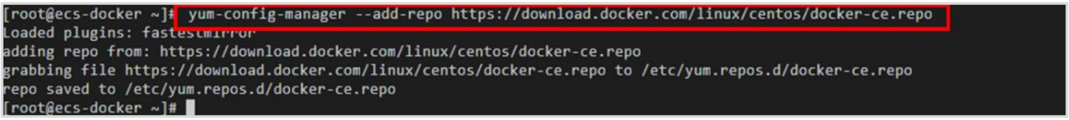


```
[root@ecs-docker ~]# yum install -y yum-utils
Loaded plugins: fas
Determining fastest mirrors
base
epel
extras
updates
(1/7): base/7/x86_64/group_gz
(2/7): epel/x86_64/group_gz
(3/7): epel/x86_64/updateinfo
(5/7): epel/x86_64/primary_db                                               12% [========-
```

Figure 6-6

Step 3 Run the following command to add the yum source:

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

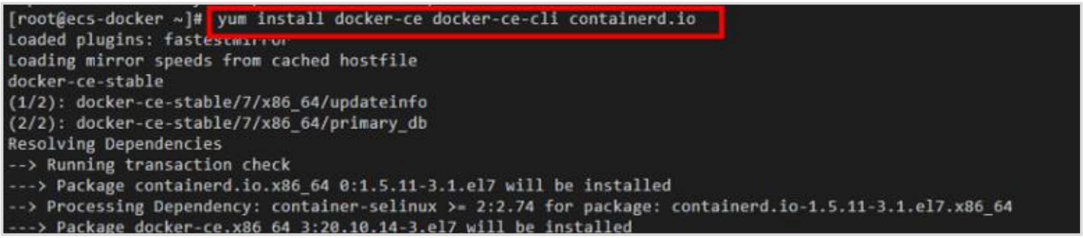


```
[root@ecs-docker ~]# yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
Loaded plugins: fastestmirror
adding repo from: https://download.docker.com/linux/centos/docker-ce.repo
grabbing file https://download.docker.com/linux/centos/docker-ce.repo to /etc/yum.repos.d/docker-ce.repo
repo saved to /etc/yum.repos.d/docker-ce.repo
[root@ecs-docker ~]#
```

Figure 6-7

Step 4 Run the following command to install Docker:

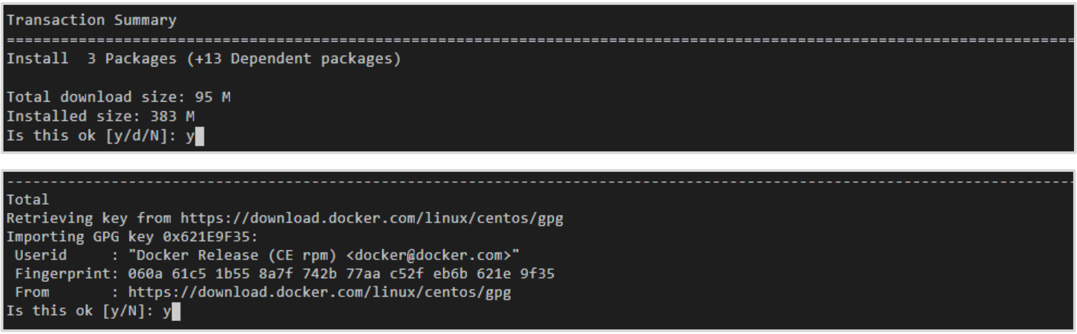
```
[root@ecs-docker ~]# yum install docker-ce docker-ce-cli containerd.io
```



```
[root@ecs-docker ~]# yum install docker-ce docker-ce-cli containerd.io
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
docker-ce-stable
(1/2): docker-ce-stable/7/x86_64/updateinfo
(2/2): docker-ce-stable/7/x86_64/primary_db
Resolving Dependencies
--> Running transaction check
---> Package containerd.io.x86_64 0:1.5.11-3.1.el7 will be installed
--> Processing Dependency: container-selinux >= 2:2.74 for package: containerd.io-1.5.11-3.1.el7.x86_64
---> Package docker-ce.x86_64 3:20.10.14-3.el7 will be installed
```

Figure 6-8

Step 5 Enter **y** twice.

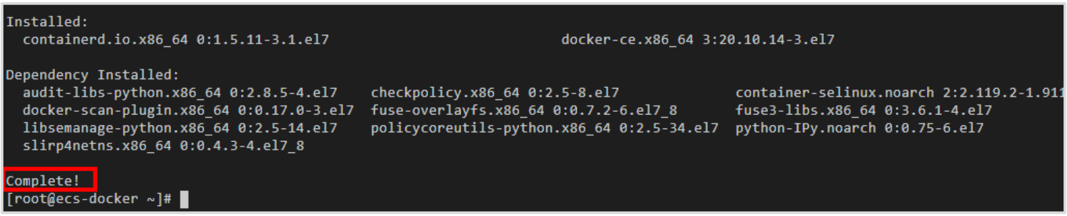


```
Transaction Summary
================================================================================================================
Install  3 Packages (+13 Dependent packages)

Total download size: 95 M
Installed size: 383 M
Is this ok [y/d/N]: y
```

```
----------------------------------------------------------------------------------------------------------------
Total
Retrieving key from https://download.docker.com/linux/centos/gpg
Importing GPG key 0x621E9F35:
 Userid     : "Docker Release (CE rpm) <docker@docker.com>"
 Fingerprint: 060a 61c5 1b55 8a7f 742b 77aa c52f eb6b 621e 9f35
 From       : https://download.docker.com/linux/centos/gpg
Is this ok [y/N]: y
```

Figure 6-9

Step 6 If **Complete!** is displayed, the installation is complete.

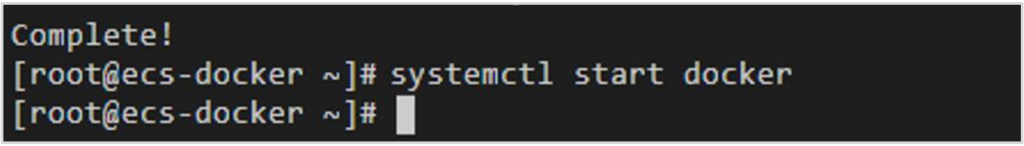


```
Installed:
  containerd.io.x86_64 0:1.5.11-3.1.el7                          docker-ce.x86_64 3:20.10.14-3.el7

Dependency Installed:
  audit-libs-python.x86_64 0:2.8.5-4.el7    checkpolicy.x86_64 0:2.5-8.el7            container-selinux.noarch 2:2.119.2-1.911
  docker-scan-plugin.x86_64 0:0.17.0-3.el7  fuse-overlayfs.x86_64 0:0.7.2-6.el7_8      fuse3-libs.x86_64 0:3.6.1-4.el7
  libsemanage-python.x86_64 0:2.5-14.el7    policycoreutils-python.x86_64 0:2.5-34.el7 python-IPy.noarch 0:0.75-6.el7
  slirp4netns.x86_64 0:0.4.3-4.el7_8

Complete!
[root@ecs-docker ~]#
```

Figure 6-10

Step 7 Run the following command to start Docker:

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

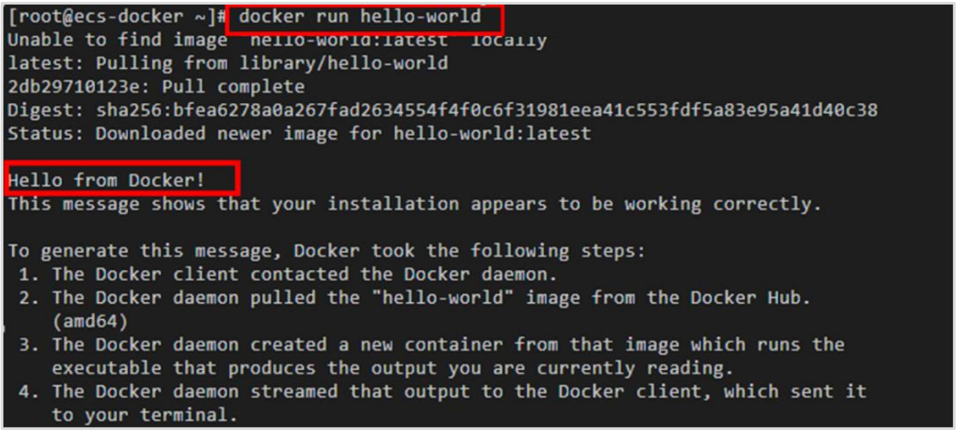


```
Complete!
[root@ecs-docker ~]# systemctl start docker
[root@ecs-docker ~]#
```

Figure 6-11

Step 8 Run the following command to check whether the Docker engine works properly: If **Hello from Docker** is displayed, the Docker engine is working properly.

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



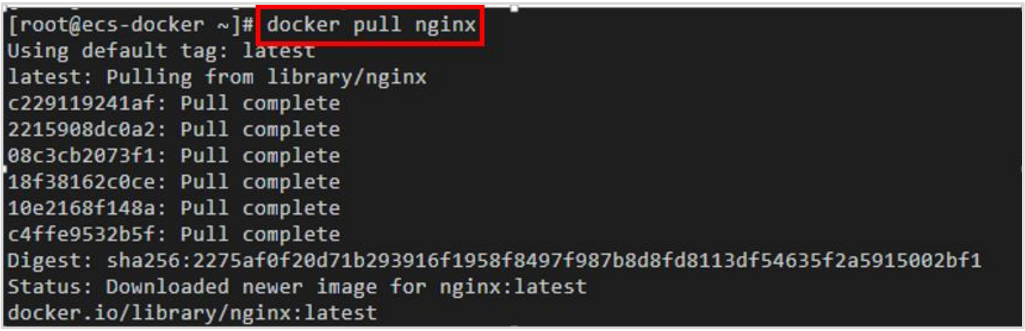
```
[root@ecs-docker ~]# docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
2db29710123e: Pull complete
Digest: sha256:bfea6278a0a267fad2634554f4f0c6f31981eea41c553fdf5a83e95a41d40c38
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.
```

Figure 6-12

6.2.1.5 Pulling and Viewing the Image

Step 1 Run the following command to pull the Nginx image:

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

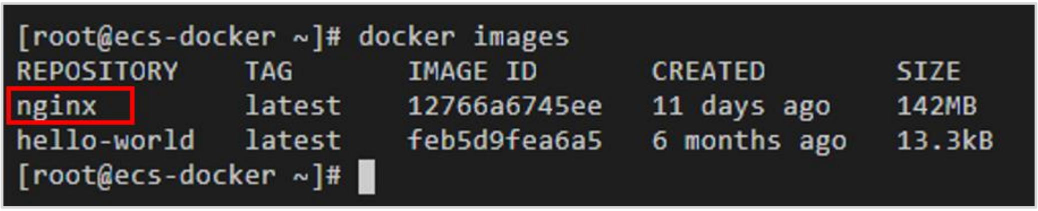


```
[root@ecs-docker ~]# docker pull nginx
Using default tag: latest
latest: Pulling from library/nginx
c229119241af: Pull complete
2215908dc0a2: Pull complete
08c3cb2073f1: Pull complete
18f38162c0ce: Pull complete
10e2168f148a: Pull complete
c4ffe9532b5f: Pull complete
Digest: sha256:2275af0f20d71b293916f1958f8497f987b8d8fd8113df54635f2a5915002bf1
Status: Downloaded newer image for nginx:latest
docker.io/library/nginx:latest
```

Figure 6-13

Step 2 Run the following command to view the local image:

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



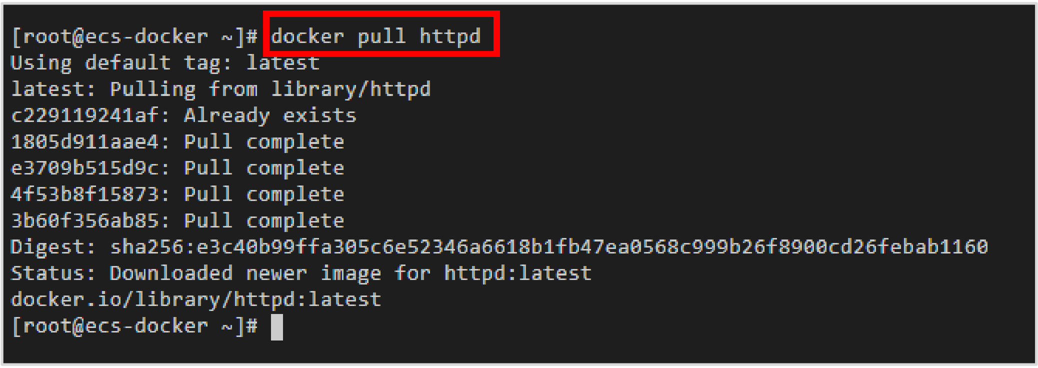
```
[root@ecs-docker ~]# docker images
REPOSITORY     TAG       IMAGE ID       CREATED        SIZE
nginx          latest    12766a6745ee   11 days ago    142MB
hello-world    latest    feb5d9fea6a5   6 months ago   13.3kB
[root@ecs-docker ~]#
```

Figure 6-14

6.2.1.6 Deploying Containers to Provide Web Services

Step 1 Run the following command to pull the httpd image to the local host:

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

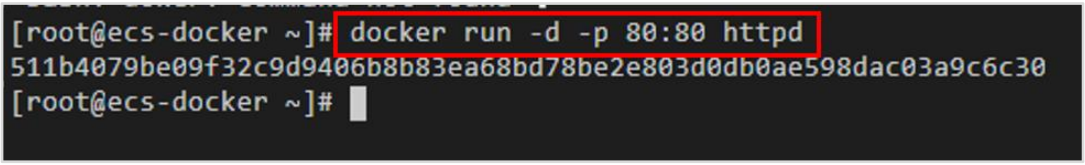


```
[root@ecs-docker ~]# docker pull httpd
Using default tag: latest
latest: Pulling from library/httpd
c229119241af: Already exists
1805d911aae4: Pull complete
e3709b515d9c: Pull complete
4f53b8f15873: Pull complete
3b60f356ab85: Pull complete
Digest: sha256:e3c40b99ffa305c6e52346a6618b1fb47ea0568c999b26f8900cd26febab1160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

Figure 6-15

Step 2 Run the following command to run the image as a container in the background and map port 80 of the container to port 80 of the host:

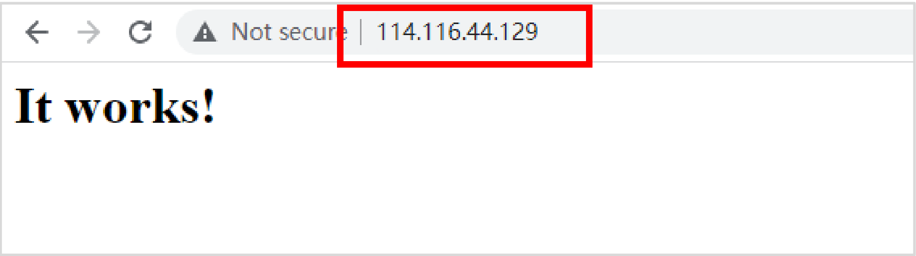
```
[root@ecs-docker ~]# docker run -d -p 80:80 httpd
```



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

Figure 6-16

Step 3 Log in to the public network address of ecs-docker.



It works!

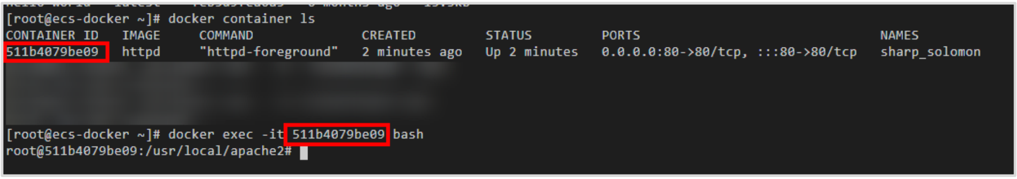
Figure 6-17

6.2.1.7 Building an Image Using a Dockerfile

Step 1 Run the following commands to access the container (the CLI becomes the interactive terminal) and view the HTML file path:

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

Note: **511b4079be09** indicates the container ID.

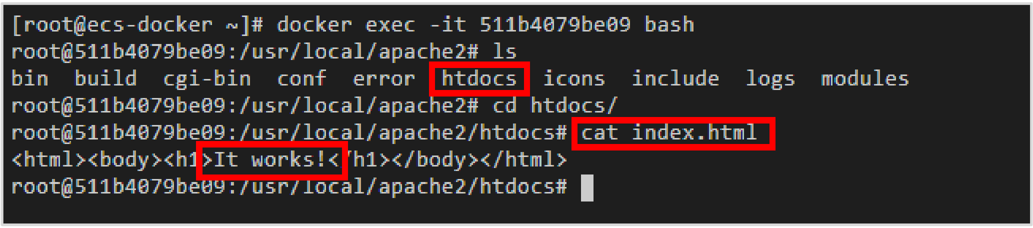


```
[root@ecs-docker ~]# docker container ls
CONTAINER ID   IMAGE     COMMAND              CREATED         STATUS         PORTS                               NAMES
511b4079be09   httpd     "httpd-foreground"   2 minutes ago   Up 2 minutes   0.0.0.0:80->80/tcp, :::80->80/tcp   sharp_solomon
[redacted]

[root@ecs-docker ~]# docker exec -it 511b4079be09 bash
root@511b4079be09:/usr/local/apache2#
```

Figure 6-18

Step 2 Run **cat** to view the **index.html** file in the **htdocs** directory. **It works** is displayed on the web page. Record file directory: **/usr/local/apache2/htdocs**.

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

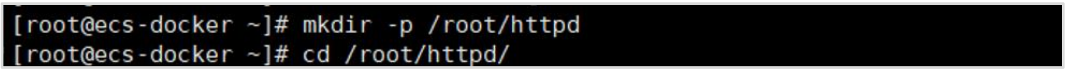


```
[root@ecs-docker ~]# docker exec -it 511b4079be09 bash
root@511b4079be09:/usr/local/apache2# ls
bin  build  cgi-bin  conf  error  htdocs  icons  include  logs  modules
root@511b4079be09:/usr/local/apache2# cd htdocs/
root@511b4079be09:/usr/local/apache2/htdocs# cat index.html
<html><body><h1>It works!</h1></body></html>
root@511b4079be09:/usr/local/apache2/htdocs#
```

Figure 6-19

Step 3 Run **exit** to exit the container and run the following commands to create an HTML file in the new path:

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

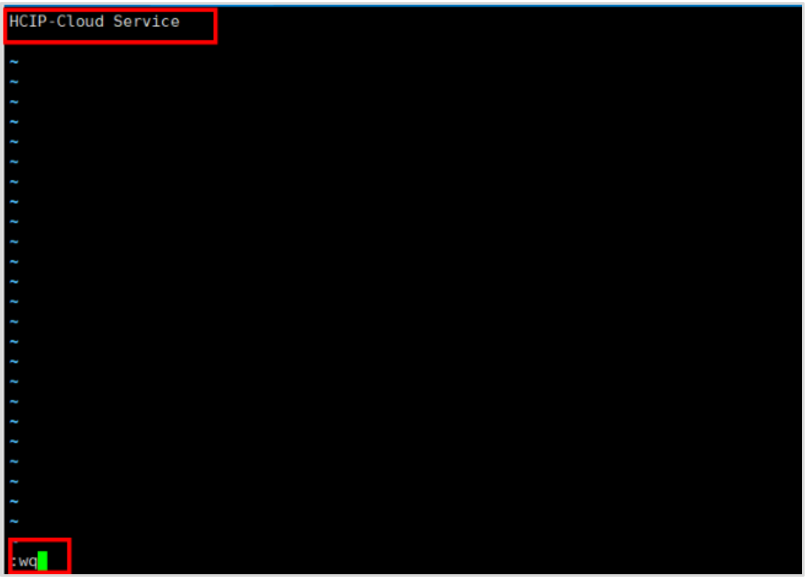


```
[root@ecs-docker ~]# mkdir -p /root/httpd
[root@ecs-docker ~]# cd /root/httpd/
```

Figure 6-20

Step 4 Run the following commands to create and edit the HTML file and write **HCIP-Cloud Service** to the file:

```
[root@ecs-docker httpd]# vi index.html                          # Create an HTML file.
HCIP-Cloud Service                                               # Fill in the HTML file.
```

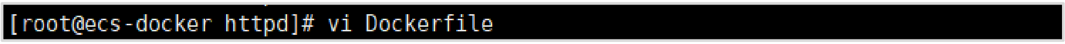


```
HCIP-Cloud Service
~
~
:wq
```

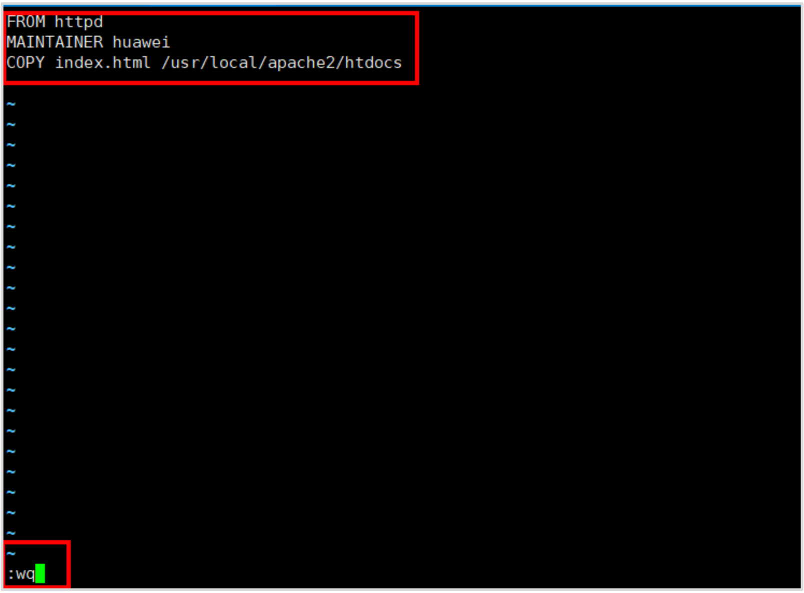
Figure 6-21

Step 5 Run the following commands to create and edit the Dockerfile:

```
[root@ecs-docker httpd]# vi Dockerfile                 # Create a Dockerfile
FROM httpd
MAINTAINER huawei
COPY index.html /usr/local/apache2/htdocs
```



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

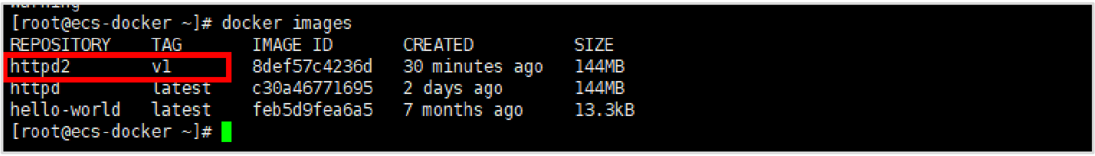


```
FROM httpd
MAINTAINER huawei
COPY index.html /usr/local/apache2/htdocs
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq
```

Figure 6-22

Step 6 Run the following commands to build a new image httpd2 using the Dockerfile:

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

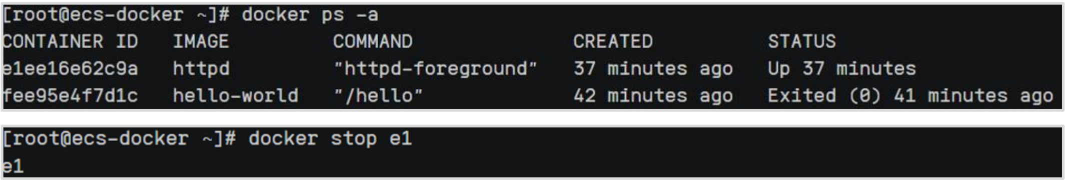


```
[root@ecs-docker ~]# docker images
REPOSITORY     TAG        IMAGE ID       CREATED          SIZE
httpd2         v1         8def57c4236d   30 minutes ago   144MB
httpd          latest     c30a46771695   2 days ago       144MB
hello-world    latest     feb5d9fea6a5   7 months ago     13.3kB
[root@ecs-docker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

Figure 6-23

Step 7 Run the following commands to stop the httpd container:

```
[root@ecs-docker ~]# docker ps -a                        # View the container list and find the ID of the httpd container.
[root@ecs-docker ~]# docker stop e1                      # Stop the httpd container. e1 is the ID of the httpd container.
```



```
[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
```

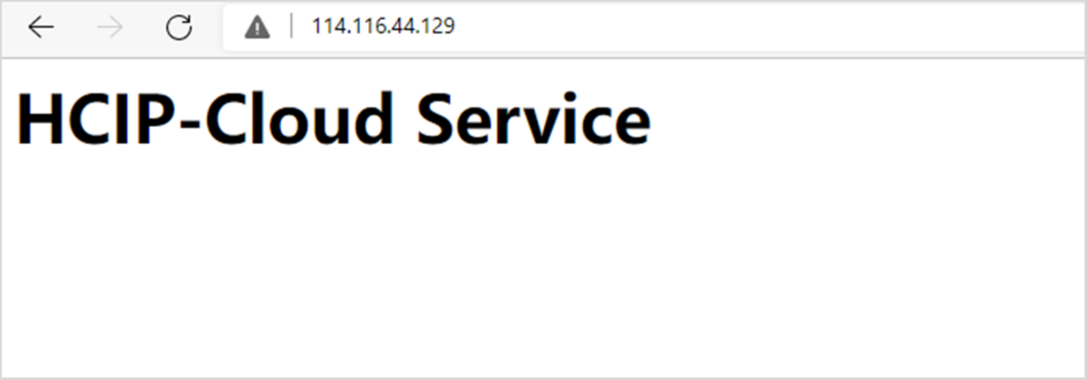
```
[root@ecs-docker ~]# docker stop e1
e1
```

Figure 6-24

Step 8 Run the following command to run the image as a container:

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

Step 9 Log in to the public network address of ecs-docker again and view the content. If the following information is displayed, the Dockerfile image is successfully built.



114.116.44.129

HCIP-Cloud Service

Figure 6-25

6.2.1.8 Pushing an Image to SWR

Step 1 In the service list, choose **SoftWare Repository for Container** > **Create Organization**.

Note: You need to push the created image to the organization.

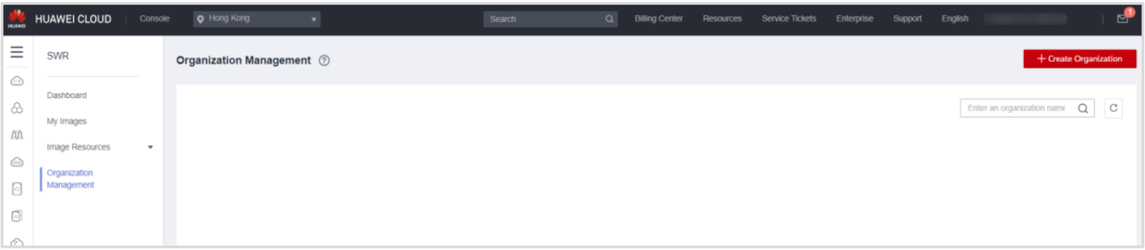
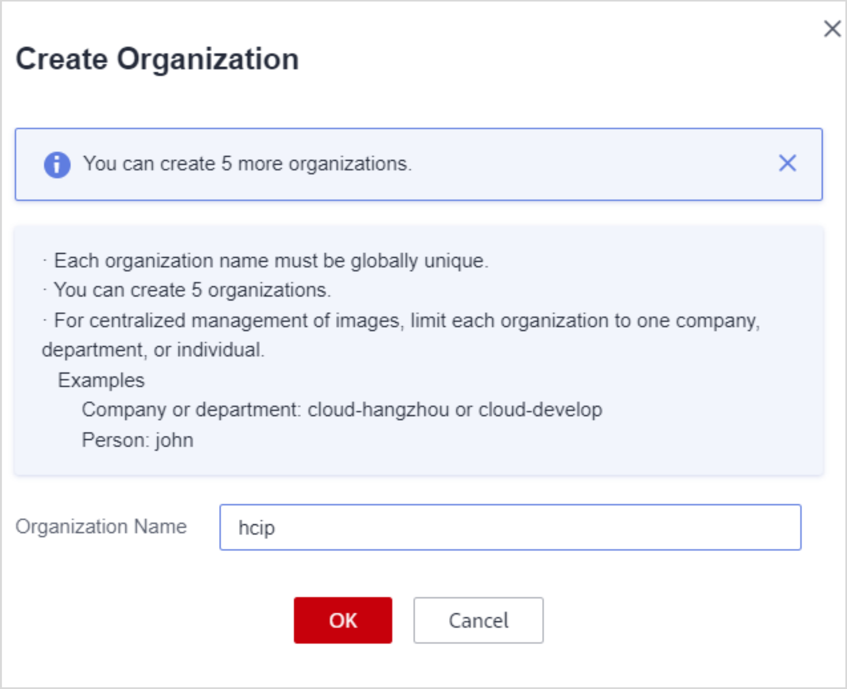


Figure 6-26

Step 2 Enter the organization name **hcip** (which is user-defined) and click **OK**.



Create Organization

You can create 5 more organizations.

- Each organization name must be globally unique.
- You can create 5 organizations.
- For centralized management of images, limit each organization to one company, department, or individual.

  Examples

  Company or department: cloud-hangzhou or cloud-develop

  Person: john

Organization Name: hcip

Figure 6-27

Step 3 Click **Generate Login Command** in the upper right corner to obtain the command.

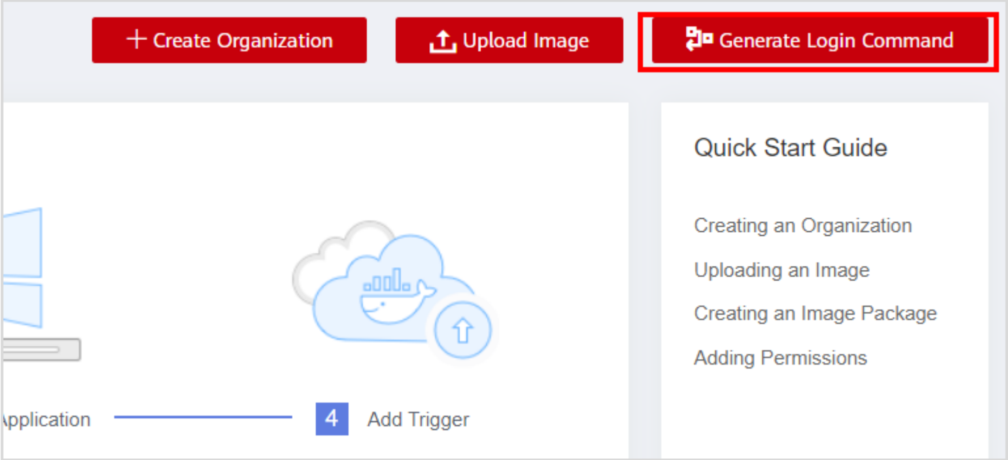
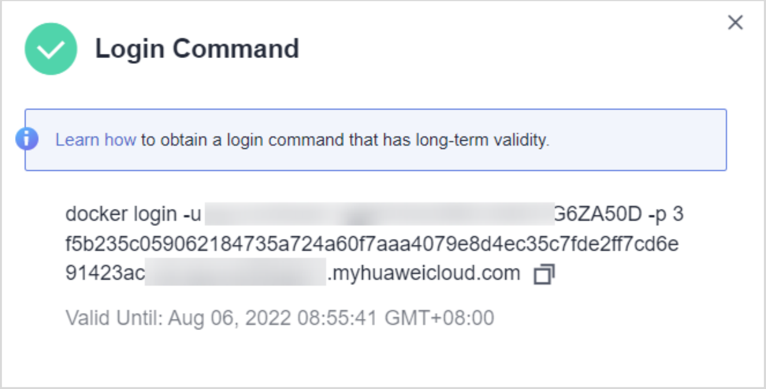


Figure 6-28

Step 4 Copy the login command.



Login Command

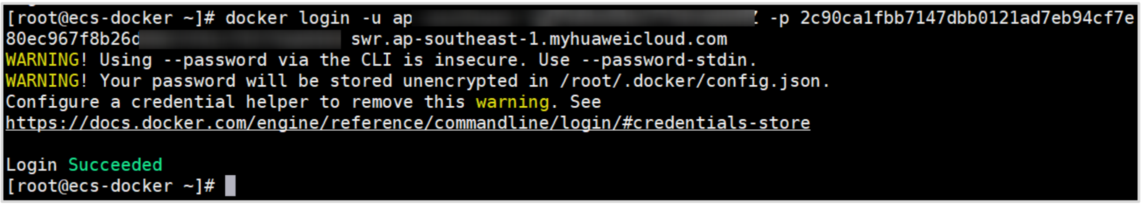
Learn how to obtain a login command that has long-term validity.

docker login -u [redacted]G6ZA50D -p 3
f5b235c059062184735a724a60f7aaa4079e8d4ec35c7fde2ff7cd6e
91423ac[redacted].myhuaweicloud.com

Valid Until: Aug 06, 2022 08:55:41 GMT+08:00

Figure 6-29

Step 5 Use Huawei Cloud CloudShell to log in to ecs-docker and run the recorded login command.

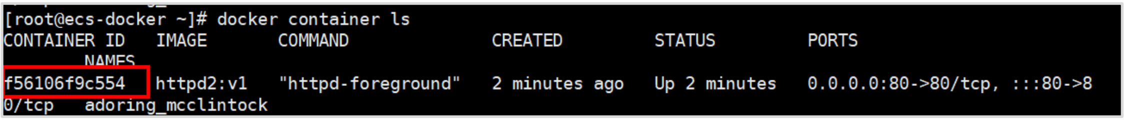


```
[root@ecs-docker ~]# docker login -u ap[redacted] -p 2c90ca1fbb7147dbb0121ad7eb94cf7e
80ec967f8b26d[redacted] swr.ap-southeast-1.myhuaweicloud.com
WARNING! Using --password via the CLI is insecure. Use --password-stdin.
WARNING! Your password will be stored unencrypted in /root/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
[root@ecs-docker ~]#
```

Figure 6-30

Step 6 After the login is successful, run the following command on the node to view the ID of the **httpd2:v1** container:

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

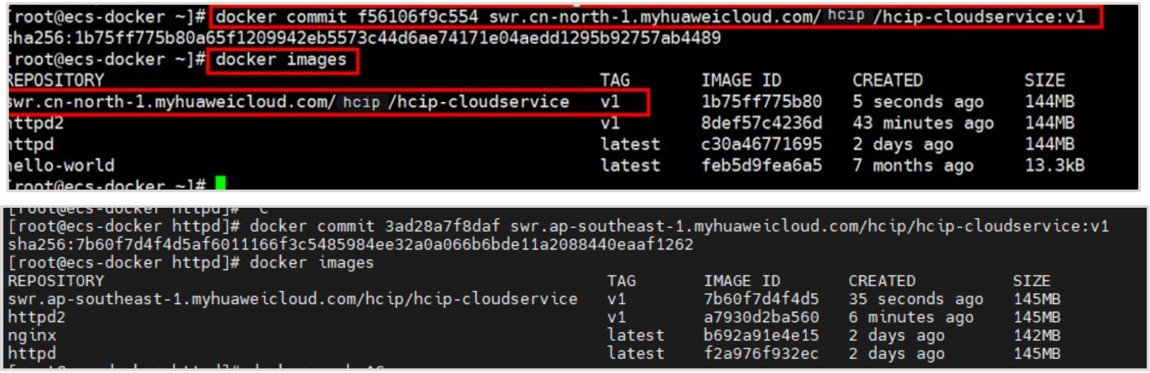


```
[root@ecs-docker ~]# docker container ls
CONTAINER ID   IMAGE       COMMAND              CREATED         STATUS         PORTS
        NAMES
f56106f9c554   httpd2:v1   "httpd-foreground"   2 minutes ago   Up 2 minutes   0.0.0.0:80->80/tcp, :::80->8
0/tcp    adoring_mcclintock
```

Figure 6-31

Step 7 Pack the **httpd2:v1** container into an image and change the image tag.

```
[root@ecs-docker ~]# docker commit f56106f9c554  swr.ap-southeast-1.myhuaweicloud.com/hcip/hcip-cloudservice:v1
#f56106f9c554: container ID
#swr.cn-north-1.myhuaweicloud.com: SWR address, which can be confirmed by viewing the last part of the login command.
#hcip: organization name
#hcip-cloudservice:v1: Image name: Tag
[root@ecs-docker ~]# docker images
```



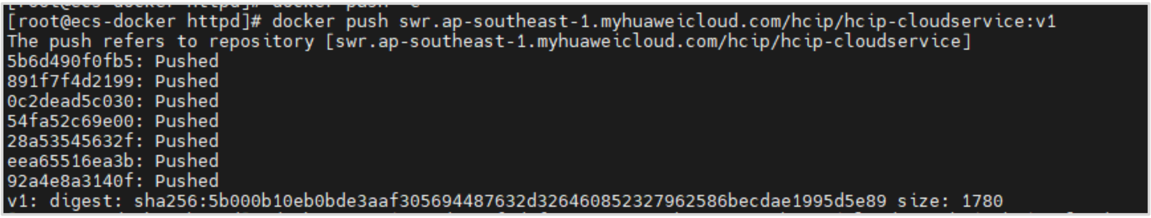
```
[root@ecs-docker ~]# docker commit f56106f9c554 swr.cn-north-1.myhuaweicloud.com/ hcip /hcip-cloudservice:v1
sha256:1b75ff775b80a65f1209942eb5573c44d6ae74171e04aedd1295b92757ab4489
[root@ecs-docker ~]# docker images
REPOSITORY                                           TAG       IMAGE ID       CREATED          SIZE
swr.cn-north-1.myhuaweicloud.com/ hcip /hcip-cloudservice    v1        1b75ff775b80   5 seconds ago    144MB
httpd2                                               v1        8def57c4236d   43 minutes ago   144MB
httpd                                                latest    c30a46771695   2 days ago       144MB
hello-world                                          latest    feb5d9fea6a5   7 months ago     13.3kB
[root@ecs-docker ~]#
```

```
[root@ecs-docker httpd]# docker commit 3ad28a7f8daf swr.ap-southeast-1.myhuaweicloud.com/hcip/hcip-cloudservice:v1
sha256:7b60f7d4f4d5af6011166f3c5485984ee32a0a066b6bde11a2088440eaaf1262
[root@ecs-docker httpd]# docker images
REPOSITORY                                           TAG       IMAGE ID       CREATED          SIZE
swr.ap-southeast-1.myhuaweicloud.com/hcip/hcip-cloudservice   v1        7b60f7d4f4d5   35 seconds ago   145MB
httpd2                                               v1        a7930d2ba560   6 minutes ago    145MB
nginx                                                latest    b692a91e4e15   2 days ago       142MB
httpd                                                latest    f2a976f932ec   2 days ago       145MB
```

Figure 6-32

Step 8 Run the following command to push the image to SWR:

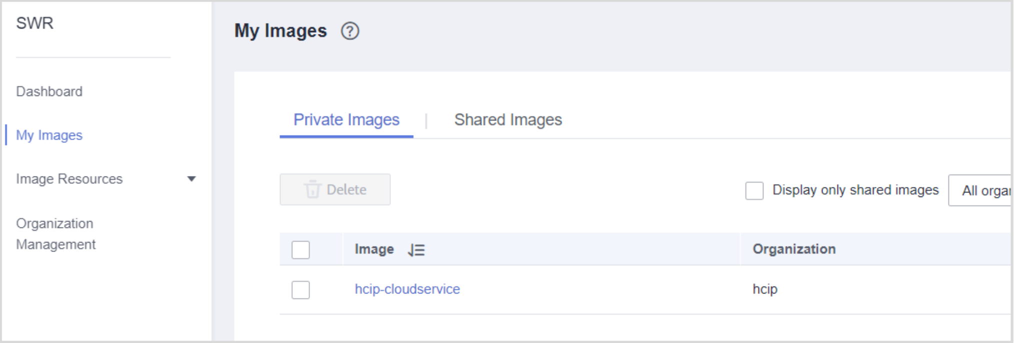
```
[root@ecs-docker ~]# docker push swr.ap-southeast-1.myhuaweicloud.com/hcip/hcip-cloudservice:v1
```



```
[root@ecs-docker httpd]# docker push swr.ap-southeast-1.myhuaweicloud.com/hcip/hcip-cloudservice:v1
The push refers to repository [swr.ap-southeast-1.myhuaweicloud.com/hcip/hcip-cloudservice]
5b6d490f0fb5: Pushed
891f7f4d2199: Pushed
0c2dead5c030: Pushed
54fa52c69e00: Pushed
28a53545632f: Pushed
eea65516ea3b: Pushed
92a4e8a3140f: Pushed
v1: digest: sha256:5b000b10eb0bde3aaf305694487632d326460852327962586becdae1995d5e89 size: 1780
```

Figure 6-33

Step 9 Log in to SWR and view the image. If the following information is displayed, the image is successfully pushed. Click the image name to view image details.



SWR

Dashboard

My Images

Image Resources

Organization Management

My Images

Private Images | Shared Images

Delete

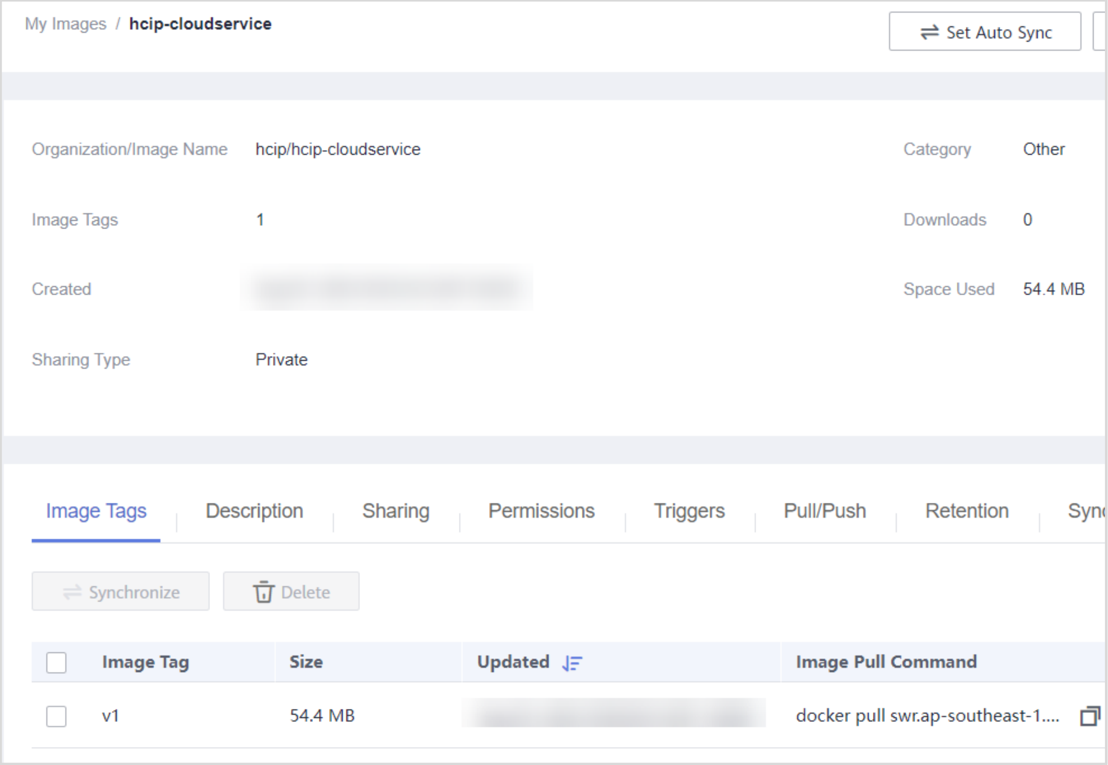
☐ Display only shared images

All orga

☐	Image	Organization
☐	hcip-cloudservice	hcip

Figure 6-34

Step 10 On the details page, the current image tag is **v1**.



My Images / **hcip-cloudservice**

Set Auto Sync

Organization/Image Name	hcip/hcip-cloudservice	Category	Other
Image Tags	1	Downloads	0
Created	[redacted]	Space Used	54.4 MB
Sharing Type	Private		

Image Tags | Description | Sharing | Permissions | Triggers | Pull/Push | Retention | Sync

Synchronize Delete

☐	Image Tag	Size	Updated	Image Pull Command
☐	v1	54.4 MB	[redacted]	docker pull swr.ap-southeast-1....

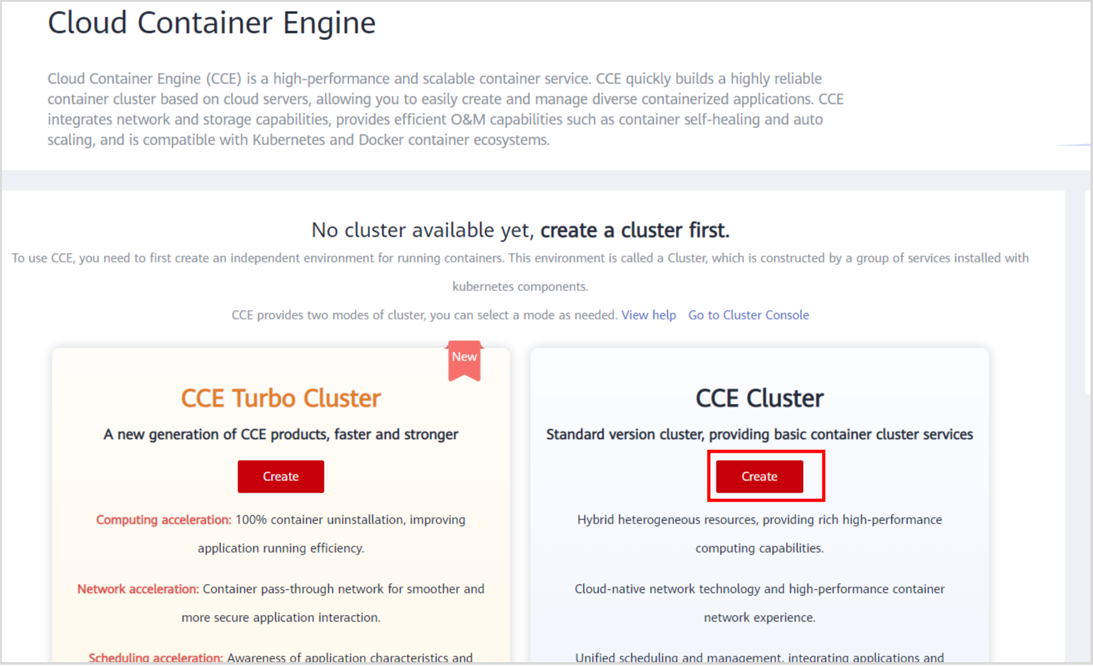
Figure 6-35

6.2.1.9 Creating a CCE and Deploying a Container

Step 1 Log in to Huawei Cloud, click **Cloud Container Engine** in the service list.

Step 2 On the CCE console, click **Create**.

Note: You need to use this cluster to pull the image and use it to deploy the container.



Cloud Container Engine

Cloud Container Engine (CCE) is a high-performance and scalable container service. CCE quickly builds a highly reliable container cluster based on cloud servers, allowing you to easily create and manage diverse containerized applications. CCE integrates network and storage capabilities, provides efficient O&M capabilities such as container self-healing and auto scaling, and is compatible with Kubernetes and Docker container ecosystems.

No cluster available yet, **create a cluster first.**

To use CCE, you need to first create an independent environment for running containers. This environment is called a Cluster, which is constructed by a group of services installed with kubernetes components.

CCE provides two modes of cluster, you can select a mode as needed. View help Go to Cluster Console

CCE Turbo Cluster

A new generation of CCE products, faster and stronger

Computing acceleration: 100% container uninstallation, improving application running efficiency.

Network acceleration: Container pass-through network for smoother and more secure application interaction.

Scheduling acceleration: Awareness of application characteristics and

CCE Cluster

Standard version cluster, providing basic container cluster services

Hybrid heterogeneous resources, providing rich high-performance computing capabilities.

Cloud-native network technology and high-performance container network experience.

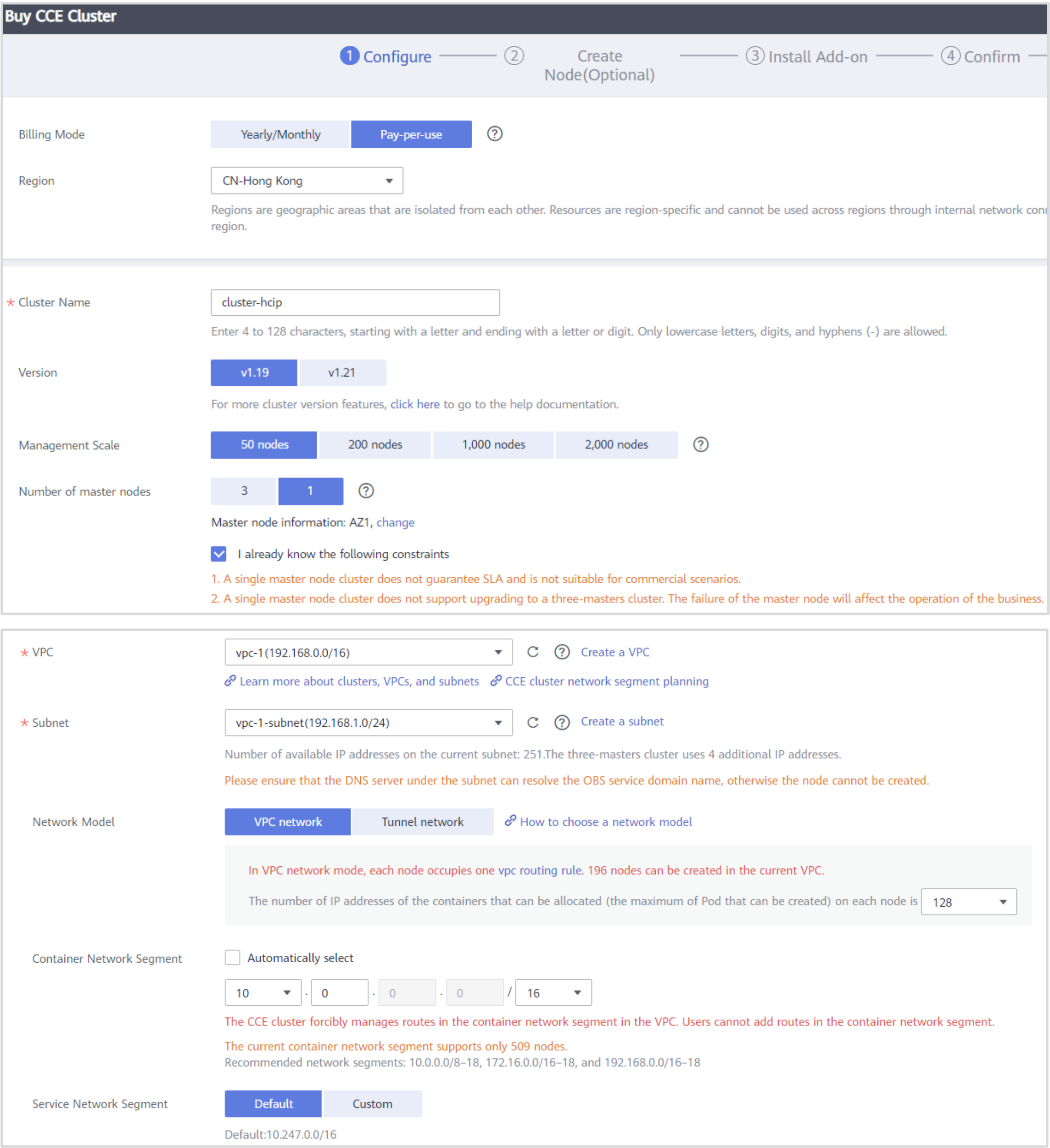
Unified scheduling and management, integrating applications and

Figure 6-36

Step 3 Set CCE cluster parameters as follows:

CCE cluster:

- **Billing Mode**: **Pay-per-use**
- **Cluster Name**: **cluster-hcip** (user-defined)
- **Version**: **v1.19**
- **Management Scale**: **50 nodes**
- **Number of master nodes**: **1**
- **Network Model**: **VPC network**
- **VPC**: **vpc-1**
- **Subnet**: **vpc-1-subnet**
- **Container Network Segment**: **10.10.0.0/16**
- **Service Network Segment**: **Default**



Buy CCE Cluster

1 Configure —— 2 Create Node(Optional) —— 3 Install Add-on —— 4 Confirm

Billing Mode: Yearly/Monthly | **Pay-per-use**

Region: CN-Hong Kong

Regions are geographic areas that are isolated from each other. Resources are region-specific and cannot be used across regions through internal network con region.

* Cluster Name: cluster-hcip

Enter 4 to 128 characters, starting with a letter and ending with a letter or digit. Only lowercase letters, digits, and hyphens (-) are allowed.

Version: **v1.19** | v1.21

For more cluster version features, click here to go to the help documentation.

Management Scale: **50 nodes** | 200 nodes | 1,000 nodes | 2,000 nodes

Number of master nodes: 3 | **1**

Master node information: AZ1, change

☑ I already know the following constraints

1. A single master node cluster does not guarantee SLA and is not suitable for commercial scenarios.
2. A single master node cluster does not support upgrading to a three-masters cluster. The failure of the master node will affect the operation of the business.

* VPC: vpc-1(192.168.0.0/16) Create a VPC

Learn more about clusters, VPCs, and subnets   CCE cluster network segment planning

* Subnet: vpc-1-subnet(192.168.1.0/24) Create a subnet

Number of available IP addresses on the current subnet: 251.The three-masters cluster uses 4 additional IP addresses.

Please ensure that the DNS server under the subnet can resolve the OBS service domain name, otherwise the node cannot be created.

Network Model: **VPC network** | Tunnel network   How to choose a network model

In VPC network mode, each node occupies one vpc routing rule. 196 nodes can be created in the current VPC.

The number of IP addresses of the containers that can be allocated (the maximum of Pod that can be created) on each node is 128

Container Network Segment: □ Automatically select

10 . 0 . 0 . 0 / 16

The CCE cluster forcibly manages routes in the container network segment in the VPC. Users cannot add routes in the container network segment.

The current container network segment supports only 509 nodes.

Recommended network segments: 10.0.0.0/8–18, 172.16.0.0/16–18, and 192.168.0.0/16–18

Service Network Segment: **Default** | Custom

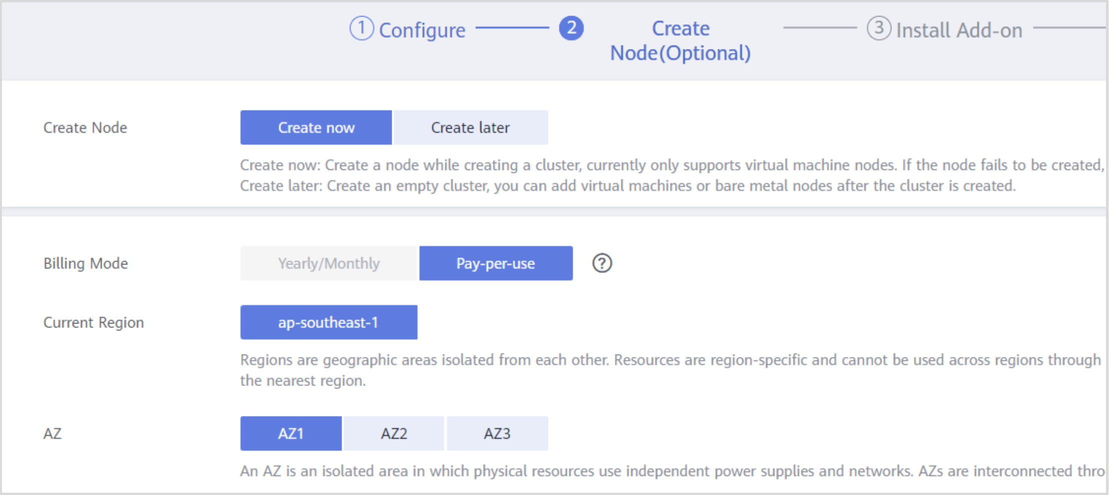
Default:10.247.0.0/16

Figure 6-37

Step 4 After the preceding configurations are complete, click **Next: Create Node**.

- Create Node: create now
- Billing Mode: Pay-per-use
- Current Region: ap-southeast-1
- AZ: default
- Node Type: VM node
- Node Name: default
- Specifications: 4 cores | 8 GB
- OS: EulerOS 2.5

- System Disk: High I/O
- Data Disk: High I/O
- Subnet: default
- EIP: Do not use
- Login Mode: Password



Create Node: Create now | Create later

Create now: Create a node while creating a cluster, currently only supports virtual machine nodes. If the node fails to be created,
Create later: Create an empty cluster, you can add virtual machines or bare metal nodes after the cluster is created.

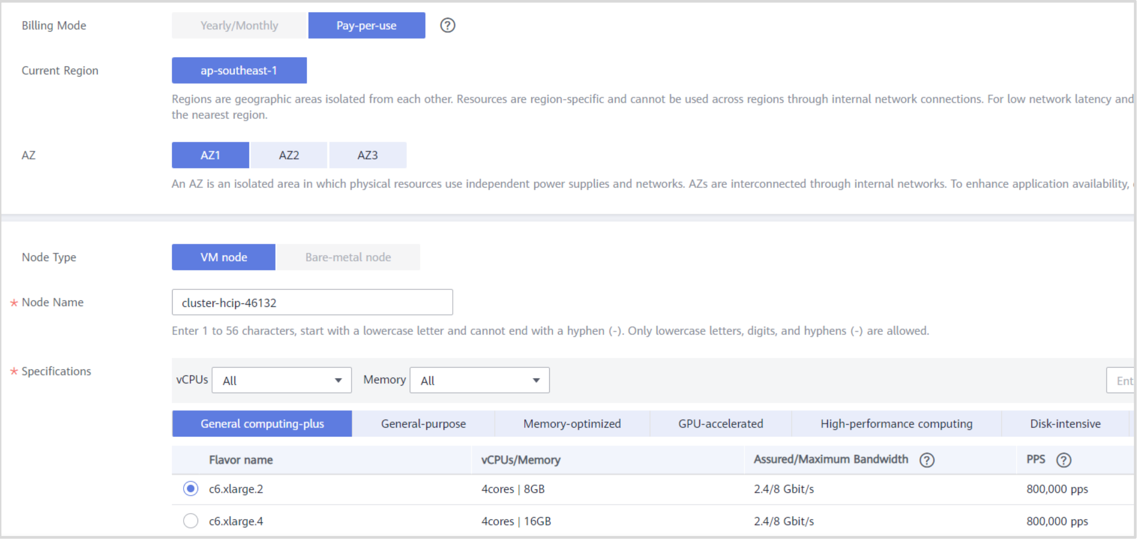
Billing Mode: Yearly/Monthly | Pay-per-use

Current Region: ap-southeast-1

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through the nearest region.

AZ: AZ1 | AZ2 | AZ3

An AZ is an isolated area in which physical resources use independent power supplies and networks. AZs are interconnected thro



Billing Mode: Yearly/Monthly | Pay-per-use

Current Region: ap-southeast-1

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and the nearest region.

AZ: AZ1 | AZ2 | AZ3

An AZ is an isolated area in which physical resources use independent power supplies and networks. AZs are interconnected through internal networks. To enhance application availability,

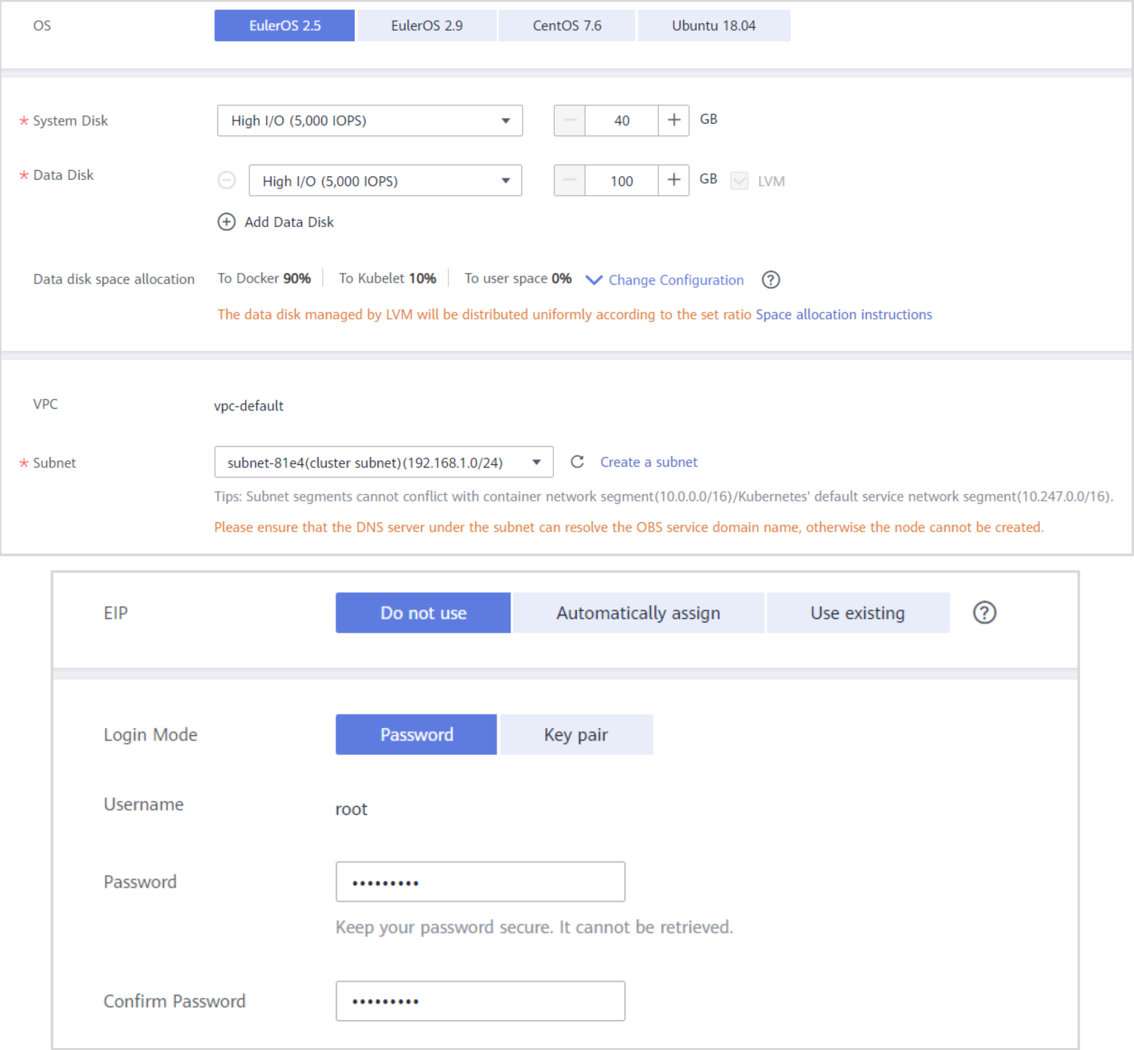
Node Type: VM node | Bare-metal node

* Node Name: cluster-hcip-46132

Enter 1 to 56 characters, start with a lowercase letter and cannot end with a hyphen (-). Only lowercase letters, digits, and hyphens (-) are allowed.

* Specifications: vCPUs All Memory All

	Flavor name	vCPUs/Memory	Assured/Maximum Bandwidth	PPS
●	c6.xlarge.2	4cores | 8GB	2.4/8 Gbit/s	800,000 pps
○	c6.xlarge.4	4cores | 16GB	2.4/8 Gbit/s	800,000 pps



OS: EulerOS 2.5 | EulerOS 2.9 | CentOS 7.6 | Ubuntu 18.04

* System Disk: High I/O (5,000 IOPS) 40 GB

* Data Disk: High I/O (5,000 IOPS) 100 GB □ LVM

Add Data Disk

Data disk space allocation: To Docker **90%** | To Kubelet **10%** | To user space **0%** Change Configuration

The data disk managed by LVM will be distributed uniformly according to the set ratio Space allocation instructions

VPC: vpc-default

* Subnet: subnet-81e4(cluster subnet)(192.168.1.0/24) Create a subnet

Tips: Subnet segments cannot conflict with container network segment(10.0.0.0/16)/Kubernetes' default service network segment(10.247.0.0/16).

Please ensure that the DNS server under the subnet can resolve the OBS service domain name, otherwise the node cannot be created.

EIP: Do not use | Automatically assign | Use existing

Login Mode: Password | Key pair

Username: root

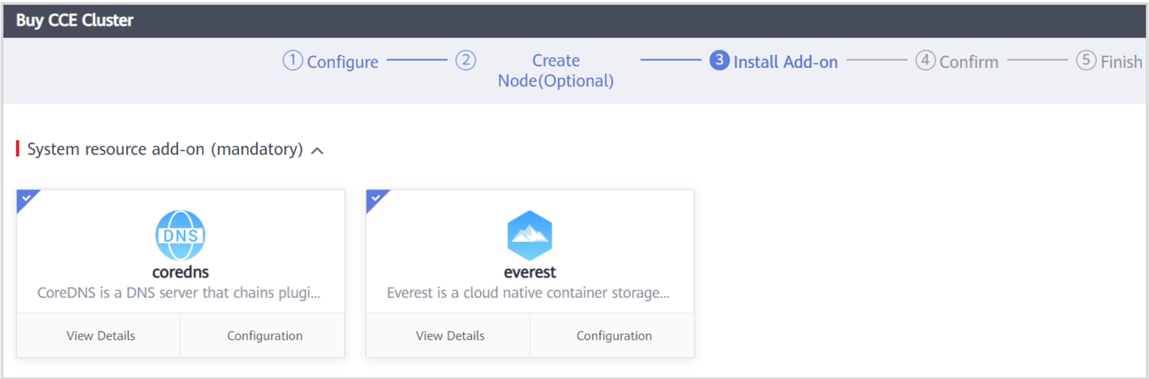
Password: •••••••••

Keep your password secure. It cannot be retrieved.

Confirm Password: •••••••••

Figure 6-38

Step 5 After the preceding configuration is complete, click **Next: Install Add-on**. Retain the default settings for the add-on.



Buy CCE Cluster

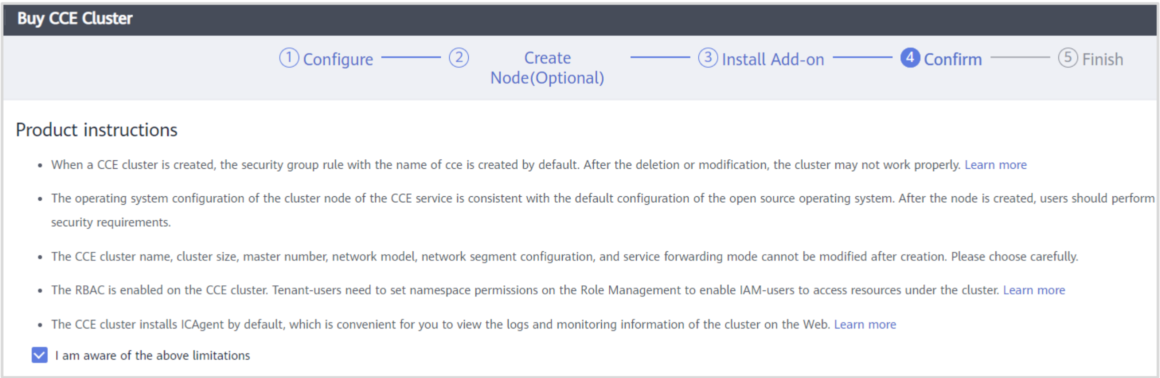
① Configure — ② Create Node(Optional) — ③ Install Add-on — ④ Confirm — ⑤ Finish

System resource add-on (mandatory)

coredns
CoreDNS is a DNS server that chains plugi...
View Details | Configuration

everest
Everest is a cloud native container storage...
View Details | Configuration

Step 6 After the preceding configuration is complete, click Next. Click **Next: Confirm**.



Buy CCE Cluster

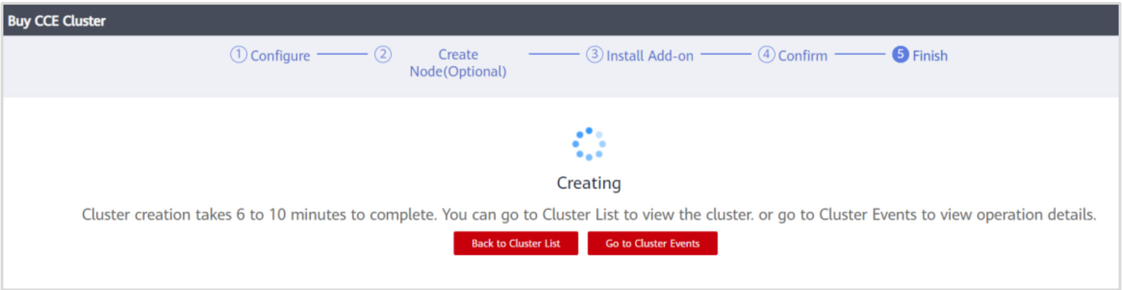
① Configure ② Create Node(Optional) ③ Install Add-on ④ Confirm ⑤ Finish

Product instructions

- When a CCE cluster is created, the security group rule with the name of cce is created by default. After the deletion or modification, the cluster may not work properly. Learn more
- The operating system configuration of the cluster node of the CCE service is consistent with the default configuration of the open source operating system. After the node is created, users should perform security requirements.
- The CCE cluster name, cluster size, master number, network model, network segment configuration, and service forwarding mode cannot be modified after creation. Please choose carefully.
- The RBAC is enabled on the CCE cluster. Tenant-users need to set namespace permissions on the Role Management to enable IAM-users to access resources under the cluster. Learn more
- The CCE cluster installs ICAgent by default, which is convenient for you to view the logs and monitoring information of the cluster on the Web. Learn more

☑ I am aware of the above limitations

Step 7 On the **Resource Management** page, select **Clusters** to view the created CCE cluster. If the cluster status is **Available**, the cluster has been created.



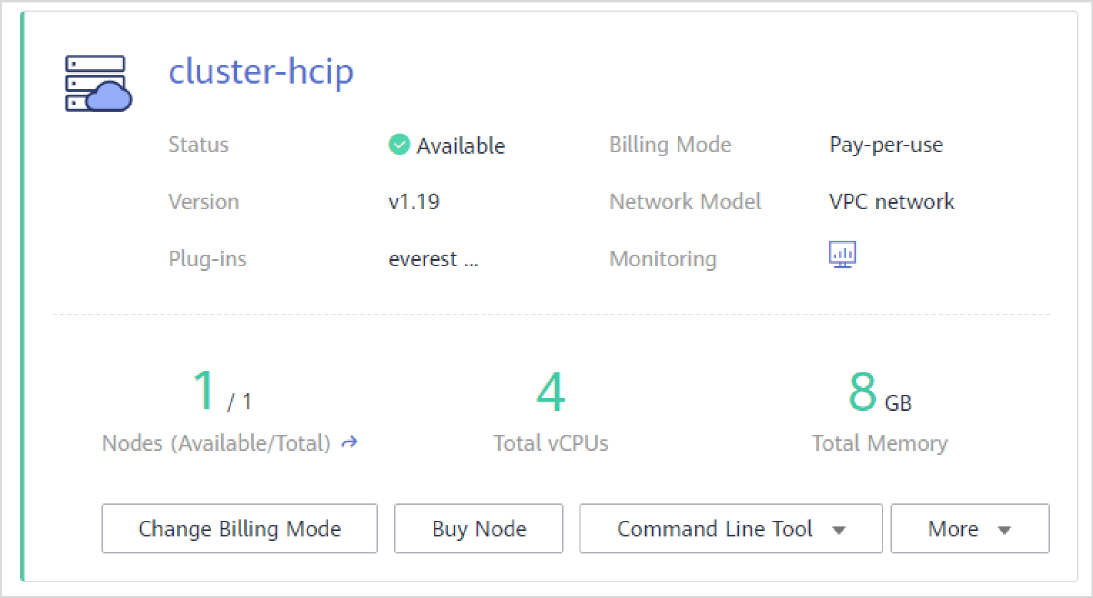
Buy CCE Cluster

① Configure ② Create Node(Optional) ③ Install Add-on ④ Confirm ⑤ Finish

Creating

Cluster creation takes 6 to 10 minutes to complete. You can go to Cluster List to view the cluster. or go to Cluster Events to view operation details.

Back to Cluster List
Go to Cluster Events



cluster-hcip

Status	Available	Billing Mode	Pay-per-use
Version	v1.19	Network Model	VPC network
Plug-ins	everest ...	Monitoring	

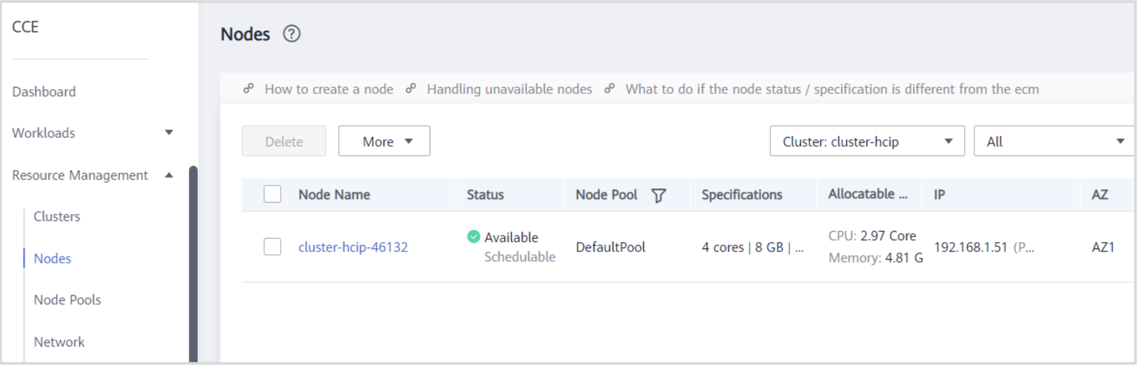
1 / 1 Nodes (Available/Total)

4 Total vCPUs

8 GB Total Memory

Figure 6-39

Step 8 Click **Nodes** on the left to check the status of the new node.

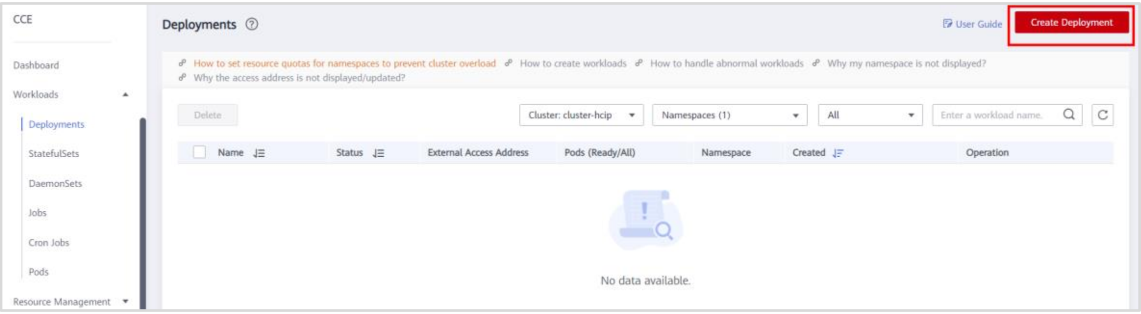


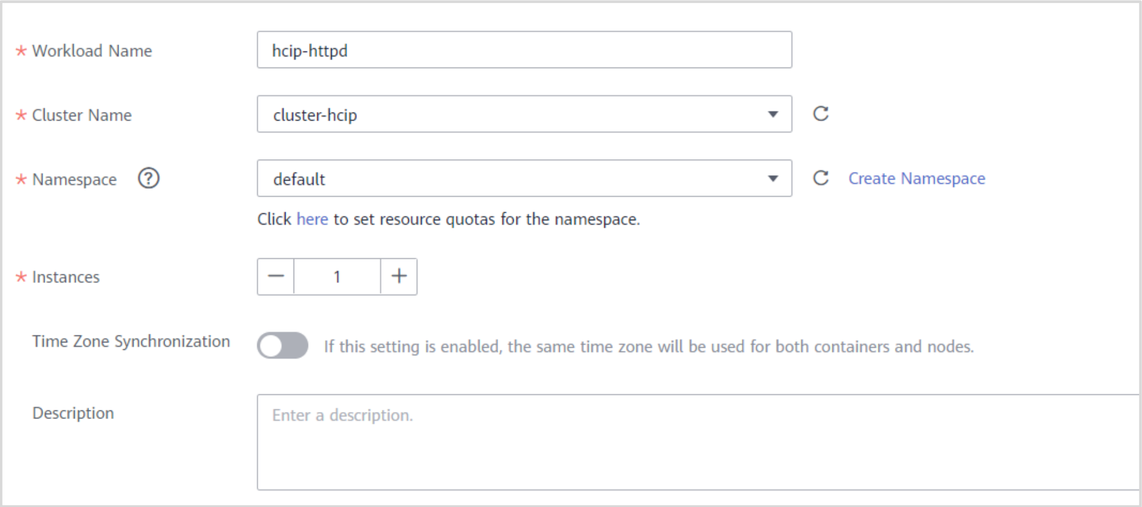
Node Name	Status	Node Pool	Specifications	Allocatable ...	IP	AZ
cluster-hcip-46132	Available Schedulable	DefaultPool	4 cores | 8 GB | ...	CPU: 2.97 Core Memory: 4.81 G	192.168.1.51 (P...	AZ1

Figure 6-40

Step 9 Choose **Workloads** > **Deployments** on the left, click **Create Deployment** in the upper right corner, and set the following parameters to create a workload.

- **Workload Name**: **hcip-httpd** (user-defined)
- **Namespace**: **default**
- Set **Instances** to **1**.
- **Select Container Image**： **My Images** | **hcip-cloud service**
- **Image Version**： v1
- **Container Name**: **container-httpd** (user-defined)





* Workload Name: hcip-httpd

* Cluster Name: cluster-hcip

* Namespace: default

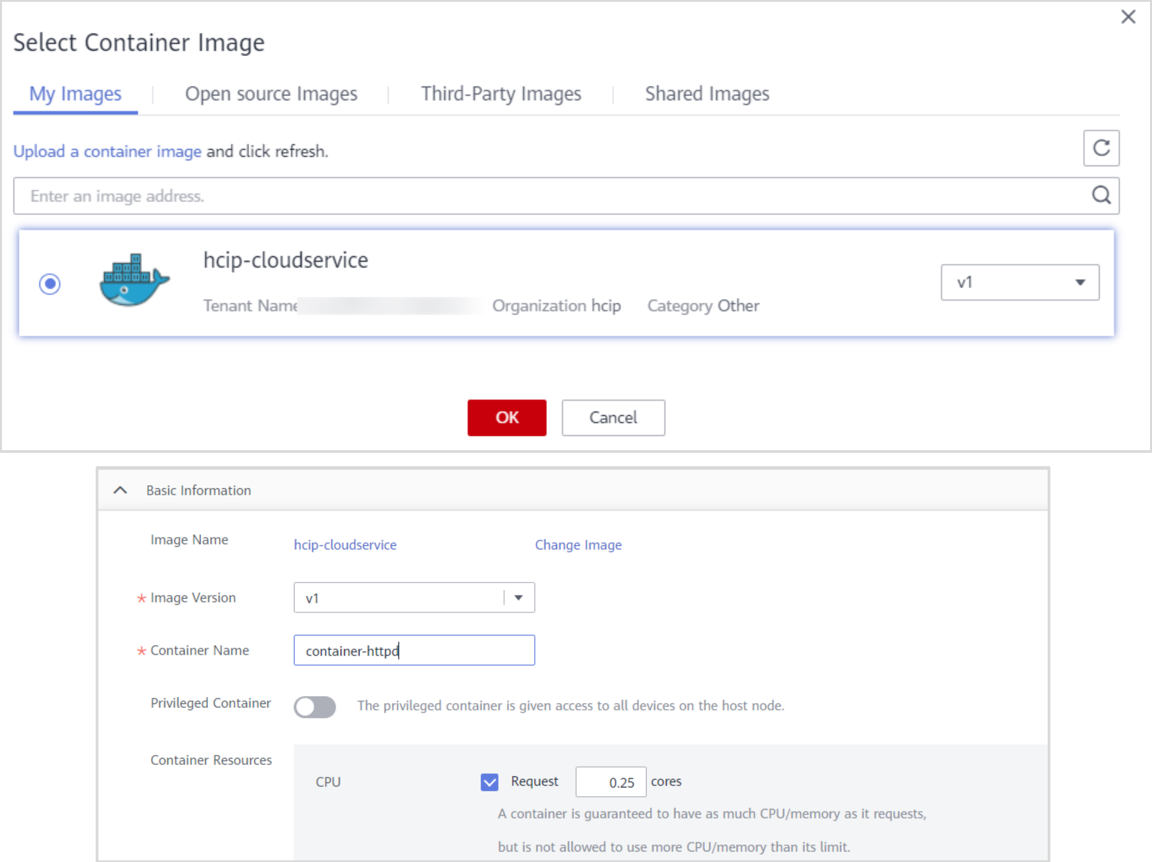
Create Namespace

Click here to set resource quotas for the namespace.

* Instances: 1

Time Zone Synchronization: If this setting is enabled, the same time zone will be used for both containers and nodes.

Description: Enter a description.



Select Container Image

My Images | Open source Images | Third-Party Images | Shared Images

Upload a container image and click refresh.

Enter an image address.

● hcip-cloudservice
Tenant Name [redacted] Organization hcip Category Other
v1

OK Cancel

Basic Information

Image Name: hcip-cloudservice Change Image

* Image Version: v1

* Container Name: container-httpd

Privileged Container: The privileged container is given access to all devices on the host node.

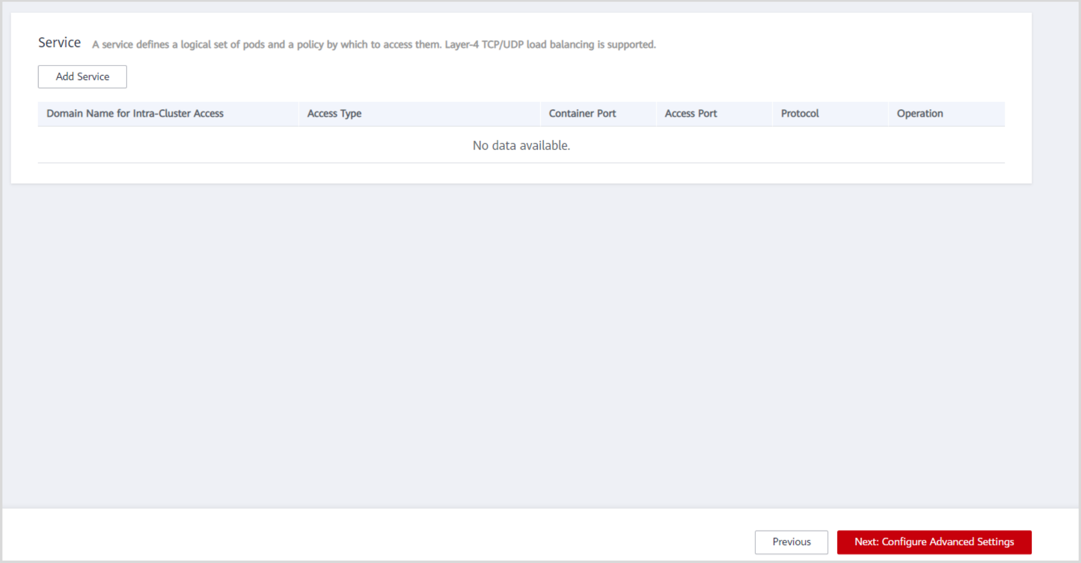
Container Resources

CPU ☑ Request 0.25 cores

A container is guaranteed to have as much CPU/memory as it requests, but is not allowed to use more CPU/memory than its limit.

Figure 6-41

Step 10 After the workload is created, click Next: **Set Application Access**. Skip the service configuration.



Service A service defines a logical set of pods and a policy by which to access them. Layer-4 TCP/UDP load balancing is supported.

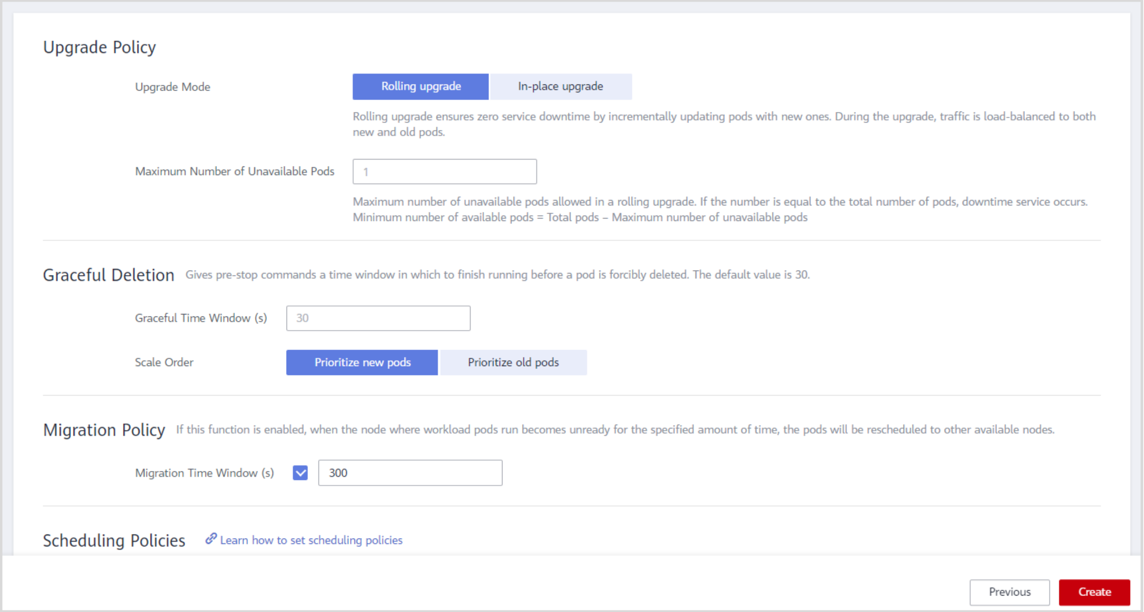
Add Service

Domain Name for Intra-Cluster Access	Access Type	Container Port	Access Port	Protocol	Operation
No data available.					

Previous Next: Configure Advanced Settings

Figure 6-42

Step 11 Retain the default settings and click **Create**.



Upgrade Policy

Upgrade Mode: [✓ Rolling upgrade] In-place upgrade

Rolling upgrade ensures zero service downtime by incrementally updating pods with new ones. During the upgrade, traffic is load-balanced to both new and old pods.

Maximum Number of Unavailable Pods: 1

Maximum number of unavailable pods allowed in a rolling upgrade. If the number is equal to the total number of pods, downtime service occurs. Minimum number of available pods = Total pods – Maximum number of unavailable pods

Graceful Deletion Gives pre-stop commands a time window in which to finish running before a pod is forcibly deleted. The default value is 30.

Graceful Time Window (s): 30

Scale Order: [✓ Prioritize new pods] Prioritize old pods

Migration Policy If this function is enabled, when the node where workload pods run becomes unready for the specified amount of time, the pods will be rescheduled to other available nodes.

Migration Time Window (s) ☑ 300

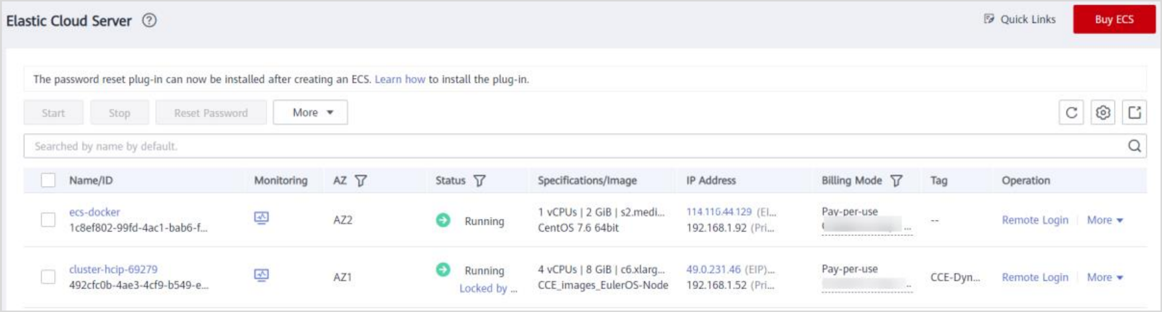
Scheduling Policies Learn how to set scheduling policies

Figure 6-43

Step 12 Return to the ECS page, purchase an EIP for the node in the CCE cluster, and bind the EIP to the node. For details, see *Compute Service Planning* or *Network Service Planning*.

Note: You need to use this EIP to implement external network access for the newly deployed workload.

- **Billing Mode**: **Pay-per-use**
- **Billed By**: **Traffic**
- **Bandwidth Size**: **10 Mbit/s**
- **Quantity**: **1**



Elastic Cloud Server

The password reset plug-in can now be installed after creating an ECS. Learn how to install the plug-in.

Searched by name by default.

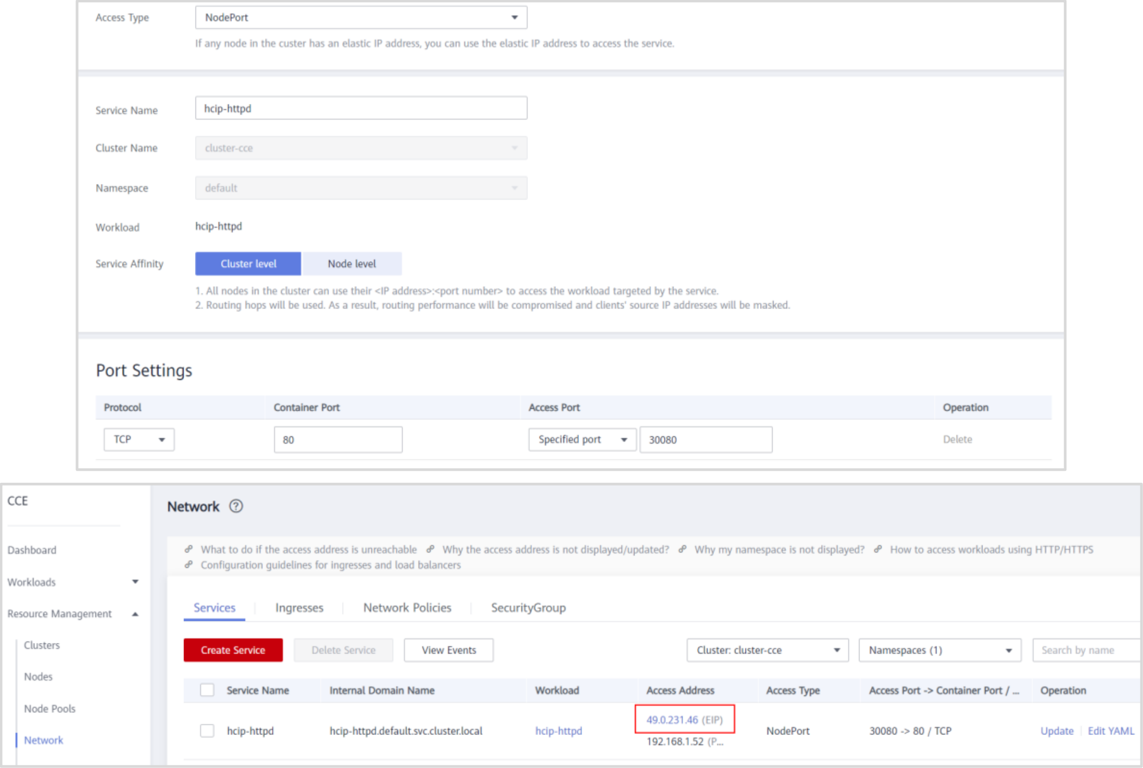
□	Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address	Billing Mode	Tag	Operation
□	ecs-docker 1c8ef802-99fd-4ac1-bab6-f...		AZ2	Running	1 vCPUs | 2 GiB | s2.medi... CentOS 7.6 64bit	114.116.44.129 (El... 192.168.1.92 (Pri...	Pay-per-use [redacted]	--	Remote Login | More
□	cluster-hcip-69279 492cfc0b-4ae3-4cf9-b549-e...		AZ1	Running Locked by ...	4 vCPUs | 8 GiB | c6.xlarg... CCE_images_EulerOS-Node	49.0.231.46 (EIP)... 192.168.1.52 (Pri...	Pay-per-use [redacted]	CCE-Dyn...	Remote Login | More

Figure 6-44

Step 13 Return to the CCE **Clusters** page, choose **Workloads** > **Deployments**. Click the target workload, for example, **hcip-httpd**. Select Services, and click **Create Service**. Set **Access Type** to **NodePort**, **Container Port** to **80**, and **Access Port** to **30080**. (Port 30080 is used as an example. You can select a port based on the site requirements.) After the configuration is complete, click **Create**. The **Resource Management** > **Network** page is displayed. Use a browser to access the EIP.

- **Service Name**: **hcip-httpd**

- Access Type: NodePort
- Service Affinity: Node level
- Protocol: TCP
- Container Port: 80
- Access Port: Specified port | 30080



Access Type: NodePort

If any node in the custer has an elastic IP address, you can use the elastic IP address to access the service.

Service Name: hcip-httpd

Cluster Name: cluster-cce

Namespace: default

Workload: hcip-httpd

Service Affinity: Cluster level | Node level

1. All nodes in the cluster can use their <IP address>:<port number> to access the workload targeted by the service.
2. Routing hops will be used. As a result, routing performance will be compromised and clients' source IP addresses will be masked.

Port Settings

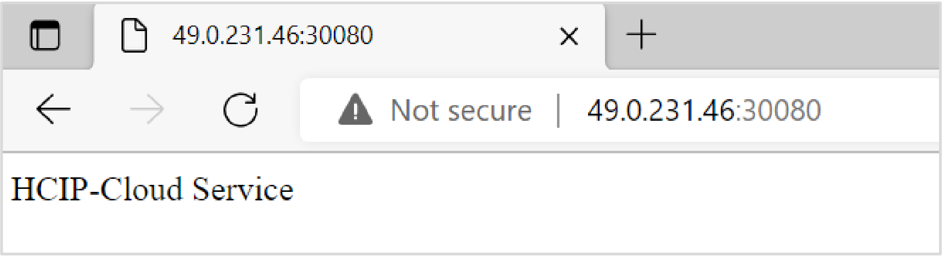
Protocol	Container Port	Access Port		Operation
TCP	80	Specified port	30080	Delete

CCE
Dashboard
Workloads
Resource Management
Clusters
Nodes
Node Pools
Network
Network
What to do if the access address is unreachable
Why the access address is not displayed/updated?
Why my namespace is not displayed?
How to access workloads using HTTP/HTTPS
Configuration guidelines for ingresses and load balancers
Services
Ingresses
Network Policies
SecurityGroup
Create Service
Delete Service
View Events
Cluster: cluster-cce
Namespaces (1)
Search by name

Service Name	Internal Domain Name	Workload	Access Address	Access Type	Access Port -> Container Port / ...	Operation
hcip-httpd	hcip-httpd.default.svc.cluster.local	hcip-httpd	49.0.231.46 (EIP) 192.168.1.52 (P...	NodePort	30080 -> 80 / TCP	Update Edit YAML

Figure 6-45

Step 14 Log in to the IP address through **http://EIP:30080**. (**http://49.0.231.46:30080** in this experiment). If the following information is displayed, the image pushed to SWR is successfully deployed on CCE.



HCIP-Cloud Service

Figure 6-46

6.2.2 FunctionGraph

FunctionGraph hosts and computes event-driven functions in a serverless context while ensuring high availability, high scalability, and zero maintenance. All you need to do is write your code and set conditions.

In actual service scenarios, there are too many unnecessary historical object versions stored in OBS, involving manual deletion and complex maintenance. In this case, you can retain the latest three versions in the bucket by using FunctionGraph.

6.2.2.1 Preparing Resources

Step 1 Use **https://cloudservice-v3.obs.cn-east-3.myhuaweicloud.com/DeleteOldVersions.zip** to download the code file.

6.2.2.2 Creating an Object Storage Bucket

Step 1 In the service list, choose **Object Storage Service**.

Description: Target bucket for executing functions.

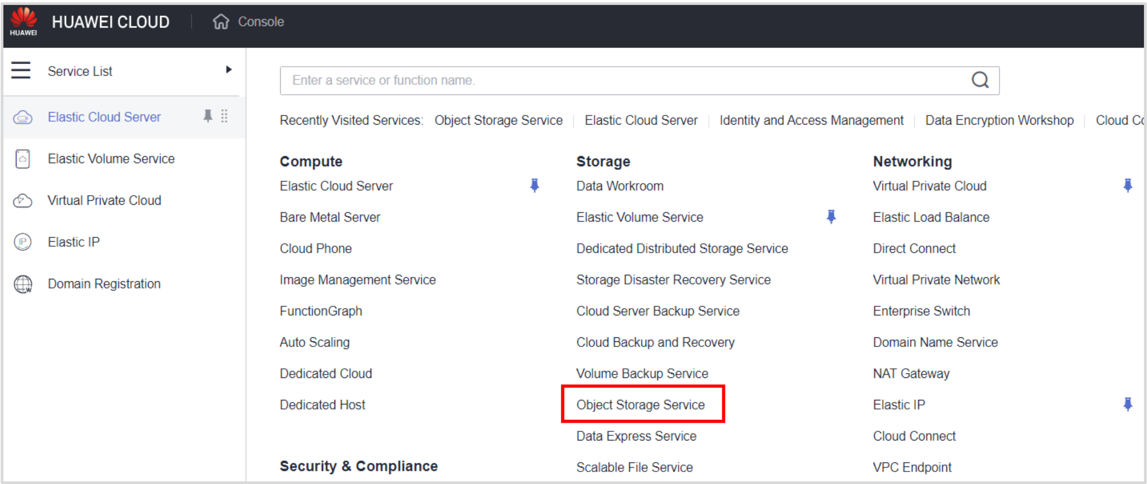
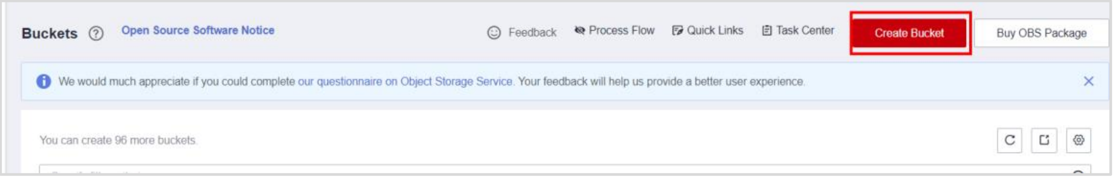


Figure 6-47

Step 2 Click **Create Bucket** in the upper right corner.



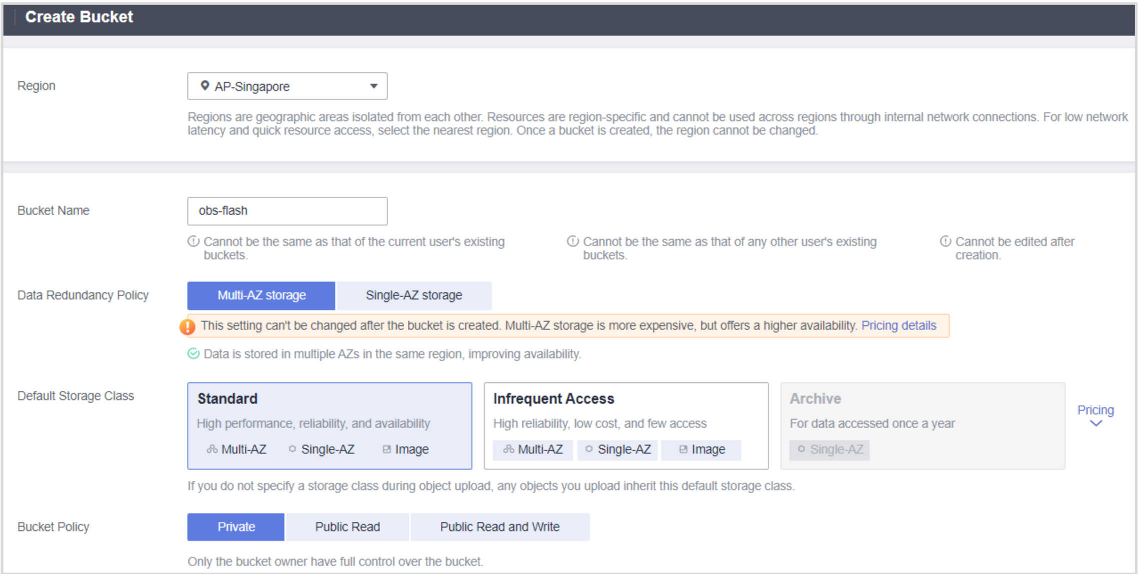
We would much appreciate if you could complete our questionnaire on Object Storage Service. Your feedback will help us provide a better user experience.

You can create 96 more buckets.

Figure 6-48

Step 3 Create an OBS bucket:

- **Region**: **AP - Singapore** (user-defined)
- **Bucket Name**: **obs-flash**
- Retain the default settings for other parameters.



Create Bucket

Region: AP-Singapore

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region. Once a bucket is created, the region cannot be changed.

Bucket Name: obs-flash

ⓘ Cannot be the same as that of the current user's existing buckets. ⓘ Cannot be the same as that of any other user's existing buckets. ⓘ Cannot be edited after creation.

Data Redundancy Policy: Multi-AZ storage | Single-AZ storage

This setting can't be changed after the bucket is created. Multi-AZ storage is more expensive, but offers a higher availability. Pricing details

Data is stored in multiple AZs in the same region, improving availability.

Default Storage Class:

- Standard: High performance, reliability, and availability — Multi-AZ, Single-AZ, Image
- Infrequent Access: High reliability, low cost, and few access — Multi-AZ, Single-AZ, Image
- Archive: For data accessed once a year — Single-AZ

Pricing

If you do not specify a storage class during object upload, any objects you upload inherit this default storage class.

Bucket Policy: Private | Public Read | Public Read and Write

Only the bucket owner have full control over the bucket.

Figure 6-49

6.2.2.3 Creating an Agency

Step 1 Select **Identity and Access Management** from the username drop-down list.

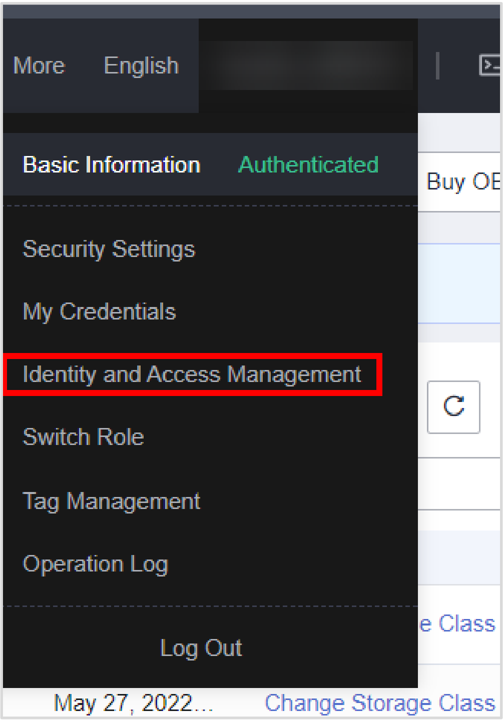
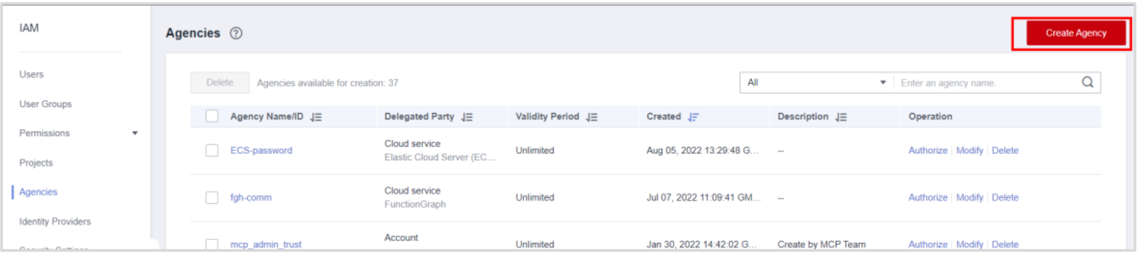


Figure 6-50

Step 2 In the navigation pane on the left, choose **Agencies** and then click **Create Agency** in the upper right corner.

Note: You need to use this agency to grant FunctionGraph permissions.



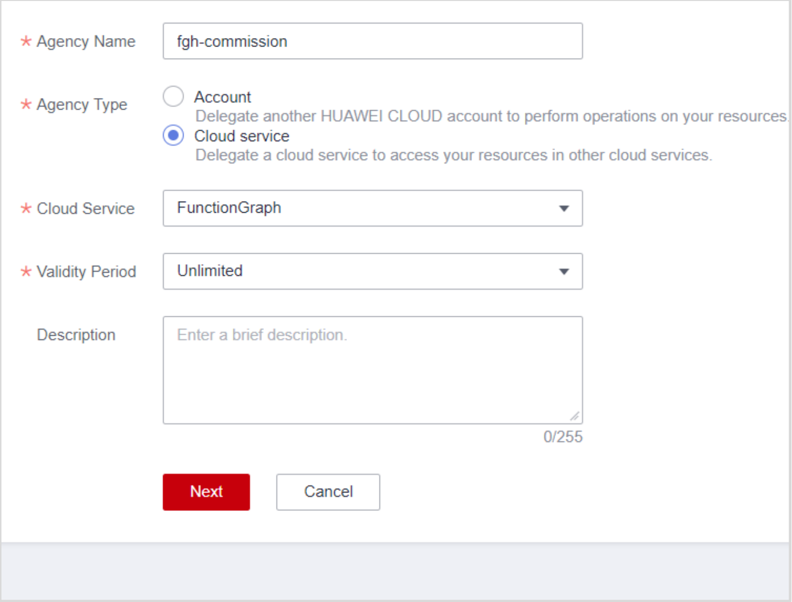
Agencies available for creation: 37

Agency Name/ID	Delegated Party	Validity Period	Created	Description	Operation
☐ ECS-password	Cloud service Elastic Cloud Server (EC...	Unlimited	Aug 05, 2022 13:29:48 G...	--	Authorize | Modify | Delete
☐ fgh-comm	Cloud service FunctionGraph	Unlimited	Jul 07, 2022 11:09:41 GM...	--	Authorize | Modify | Delete
☐ mcp_admin_trust	Account	Unlimited	Jan 30, 2022 14:42:02 G...	Create by MCP Team	Authorize | Modify | Delete

Figure 6-51

Step 3 Configure the agency name and type, and cloud service as follows:

- **Agency Name: fgh-commission**
- **Agency Type: Cloud service**
- **Cloud Service**: Select **FunctionGraph**.
- **Validity Period: Unlimited**



* Agency Name: fgh-commission

* Agency Type:
○ Account
Delegate another HUAWEI CLOUD account to perform operations on your resources
● Cloud service
Delegate a cloud service to access your resources in other cloud services.

* Cloud Service: FunctionGraph

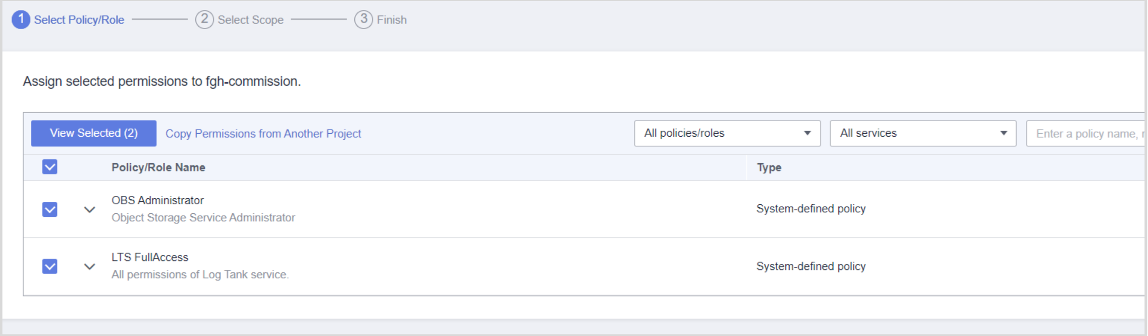
* Validity Period: Unlimited

Description: Enter a brief description.
0/255

Figure 6-52

- Select **OBS Administrator** and **LTS FullAccess**, as shown in the following figure.

Note: FunctionGraph needs to call OBS and LTS.

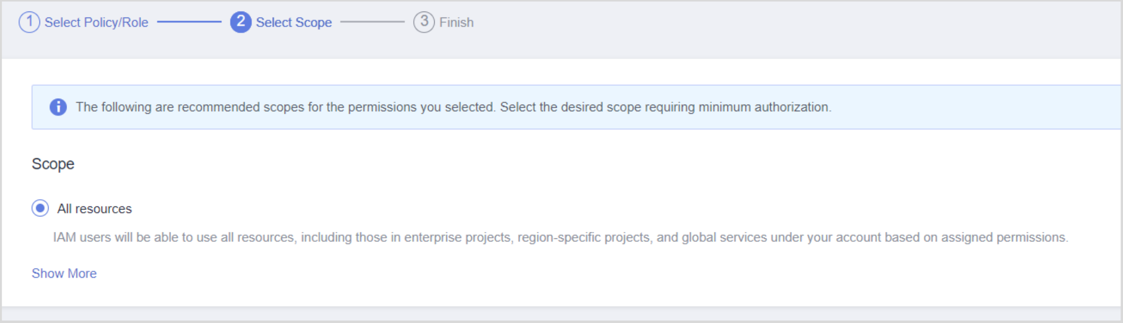


Assign selected permissions to fgh-commission.

☑	Policy/Role Name	Type
☑	OBS Administrator Object Storage Service Administrator	System-defined policy
☑	LTS FullAccess All permissions of Log Tank service.	System-defined policy

Figure 6-53

- Retain the default values for other parameters and click **OK**.



1 Select Policy/Role — 2 Select Scope — 3 Finish

The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

Scope

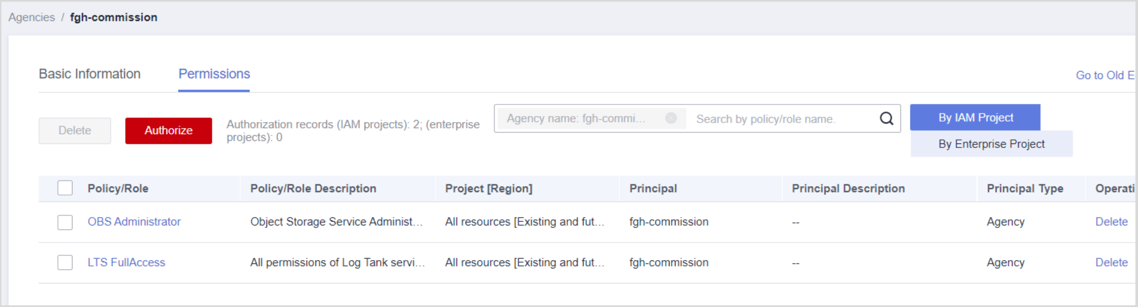
● All resources

IAM users will be able to use all resources, including those in enterprise projects, region-specific projects, and global services under your account based on assigned permissions.

Show More

Figure 6-54

Step 4 If you can view the agency in the agency list, as shown in the following figure, the agency is created successfully.



Agencies / fgh-commission

Basic Information | Permissions | Go to Old E

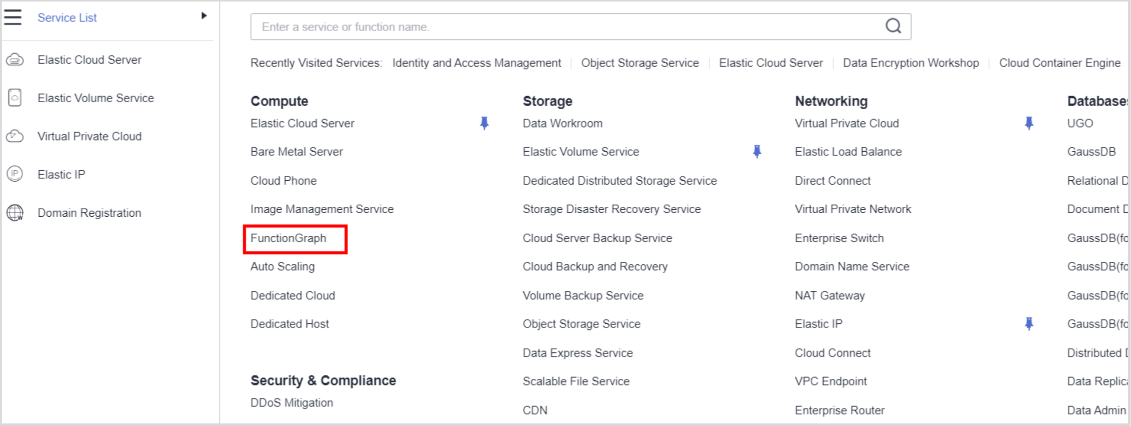
Delete | Authorize | Authorization records (IAM projects): 2; (enterprise projects): 0 | Agency name: fgh-commi... | Search by policy/role name. | By IAM Project | By Enterprise Project

□	Policy/Role	Policy/Role Description	Project [Region]	Principal	Principal Description	Principal Type	Operati
□	OBS Administrator	Object Storage Service Administ...	All resources [Existing and fut...	fgh-commission	--	Agency	Delete
□	LTS FullAccess	All permissions of Log Tank servi...	All resources [Existing and fut...	fgh-commission	--	Agency	Delete

Figure 6-55

6.2.2.4 Creating a Function

Step 1 In the service list, choose **FunctionGraph**.



Service List

Elastic Cloud Server
Elastic Volume Service
Virtual Private Cloud
Elastic IP
Domain Registration

Enter a service or function name.

Recently Visited Services: Identity and Access Management | Object Storage Service | Elastic Cloud Server | Data Encryption Workshop | Cloud Container Engine

Compute
Elastic Cloud Server
Bare Metal Server
Cloud Phone
Image Management Service
FunctionGraph
Auto Scaling
Dedicated Cloud
Dedicated Host

Security & Compliance
DDoS Mitigation

Storage
Data Workroom
Elastic Volume Service
Dedicated Distributed Storage Service
Storage Disaster Recovery Service
Cloud Server Backup Service
Cloud Backup and Recovery
Volume Backup Service
Object Storage Service
Data Express Service
Scalable File Service
CDN

Networking
Virtual Private Cloud
Elastic Load Balance
Direct Connect
Virtual Private Network
Enterprise Switch
Domain Name Service
NAT Gateway
Elastic IP
Cloud Connect
VPC Endpoint
Enterprise Router

Database
UGO
GaussDB
Relational D
Document D
GaussDB(fo
GaussDB(fo
GaussDB(fo
GaussDB(fo
Distributed I
Data Replic
Data Admin

Figure 6-56

Step 2 On the FunctionGraph console, click **Create Function** in the upper right corner.

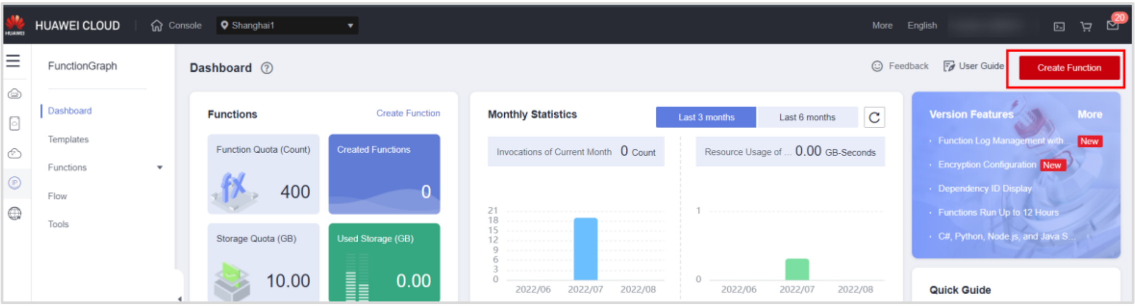
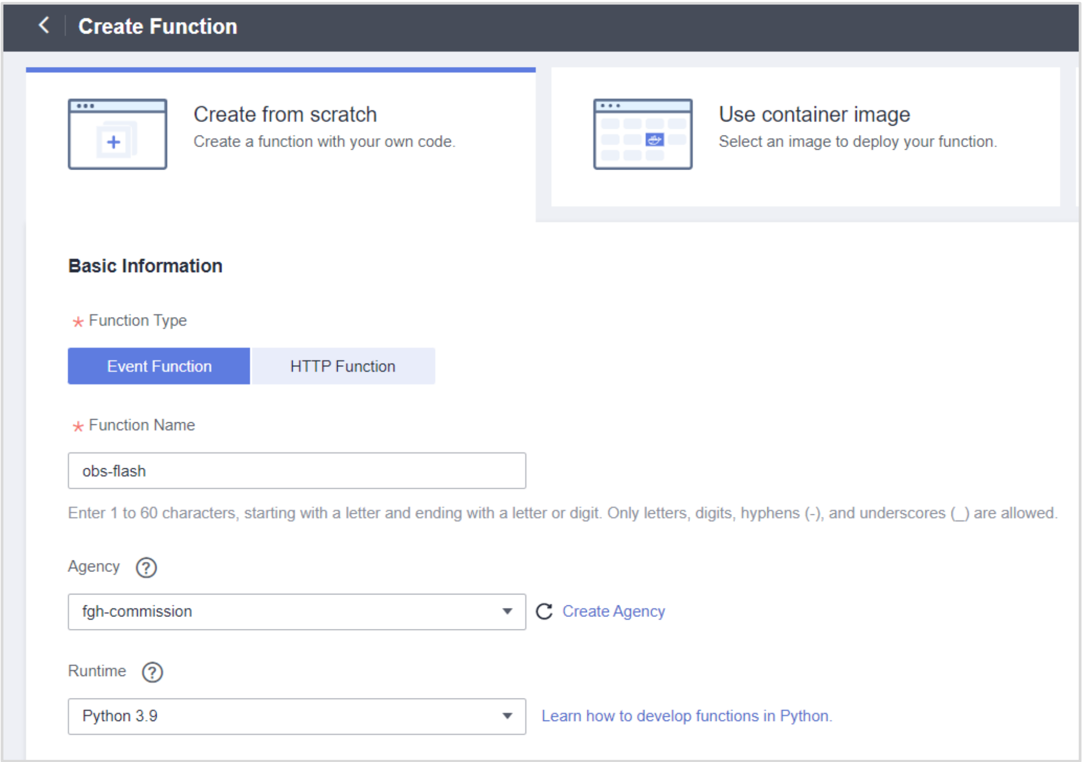


Figure 6-57

Step 3 Create a function as follows:

- **Function Type**: **Event Function**
- **Region**: **AP-Singapore**
- **Function Name**: **obs-flash**
- **Agency**: **fgh-commission**
- **Runtime**: **Python 3.9**


Create Function
Create from scratch
Create a function with your own code.
Use container image
Select an image to deploy your function.
Basic Information
Event Function
HTTP Function
Create Agency
Learn how to develop functions in Python.

* Function Type: Event Function

* Function Name: obs-flash

Enter 1 to 60 characters, starting with a letter and ending with a letter or digit. Only letters, digits, hyphens (-), and underscores (_) are allowed.

Agency: fgh-commission

Runtime: Python 3.9

Figure 6-58

6.2.2.5 Configuring Simple Message Notification (SMN)

Step 1 On the **Service List** page, select **Simple Message Notification** under **Management & Governance**.

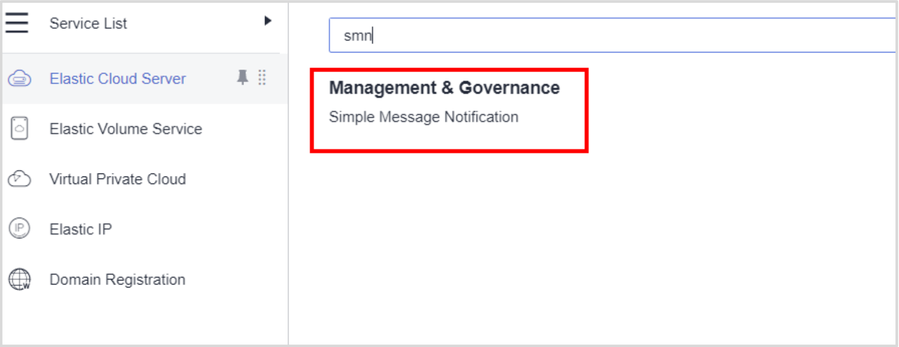


Figure 6-59

Step 2 In the navigation pane, choose **Topic Management** > **Topics**. Then, click **Create Topic** in the upper right corner.

Note: In subsequent exercises, you need to use this SMN topic to trigger FunctionGraph.

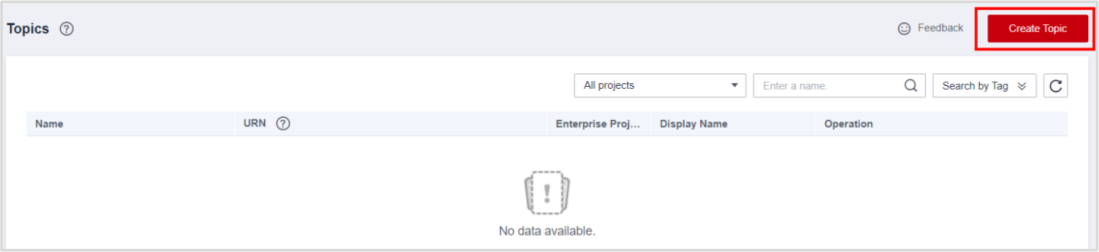
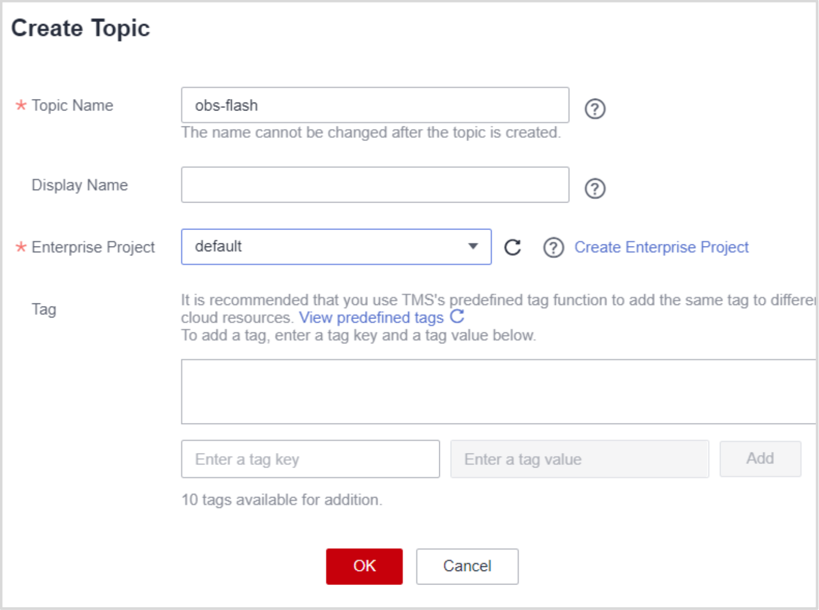


Figure 6-60

Step 3 Set **Topic Name** to **obs-flash** and click **OK**.


Create Topic

* Topic Name: obs-flash

The name cannot be changed after the topic is created.

Display Name:

* Enterprise Project: default

Create Enterprise Project

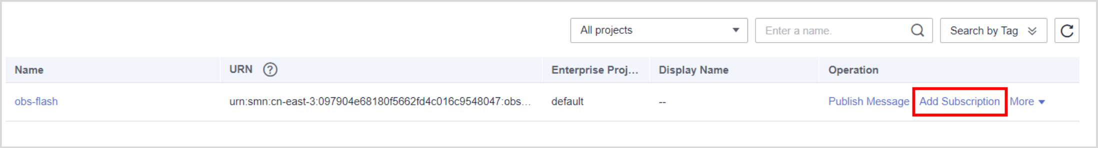
Tag: It is recommended that you use TMS's predefined tag function to add the same tag to differe cloud resources. View predefined tags

To add a tag, enter a tag key and a tag value below.

10 tags available for addition.

Figure 6-61

Step 4 Click **Add Subscription** corresponding to **obs-flash** and add a subscription as follows:



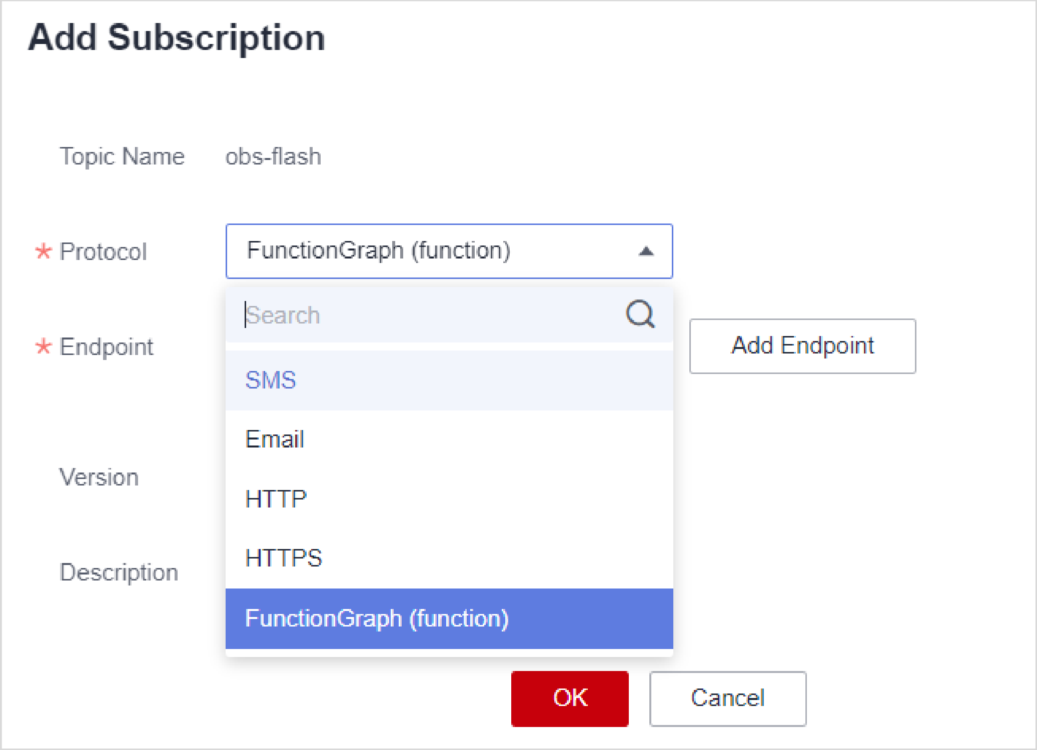
All projects | Enter a name. | Search by Tag

Name	URN	Enterprise Proj...	Display Name	Operation
obs-flash	urn:smn:cn-east-3:097904e68180f5662fd4c016c9548047:obs...	default	--	Publish Message Add Subscription More

Figure 6-62

- Select **FunctionGraph (function)** for **Protocol** and **obs-flash** for **Endpoint**.

Note: Select the created FunctionGraph function as the endpoint. When SMN is triggered, FunctionGraph will be notified.



Add Subscription

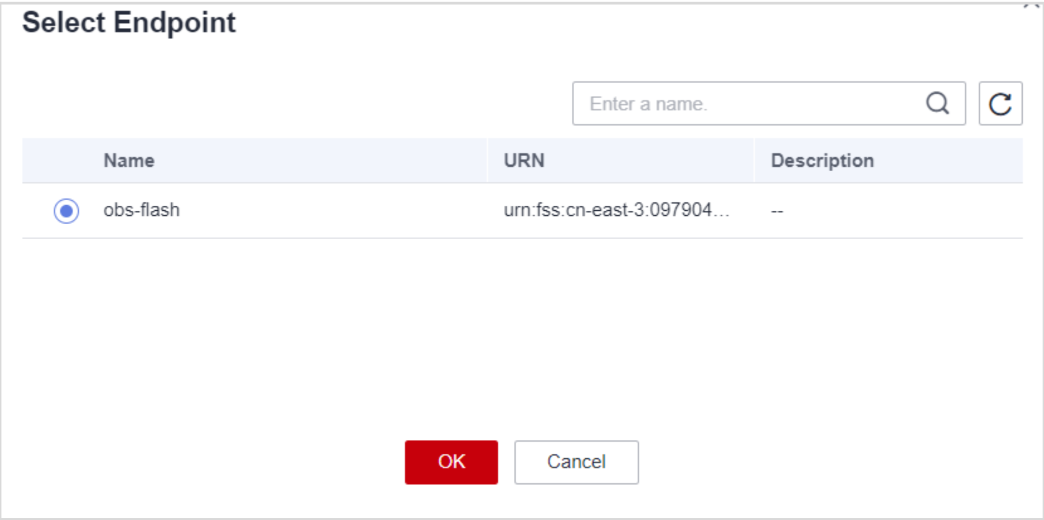
Topic Name obs-flash

* Protocol FunctionGraph (function)

* Endpoint

Version

Description



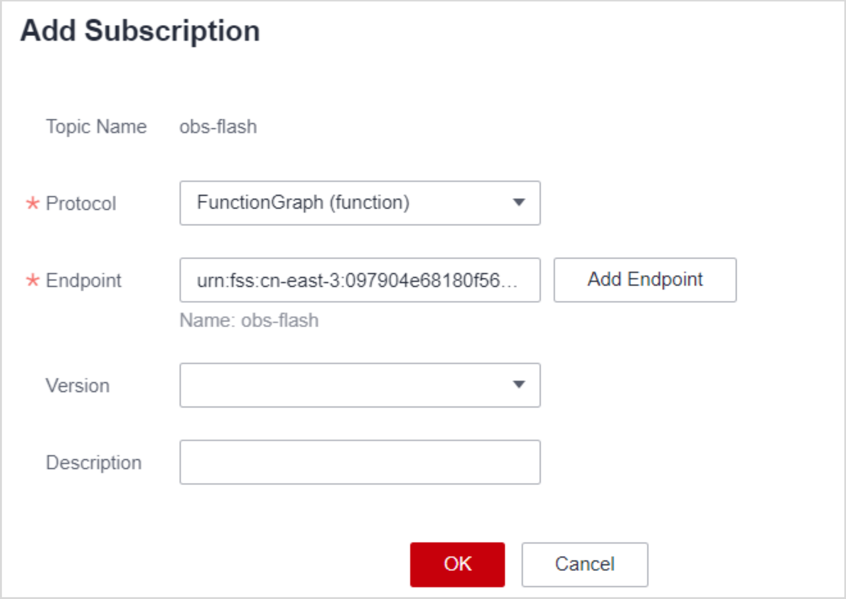
Select Endpoint

Enter a name.

	Name	URN	Description
●	obs-flash	urn:fss:cn-east-3:097904...	--

Figure 6-63

- After the preceding configuration is complete (the version does not need to be selected), click **OK**.



Add Subscription

Topic Name: obs-flash

* Protocol: FunctionGraph (function)

* Endpoint: urn:fss:cn-east-3:097904e68180f56...

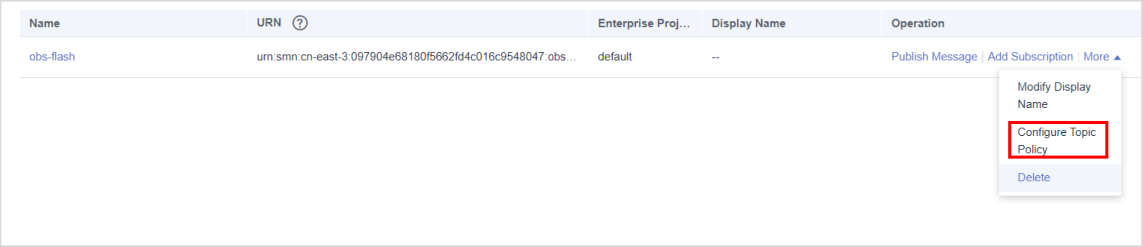
Name: obs-flash

Version:

Description:

Figure 6-64

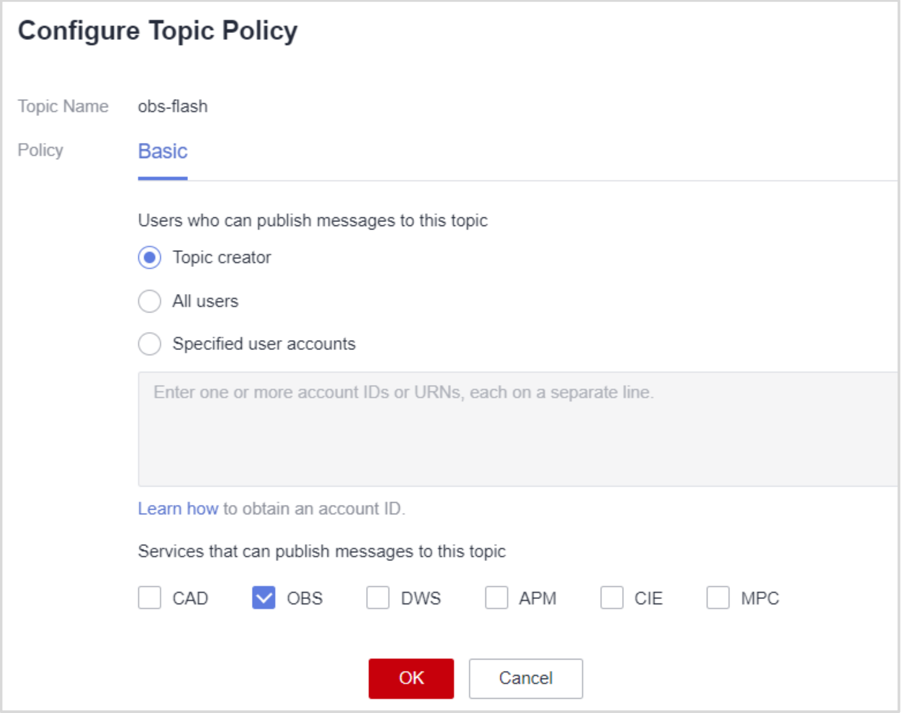
Step 5 Locate the **obs-flash** topic, click **More** in the **Operation** column, and select **Configure Topic Policy**.



Name	URN	Enterprise Proj...	Display Name	Operation
obs-flash	urn:smn:cn-east-3:097904e68180f5662fd4c016c9548047:obs...	default	--	Publish Message | Add Subscription | More

Figure 6-65

- Select **OBS** for **Services that can publish messages to this topic** and click **OK**.



Configure Topic Policy

Topic Name obs-flash

Policy Basic

Users who can publish messages to this topic

● Topic creator

○ All users

○ Specified user accounts

Enter one or more account IDs or URNs, each on a separate line.

Learn how to obtain an account ID.

Services that can publish messages to this topic

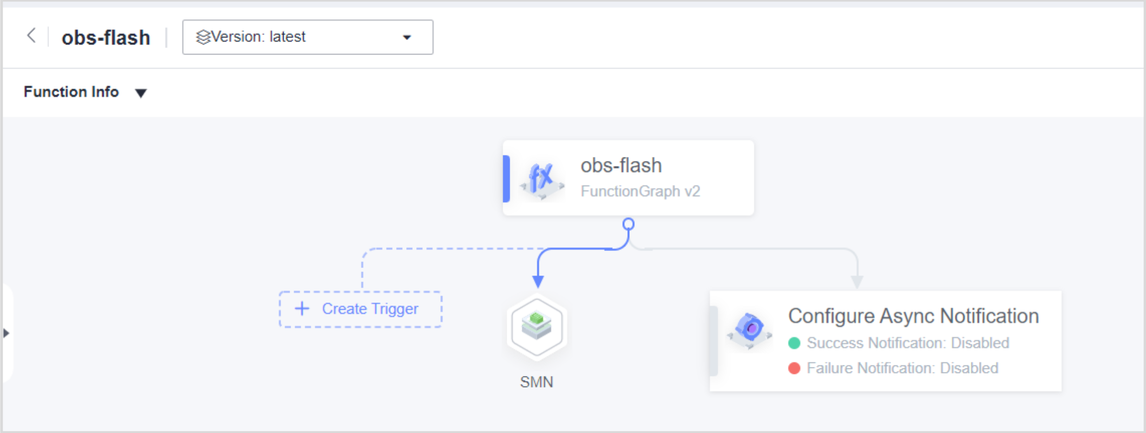
□ CAD ☑ OBS □ DWS □ APM □ CIE □ MPC

OK Cancel

Figure 6-66

6.2.2.6 Configuring a Function Workflow

Step 1 Choose **FunctionGraph** > **Functions** > **Function List**, click the created function, for example, **obs-flash**, and check whether a trigger is generated. The SMN trigger in the following figure is the newly generated trigger.



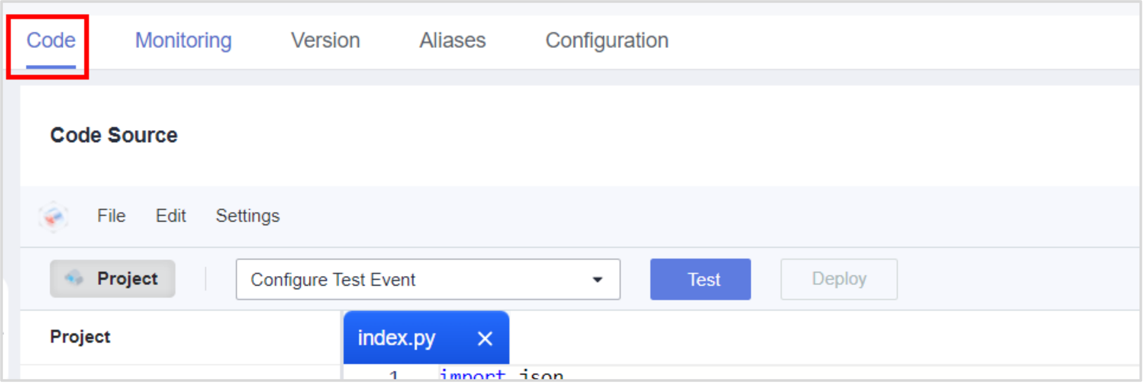
obs-flash Version: latest

Function Info

obs-flash
FunctionGraph v2
+ Create Trigger
SMN
Configure Async Notification
Success Notification: Disabled
Failure Notification: Disabled

Figure 6-67

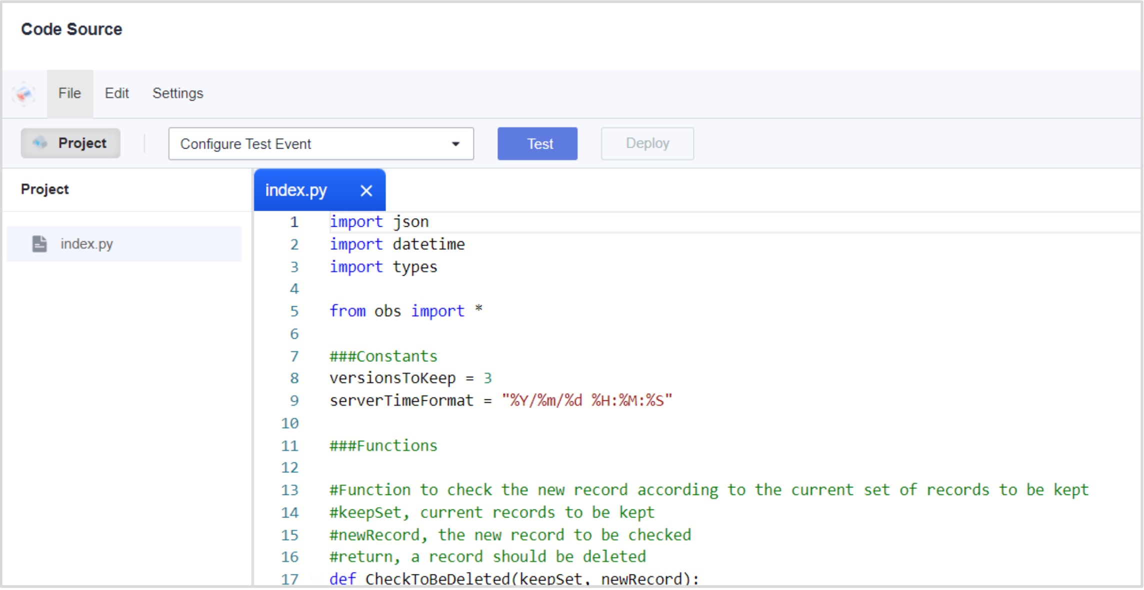
Step 2 On the function page, click the **Code** tab.



```
import json
```

Figure 6-68

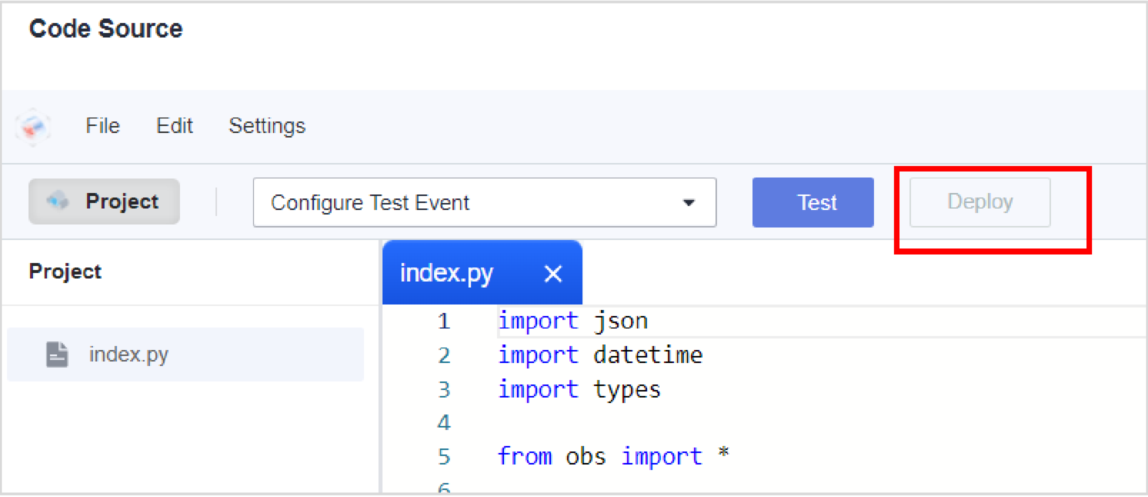
Step 3 Copy the content in the code file downloaded in 6.2.2.1 to the **index.py** file (overwrite the original content).



```
import json
import datetime
import types

from obs import *

###Constants
versionsToKeep = 3
serverTimeFormat = "%Y/%m/%d %H:%M:%S"

###Functions

#Function to check the new record according to the current set of records to be kept
#keepSet, current records to be kept
#newRecord, the new record to be checked
#return, a record should be deleted
def CheckToBeDeleted(keepSet, newRecord):
```

Figure 6-69

Step 4 Click **Deploy**.



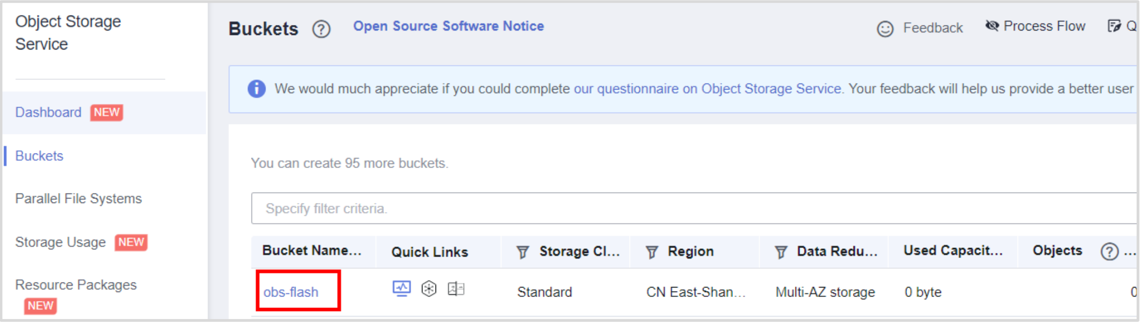
```
import json
import datetime
import types

from obs import *
```

Figure 6-70

6.2.2.7 Configuring the Object Storage Bucket

Step 1 In the service list, choose **Object Storage Service**.

Step 2 Click the new bucket **obs-flash**.



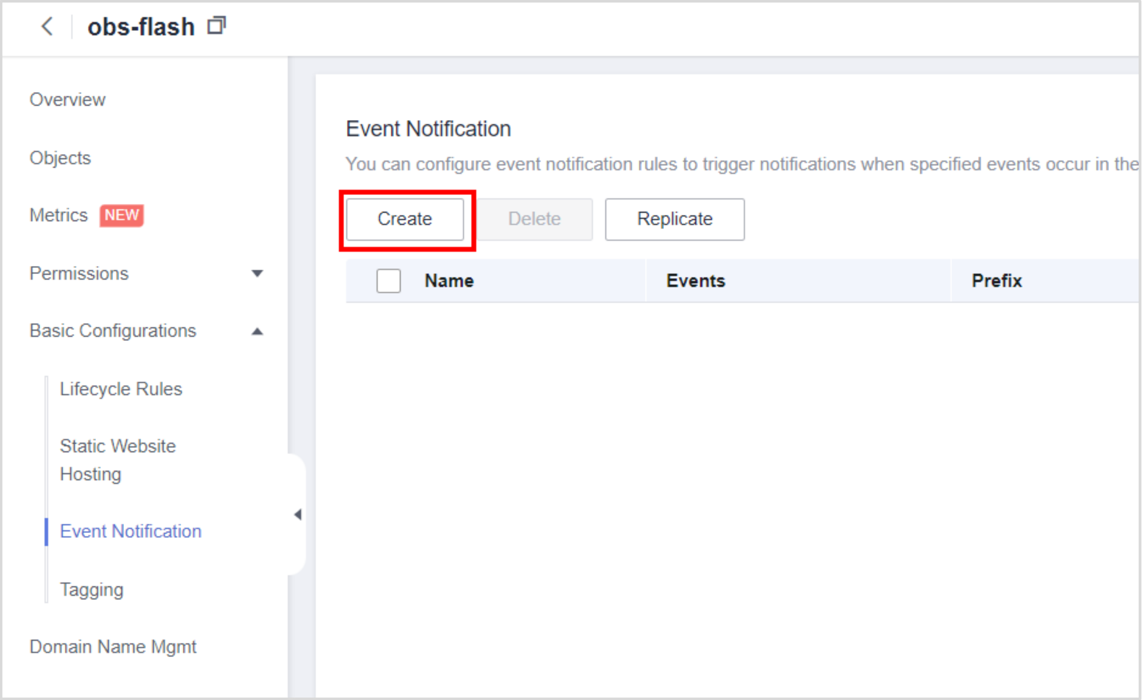
We would much appreciate if you could complete our questionnaire on Object Storage Service. Your feedback will help us provide a better user

You can create 95 more buckets.

Bucket Name...	Quick Links	Storage Cl...	Region	Data Redu...	Used Capacit...	Objects
obs-flash		Standard	CN East-Shan...	Multi-AZ storage	0 byte	0

Figure 6-71

Step 3 On the navigation pane on the left, choose **Basic Configurations** > **Event Notification** and click **Create** on the right.



Event Notification

You can configure event notification rules to trigger notifications when specified events occur in the

□ Name	Events	Prefix

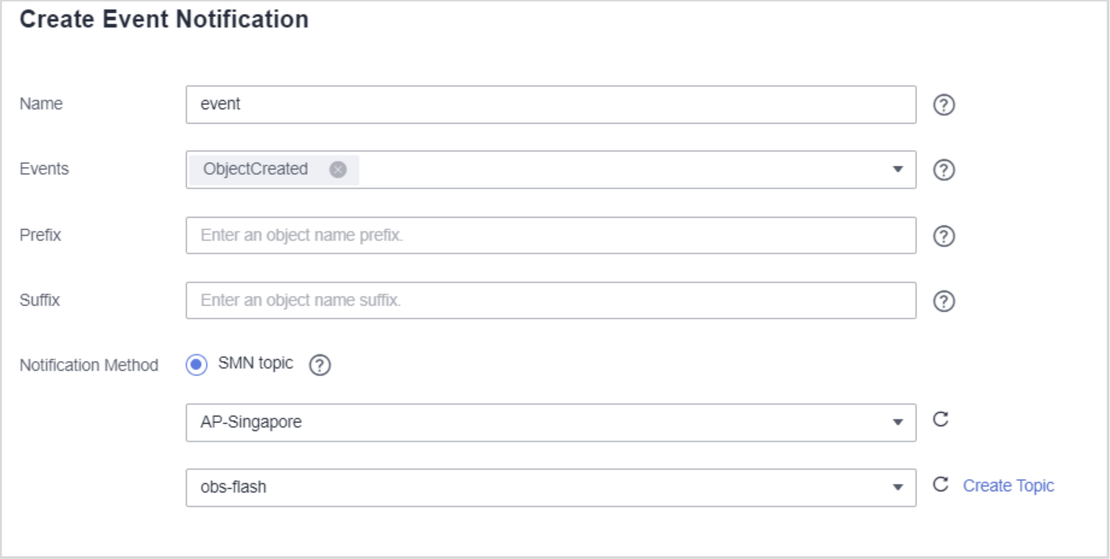
Figure 6-72

Step 4 Create an event notification as follows:

Note: When an object is created in the bucket, this event notification will trigger an SMN message and be forwarded to FunctionGraph.

- **Name**: **event-xxx**(user-defined)
- **Events**: **ObjectCreated**

- **Notification Method: SMN topic | AP-Singapore | obs-flash**



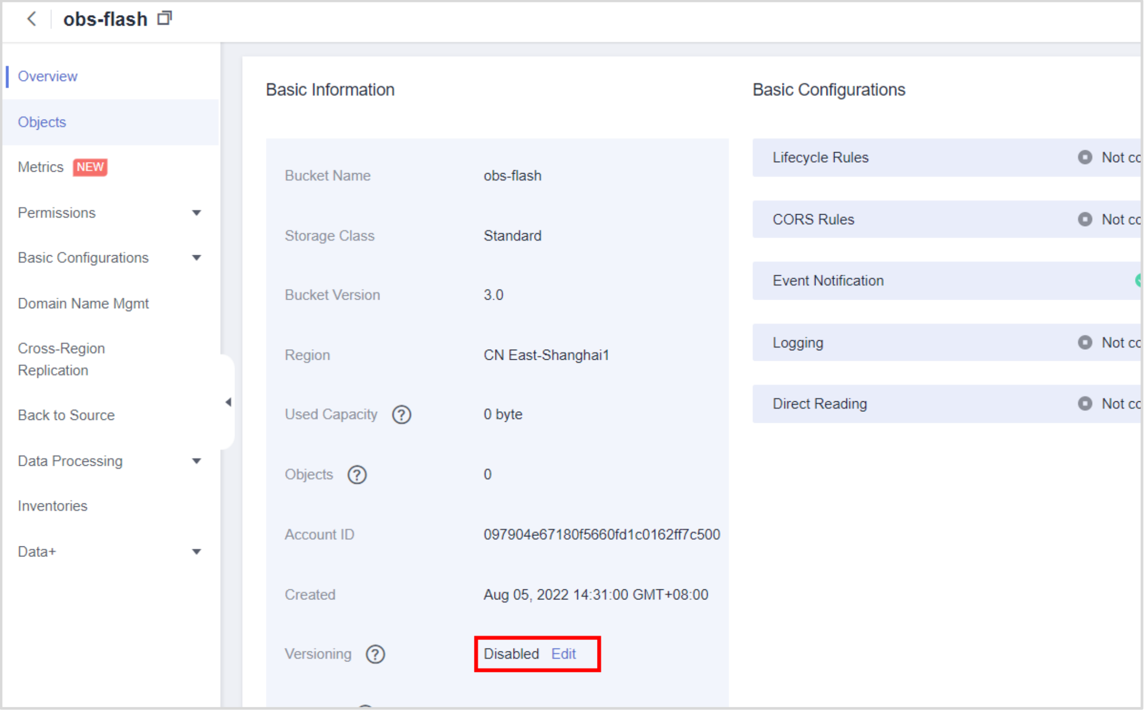
Create Event Notification

Name	event
Events	ObjectCreated
Prefix	Enter an object name prefix.
Suffix	Enter an object name suffix.
Notification Method	● SMN topic
	AP-Singapore
	obs-flash

Figure 6-73

Step 5 On the navigation pane on the left, choose **Overview** > **Objects**. Click **Edit** next to **Versioning**.

Note: You need to upload multiple versions of an object to test the execution of a function.



Basic Information

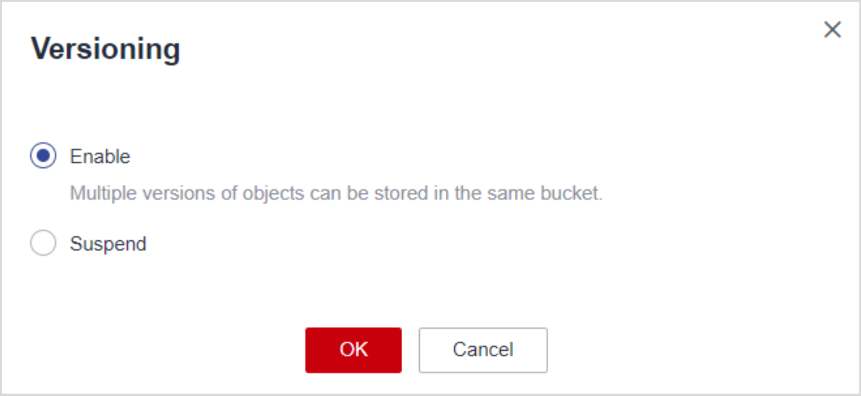
Bucket Name	obs-flash
Storage Class	Standard
Bucket Version	3.0
Region	CN East-Shanghai1
Used Capacity	0 byte
Objects	0
Account ID	097904e67180f5660fd1c0162ff7c500
Created	Aug 05, 2022 14:31:00 GMT+08:00
Versioning	Disabled Edit

Basic Configurations

Lifecycle Rules	Not cc
CORS Rules	Not cc
Event Notification	
Logging	Not cc
Direct Reading	Not cc

Figure 6-74

Step 6 In the displayed dialog box, select **Enable** and click **OK**.



Versioning

● Enable

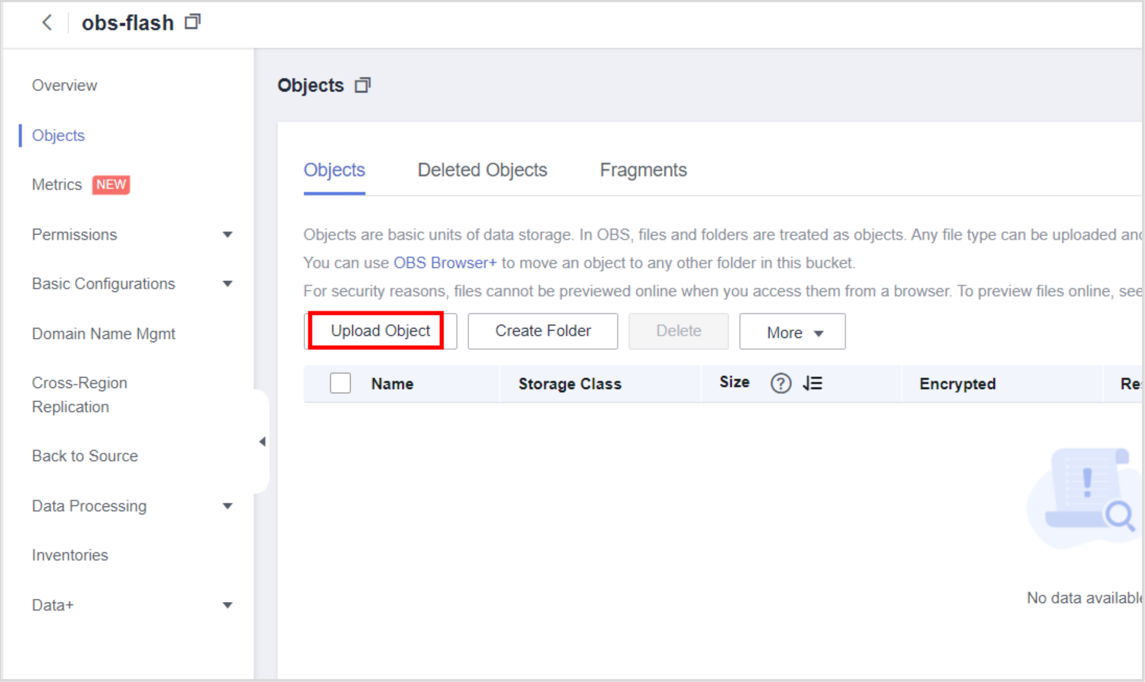
Multiple versions of objects can be stored in the same bucket.

○ Suspend

Figure 6-75

6.2.2.8 Uploading an Object to the Object Storage Bucket

Step 1 Choose **Overview** > **Objects**. Click the **Objects** tab. Click **Upload Object**.



Objects are basic units of data storage. In OBS, files and folders are treated as objects. Any file type can be uploaded an

You can use OBS Browser+ to move an object to any other folder in this bucket.

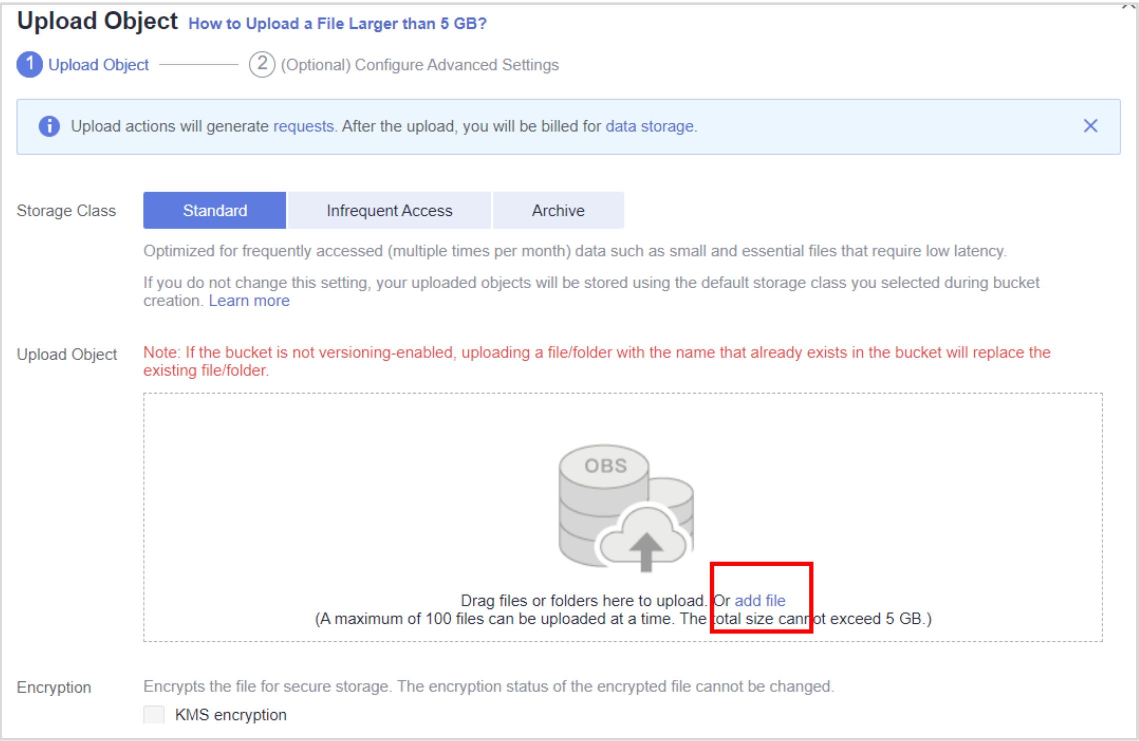
For security reasons, files cannot be previewed online when you access them from a browser. To preview files online, see

□ Name	Storage Class	Size	Encrypted	Re

No data availabl

Figure 6-76

Step 2 Click **add file**.



Upload Object How to Upload a File Larger than 5 GB?

1 Upload Object —— 2 (Optional) Configure Advanced Settings

Upload actions will generate requests. After the upload, you will be billed for data storage.

Storage Class: Standard | Infrequent Access | Archive

Optimized for frequently accessed (multiple times per month) data such as small and essential files that require low latency.

If you do not change this setting, your uploaded objects will be stored using the default storage class you selected during bucket creation. Learn more

Upload Object: Note: If the bucket is not versioning-enabled, uploading a file/folder with the name that already exists in the bucket will replace the existing file/folder.

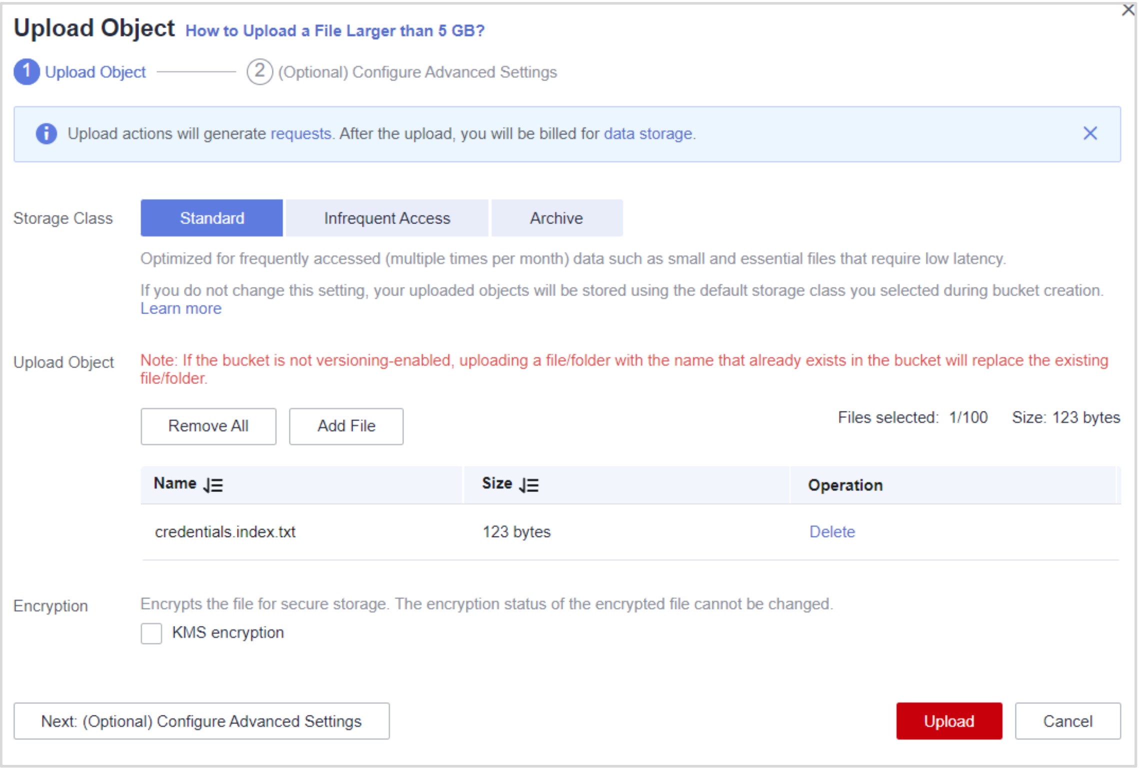
Drag files or folders here to upload. Or add file
(A maximum of 100 files can be uploaded at a time. The total size cannot exceed 5 GB.)

Encryption: Encrypts the file for secure storage. The encryption status of the encrypted file cannot be changed.

□ KMS encryption

Figure 6-77

Step 3 Select a small test file from the local PC and click **Upload**.



Upload Object How to Upload a File Larger than 5 GB?

1 Upload Object —— 2 (Optional) Configure Advanced Settings

Upload actions will generate requests. After the upload, you will be billed for data storage.

Storage Class: Standard | Infrequent Access | Archive

Optimized for frequently accessed (multiple times per month) data such as small and essential files that require low latency.

If you do not change this setting, your uploaded objects will be stored using the default storage class you selected during bucket creation. Learn more

Upload Object: Note: If the bucket is not versioning-enabled, uploading a file/folder with the name that already exists in the bucket will replace the existing file/folder.

Remove All | Add File — Files selected: 1/100 Size: 123 bytes

Name	Size	Operation
credentials.index.txt	123 bytes	Delete

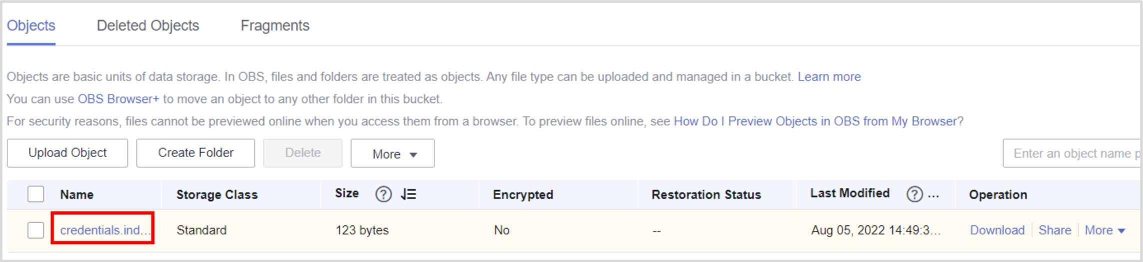
Encryption: Encrypts the file for secure storage. The encryption status of the encrypted file cannot be changed.

□ KMS encryption

Next: (Optional) Configure Advanced Settings | Upload | Cancel

Figure 6-78

Step 4 Repeat this operation twice and click the object name.



Objects are basic units of data storage. In OBS, files and folders are treated as objects. Any file type can be uploaded and managed in a bucket. Learn more

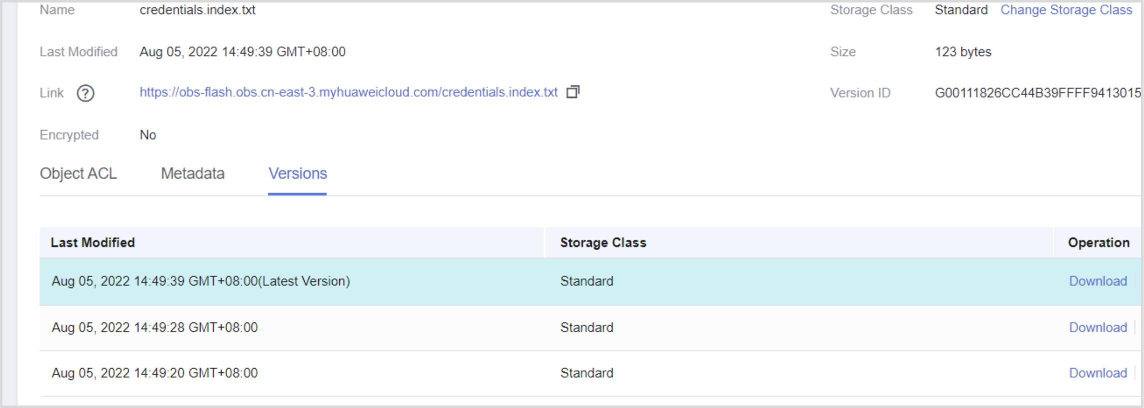
You can use OBS Browser+ to move an object to any other folder in this bucket.

For security reasons, files cannot be previewed online when you access them from a browser. To preview files online, see How Do I Preview Objects in OBS from My Browser?

□	Name	Storage Class	Size	Encrypted	Restoration Status	Last Modified	Operation
□	credentials.ind...	Standard	123 bytes	No	--	Aug 05, 2022 14:49:3...	Download | Share | More

Figure 6-79

Step 5 Click the **Versions** tab to view the saved version files. You can determine the version by viewing the revision time of the files.


Name credentials.index.txt

Storage Class Standard Change Storage Class

Last Modified Aug 05, 2022 14:49:39 GMT+08:00

Size 123 bytes

Link https://obs-flash.obs.cn-east-3.myhuaweicloud.com/credentials.index.txt

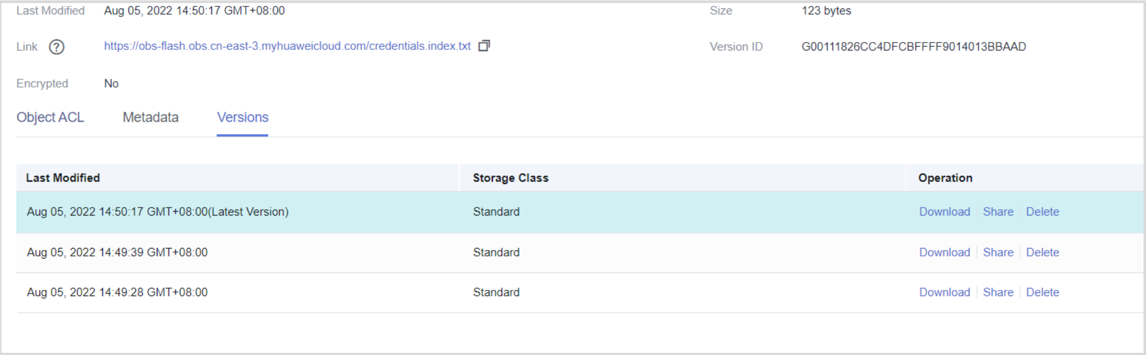
Version ID G00111826CC44B39FFFF9413015

Encrypted No

Last Modified	Storage Class	Operation
Aug 05, 2022 14:49:39 GMT+08:00(Latest Version)	Standard	Download
Aug 05, 2022 14:49:28 GMT+08:00	Standard	Download
Aug 05, 2022 14:49:20 GMT+08:00	Standard	Download

Figure 6-80

Step 6 Perform the upload operation again and check the historical versions again. It is found that only the latest three version files are retained and the earliest uploaded version is updated. The earlier version has been updated, indicating that the function workflow has been triggered and taken effect.


Last Modified Aug 05, 2022 14:50:17 GMT+08:00

Size 123 bytes

Link https://obs-flash.obs.cn-east-3.myhuaweicloud.com/credentials.index.txt

Version ID G00111826CC4DFCBFFFF9014013BBAAD

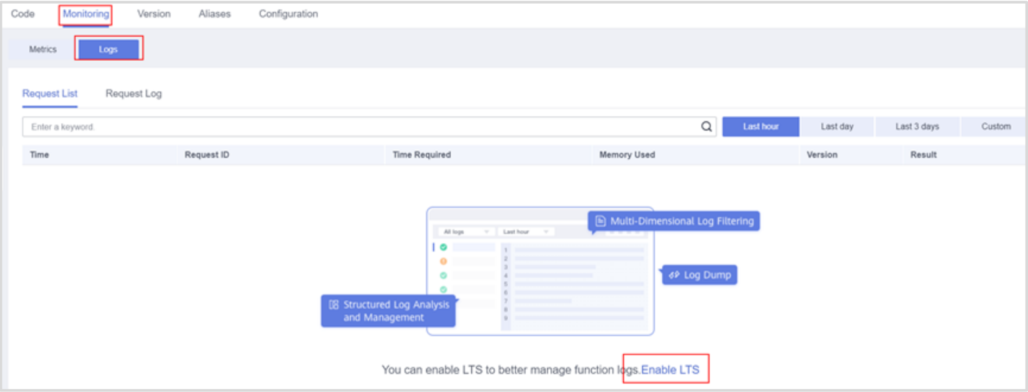
Encrypted No

Last Modified	Storage Class	Operation
Aug 05, 2022 14:50:17 GMT+08:00(Latest Version)	Standard	Download | Share | Delete
Aug 05, 2022 14:49:39 GMT+08:00	Standard	Download | Share | Delete
Aug 05, 2022 14:49:28 GMT+08:00	Standard	Download | Share | Delete

Figure 6-81

6.2.2.9 Viewing FunctionGraph Execution Logs

Step 1 On the **Monitoring** tab page of the created **obs-flash** function, click the **Logs** tab, and click **Enable LTS**.

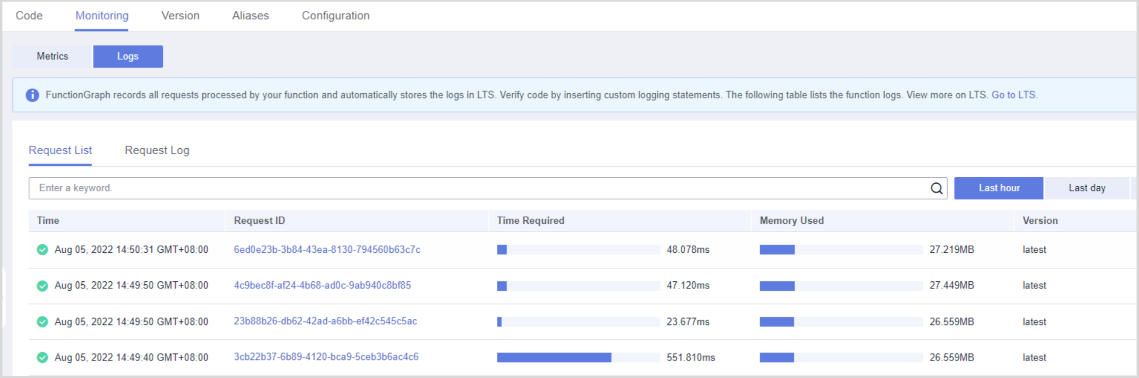


You can enable LTS to better manage function logs.Enable LTS

Figure 6-82

Step 2 Go back to the OBS page and upload the same file again (the file can be uploaded for multiple times) to trigger FunctionGraph to delete the historical version.

Step 3 Return to the **obs-flash** function page and choose **Monitoring** > **Logs** to view the calling status of the current function. Note: After the OBS file is uploaded, it may take several minutes to view the log information.



FunctionGraph records all requests processed by your function and automatically stores the logs in LTS. Verify code by inserting custom logging statements. The following table lists the function logs. View more on LTS. Go to LTS.

Time	Request ID	Time Required	Memory Used	Version
Aug 05, 2022 14:50:31 GMT+08:00	6ed0e23b-3b84-43ea-8130-794560b63c7c	48.078ms	27.219MB	latest
Aug 05, 2022 14:49:50 GMT+08:00	4c9bec8f-af24-4b68-ad0c-9ab940c8bf85	47.120ms	27.449MB	latest
Aug 05, 2022 14:49:50 GMT+08:00	23b88b26-db62-42ad-a6bb-ef42c545c5ac	23.677ms	26.559MB	latest
Aug 05, 2022 14:49:40 GMT+08:00	3cb22b37-6b89-4120-bca9-5ceb3b6ac4c6	551.810ms	26.559MB	latest

Figure 6-83

6.3 Clearing Resources

Step 1 Delete workloads.

Choose **Service List** > **Cloud Container Engine**. In the navigation pane, choose **Workloads** > **Deployments**, locate the Deployment created in this exercise and choose **More** > **Delete** in the **Operation** column.

Step 2 Delete the CCE node.

Choose **Service List** > **Cloud Container Engine**. In the navigation pane, choose **Resource Management** > **Nodes**. In the node list, locate the node created in this exercise and choose **More** > **Delete** in the **Operation** column.

Step 3 Delete the SWR organization.

- Choose **Service List** > **SoftWare Repository for Container**. In the navigation pane, click **Organization Management**. Locate the organization created in this exercise and click the organization name to go to the details page.

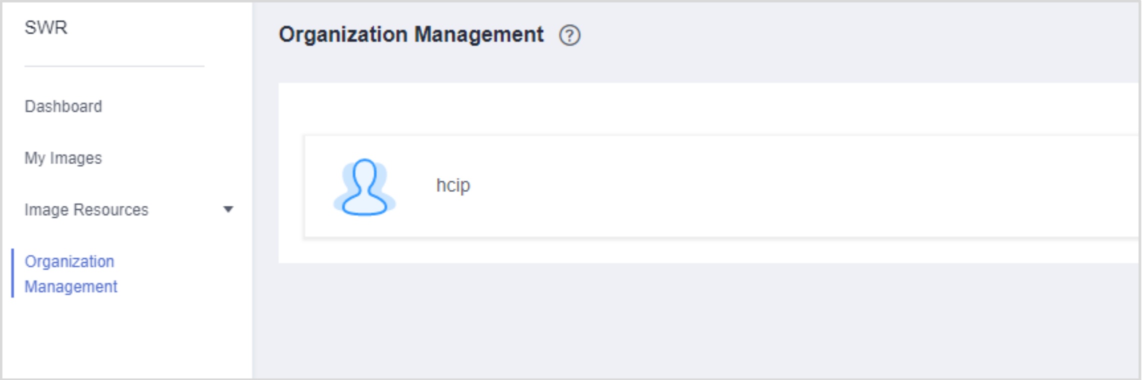


Figure 6-84

- Click **Images** and click the name of the image created in this exercise.

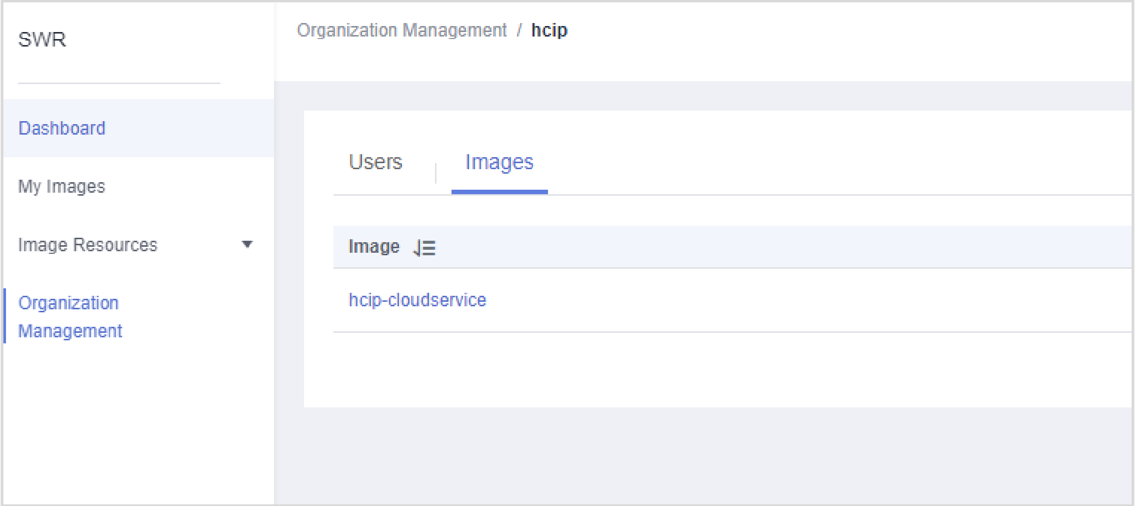
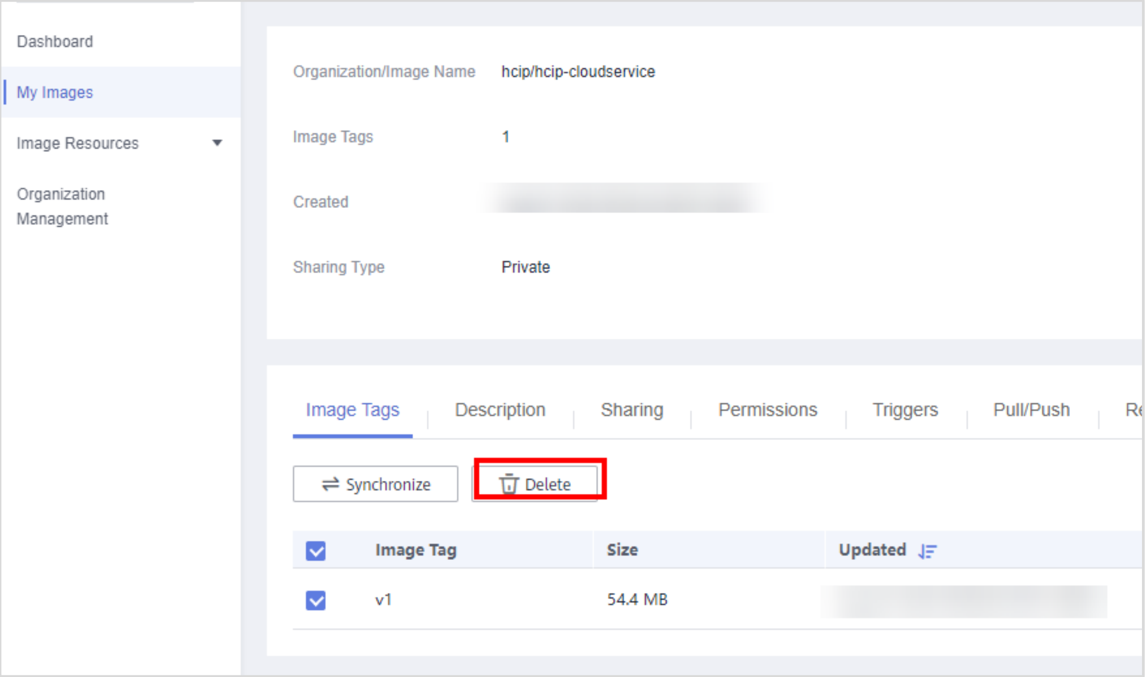


Figure 6-85

- On the displayed page, select all image versions and click **Delete**.

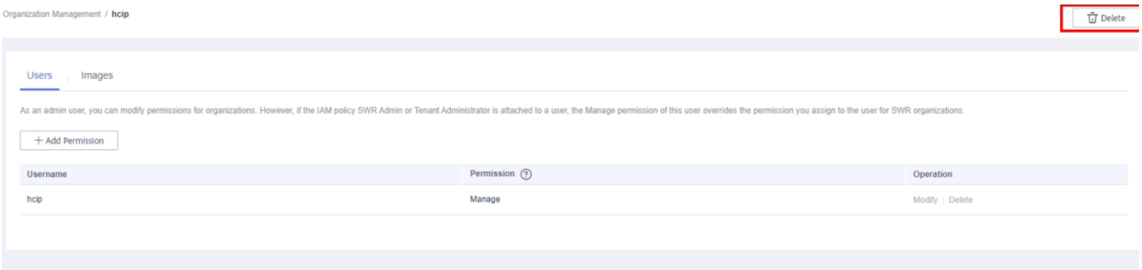


Organization/Image Name	hcip/hcip-cloudservice
Image Tags	1
Created	[redacted]
Sharing Type	Private

☑	Image Tag	Size	Updated
☑	v1	54.4 MB	[redacted]

Figure 6-86

- In the navigation pane, click **Organization Management**. Locate the organization created in this exercise, click the organization name to go to the details page, and click **Delete** in the upper right corner.



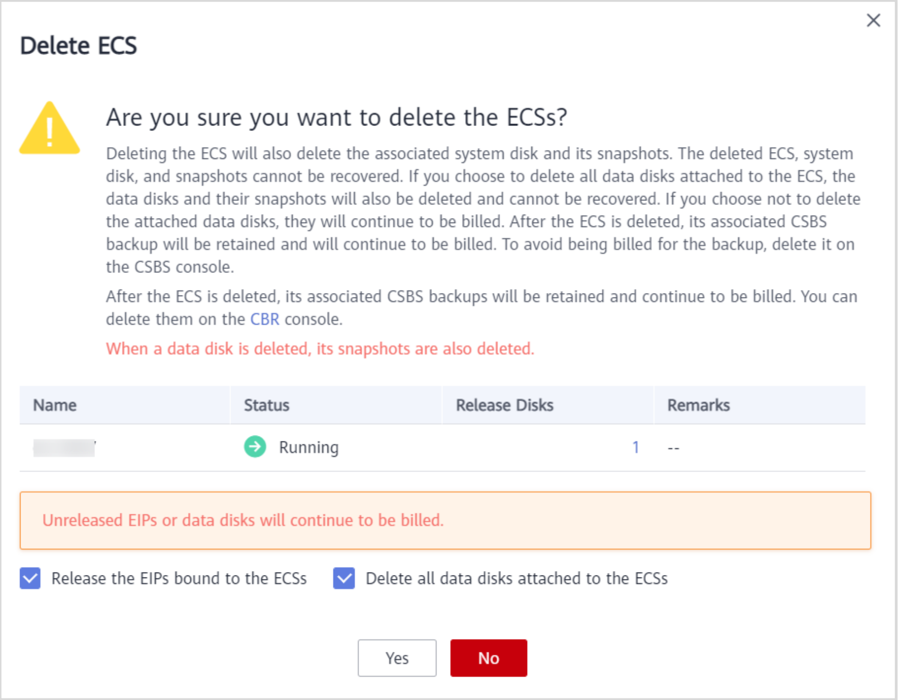
As an admin user, you can modify permissions for organizations. However, if the IAM policy SWR Admin or Tenant Administrator is attached to a user, the Manage permission of this user overrides the permission you assign to the user for SWR organizations.

Username	Permission	Operation
hcip	Manage	Modify | Delete

Figure 6-87

Step 4 Delete the ECS.

- In the service list, choose **Elastic Cloud Server** under **Compute**. In the ECS list, locate the ECS created in this exercise and choose **More** > **Delete** in the **Operation** column.
- In the displayed dialog box, select the check boxes shown in the following figure and click **Yes**.



Delete ECS

Are you sure you want to delete the ECSs?

Deleting the ECS will also delete the associated system disk and its snapshots. The deleted ECS, system disk, and snapshots cannot be recovered. If you choose to delete all data disks attached to the ECS, the data disks and their snapshots will also be deleted and cannot be recovered. If you choose not to delete the attached data disks, they will continue to be billed. After the ECS is deleted, its associated CSBS backup will be retained and will continue to be billed. To avoid being billed for the backup, delete it on the CSBS console.

After the ECS is deleted, its associated CSBS backups will be retained and continue to be billed. You can delete them on the CBR console.

When a data disk is deleted, its snapshots are also deleted.

Name	Status	Release Disks	Remarks
[redacted]	Running	1	--

Unreleased EIPs or data disks will continue to be billed.

☑ Release the EIPs bound to the ECSs ☑ Delete all data disks attached to the ECSs

Figure 6-88

Step 5 Delete the security groups.

In the service list, choose **Virtual Private Cloud** under **Networking**. On the network console, choose **Access Control** > **Security Groups**. In the security group list, locate the security group created in this exercise and click **Delete** in the **Operation** column.

Step 6 Delete the subnet and VPC.

- In the service list, choose **Virtual Private Cloud** under **Networking**. On the network console, choose **Subnets**. In the subnet list, locate the subnet created in this exercise and click **Delete** in the **Operation** column.
- Choose **Virtual Private Cloud** in the navigation pane on the left. In the VPC list, locate the VPC created in this exercise and click **Delete** in the **Operation** column.

Step 7 Delete the FunctionGraph function.

Choose **Service List** > **FunctionGraph**. On the **Functions** page on the left, locate the function created in this exercise and click **Delete** in the **Operation** column.

Step 8 Delete the SMN topic.

In the service list, choose **Simple Message Notification**. In the navigation pane, choose **Topic Management** > **Topics**. In the right pane, locate the topic created in this exercise and choose **More** > **Delete** in the **Operation** column.

Step 9 Delete the agency.

- In the upper right corner of the page, hover the mouse over the username and select **Identity and Access Management**.

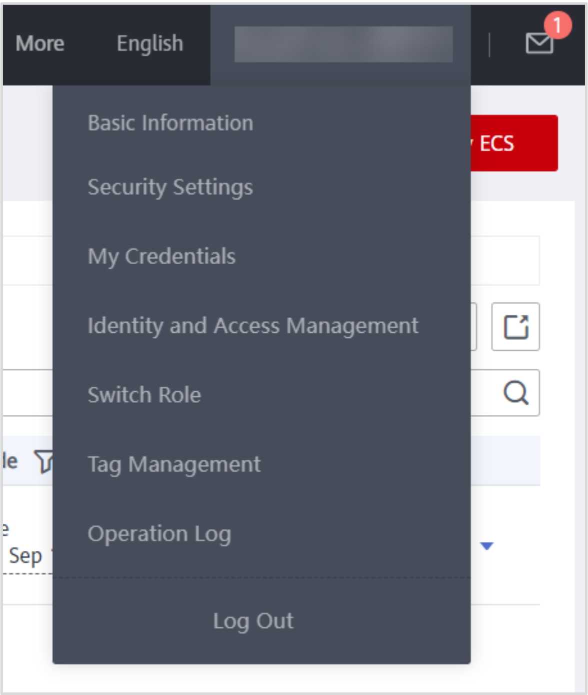


Figure 6-89

- In the navigation pane on the left, choose **Agencies**. In the agency list, locate the agency created in this exercise and click **Delete** in the **Operation** column.

Step 10 Delete the OBS bucket.

In the service list, choose **Object Storage Service**. In the bucket list, locate the bucket purchased in this exercise and click **Delete** in the **Operation** column.

6.4 Quiz

Question: What are the advantages of Huawei Cloud CCE?

Answer: Huawei Cloud CCE supports Deployments, StatefulSets, DaemonSets, jobs, and cron jobs. It supports application upgrade and scaling of nodes and workloads, streamlines deployment and upgrade, and allows hitless upgrade and automated O&M.

7 Microservice Application Deployment

7.1 Introduction

7.1.1 About This Exercise

A weather forecast microservice application provides weather forecasts as well as displays ultraviolet (UV) and humidity indexes. This exercise uses a weather forecast application to demonstrate the application scenarios of the microservice architecture and best practices of managing the runtime environment and setting up pipelines on ServiceStage.

A weather forecast service consists of a frontend application and a backend application. The frontend application weathermapweb is developed using Node.js and connected to a microservice engine using Mesher to discover the backend application. The backend application is implemented using the Java microservice development framework and includes microservices fusionweather, forecast, weather-beta, and weather.

This exercise uses the CN-Hong Kong region as an example. Trainees can select regions as required. Multiple microservice components are deployed in the environment. You are advised to configure related names based on this manual.

7.1.2 Objectives

Understand the concepts and application scenarios of the microservice architecture.

Understand methods of using ServiceStage to manage the runtime environment and build pipelines.

Understand methods and design principles for building and deploying microservices using ServiceStage.

7.1.3 Related Software

The fusionweather aggregation microservice provides comprehensive weather forecast functions by accessing the weather and forecast services. The forecast microservice allows you to query the weather in the next few days. The weather microservice allows you to query weather and humidity. The weather-beta microservice is a new version of the weather microservice and supports the function of querying the UA rays of a specified city. (This microservice is used for dark launch and does not need to be deployed in this exercise.)

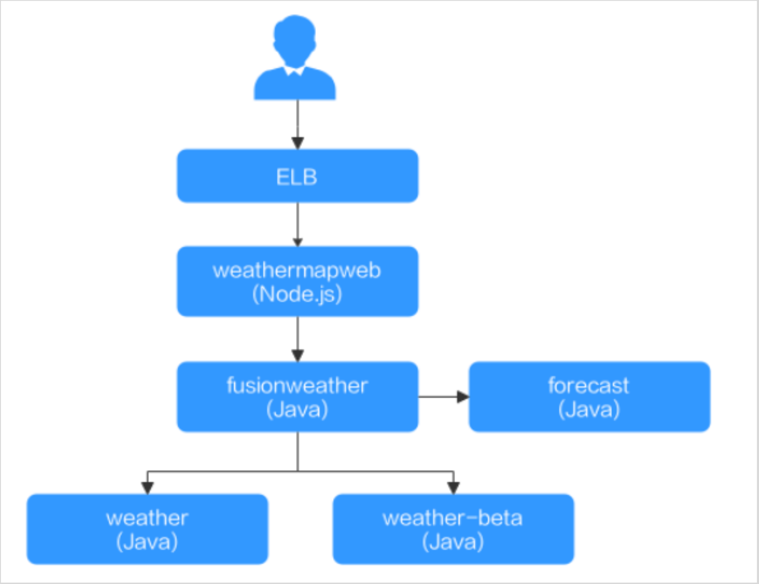


Figure 7-1

GitHub is a platform for hosting open-source and private software projects. It supports only Git as the version library format.

7.2 Procedure

7.2.1 Preparations

7.2.1.1 Preparing Resources

Step 1 Log in to Huawei Cloud and choose **My Credentials**.

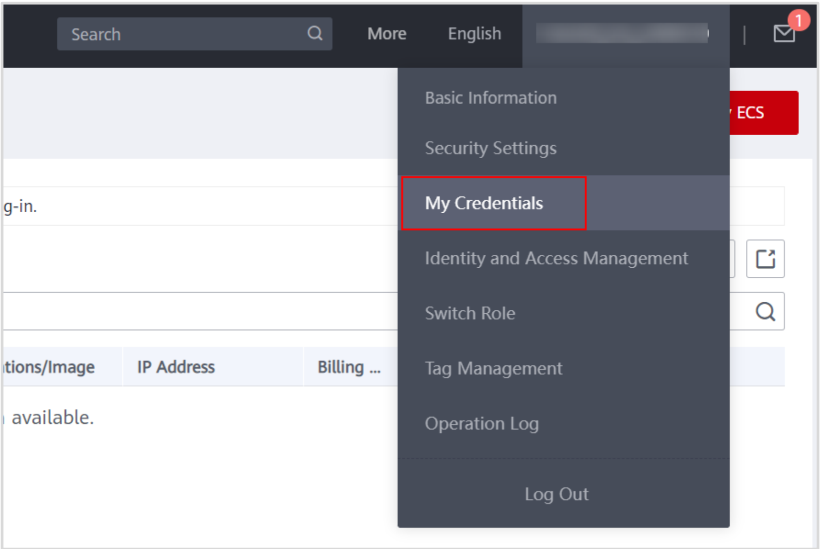
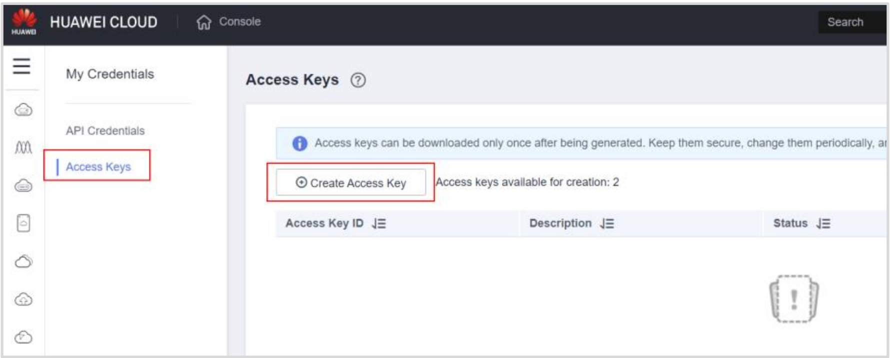


Figure 7-2

Step 2 Choose **Access Keys** and click **Create Access Key** on the right.

This access key will be used to create a key in ServiceStage.

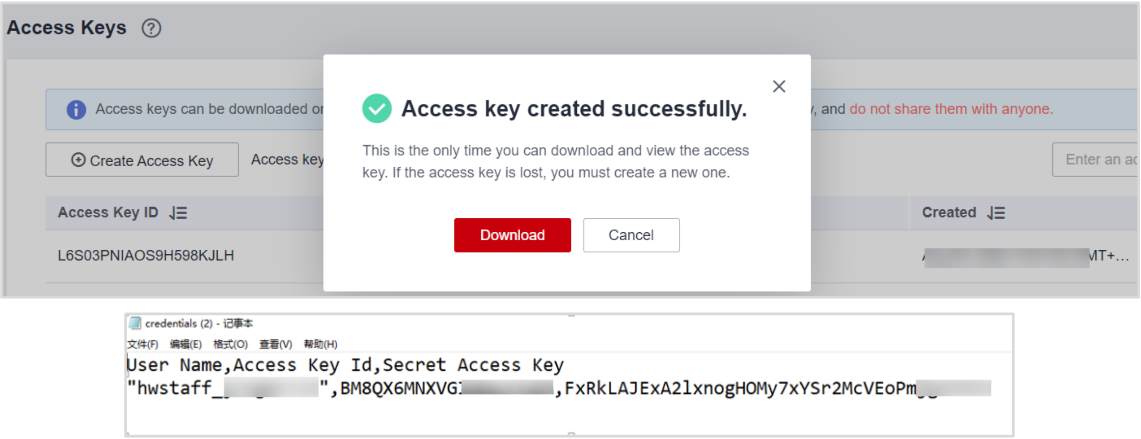


Access keys can be downloaded only once after being generated. Keep them secure, change them periodically, ar

Access keys available for creation: 2

Figure 7-3

Step 3 In the dialog box that is displayed, click **Download** and record the information.



Access keys can be downloaded or

Access key

, and do not share them with anyone.

L6S03PNIAOS9H598KJLH

Access key created successfully.

This is the only time you can download and view the access key. If the access key is lost, you must create a new one.

[redacted] MT+...

credentials (2) - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
User Name,Access Key Id,Secret Access Key
"hwstaff_[redacted]",BM8QX6MNXVG[redacted],FxRkLAJExA2lxnogHOMy7xYSr2McVEoPm[redacted]
```

Figure 7-4

Step 4 Create a VPC and subnet. For details, see the previous content.

CCE clusters will be created in this VPC.

Basic settings:

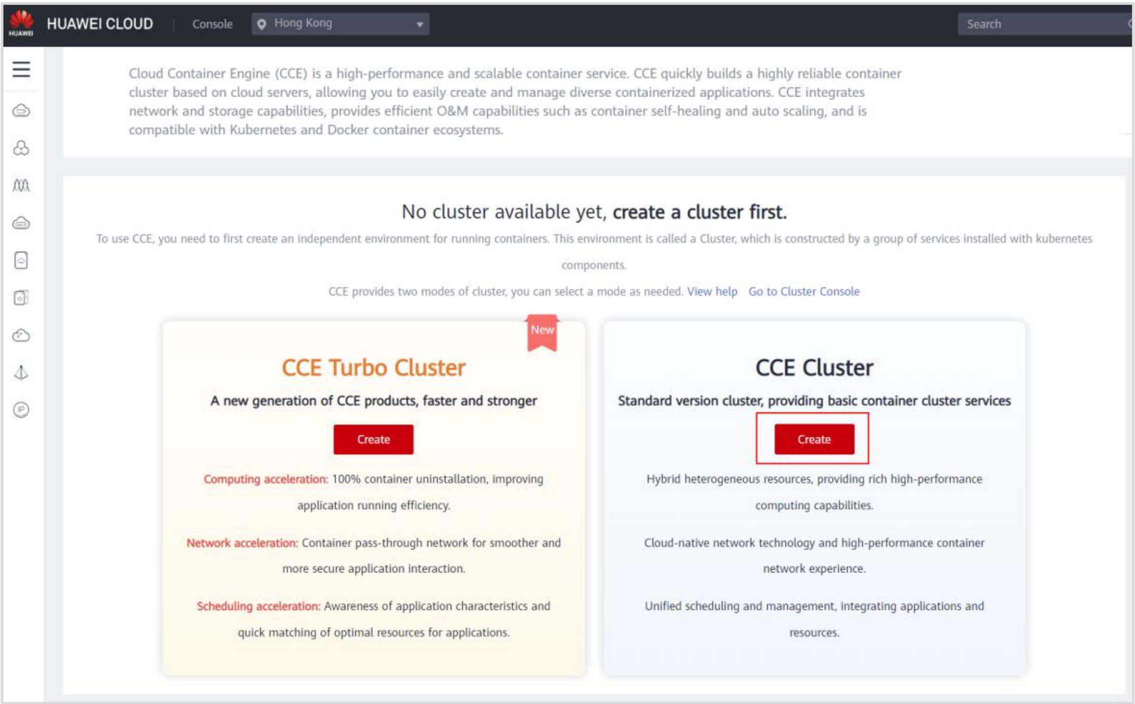
- **Region**: **CN-Hong Kong**
- **Name**: **vpc-servicestage**
- **IPv4 CIDR Block**: **192.168.0.0/16**

Default subnet

- **AZ**: **AZ2**(user-defined)
- **Name**: **subnet-servicestage**
- **IPv4 CIDR Block**: **192.168.20.0/24**

Step 5 Create a CCE cluster.

This CCE cluster will be used for container-based deployment of microservices.



Cloud Container Engine (CCE) is a high-performance and scalable container service. CCE quickly builds a highly reliable container cluster based on cloud servers, allowing you to easily create and manage diverse containerized applications. CCE integrates network and storage capabilities, provides efficient O&M capabilities such as container self-healing and auto scaling, and is compatible with Kubernetes and Docker container ecosystems.

No cluster available yet, **create a cluster first.**

To use CCE, you need to first create an independent environment for running containers. This environment is called a Cluster, which is constructed by a group of services installed with kubernetes components.

CCE provides two modes of cluster, you can select a mode as needed. View help Go to Cluster Console

CCE Turbo Cluster

New

A new generation of CCE products, faster and stronger

Create

Computing acceleration: 100% container uninstallation, improving application running efficiency.

Network acceleration: Container pass-through network for smoother and more secure application interaction.

Scheduling acceleration: Awareness of application characteristics and quick matching of optimal resources for applications.

CCE Cluster

Standard version cluster, providing basic container cluster services

Create

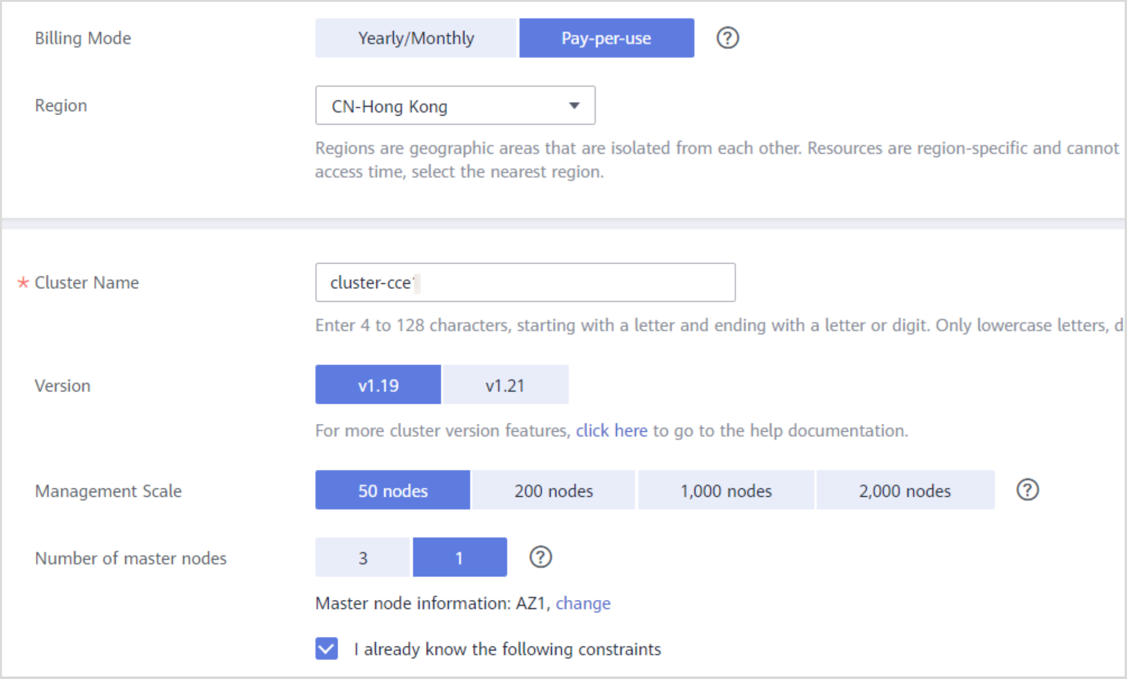
Hybrid heterogeneous resources, providing rich high-performance computing capabilities.

Cloud-native network technology and high-performance container network experience.

Unified scheduling and management, integrating applications and resources.

Figure 7-5

- Region: CN-Hong Kong
- Billing Mode: Pay-per-use
- Cluster Name: cluster-cce
- Version: v1.19
- Management Scale: 50 nodes
- Number of master nodes: 1 （This experiment is a test environment. Therefore, one node is selected. Three nodes are recommended in the production environment）



Billing Mode: Yearly/Monthly | **Pay-per-use** ⓘ

Region: CN-Hong Kong ▾

Regions are geographic areas that are isolated from each other. Resources are region-specific and cannot access time, select the nearest region.

* Cluster Name: cluster-cce

Enter 4 to 128 characters, starting with a letter and ending with a letter or digit. Only lowercase letters, d

Version: **v1.19** | v1.21

For more cluster version features, click here to go to the help documentation.

Management Scale: **50 nodes** | 200 nodes | 1,000 nodes | 2,000 nodes ⓘ

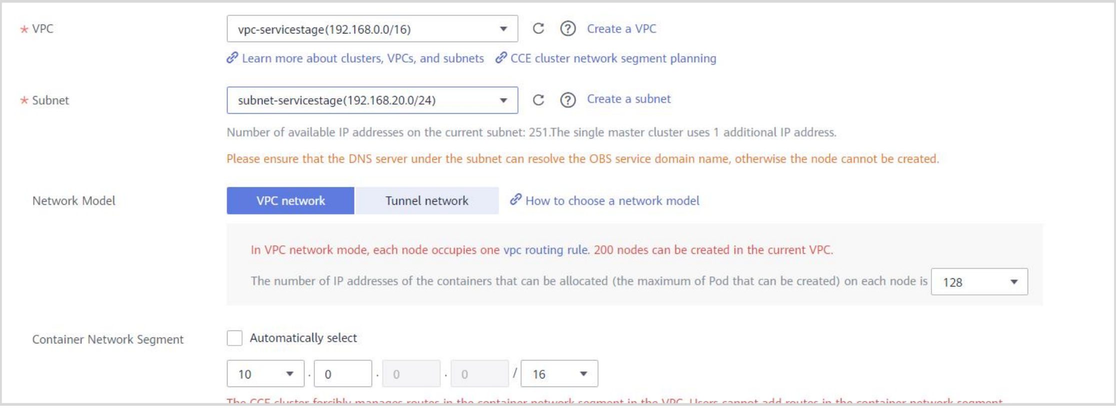
Number of master nodes: 3 | **1** ⓘ

Master node information: AZ1, change

☑ I already know the following constraints

Figure 7-6

- **Network Model: VPC network**
- **VPC: vpc-servicestage**
- **Subnet: subnet-servicestage**
- **Container Network Segment**: Retain the default value.
- **Create Node: Create later**



* VPC: vpc-servicestage(192.168.0.0/16) ▾ Create a VPC

Learn more about clusters, VPCs, and subnets CCE cluster network segment planning

* Subnet: subnet-servicestage(192.168.20.0/24) ▾ Create a subnet

Number of available IP addresses on the current subnet: 251.The single master cluster uses 1 additional IP address.

Please ensure that the DNS server under the subnet can resolve the OBS service domain name, otherwise the node cannot be created.

Network Model: **VPC network** | Tunnel network How to choose a network model

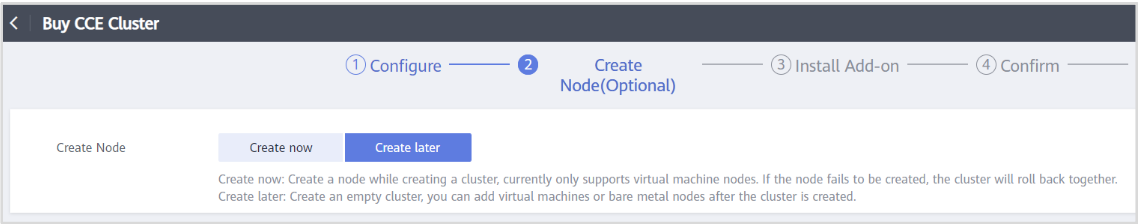
In VPC network mode, each node occupies one vpc routing rule. 200 nodes can be created in the current VPC.

The number of IP addresses of the containers that can be allocated (the maximum of Pod that can be created) on each node is 128 ▾

Container Network Segment: □ Automatically select

10 ▾ . 0 . 0 . 0 / 16 ▾

The CCE cluster forcibly manages routes in the container network segment in the VPC. Users cannot add routes in the container network segment.

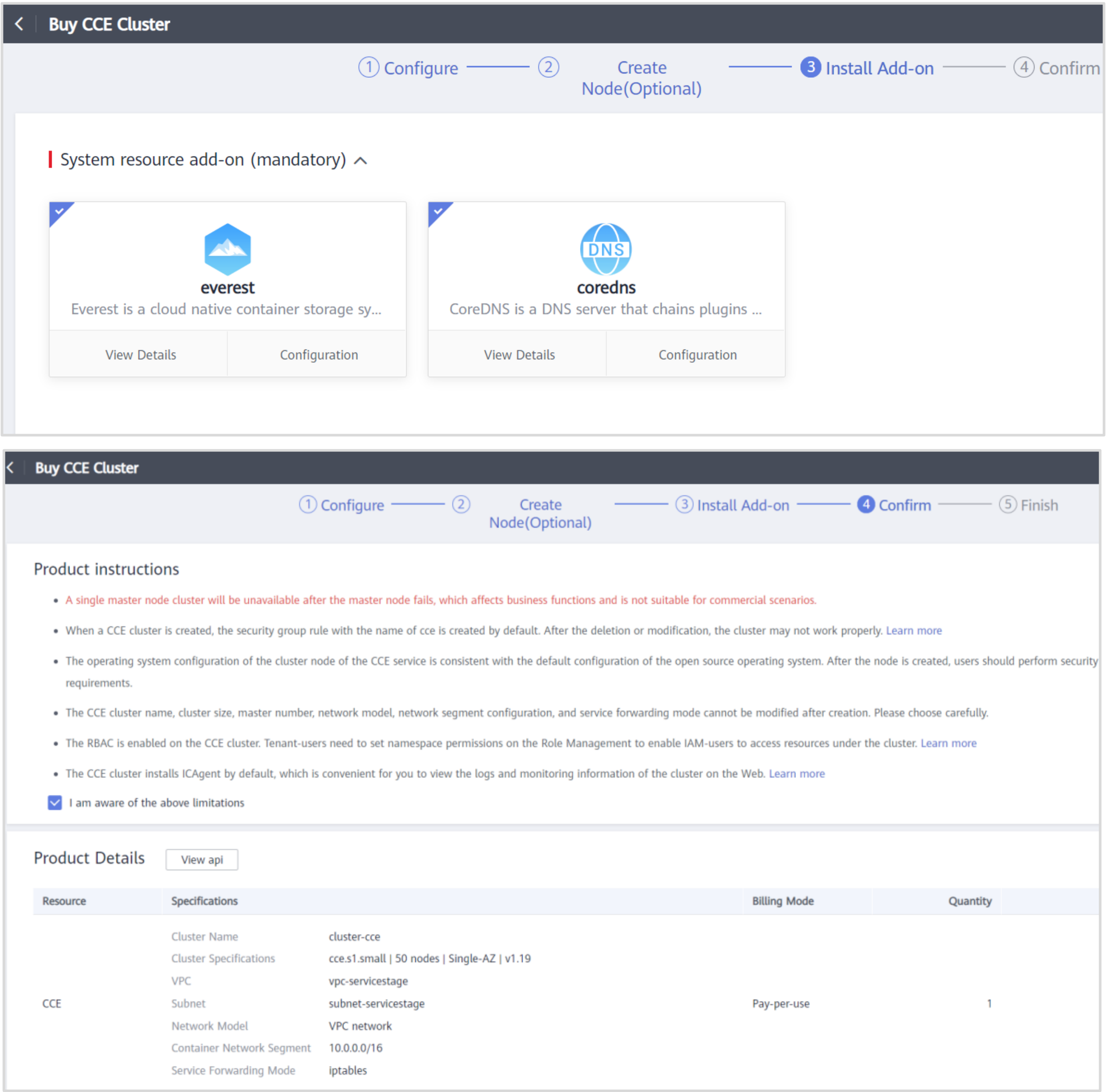


Buy CCE Cluster

① Configure — ② Create Node(Optional) — ③ Install Add-on — ④ Confirm

Create Node: Create now | **Create later**

Create now: Create a node while creating a cluster, currently only supports virtual machine nodes. If the node fails to be created, the cluster will roll back together.
Create later: Create an empty cluster, you can add virtual machines or bare metal nodes after the cluster is created.



System resource add-on (mandatory)

Product instructions

- A single master node cluster will be unavailable after the master node fails, which affects business functions and is not suitable for commercial scenarios.
- When a CCE cluster is created, the security group rule with the name of cce is created by default. After the deletion or modification, the cluster may not work properly. Learn more
- The operating system configuration of the cluster node of the CCE service is consistent with the default configuration of the open source operating system. After the node is created, users should perform security requirements.
- The CCE cluster name, cluster size, master number, network model, network segment configuration, and service forwarding mode cannot be modified after creation. Please choose carefully.
- The RBAC is enabled on the CCE cluster. Tenant-users need to set namespace permissions on the Role Management to enable IAM-users to access resources under the cluster. Learn more
- The CCE cluster installs ICAgent by default, which is convenient for you to view the logs and monitoring information of the cluster on the Web. Learn more

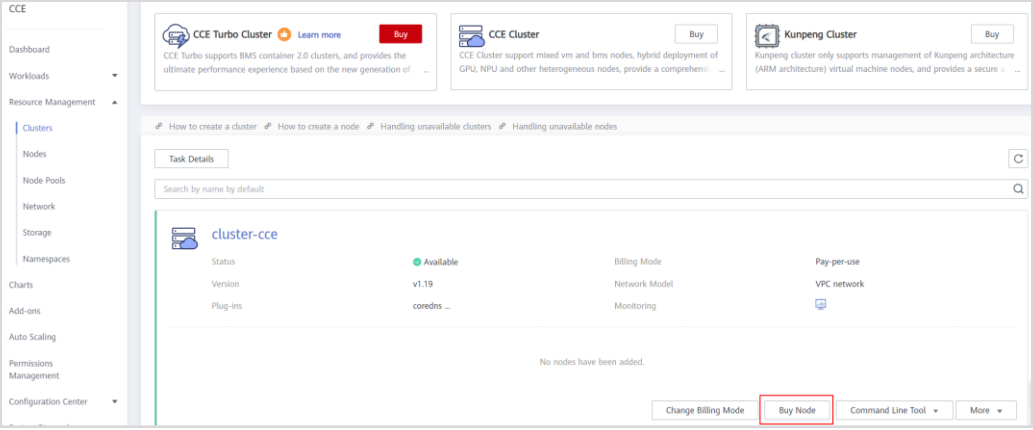
☑ I am aware of the above limitations

Product Details View api

Resource	Specifications		Billing Mode	Quantity
CCE	Cluster Name	cluster-cce	Pay-per-use	1
	Cluster Specifications	cce.s1.small | 50 nodes | Single-AZ | v1.19		
	VPC	vpc-servicestage		
	Subnet	subnet-servicestage		
	Network Model	VPC network		
	Container Network Segment	10.0.0.0/16		
	Service Forwarding Mode	iptables		

Figure 7-7

Step 6 After the cluster is created, click **Buy Node** to create a node for the CCE cluster.



CCE Turbo supports BMS container 2.0 clusters, and provides the ultimate performance experience based on the new generation of ...

CCE Cluster support mixed vm and bms nodes, hybrid deployment of GPU, NPU and other heterogeneous nodes, provide a comprehensi ...

Kunpeng cluster only supports management of Kunpeng architecture (ARM architecture) virtual machine nodes, and provides a secure a ...

cluster-cce

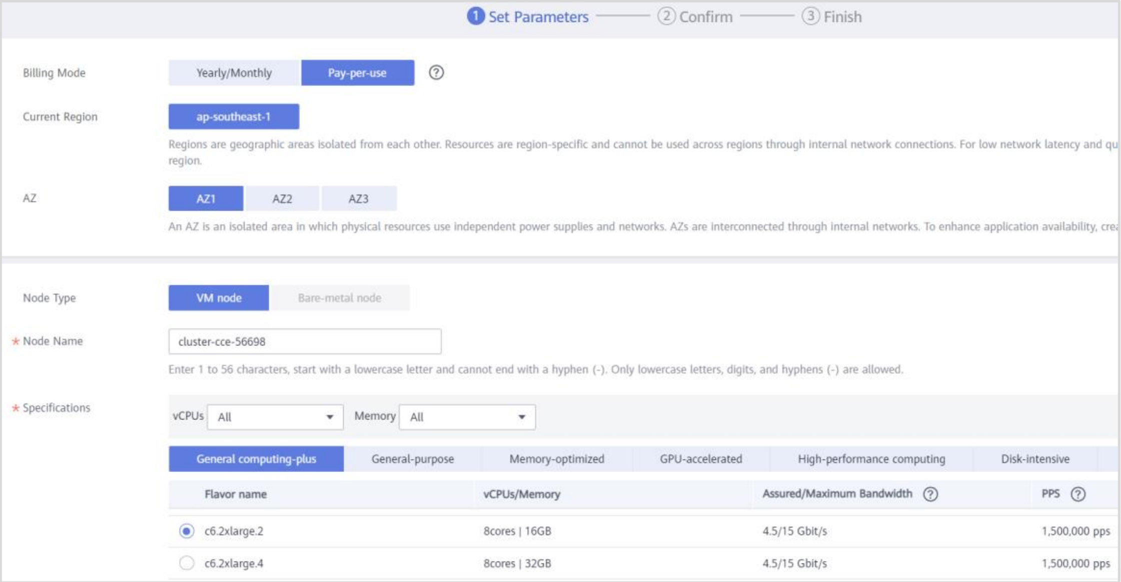
Status	Available	Billing Mode	Pay-per-use
Version	v1.19	Network Model	VPC network
Plug-ins	coredns ...	Monitoring	

No nodes have been added.

Figure 7-8

Step 7 Set the parameters as follows, confirm the configuration, and click **Submit**.

- **Billing Mode: Pay-per-use**
- **AZ: Random**
- **Node Type: VM node**
- **Node Name**: Use the default name or customize one.
- **Specifications: 8 cores | 16 GB**



Billing Mode: Yearly/Monthly [✓ Pay-per-use]

Current Region: ap-southeast-1

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and qu region.

AZ: [✓ AZ1] AZ2 AZ3

An AZ is an isolated area in which physical resources use independent power supplies and networks. AZs are interconnected through internal networks. To enhance application availability, crea

Node Type: [✓ VM node] Bare-metal node

* Node Name: cluster-cce-56698

Enter 1 to 56 characters, start with a lowercase letter and cannot end with a hyphen (-). Only lowercase letters, digits, and hyphens (-) are allowed.

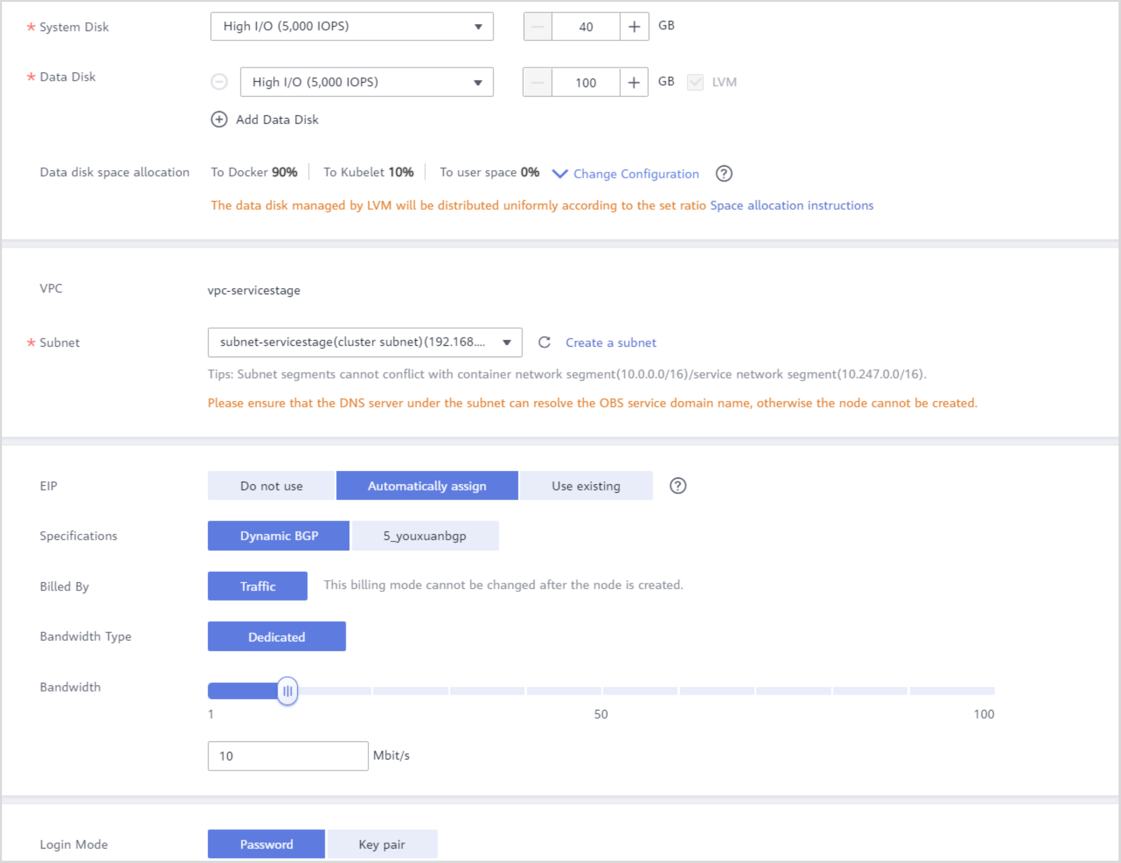
* Specifications: vCPUs: All Memory: All

[✓ General computing-plus] General-purpose Memory-optimized GPU-accelerated High-performance computing Disk-intensive

	Flavor name	vCPUs/Memory	Assured/Maximum Bandwidth	PPS
●	c6.2xlarge.2	8cores | 16GB	4.5/15 Gbit/s	1,500,000 pps
○	c6.2xlarge.4	8cores | 32GB	4.5/15 Gbit/s	1,500,000 pps

Figure 7-9

- **OS: EulerOS 2.5**
- **System Disk**: Use the default setting.
- **Data Disk**: Use the default setting.
- **Subnet: subnet-servicestage**
- **EIP: Automatically assign**
- **Billed By: Traffic**
- **Bandwidth: 10 Mbit/s**
- **Login Mode: Password**
- **Password**: Customize one.



* System Disk: High I/O (5,000 IOPS) — 40 GB

* Data Disk: High I/O (5,000 IOPS) — 100 GB ☐ LVM

Add Data Disk

Data disk space allocation: To Docker **90%** | To Kubelet **10%** | To user space **0%** Change Configuration

The data disk managed by LVM will be distributed uniformly according to the set ratio Space allocation instructions

VPC: vpc-servicestage

* Subnet: subnet-servicestage(cluster subnet)(192.168.... Create a subnet

Tips: Subnet segments cannot conflict with container network segment(10.0.0.0/16)/service network segment(10.247.0.0/16).

Please ensure that the DNS server under the subnet can resolve the OBS service domain name, otherwise the node cannot be created.

EIP: Do not use | **Automatically assign** | Use existing

Specifications: **Dynamic BGP** | 5_youxuanbgp

Billed By: **Traffic** This billing mode cannot be changed after the node is created.

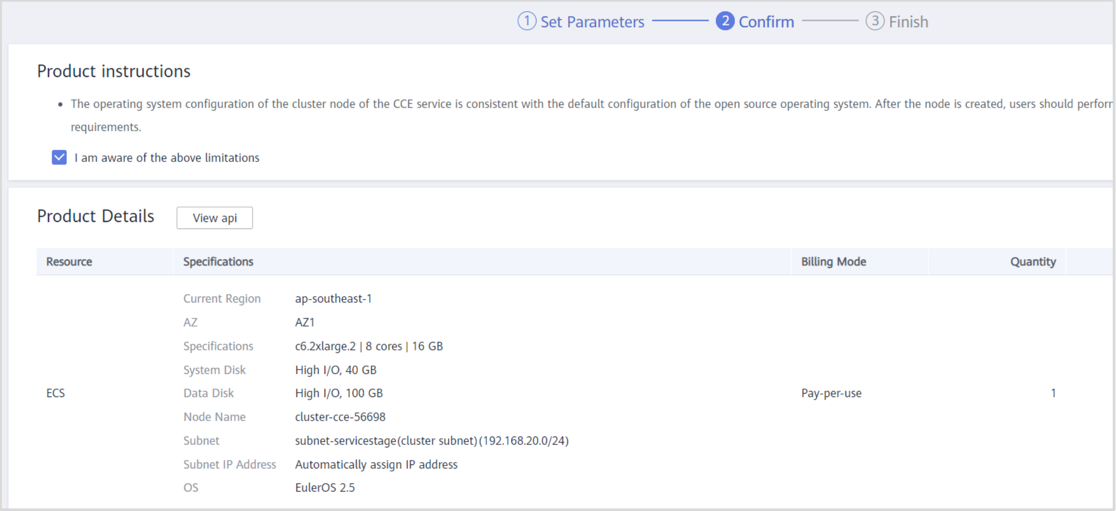
Bandwidth Type: **Dedicated**

Bandwidth: 10 Mbit/s

Login Mode: **Password** | Key pair

Figure 7-10

Step 8 Confirm the configuration and click **Finish**.



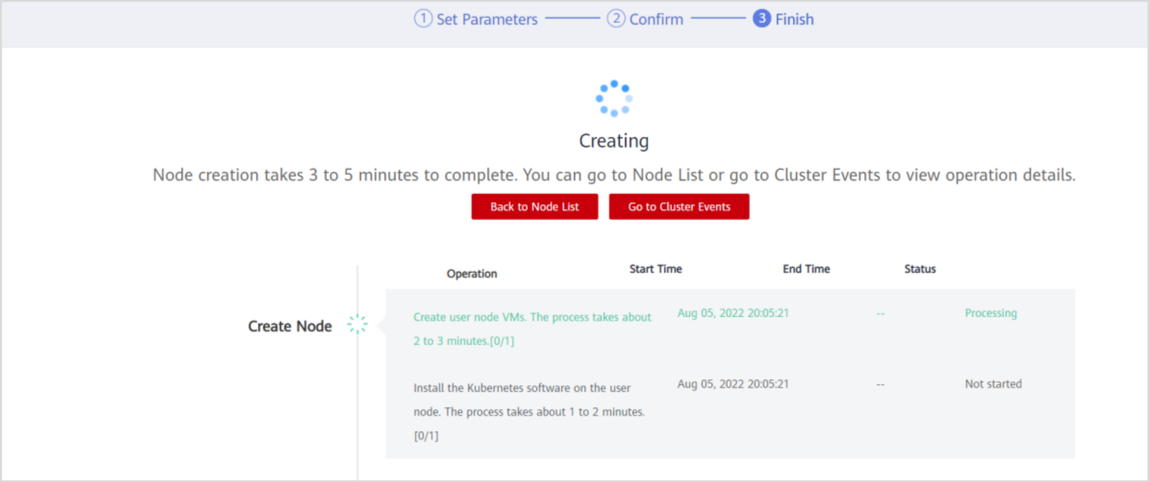
Product instructions

- The operating system configuration of the cluster node of the CCE service is consistent with the default configuration of the open source operating system. After the node is created, users should perforr requirements.

☑ I am aware of the above limitations

Product Details View api

Resource	Specifications		Billing Mode	Quantity
ECS	Current Region	ap-southeast-1	Pay-per-use	1
	AZ	AZ1		
	Specifications	c6.2xlarge.2 | 8 cores | 16 GB		
	System Disk	High I/O, 40 GB		
	Data Disk	High I/O, 100 GB		
	Node Name	cluster-cce-56698		
	Subnet	subnet-servicestage(cluster subnet)(192.168.20.0/24)		
	Subnet IP Address	Automatically assign IP address		
	OS	EulerOS 2.5		



① Set Parameters —— ② Confirm —— ③ Finish

Creating

Node creation takes 3 to 5 minutes to complete. You can go to Node List or go to Cluster Events to view operation details.

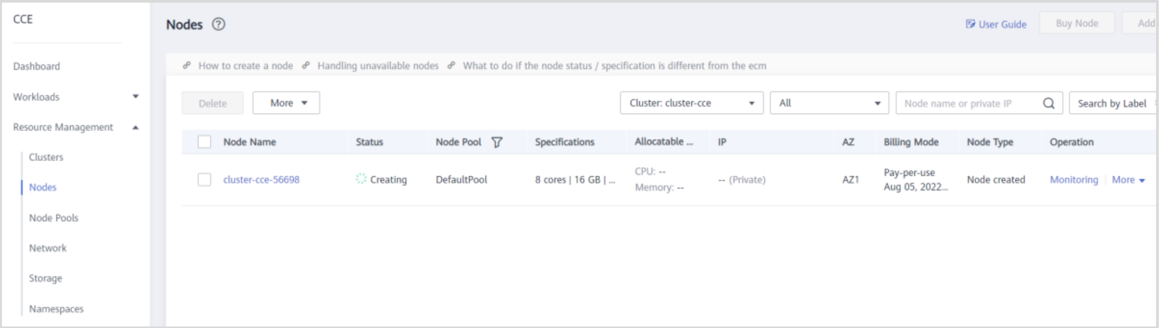
Back to Node List | Go to Cluster Events

Create Node

Operation	Start Time	End Time	Status
Create user node VMs. The process takes about 2 to 3 minutes.[0/1]	Aug 05, 2022 20:05:21	--	Processing
Install the Kubernetes software on the user node. The process takes about 1 to 2 minutes.[0/1]	Aug 05, 2022 20:05:21	--	Not started

Figure 7-11

Step 9 On the **Nodes** page that is displayed, view the information about the created node.



Nodes

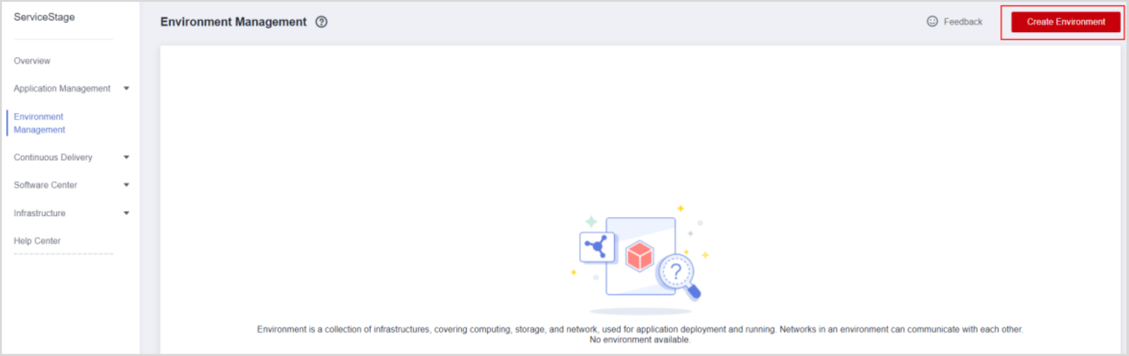
How to create a node · Handling unavailable nodes · What to do if the node status / specification is different from the ecm

Node Name	Status	Node Pool	Specifications	Allocatable ...	IP	AZ	Billing Mode	Node Type	Operation
cluster-cce-56698	Creating	DefaultPool	8 cores | 16 GB | ...	CPU: -- Memory: --	-- (Private)	AZ1	Pay-per-use Aug 05, 2022...	Node created	Monitoring More

Figure 7-12

7.2.1.2 Creating an Environment

Step 1 Log in to ServiceStage, choose **Environment Management**, and click **Create Environment**.



Environment Management

Environment is a collection of infrastructures, covering computing, storage, and network, used for application deployment and running. Networks in an environment can communicate with each other.

No environment available.

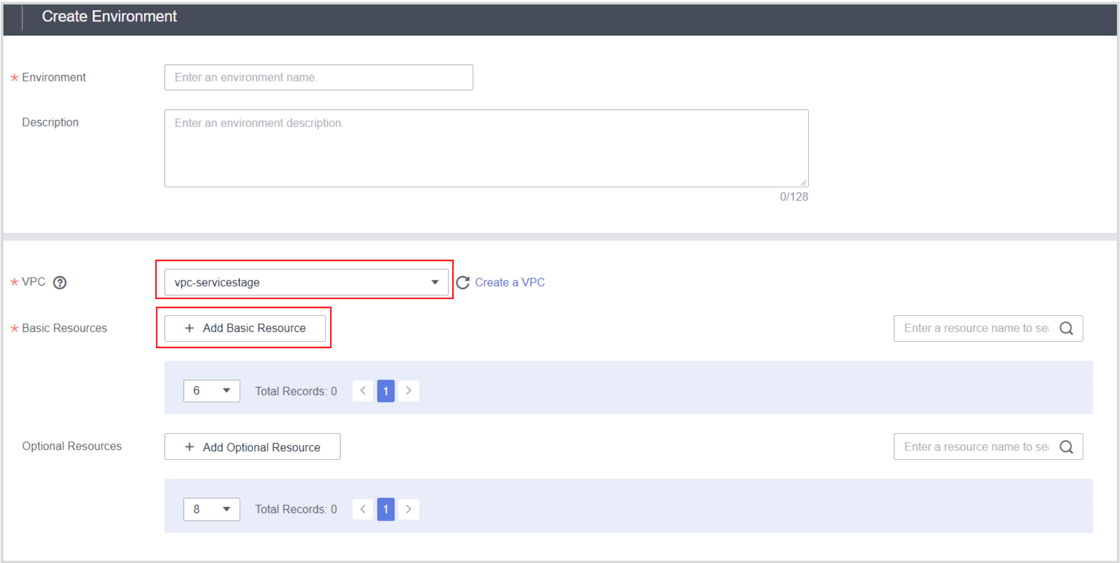
Figure 7-13

Step 2 Set the following parameters and click **Add Basic Resource**.

This environment will be selected for subsequent microservice deployment.

- **Environment: test-env**

- **VPC: vpc-1**



Create Environment

* Environment: Enter an environment name.

Description: Enter an environment description. 0/128

* VPC: vpc-servicestage ▾ Create a VPC

* Basic Resources: + Add Basic Resource — Enter a resource name to se

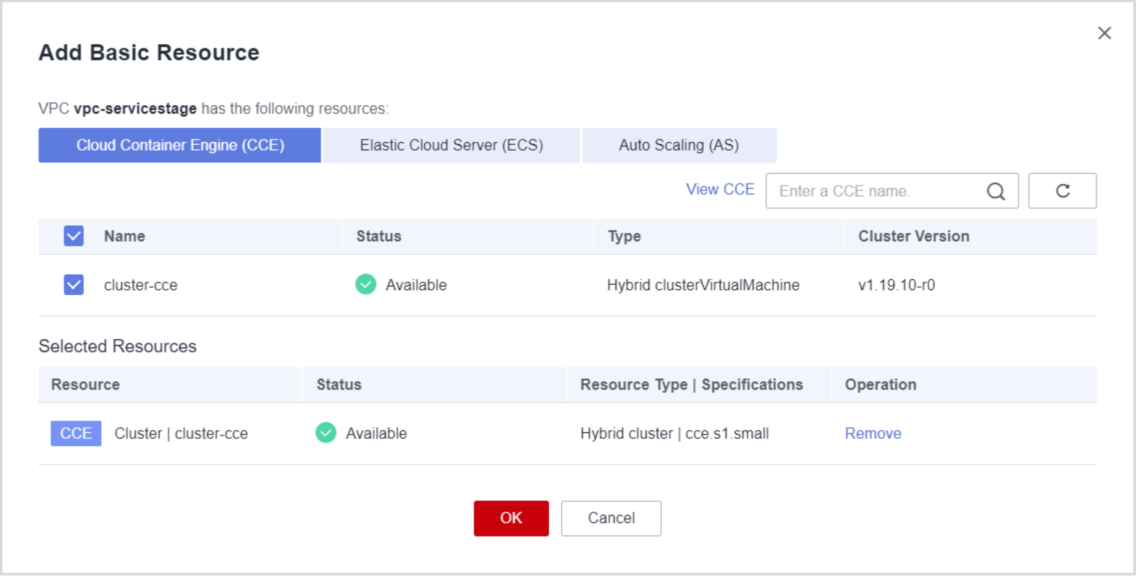
6 ▾ Total Records: 0 < 1 >

Optional Resources: + Add Optional Resource — Enter a resource name to se

8 ▾ Total Records: 0 < 1 >

Figure 7-14

Step 3 On the **Cloud Container Engine (CCE)** tab page, select the created CCE cluster and click **OK**.



Add Basic Resource

VPC **vpc-servicestage** has the following resources:

Cloud Container Engine (CCE) | Elastic Cloud Server (ECS) | Auto Scaling (AS)

View CCE — Enter a CCE name.

☑ Name	Status	Type	Cluster Version
☑ cluster-cce	✓ Available	Hybrid clusterVirtualMachine	v1.19.10-r0

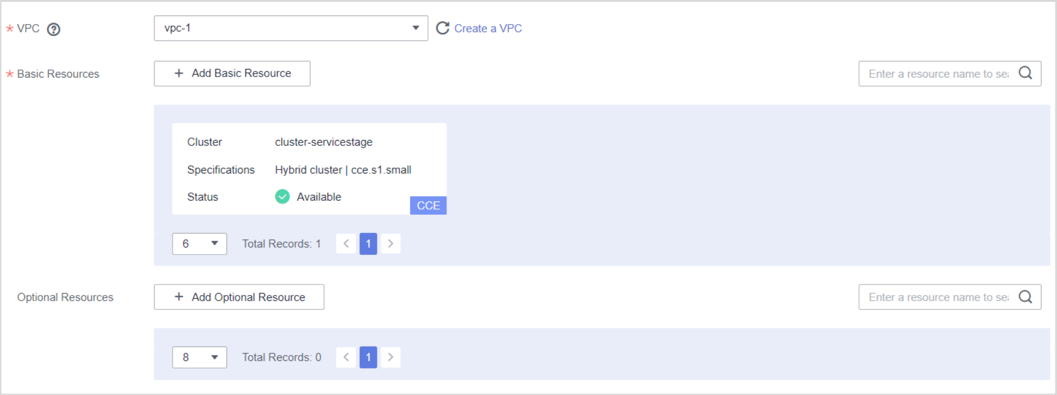
Selected Resources

Resource	Status	Resource Type | Specifications	Operation
CCE Cluster | cluster-cce	✓ Available	Hybrid cluster | cce.s1.small	Remove

OK Cancel

Figure 7-15

Step 4 Click **Add Optional Resource**.



* VPC ⓘ vpc-1 ▾ Create a VPC

* Basic Resources ＋ Add Basic Resource Enter a resource name to sea

Cluster	cluster-servicestage
Specifications	Hybrid cluster | cce.s1.small
Status	Available

CCE

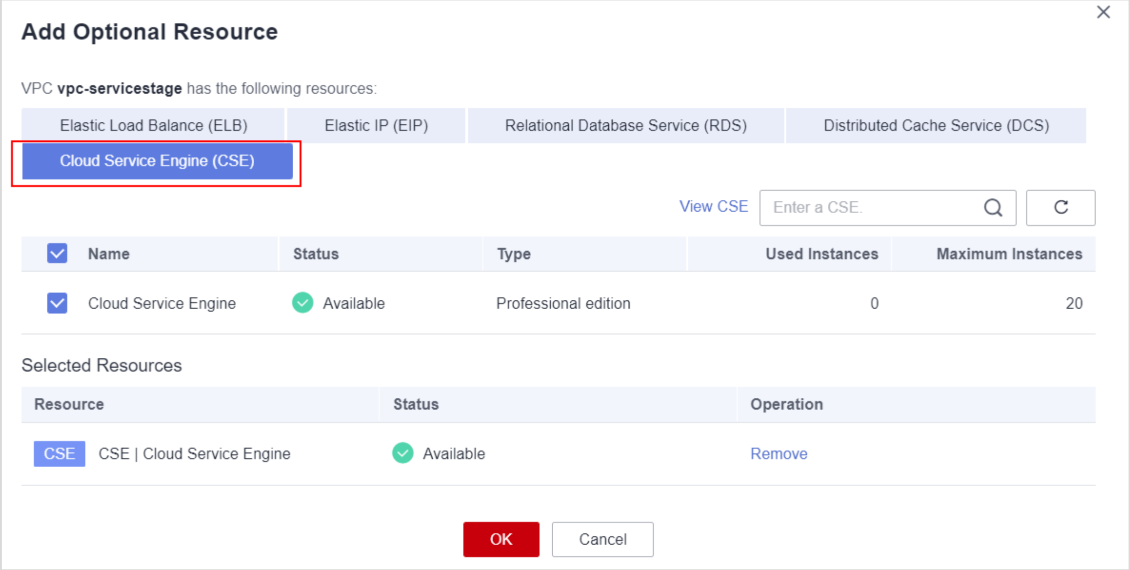
6 ▾ Total Records: 1 ‹ 1 ›

Optional Resources ＋ Add Optional Resource Enter a resource name to sea

8 ▾ Total Records: 0 ‹ 1 ›

Figure 7-16

Step 5 On the **Cloud Service Engine (CSE)** tab page, select **Cloud Service Engine**, click **OK**, and click **Create Now**.



Add Optional Resource ✕

VPC **vpc-servicestage** has the following resources:

Elastic Load Balance (ELB) | Elastic IP (EIP) | Relational Database Service (RDS) | Distributed Cache Service (DCS) | Cloud Service Engine (CSE)

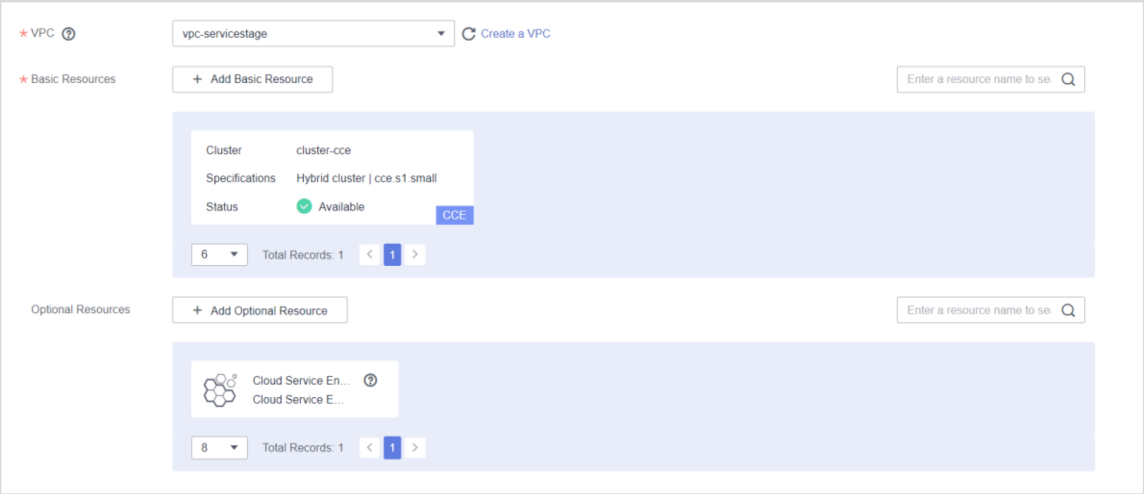
View CSE Enter a CSE.

☑ Name	Status	Type	Used Instances	Maximum Instances
☑ Cloud Service Engine	Available	Professional edition	0	20

Selected Resources

Resource	Status	Operation
CSE CSE | Cloud Service Engine	Available	Remove

OK Cancel



* VPC ⓘ vpc-servicestage ▾ Create a VPC

* Basic Resources ＋ Add Basic Resource Enter a resource name to sea

Cluster	cluster-cce
Specifications	Hybrid cluster | cce.s1.small
Status	Available

CCE

6 ▾ Total Records: 1 ‹ 1 ›

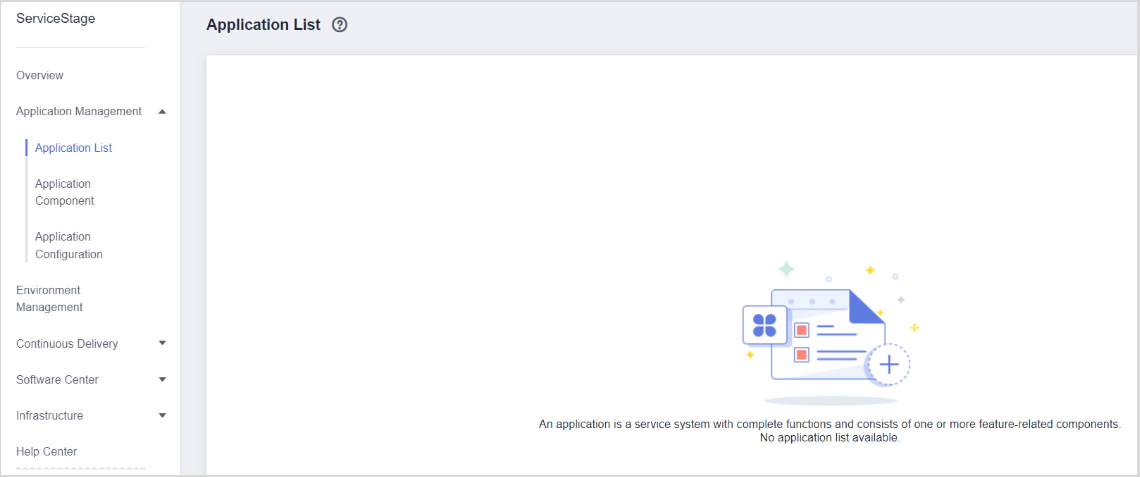
Optional Resources ＋ Add Optional Resource Enter a resource name to sea

Cloud Service En... ⓘ
Cloud Service E...

8 ▾ Total Records: 1 ‹ 1 ›

Figure 7-17

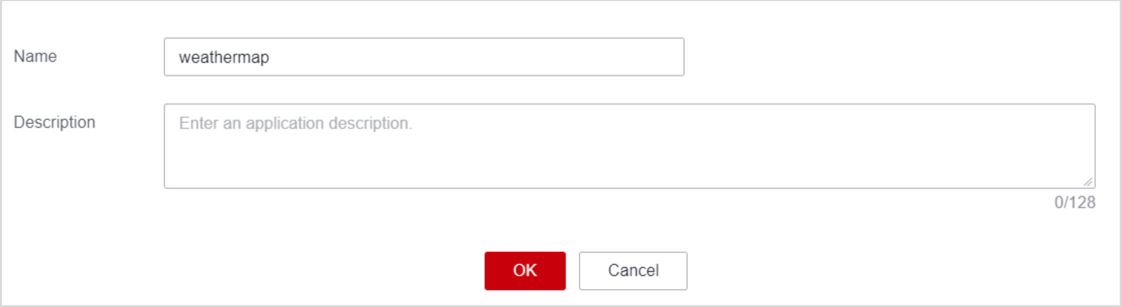
Step 6 Choose **ServiceStage** from **Service List**. In the **Application List**, click **Create Application** in the upper right corner.



An application is a service system with complete functions and consists of one or more feature-related components.
No application list available.

Figure 7-18

Step 7 Set **Name** to **weathermap** and click **OK**.



Name: weathermap

Description: Enter an application description.

0/128

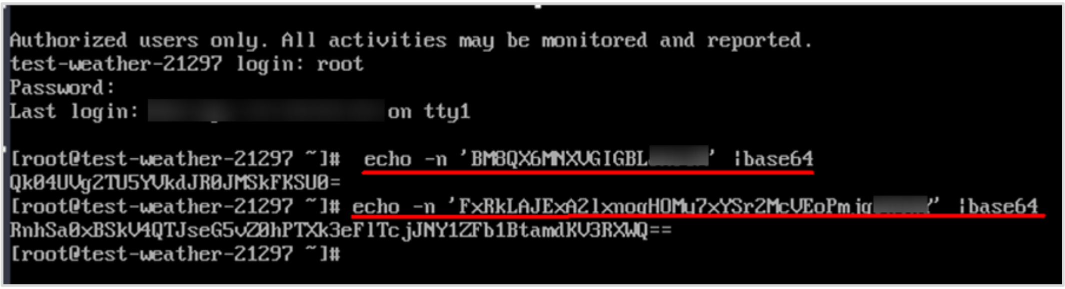
Figure 7-19

7.2.1.3 Creating a Secret

Step 1 Encode the AK/SK obtained using Base64. In the local Linux environment, run the **echo -n '***Content to be encoded***' | base64** command.

Note：You can also create an ECS and run related commands in the ECS.

```
echo -n 'BM8QX6MNXVGIGXXXXXXX' | base64                              #AK
echo -n 'FxRkLAJExA2lxnogHOMy7xYSr2McVEoXXXXXXXXXX' | base64       #SK
```

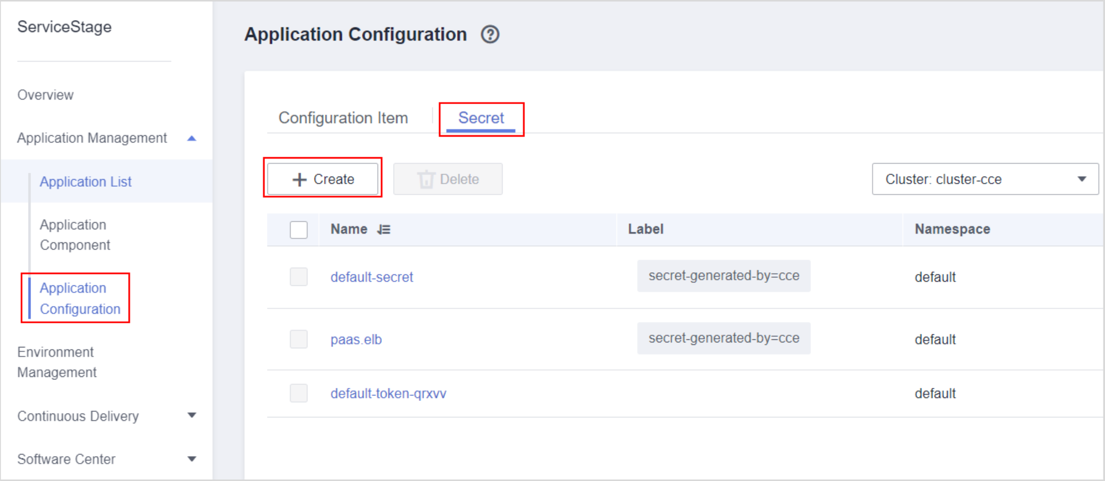


```
Authorized users only. All activities may be monitored and reported.
test-weather-21297 login: root
Password:
Last login: [redacted] on tty1

[root@test-weather-21297 ~]#  echo -n 'BM8QX6MNXUGIGBL[redacted]' |base64
Qk04UUg2TU5YVkdJR0JMSkFKSU0=
[root@test-weather-21297 ~]# echo -n 'FxRkLAJExA21xnoqHOMu7xYSr2McVEoPmjq[redacted]' |base64
RnhSa0xBSkV4QTJseG5vZ0hPTXk3eF1TcjJNY1ZFb1BtamdKU3RXWQ==
[root@test-weather-21297 ~]#
```

Figure 7-20

Step 2 Log in to ServiceStage and choose **Application Management** > **Application Configuration** > **Secret** > **Create**.

You can create a secret for the frontend application component weathermapweb that is based on the Mesher framework. After the component is deployed and running, Mesher automatically reads the secret information.

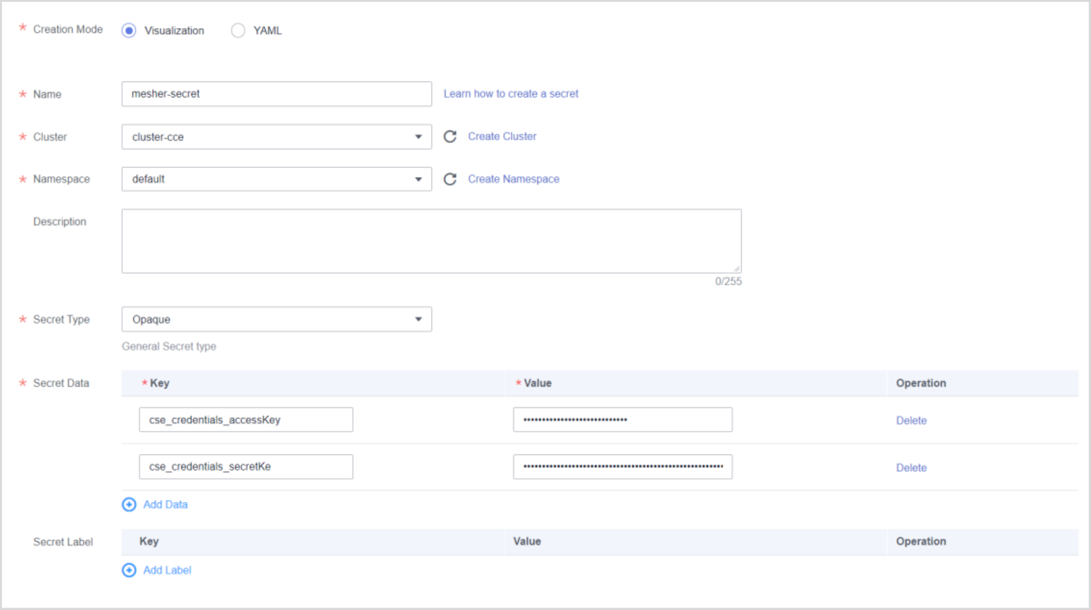


Name	Label	Namespace
default-secret	secret-generated-by=cce	default
paas.elb	secret-generated-by=cce	default
default-token-qrxvv		default

Figure 7-21

Step 3 Set the parameters as follows:

- **Creation Mode**: **Visualization**
- **Name**: **mesher-secret**
- **Cluster**: **cluster-cce**
- **Namespace**: **default**
- **Secret Type**: **Opaque**
- **Secret Data**: cse_credentials_accessKey | encoded AK; cse_credentials_secretKey | encoded SK



* Creation Mode ● Visualization ○ YAML

* Name: mesher-secret — Learn how to create a secret

* Cluster: cluster-cce — Create Cluster

* Namespace: default — Create Namespace

Description: 0/255

* Secret Type: Opaque

General Secret type

* Secret Data

* Key	* Value	Operation
cse_credentials_accessKey	•••••••••••••••••••••••••••	Delete
cse_credentials_secretKe	••	Delete

Add Data

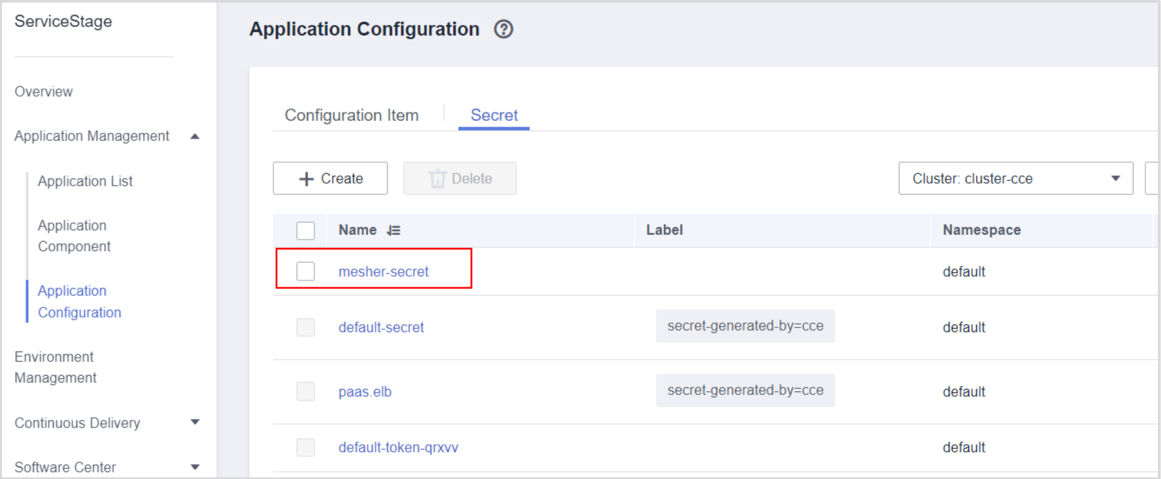
Secret Label

Key	Value	Operation

Add Label

Figure 7-22

Step 4 If the created secret is displayed in the secret list, the secret is created.



Application Configuration

Configuration Item | Secret

+ Create | Delete | Cluster: cluster-cce

□	Name	Label	Namespace
□	mesher-secret		default
□	default-secret	secret-generated-by=cce	default
□	paas.elb	secret-generated-by=cce	default
□	default-token-qrxvv		default

Figure 7-23

7.2.1.4 Preparing the Weather Forecast Source Code

If you do not have a GitHub account, log in to the GitHub official website and register an account.

Step 1 Log in to the GitHub account and click the **Repositories** tab on the personal homepage.

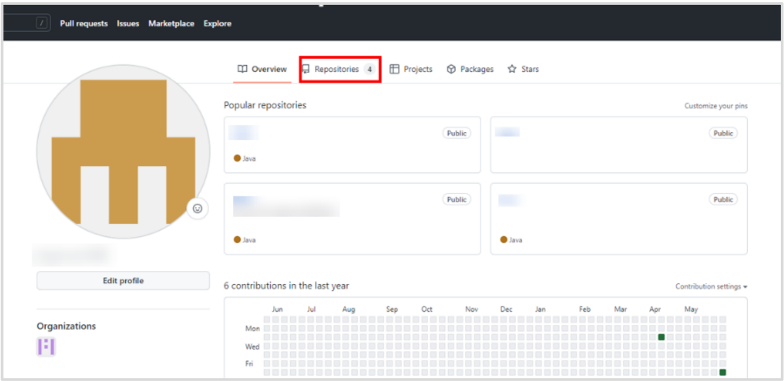


Figure 7-24

Step 2 Click **New** to create an organization.

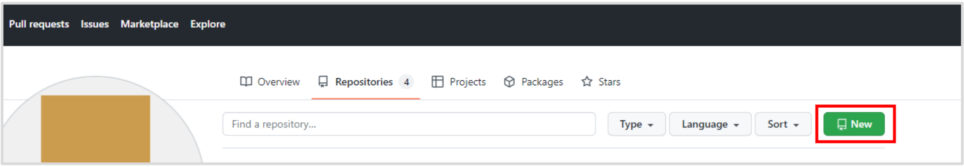
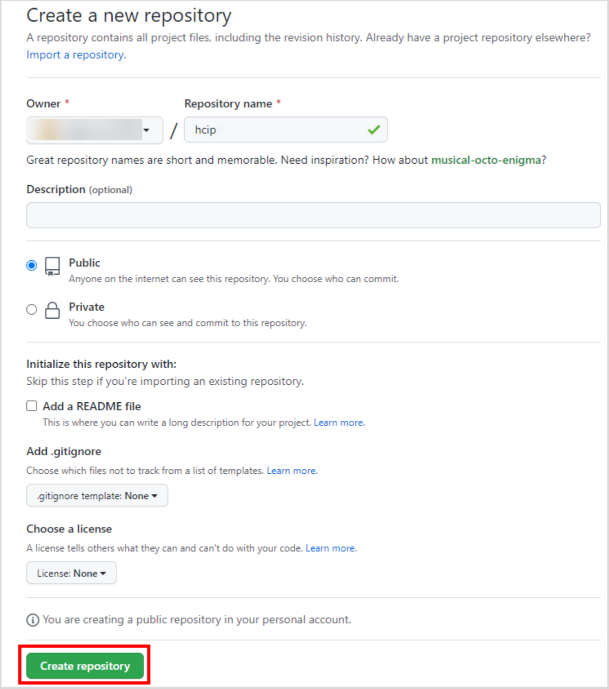


Figure 7-25

Step 3 Create a repository based on the following configurations and click **Create repository**.

- **Repository name**: **hcip**
- Retain the default settings for other parameters.



Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? Import a repository.

Owner * / Repository name *

hcip ✓

Great repository names are short and memorable. Need inspiration? How about musical-octo-enigma?

Description (optional)

● Public
Anyone on the internet can see this repository. You choose who can commit.

○ Private
You choose who can see and commit to this repository.

Initialize this repository with:
Skip this step if you're importing an existing repository.

□ Add a README file
This is where you can write a long description for your project. Learn more.

Add .gitignore
Choose which files not to track from a list of templates. Learn more.

.gitignore template: None ▾

Choose a license
A license tells others what they can and can't do with your code. Learn more.

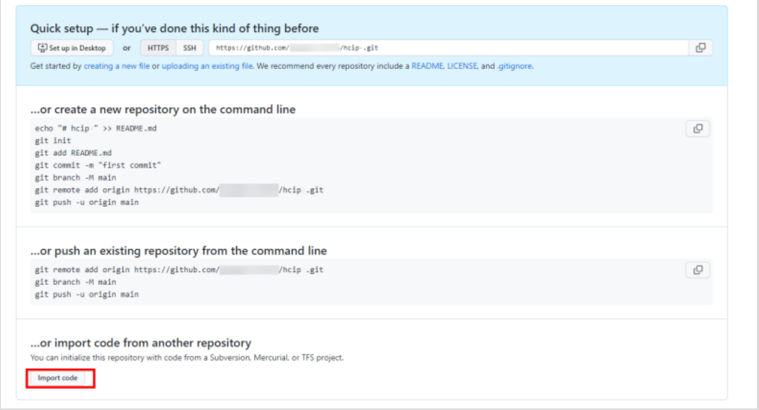
License: None ▾

ⓘ You are creating a public repository in your personal account.

Create repository

Figure 7-26

Step 4 On the page that is displayed, click **Import code** to import the source code.



Quick setup — if you've done this kind of thing before

https://github.com/[redacted]/hcip .git

Get started by creating a new file or uploading an existing file. We recommend every repository include a README, LICENSE, and .gitignore.

...or create a new repository on the command line

```
echo "# hcip " >> README.md
git init
git add README.md
git commit -m "first commit"
git branch -M main
git remote add origin https://github.com/[redacted]/hcip .git
git push -u origin main
```

...or push an existing repository from the command line

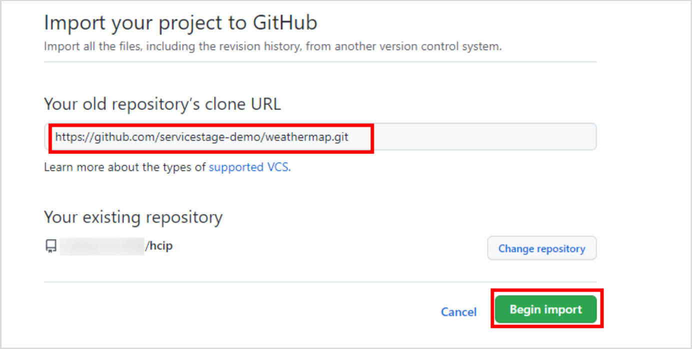
```
git remote add origin https://github.com/[redacted]/hcip .git
git branch -M main
git push -u origin main
```

...or import code from another repository

You can initialize this repository with code from a Subversion, Mercurial, or TFS project.

Figure 7-27

Step 5 On the page that is displayed, enter the source code address https://github.com/servicestage-demo/weathermap.git and click **Begin import**.



Import your project to GitHub

Import all the files, including the revision history, from another version control system.

Your old repository's clone URL

https://github.com/servicestage-demo/weathermap.git

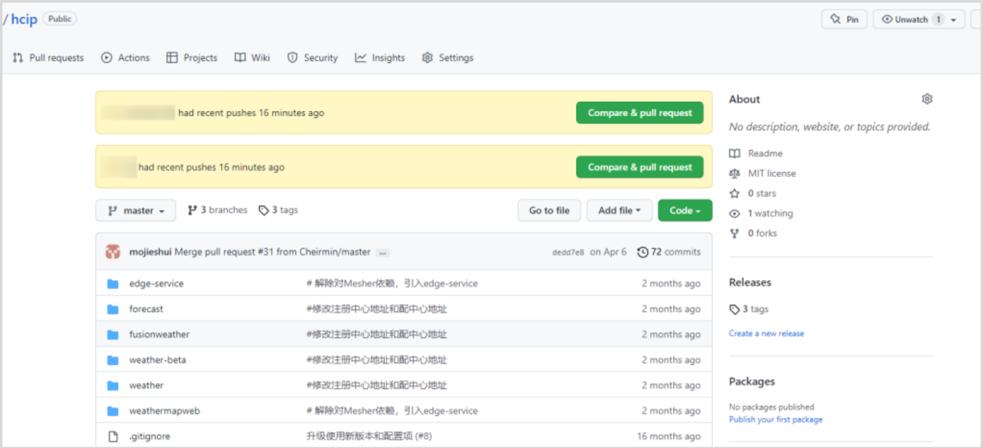
Learn more about the types of supported VCS.

Your existing repository

[redacted]/hcip

Figure 7-28

Step 6 Check whether the source code file of the weather forecast service has been imported to the **hcip** repository.



/ hcip Public

[redacted] had recent pushes 16 minutes ago

[redacted] had recent pushes 16 minutes ago

mojieshui Merge pull request #31 from Cheirmin/master … dedd7e8 on Apr 6 72 commits

edge-service	# 解除对Mesher依赖，引入edge-service	2 months ago
forecast	#修改注册中心地址和配中心地址	2 months ago
fusionweather	#修改注册中心地址和配中心地址	2 months ago
weather-beta	#修改注册中心地址和配中心地址	2 months ago
weather	#修改注册中心地址和配中心地址	2 months ago
weathermapweb	# 解除对Mesher依赖，引入edge-service	2 months ago
.gitignore	升级使用新版本和配置项 (#8)	16 months ago

About

No description, website, or topics provided.

Readme
MIT license
0 stars
1 watching
0 forks

Releases

3 tags

Create a new release

Packages

No packages published
Publish your first package

Figure 7-29

7.2.1.5 Setting GitHub Repository Authorization

Step 1 Log in to ServiceStage, choose **Continuous Delivery** > **Repository Authorization**, and click **Create Authorization**.

You will use this repository for authorization to build and deploy microservices.

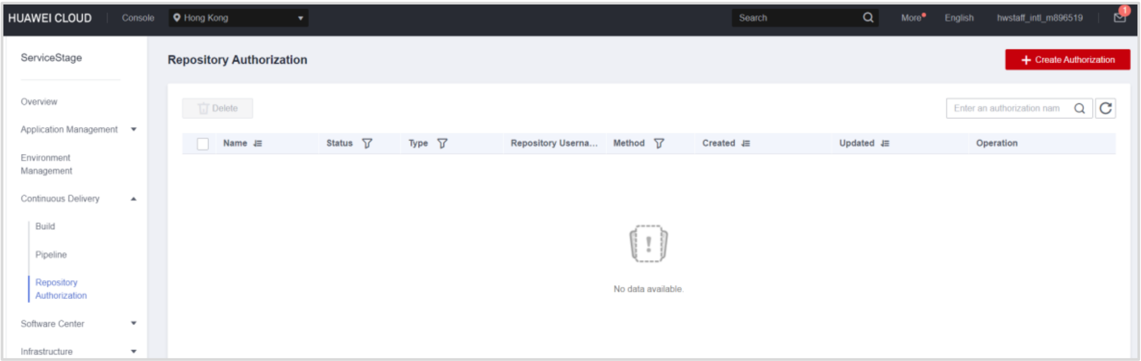
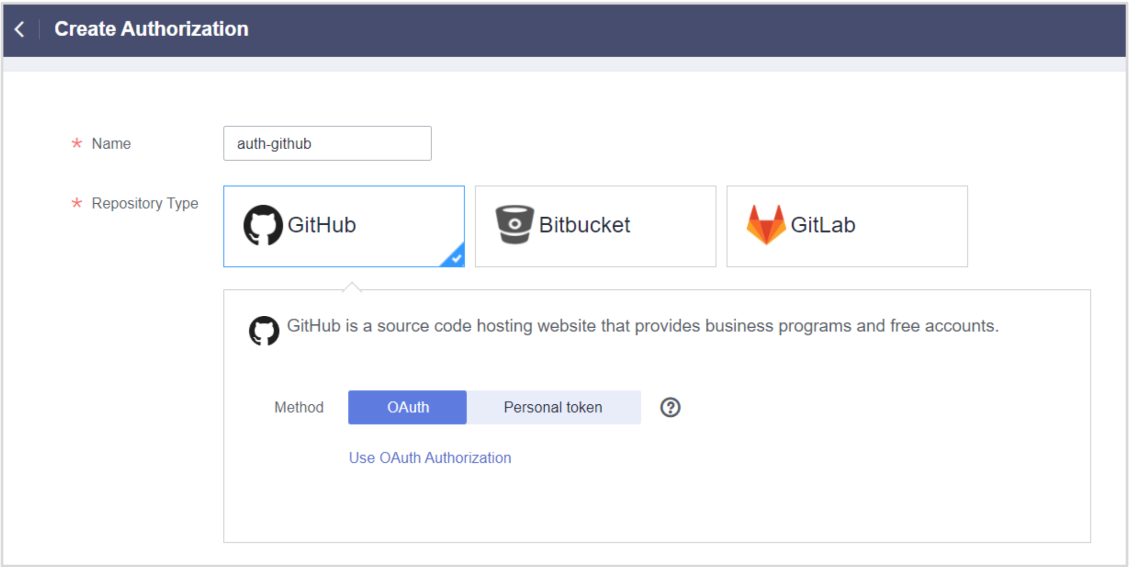


Figure 7-30

Step 2 Set authorization parameters as follows:

- **Name: auth-github**
- **Repository Type**: **GitHub**
- **Method**: **OAuth**

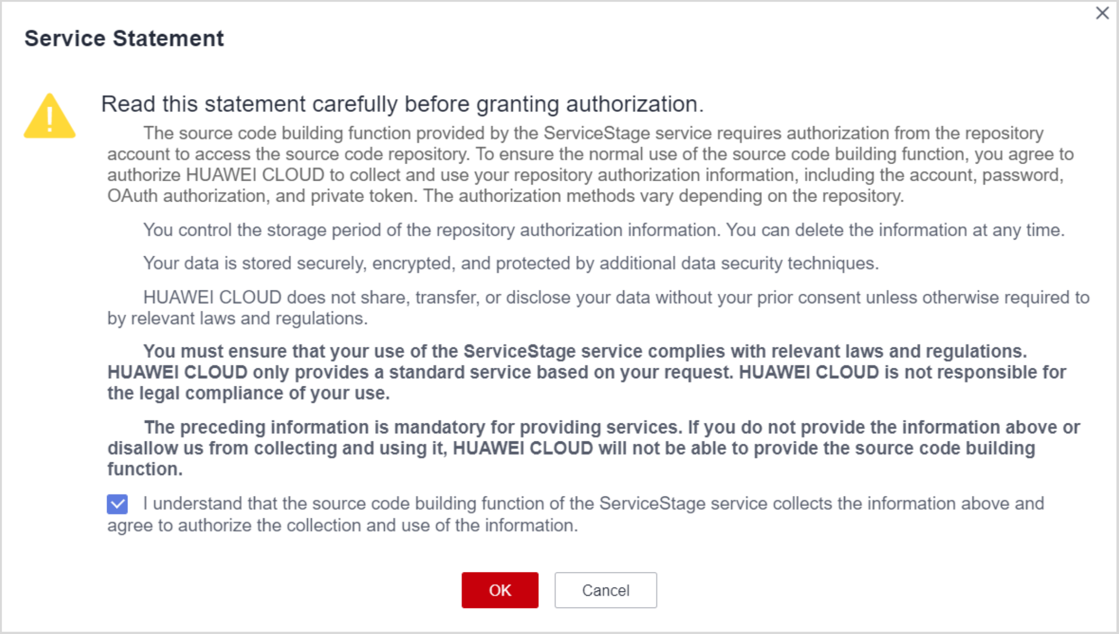

Create Authorization

* Name auth-github

* Repository Type GitHub

GitHub is a source code hosting website that provides business programs and free accounts.

Method OAuth



Service Statement

Read this statement carefully before granting authorization.

The source code building function provided by the ServiceStage service requires authorization from the repository account to access the source code repository. To ensure the normal use of the source code building function, you agree to authorize HUAWEI CLOUD to collect and use your repository authorization information, including the account, password, OAuth authorization, and private token. The authorization methods vary depending on the repository.

You control the storage period of the repository authorization information. You can delete the information at any time.

Your data is stored securely, encrypted, and protected by additional data security techniques.

HUAWEI CLOUD does not share, transfer, or disclose your data without your prior consent unless otherwise required to by relevant laws and regulations.

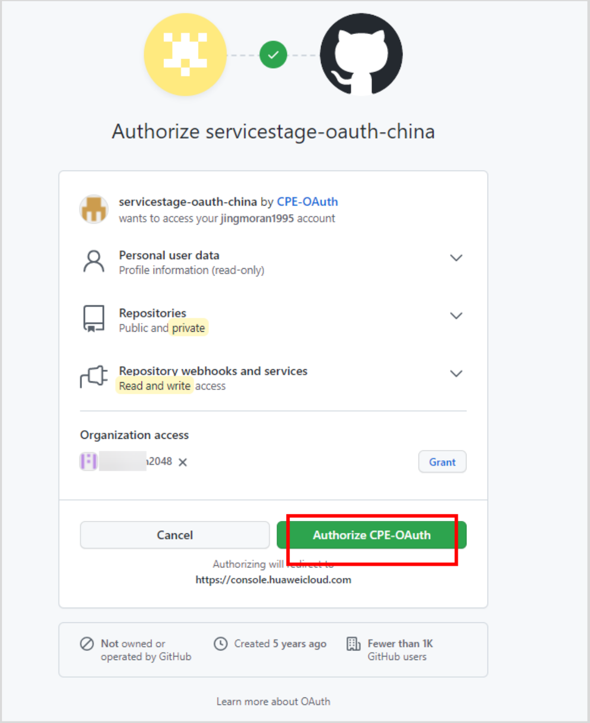
You must ensure that your use of the ServiceStage service complies with relevant laws and regulations. HUAWEI CLOUD only provides a standard service based on your request. HUAWEI CLOUD is not responsible for the legal compliance of your use.

The preceding information is mandatory for providing services. If you do not provide the information above or disallow us from collecting and using it, HUAWEI CLOUD will not be able to provide the source code building function.

☑ I understand that the source code building function of the ServiceStage service collects the information above and agree to authorize the collection and use of the information.

Figure 7-31

Step 3 In the displayed dialog box, click **Authorize CPE-OAuth**.



Authorize servicestage-oauth-china

servicestage-oauth-china by CPE-OAuth
wants to access your jingmoran1995 account

Personal user data
Profile information (read-only)

Repositories
Public and private

Repository webhooks and services
Read and write access

Organization access
[redacted]2048 ×

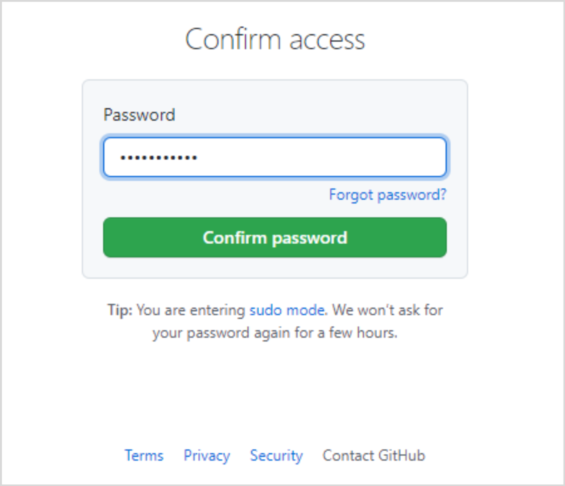
Authorizing will redirect to
https://console.huaweicloud.com

Not owned or operated by GitHub
Created 5 years ago
Fewer than 1K GitHub users

Learn more about OAuth

Figure 7-32

Step 4 In the dialog box that is displayed, enter the password for confirmation.



Confirm access

Password

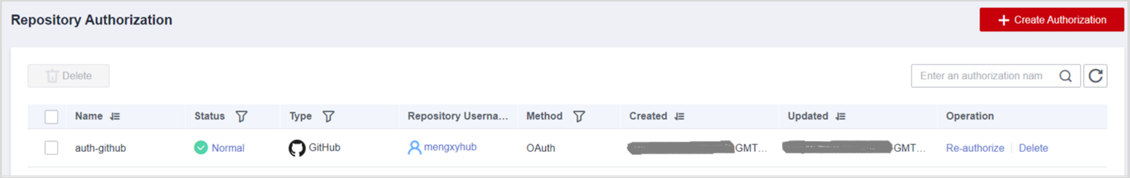
Forgot password?

Confirm password

Tip: You are entering sudo mode. We won't ask for your password again for a few hours.

Figure 7-33

Step 5 View the created authorization. If the status is Normal, the repository authorization is successfully created.



Repository Authorization

□	Name	Status	Type	Repository Userna...	Method	Created	Updated	Operation
□	auth-github	Normal	GitHub	mengxyhub	OAuth	[redacted]GMT...	[redacted]GMT...	Re-authorize | Delete

Figure 7-34

7.2.1.6 Creating an Organization

Step 1 Log in to ServiceStage and choose **Software Center** > **Organization**.

Resources in subsequent exercise will be associated with this organization.

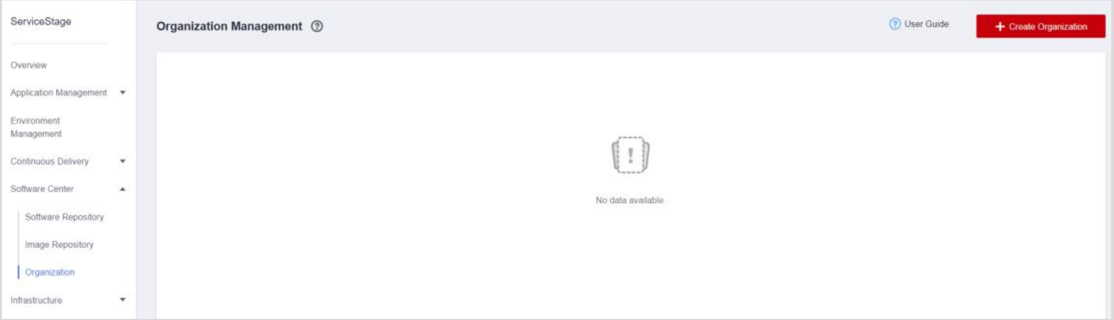
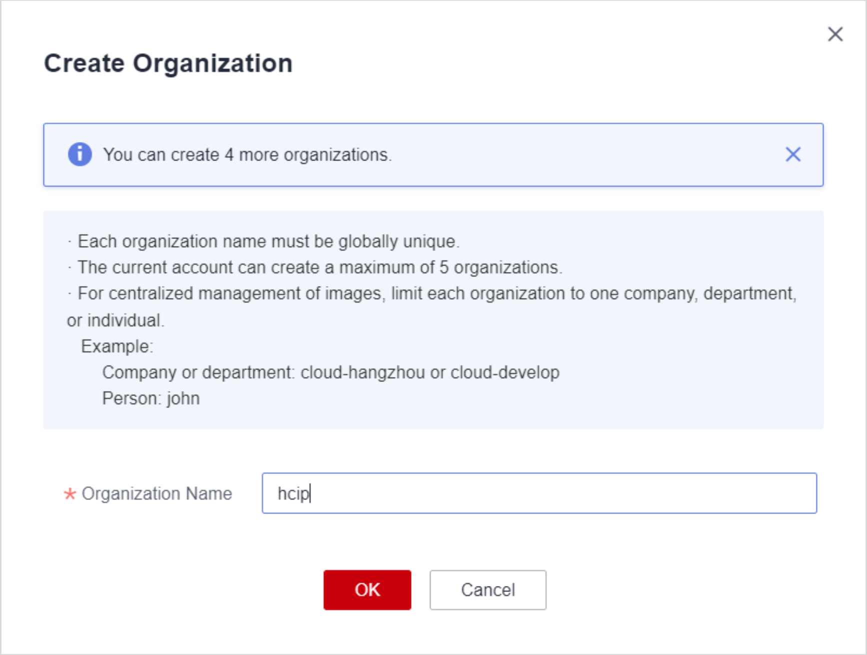


Figure 7-35

Step 2 Click **Create Organization**. On the displayed page, enter the organization name **hcip** and click **OK**.



Create Organization

You can create 4 more organizations.

· Each organization name must be globally unique.
· The current account can create a maximum of 5 organizations.
· For centralized management of images, limit each organization to one company, department, or individual.
Example:
Company or department: cloud-hangzhou or cloud-develop
Person: john

* Organization Name: hcip

Figure 7-36

7.2.2 Building a Microservice

ServiceStage provides one-click application delivery pipelines and supports flexible customization. You can pack and build applications based on the source code and software packages. Project pipelines automatically implement the entire process of code obtaining, compilation, packaging, archiving, and deployment. It helps you shorten the service rollout duration and quickly seize the market in practice.

ServiceStage pulls source code from source code repositories, such as DevCloud, GitHub, Gitee, Bitbucket, and GitLab.

In this exercise, you can create a build job on ServiceStage based on the source code to obtain the weathermap source code from GitHub, compile and pack the source code into an image, and archive the image to the image repository.

7.2.2.1 Creating a Build Job of Backend Applications

Step 1 Log in to ServiceStage, choose **Continuous Delivery** > **Build**, and click **Create Source Code Job**.

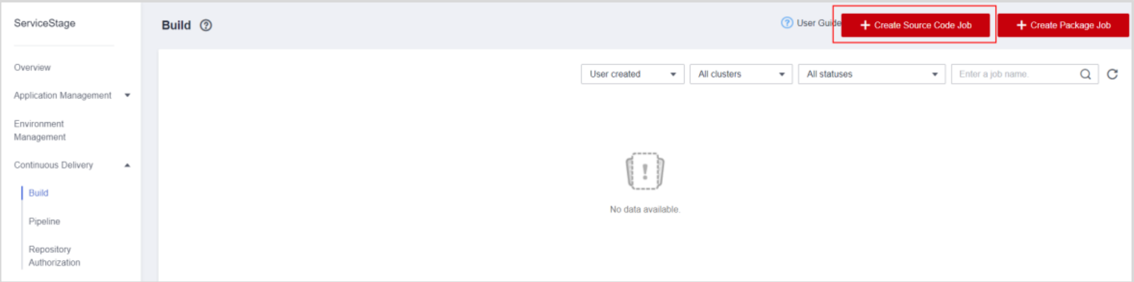
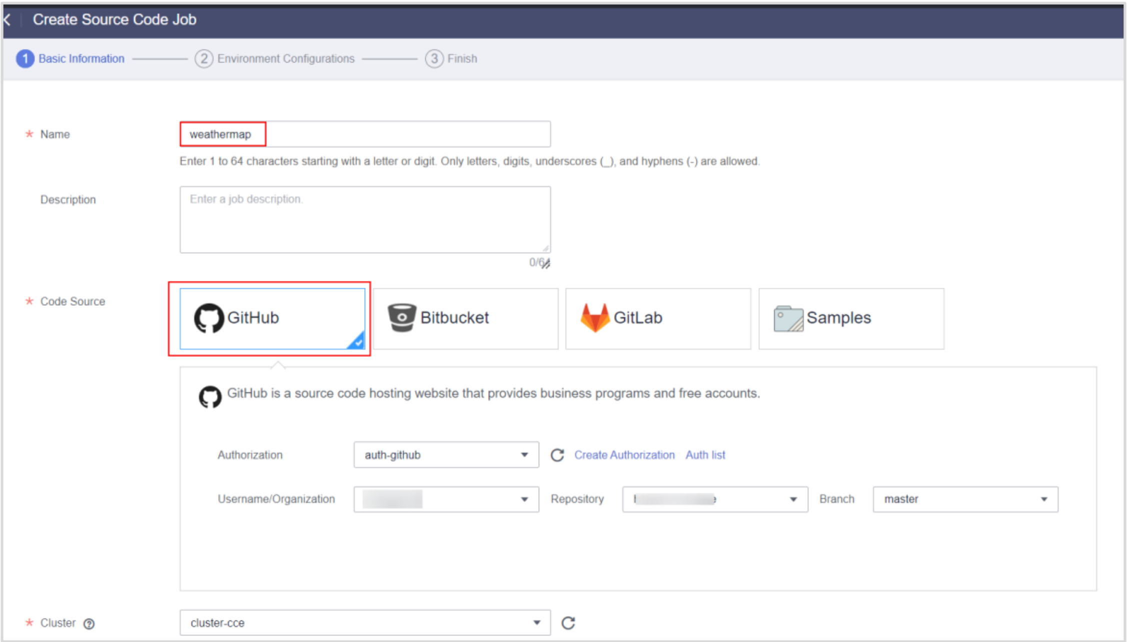


Figure 7-37

Step 2 Set build project parameters as follows and click **Next** to set the environment.

- **Name: weathermap**
- **Code Source: GitHub**
- **Authorization: auth-github** (Select the repository authorization created.)
- **Username/Organization**: Retain the default value (username/organization of your GitHub account).
- **Repository: hcip** (name of the repository created in GitHub)
- **Branch: master**
- **Cluster: cluster-servicestage** (Select the CCE cluster created.)



Create Source Code Job

1 Basic Information — 2 Environment Configurations — 3 Finish

* Name: weathermap

Enter 1 to 64 characters starting with a letter or digit. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Description: Enter a job description. 0/64

* Code Source: GitHub | Bitbucket | GitLab | Samples

GitHub is a source code hosting website that provides business programs and free accounts.

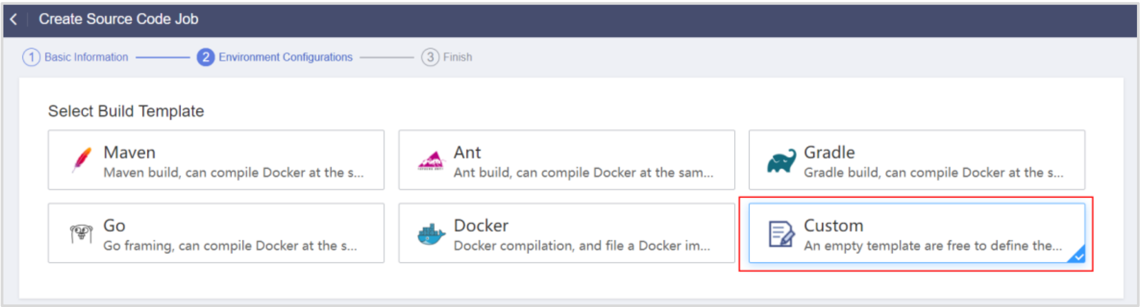
Authorization: auth-github — Create Authorization — Auth list

Username/Organization: [redacted] Repository: [redacted] Branch: master

* Cluster: cluster-cce

Figure 7-38

Step 3 Select **Custom** and click **Advanced Settings**.



Create Source Code Job

1 Basic Information — 2 Environment Configurations — 3 Finish

Select Build Template

Maven
Maven build, can compile Docker at the s...

Ant
Ant build, can compile Docker at the sam...

Gradle
Gradle build, can compile Docker at the s...

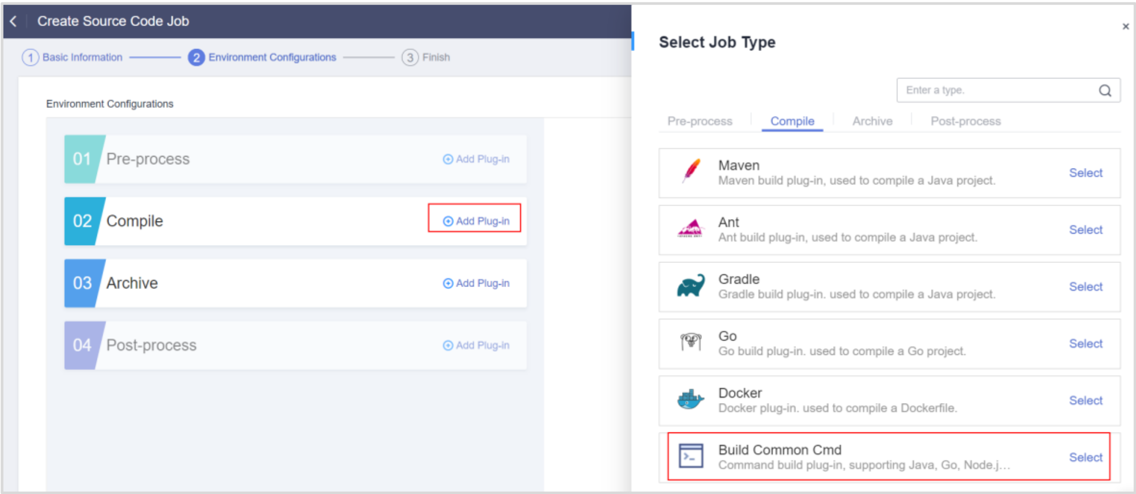
Go
Go framing, can compile Docker at the s...

Docker
Docker compilation, and file a Docker im...

Custom
An empty template are free to define the...

Figure 7-39

Step 4 Select **Compile** and click **Add Plug-in**. In the displayed right area, select **Build Common Cmd**. Then, select **Java** for **Language**, and set parameters.



Create Source Code Job

1 Basic Information — 2 Environment Configurations — 3 Finish

Environment Configurations

01 Pre-process ⊕ Add Plug-in

02 Compile ⊕ Add Plug-in

03 Archive ⊕ Add Plug-in

04 Post-process ⊕ Add Plug-in

Select Job Type

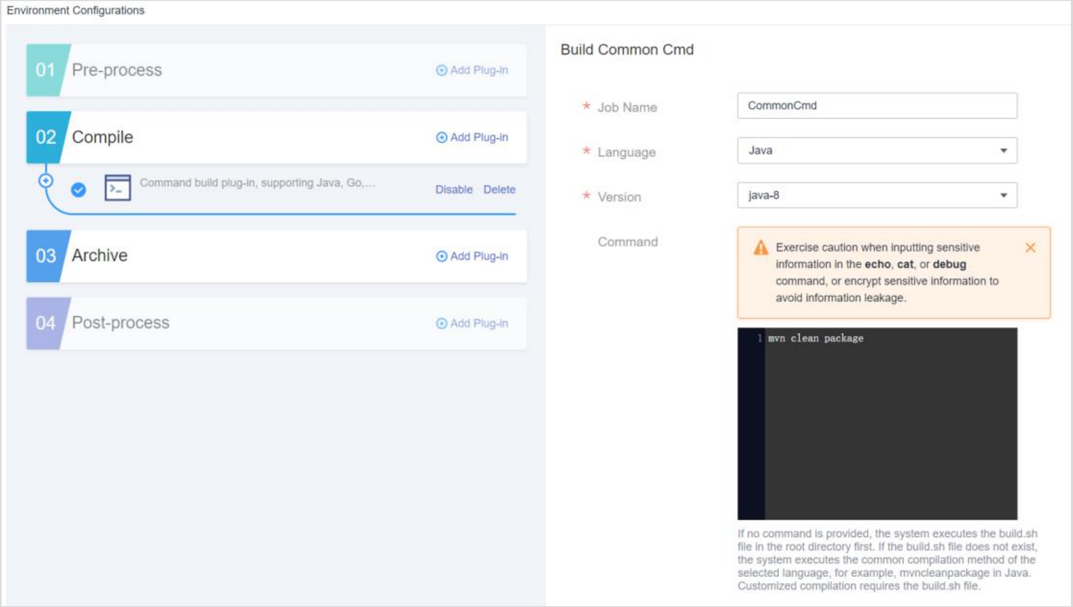
Enter a type.

Pre-process | Compile | Archive | Post-process

Maven	Maven build plug-in, used to compile a Java project.	Select
Ant	Ant build plug-in, used to compile a Java project.	Select
Gradle	Gradle build plug-in. used to compile a Java project.	Select
Go	Go build plug-in. used to compile a Go project.	Select
Docker	Docker plug-in. used to compile a Dockerfile.	Select
Build Common Cmd	Command build plug-in, supporting Java, Go, Node.j…	Select

Figure 7-40

- Job Name: CommonCmd
- Language: Java
- Version: java-8



Environment Configurations

01 Pre-process ⊕ Add Plug-in

02 Compile ⊕ Add Plug-in

Command build plug-in, supporting Java, Go,… Disable Delete

03 Archive ⊕ Add Plug-in

04 Post-process ⊕ Add Plug-in

Build Common Cmd

* Job Name: CommonCmd

* Language: Java

* Version: java-8

Command

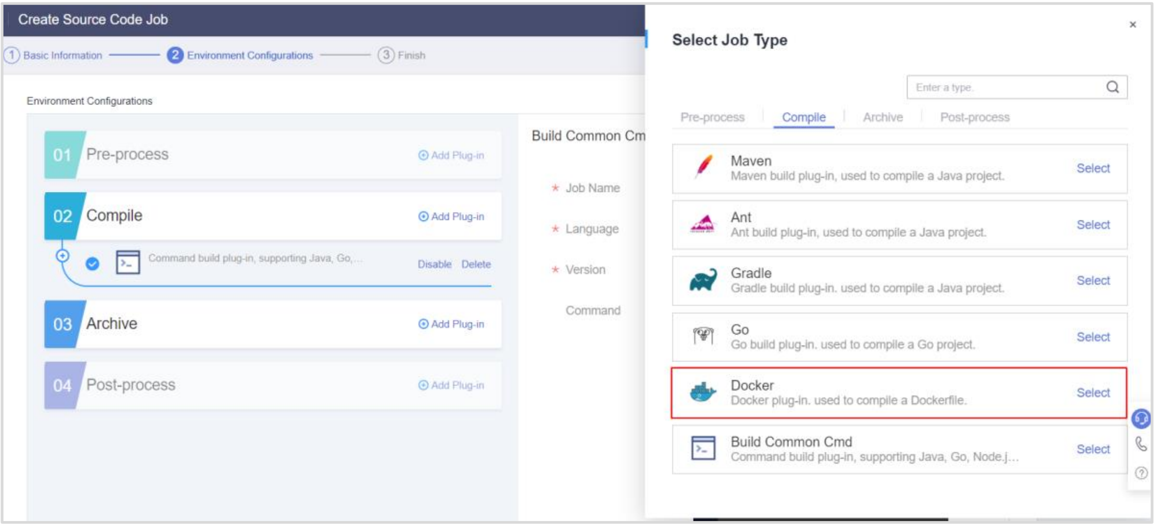
Exercise caution when inputting sensitive information in the **echo**, **cat**, or **debug** command, or encrypt sensitive information to avoid information leakage.

```
mvn clean package
```

If no command is provided, the system executes the build.sh file in the root directory first. If the build.sh file does not exist, the system executes the common compilation method of the selected language, for example, mvncleanpackage in Java. Customized compilation requires the build.sh file.

Figure 7-41

Step 5 In the **Compile** area, click **Add Plug-in**, select **Docker**, and add four build jobs with parameters setting as follows:



Create Source Code Job

1 Basic Information — 2 Environment Configurations — 3 Finish

Environment Configurations

- 01 Pre-process ⊕ Add Plug-in
- 02 Compile ⊕ Add Plug-in
  - Command build plug-in, supporting Java, Go, ... Disable Delete
- 03 Archive ⊕ Add Plug-in
- 04 Post-process ⊕ Add Plug-in

Build Common Cm

* Job Name

* Language

* Version

Command

Select Job Type ×

Enter a type.

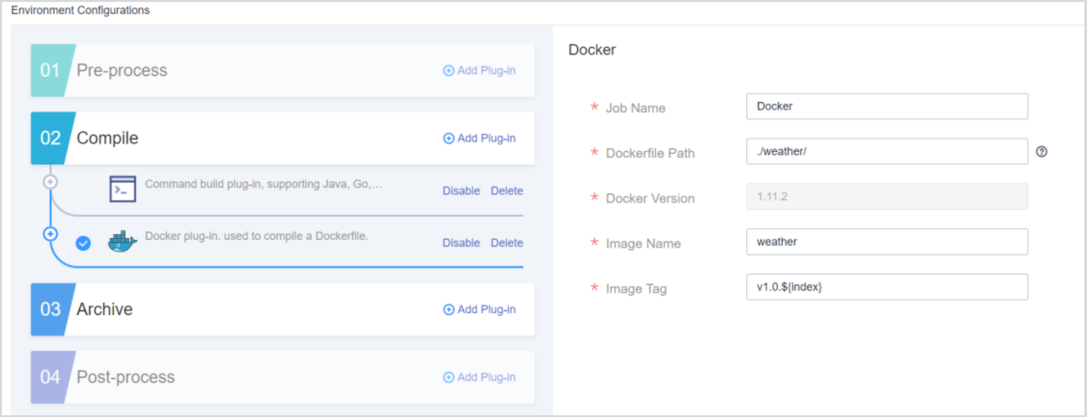
Pre-process | Compile | Archive | Post-process

Maven Maven build plug-in, used to compile a Java project.	Select
Ant Ant build plug-in, used to compile a Java project.	Select
Gradle Gradle build plug-in, used to compile a Java project.	Select
Go Go build plug-in, used to compile a Go project.	Select
Docker Docker plug-in, used to compile a Dockerfile.	Select
Build Common Cmd Command build plug-in, supporting Java, Go, Node.j...	Select

Figure 7-42

Step 6 Create the first build job:

- **Job Name**: **Docker** (Retain the default value. You can set this parameter as required. The same applies to the following.)
- **Dockerfile Path**: **./weather/**
- **Image Name**: **weather**
- **Image Tag**: **v1.0.${index}**



Environment Configurations

- 01 Pre-process ⊕ Add Plug-in
- 02 Compile ⊕ Add Plug-in
  - Command build plug-in, supporting Java, Go,... Disable Delete
  - Docker plug-in, used to compile a Dockerfile. Disable Delete
- 03 Archive ⊕ Add Plug-in
- 04 Post-process ⊕ Add Plug-in

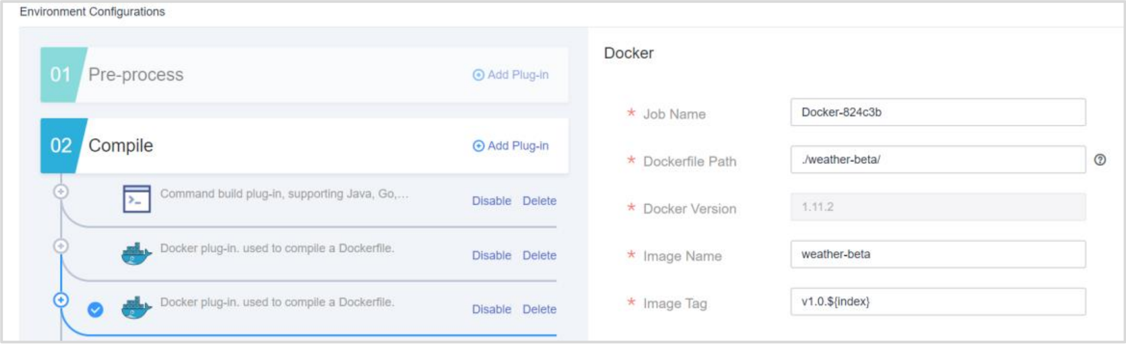
Docker

* Job Name	Docker
* Dockerfile Path	./weather/
* Docker Version	1.11.2
* Image Name	weather
* Image Tag	v1.0.${index}

Figure 7-43

Step 7 Repeat the preceding steps to create the second build job.

- **Job Name**: **Docker-4xsb8p**
- **Dockerfile Path**: **./weather-beta/**
- **Image Name**: **weather-beta**
- **Image Tag**: **v1.0.${index}**

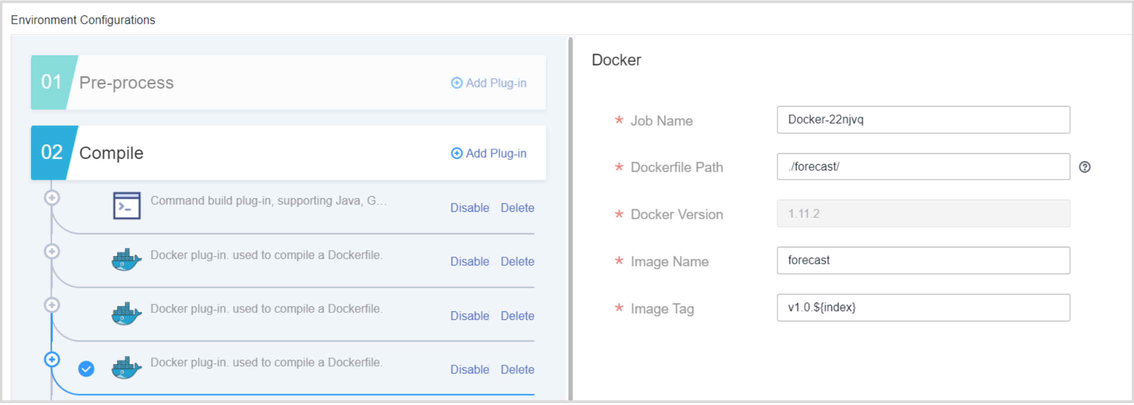

Environment Configurations
01 Pre-process
Add Plug-in
02 Compile
Add Plug-in
Command build plug-in, supporting Java, Go,...
Docker plug-in. used to compile a Dockerfile.
Docker plug-in. used to compile a Dockerfile.
Disable Delete
Docker

- Job Name: Docker-824c3b
- Dockerfile Path: ./weather-beta/
- Docker Version: 1.11.2
- Image Name: weather-beta
- Image Tag: v1.0.${index}

Figure 7-44

Step 8 Repeat the preceding steps to create the third build job.

- Job Name: Docker-5e40k3
- Dockerfile Path: ./forecast/
- Image Name: forecast
- Image Tag: v1.0.${index}

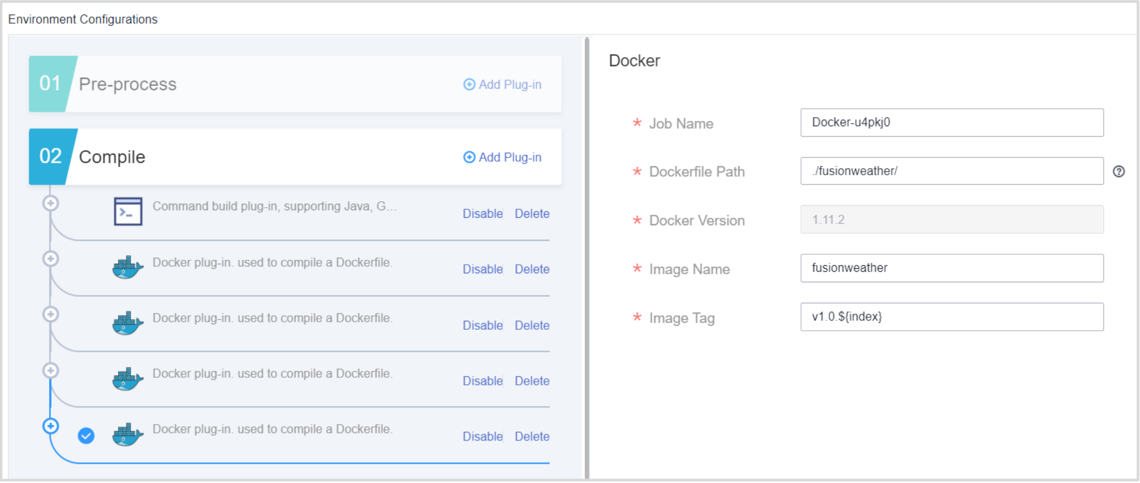

Environment Configurations
01 Pre-process
Add Plug-in
02 Compile
Add Plug-in
Command build plug-in, supporting Java, G...
Docker plug-in. used to compile a Dockerfile.
Docker plug-in. used to compile a Dockerfile.
Docker plug-in. used to compile a Dockerfile.
Disable Delete
Docker

- Job Name: Docker-22njvq
- Dockerfile Path: ./forecast/
- Docker Version: 1.11.2
- Image Name: forecast
- Image Tag: v1.0.${index}

Figure 7-45

Step 9 Repeat the preceding steps to create the fourth build job.

- Job Name: Docker-aom49h
- Dockerfile Path: ./fusionweather/
- Image Name: fusionweather
- Image Tag: v1.0.${index}



Environment Configurations

01 Pre-process ⊕ Add Plug-in

02 Compile ⊕ Add Plug-in

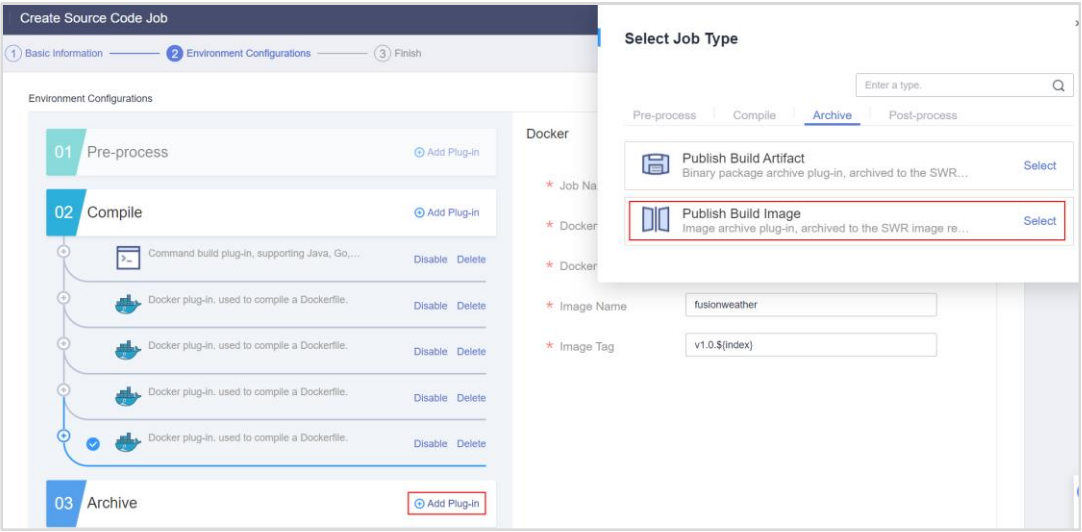
- Command build plug-in, supporting Java, G... Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete
- ✓ Docker plug-in. used to compile a Dockerfile. Disable Delete

Docker

* Job Name	Docker-u4pkj0
* Dockerfile Path	./fusionweather/
* Docker Version	1.11.2
* Image Name	fusionweather
* Image Tag	v1.0.${index}

Figure 7-46

Step 10 Select **Archive** and click **Add Plug-in**. In the displayed right area, select **Publish Build Image**.



Create Source Code Job

1 Basic Information — 2 Environment Configurations — 3 Finish

Environment Configurations

01 Pre-process ⊕ Add Plug-in

02 Compile ⊕ Add Plug-in

- Command build plug-in, supporting Java, Go,... Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete
- ✓ Docker plug-in. used to compile a Dockerfile. Disable Delete

03 Archive ⊕ Add Plug-in

Docker

* Job Na	
* Docker	
* Docker	
* Image Name	fusionweather
* Image Tag	v1.0.${index}

Select Job Type

Enter a type.

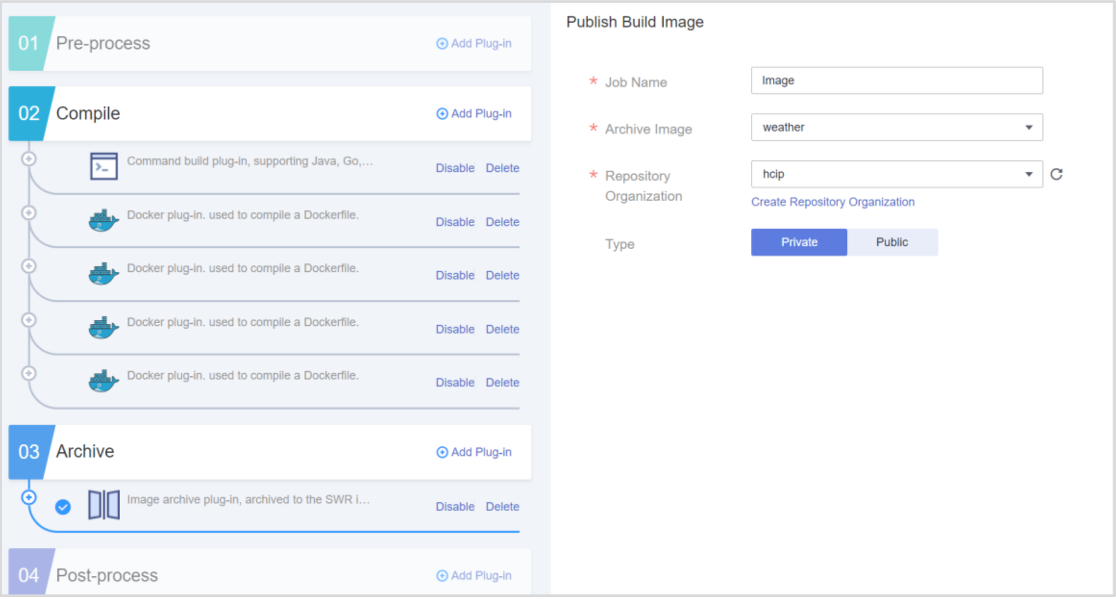
Pre-process | Compile | Archive | Post-process

- Publish Build Artifact — Binary package archive plug-in, archived to the SWR... Select
- Publish Build Image — Image archive plug-in, archived to the SWR image re... Select

Figure 7-47

Step 11 In **Archive**, select the four created images (weather, weather-beta, forecast, and fusionweather), retain the default values for **Job Name**, and select the created repository organization **hcip** for **Repository Organization**.

After jobs are added, the image package is automatically archived to the image repository for subsequent operations.


01 Pre-process
Add Plug-in
02 Compile
Add Plug-in
Command build plug-in, supporting Java, Go,...
Disable Delete
Docker plug-in. used to compile a Dockerfile.
Disable Delete
Docker plug-in. used to compile a Dockerfile.
Disable Delete
Docker plug-in. used to compile a Dockerfile.
Disable Delete
Docker plug-in. used to compile a Dockerfile.
Disable Delete
03 Archive
Add Plug-in
Image archive plug-in, archived to the SWR i...
Disable Delete
04 Post-process
Add Plug-in

Publish Build Image

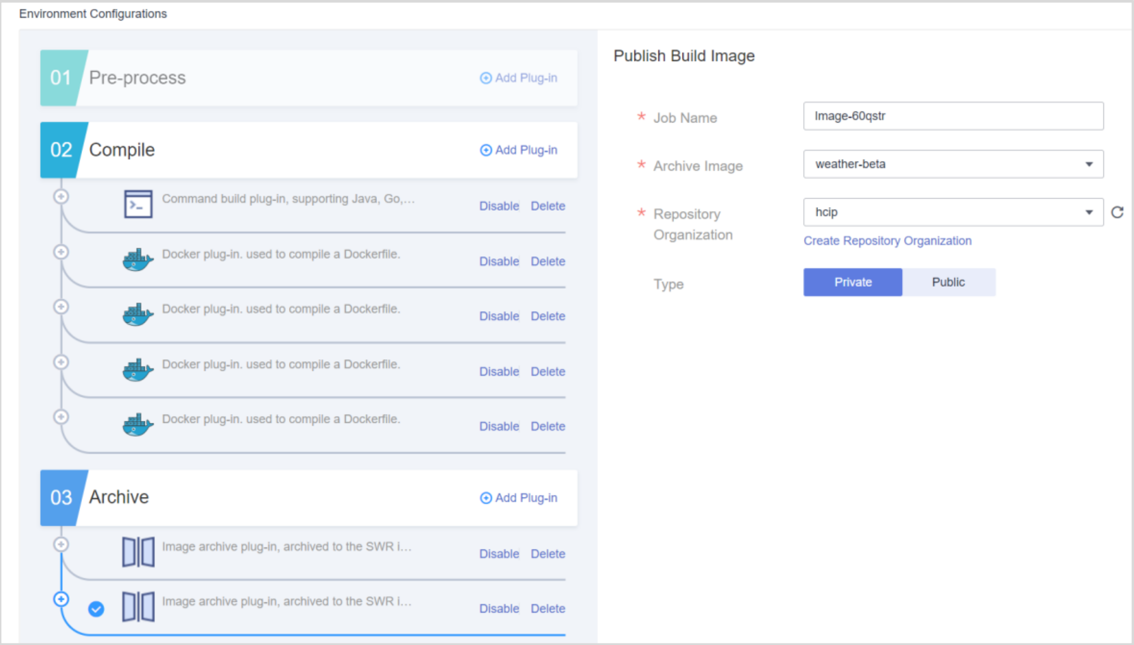
* Job Name: Image

* Archive Image: weather

* Repository Organization: hcip

Create Repository Organization

Type: Private Public


Environment Configurations

01 Pre-process
Add Plug-in
02 Compile
Add Plug-in
Command build plug-in, supporting Java, Go,...
Disable Delete
Docker plug-in. used to compile a Dockerfile.
Disable Delete
Docker plug-in. used to compile a Dockerfile.
Disable Delete
Docker plug-in. used to compile a Dockerfile.
Disable Delete
Docker plug-in. used to compile a Dockerfile.
Disable Delete
03 Archive
Add Plug-in
Image archive plug-in, archived to the SWR i...
Disable Delete
Image archive plug-in, archived to the SWR i...
Disable Delete

Publish Build Image

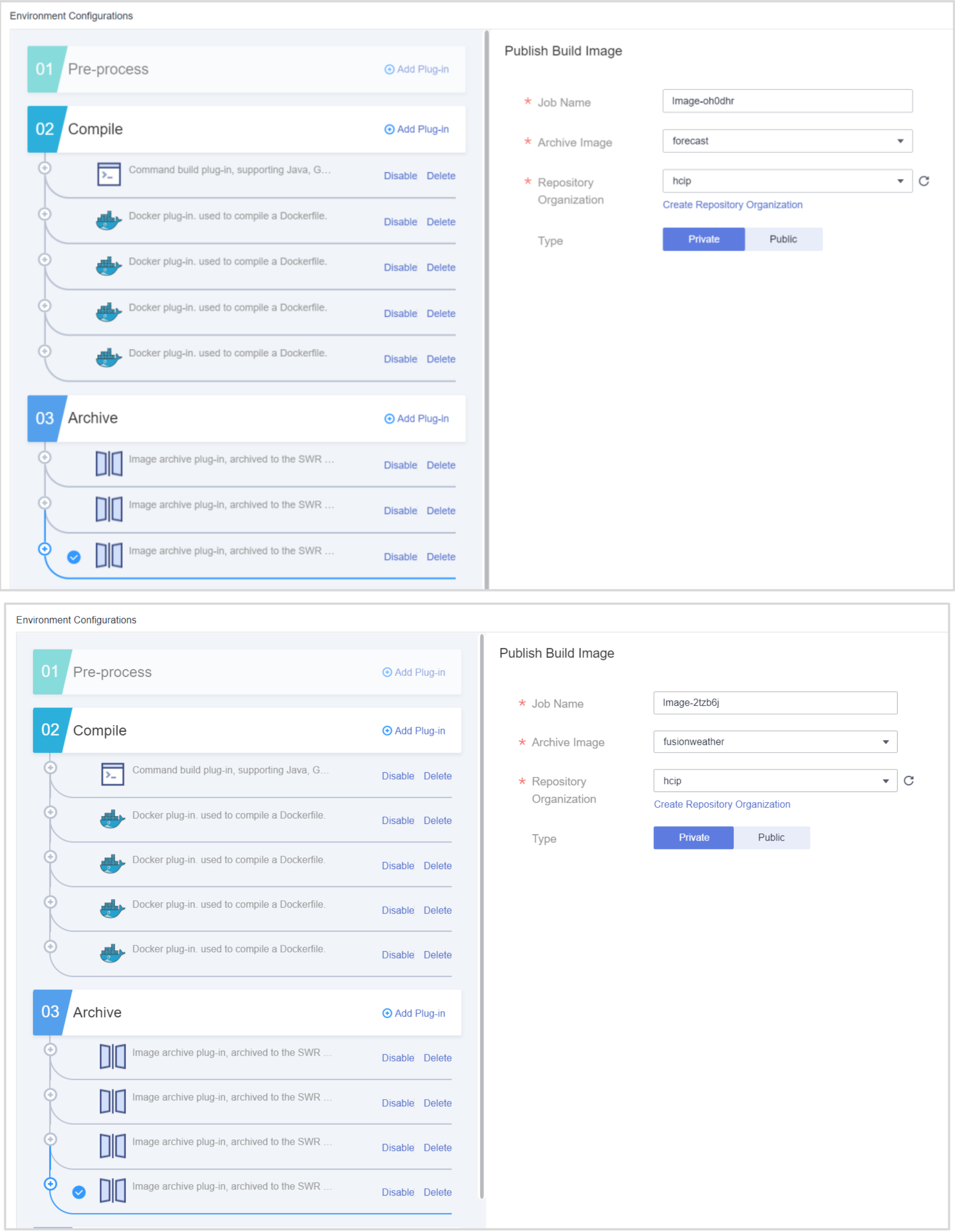
* Job Name: Image-60qstr

* Archive Image: weather-beta

* Repository Organization: hcip

Create Repository Organization

Type: Private Public



Environment Configurations

01 Pre-process ⊕ Add Plug-in

02 Compile ⊕ Add Plug-in

- Command build plug-in, supporting Java, G... Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete

03 Archive ⊕ Add Plug-in

- Image archive plug-in, archived to the SWR ... Disable Delete
- Image archive plug-in, archived to the SWR ... Disable Delete
- ✓ Image archive plug-in, archived to the SWR ... Disable Delete

Publish Build Image

* Job Name: image-oh0dhr

* Archive Image: forecast

* Repository Organization: hcip

Create Repository Organization

Type: Private Public

Environment Configurations

01 Pre-process ⊕ Add Plug-in

02 Compile ⊕ Add Plug-in

- Command build plug-in, supporting Java, G... Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete
- Docker plug-in. used to compile a Dockerfile. Disable Delete

03 Archive ⊕ Add Plug-in

- Image archive plug-in, archived to the SWR ... Disable Delete
- Image archive plug-in, archived to the SWR ... Disable Delete
- Image archive plug-in, archived to the SWR ... Disable Delete
- ✓ Image archive plug-in, archived to the SWR ... Disable Delete

Publish Build Image

* Job Name: image-2tzb6j

* Archive Image: fusionweather

* Repository Organization: hcip

Create Repository Organization

Type: Private Public

Figure 7-48

Step 12 Click **Build** to start a build job. If the information shown in the following figure is displayed, the background application **weathermap** is successfully built.

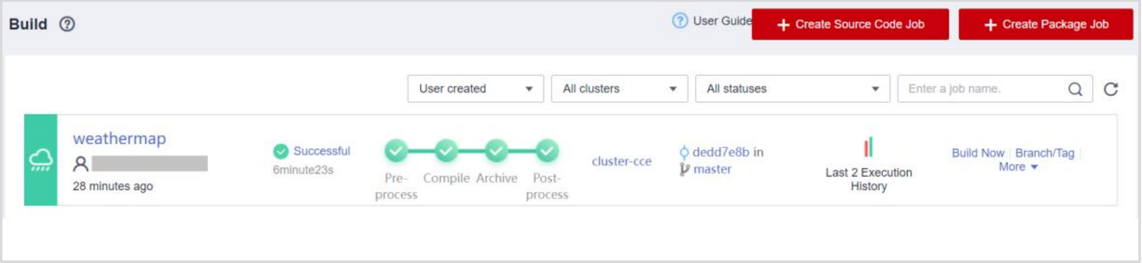


Figure 7-49

7.2.2.2 Creating a Build Job of Frontend Applications

Step 1 Log in to ServiceStage, choose **Continuous Delivery** > **Build**, and click **Create Source Code Job**.

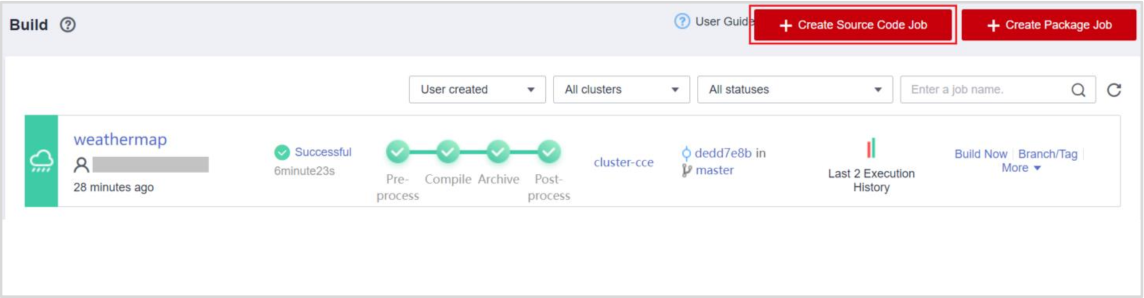
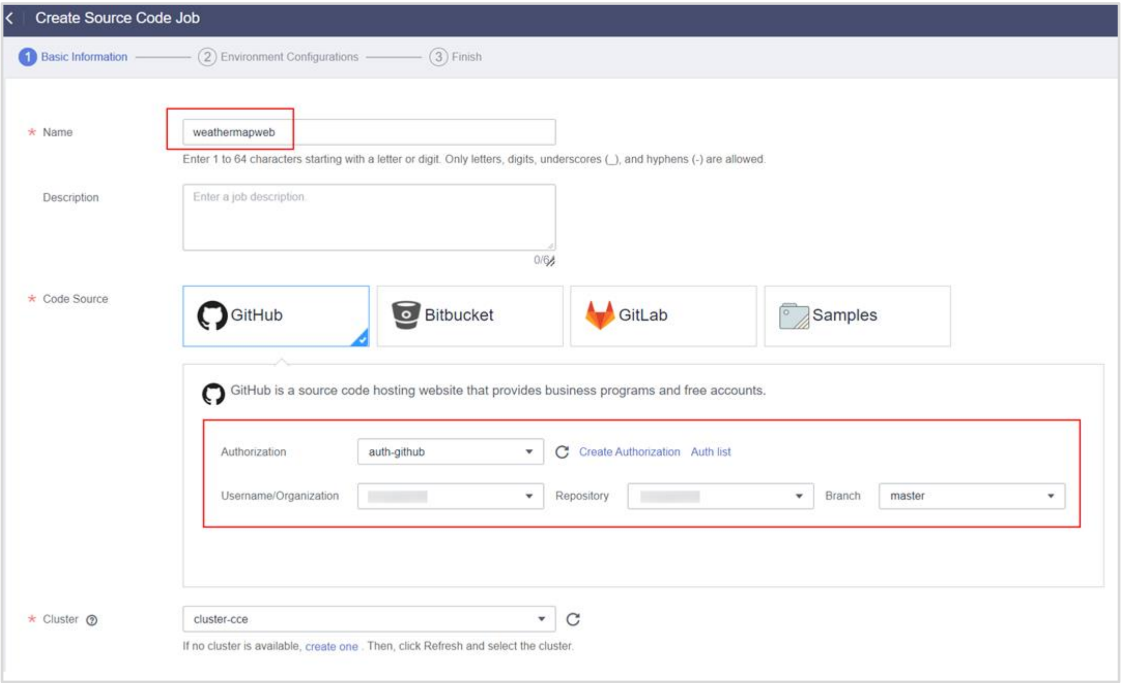


Figure 7-50

Step 2 Set basic configurations as follows and click **Next**.

- **Name: weathermapweb**
- **Code Source: GitHub**
- **Authorization: auth-github**
- **Username/Organization**: Retain the default value (username/organization of your GitHub account).
- **Repository: hcip**
- **Branch: master**
- **Cluster: cluster-cce** (Select the CCE cluster created.)



Create Source Code Job

1 Basic Information — 2 Environment Configurations — 3 Finish

* Name: weathermapweb

Enter 1 to 64 characters starting with a letter or digit. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Description: Enter a job description 0/64

* Code Source: GitHub | Bitbucket | GitLab | Samples

GitHub is a source code hosting website that provides business programs and free accounts.

Authorization: auth-github Create Authorization Auth list

Username/Organization: [redacted] Repository: [redacted] Branch: master

* Cluster: cluster-cce

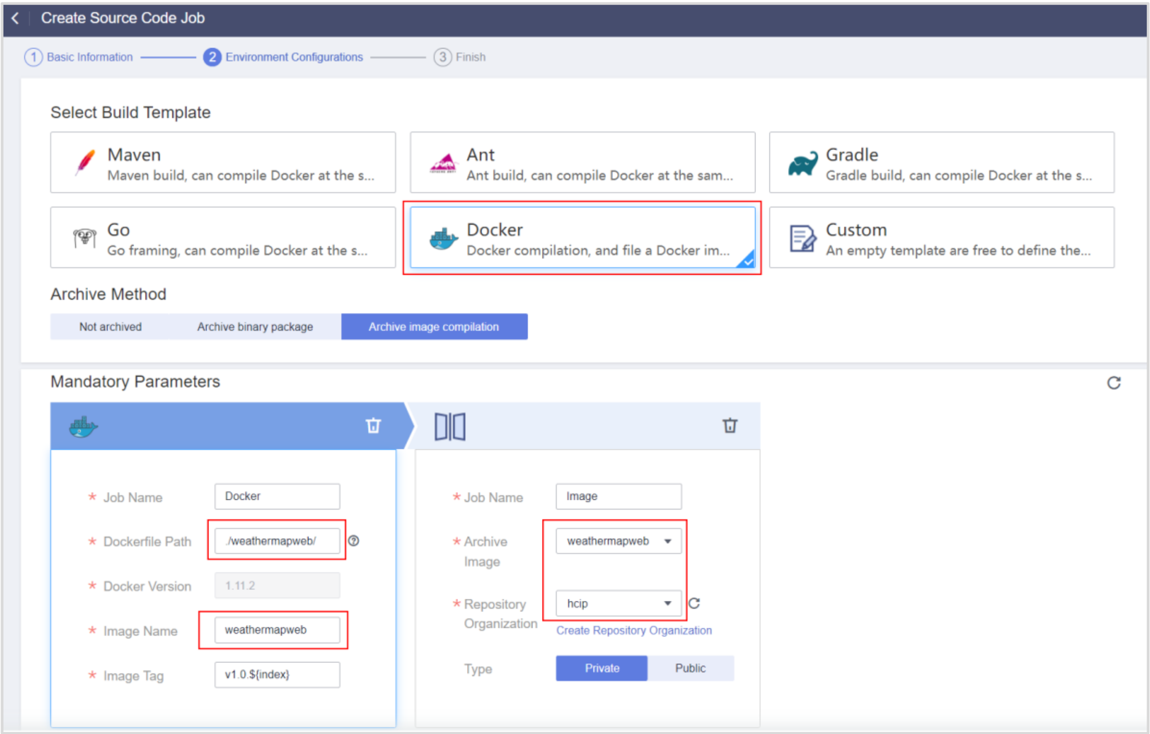
If no cluster is available, create one . Then, click Refresh and select the cluster.

Figure 7-51

Step 3 Select a Docker build template.

Compile Docker to add a build job, and specify the job parameters as follows.

- **Dockerfile Path**: **./weathermapweb/**
- **Image Name**: **weathermapweb**
- **Repository Organization**: **hcip**
- **Branch**: **master**
- Retain the default values for other parameters.


Create Source Code Job
1 Basic Information
2 Environment Configurations
3 Finish
Select Build Template
Maven
Maven build, can compile Docker at the s...
Ant
Ant build, can compile Docker at the sam...
Gradle
Gradle build, can compile Docker at the s...
Go
Go framing, can compile Docker at the s...
Docker
Docker compilation, and file a Docker im...
Custom
An empty template are free to define the...
Archive Method
Not archived
Archive binary package
Archive image compilation
Mandatory Parameters

* Job Name: Docker

* Dockerfile Path: ./weathermapweb/

* Docker Version: 1.11.2

* Image Name: weathermapweb

* Image Tag: v1.0.${index}

* Job Name: Image

* Archive Image: weathermapweb

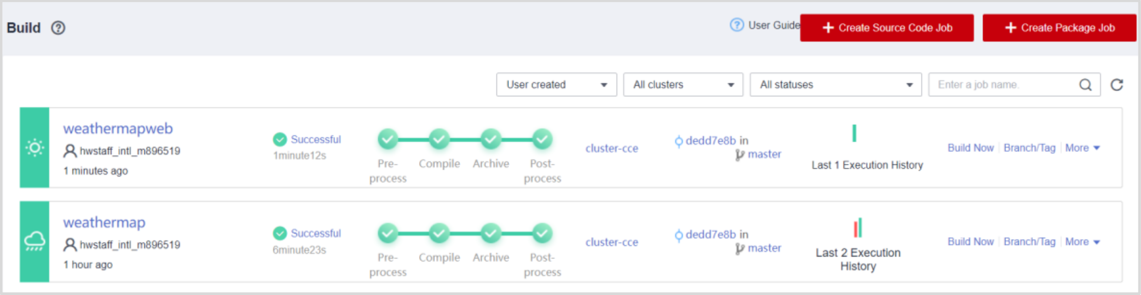
* Repository Organization: hcip

Create Repository Organization

Type: Private | Public

Figure 7-52

Step 4 Click **Build**. If the following information is displayed, the frontend application **weathermapweb** is successfully built.



weathermapweb
hwstaff_intl_m896519
1 minutes ago
Successful 1minute12s
Pre-process Compile Archive Post-process
cluster-cce
dedd7e8b in master
Last 1 Execution History

weathermap
hwstaff_intl_m896519
1 hour ago
Successful 6minute23s
Pre-process Compile Archive Post-process
cluster-cce
dedd7e8b in master
Last 2 Execution History

Figure 7-53

7.2.3 Deploying a Microservice

ServiceStage allows you to quickly deploy microservices in containers (such as CCE) or VMs (such as ECS), or in serverless mode (such as CCI), and supports deployment using source code, JAR/WAR packages, or Docker images. In addition, ServiceStage allows you to deploy, upgrade, roll back, start, stop, and delete applications developed in different programming languages, such as Java, PHP, Node.js, Go, and Python.

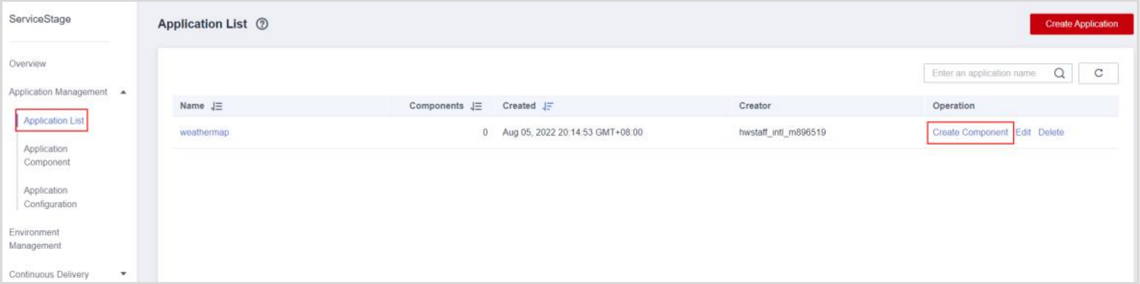
In this exercise, backend components developed in Java and frontend components developed in Node.js are used.

7.2.3.1 Creating and Deploying Backend Application Components

You need to deploy applications in container-based mode and register microservice instances with CSE.

Step 1 Log in to ServiceStage and choose **Application Management** > **Application List**.

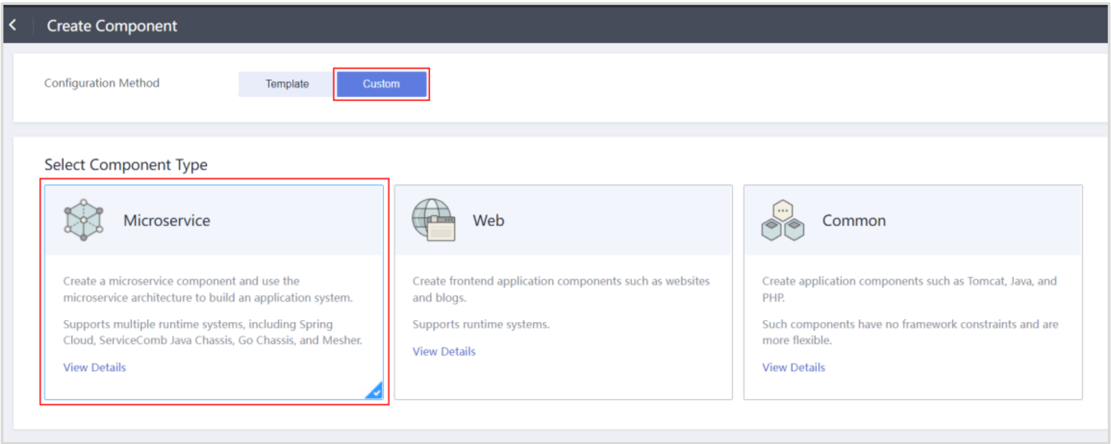
Step 2 Click **Create Component** in the **Operation** column.



Name	Components	Created	Creator	Operation
weathermap	0	Aug 05, 2022 20:14:53 GMT+08:00	hwstaff_intl_m896519	Create Component Edit Delete

Figure 7-54

Step 3 Select **Custom** in **Configuration Method** and **Microservice** for **Select Component Type**, and click **Next**.



Microservice

Create a microservice component and use the microservice architecture to build an application system.

Supports multiple runtime systems, including Spring Cloud, ServiceComb Java Chassis, Go Chassis, and Mesher.

View Details

Web

Create frontend application components such as websites and blogs.

Supports runtime systems.

View Details

Common

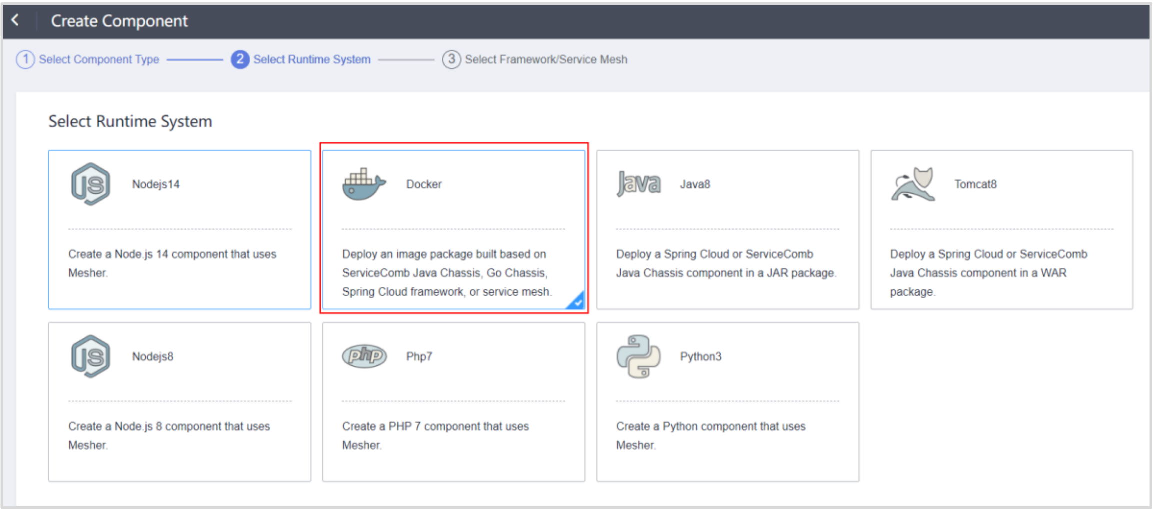
Create application components such as Tomcat, Java, and PHP.

Such components have no framework constraints and are more flexible.

View Details

Figure 7-55

Step 4 Select **Docker** in **Select Runtime System** and click **Next**.



Nodejs14

Create a Node.js 14 component that uses Mesher.

Docker

Deploy an image package built based on ServiceComb Java Chassis, Go Chassis, Spring Cloud framework, or service mesh.

Java8

Deploy a Spring Cloud or ServiceComb Java Chassis component in a JAR package.

Tomcat8

Deploy a Spring Cloud or ServiceComb Java Chassis component in a WAR package.

Nodejs8

Create a Node.js 8 component that uses Mesher.

Php7

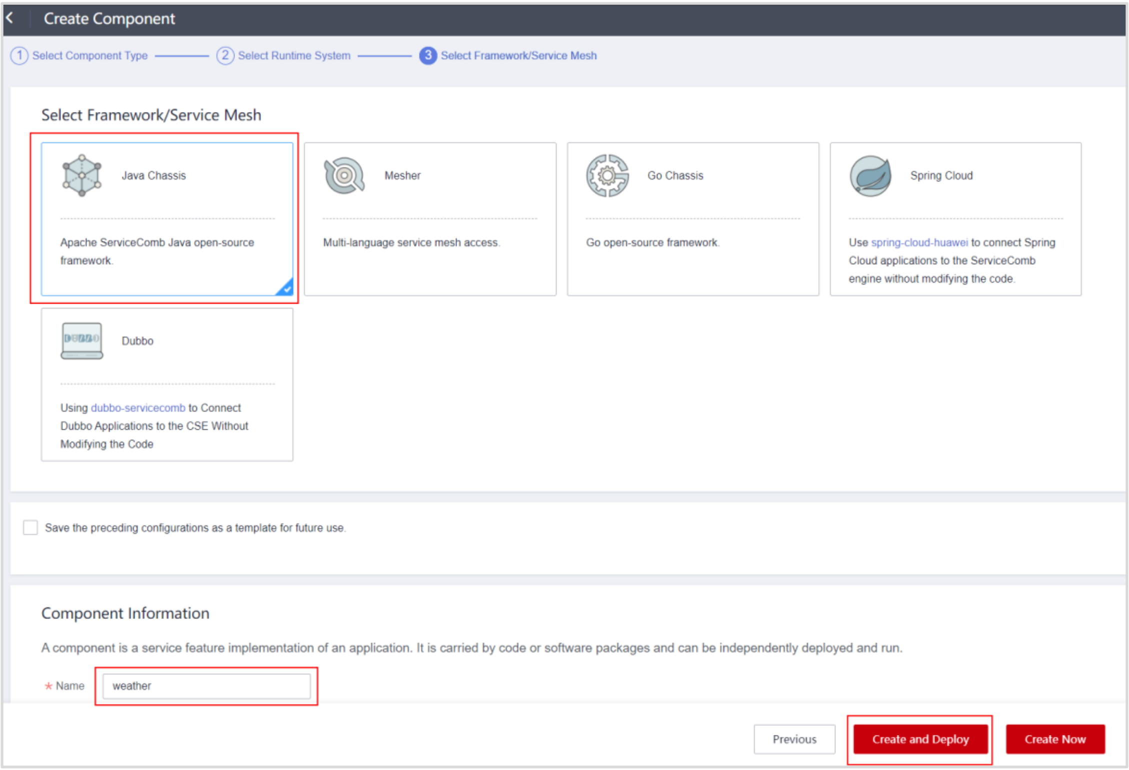
Create a PHP 7 component that uses Mesher.

Python3

Create a Python component that uses Mesher.

Figure 7-56

Step 5 Select **Java Chassis** in **Select Framework/Service Mesh** and set **Name** to **weather**. Click **Create and Deploy** to deploy the component.


Create Component
1 Select Component Type
2 Select Runtime System
3 Select Framework/Service Mesh
Select Framework/Service Mesh
Java Chassis
Apache ServiceComb Java open-source framework.
Mesher
Multi-language service mesh access.
Go Chassis
Go open-source framework.
Spring Cloud
Use spring-cloud-huawei to connect Spring Cloud applications to the ServiceComb engine without modifying the code.
Dubbo
Using dubbo-servicecomb to Connect Dubbo Applications to the CSE Without Modifying the Code
□ Save the preceding configurations as a template for future use.
Component Information
A component is a service feature implementation of an application. It is carried by code or software packages and can be independently deployed and run.
Previous
Create and Deploy
Create Now

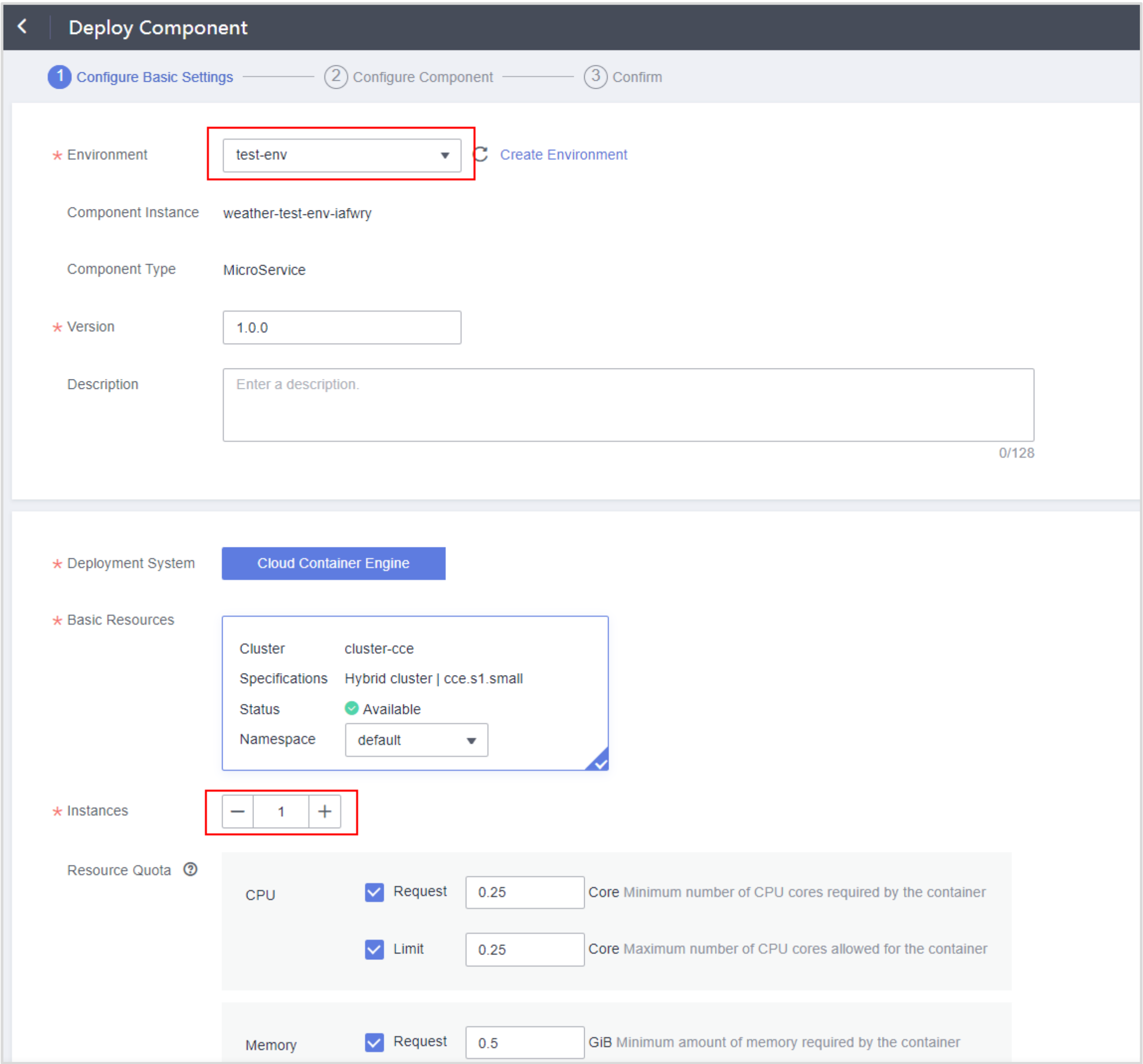
* Name: weather

Figure 7-57

Step 6 Set the parameters as follows and click **Next**.

After an application component is deployed, the microservice is registered with the configured microservice engine. All applications must be registered with the same microservice engine.

- **Environment**: **test-env** (Select the environment created.)
- **Version**: **default**
- **Deployment System**: **Cloud Container Engine**
- **Instances**: **1**
- Retain the default settings for other parameters.



Deploy Component

1 Configure Basic Settings — 2 Configure Component — 3 Confirm

* Environment: test-env

Component Instance: weather-test-env-iafwry

Component Type: MicroService

* Version: 1.0.0

Description: Enter a description. 0/128

* Deployment System: Cloud Container Engine

* Basic Resources:
Cluster: cluster-cce
Specifications: Hybrid cluster | cce.s1.small
Status: Available
Namespace: default

* Instances: 1

Resource Quota

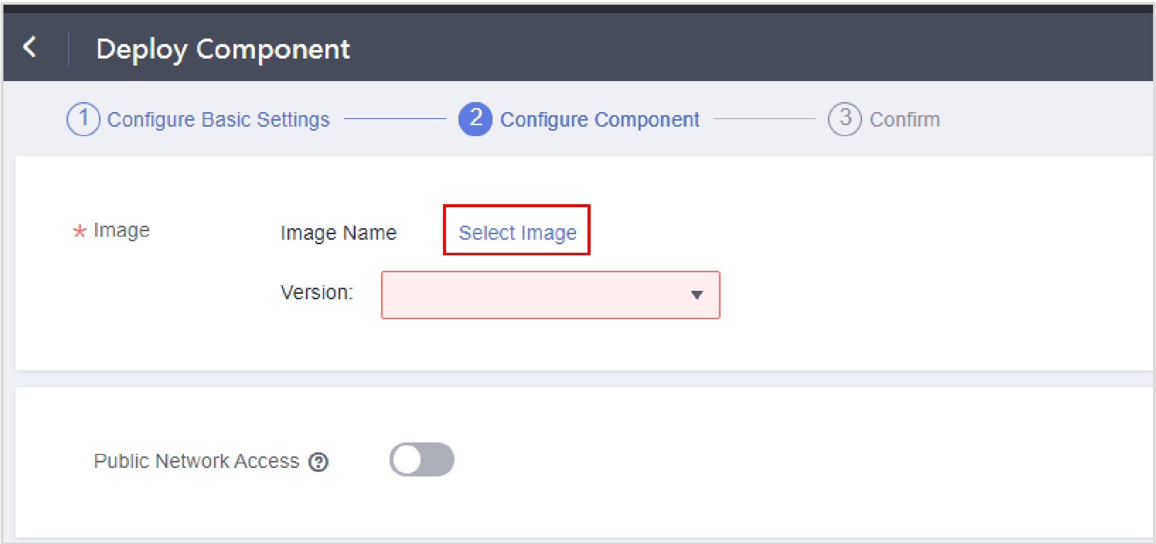
CPU: ☑ Request 0.25 Core Minimum number of CPU cores required by the container

☑ Limit 0.25 Core Maximum number of CPU cores allowed for the container

Memory: ☑ Request 0.5 GiB Minimum amount of memory required by the container

Figure 7-58

Step 7 Click **Select Image**.



Deploy Component

1 Configure Basic Settings — 2 Configure Component — 3 Confirm

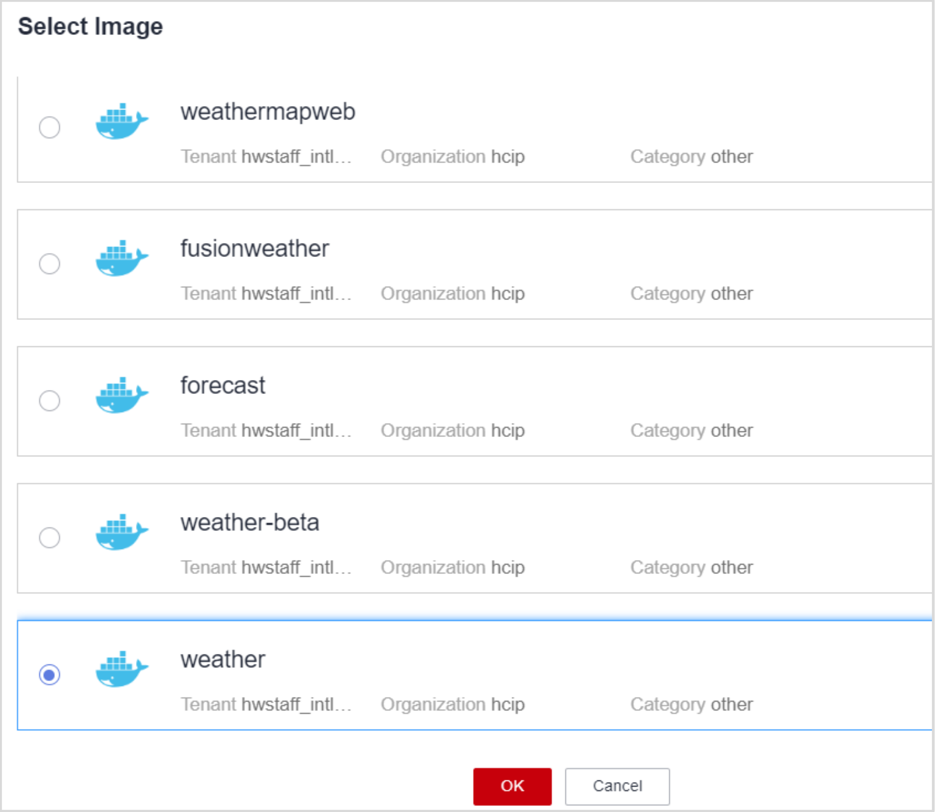
* Image: Image Name

Version:

Public Network Access

Figure 7-59

Step 8 In the displayed dialog box, select the **weather** image. Click **OK**.



Select Image

○ weathermapweb
Tenant hwstaff_intl... Organization hcip Category other

○ fusionweather
Tenant hwstaff_intl... Organization hcip Category other

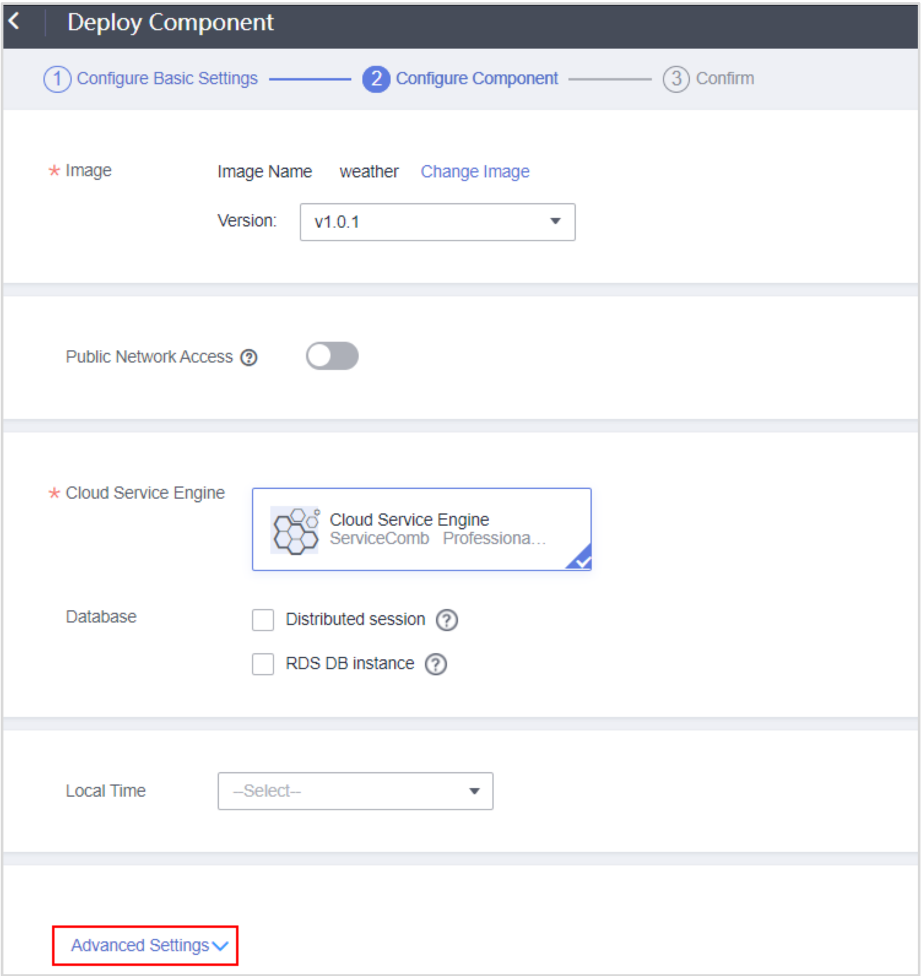
○ forecast
Tenant hwstaff_intl... Organization hcip Category other

○ weather-beta
Tenant hwstaff_intl... Organization hcip Category other

● weather
Tenant hwstaff_intl... Organization hcip Category other

Figure 7-60

Step 9 Retain the default settings for other parameters.



Deploy Component

① Configure Basic Settings ② Configure Component ③ Confirm

* Image: Image Name weather Change Image

Version: v1.0.1

Public Network Access ○

* Cloud Service Engine: Cloud Service Engine ServiceComb Professiona...

Database: □ Distributed session □ RDS DB instance

Local Time: --Select--

Advanced Settings

Figure 7-61

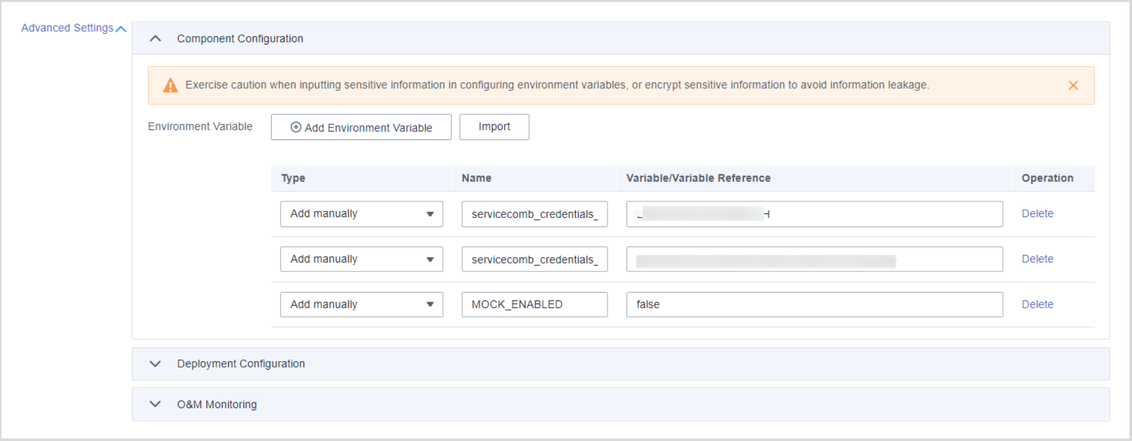
Step 10 In the **Advanced Settings** pane, add the following environment variables:

- **MOCK_ENABLED**: false

If an EIP has been bound to the ECS node in the CCE cluster created and the node can access the public network, set this parameter to **false** or do not set this parameter. The weather data used by the application is real-time data.

- **servicecomb_credentials_accessKey**: AK obtained in section 7.2.1.1.
- **servicecomb_credentials_secretKey**: SK obtained in section 7.2.1.1.

If the professional microservice engine is used, you need to configure an AK/SK.

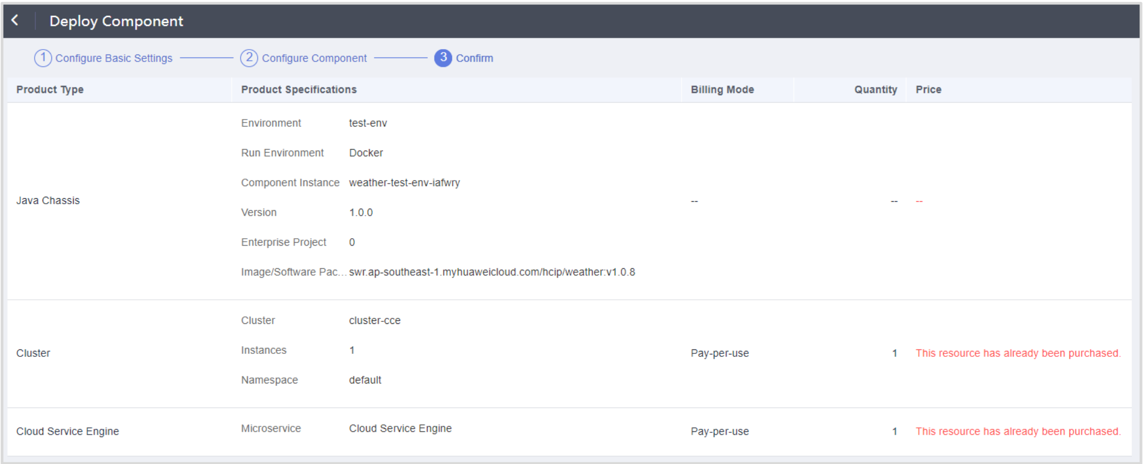


Exercise caution when inputting sensitive information in configuring environment variables, or encrypt sensitive information to avoid information leakage.

Type	Name	Variable/Variable Reference	Operation
Add manually	servicecomb_credentials_	[redacted]	Delete
Add manually	servicecomb_credentials_	[redacted]	Delete
Add manually	MOCK_ENABLED	false	Delete

Figure 7-62

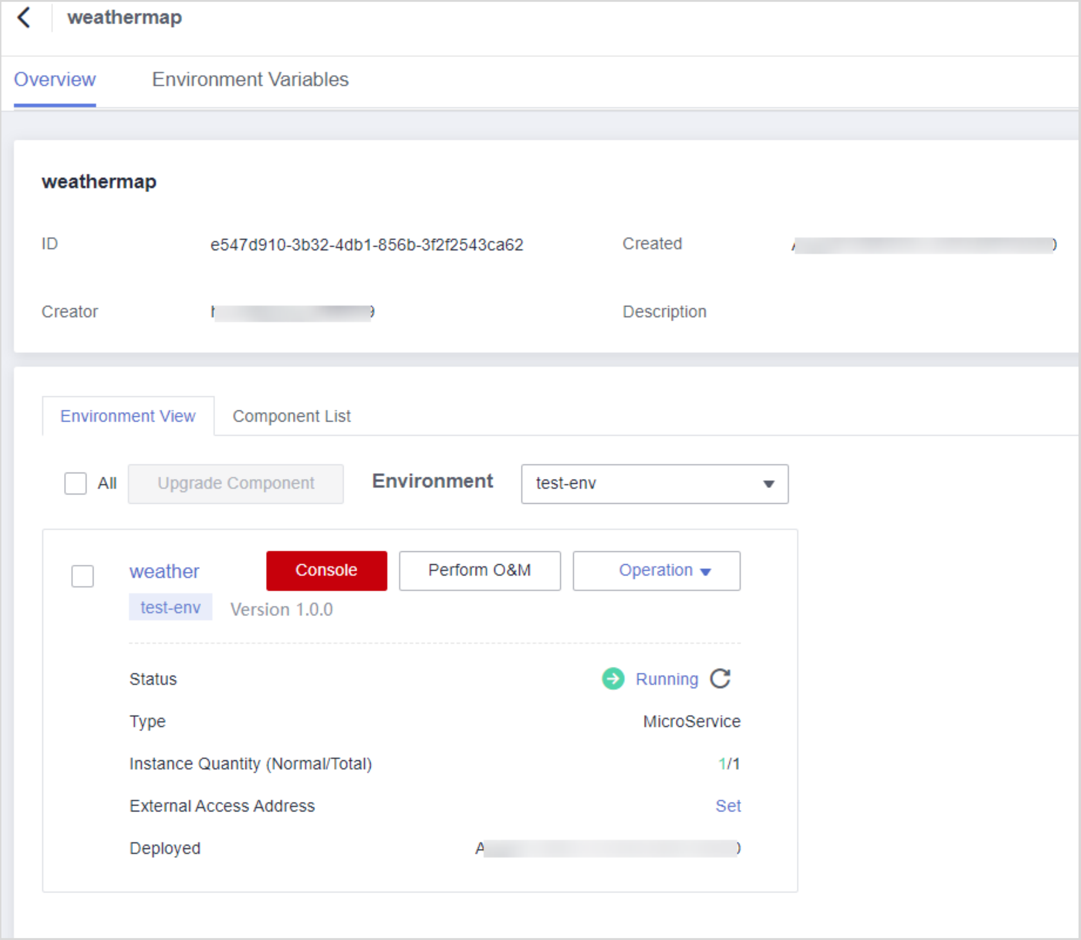
Step 11 Click **Next** to confirm the specifications. Click **Deploy** to deploy the component.



Product Type	Product Specifications		Billing Mode	Quantity	Price
Java Chassis	Environment	test-env	--	--	--
	Run Environment	Docker			
	Component Instance	weather-test-env-iafwry			
	Version	1.0.0			
	Enterprise Project	0			
	Image/Software Pac...	swr.ap-southeast-1.myhuaweicloud.com/hcip/weather:v1.0.8			
Cluster	Cluster	cluster-cce	Pay-per-use	1	This resource has already been purchased.
	Instances	1			
	Namespace	default			
Cloud Service Engine	Microservice	Cloud Service Engine	Pay-per-use	1	This resource has already been purchased.

Figure 7-63

Step 12 Check the status of the deployed component. If the **weather** service is in the Running state, the component has been deployed.



weathermap

Overview Environment Variables

weathermap

ID e547d910-3b32-4db1-856b-3f2f2543ca62

Created [redacted]

Creator [redacted]

Description

Environment View Component List

□ All Upgrade Component Environment test-env

□ weather test-env Version 1.0.0

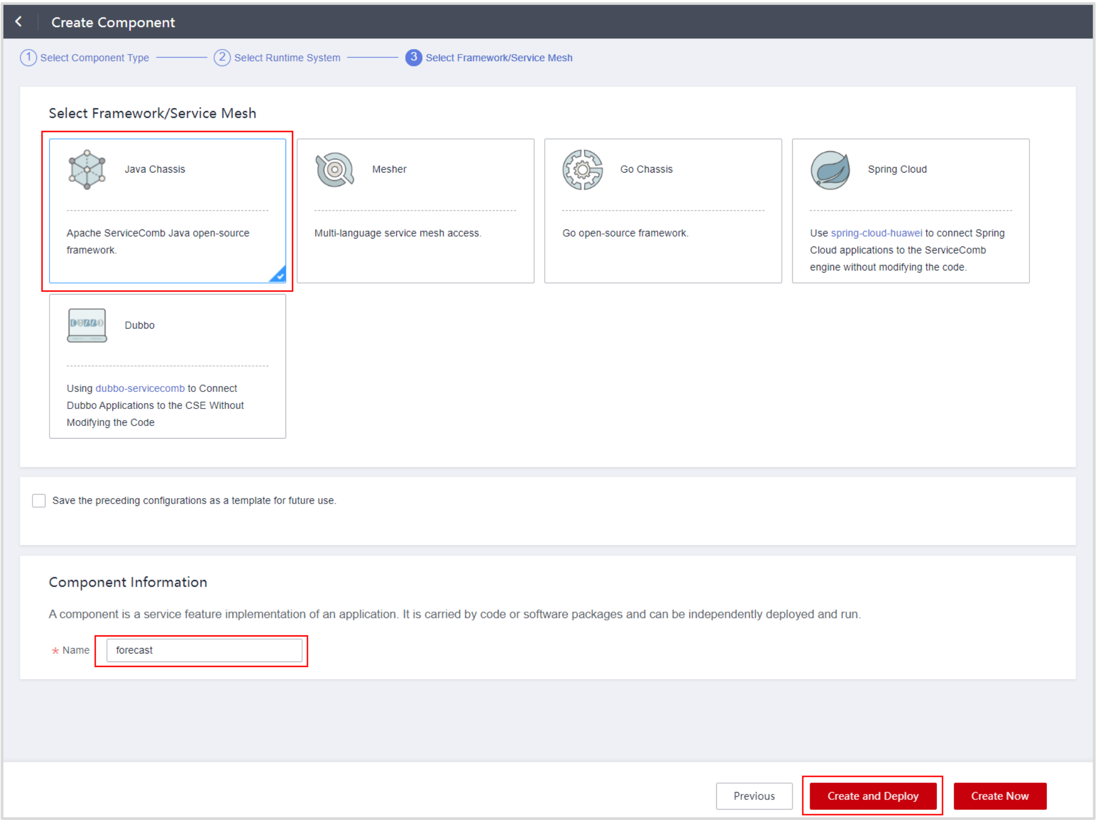
Status	Running
Type	MicroService
Instance Quantity (Normal/Total)	1/1
External Access Address	Set
Deployed	[redacted]

Figure 7-64

Step 13 Repeat the preceding steps to create and deploy the **forecast** and **fusionweather** components.

Deploy the **forecast** component.

- **Framework/Service Mesh**: **Java Chassis**
- **Name**: **forecast**



Select Framework/Service Mesh

Apache ServiceComb Java open-source framework.

Multi-language service mesh access.

Go open-source framework.

Use spring-cloud-huawei to connect Spring Cloud applications to the ServiceComb engine without modifying the code.

Using dubbo-servicecomb to Connect Dubbo Applications to the CSE Without Modifying the Code

□ Save the preceding configurations as a template for future use.

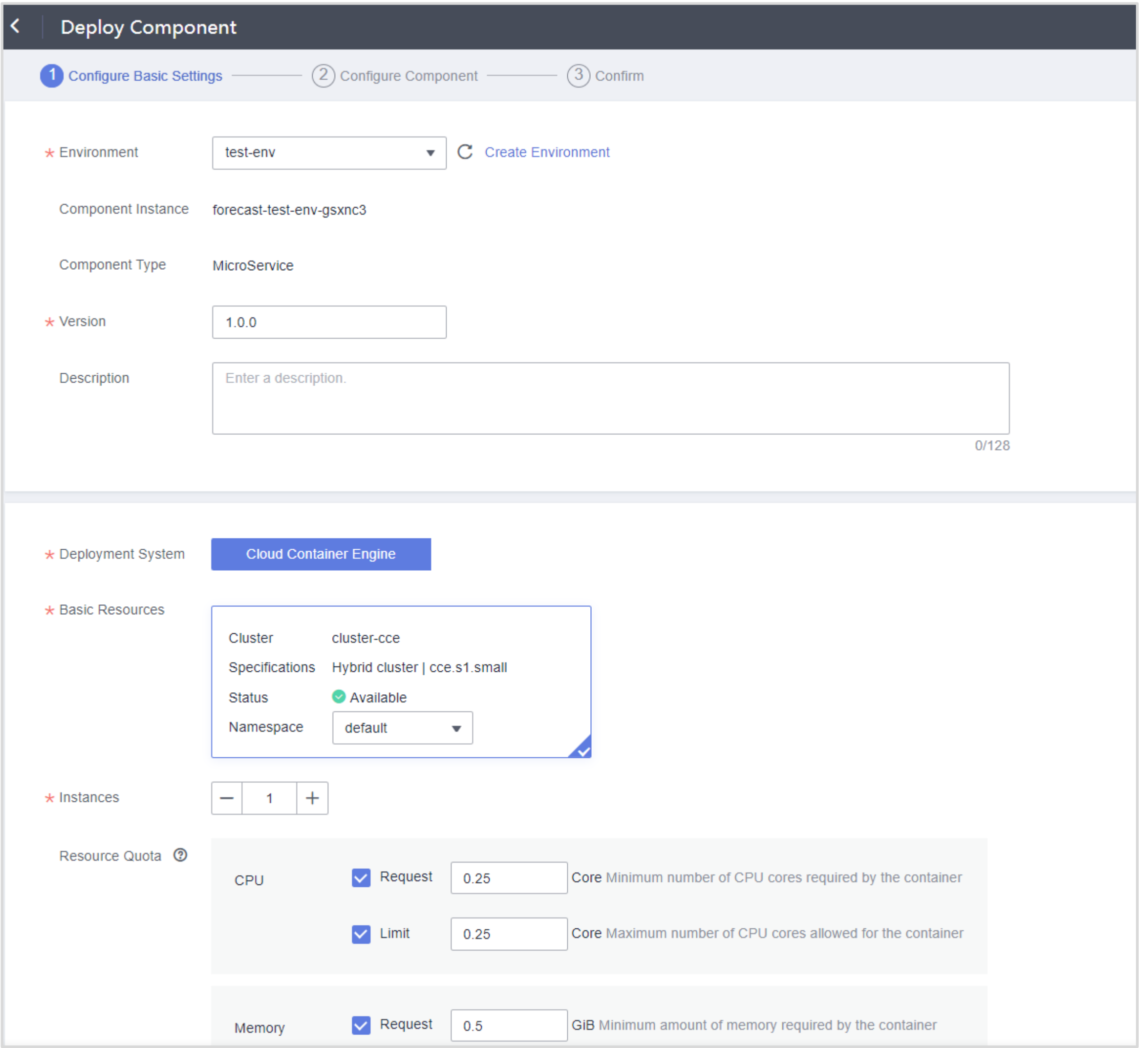
Component Information

A component is a service feature implementation of an application. It is carried by code or software packages and can be independently deployed and run.

* Name: forecast

Figure 7-65

- **Environment: test-env**
- **Version: default**
- **Deployment System: Cloud Container Engine**
- **Instances: 1**
- Retain the default settings for other parameters.



Deploy Component

1 Configure Basic Settings — 2 Configure Component — 3 Confirm

* Environment: test-env (Create Environment)

Component Instance: forecast-test-env-gsxnc3

Component Type: MicroService

* Version: 1.0.0

Description: Enter a description. 0/128

* Deployment System: Cloud Container Engine

* Basic Resources:

Cluster: cluster-cce
Specifications: Hybrid cluster | cce.s1.small
Status: Available
Namespace: default

* Instances: 1

Resource Quota

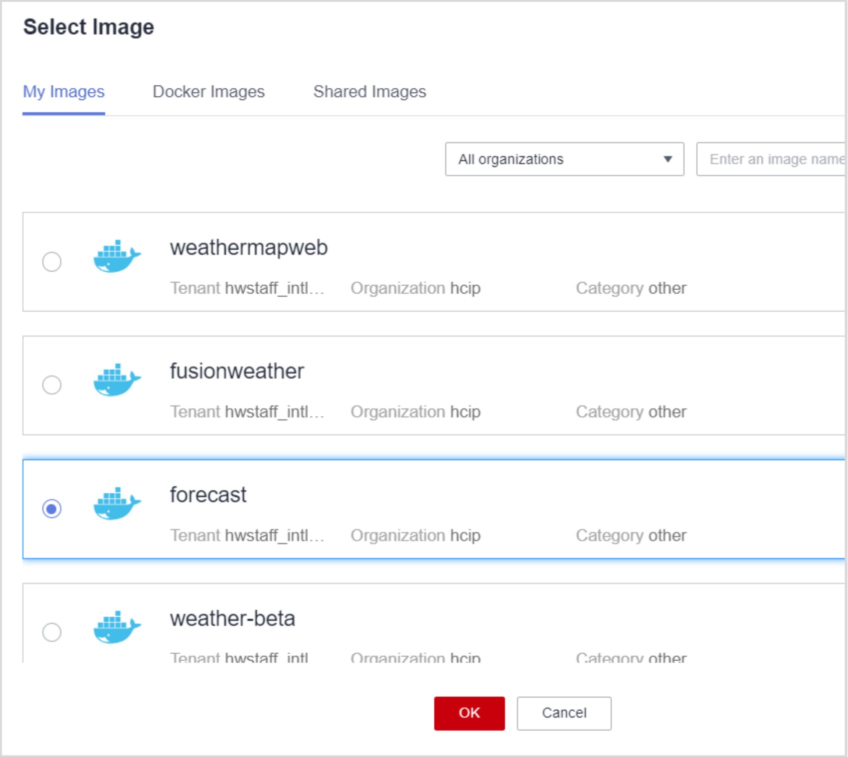
CPU ☑ Request 0.25 Core Minimum number of CPU cores required by the container

☑ Limit 0.25 Core Maximum number of CPU cores allowed for the container

Memory ☑ Request 0.5 GiB Minimum amount of memory required by the container

Figure 7-66

- Select the **forecast** image.



Select Image

My Images | Docker Images | Shared Images

All organizations ▾ | Enter an image name

○ weathermapweb
Tenant hwstaff_intl... Organization hcip Category other

○ fusionweather
Tenant hwstaff_intl... Organization hcip Category other

● forecast
Tenant hwstaff_intl... Organization hcip Category other

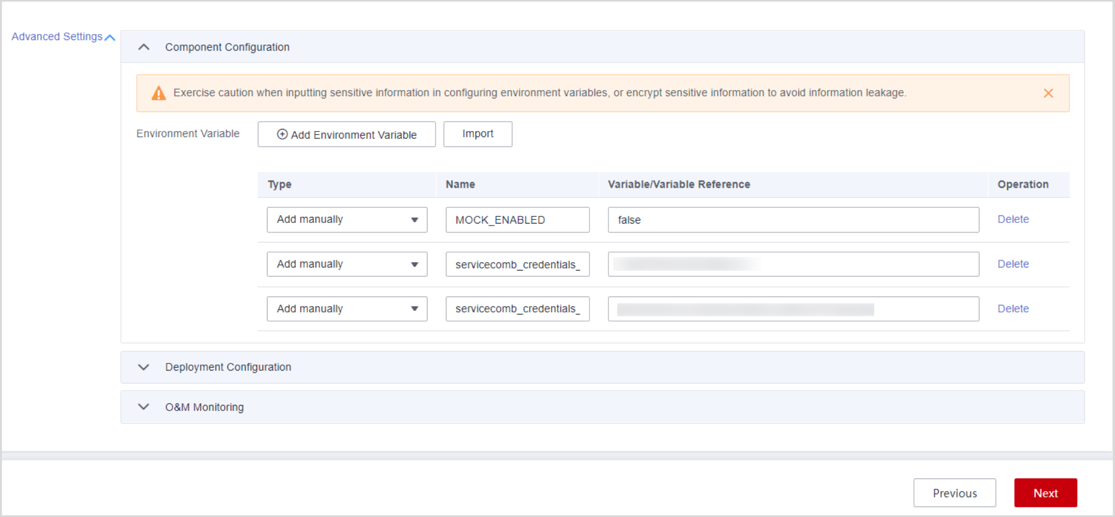
○ weather-beta
Tenant hwstaff_intl Organization hcip Category other

OK | Cancel

Figure 7-67

In the **Advanced Settings** pane, add the following environment variables:

- **MOCK_ENABLED**: false
- **servicecomb_credentials_accessKey**: AK obtained in section 7.2.1.1.
- **servicecomb_credentials_secretKey**: SK obtained in section 7.2.1.1.



Advanced Settings ^

Component Configuration

Exercise caution when inputting sensitive information in configuring environment variables, or encrypt sensitive information to avoid information leakage.

Environment Variable | ⊕ Add Environment Variable | Import

Type	Name	Variable/Variable Reference	Operation
Add manually ▾	MOCK_ENABLED	false	Delete
Add manually ▾	servicecomb_credentials_	[redacted]	Delete
Add manually ▾	servicecomb_credentials_	[redacted]	Delete

Deployment Configuration

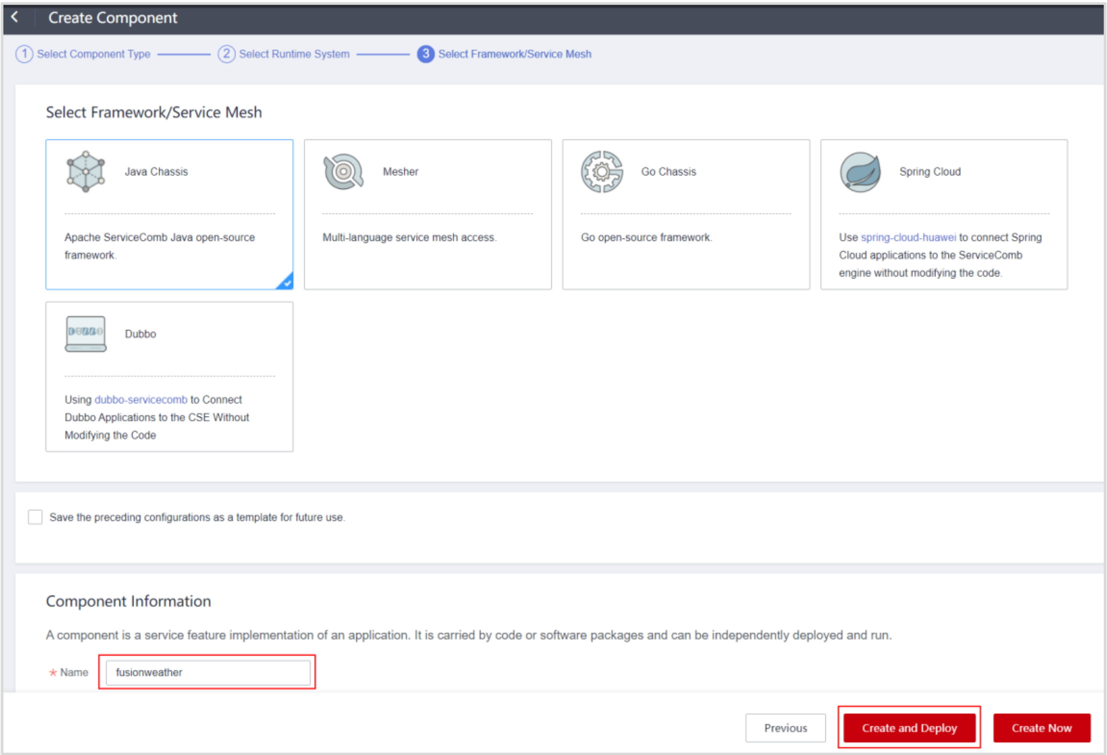
O&M Monitoring

Previous | Next

Figure 7-68

Deploy the **fusionweather** component.

- **Framework/Service Mesh: Java Chassis**
- **Name: fusionweather**



Create Component

1 Select Component Type — 2 Select Runtime System — 3 Select Framework/Service Mesh

Select Framework/Service Mesh

Java Chassis: Apache ServiceComb Java open-source framework.

Mesher: Multi-language service mesh access.

Go Chassis: Go open-source framework.

Spring Cloud: Use spring-cloud-huawei to connect Spring Cloud applications to the ServiceComb engine without modifying the code.

Dubbo: Using dubbo-servicecomb to Connect Dubbo Applications to the CSE Without Modifying the Code

□ Save the preceding configurations as a template for future use.

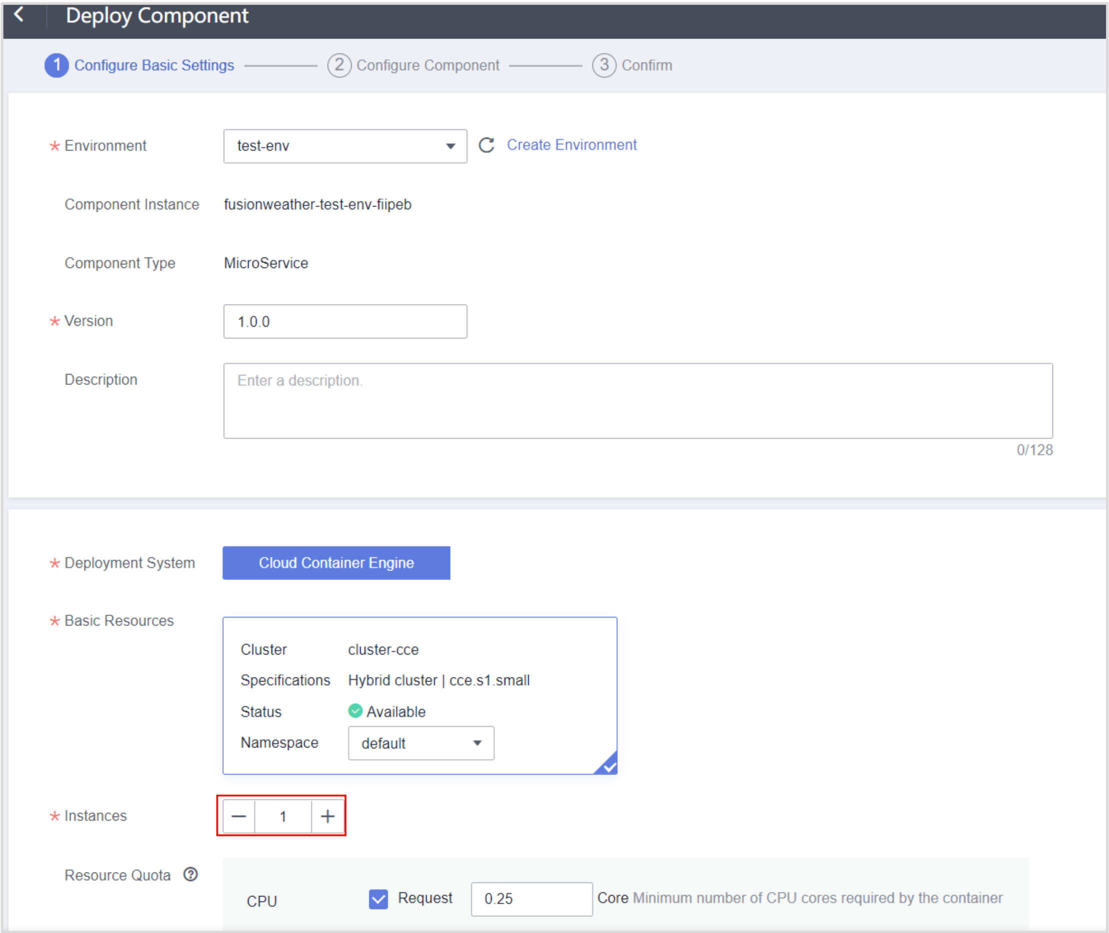
Component Information

A component is a service feature implementation of an application. It is carried by code or software packages and can be independently deployed and run.

* Name: fusionweather

Figure 7-69

- **Environment: test-env**
- **Version: default**
- **Deployment System: Cloud Container Engine**
- **Instances: 1**
- Retain the default settings for other parameters.



Deploy Component

1 Configure Basic Settings — 2 Configure Component — 3 Confirm

* Environment: test-env — Create Environment

Component Instance: fusionweather-test-env-fiipeb

Component Type: MicroService

* Version: 1.0.0

Description: Enter a description. 0/128

* Deployment System: Cloud Container Engine

* Basic Resources:

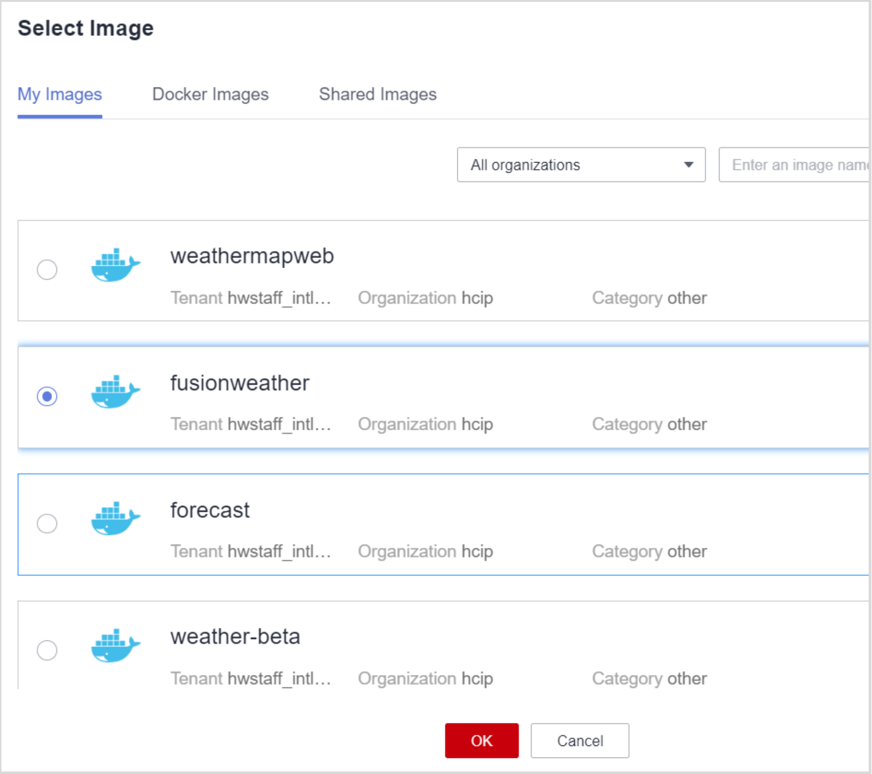
Cluster	cluster-cce
Specifications	Hybrid cluster | cce.s1.small
Status	Available
Namespace	default

* Instances: 1

Resource Quota: CPU ☑ Request 0.25 Core Minimum number of CPU cores required by the container

Figure 7-70

- Select the **fusionweather** image.



Select Image

My Images Docker Images Shared Images

All organizations ▾ | Enter an image name

○ weathermapweb
Tenant hwstaff_intl… Organization hcip Category other

● fusionweather
Tenant hwstaff_intl… Organization hcip Category other

○ forecast
Tenant hwstaff_intl… Organization hcip Category other

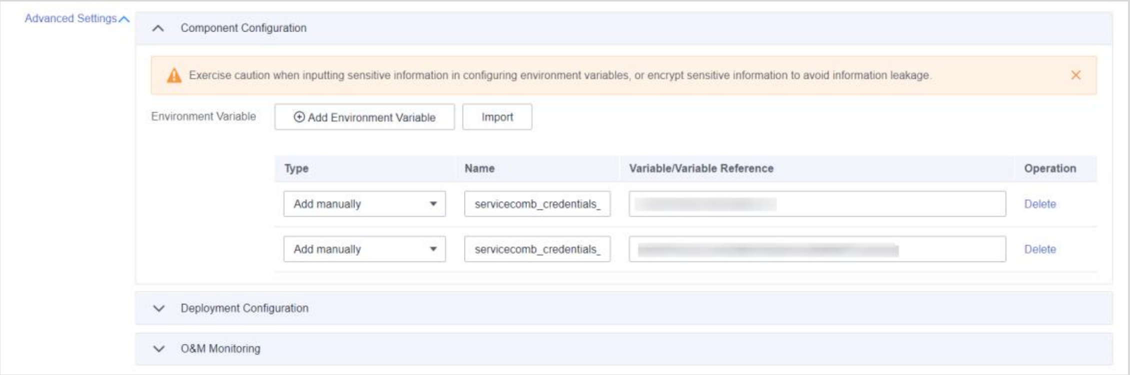
○ weather-beta
Tenant hwstaff_intl… Organization hcip Category other

OK Cancel

Figure 7-71

In the **Advanced Settings** pane, add the following environment variables:

- **servicecomb_credentials_accessKey**: AK obtained in section 7.2.1.1.
- **servicecomb_credentials_secretKey**: SK obtained in section 7.2.1.1.



Advanced Settings

Component Configuration

Exercise caution when inputting sensitive information in configuring environment variables, or encrypt sensitive information to avoid information leakage.

Environment Variable: Add Environment Variable | Import

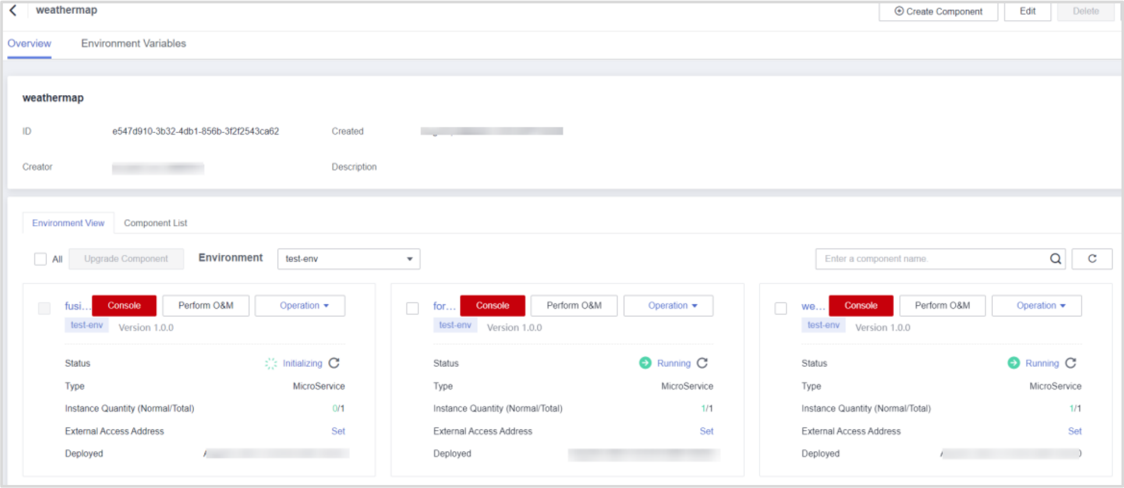
Type	Name	Variable/Variable Reference	Operation
Add manually ▾	servicecomb_credentials_	[redacted]	Delete
Add manually ▾	servicecomb_credentials_	[redacted]	Delete

Deployment Configuration

O&M Monitoring

Figure 7-72

Step 14 On ServiceStage, click the created application **weathermap** to view the microservice deployment status. As shown in the following figure, the three services are Normal, indicating that the backend application components fusionweather, forecast, and weather have been deployed.



weathermap

ID e547d910-3b32-4db1-856b-3f2f2543ca62 Created [redacted]

Creator [redacted] Description

Environment test-env

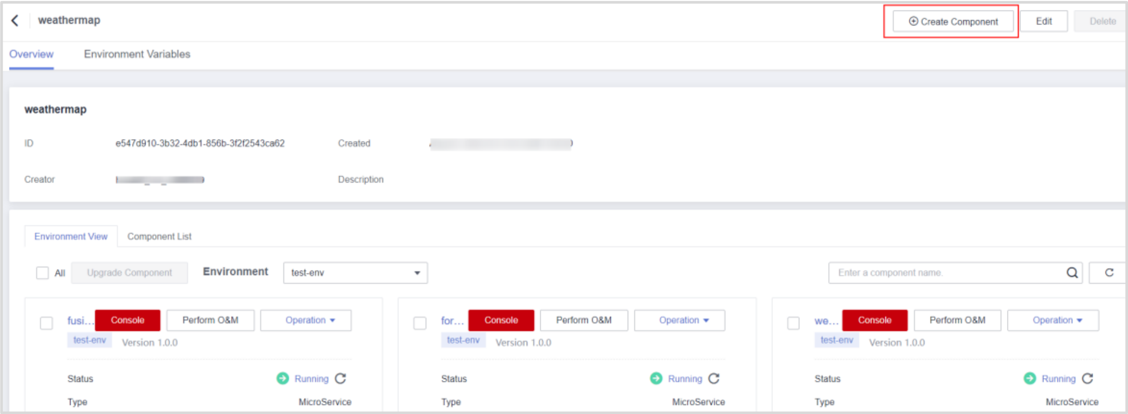
	fusi...	for...	we...
	test-env Version 1.0.0	test-env Version 1.0.0	test-env Version 1.0.0
Status	Initializing	Running	Running
Type	MicroService	MicroService	MicroService
Instance Quantity (Normal/Total)	0/1	1/1	1/1
External Access Address	Set	Set	Set
Deployed	[redacted]	[redacted]	[redacted]

Figure 7-73

7.2.3.2 Creating and Deploying Frontend Application Components

Step 1 Log in to ServiceStage and choose **Application Management** > **Application List**.

Step 2 Click an application. On the **Overview** tab page, click **Create Component**.



weathermap

ID e547d910-3b32-4db1-856b-3f2f2543ca62 Created [redacted]

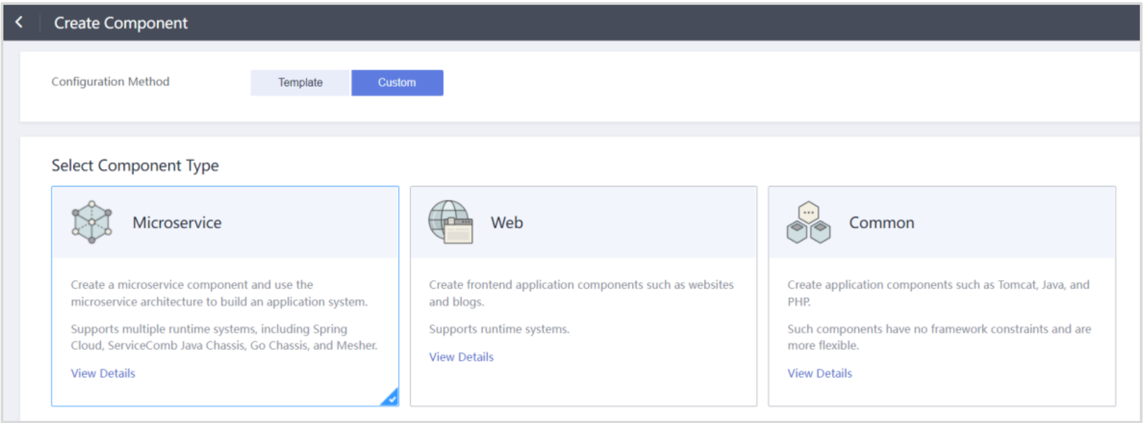
Creator [redacted] Description

Environment test-env

	fusi...	for...	we...
	test-env Version 1.0.0	test-env Version 1.0.0	test-env Version 1.0.0
Status	Running	Running	Running
Type	MicroService	MicroService	MicroService

Figure 7-74

Step 3 Select **Custom** for **Configuration Method**. On the page that is displayed, select **Microservice** and click **Next**.



Configuration Method Custom

Select Component Type

Microservice

Create a microservice component and use the microservice architecture to build an application system.

Supports multiple runtime systems, including Spring Cloud, ServiceComb Java Chassis, Go Chassis, and Mesher.

Web

Create frontend application components such as websites and blogs.

Supports runtime systems.

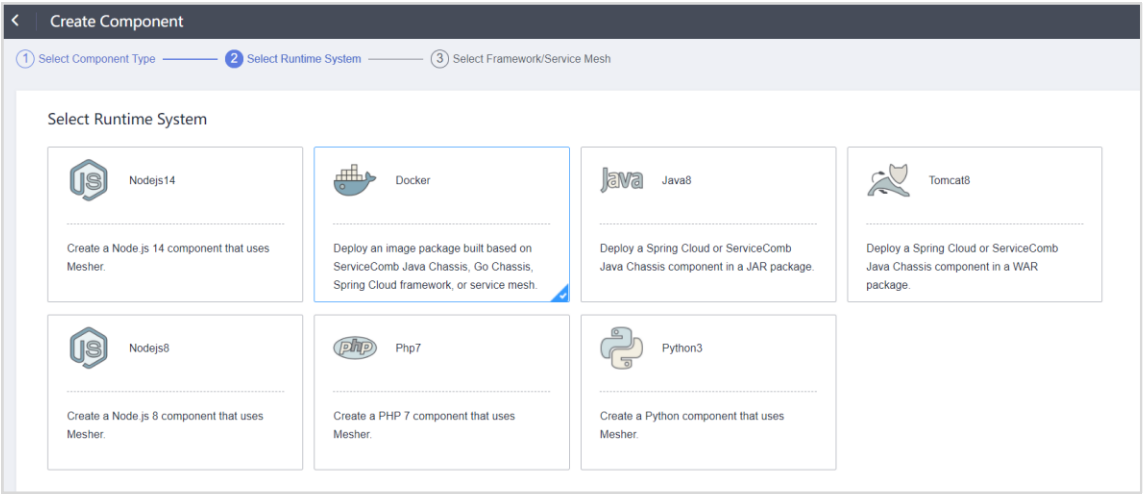
Common

Create application components such as Tomcat, Java, and PHP.

Such components have no framework constraints and are more flexible.

Figure 7-75

Step 4 Select **Docker** for **Runtime System** and click **Next**.



Select Runtime System

Nodejs14 — Create a Node.js 14 component that uses Mesher.

Docker — Deploy an image package built based on ServiceComb Java Chassis, Go Chassis, Spring Cloud framework, or service mesh.

Java8 — Deploy a Spring Cloud or ServiceComb Java Chassis component in a JAR package.

Tomcat8 — Deploy a Spring Cloud or ServiceComb Java Chassis component in a WAR package.

Nodejs8 — Create a Node.js 8 component that uses Mesher.

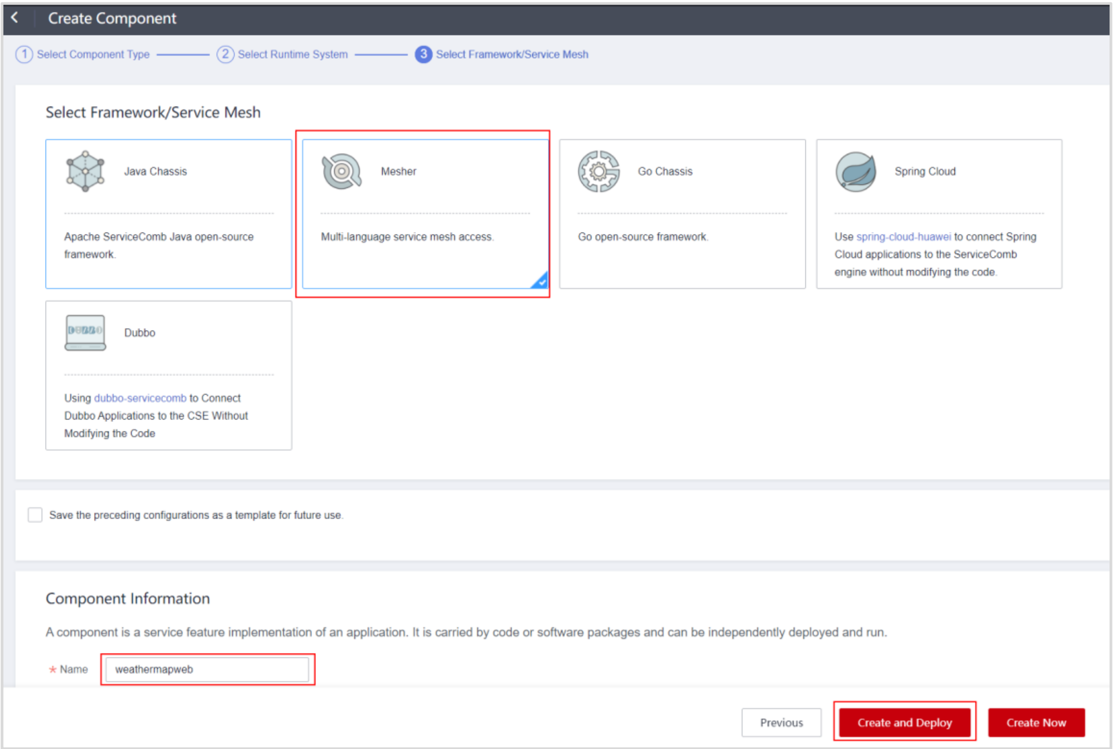
Php7 — Create a PHP 7 component that uses Mesher.

Python3 — Create a Python component that uses Mesher.

Figure 7-76

Step 5 Create a service component as follows and click **Next**.

- **Framework/Service Mesh: Mesher**
- **Name: weathermapweb**



Select Framework/Service Mesh

Java Chassis — Apache ServiceComb Java open-source framework.

Mesher — Multi-language service mesh access.

Go Chassis — Go open-source framework.

Spring Cloud — Use spring-cloud-huawei to connect Spring Cloud applications to the ServiceComb engine without modifying the code.

Dubbo — Using dubbo-servicecomb to Connect Dubbo Applications to the CSE Without Modifying the Code

□ Save the preceding configurations as a template for future use.

Component Information

A component is a service feature implementation of an application. It is carried by code or software packages and can be independently deployed and run.

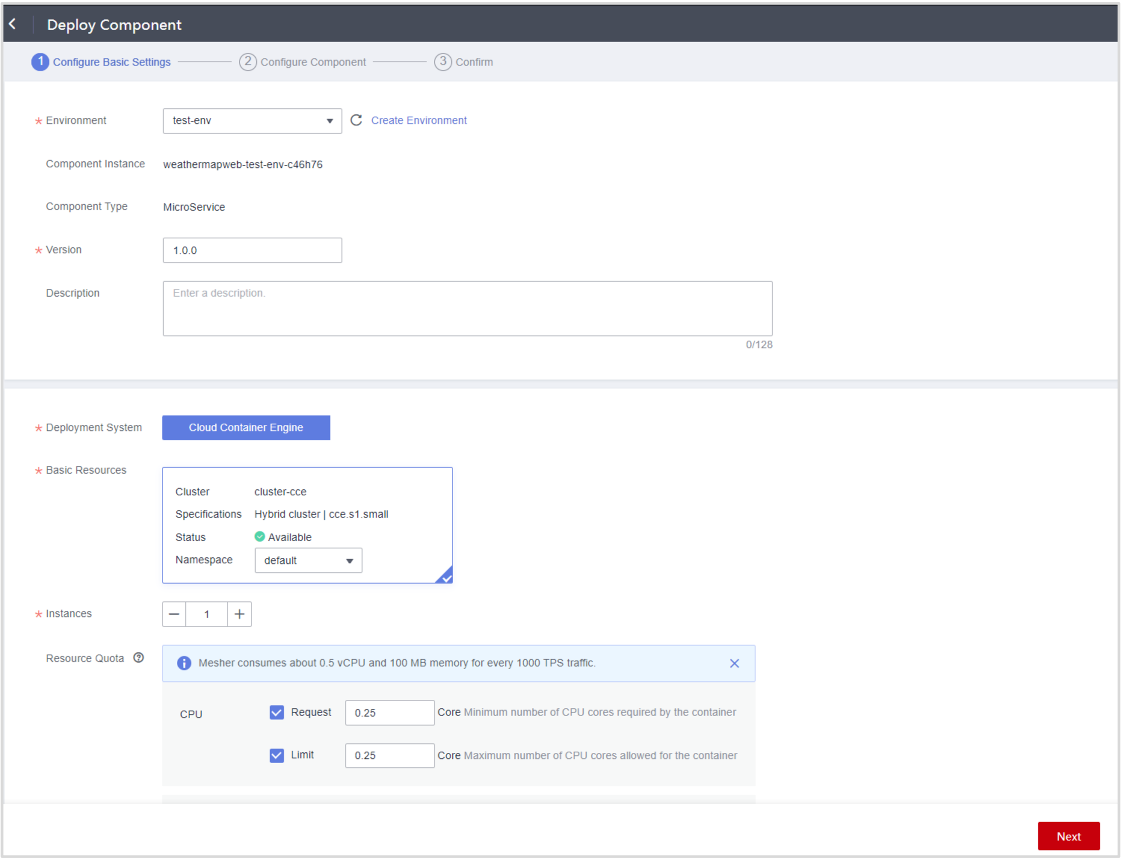
* Name: weathermapweb

Figure 7-77

Step 6 Set the parameters as follows: Click **Next** to configure the component.

- **Environment: test-env**

- **Version: default**
- **Deployment System: Cloud Container Engine**
- **Instances: 1**
- Retain the default settings for other parameters.



Deploy Component

① Configure Basic Settings —— ② Configure Component —— ③ Confirm

* Environment: test-env — Create Environment

Component Instance: weathermapweb-test-env-c46h76

Component Type: MicroService

* Version: 1.0.0

Description: Enter a description. 0/128

* Deployment System: Cloud Container Engine

* Basic Resources:
Cluster: cluster-cce
Specifications: Hybrid cluster | cce.s1.small
Status: Available
Namespace: default

* Instances: 1

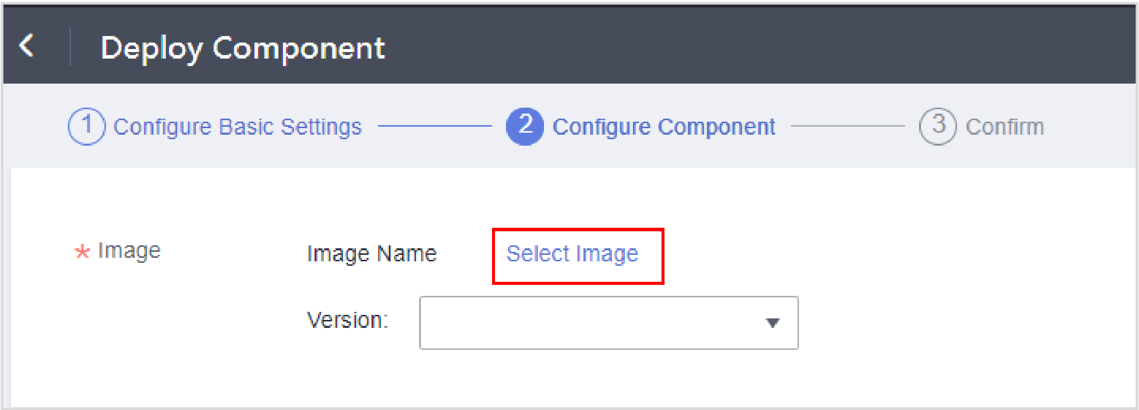
Resource Quota: Mesher consumes about 0.5 vCPU and 100 MB memory for every 1000 TPS traffic.

CPU ☑ Request 0.25 Core Minimum number of CPU cores required by the container
☑ Limit 0.25 Core Maximum number of CPU cores allowed for the container

Next

Figure 7-78

Step 7 Click **Select Container Image**.



Deploy Component

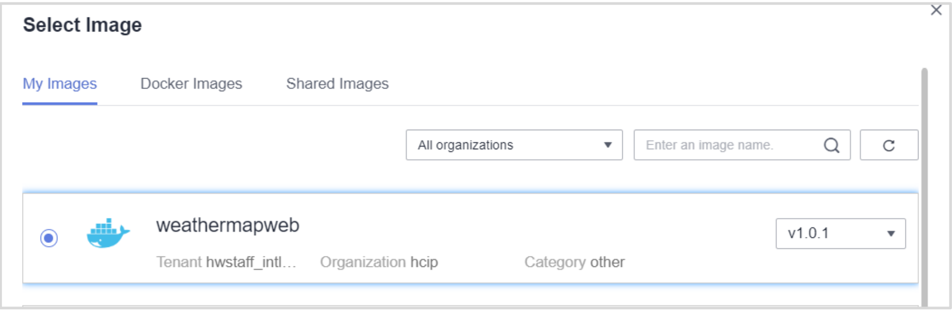
① Configure Basic Settings —— ② Configure Component —— ③ Confirm

* Image Image Name Select Image

Version:

Figure 7-79

Step 8 In the displayed dialog box, select the **weathermapweb** image. Click **OK**.



Select Image

My Images | Docker Images | Shared Images

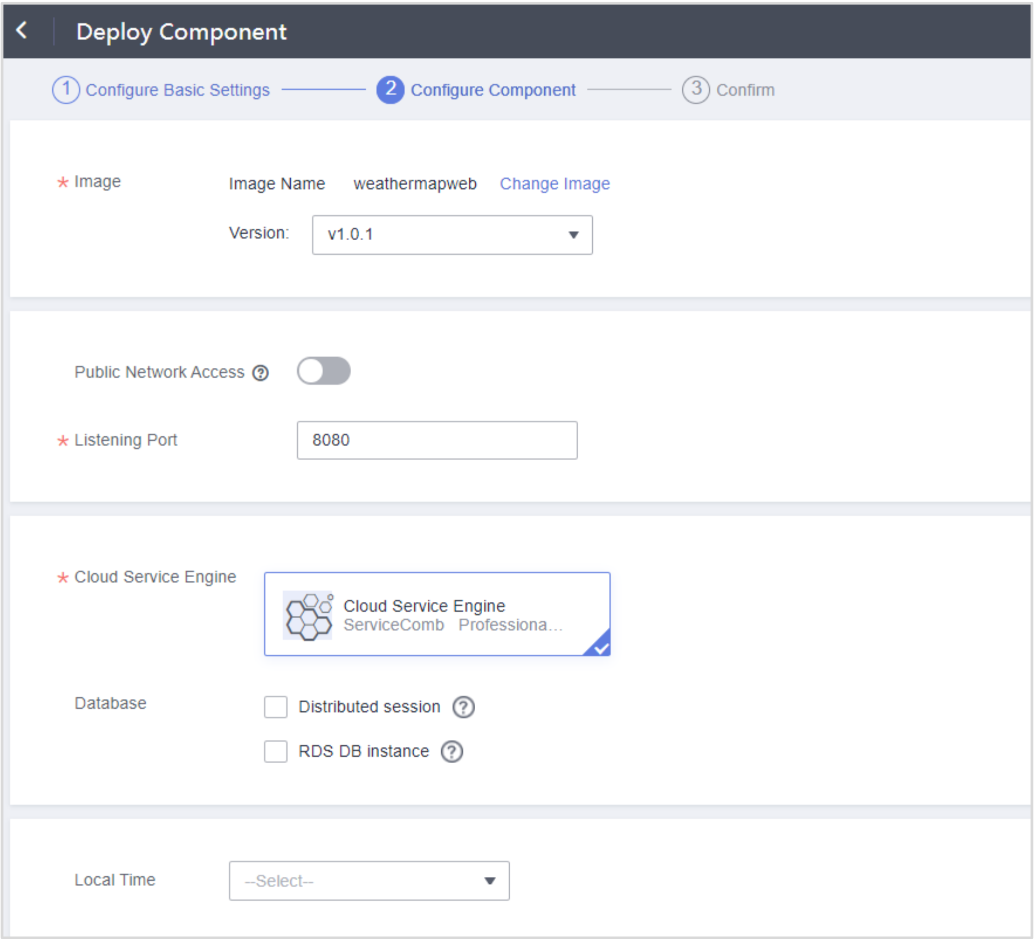
All organizations | Enter an image name.

● weathermapweb — v1.0.1

Tenant hwstaff_intl... Organization hcip Category other

Figure 7-80

Step 9 Retain the default settings for other parameters，Click **Next**.



Deploy Component

1 Configure Basic Settings — 2 Configure Component — 3 Confirm

* Image: Image Name weathermapweb Change Image

Version: v1.0.1

Public Network Access: off

* Listening Port: 8080

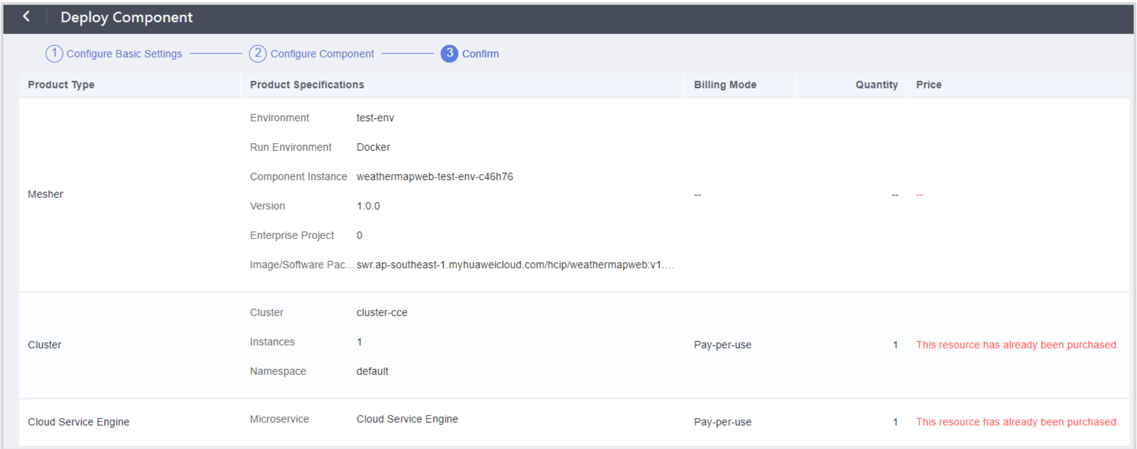
* Cloud Service Engine: Cloud Service Engine ServiceComb Professiona...

Database: □ Distributed session □ RDS DB instance

Local Time: --Select--

Figure 7-81

Step 10 Click **Deploy** to deploy the component.



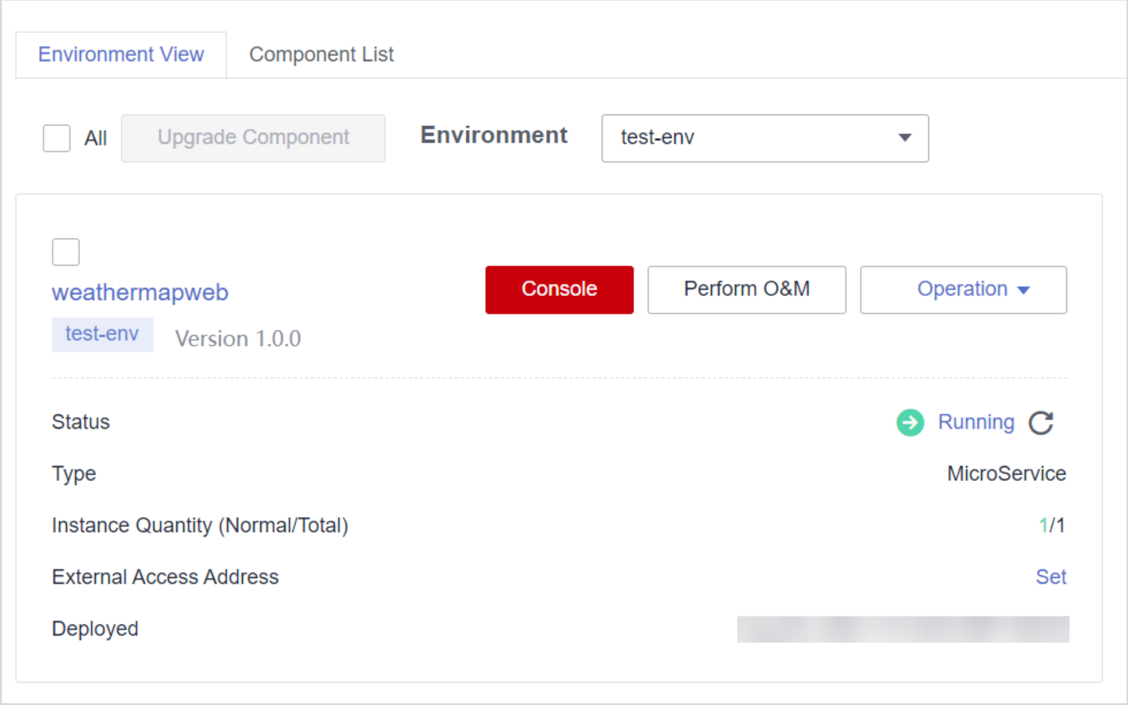
Deploy Component

① Configure Basic Settings — ② Configure Component — ③ Confirm

Product Type	Product Specifications		Billing Mode	Quantity	Price
Mesher	Environment	test-env	--	--	--
	Run Environment	Docker			
	Component Instance	weathermapweb-test-env-c46h76			
	Version	1.0.0			
	Enterprise Project	0			
	Image/Software Pac...	swr.ap-southeast-1.myhuaweicloud.com/hcip/weathermapweb:v1....			
Cluster	Cluster	cluster-cce	Pay-per-use	1	This resource has already been purchased.
	Instances	1			
	Namespace	default			
Cloud Service Engine	Microservice	Cloud Service Engine	Pay-per-use	1	This resource has already been purchased.

Figure 7-82

Step 11 View the deployed microservices. If the **weathermapweb** service is Running, the service component has been deployed.



Environment View | Component List

□ All | Upgrade Component | Environment: test-env ▾

□ weathermapweb

test-env Version 1.0.0

Console | Perform O&M | Operation ▾

Status: Running

Type: MicroService

Instance Quantity (Normal/Total): 1/1

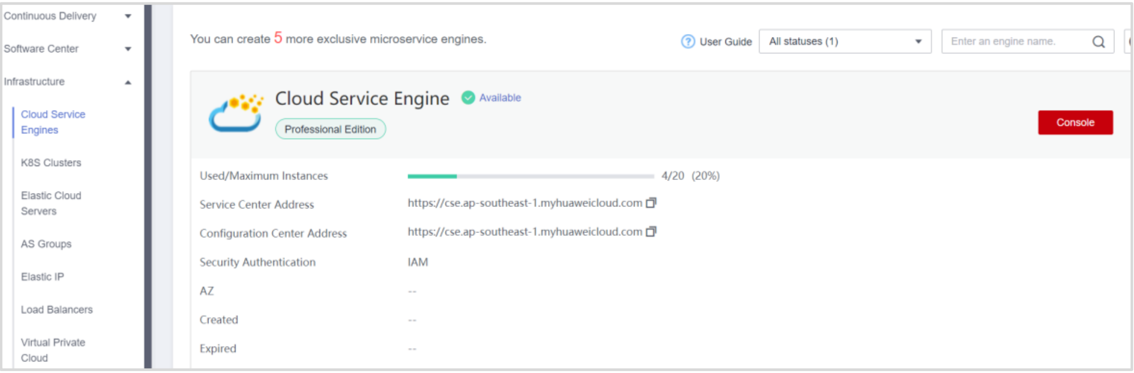
External Access Address: Set

Deployed: [redacted]

Figure 7-83

Step 12 Log in to ServiceStage and choose **Infrastructure** > **Cloud Service Engines**.

Step 13 Select the microservice engine created and click **Console**.



Continuous Delivery
Software Center
Infrastructure
Cloud Service Engines
K8S Clusters
Elastic Cloud Servers
AS Groups
Elastic IP
Load Balancers
Virtual Private Cloud

You can create 5 more exclusive microservice engines.

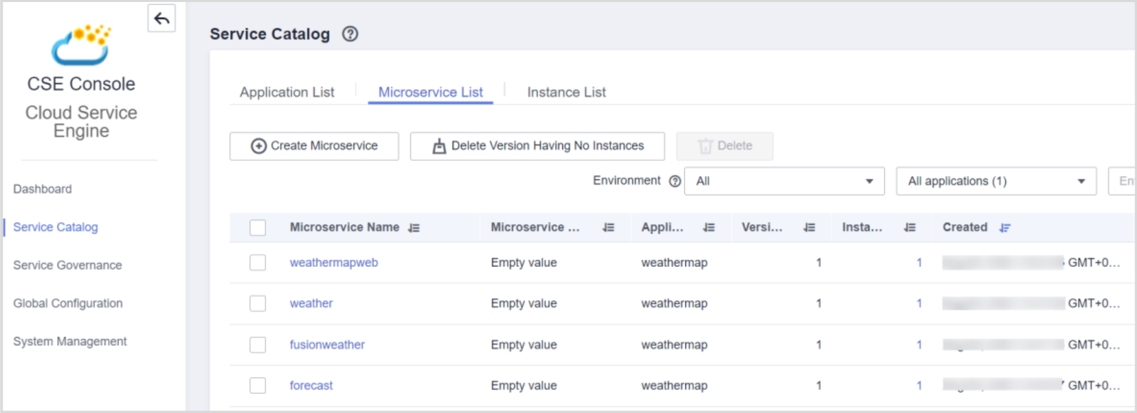
User Guide | All statuses (1) | Enter an engine name.

Cloud Service Engine Available
Professional Edition
Console

Used/Maximum Instances	4/20 (20%)
Service Center Address	https://cse.ap-southeast-1.myhuaweicloud.com
Configuration Center Address	https://cse.ap-southeast-1.myhuaweicloud.com
Security Authentication	IAM
AZ	--
Created	--
Expired	--

Figure 7-84

Step 14 On the **Microservice List** page, if the following microservices are displayed and the number of microservice instances is not 0, the deployment is successful:



CSE Console
Cloud Service Engine
Dashboard
Service Catalog
Service Governance
Global Configuration
System Management

Service Catalog

Application List | Microservice List | Instance List

Create Microservice | Delete Version Having No Instances | Delete

Environment: All | All applications (1)

☐	Microservice Name	Microservice ...	Appli...	Versi...	Insta...	Created
☐	weathermapweb	Empty value	weathermap	1	1	[redacted] GMT+0...
☐	weather	Empty value	weathermap	1	1	[redacted] GMT+0...
☐	fusionweather	Empty value	weathermap	1	1	[redacted] GMT+0...
☐	forecast	Empty value	weathermap	1	1	[redacted] GMT+0...

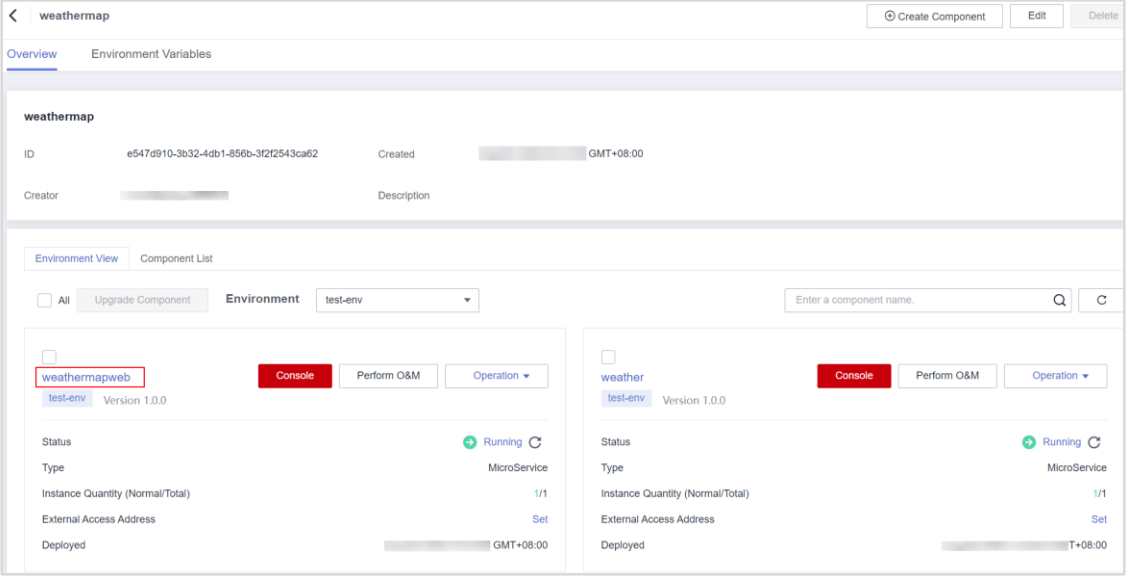
Figure 7-85

7.2.3.3 Setting the Access Mode

Step 1 Log in to ServiceStage and choose **Application Management** > **Application List**.

Step 2 Click **weathermap** to go to the **Overview** page.

Step 3 Click **weathermapweb**. The **Overview** page is displayed.



weathermap

⊕ Create Component | Edit | Delete

Overview | Environment Variables

weathermap

ID e547d910-3b32-4db1-856b-3f2f2543ca62 Created [redacted] GMT+08:00

Creator [redacted] Description

Environment View | Component List

□ All Upgrade Component Environment test-env

Enter a component name.

□ weathermapweb test-env Version 1.0.0 Console | Perform O&M | Operation

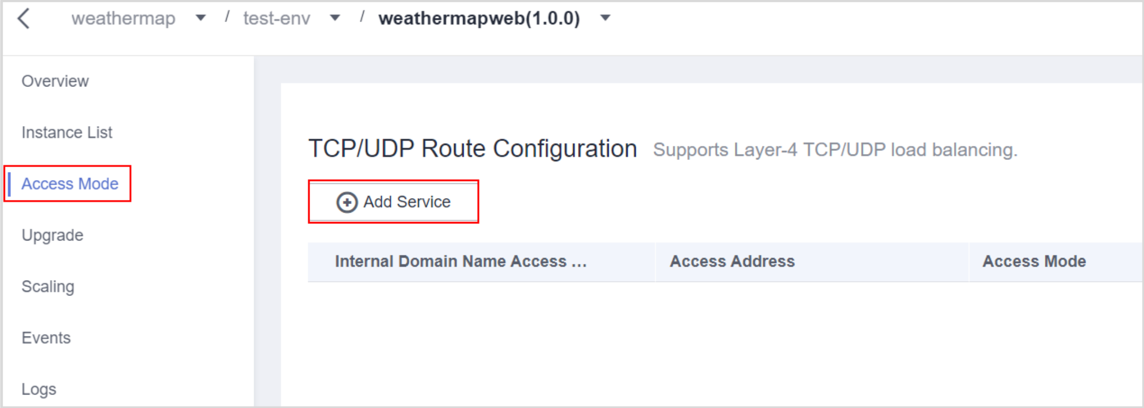
Status: Running
Type: MicroService
Instance Quantity (Normal/Total): 1/1
External Access Address: Set
Deployed: [redacted] GMT+08:00

□ weather test-env Version 1.0.0 Console | Perform O&M | Operation

Status: Running
Type: MicroService
Instance Quantity (Normal/Total): 1/1
External Access Address: Set
Deployed: [redacted] T+08:00

Figure 7-86

Step 4 Choose **Access Mode** > **Add Service**.



weathermap / test-env / weathermapweb(1.0.0)

Overview
Instance List
Access Mode
Upgrade
Scaling
Events
Logs

TCP/UDP Route Configuration Supports Layer-4 TCP/UDP load balancing.

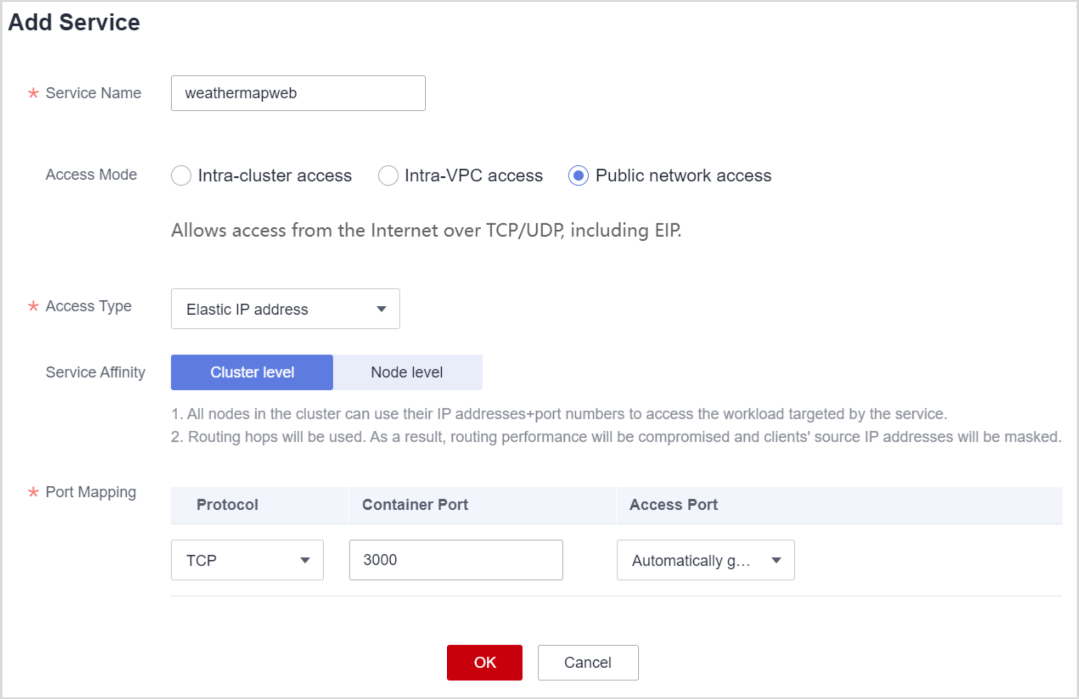
⊕ Add Service

Internal Domain Name Access ...	Access Address	Access Mode

Figure 7-87

Step 5 Set the parameters as follows:

- Service Name: weathermapweb
- **Access Mode: Public network access**
- **Access Type: Elastic IP address**
- **Service Affinity: Cluster level**
- **Port Mapping: TCP | 3000 | Automatically generated**



Add Service

* Service Name: weathermapweb

Access Mode: ○ Intra-cluster access ○ Intra-VPC access ● Public network access

Allows access from the Internet over TCP/UDP, including EIP.

* Access Type: Elastic IP address

Service Affinity: Cluster level | Node level

1. All nodes in the cluster can use their IP addresses+port numbers to access the workload targeted by the service.
2. Routing hops will be used. As a result, routing performance will be compromised and clients' source IP addresses will be masked.

* Port Mapping

Protocol	Container Port	Access Port
TCP	3000	Automatically g…

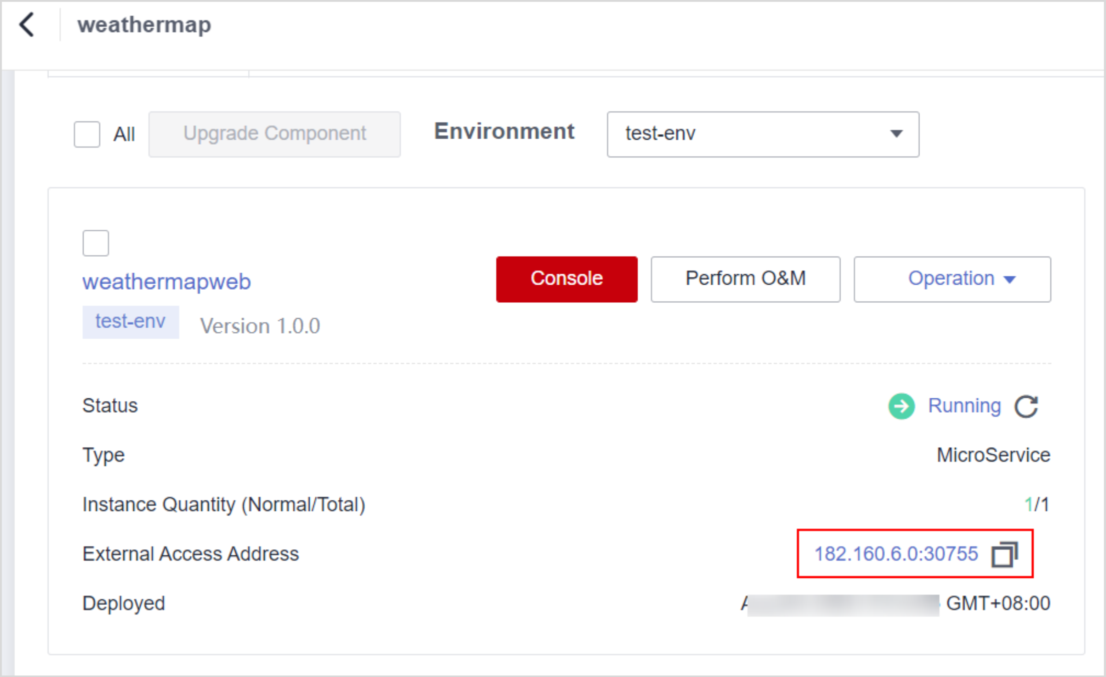
Figure 7-88

7.3 Verifying the Result

Step 1 Log in to ServiceStage and choose **Application Management** > **Application List**.

Step 2 Click the application created (for example, **weathermap**). The **Overview** page is displayed.

Step 3 Click the link next to **External Access Address** of the **weathermapweb** application component.



weathermap

□ All | Upgrade Component | **Environment** | test-env

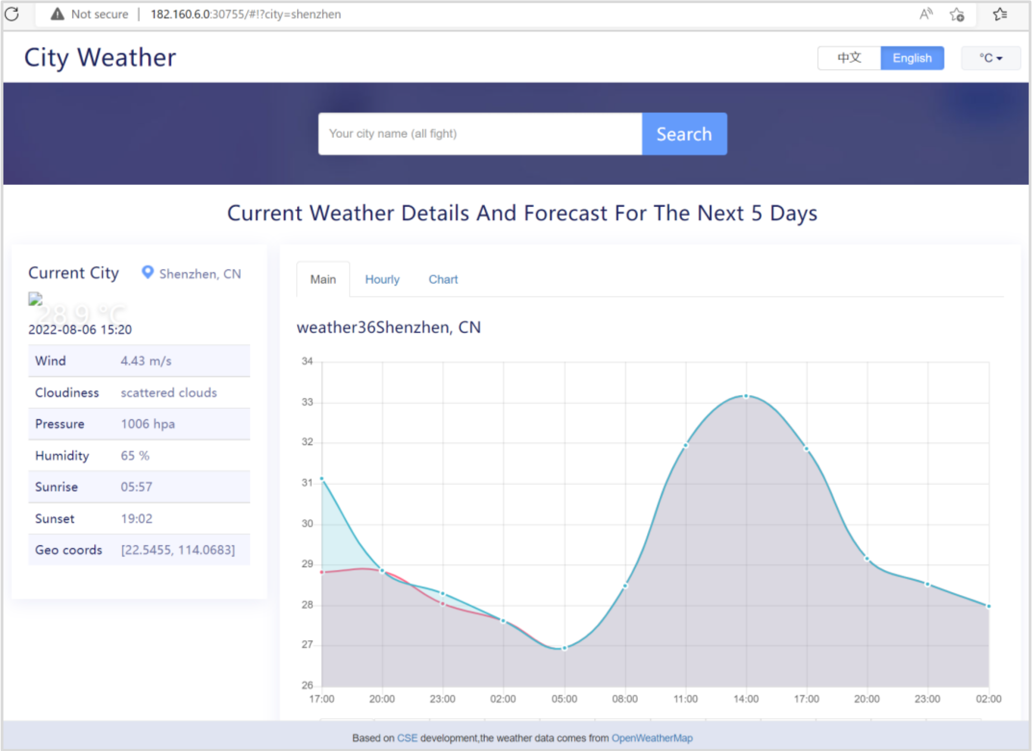
□
weathermapweb
test-env Version 1.0.0

Status	Running
Type	MicroService
Instance Quantity (Normal/Total)	1/1
External Access Address	182.160.6.0:30755
Deployed	[redacted] GMT+08:00

Figure 7-89

Step 4 If the information shown in the following figure is displayed, the weather forecast application is successfully deployed.

When you access the application for the first time, it takes some time for the weather system to be ready. If the preceding page is not displayed, refresh the page.



Not secure | 182.160.6.0:30755/#!?city=shenzhen

City Weather

Current Weather Details And Forecast For The Next 5 Days

Current City Shenzhen, CN
2022-08-06 15:20

Wind	4.43 m/s
Cloudiness	scattered clouds
Pressure	1006 hpa
Humidity	65 %
Sunrise	05:57
Sunset	19:02
Geo coords	[22.5455, 114.0683]

Based on CSE development,the weather data comes from OpenWeatherMap

Figure 7-90

7.4 Clearing Resources

Step 1 Delete a microservice.

- Log in to ServiceStage, choose **Application Management** > **Application List**, and click application **weathermap**. The **Overview** page is displayed.
- On the **Environment View** tab page, select the component and choose **Operation** > **Delete**.
- Back to the **Application List** and click **Delete** in the **Operation** column of application **weathermap**.

Step 2 Delete the build job.

Log in to ServiceStage, choose **Continuous Delivery** > **Build**, select a build job, and choose **More** > **Delete**.

Step 3 Delete repository authorization.

Log in to ServiceStage, choose **Continuous Delivery** > **Repository Authorization**, select an authorization, and choose **More** > **Delete**.

Step 4 Deletes an organization.

Log in to ServiceStage, choose **Software Center** > **Organization**, select an organization, and click **Delete**.

Step 5 Delete an environment.

Log in to ServiceStage, choose **Environment Management**, select an environment, and click **Delete**.

Step 6 Delete a CCE node.

Choose **Cloud Container Engine** from **Service List**. In the navigation pane on the left, choose **Nodes**. In the node list, select the node and choose **More** > **Delete**.

Step 7 Delete the subnet and VPC.

- In the service list, choose **Virtual Private Cloud** under **Networking**. On the network console, choose **Subnets**. In the subnet list, locate the subnet created in this exercise and click **Delete** in the **Operation** column.
- Choose **Virtual Private Cloud** in the navigation pane on the left. In the VPC list, locate the VPC created in this exercise and click **Delete** in the **Operation** column.

7.5 Quiz

Question: After an application component is deployed, the status is **Not ready**, indicating that the application component fails to be deployed. How do I check the cause of this failure?

Answer: Log in to ServiceStage, choose **Application Management** > **Application List**, and click the application. On the **Overview** page that is displayed, select and click the abnormal component. Then, choose **Instance List**, click the arrow button before the instance name, and click **Event**. In the event list, view the event description to determine the cause of the application component deployment failure.

8 Cloud O&M Design

8.1 Introduction

8.1.1 About This Exercise

This exercise consists of three parts:

1. Cloud Eye: View metrics on Cloud Eye and configure server, site, and event monitoring.
2. AOM: Connect an ECS to AOM and configure threshold rules, log dump, and log analysis.

This exercise uses the CN-Hong Kong region as an example. Trainees can select other regions as required.

8.1.2 Objectives

Understand the configuration and usage principles of Cloud Eye.

Master the methods and principles of alarm monitoring and log collection/analysis using AOM.

8.1.3 Related Software

Tomcat is an open-source web application server. It is lightweight and commonly used in small- or medium-sized systems or in scenarios with a small number of concurrent users. It is preferred for Java Server Pages (JSP) program development and commissioning.

Java Development Kit (JDK) is a Java development tool package. It is the core of Java, including the Java runtime environment, Java tools (JAVAC/JAVA/JDB), and basic Java class libraries.

8.2 Procedure

8.2.1 Preparations

8.2.1.1 Creating a VPC by Referring to the Preceding Exercise

Basic settings:

- **Region**: **CN-Hong Kong**
- **Name**: **vpc-1**
- **IPv4 CIDR Block**: **192.168.0.0/16**

Default subnet:

- **Name**: **vpc-1-subnet**
- **IPv4 CIDR Block**: **192.168.1.0/24**

8.2.1.2 Creating an ECS by Referring to the Preceding Exercise

Note: This ECS is used only for O&M tests.

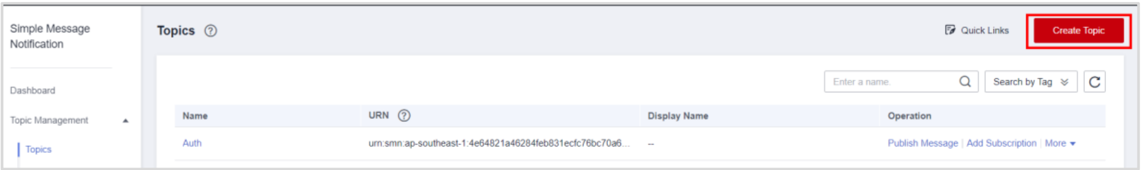
Configure the **test** ECS as follows:

- **Billing Mode**: **Pay-per-use**
- **Region**: **CN-Hong Kong**
- **AZ**: **Random**
- **CPU Architecture**: **x86**
- **Specifications**: **1 vCPUs | 2 GiB**
- **Image**: **Public image** | **CentOS 7.6 64 bit**
- **Host Security**: **Enable** | **Basic (free)**
- **System Disk**: **40 GiB**
- **Network**: **vpc-1** | **vpc-1-subnet** | **Automatically assign IP address**
- **Security Group**: **default**
- **EIP**: **Auto assign**
- **EIP Type**: **Dynamic BGP**
- **Billed By**: **Traffic**
- **Bandwidth Size**: **10 Mbit/s**
- **ECS Name**: **test**
- **Password**: custom password of the **root** user

8.2.1.3 Creating an SMN Topic

Step 1 In the service list, select **Simple Message Notification**.

Step 2 In the navigation pane, choose **Topic Management** > **Topics**. Then, click **Create Topic** in the upper right corner.

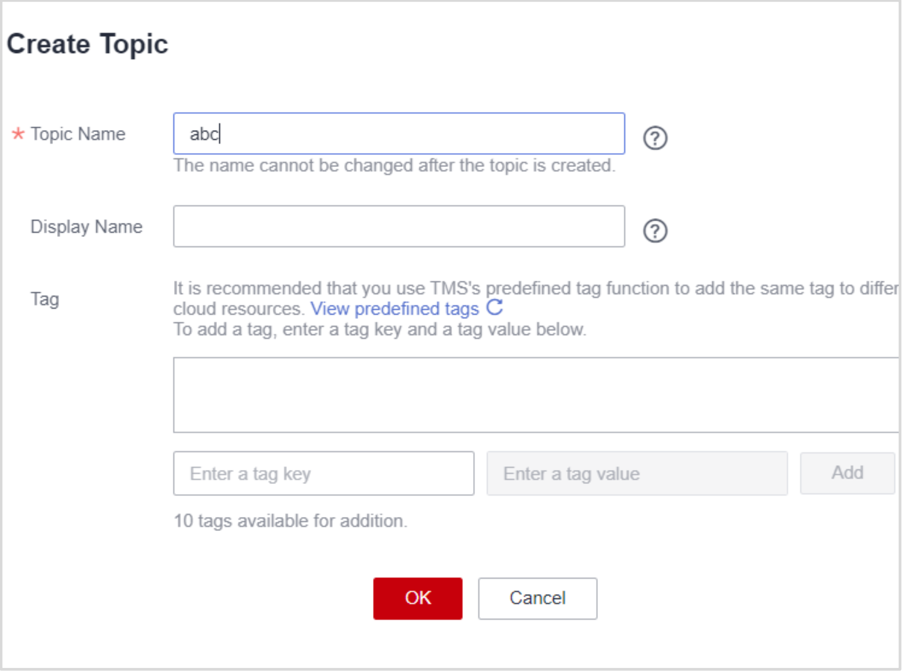


Name	URN	Display Name	Operation
Auth	urn:smn:ap-southeast-1:4e64821a46284feb831ecfc76bc70a6...	--	Publish Message | Add Subscription | More

Figure 8-1

Step 3 Set a topic name and click **OK**.

Note: This topic is shared by multiple services. Trainees can customize their own topic name. **abc** is used as an example here.



Create Topic

* Topic Name: abc

The name cannot be changed after the topic is created.

Display Name:

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to differ cloud resources. View predefined tags

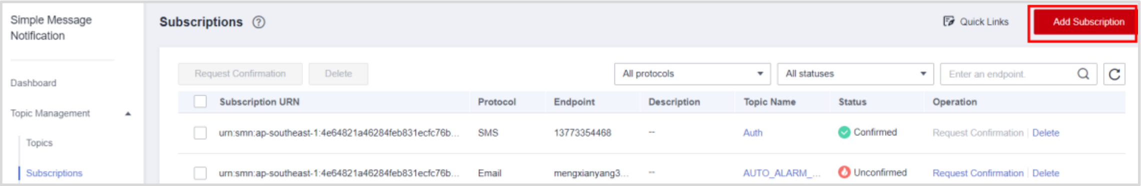
To add a tag, enter a tag key and a tag value below.

10 tags available for addition.

Figure 8-2

Step 4 Add a subscription.

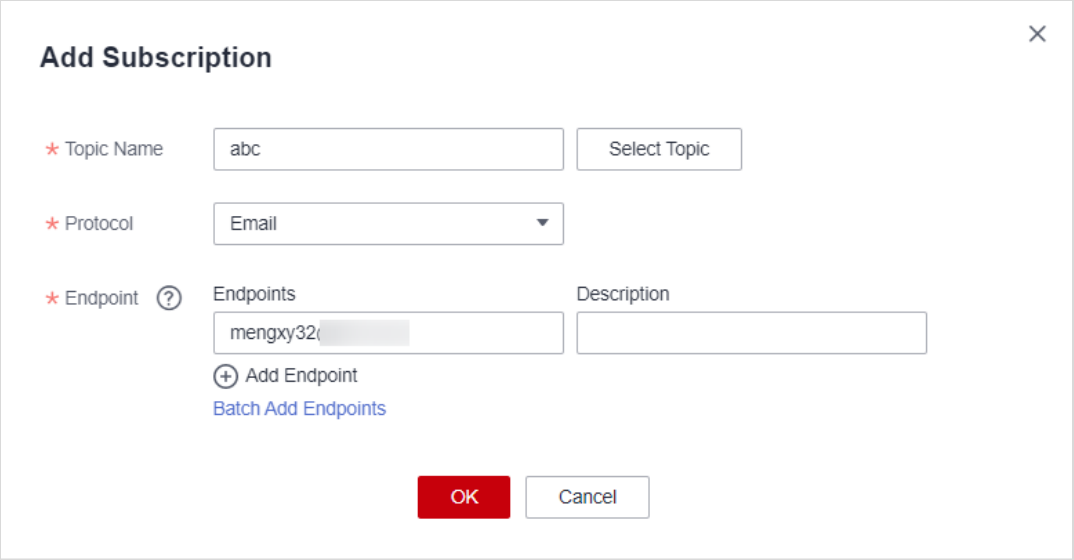
- In the navigation pane, choose **Subscriptions**. Then, click **Add Subscription** in the upper right corner.



Subscription URN	Protocol	Endpoint	Description	Topic Name	Status	Operation
urn:smn:ap-southeast-1:4e64821a46284feb831ecfc76b...	SMS	13773354468	--	Auth	Confirmed	Request Confirmation | Delete
urn:smn:ap-southeast-1:4e64821a46284feb831ecfc76b...	Email	mengxianyang3...	--	AUTO_ALARM_...	Unconfirmed	Request Confirmation | Delete

Figure 8-3

- Set **Topic Name** to **abc**, set **Protocol** to **Email** or **SMS** (**Email** is used as an example here), specify **Endpoint**, and click **OK**.

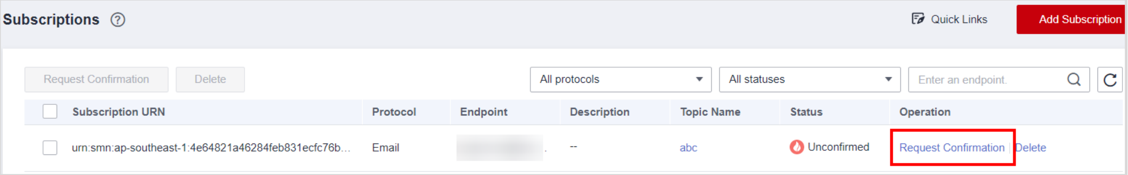


Add Subscription

* Topic Name	abc	Select Topic
* Protocol	Email	
* Endpoint	Endpoints: mengxy32([redacted]	Description:

Figure 8-4

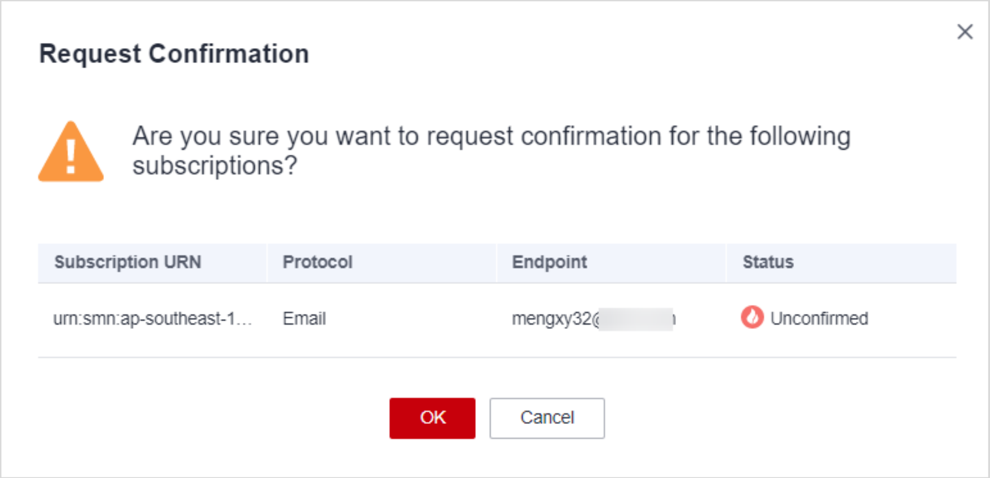
Step 5 In the subscription list, view the created subscription and click **Request Confirmation**.



□	Subscription URN	Protocol	Endpoint	Description	Topic Name	Status	Operation
□	urn:smn:ap-southeast-1:4e64821a46284feb831ecfc76b...	Email	[redacted]	--	abc	Unconfirmed	Request Confirmation | Delete

Figure 8-5

Step 6 In the displayed dialog box, click **OK**.



Request Confirmation

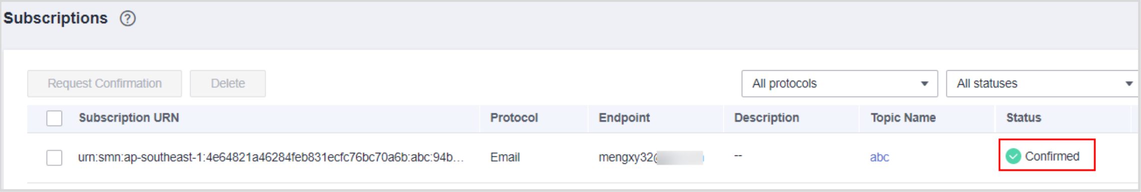
Are you sure you want to request confirmation for the following subscriptions?

Subscription URN	Protocol	Endpoint	Status
urn:smn:ap-southeast-1...	Email	mengxy32([redacted]	Unconfirmed

Figure 8-6

Step 7 Check the subscription email and confirm the subscription.

Step 8 Return to the subscription list and check whether the subscription status changes to **Confirmed**. If yes, the subscription is successfully added.



Subscriptions

Request Confirmation | Delete | All protocols | All statuses

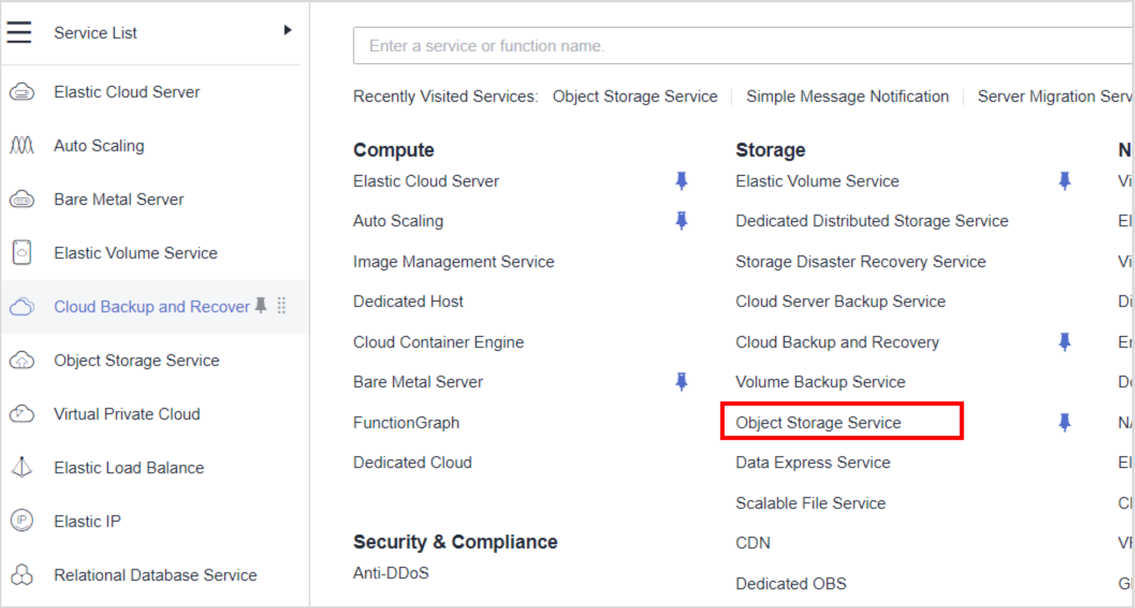
□	Subscription URN	Protocol	Endpoint	Description	Topic Name	Status
□	urn:smn:ap-southeast-1:4e64821a46284feb831ecfc76bc70a6b:abc:94b...	Email	mengxy32[redacted]	--	abc	Confirmed

Figure 8-7

8.2.1.4 Creating an OBS Bucket

Step 1 In the service list, choose **Object Storage Service**.

Note: This bucket is used for dumping AOM logs.



Service List

- Elastic Cloud Server
- Auto Scaling
- Bare Metal Server
- Elastic Volume Service
- Cloud Backup and Recover
- Object Storage Service
- Virtual Private Cloud
- Elastic Load Balance
- Elastic IP
- Relational Database Service

Enter a service or function name.

Recently Visited Services: Object Storage Service | Simple Message Notification | Server Migration Serv

Compute

Elastic Cloud Server

Auto Scaling

Image Management Service

Dedicated Host

Cloud Container Engine

Bare Metal Server

FunctionGraph

Dedicated Cloud

Security & Compliance

Anti-DDoS

Storage

Elastic Volume Service

Dedicated Distributed Storage Service

Storage Disaster Recovery Service

Cloud Server Backup Service

Cloud Backup and Recovery

Volume Backup Service

Object Storage Service

Data Express Service

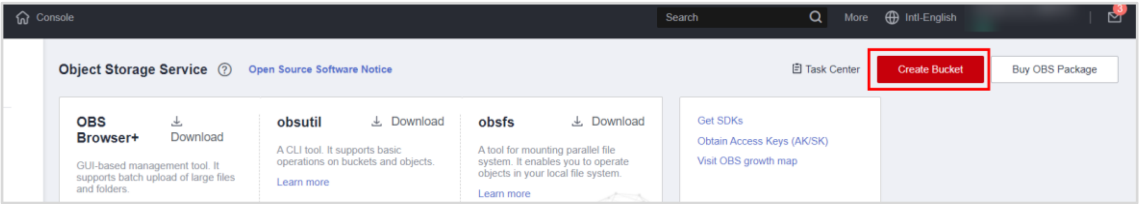
Scalable File Service

CDN

Dedicated OBS

Figure 8-8

Step 2 Click **Create Bucket** in the upper right corner.



[redacted]

Object Storage Service | Open Source Software Notice | Task Center | Create Bucket | Buy OBS Package

OBS Browser+ Download
GUI-based management tool. It supports batch upload of large files and folders.

obsutil Download
A CLI tool. It supports basic operations on buckets and objects.
Learn more

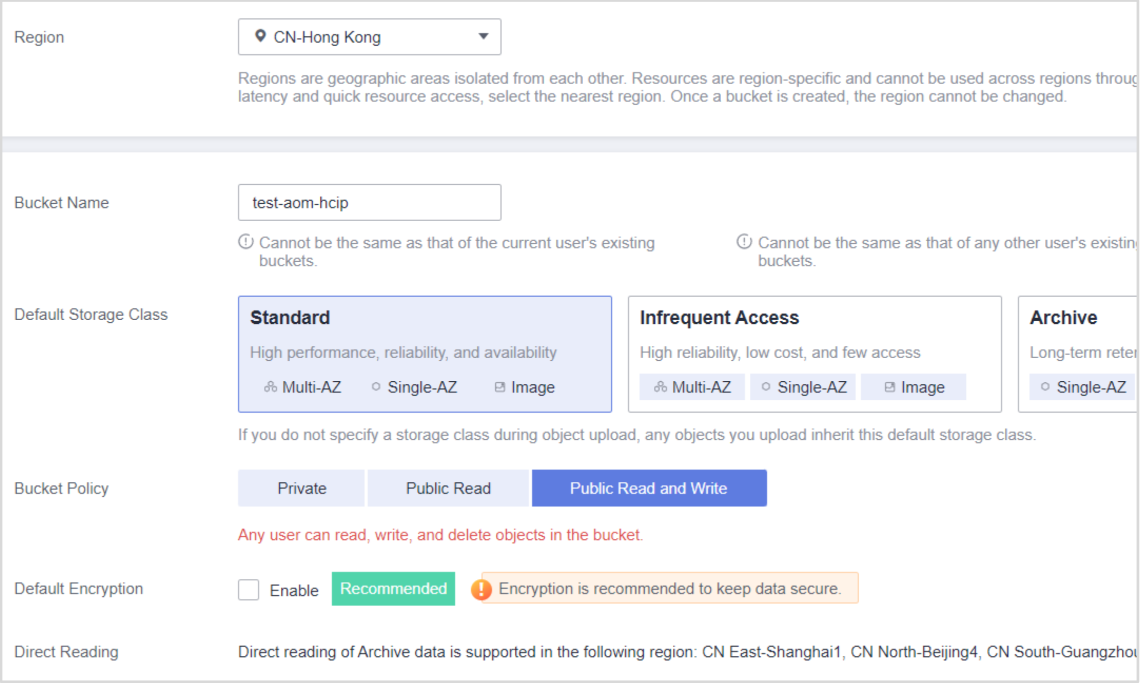
obsfs Download
A tool for mounting parallel file system. It enables you to operate objects in your local file system.
Learn more

Get SDKs
Obtain Access Keys (AK/SK)
Visit OBS growth map

Figure 8-9

Step 3 Create an OBS bucket:

- **Region**: **CN-Hong Kong**
- **Bucket Name**: **test-aom-hcip**（user-defined）
- **Default Storage Class:** Standard
- **Bucket Policy**: **Public Read and Write**
- Retain the default settings for other parameters.



Region: CN-Hong Kong

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions throug latency and quick resource access, select the nearest region. Once a bucket is created, the region cannot be changed.

Bucket Name: test-aom-hcip

ⓘ Cannot be the same as that of the current user's existing buckets.

ⓘ Cannot be the same as that of any other user's existin buckets.

Default Storage Class:

- **Standard** – High performance, reliability, and availability – Multi-AZ, Single-AZ, Image
- **Infrequent Access** – High reliability, low cost, and few access – Multi-AZ, Single-AZ, Image
- **Archive** – Long-term reter – Single-AZ

If you do not specify a storage class during object upload, any objects you upload inherit this default storage class.

Bucket Policy: Private | Public Read | Public Read and Write

Any user can read, write, and delete objects in the bucket.

Default Encryption: □ Enable Recommended ! Encryption is recommended to keep data secure.

Direct Reading: Direct reading of Archive data is supported in the following region: CN East-Shanghai1, CN North-Beijing4, CN South-Guangzhou

Figure 8-10

8.2.2 Cloud Eye

Cloud Eye is a multi-dimensional monitoring service. With Cloud Eye, you can view the resource usage and service running status in the cloud, and respond to exceptions in a timely manner to ensure smooth service running.

After enabling a cloud service supported by Cloud Eye, you can view the running status of the cloud service and the usage of each metric, and create alarm rules for metrics on the Cloud Eye console.

You can monitor cloud service metrics (such as CPU/memory/disk usage) to ensure smooth service running and prevent service interruption caused by overuse of resources.

You can query system events and custom events reported to Cloud Eye through APIs. You can also create alarm rules for both system events and custom events. When specific events occur, Cloud Eye generates alarms for them.

8.2.2.1 Metric Monitoring

Step 1 Log in to the Huawei Cloud console and choose **Cloud Eye** from the service list.

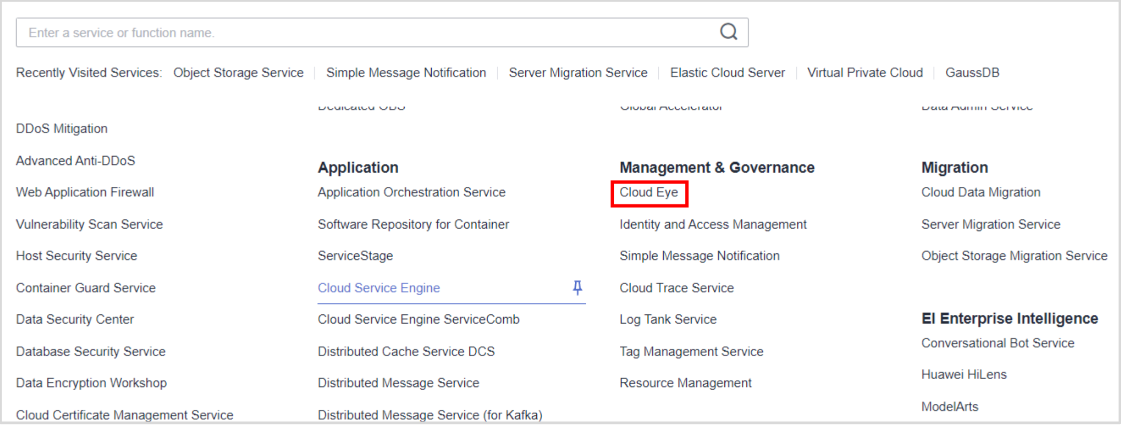
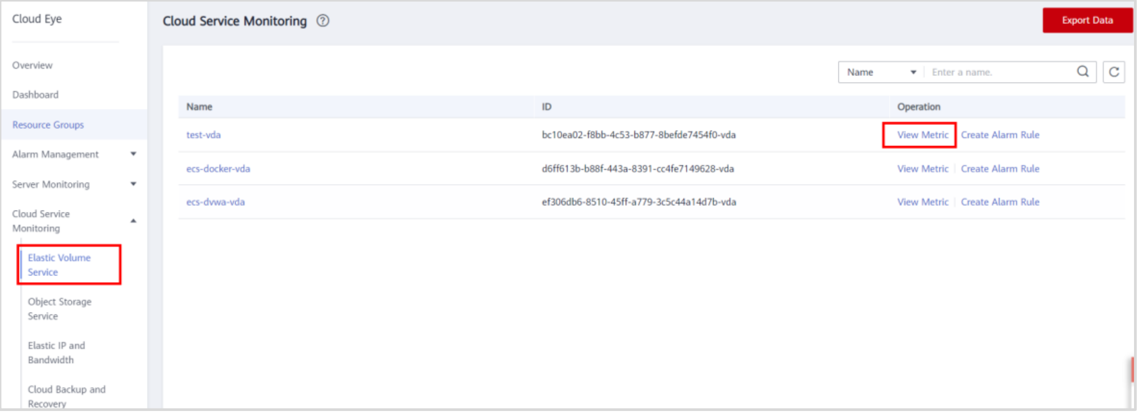

Enter a service or function name.
Recently Visited Services: Object Storage Service | Simple Message Notification | Server Migration Service | Elastic Cloud Server | Virtual Private Cloud | GaussDB
DDoS Mitigation
Advanced Anti-DDoS
Web Application Firewall
Vulnerability Scan Service
Host Security Service
Container Guard Service
Data Security Center
Database Security Service
Data Encryption Workshop
Cloud Certificate Management Service
Application
Application Orchestration Service
Software Repository for Container
ServiceStage
Cloud Service Engine
Cloud Service Engine ServiceComb
Distributed Cache Service DCS
Distributed Message Service
Distributed Message Service (for Kafka)
Management & Governance
Cloud Eye
Identity and Access Management
Simple Message Notification
Cloud Trace Service
Log Tank Service
Tag Management Service
Resource Management
Migration
Cloud Data Migration
Server Migration Service
Object Storage Migration Service
EI Enterprise Intelligence
Conversational Bot Service
Huawei HiLens
ModelArts

Figure 8-11

Step 2 In the navigation pane, choose **Cloud Service Monitoring** > **Elastic Volume Service**, locate the target resource, and click **View Metric** in the **Operation** column. The metric monitoring page is displayed.

Wait for 7 to 8 minutes to view metrics after an ECS is deployed.



Name	ID	Operation
test-vda	bc10ea02-f8bb-4c53-b877-8befde7454f0-vda	View Metric Create Alarm Rule
ecs-docker-vda	d6ff613b-b88f-443a-8391-cc4fe7149628-vda	View Metric | Create Alarm Rule
ecs-dvwa-vda	ef306db6-8510-45ff-a779-3c5c44a14d7b-vda	View Metric | Create Alarm Rule

Figure 8-12

You can view graphs based on raw data collected in the last **1h**, **3h**, **12h**, **1d**, and **7d**. In the upper right corner of the graph, the maximum and minimum values of the metric in the corresponding time period are dynamically displayed. You can also enable **Auto Refresh** to view the data refreshed every minute.

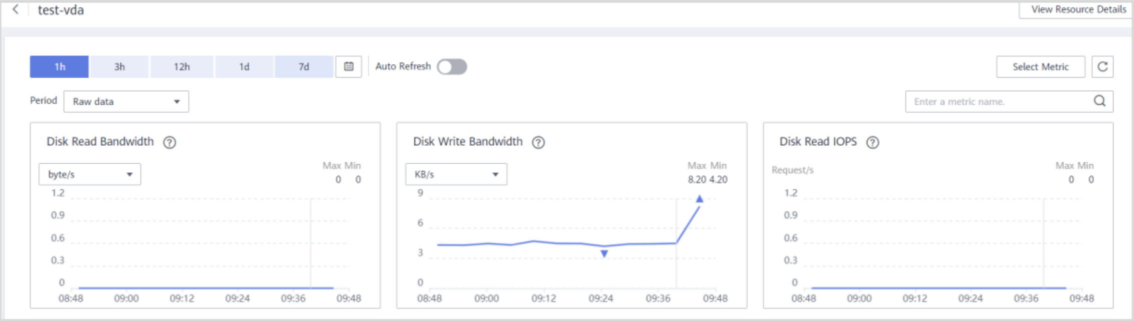
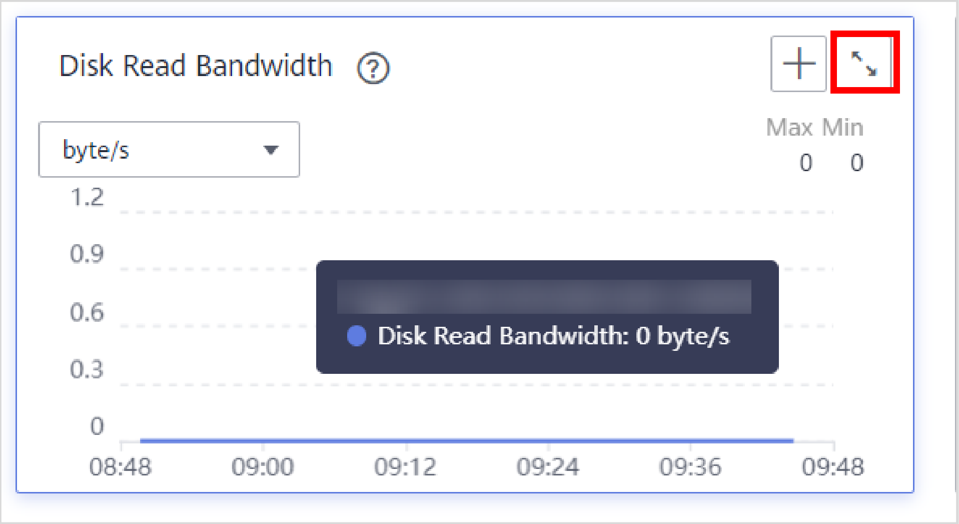


Figure 8-13

Step 3 Click **Select Metric** in the upper right corner of the page.

On the displayed page, select target metrics, and drag and drop them at desired locations for monitoring.

Step 4 Hover over a metric and click ⤡ in the upper right corner of the metric graph. The monitoring details page is displayed.



Disk Read Bandwidth ?

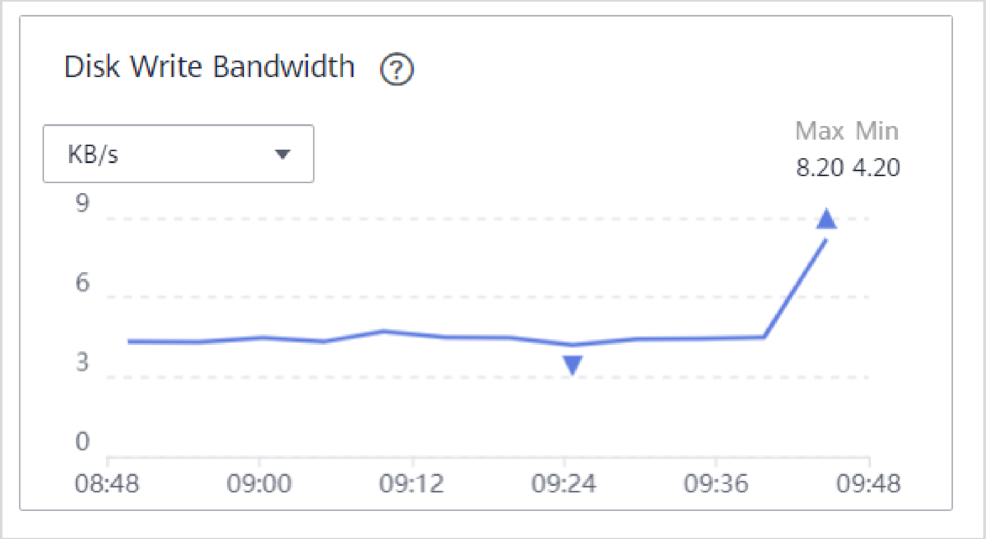
byte/s

Max Min
0 0

Disk Read Bandwidth: 0 byte/s

Figure 8-14

You can view the metric monitoring details in a longer time range. In the upper left corner, you can select **1h**, **3h**, **12h**, **1d**, **7d**, or **30d** to view monitoring data. You can also customize a time range (up to six months).



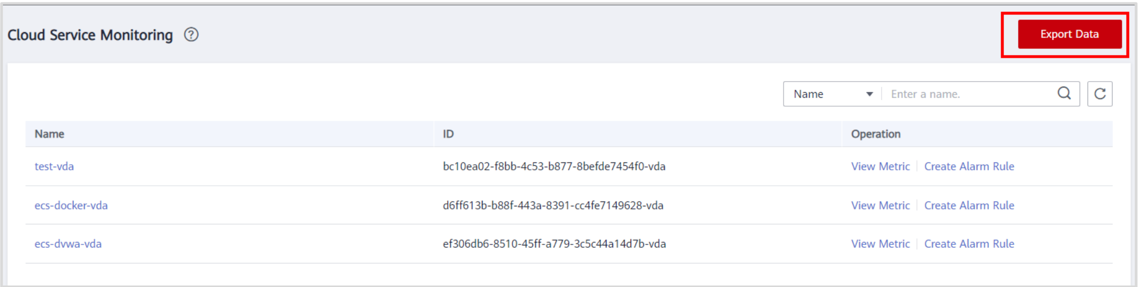
Disk Write Bandwidth ?

KB/s

Max Min
8.20 4.20

Figure 8-15

To export data, click **Export Data** on the **Cloud Service Monitoring** page, set parameters as prompted, and click **Export**.



Name	ID	Operation
test-vda	bc10ea02-f8bb-4c53-b877-8befde7454f0-vda	View Metric | Create Alarm Rule
ecs-docker-vda	d6ff613b-b88f-443a-8391-cc4fe7149628-vda	View Metric | Create Alarm Rule
ecs-dvwa-vda	ef306db6-8510-45ff-a779-3c5c44a14d7b-vda	View Metric | Create Alarm Rule

Figure 8-16

8.2.2.2 Server Monitoring

Step 1 Log in to the Huawei Cloud console and choose **Cloud Eye** from the service list.

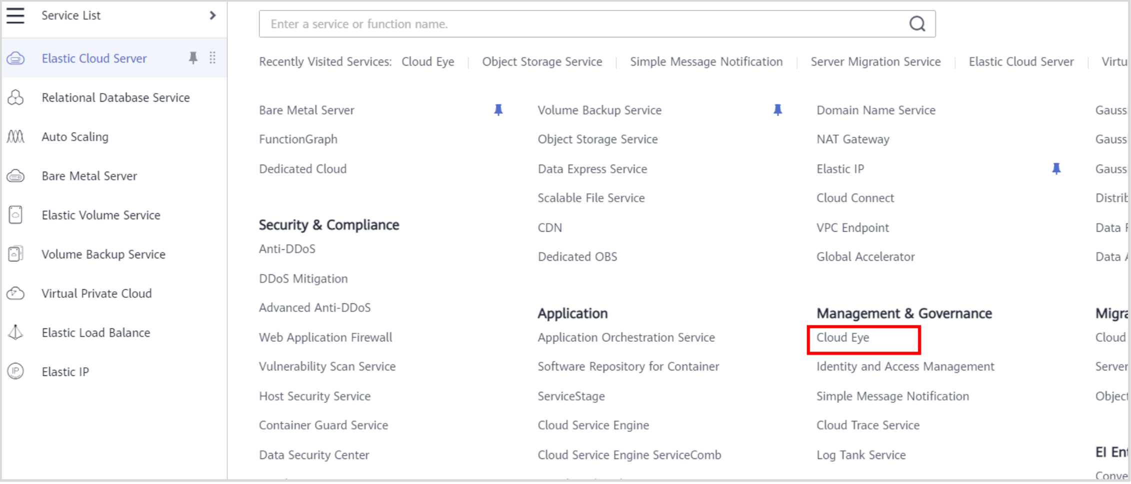
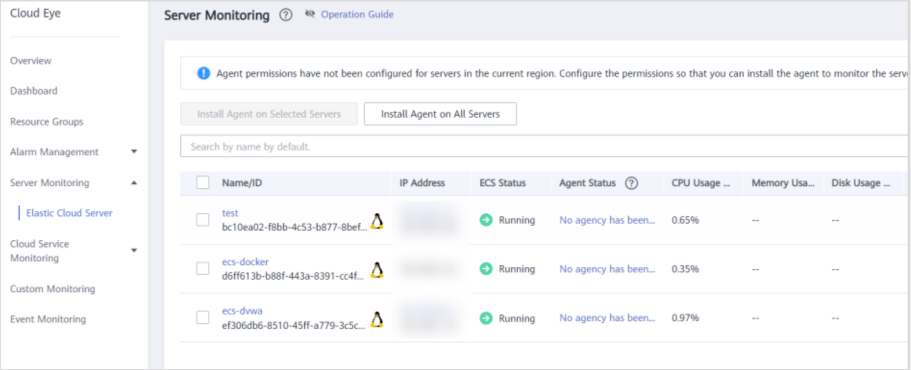


Figure 8-17

Step 2 In the navigation pane, choose **Server Monitoring**.

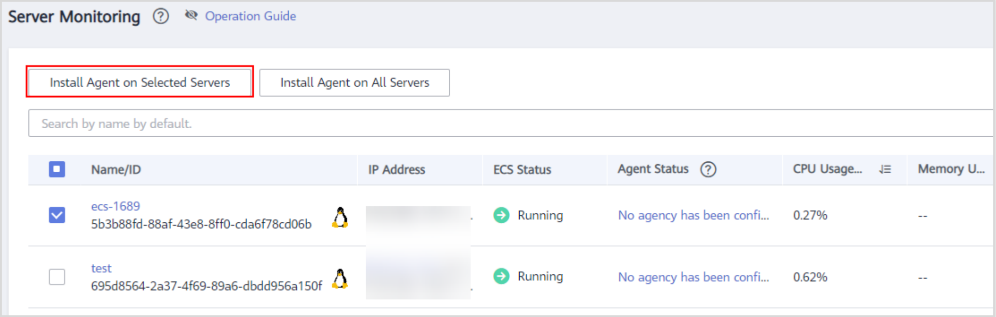


Agent permissions have not been configured for servers in the current region. Configure the permissions so that you can install the agent to monitor the serv

□	Name/ID	IP Address	ECS Status	Agent Status	CPU Usage ...	Memory Usa...	Disk Usage ...
□	test bc10ea02-f8bb-4c53-b877-8bef...	[redacted]	Running	No agency has been...	0.65%	--	--
□	ecs-docker d6ff613b-b88f-443a-8391-cc4f...	[redacted]	Running	No agency has been...	0.35%	--	--
□	ecs-dvwa ef306db6-8510-45ff-a779-3c5c...	[redacted]	Running	No agency has been...	0.97%	--	--

Figure 8-18

Step 3 （Optional）On the displayed page, select the ECS where the agent is to be installed. (If there are ECSs on which the agent is not installed) 1. Install the agent in one click. If the agent has been installed, skip this step.



Server Monitoring ⓘ Operation Guide

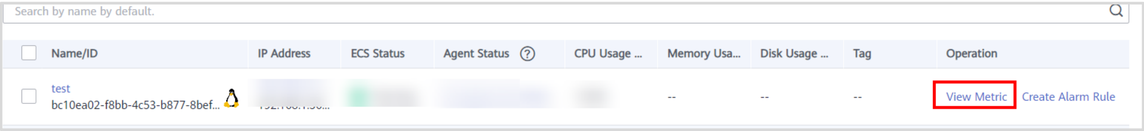
Install Agent on Selected Servers | Install Agent on All Servers

Search by name by default.

☑	Name/ID	IP Address	ECS Status	Agent Status ⓘ	CPU Usage...	Memory U...
☑	ecs-1689 5b3b88fd-88af-43e8-8ff0-cda6f78cd06b	[redacted]	Running	No agency has been confi...	0.27%	--
□	test 695d8564-2a37-4f69-89a6-dbdd956a150f	[redacted]	Running	No agency has been confi...	0.62%	--

Figure 8-19

Step 4 Locate the target ECS and click **View Metric** in the **Operation** column to view its monitoring data.



Search by name by default.

□	Name/ID	IP Address	ECS Status	Agent Status ⓘ	CPU Usage ...	Memory Usa...	Disk Usage ...	Tag	Operation
□	test bc10ea02-f8bb-4c53-b877-8bef...	[redacted]	[redacted]	[redacted]	[redacted]	--	--	--	View Metric Create Alarm Rule

Figure 8-20

OS Monitoring, **Basic Monitoring**, and **Process Monitoring** are available.

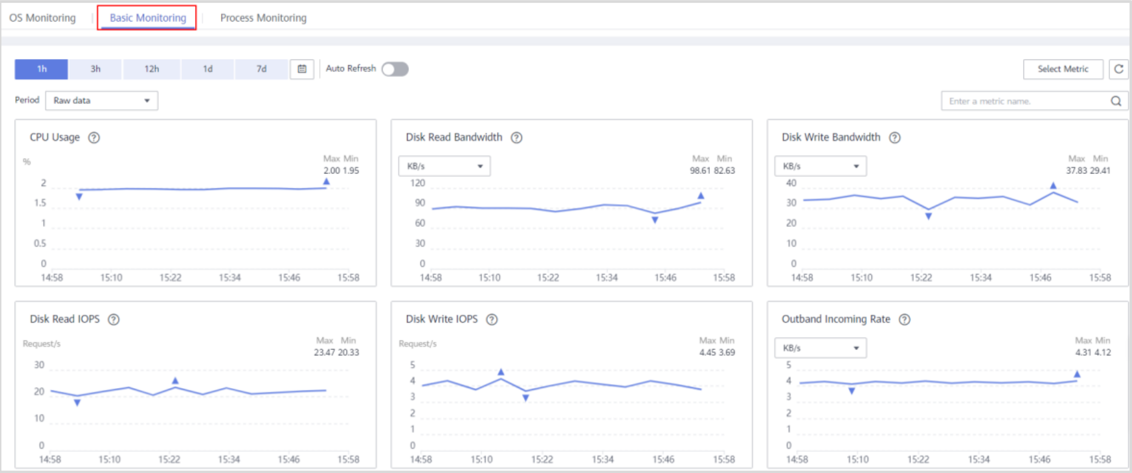
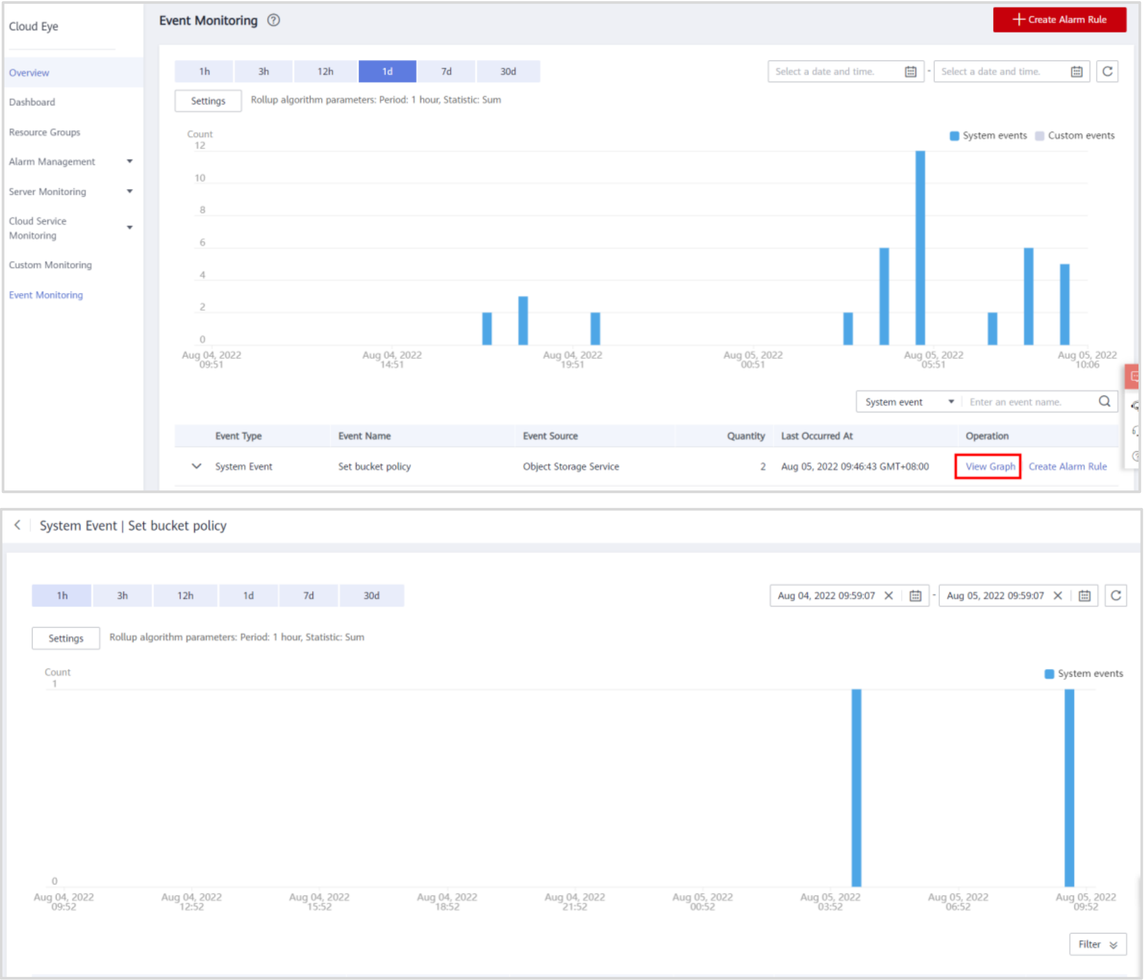


Figure 8-21

8.2.2.3 Event Monitoring

Step 1 In the navigation pane, choose **Event Monitoring**. All system events and custom events generated in the last 24 hours are displayed by default. Locate the target event and click **View Graph** in the **Operation** column to view its graph.



Event Type	Event Name	Event Source	Quantity	Last Occurred At	Operation
System Event	Set bucket policy	Object Storage Service	2	Aug 05, 2022 09:46:43 GMT+08:00	View Graph Create Alarm Rule

Figure 8-22

Step 2 On the **Event Monitoring** page, click **Create Alarm Rule** in the upper right corner.

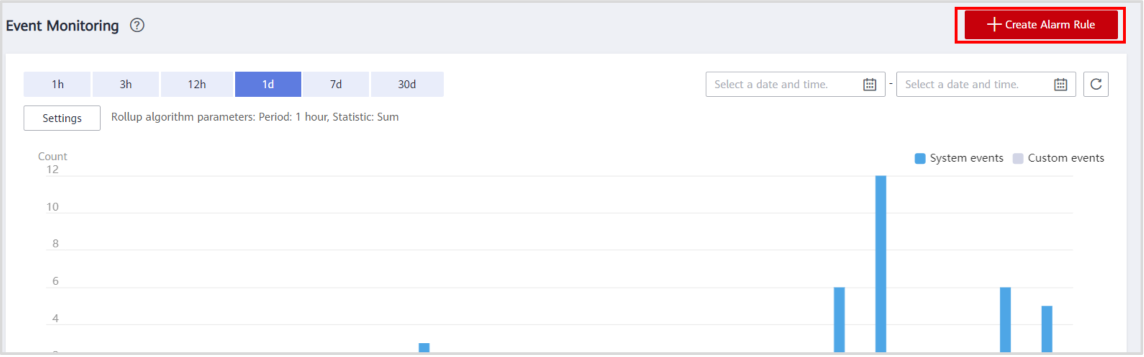
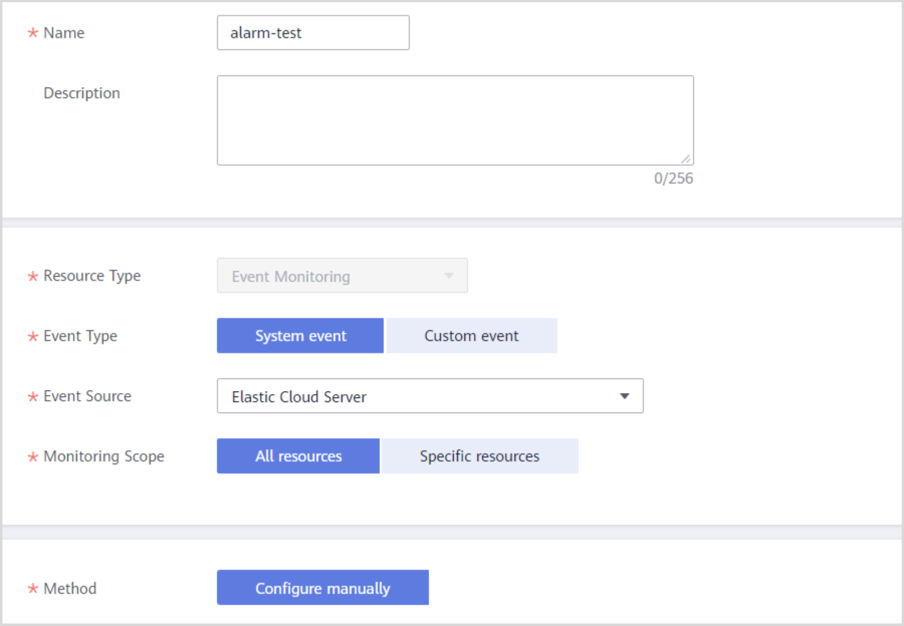


Figure 8-23

Step 3 Configure the alarm rule name, policy, notification, and other parameters as prompted.

- Name: alarm-test
- Event Type: System event
- Event Source: Elastic Cloud Server

- **Monitoring Scope**: **All resources**
- **Method**: **Configure manually**
- **Alarm Policy**: Retain the default setting.



* Name: alarm-test

Description:

0/256

* Resource Type: Event Monitoring

* Event Type: **System event** | Custom event

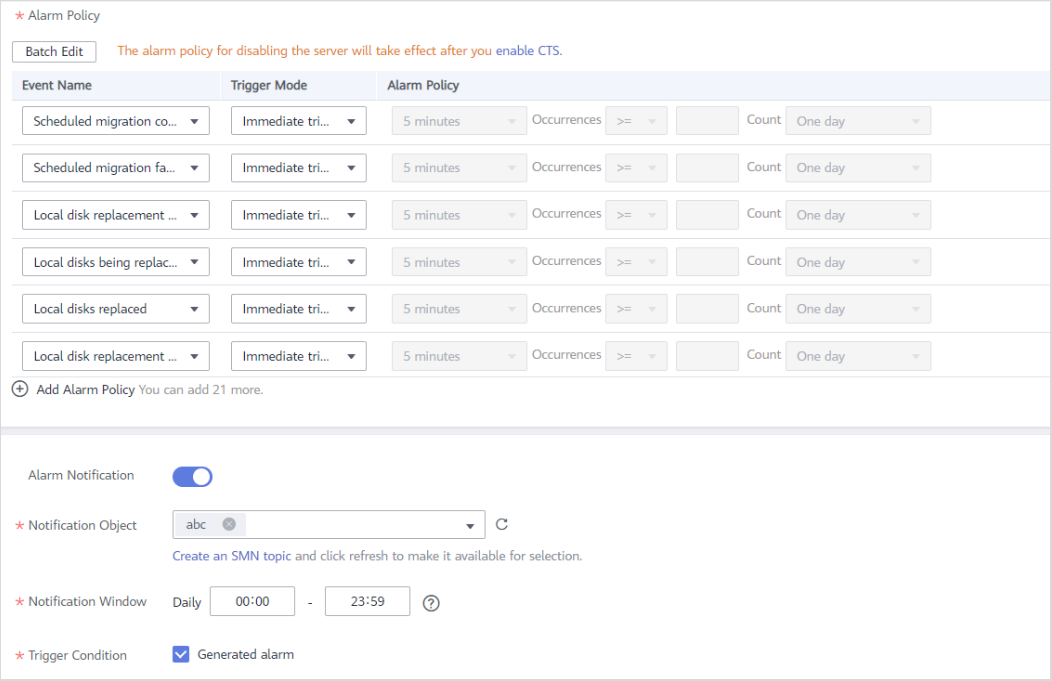
* Event Source: Elastic Cloud Server

* Monitoring Scope: **All resources** | Specific resources

* Method: **Configure manually**

Figure 8-24

- **Notification Object**: **abc** (created during preparation)
- Retain the default settings for other parameters.



* Alarm Policy

Batch Edit   The alarm policy for disabling the server will take effect after you enable CTS.

Event Name	Trigger Mode	Alarm Policy						
Scheduled migration co...	Immediate tri...	5 minutes	Occurrences	>=		Count	One day
Scheduled migration fa...	Immediate tri...	5 minutes	Occurrences	>=		Count	One day
Local disk replacement ...	Immediate tri...	5 minutes	Occurrences	>=		Count	One day
Local disks being replac...	Immediate tri...	5 minutes	Occurrences	>=		Count	One day
Local disks replaced	Immediate tri...	5 minutes	Occurrences	>=		Count	One day
Local disk replacement ...	Immediate tri...	5 minutes	Occurrences	>=		Count	One day

⊕ Add Alarm Policy You can add 21 more.

Alarm Notification: ●

* Notification Object: abc

Create an SMN topic and click refresh to make it available for selection.

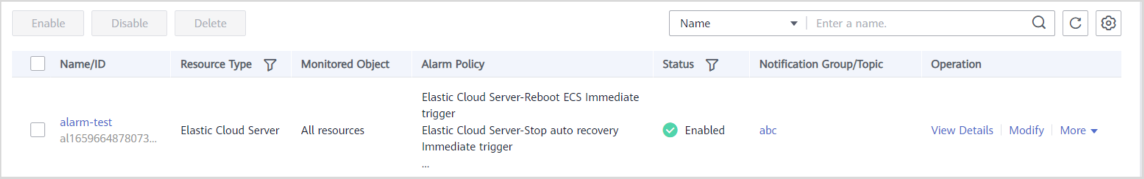
* Notification Window: Daily 00:00 - 23:59

* Trigger Condition: ☑ Generated alarm

Figure 8-25

After you create the alarm rule, if the metric data triggers the present alarm policy, Cloud Eye will immediately send SMN notifications.

Step 4 Check whether the status of the alarm rule is **Enabled**. If yes, the alarm rule is successfully created.



Name/ID	Resource Type	Monitored Object	Alarm Policy	Status	Notification Group/Topic	Operation
alarm-test al1659664878073...	Elastic Cloud Server	All resources	Elastic Cloud Server-Reboot ECS Immediate trigger Elastic Cloud Server-Stop auto recovery Immediate trigger ...	Enabled	abc	View Details | Modify | More

Figure 8-26

8.2.3 AOM

AOM is a one-stop, multidimensional O&M management platform for cloud applications. It monitors applications and related cloud resources in real time, analyzes application health status, and provides flexible data visualization functions. It helps you detect faults in a timely manner and monitor running status of applications, services, and other resources in real time.

By setting alarm rules, you can learn about the resource usage, trend, and alarms of hosts in a timely manner. Administrators can quickly respond to exceptions to ensure smooth host running.

AOM also provides powerful log management capabilities. You can quickly search for required logs among a large quantity of logs, and dump logs to buckets for long-term storage. You can also set statistical rules so that AOM periodically counts keywords and generates metric data for real-time system performance and service monitoring.

8.2.3.1 Alarm Monitoring

Step 1 In the service list, choose **Application Operations Management**.

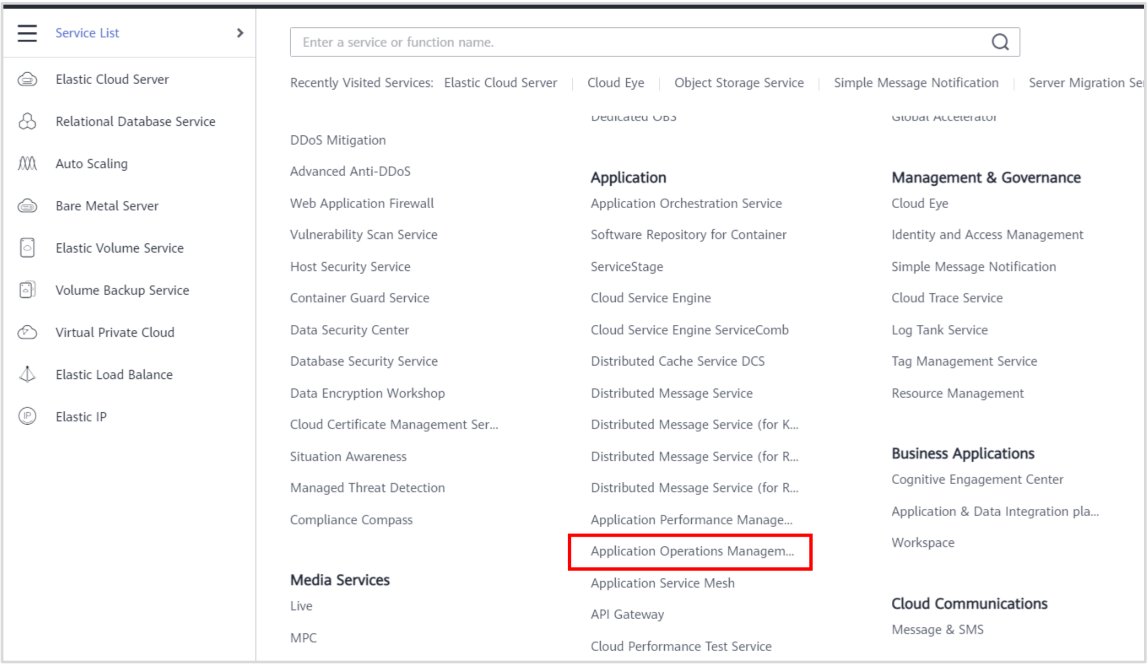
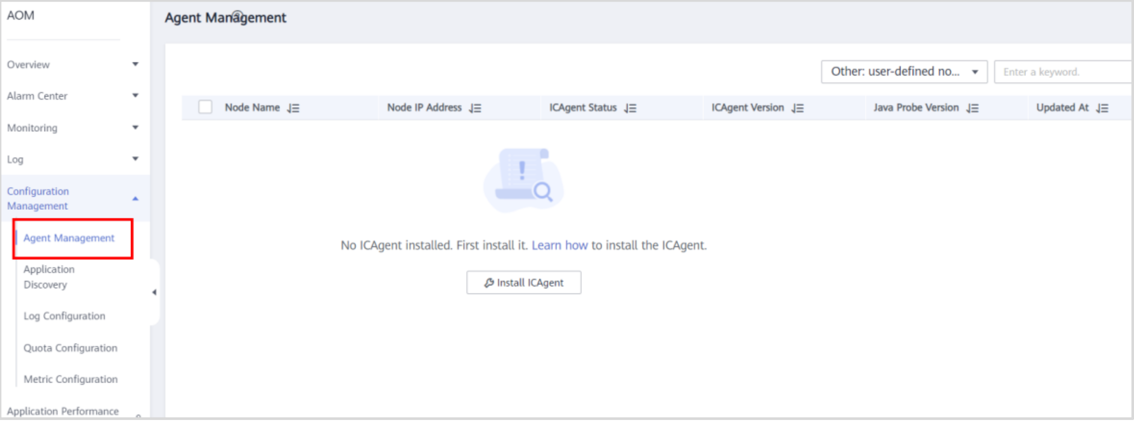

Service List
Elastic Cloud Server
Relational Database Service
Auto Scaling
Bare Metal Server
Elastic Volume Service
Volume Backup Service
Virtual Private Cloud
Elastic Load Balance
Elastic IP
Enter a service or function name.
Recently Visited Services: Elastic Cloud Server | Cloud Eye | Object Storage Service | Simple Message Notification | Server Migration Se
DDoS Mitigation
Advanced Anti-DDoS
Web Application Firewall
Vulnerability Scan Service
Host Security Service
Container Guard Service
Data Security Center
Database Security Service
Data Encryption Workshop
Cloud Certificate Management Ser...
Situation Awareness
Managed Threat Detection
Compliance Compass
Media Services
Live
MPC
Application
Application Orchestration Service
Software Repository for Container
ServiceStage
Cloud Service Engine
Cloud Service Engine ServiceComb
Distributed Cache Service DCS
Distributed Message Service
Distributed Message Service (for K...
Distributed Message Service (for R...
Distributed Message Service (for R...
Application Performance Manage...
Application Operations Managem...
Application Service Mesh
API Gateway
Cloud Performance Test Service
Management & Governance
Cloud Eye
Identity and Access Management
Simple Message Notification
Cloud Trace Service
Log Tank Service
Tag Management Service
Resource Management
Business Applications
Cognitive Engagement Center
Application & Data Integration pla...
Workspace
Cloud Communications
Message & SMS

Figure 8-27

Step 2 In the navigation pane, choose **Configuration Management** > **Agent Management**. On the displayed page, click **Install ICAgent**.

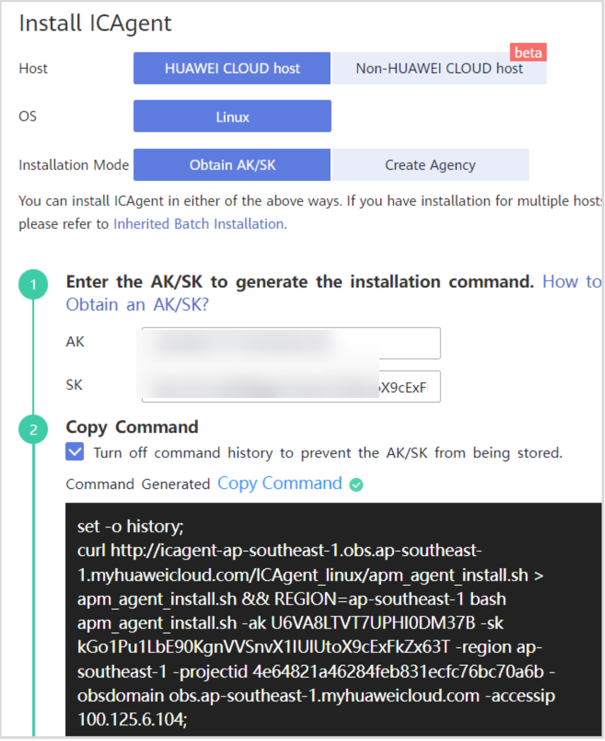
Note: ICAgents collect metrics, logs, and application performance data. For hosts purchased on the ECS or BMS console, manually install ICAgents.



No ICAgent installed. First install it. Learn how to install the ICAgent.

Figure 8-28

Step 3 On the displayed page, enter the AK/SK downloaded in section 7.2.1.1 and copy the installation command.



You can install ICAgent in either of the above ways. If you have installation for multiple host: please refer to Inherited Batch Installation.

1 Enter the AK/SK to generate the installation command. How to Obtain an AK/SK?

AK [redacted]

SK [redacted]

2 Copy Command

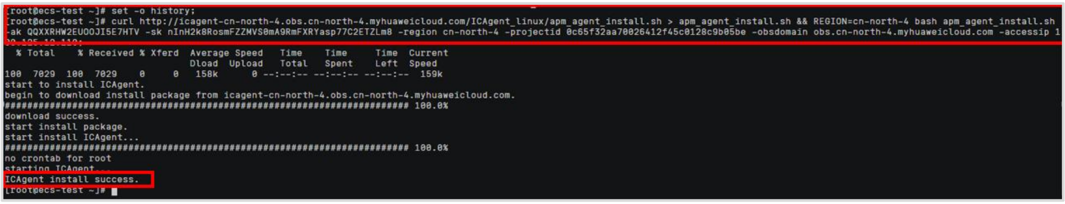
☑ Turn off command history to prevent the AK/SK from being stored.

Command Generated Copy Command ✓

```
set -o history;
curl http://icagent-ap-southeast-1.obs.ap-southeast-
1.myhuaweicloud.com/ICAgent_linux/apm_agent_install.sh >
apm_agent_install.sh && REGION=ap-southeast-1 bash
apm_agent_install.sh -ak U6VA8LTVT7UPHI0DM37B -sk
kGo1Pu1LbE90KgnVVSnvX1IUIUtoX9cExFkZx63T -region ap-
southeast-1 -projectid 4e64821a46284feb831ecfc76bc70a6b -
obsdomain obs.ap-southeast-1.myhuaweicloud.com -accessip
100.125.6.104;
```

Figure 8-29

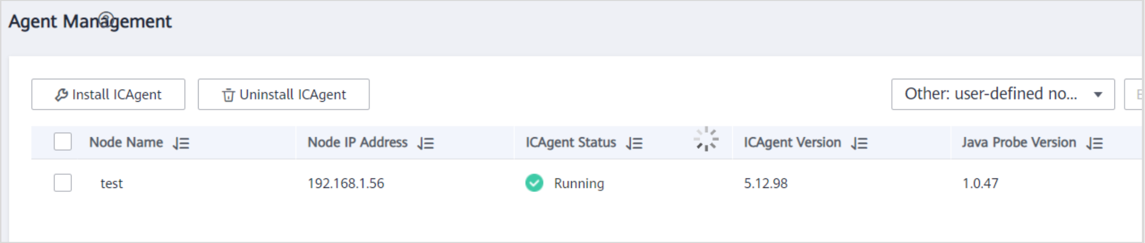
Step 4 Log in to the **test** ECS and run the copied command to install the ICAgent. If **ICAgent install success** is displayed, the installation is complete.



```
[root@ecs-test ~]# set -o history;
[root@ecs-test ~]# curl http://icagent-cn-north-4.obs.cn-north-4.myhuaweicloud.com/ICAgent_linux/apm_agent_install.sh > apm_agent_install.sh && REGION=cn-north-4 bash apm_agent_install.sh
-ak QQXXRHW2EUOOJI5E7HTV -sk nInH2k8RosmFZZMVS8mA9RmFXRYasp77C2ETZLm8 -region cn-north-4 -projectid 0c65f32aa70026412f45c0128c9b05be -obsdomain obs.cn-north-4.myhuaweicloud.com -accessip 1
[illegible]
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  7029  100  7029    0     0   158k      0 --:--:-- --:--:-- --:--:--  159k
start to install ICAgent.
begin to download install package from icagent-cn-north-4.obs.cn-north-4.myhuaweicloud.com.
######################################################################## 100.0%
download success.
start install package.
start install ICAgent...
######################################################################## 100.0%
no crontab for root
starting ICAgent...
ICAgent install success.
[root@ecs-test ~]#
```

Figure 8-30

Step 5 Return to the **Agent Management** page and refresh the page. If the ICAgent status of the **test** ECS is **Running**, the ICAgent is successfully installed.

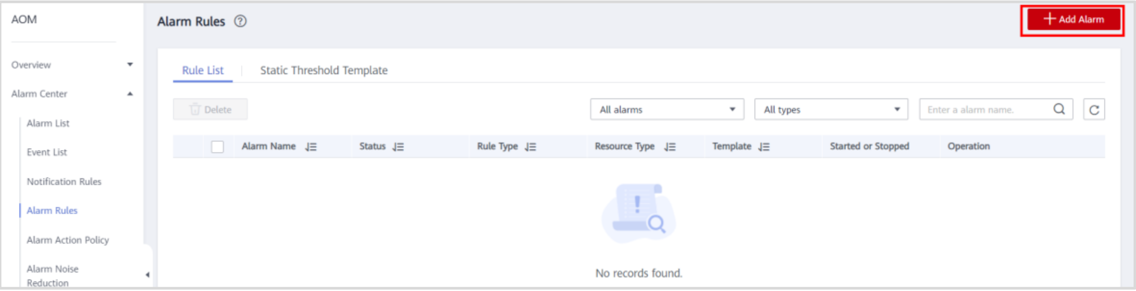


Agent Management

	Node Name	Node IP Address	ICAgent Status	ICAgent Version	Java Probe Version
□	test	192.168.1.56	Running	5.12.98	1.0.47

Figure 8-31

Step 6 In the navigation pane, choose **Alarm Center** > **Alarm Rules**. Then, click **Add Alarm** in the upper right corner.



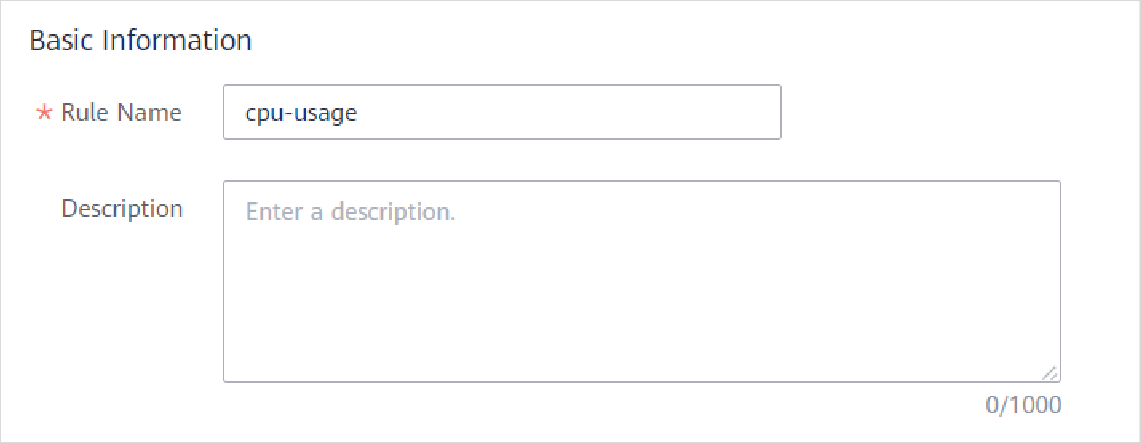
□	Alarm Name	Status	Rule Type	Resource Type	Template	Started or Stopped	Operation

No records found.

Figure 8-32

Step 7 Add an alarm rule:

- **Rule Name**: **cpu-usage**

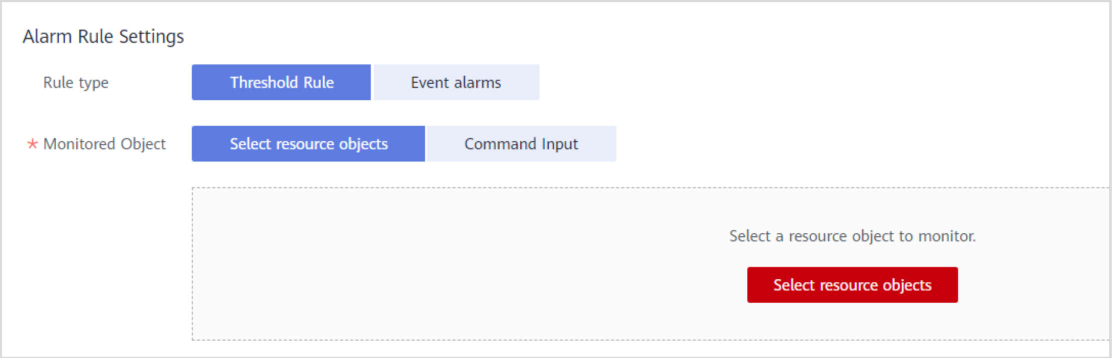


Basic Information

* Rule Name	cpu-usage
Description	Enter a description.

Figure 8-33

- **Rule Type**: **Threshold Rule**
- **Monitored Object**: **Select resource objects**
- Click **Select resource objects**.



Alarm Rule Settings

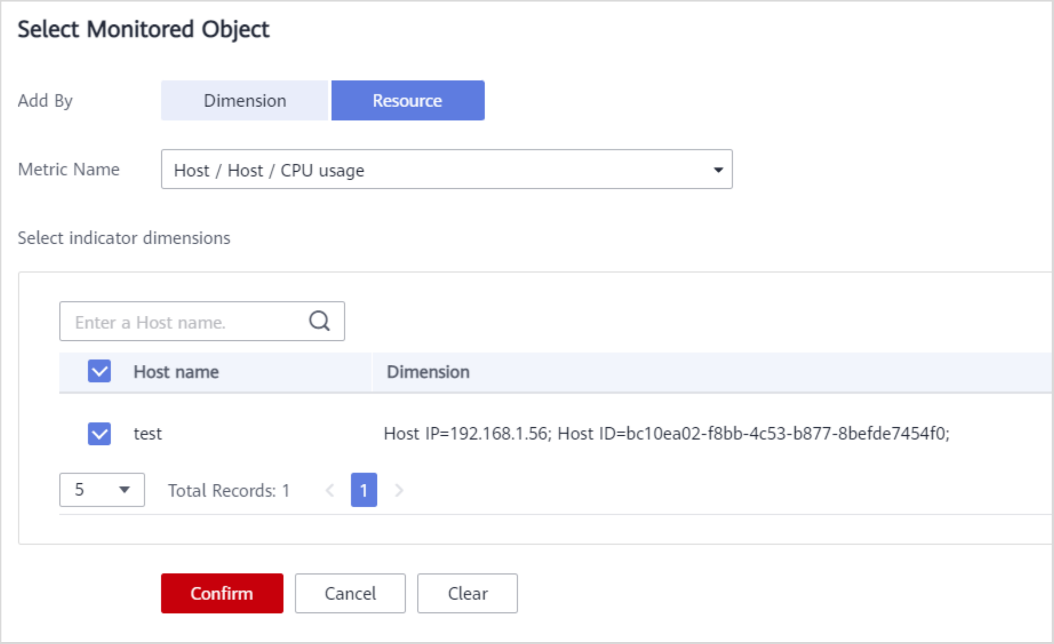
Rule type: Threshold Rule | Event alarms

* Monitored Object: Select resource objects | Command Input

Select a resource object to monitor.

Figure 8-34

- **Add By**: **Resource**
- **Metric Name**: Host/Host/CPU usage (This metric is used as an example. Trainees can select a metric based on site requirements. It may take a while to discover a newly deployed ECS.)
- **Select indicator dimensions**: **test**



Select Monitored Object

Add By: Dimension | Resource

Metric Name: Host / Host / CPU usage

Select indicator dimensions

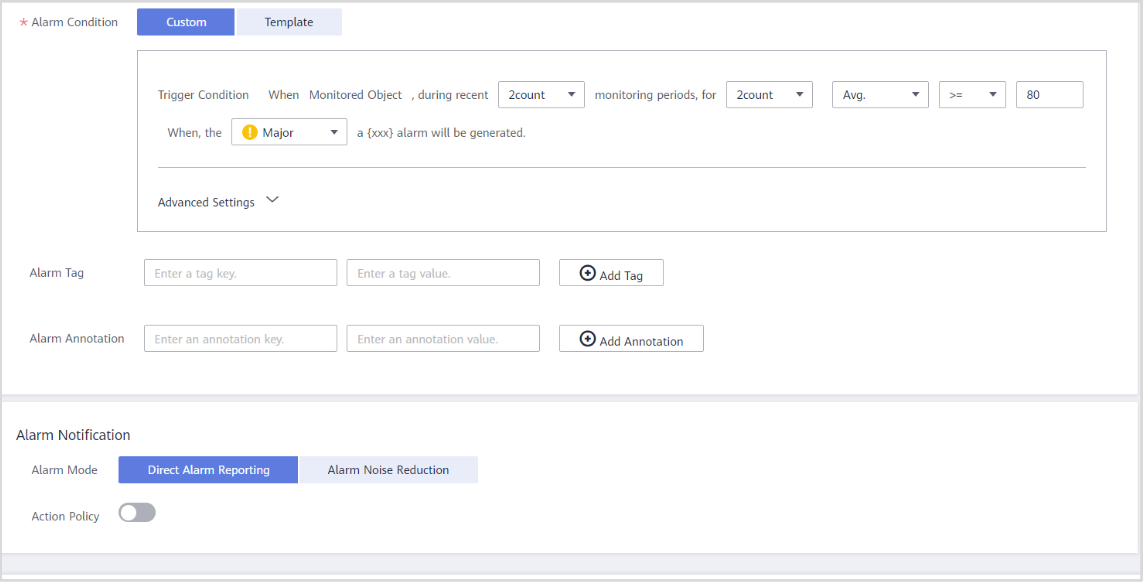
Enter a Host name.

☑ Host name	Dimension
☑ test	Host IP=192.168.1.56; Host ID=bc10ea02-f8bb-4c53-b877-8befde7454f0;

5 Total Records: 1 1

Figure 8-35

- **Alarm Condition**: **Custom**
- **Trigger conditions**: **2 | 2 | Avg. | >= | 80 | Major** (This condition is used as an example. Trainees can configure trigger conditions based on site requirements.)



* Alarm Condition: Custom | Template

Trigger Condition: When Monitored Object , during recent 2count monitoring periods, for 2count Avg. >= 80

When, the Major a {xxx} alarm will be generated.

Advanced Settings

Alarm Tag: Enter a tag key. Enter a tag value. Add Tag

Alarm Annotation: Enter an annotation key. Enter an annotation value. Add Annotation

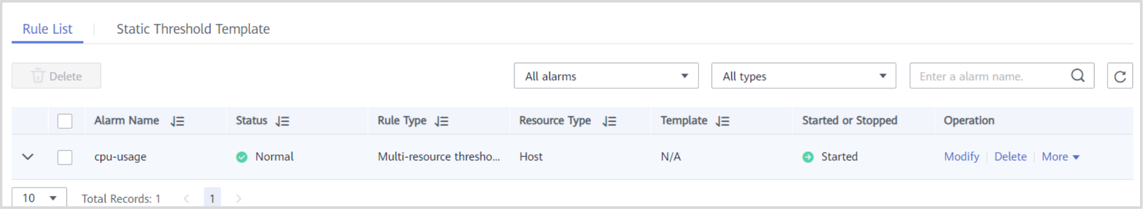
Alarm Notification

Alarm Mode: Direct Alarm Reporting | Alarm Noise Reduction

Action Policy: ○

Figure 8-36

Step 8 Check whether the status of the created rule is **Started**. If yes, the alarm rule is successfully created.



	Alarm Name	Status	Rule Type	Resource Type	Template	Started or Stopped	Operation
□	cpu-usage	Normal	Multi-resource thresho...	Host	N/A	Started	Modify | Delete | More

10 Total Records: 1 < 1 >

Figure 8-37

Step 9 In the navigation pane, choose **Overview** > **O&M**. On the displayed page, view the monitoring information of the connected resource.

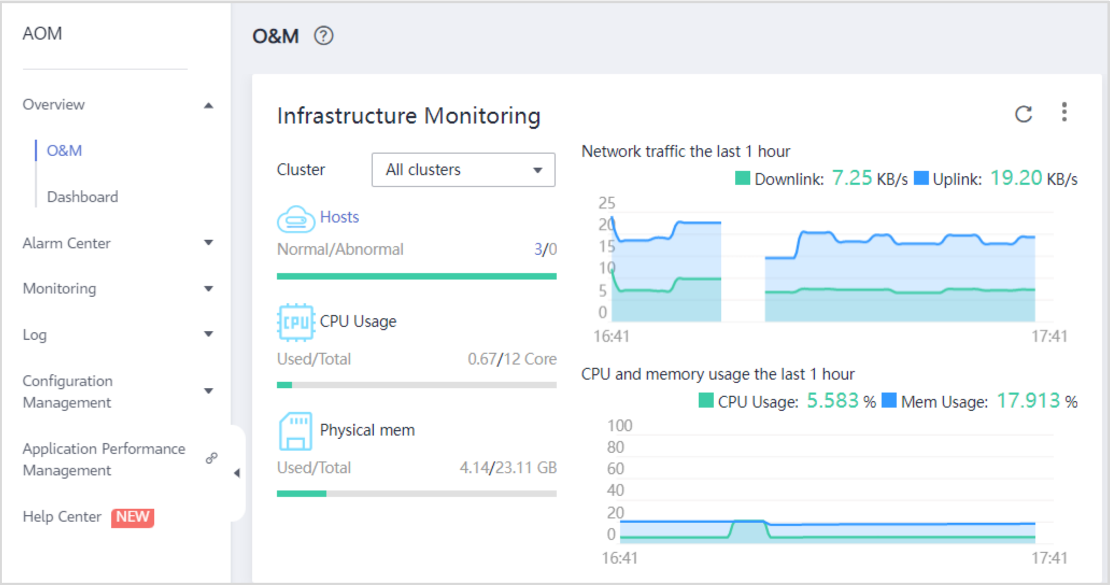


Figure 8-38

8.2.3.2 Log Collection

When a host system is abnormal, its logs will contain many errors. To identify an exception in a timely manner, you can use AOM to count the number of errors in logs and set alarm rules.

Step 1 In the navigation pane, choose **Log** > **Log Dumps**. Then, click **Add Log Dump** in the upper right corner.

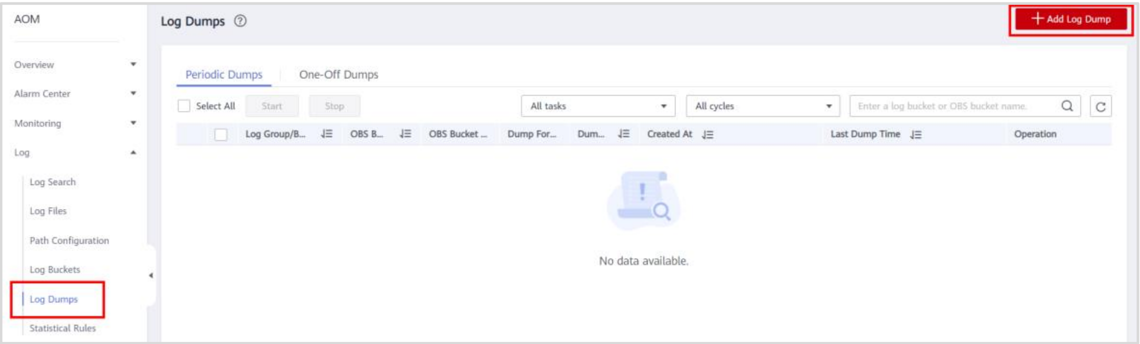
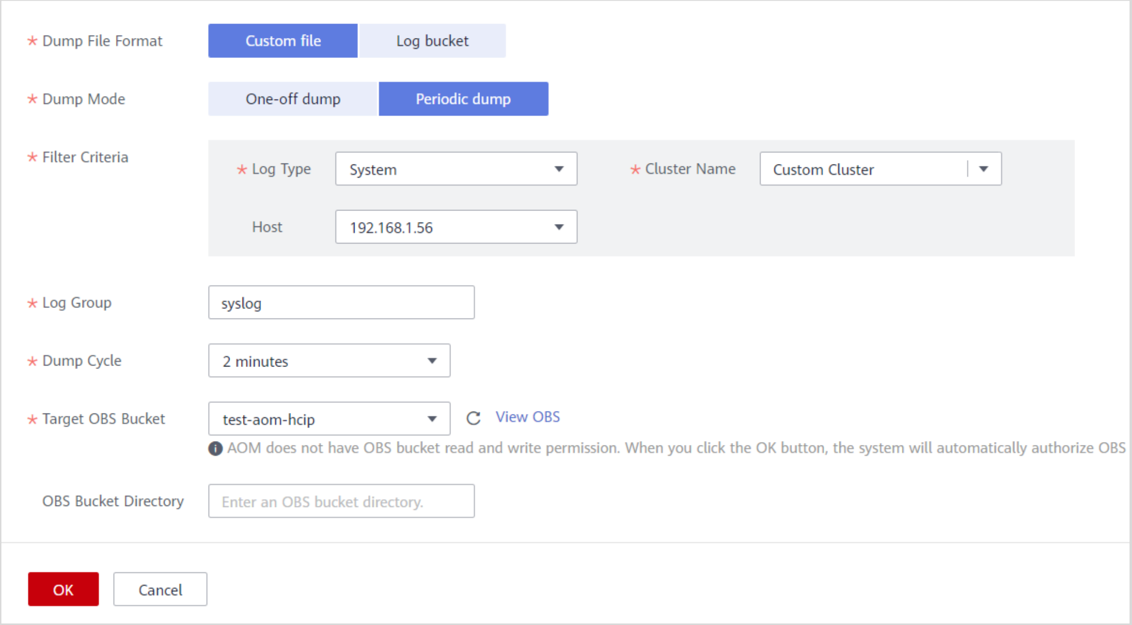


Figure 8-39

Step 2 Add a log dump:

- **Dump File Format**: **Custom file**
- **Dump Mode**: **Periodic dump**
- **Log Type**: **System**
- **Cluster Name**: **Custom Cluster**
- **Host**: **192.168.3.219** (private IP address of the **test** ECS)
- **Log Group**: **syslog**
- **Target OBS Bucket**: **test-aom-hcip** (created during preparation)



* Dump File Format: Custom file | Log bucket

* Dump Mode: One-off dump | Periodic dump

* Filter Criteria:
* Log Type: System
* Cluster Name: Custom Cluster
Host: 192.168.1.56

* Log Group: syslog

* Dump Cycle: 2 minutes

* Target OBS Bucket: test-aom-hcip

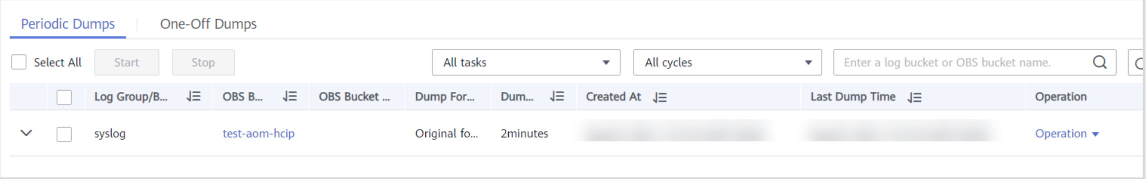
View OBS

AOM does not have OBS bucket read and write permission. When you click the OK button, the system will automatically authorize OBS

OBS Bucket Directory: Enter an OBS bucket directory.

Figure 8-40

Step 3 View the creation time and last dump time on the log dump page.



	Log Group/B...	OBS B...	OBS Bucket ...	Dump For...	Dum...	Created At	Last Dump Time	Operation
□	syslog	test-aom-hcip		Original fo...	2minutes	[redacted]	[redacted]	Operation

Figure 8-41

Step 4 In the navigation pane, choose **Log** > **Log Buckets**. Then, click **Add Log Bucket**.

Note: This log bucket will be used when you create a statistical rule.

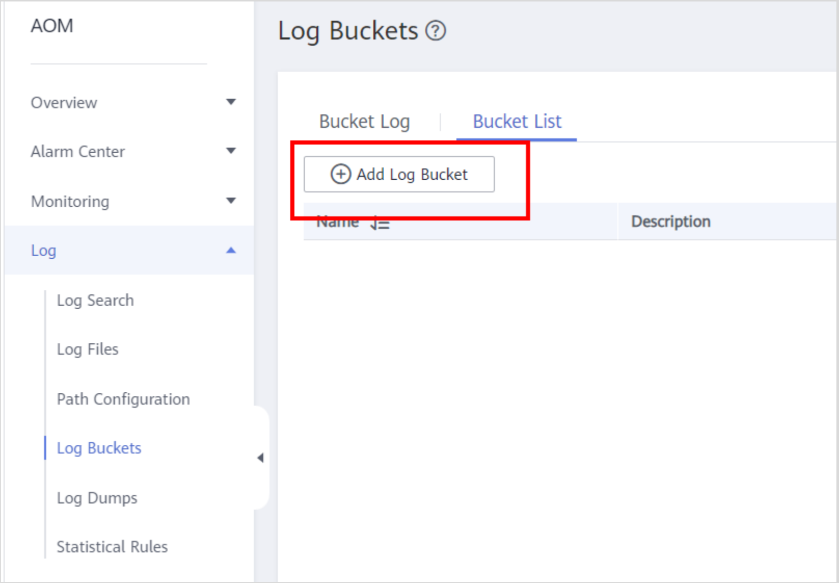
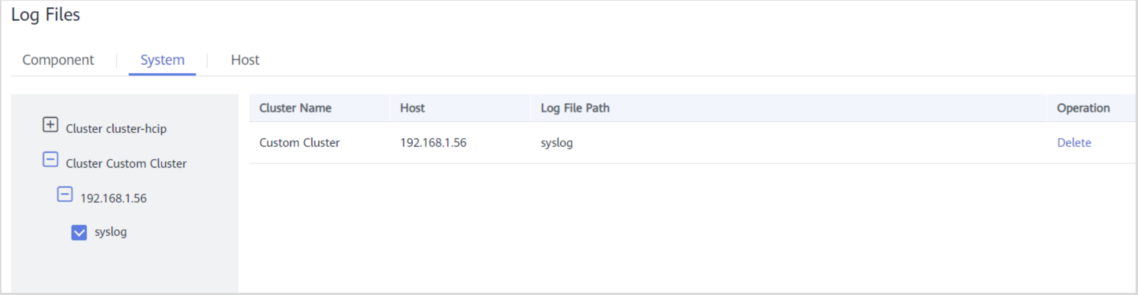


Figure 8-42

Step 5 Add a log bucket:

- **Log Bucket**: **syslog**
- **Log File**: **System | Custom Cluster | 192.168.3.219 | syslog**

Note: **192.168.3.219** is the private IP address of the **test** ECS.



Cluster Name	Host	Log File Path	Operation
Custom Cluster	192.168.1.56	syslog	Delete

Figure 8-43

Step 6 In the navigation pane, choose **Log** > **Statistical Rules**. Then, click **Create Statistical Rule** in the upper right corner.

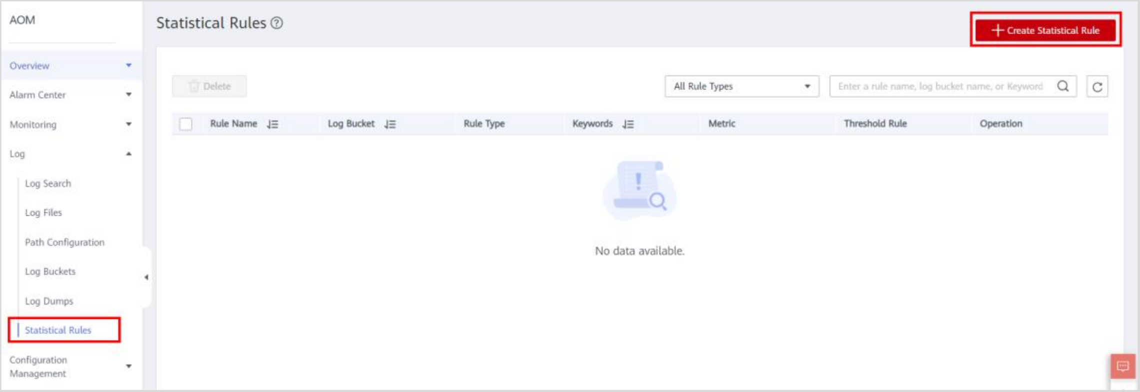
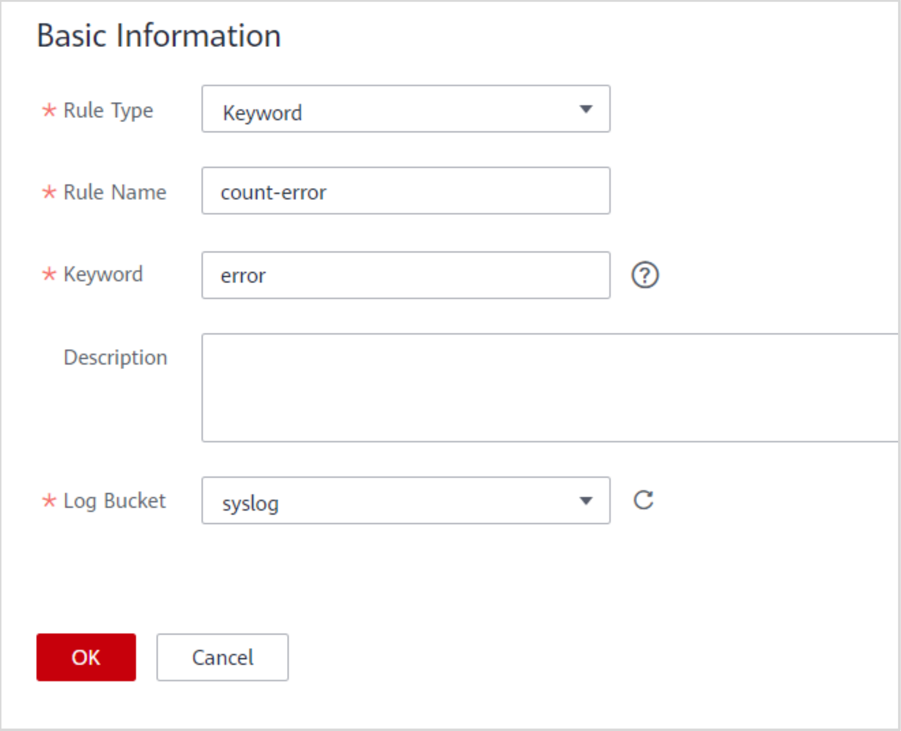


Figure 8-44

Step 7 Create a statistical rule:

- **Rule Type**: **Keyword**
- **Rule Name**: **count-error**
- **Keyword**: **error**
- **Log Bucket**: **syslog**

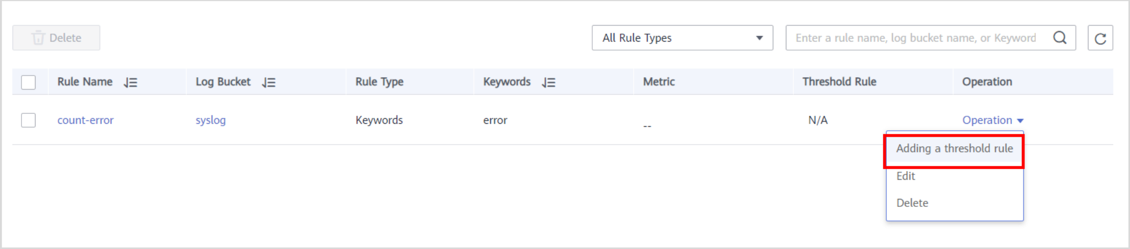


Basic Information

* Rule Type	Keyword
* Rule Name	count-error
* Keyword	error
Description	
* Log Bucket	syslog

Figure 8-45

Step 8 Locate the created statistical rule and click **Adding a threshold rule** in the **Operation** column.

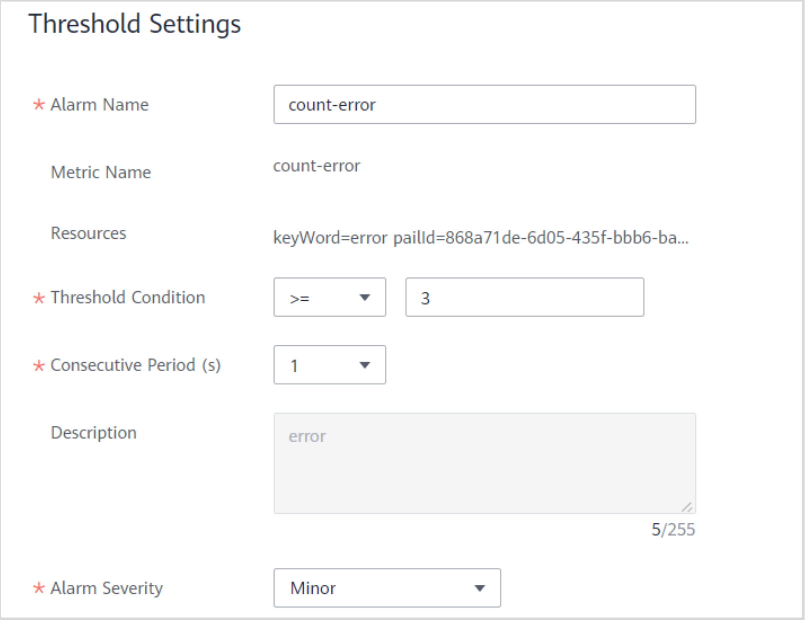


□	Rule Name	Log Bucket	Rule Type	Keywords	Metric	Threshold Rule	Operation
□	count-error	syslog	Keywords	error	--	N/A	Operation

Figure 8-46

Step 9 Create a threshold rule:

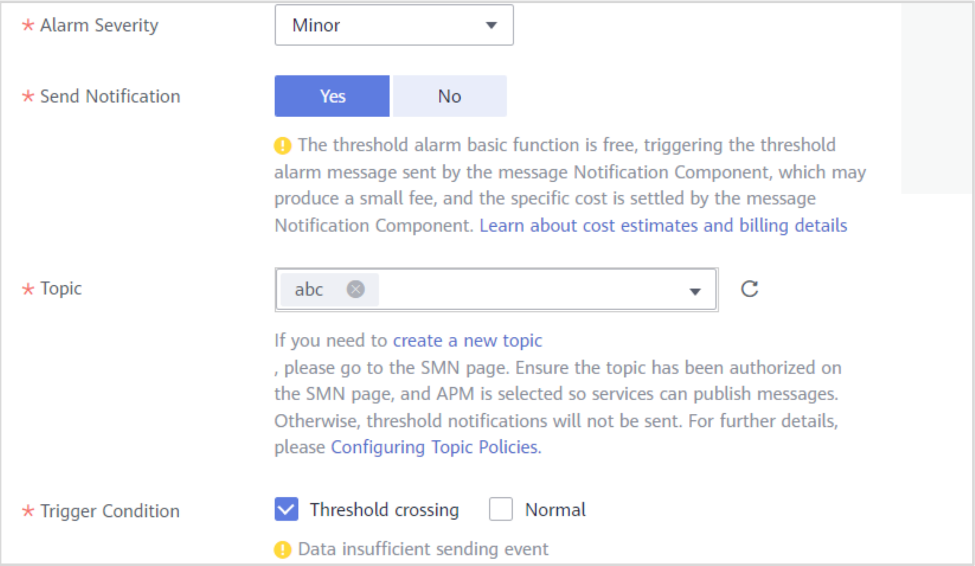
- Alarm Name: count-error
- Statistic Method: Average
- Statistical Cycle: 1 minute
- Threshold Condition: >= | 3
- Consecutive Period (s): 1
- Alarm Severity: Minor
- Send Notification: Yes
- Topic: abc
- Trigger Condition: Threshold crossing



Threshold Settings

* Alarm Name	count-error
Metric Name	count-error
Resources	keyWord=error paiId=868a71de-6d05-435f-bbb6-ba...
* Threshold Condition	>= 3
* Consecutive Period (s)	1
Description	error 5/255
* Alarm Severity	Minor

Figure 8-47



* Alarm Severity: Minor

* Send Notification: Yes No

The threshold alarm basic function is free, triggering the threshold alarm message sent by the message Notification Component, which may produce a small fee, and the specific cost is settled by the message Notification Component. Learn about cost estimates and billing details

* Topic: abc

If you need to create a new topic
, please go to the SMN page. Ensure the topic has been authorized on the SMN page, and APM is selected so services can publish messages. Otherwise, threshold notifications will not be sent. For further details, please Configuring Topic Policies.

* Trigger Condition: ☑ Threshold crossing □ Normal

Data insufficient sending event

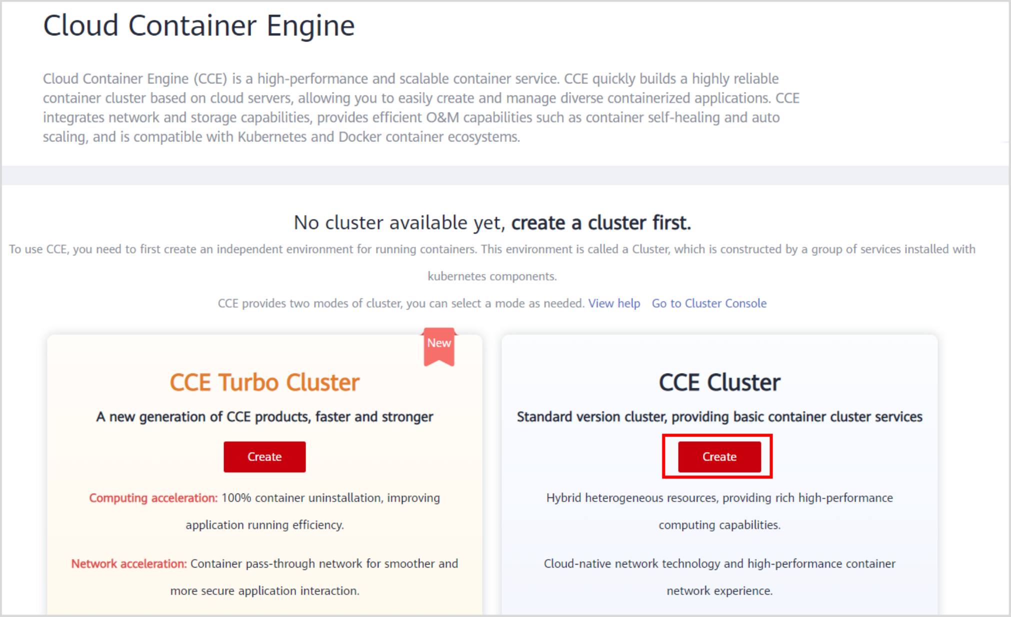
Figure 8-48

After the threshold rule is created, if the statistical result exceeds the threshold, an SMS message or email notification will be sent immediately. O&M personnel can then locate and rectify the fault at the earliest time.

8.2.3.3 CCE Cluster Monitoring

Step 1 Create a CCE cluster. For more information, see CCE-related sections.

Note: This CCE cluster will be monitored by AOM.



Cloud Container Engine

Cloud Container Engine (CCE) is a high-performance and scalable container service. CCE quickly builds a highly reliable container cluster based on cloud servers, allowing you to easily create and manage diverse containerized applications. CCE integrates network and storage capabilities, provides efficient O&M capabilities such as container self-healing and auto scaling, and is compatible with Kubernetes and Docker container ecosystems.

No cluster available yet, **create a cluster first.**

To use CCE, you need to first create an independent environment for running containers. This environment is called a Cluster, which is constructed by a group of services installed with kubernetes components.

CCE provides two modes of cluster, you can select a mode as needed. View help Go to Cluster Console

CCE Turbo Cluster

A new generation of CCE products, faster and stronger

Computing acceleration: 100% container uninstallation, improving application running efficiency.

Network acceleration: Container pass-through network for smoother and more secure application interaction.

CCE Cluster

Standard version cluster, providing basic container cluster services

Hybrid heterogeneous resources, providing rich high-performance computing capabilities.

Cloud-native network technology and high-performance container network experience.

Figure 8-49

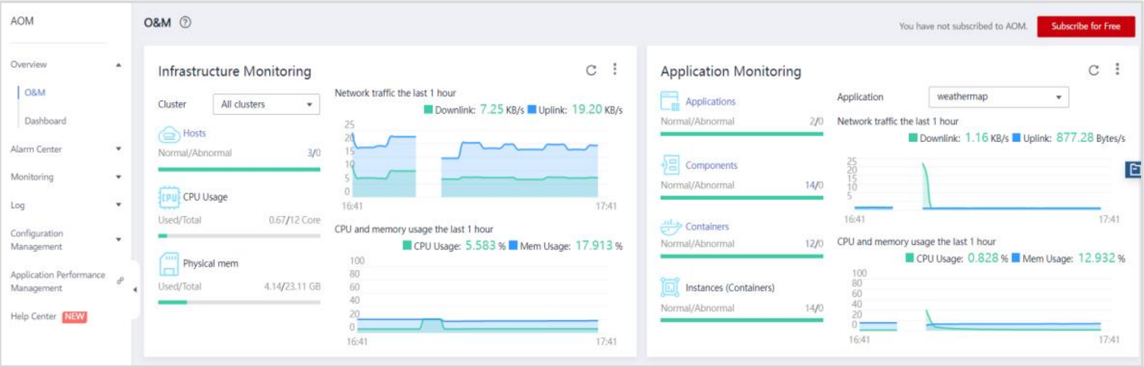
Create a cluster:

- **Region**: **CN-Hong Kong**
- **Billing Mode**: **Pay-per-use**
- **Cluster Name**: **cluster-cce** (user-defined)
- **Version**: **v1.19**
- **Management Scale**: **50 nodes**
- **Number of master nodes**: **1**
- **Network Model**: **VPC network**
- **VPC**: **vpc-1** (Reuse the created VPC or customize one.)
- **Subnet**: **vpc-1-subnet** (Reuse the created subnet or customize one.)

Create a node:

- **Billing Mode**: **Pay-per-use**
- **AZ**: Random
- **Node Type**: **VM node**
- **Specifications**: **4cores | 8GB**
- **System Disk**: Use the default setting.
- **Data Disk**: Use the default setting.
- **OS**: **Default**
- **Node Name**: Use the default name or customize one.
- **Password**: Customize one.
- **Subnet**: **vpc-1-subnet** (Reuse the created subnet.)
- **EIP**: **Do not use**
- **Login Mode**: **Password**

Step 2 In the service list, choose **Application Operations Management**. In the navigation pane, choose **Overview** > **O&M** to view monitoring information. You can monitor resources, applications, and application user experience on this page. You can also monitor the running status of the CCE cluster.



Infrastructure Monitoring

Cluster: All clusters

Hosts — Normal/Abnormal 3/0

CPU Usage — Used/Total 0.67/12 Core

Physical mem — Used/Total 4.14/23.11 GB

Network traffic the last 1 hour — Downlink: 7.25 KB/s Uplink: 19.20 KB/s

CPU and memory usage the last 1 hour — CPU Usage: 5.583 % Mem Usage: 17.913 %

Application Monitoring

Applications — Normal/Abnormal 2/0

Components — Normal/Abnormal 14/0

Containers — Normal/Abnormal 12/0

Instances (Containers) — Normal/Abnormal 14/0

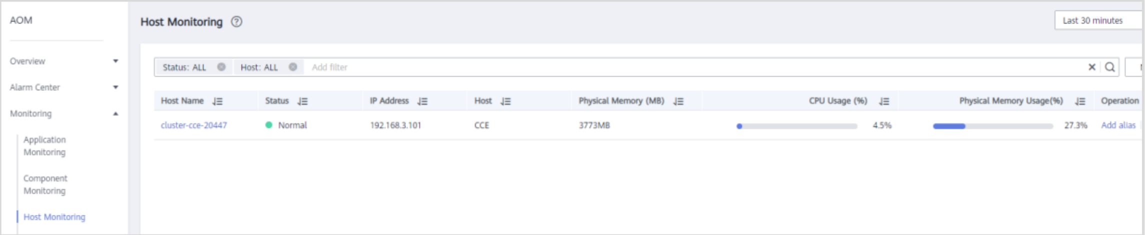
Application: weathermap

Network traffic the last 1 hour — Downlink: 1.16 KB/s Uplink: 877.28 Bytes/s

CPU and memory usage the last 1 hour — CPU Usage: 0.828 % Mem Usage: 12.932 %

Figure 8-50

Step 3 In the navigation pane, choose **Monitoring** > **Host Monitoring**. You can monitor host resource usage and health status of the CCE cluster, as well as the usage of common system devices such as disks and CPUs.

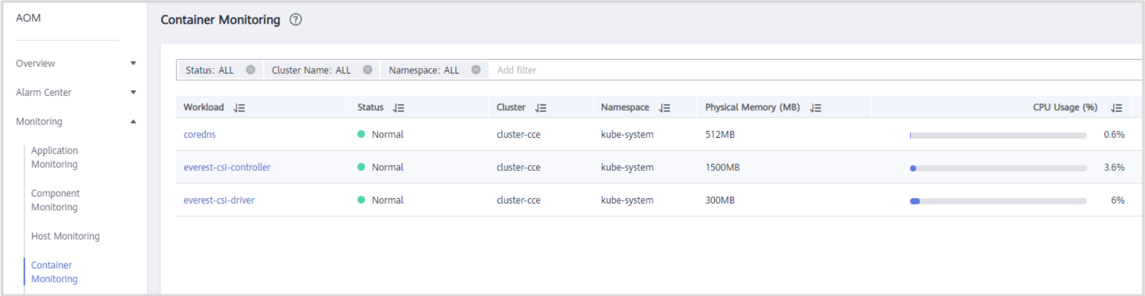


Status: ALL Host: ALL

Host Name	Status	IP Address	Host	Physical Memory (MB)	CPU Usage (%)	Physical Memory Usage(%)	Operation
cluster-cce-20447	● Normal	192.168.3.101	CCE	3773MB	4.5%	27.3%	Add alias

Figure 8-51

Step 4 In the navigation pane, choose **Monitoring** > **Container Monitoring** to view information about plug-ins and containers in the CCE cluster.



Status: ALL Cluster Name: ALL Namespace: ALL

Workload	Status	Cluster	Namespace	Physical Memory (MB)	CPU Usage (%)
coredns	● Normal	cluster-cce	kube-system	512MB	0.6%
everest-csi-controller	● Normal	cluster-cce	kube-system	1500MB	3.6%
everest-csi-driver	● Normal	cluster-cce	kube-system	300MB	6%

Figure 8-52

8.3 Clearing Resources

Step 1 Delete the SMN topic.

In the service list, choose **Simple Message Notification**. In the navigation pane, choose **Topic Management** > **Topics**. In the right pane, locate the topic created in this exercise and choose **More** > **Delete** in the **Operation** column.

Step 2 Delete the alarm rule.

On the AOM console, choose **Alarm Center** > **Alarm Rules** in the navigation pane, locate the alarm rule created in this exercise, and click **Delete** in the **Operation** column.

Step 3 Delete the statistical rule.

On the AOM console, choose **Log** > **Statistical Rules** in the navigation pane, locate the statistical rule created in this exercise, and click **Delete** in the **Operation** column.

Step 4 Delete the log bucket.

On the AOM console, choose **Log** > **Log Buckets** in the navigation pane, locate the log bucket created in this exercise, and click **Delete** in the **Operation** column.

Step 5 Delete the log dump.

On the AOM console, choose **Log** > **Log Dumps** in the navigation pane, locate the log dump created in this exercise, and click **Delete** in the **Operation** column.

Step 6 Delete the ECS.

- In the service list, choose **Elastic Cloud Server** under **Compute**. In the ECS list, locate the ECS created in this exercise and choose **More** > **Delete** in the **Operation** column.
- In the displayed dialog box, select the check boxes shown in the following figure and click **Yes**.

Step 7 Delete the security group.

In the service list, choose **Virtual Private Cloud** under **Networking**. On the network console, choose **Access Control** > **Security Groups**. In the security group list, locate the security group created in this exercise and click **Delete** in the **Operation** column.

Step 8 Delete the subnet and VPC.

- In the service list, choose **Virtual Private Cloud** under **Networking**. On the network console, choose **Subnets**. In the subnet list, locate the subnet created in this exercise and click **Delete** in the **Operation** column.
- On the network console, choose **My VPCs**. In the VPC list, locate the VPC created in this exercise, and click **Delete** in the **Operation** column.

8.4 Quiz

Question: How does AOM obtain a custom host IP address on the Agent management page?

Answer: By default, AOM traverses all NICs on a VM and obtains the IP addresses of the Ethernet, bond, and wireless NICs based on priorities in descending order. To ensure that

AOM obtains the IP address of a specific NIC, set the **IC_NET_CARD=Desired NIC name** environment variable when starting the ICAgent.