

Huawei Cloud Service Certification Training

# HCIA-Cloud Service

## Lab Guide

Version: 3.5



HUAWEI TECHNOLOGIES CO., LTD

**Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.**

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

#### **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

#### **Notice**

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

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

## **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. It supports the development of ICT infrastructure that features Cloud-Pipe-Device synergy. Our certification is always evolving to reflect the latest trends in ICT development.

Huawei Certification consists of three categories: ICT Infrastructure Certification, Basic Software & Hardware Certification, and Cloud Platform & Services 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).

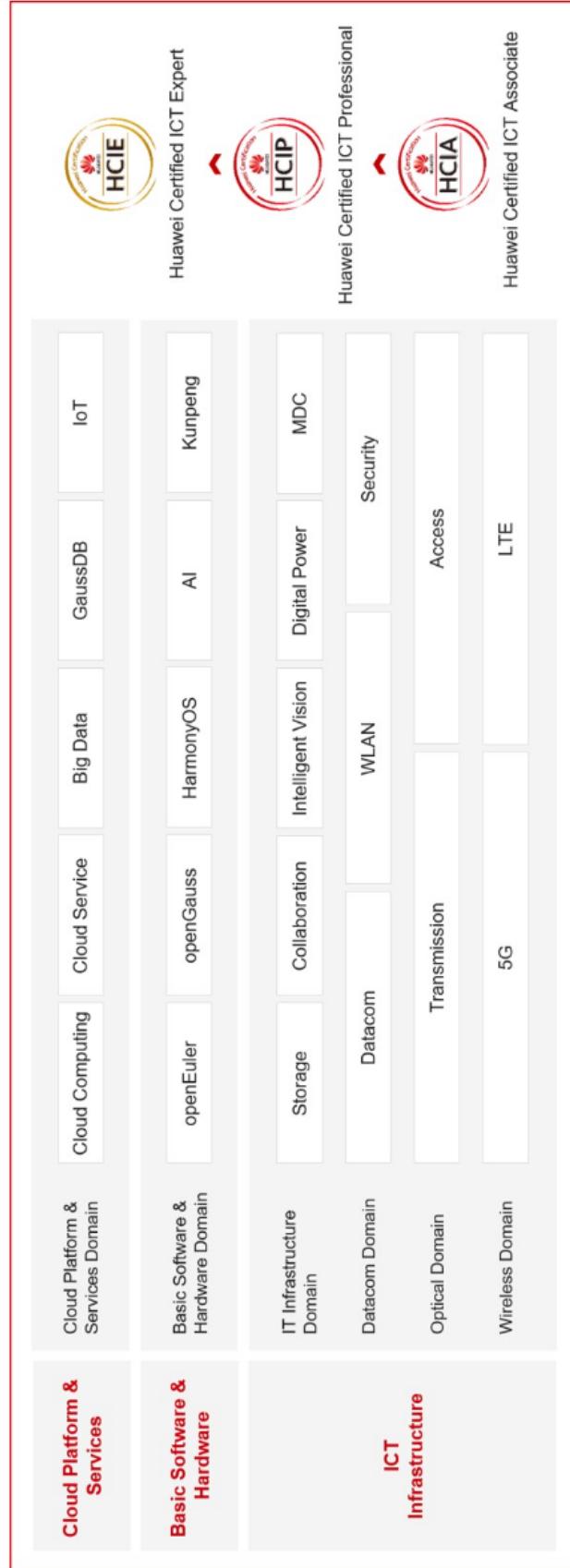
Our programs cover all ICT fields and follow the industry's trend of ICT convergence. With our leading talent development system and certification standards, we are committed to fostering new digital ICT talent and building a sound ICT talent ecosystem.

HCIA-Cloud Service (Huawei Certified ICT Associate-Cloud Service) aims to cultivate cloud engineers who are capable of building enterprise IT architectures and using and managing cloud services through common cloud services such as compute, storage, and network services. This document is intended for trainees who take the HCIA-Cloud Service exam and technical personnel who want to understand the basics of cloud computing and how to use, manage, and maintain Huawei cloud services. The HCIA-Cloud Service certification covers basic cloud knowledge and operations and usage of compute, storage, network, and O&M services in HUAWEI CLOUD.

Passing the HCIA-Cloud Service certification proves that you have a certain understanding of Huawei cloud service products and technologies and are capable of independently using Huawei cloud service products.

Enterprises have HCIA-Cloud Service certified engineers, which means that they have mastered the application scenarios and usage methods of various Huawei cloud service products, facilitating cloud transformation in their ICT environments.

## Huawei Career Certification



# About This Document

---

## Overview

This document is a training course for the HCIA-Cloud Service certification. It is intended for those who are preparing for the HCIA-Cloud Service exam or those who want to learn about how to use, manage, and maintain cloud services.

## Description

This document includes exercises on HUAWEI CLOUD operations, exercises on compute, networking, storage, and O&M services, and comprehensive exercises. These exercises can help you understand the functions and positions of the cloud services.

- Experiment 1: HUAWEI CLOUD operation Guide
  - The exercises include registering a HUAWEI CLOUD account, logging in to the console, configuring IAM, as well as purchasing, trying, and releasing cloud services.
- Experiment 2: Compute Services Practice
  - Exercises on compute services including Elastic Cloud Server (ECS), Image Management Service (IMS), and Auto Scaling (AS). The exercises involve ECS lifecycle management, image management, and auto scaling.
- Experiment 3: Network Services Practice
  - This experiment describes how to use network services, including enabling communication between ECSs in the same Virtual Private Cloud (VPC), using security groups, Elastic IP (EIP), Virtual Private Network (VPN), and using Elastic Load Balance (ELB) to distribute traffic among backend servers.
- Experiment 4: Storage Services Practice
  - This experiment describes how to use storage services, including using and managing Elastic Volume Service (EVS), Object Storage Service (OBS), and Scalable File Service (SFS).
- Experiment 5: O&M Services Practice
  - Exercises on O&M services, including using Cloud Trace Service (CTS) to track operations, using the Cloud Eye to monitor cloud services, and using Log Tank Service (LTS) to search for logs
- Experiment 6: Comprehensive Exercise: Deploying an Enterprise Website on HUAWEI CLOUD
  - This experiment is a comprehensive practice. ECSs and RDS instances are used as service nodes and data nodes respectively. A VPC provides network resources for ECSs. Based on service requirements and policies, the AS service

dynamically adjusts the number of ECSs that function as service nodes to ensure stable and healthy service running. Load balancing is used to automatically distribute access traffic to multiple service nodes, achieving higher fault tolerance performance of applications. Cloud Eye is used to monitor service status.

## Background Knowledge Required

This course is a basic course for Huawei certification. To better master the contents of this document, the readers of this document must meet the following basic requirements:

- Basic IT knowledge
- Be familiar with servers and common operating systems (such as Linux).
- Basic knowledge of storage and networking

## Experiment Environment Overview

All exercises will be performed on the [HUAWEI CLOUD official website](#). The cloud service is under fast iterative development, so some screenshots in this document might be different from those on the official website.

You can visit the [Help Center](#) to learn more about using the cloud services.

For details about the experiment resources and expenses involved in this document, see the *HCIA-Cloud Service V3.5 Resource List*. The actual costs may vary, depending on your use of the cloud services.

# Contents

---

<b>About This Document .....</b>	<b>3</b>
Overview .....	3
Description .....	3
Background Knowledge Required .....	4
Experiment Environment Overview .....	4
<b>1 Getting Started with HUAWEI CLOUD .....</b>	<b>8</b>
1.1 Introduction .....	8
1.1.1 About This Lab .....	8
1.1.2 Objectives .....	8
1.2 Configuration Procedure .....	8
1.2.1 Configuration Roadmap .....	8
1.2.2 Configuration Procedure .....	9
1.2.3 Creating an IAM User and Assigning Permissions .....	12
1.2.4 Creating and Configuring a VPC .....	19
1.3 Exercises.....	21
<b>2 Compute Services .....</b>	<b>22</b>
2.1 Introduction .....	22
2.1.1 About This Exercise .....	22
2.1.2 Objectives .....	22
2.2 Tasks .....	22
2.2.1 Roadmap .....	22
2.2.2 ECS Lifecycle Management .....	23
2.2.3 Creating a Linux System Disk Image from an ECS .....	33
2.2.4 AS Operations .....	43
2.2.5 Deleting Resources .....	53
2.3 Exercises.....	53
<b>3 Networking Services .....</b>	<b>54</b>
3.1 Introduction .....	54
3.1.1 About This Exercise .....	54
3.1.2 Objectives .....	55
3.2 Tasks .....	55
3.2.1 Roadmap .....	55
3.2.2 Creating VPCs .....	56
3.2.3 Buying ECSS.....	59

3.2.4 Verifying Network Service Functions.....	63
3.2.5 Deleting Resources .....	86
3.3 Exercises.....	86
<b>4 Storage Services.....</b>	<b>88</b>
4.1 EVS.....	88
4.1.1 Introduction .....	88
4.1.2 Tasks.....	88
4.2 OBS .....	100
4.2.1 Introduction .....	100
4.2.2 Tasks.....	101
4.3 SFS .....	116
4.3.1 Introduction .....	116
4.3.2 Tasks.....	117
4.3.3 Deleting Resources .....	125
4.4 Self-learning homework .....	127
<b>5 O&amp;M Services .....</b>	<b>128</b>
5.1 Introduction.....	128
5.1.1 About This Exercise .....	128
5.1.2 Objectives .....	128
5.2 Tasks .....	128
5.2.2 Configuring CTS - key event notifications .....	129
5.2.3 Use Cloud Eye - Monitoring ECS.....	137
5.2.4 LTS-Viewing ECS Logs .....	143
5.3 Deleting Resources .....	152
5.4 Self-learning homework .....	153
<b>6 Comprehensive Exercise: Deploying an Enterprise Website on HUAWEI CLOUD .....</b>	<b>154</b>
6.1 Background.....	154
6.2 Solution.....	154
6.3 Preparations .....	155
6.3.1 Logging In to HUAWEI CLOUD .....	155
6.3.2 Creating a VPC.....	156
6.3.3 Creating and Configuring a Security Group.....	157
6.3.4 Buying an ECS .....	159
6.3.5 Buying an RDS DB Instance .....	162
6.4 Setting Up the Linux, Apache, MySQL, PHP (LAMP) Environment .....	166
6.4.1 Installing LAMP.....	166
6.4.2 Creating a Database for WordPress.....	169

6.4.3 Installing WordPress .....	171
6.5 Achieving High Availability for Web Servers.....	175
6.5.1 Creating a Shared Load Balancer .....	175
6.5.2 Creating an Image .....	179
6.5.3 Configuring AS.....	181
6.6 Visiting the Website.....	186
6.7 Monitoring Resources.....	187
6.8 Deleting Resources .....	189
6.8.1 Deleting ECSs .....	189
6.8.2 Deleting the RDS DB Instance.....	190
6.8.3 Deleting the Image .....	191
6.8.4 Deleting the Load Balancer.....	191
6.8.5 Deleting AS Resources .....	192
6.8.6 Deleting VPC Resources.....	192
<b>7 Acronyms and Abbreviations.....</b>	<b>195</b>

# 1

# Getting Started with HUAWEI CLOUD

## 1.1 Introduction

### 1.1.1 About This Lab

- Register a HUAWEI CLOUD account, log in using the account, create an IAM user and user group, and purchase and release cloud resources.

### 1.1.2 Objectives

Upon completion of this task, you will be able to:

- Understand HUAWEI CLOUD accounts, subaccounts, and related configurations.
- How to register a HUAWEI CLOUD account.
- Learn how to purchase and release HUAWEI CLOUD resources.

## 1.2 Configuration Procedure

### 1.2.1 Configuration Roadmap

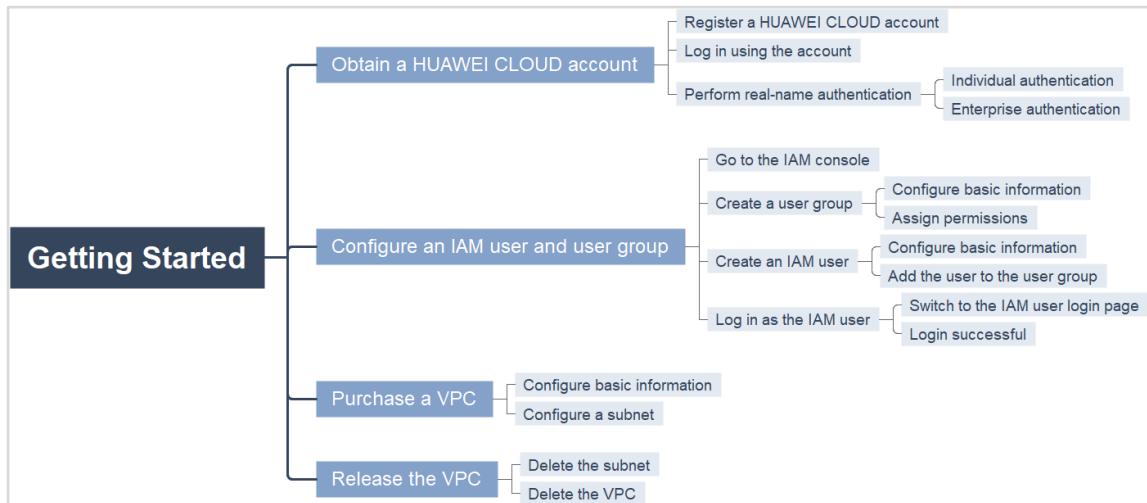
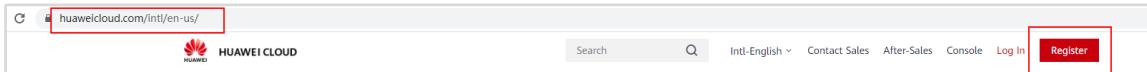


Figure 1-1 Configuration flowchart

## 1.2.2 Configuration Procedure

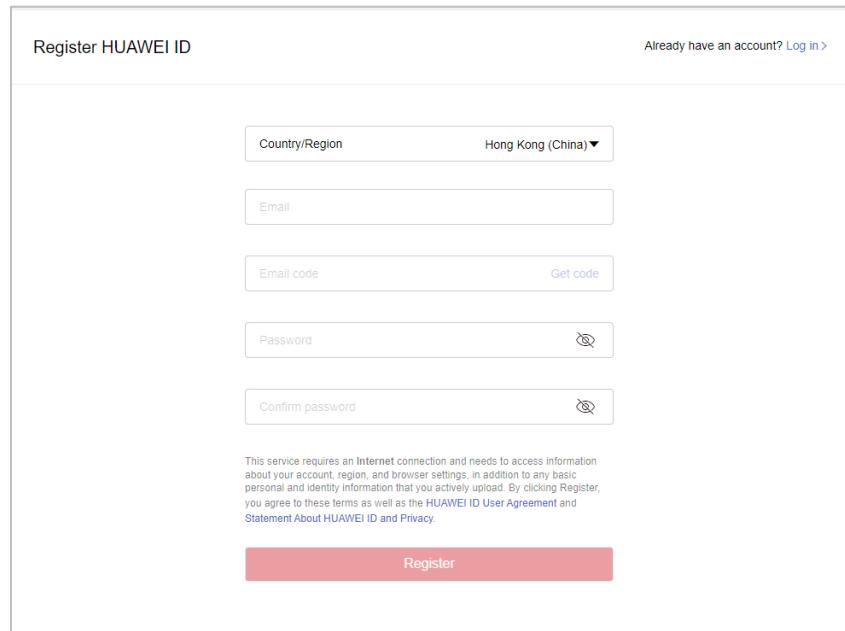
If you want to use cloud service resources on HUAWEI CLOUD, you need to have a HUAWEI CLOUD account. Your account lets you use HUAWEI CLOUD resources and pay for their use. Therefore, you need to register a HUAWEI CLOUD account first.

Step 1 Visit [HUAWEI CLOUD official website](https://huaweicloud.com/intl/en-us/), and click **Register** in the upper right.



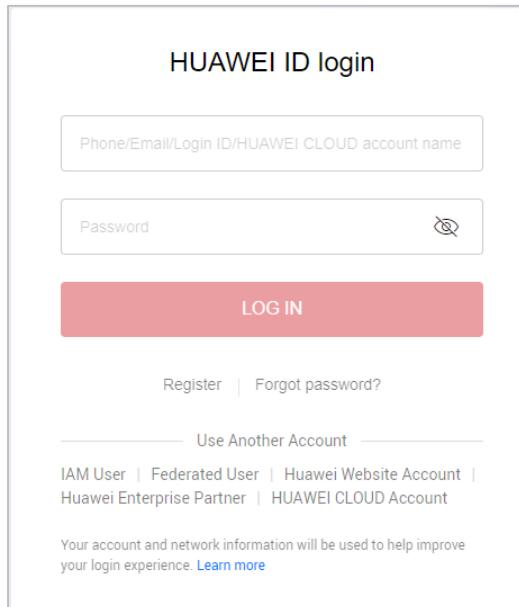
**Figure 1-2 Visiting the HUAWEI CLOUD official website**

Step 2 Enter the information required.

A screenshot of the "Register HUAWEI ID" form. The form includes fields for "Country/Region" (set to "Hong Kong (China)"), "Email", "Email code" (with a "Get code" button), "Password" (with a visibility icon), and "Confirm password" (with a visibility icon). Below the form is a terms and conditions disclaimer and a large red "Register" button.

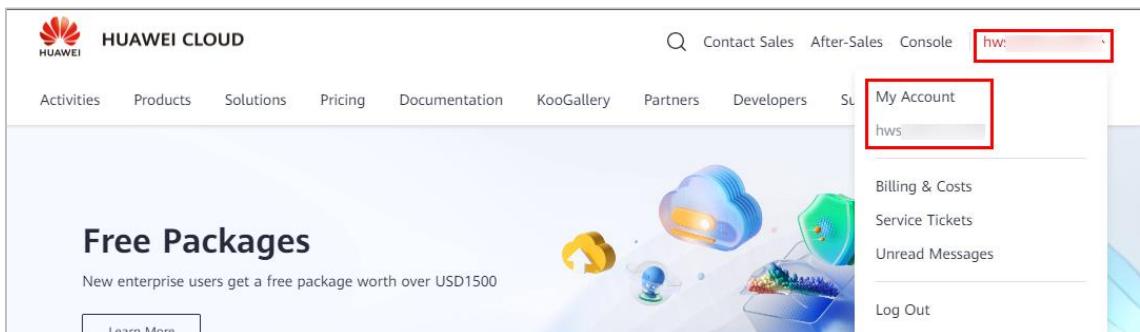
**Figure 1-3 Registering a HUAWEI CLOUD account**

Step 3 Log in to HUAWEI CLOUD using your new account.



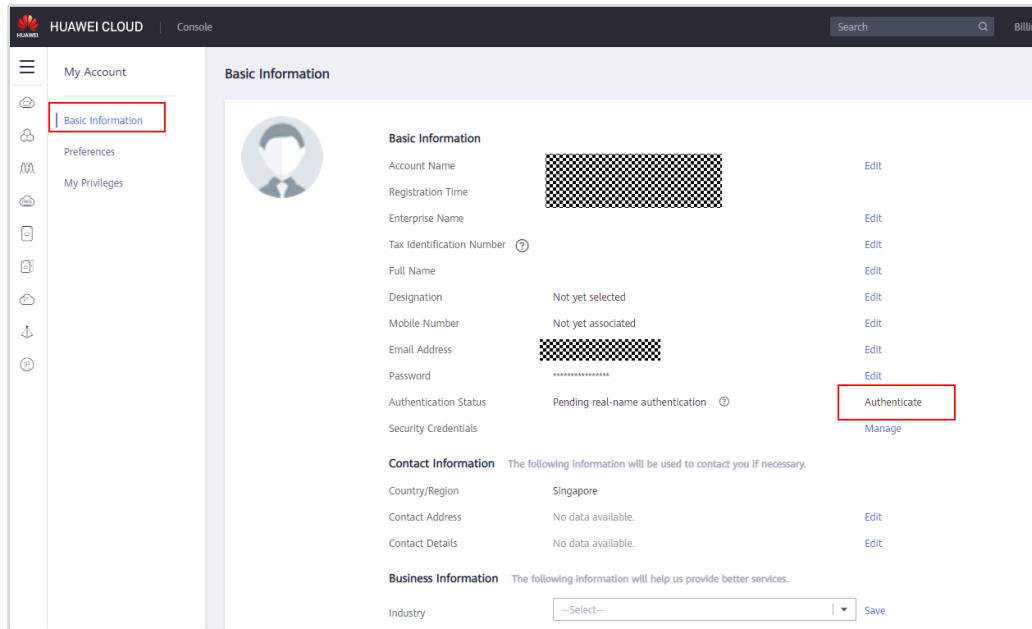
**Figure 1-4 Logging in to HUAWEI CLOUD**

Step 4 Click **YOURUSERNAME** in the upper right and choose **My Account**.



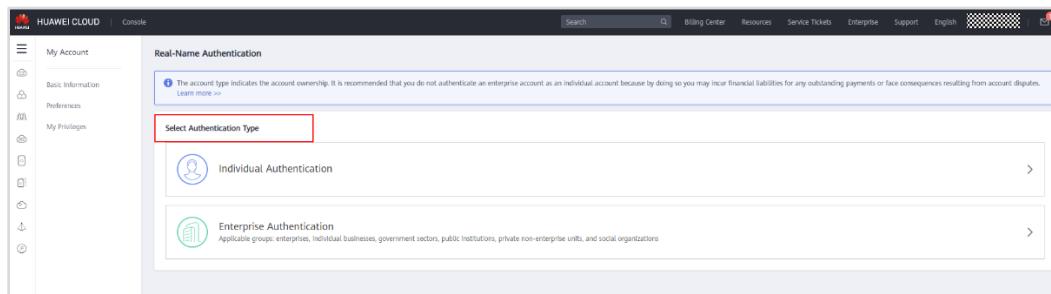
**Figure 1-5 Accessing the console**

Step 5 Click **Basic Information** and Select **Authenticate** next to Authentication Status.



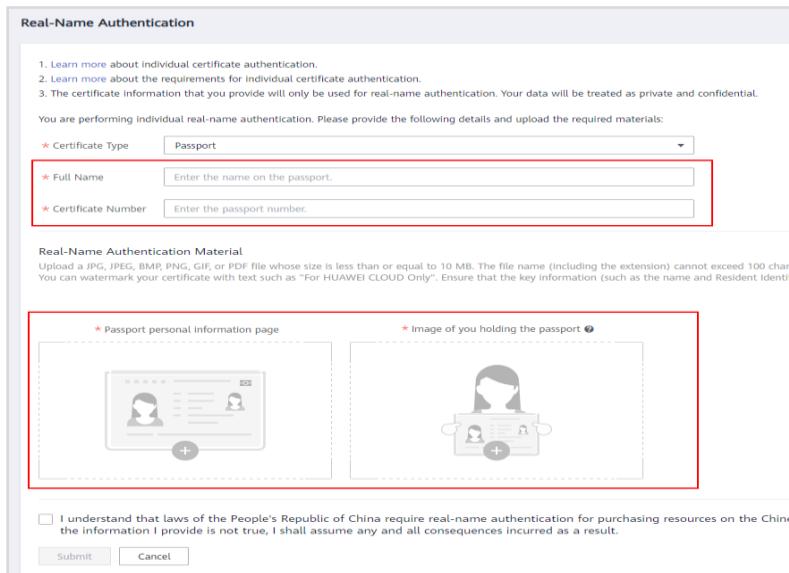
**Figure 1-6 Clicking Authenticate**

**Step 6 Select a type that matches your account. Here, we'll select **Individual Authentication**.**



**Figure 1-7 Selecting an authentication type**

**Step 7 Complete the information required.**



The screenshot shows the 'Real-Name Authentication' page. At the top, there are three numbered steps: 1. Learn more about individual certificate authentication., 2. Learn more about the requirements for individual certificate authentication., and 3. The certificate information that you provide will only be used for real-name authentication. Your data will be treated as private and confidential.

You are performing individual real-name authentication. Please provide the following details and upload the required materials:

\* Certificate Type: Passport

\* Full Name: Enter the name on the passport.

\* Certificate Number: Enter the passport number.

**Real-Name Authentication Material**

Upload a JPG, JPEG, BMP, PNG, GIF, or PDF file whose size is less than or equal to 10 MB. The file name (including the extension) cannot exceed 100 characters. You can watermark your certificate with text such as "For HUAWEI CLOUD Only". Ensure that the key information (such as the name and Resident Identity Card number) is clearly visible.

\* Passport personal information page: A placeholder for a passport photo.

\* Image of you holding the passport: A placeholder for a photo of the user holding their passport.

I understand that laws of the People's Republic of China require real-name authentication for purchasing resources on the China Cloud. If the information I provide is not true, I shall assume any and all consequences incurred as a result.

Submit Cancel

**Figure 1-8 Individual authentication**

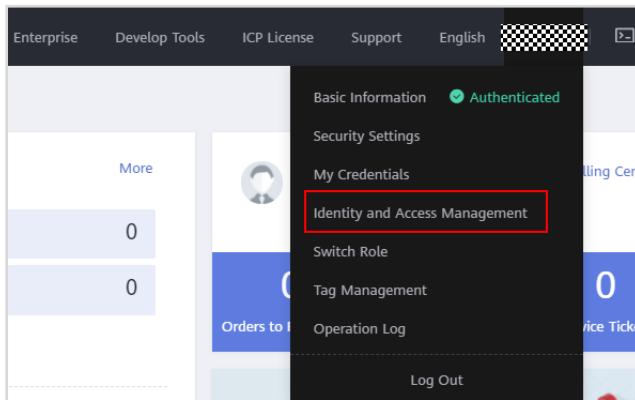
Step 8 Once complete, refresh the **Real-Name Authentication** page. The authentication is successful, so let's proceed to the next exercise.

### 1.2.3 Creating an IAM User and Assigning Permissions

To share resources in your HUAWEI CLOUD account without giving others your account and password, create an IAM user and assign the user permissions for specific resources.

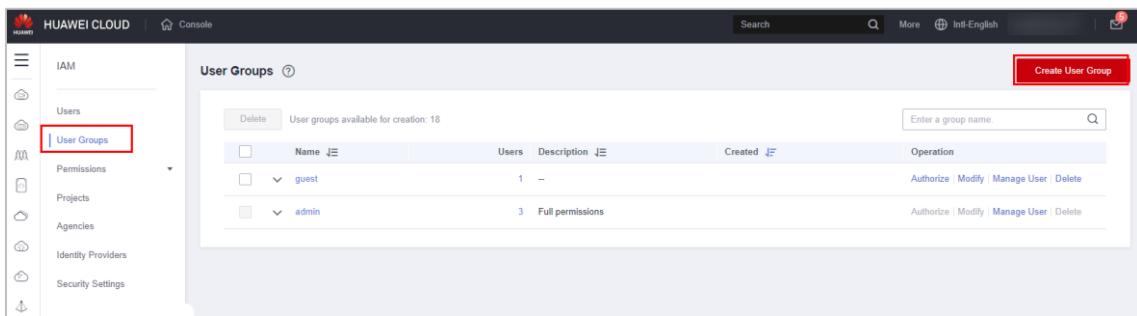
A user created by a HUAWEI CLOUD account in IAM is the user who uses cloud services and has independent identity credentials (passwords and access keys) to use resources based on the permissions granted by the account. IAM users are not charged or paid independently. They are paid by their own HUAWEI CLOUD accounts.

Step 1 Go to the management console, hover over your username in the upper right, and choose **Identity and Access Management** from the drop-down list.



**Figure 1-9 Choosing Identity and Access Management**

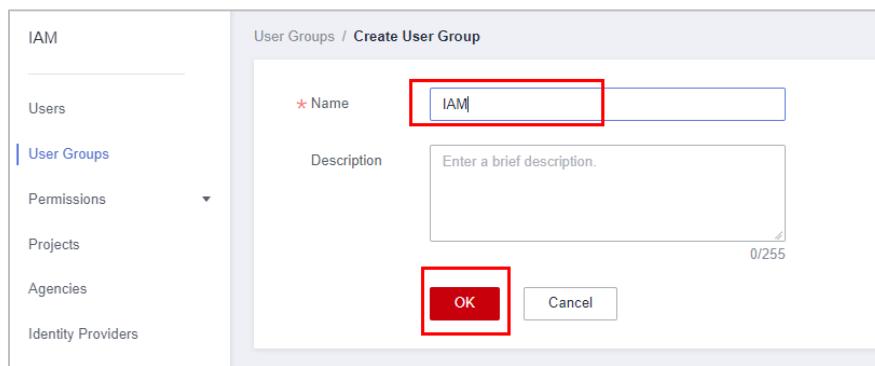
Step 2 A user group is a collection of users. IAM uses the user group function to authorize users. Choose **User Groups** in the navigation pane, and click **Create User Group**.



Name	Users	Description	Created	Operation
guest	1	--	08:00	<a href="#">Authorize</a>   <a href="#">Modify</a>   <a href="#">Manage User</a>   <a href="#">Delete</a>
admin	3	Full permissions	T+08:00	<a href="#">Authorize</a>   <a href="#">Modify</a>   <a href="#">Manage User</a>   <a href="#">Delete</a>

**Figure 1-10 Creating a user group**

Step 3 Enter a user group name and click **OK**.



User Groups / Create User Group

Name: **IAM**

Description: Enter a brief description.

OK Cancel

**Figure 1-11 Configuring the user group information**

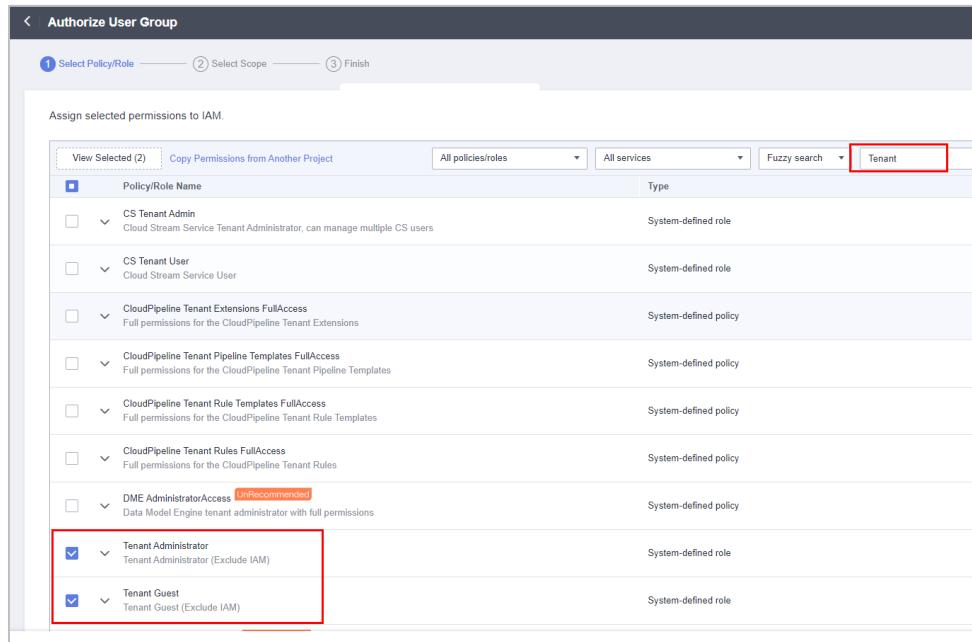
Step 4 After the user group is created, click **Authorize** to add permissions to the user group.



Name	Users	Description	Created	Operation
IAM	0	--	08:00	<b>Authorize</b>   <a href="#">Modify</a>   <a href="#">Manage User</a>   <a href="#">Delete</a>
guest	1	--		<a href="#">Authorize</a>   <a href="#">Modify</a>   <a href="#">Manage User</a>   <a href="#">Delete</a>
admin	3	Full permissions	T+08:00	<a href="#">Authorize</a>   <a href="#">Modify</a>   <a href="#">Manage User</a>   <a href="#">Delete</a>

**Figure 1-12 Click Authorize**

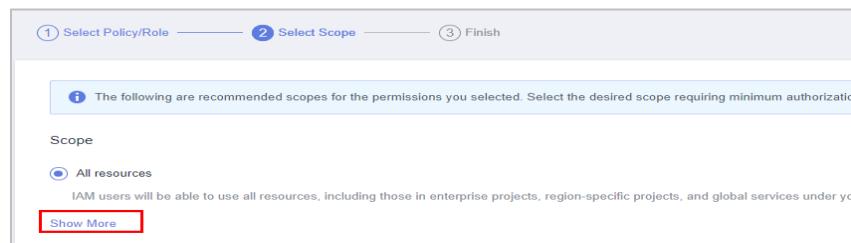
Step 5 Enter *Tenant* in the upper right corner, select **Tenant Guest** and **Tenant Administrator**, and click Next.



Policy/Role Name	Type
CS Tenant Admin	System-defined role
CS Tenant User	System-defined role
CloudPipeline Tenant Extensions FullAccess	System-defined policy
CloudPipeline Tenant Pipeline Templates FullAccess	System-defined policy
CloudPipeline Tenant Rule Templates FullAccess	System-defined policy
CloudPipeline Tenant Rules FullAccess	System-defined policy
DME AdministratorAccess	System-defined policy
Tenant Administrator (Exclude IAM)	System-defined role
Tenant Guest (Exclude IAM)	System-defined role

**Figure 1-13 Select Permissions**

Step 6 Click show more.



The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

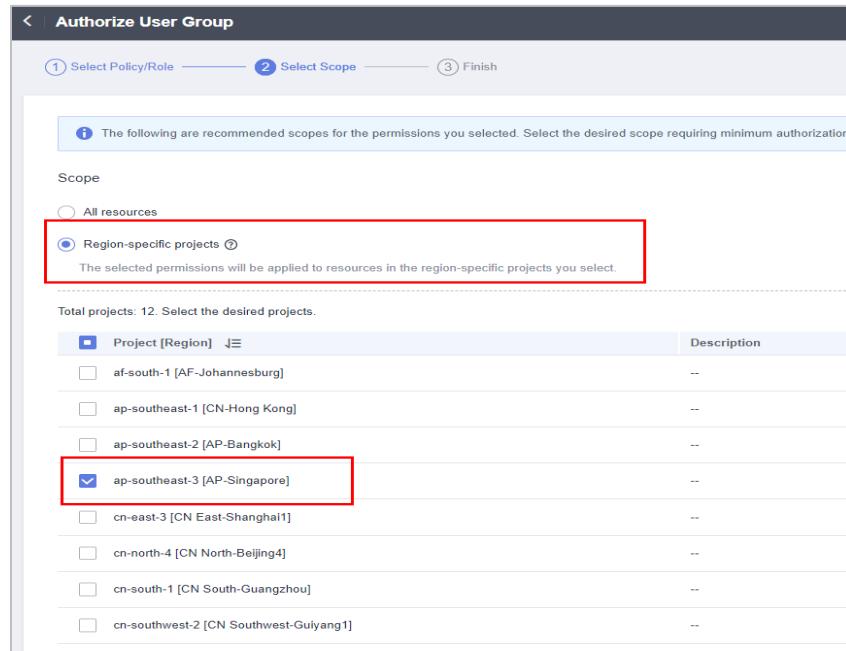
Scope

All resources

Show More

**Figure 1-14 Show More**

Step 7 Under Scope, click Region-specific projects, and select AP-Singapore, and click OK.



The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

All resources

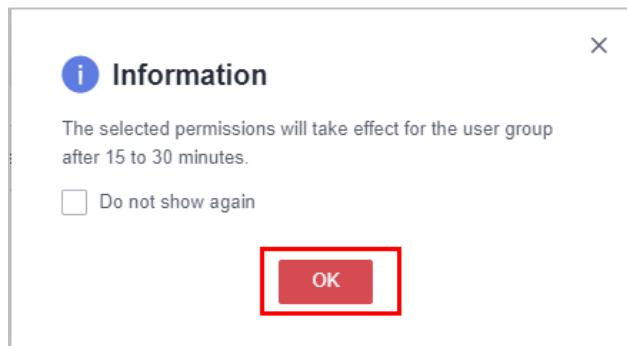
Region-specific projects ⓘ  
The selected permissions will be applied to resources in the region-specific projects you select.

Total projects: 12. Select the desired projects.

Project [Region]	Description
<input type="checkbox"/> af-south-1 [AF-Johannesburg]	--
<input type="checkbox"/> ap-southeast-1 [CN-Hong Kong]	--
<input type="checkbox"/> ap-southeast-2 [AP-Bangkok]	--
<input checked="" type="checkbox"/> ap-southeast-3 [AP-Singapore]	--
<input type="checkbox"/> cn-east-3 [CN East-Shanghai1]	--
<input type="checkbox"/> cn-north-4 [CN North-Beijing4]	--
<input type="checkbox"/> cn-south-1 [CN South-Guangzhou]	--
<input type="checkbox"/> cn-southwest-2 [CN Southwest-Guiyang1]	--

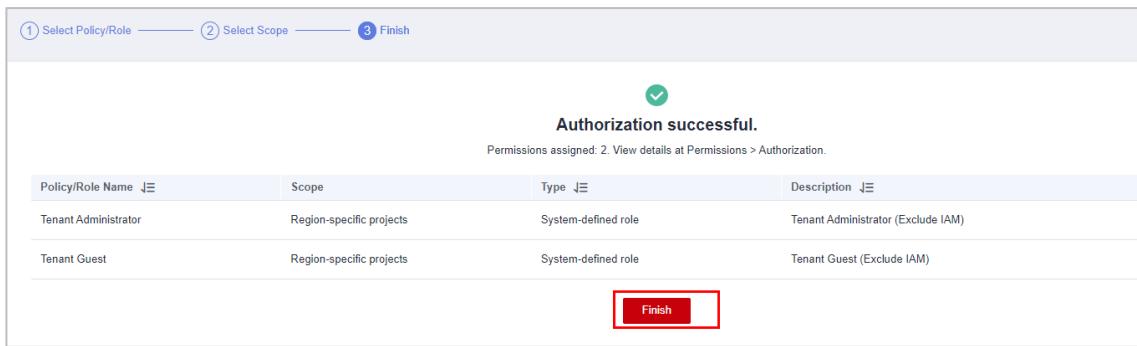
**Figure 1-15 Select the desired projects**

Step 8 On the Information page, click OK.



**Figure 1-16 Information Page**

Step 9 Comfirm all information, and Finish.



① Select Policy/Role ————— ② Select Scope ————— ③ Finish

✓ Authorization successful.

Permissions assigned: 2. View details at Permissions > Authorization.

Policy/Role Name	Scope	Type	Description
Tenant Administrator	Region-specific projects	System-defined role	Tenant Administrator (Exclude IAM)
Tenant Guest	Region-specific projects	System-defined role	Tenant Guest (Exclude IAM)

**Finish**

**Figure 1-17 Finish**

Step 10 Go to the **Users** page, and click **Create User** in the upper right.

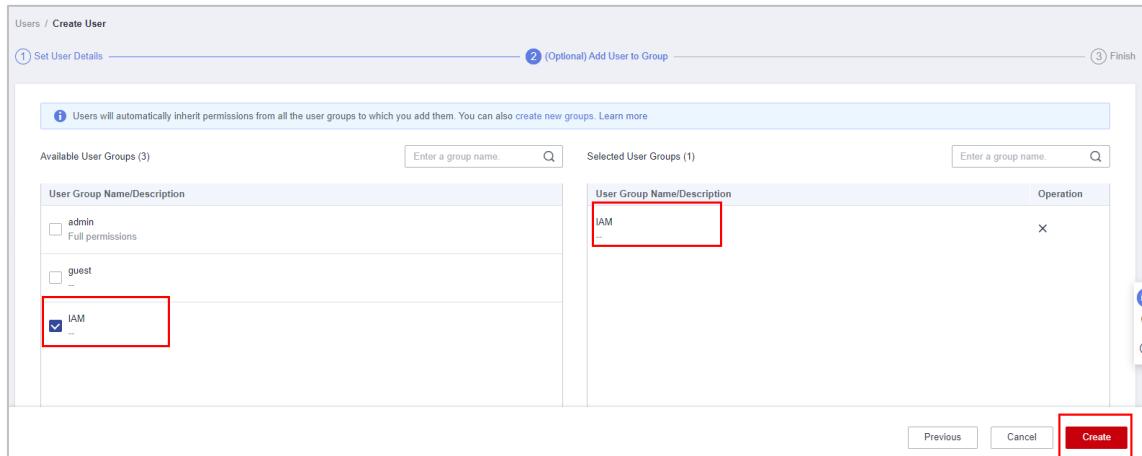
**Figure 1-18 Creating a user**

Step 11 Configure the user information and click **Next**.

- **Username:** a custom username. Here we'll use **myname**.
- Access Type: Management console access
- **Credential Type:** Select **Set now** and enter a password. Here we'll set it as **Huawei@135**. Then deselect **Require password reset at first login**.
- Login Protection: Disable

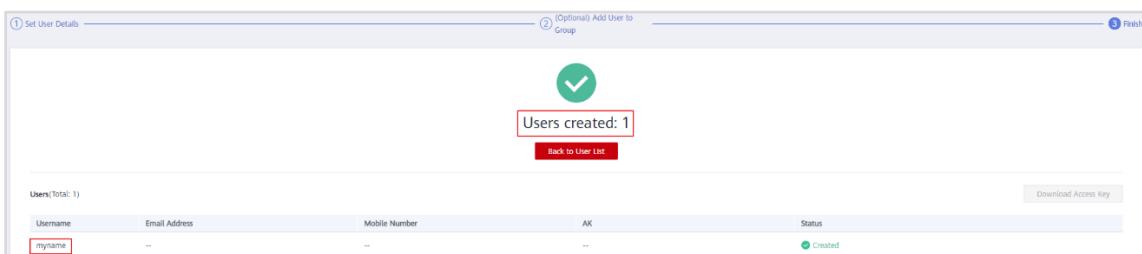
**Figure 1-19 Configuring the basic user information**

Step 12 Select the user group you created and click **Create**.



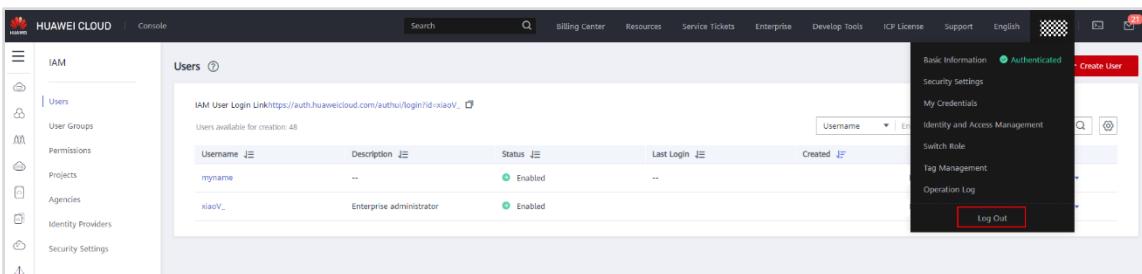
**Figure 1-20 Adding the user to the created user group**

Step 13 View the results. The user is created when you see this page.



**Figure 1-21 User created successfully**

Step 14 Log out of the account and log in again as the IAM user.



**Figure 1-22 Logging out of the account**

Step 15 Click IAM User.

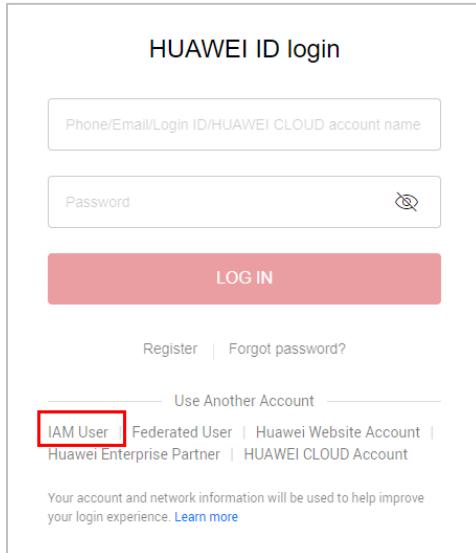


Figure 1-23 Clicking IAM User

Step 16 Log in as the IAM user you created.

- **Tenant name or HUAWEI CLOUD account name:** the name of the HUAWEI CLOUD account you have registered and authenticated
- **IAM user name or email address:** the name of the IAM user you created
- **IAM user password:** the password of the IAM user

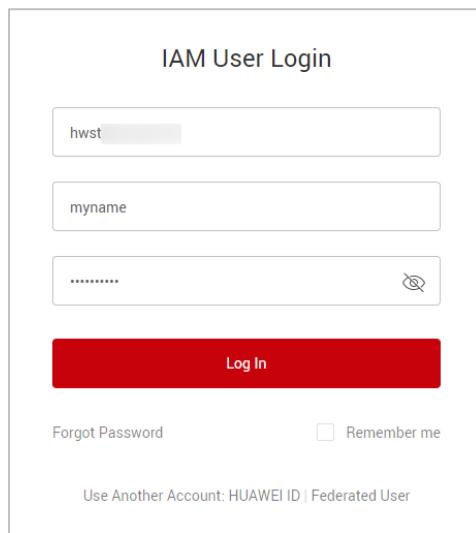
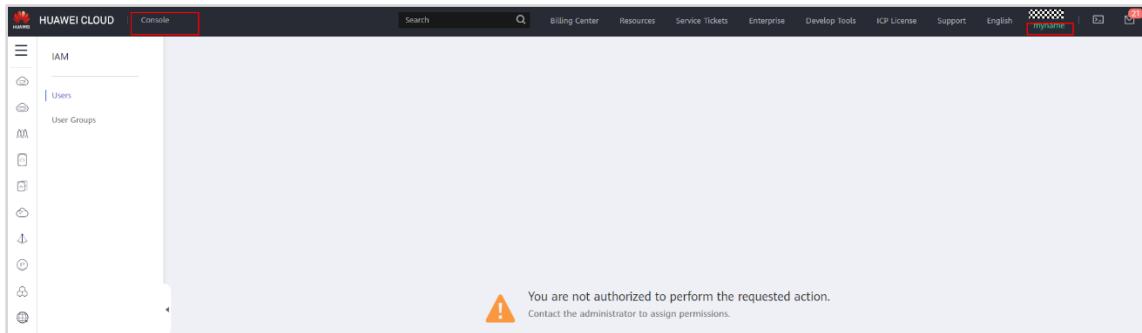


Figure 1-24 Logging in as an IAM user

Step 17 After login, click **Console** in the upper left. Your account is functioning normally if you see the home page of the console as shown here.



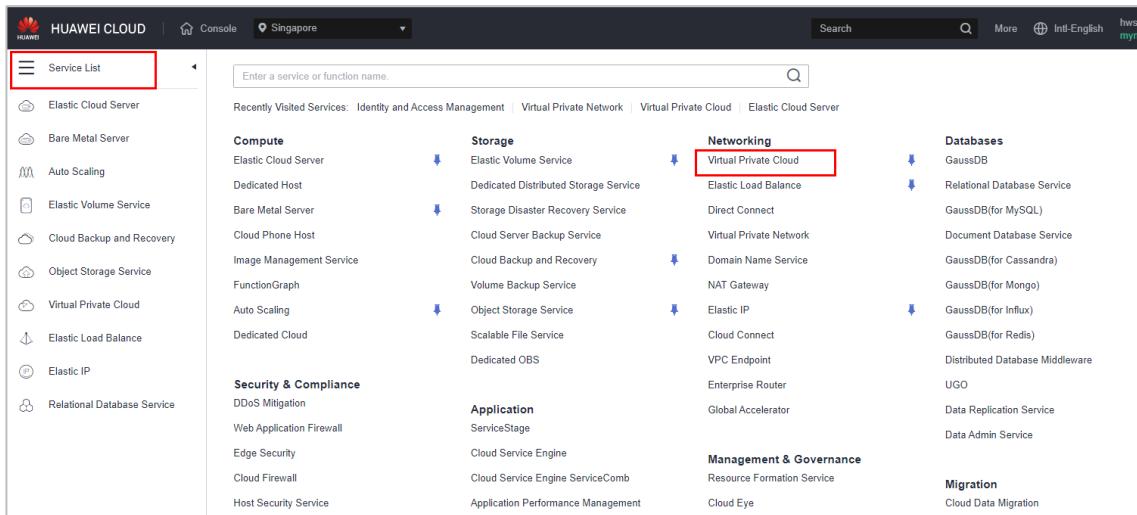
**Figure 1-25 IAM user login successful**

Congratulations. We've completed configuration in IAM.

## 1.2.4 Creating and Configuring a VPC

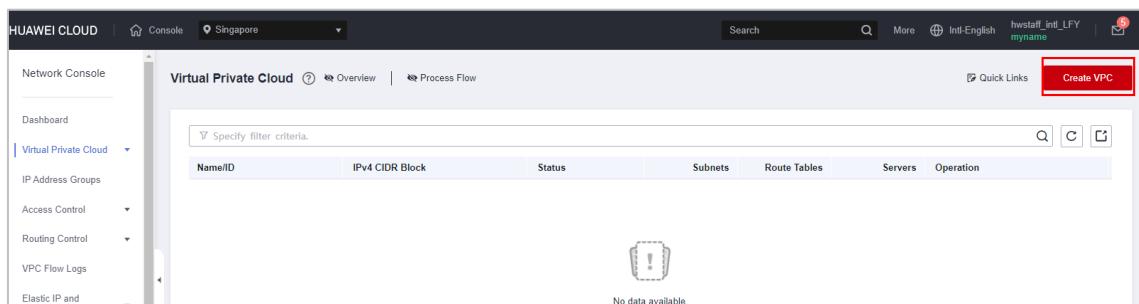
Next, let's create and configure a Virtual Private Cloud (VPC) and check that the IAM user has permissions to use resources.

**Step 1** Log in to the IAM server as an IAM user. (If you have logged in to the IAM server, you do not need to log in again.) Click **Console** and choose **Service List > Virtual Private Cloud**.



**Figure 1-26 Choosing Virtual Private Cloud**

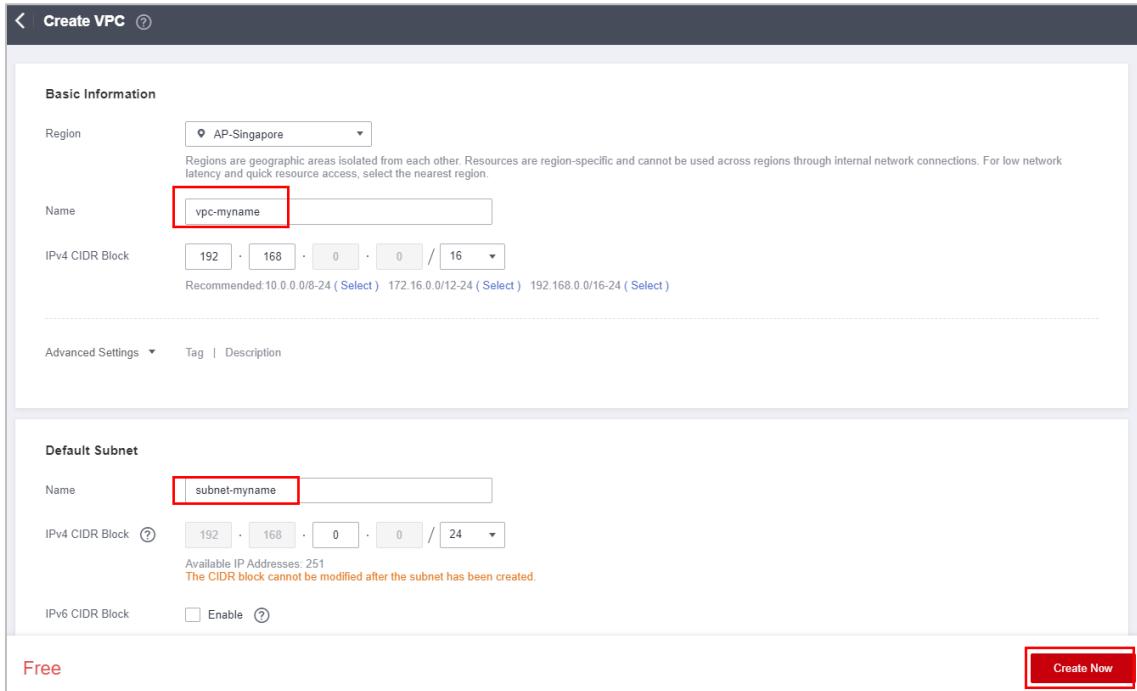
**Step 2** Click Create VPC.



**Figure 1-27 Creating a VPC**

### Step 3 Configure the VPC parameters and click **Create Now**.

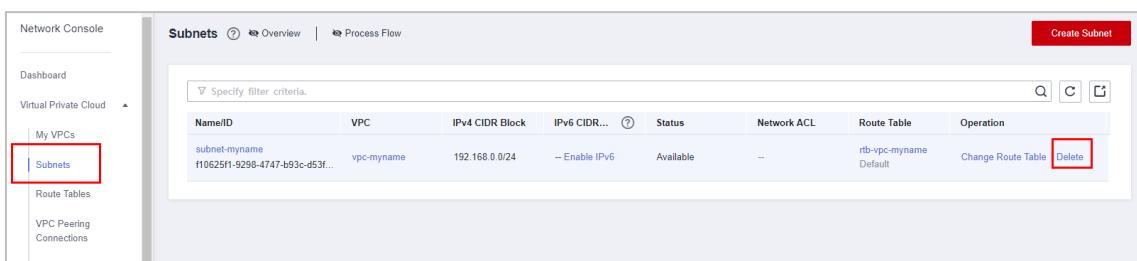
- Region: AP-Singapore
- Name: a custom name
- Retain the default settings for other parameters.



**Figure 1-28 Configuring the VPC**

After you created a VPC, you can create other Compute Instances or Storage resources in the VPC, and you can use the network resources in this VPC.

### Step 4 Delete the subnet of the VPC, you need to delete the subnet information first.



**Figure 1-29 Deleting the subnet**

### Step 5 Delete the VPC. When the number of subnets in the VPC to be deleted is 0, you can delete this VPC.

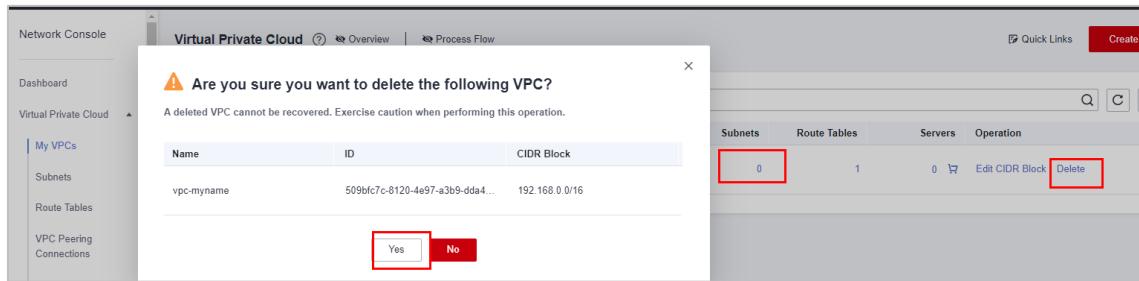


Figure 1-30 Deleting the VPC

## 1.3 Exercises

1. Create an IAM user with a custom name like **user1**.
2. Create a user group with a custom name like **group1**.
3. Grant the user group read-only permissions for the Enterprise Project Management (EPS) service.
4. Log in as the IAM user and check whether you can create a new VPC or modify the existing one.
5. Log in using the HUAWEI CLOUD account, release the VPC, and delete the IAM user and user group.

# 2 Compute Services

## 2.1 Introduction

### 2.1.1 About This Exercise

Elastic Cloud Server (ECS) provides scalable, on-demand computing cloud servers for secure, flexible, and efficient applications and ensures stable and interrupted running of services.

An image is a template used to create a server or disk.

Image Management Service (IMS) enables full-lifecycle management for images, templates used to create servers or disks, helping you quickly deploy services.

Auto Scaling (AS) automatically adjusts ECS instances based on your service requirements and configured AS policies. You can configure a scheduled, periodic, or alarm policy to adapt resources to the fluctuating service load, preventing unnecessary cloud service charges and ensuring services run stably.

This experiment introduces the comprehensive experiment of ECS, IMS, and AS. including creating and logging in to an ECS, modifying ECS resources, creating private images, creating shared images, and scaling resources.

### 2.1.2 Objectives

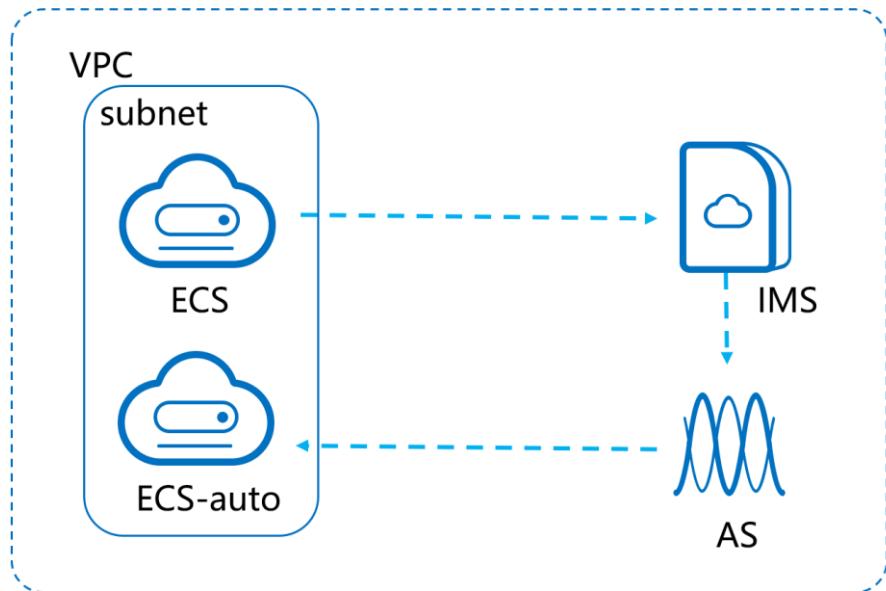
After completing this exercise, you will be able to master the basic operations of the three computing services (ECS, IMS, and AS). The details are as follows:

- How to Use ECSs
- Learn how to use IMS.
- Learn how to use the AS service.

## 2.2 Tasks

### 2.2.1 Roadmap

- Create and log in to an ECS.
- Modify ECS specifications.
- Create a Linux system disk image from an ECS.
- Modify and share an image.
- Create AS configurations, AS configuration groups, and AS policies.



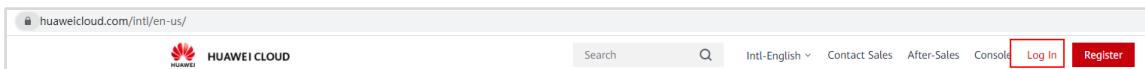
**Figure 2-1 Topology**

## 2.2.2 ECS Lifecycle Management

In this exercise, We only create ECSs running Linux. You can create a Windows private image to create a Windows ECS referring to the official document.

### 2.2.2.1 Creating Two Types of ECSs

Step 1 Go to [HUAWEI CLOUD official website](https://huaweicloud.com/intl/en-us/), and click **Log In** in the upper right corner.



**Figure 2-2 Logging in to HUAWEI COULD**

Step 2 Enter your username and password to log in, click **Console**, and choose the **AP-Singapore** region.

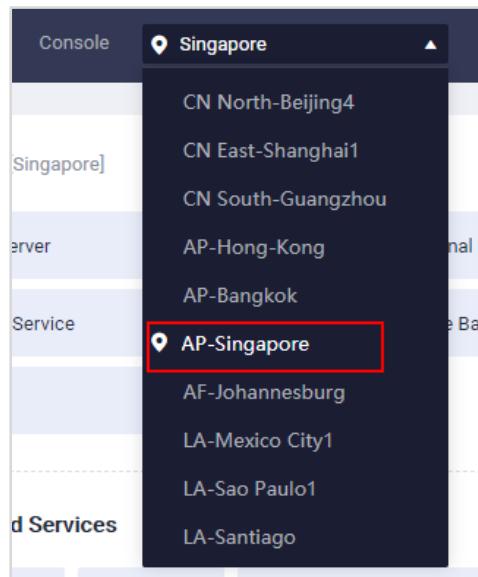


Figure 2-3 Choosing AP-Singapore

Step 3 In Service List on the left, choose Virtual Private Cloud.

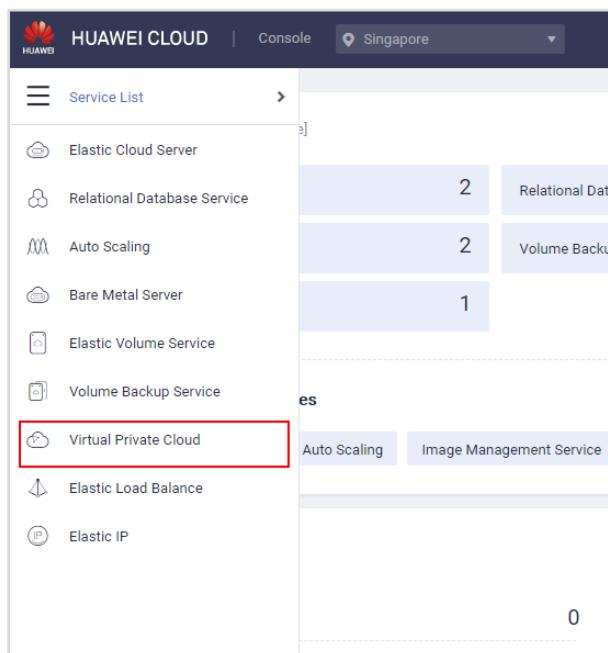
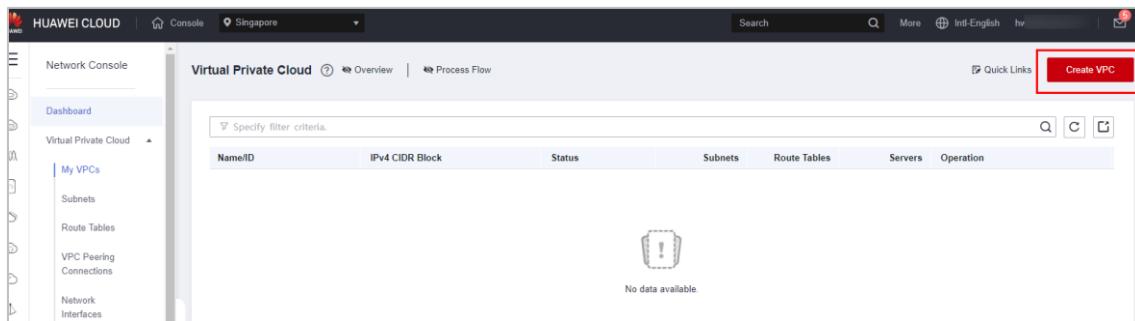


Figure 2-4 Choosing Virtual Private Cloud

Step 4 Click Create VPC.



**Figure 2-5 Create VPC**

Step 5 Configure the VPC parameters as follows and click **Create Now**.

- Region: AP-Singapore
- Name: Enter a name.
- Retain the default settings for other parameters.

Basic Information	
Region	AP-Singapore
Name	vpc-hcia
IPv4 CIDR Block	192 · 168 · 0 · 0 / 16
Advanced Settings Tag   Description	

Default Subnet	
Name	subnet-hcia
IPv4 CIDR Block	192 · 168 · 0 · 0 / 24
Available IP Addresses: 251 The CIDR block cannot be modified after the subnet has been created.	
IPv6 CIDR Block	<input type="checkbox"/> Enable
<b>Create Now</b>	

**Figure 2-6 Configuring the VPC**

Step 6 Switch to **Virtual Private Cloud** page and view the created VPC.

Name/ID	IPv4 CIDR Block	Status	Subnets	Route Tables	Servers	Operation
vpc-hcia 9f8a1474-95eb-4391-903b-156...	192.168.0.0/16 (Primary CIDR block)	Available	1	1	0	<a href="#">Edit CIDR Block</a>   <a href="#">Delete</a>

**Figure 2-7 Viewing the VPC**

Step 7 Click Service List on the left and choose Compute > Elastic Cloud Server.

The screenshot shows the HUAWEI CLOUD Console interface. At the top, there's a navigation bar with the HUAWEI logo, 'HUAWEI CLOUD', 'Console', 'Singapore', a search bar, and links for 'Billing Center', 'Resources', and 'Service Tickets'. Below the navigation is a 'Service List' sidebar with icons for various services like 'Elastic Cloud Server', 'Relational Database Service', 'Auto Scaling', etc. The main area is divided into four sections: 'Compute' (with 'Elastic Cloud Server' highlighted), 'Storage', 'Networking', and 'Databases'. Each section lists specific services like 'Virtual Private Cloud', 'Elastic Volume Service', etc.

**Figure 2-8 Choosing Elastic Cloud Server**

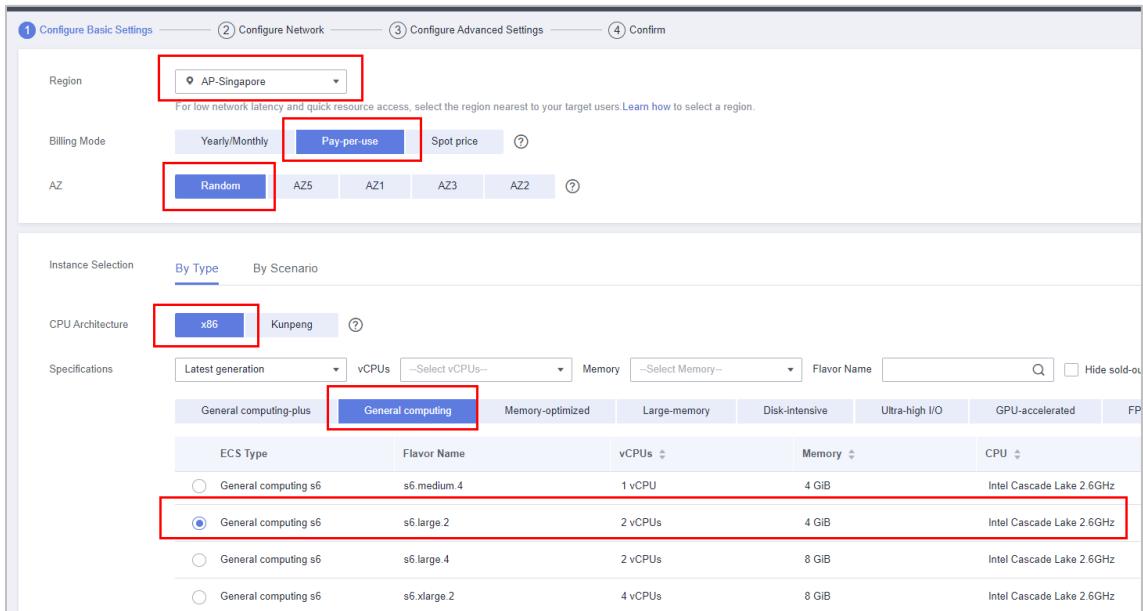
### Step 8 Click Buy ECS.

The screenshot shows the 'Elastic Cloud Server' console page. On the left is a sidebar with 'Cloud Server Console' and 'Elastic Cloud Server' selected. The main area has a heading 'Elastic Cloud Server' with a 'Buy ECS' button highlighted with a red box. Below it is a message about a password reset plug-in update. At the bottom is a search bar and a filter section with columns like 'Name/ID', 'Monitor...', 'Security', 'AZ', 'Status', 'Specification...', 'IP Address', 'Billing M...', 'Tag', and 'Operation'.

**Figure 2-9 Buy ECS**

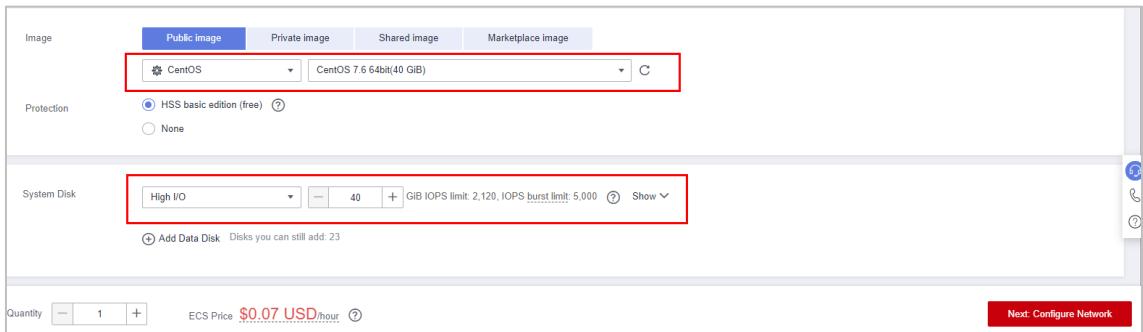
### Step 9 Configure basic settings as follows:

- Region: AP-Singapore
- Billing Mode: Pay-per-use
- AZ: Random
- CPU Architecture: x86
- Specifications: General computing, s6.large.2, 2 vCPUs | 4 GB (configure based on your requirements)



**Figure 2-10 Configure Basic Settings**

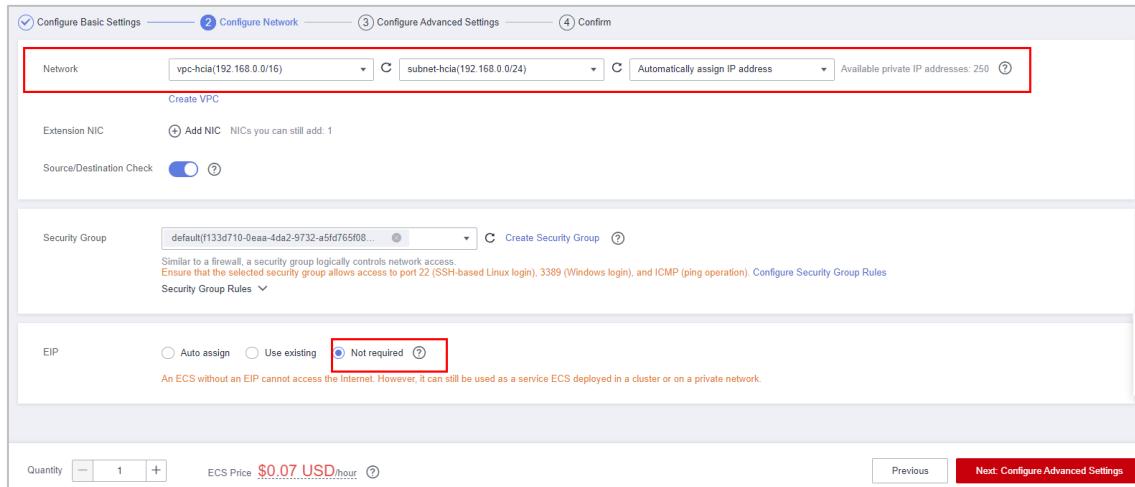
- **Image:** Public Image, CentOS, CentOS 7.6 64bit (40 GB)
- **Host Security:** HSS basic edition(free)
- **System Disk:** High I/O, 40 GB



**Figure 2-11 Configure Basic Settings**

Step 10 Click **Next: Configure Network**. The **Configure Network** page is displayed. Configure the parameters as follows:

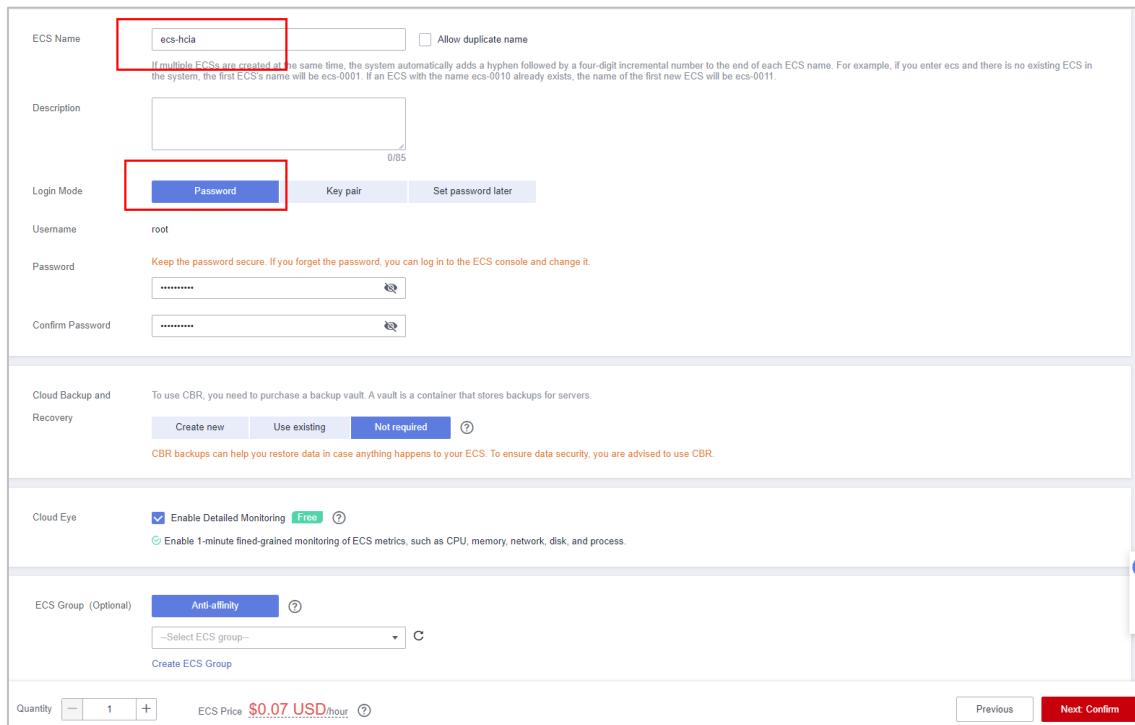
- **Network:** Choose the created VPC.
- **Extension NIC:** Retain the default settings.
- **Security Group:** Retain the default settings.
- **EIP:** Not required



**Figure 2-12 Configure Network**

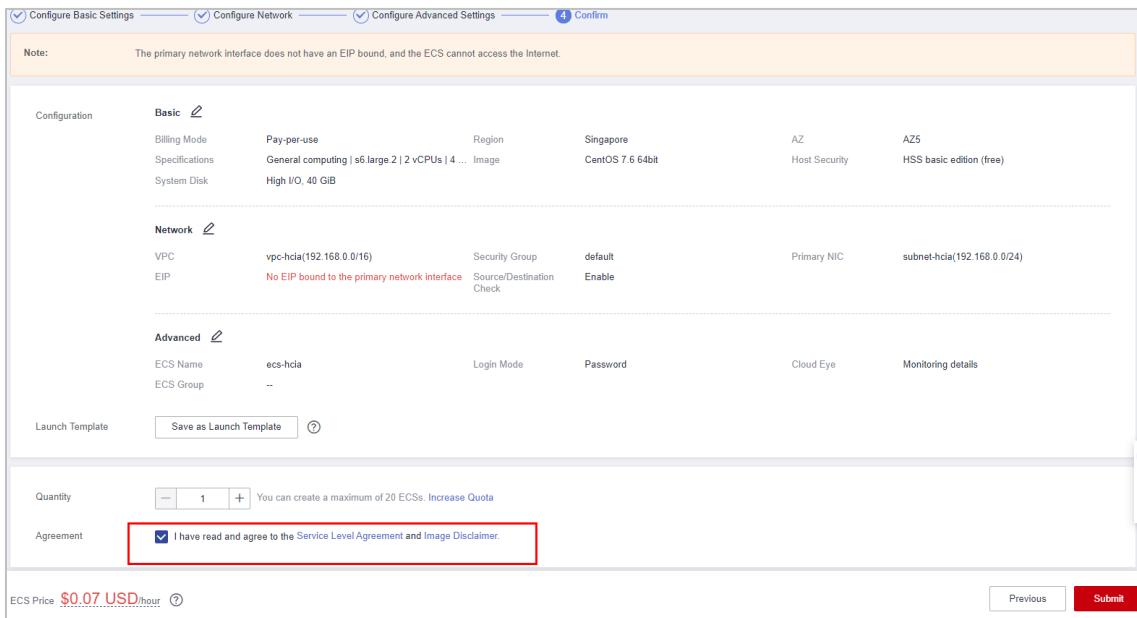
**Step 11** Click **Next: Configure Advanced Settings**. The **Configure Advanced Settings** page is displayed. Configure the parameters as follows:

- **ECS Name:** **ecs-hcia** (Change as required.)
- **Login Mode:** Password
- **Username:** root
- **Password:** Set your own password
- **Cloud Backup and Recovery:** Not required
- **ECS Group (Optional):** Retain the default settings
- **Advanced Options:** Retain the default settings

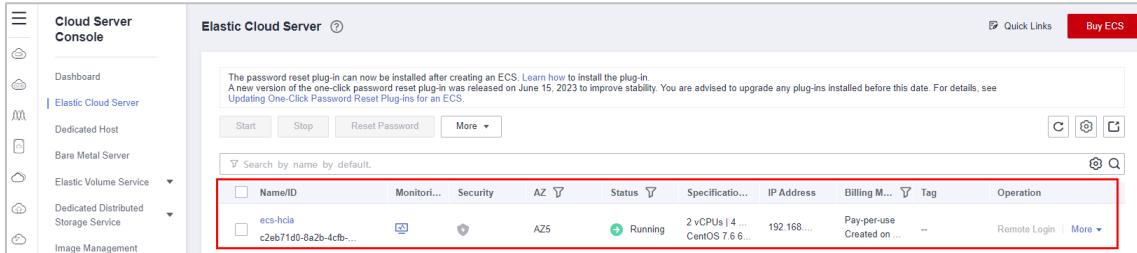


**Figure 2-13 Configure Advanced Settings**

**Step 12 Click Next: Confirm.** After confirming the ECS configurations, select **I have read and agree to the Service Level Agreement and Image Disclaimer**, and click **Submit**. After about 10 seconds, you can view the created ECS on the **Elastic Cloud Server** page. If the **Status** is **Running**, the ECS can work normally.



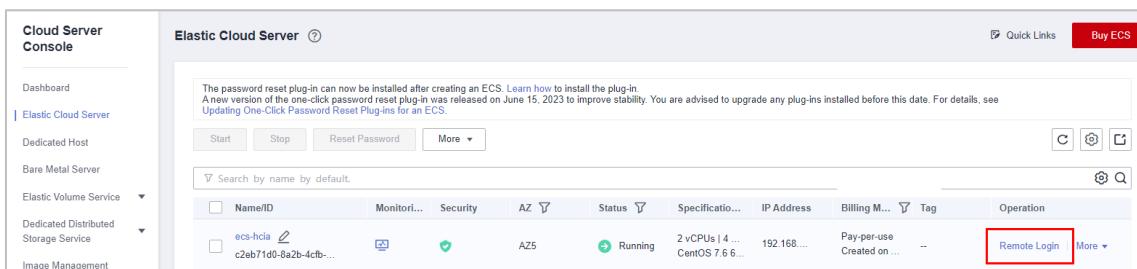
**Figure 2-14 Purchasing ECS**



**Figure 2-15 Viewing the created ECS**

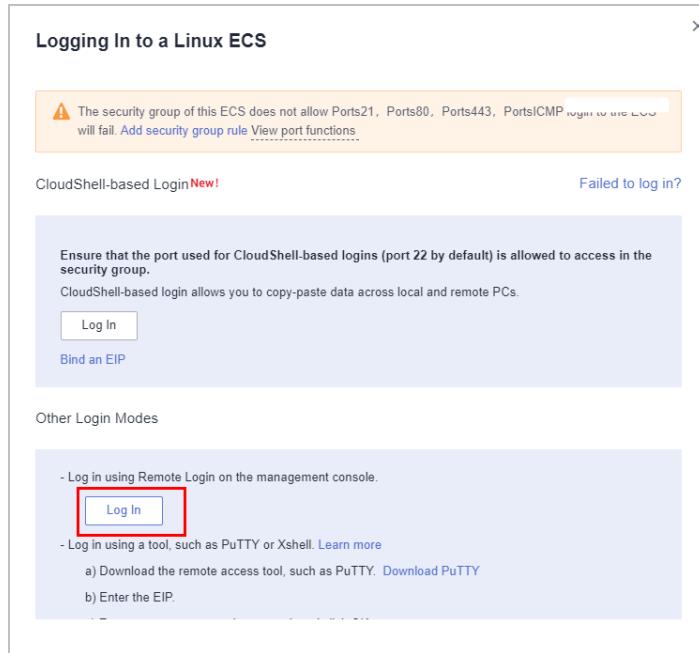
### 2.2.2.2 Logging In to an ECS

**Step 1 On the Elastic Cloud Server page, you can view the ECS AZ and its status. Click Remote Login in the Operation column on the right.**



**Figure 2-16 Remotely logging in to the ECS**

Step 2 The created ECS is not bound to an EIP. Therefore, you cannot log in to the ECS in CloudShell-based mode or remote login tools (SSH tool). So, Select **Other Login Modes** > Click **Log In**.



**Figure 2-17 Get Password**

Step 3 Click the CLI and enter the user name and password.

**ecs-hcia login: root**

**Password:** Enter a password, for example, **Huawei@1234**.

Linux ECSs do not have a GUI. After you log in the Linux ECS remotely, enter **root** after **ecs-linux login**, and then press **Enter** to input the password. The password is entered in ciphertext. Ensure that the password is correct before pressing **Enter**. If **Welcome to Huawei Cloud Service** is displayed, the ECS login was successful.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.92.1.el7.x86_64 on an x86_64

ecs-hcia login: root
Password:

Welcome to Huawei Cloud Service

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

**Figure 2-18 Successfully logging in to Linux**

If a page similar to the one in preceding figure is displayed, the Linux ECS login was successful.

### 2.2.2.3 Modifying ECS Specifications

Step 1 On the **Elastic Cloud Server** page, view the status of the target ECS.

Step 2 If the ECS is not in the stopped state, select it and click **Stop**. If the **Stop ECS** page is displayed, select **Forcibly stop the preceding ECSs** and click **Yes**.

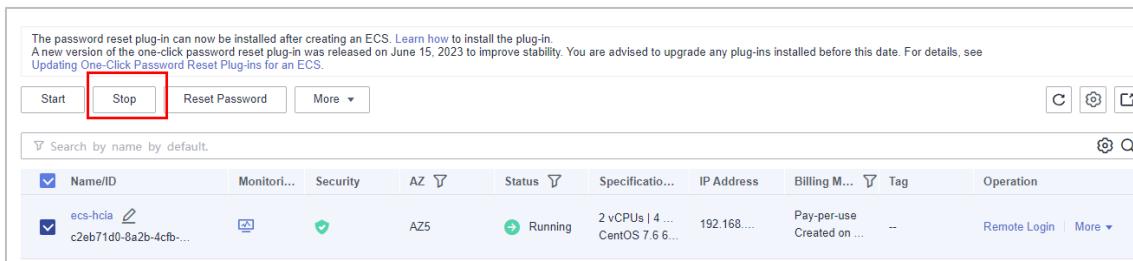


Figure 2-19 Stopping the ECS

Step 3 After the ECS has stopped, click **More** in the **Operation** column of this ECS and choose **Modify Specifications**.

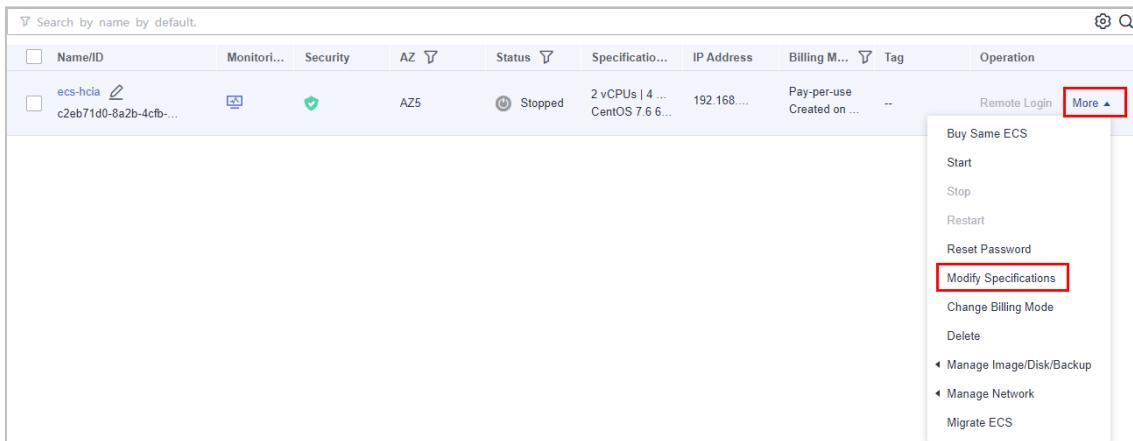


Figure 2-20 Modifying ECS Specifications

Step 4 In the **Modify Specifications** dialog box, select the desired ECS type, vCPUs, and memory size based on service requirements. In this exercise, the memory size is changed from 4 GB to 8 GB. Click **Next**.

Modify ECS Specifications

**Note** The ECS you are modifying is a pay-per-use ECS, so the price for vCPUs and memory may change. Do not perform other operations after you click Submit. Otherwise, ECS services may be interrupted. Modifying ECS specifications will not affect data in system and data disks.

Current Configuration							
ECS Name	ecs-hcia	ID	c2eb71d0-8a2b-4cfb-9d83-6f070a3c0edf				
Image	CentOS 7.6 64bit	Billing Mode	Pay-per-use				
Specifications	General computing   s6.large.2   2 vCPUs   4 GiB	Region	Singapore				
Latest generation <input type="button" value="vCPUs"/> <input type="button" value="Select vCPUs..."/> <input type="button" value="Memory"/> <input type="button" value="Select Memory..."/> Flavor Name <input type="text"/> <input type="button" value="Search"/>							
<input type="radio"/> General computing-plus <input checked="" type="radio"/> General computing <input type="radio"/> Memory-optimized <input type="button" value="?"/>							
ECS Type	Flavor Name	vCPUs	Memory	CPU	Assured / Maximum Bandwidth	Packets Per Second	<input type="button" value="?"/>
General computing s6	s6.medium.4	1 vCPU	4 GiB	Intel Cascade Lake 2...	0.1 / 0.8 Gbit/s	100,000 PPS	<input type="button" value="?"/>
General computing s6	s6.large.2	2 vCPUs	4 GiB	Intel Cascade Lake 2...	0.2 / 1.5 Gbit/s	150,000 PPS	<input type="button" value="?"/>
General computing s6	<b>s6.large.4</b>	2 vCPUs	8 GiB	Intel Cascade Lake 2...	0.2 / 1.5 Gbit/s	150,000 PPS	<input type="button" value="?"/>
General computing s6	s6.xlarge.2	4 vCPUs	8 GiB	Intel Cascade Lake 2...	0.35 / 2 Gbit/s	250,000 PPS	<input type="button" value="?"/>
ECS Price <b>\$0.08 USD/hour</b> <input type="button" value="?"/>							
<input type="button" value="Next"/>							

**Figure 2-21 Choosing target specifications**

**Step 5** After confirming the new ECS specifications, select **I have read and agree to the Image Disclaimer** and click **Submit**. Go to the **Elastic Cloud Server** page and you will see that the ECS status is **Resized**.

Modify ECS Specifications

**Details**

Resource	Configuration	Current Specifications	New Specifications	Price
Elastic Cloud Server	ECS Name: ecs-hcia ID: c2eb71d0-8a2b-4cfb-9d83-6f070a3c0edf Billing Mode: Pay-per-use	General computing s6.large.2   2 vCPUs   4 GiB	General computing <b>s6.large.4</b>   2 vCPUs   8 GiB	<b>\$0.08 /hour</b>

I have read and agree to the Image Disclaimer

ECS Price **\$0.08 USD/hour**

**Figure 2-22 Comfirm Specifications**

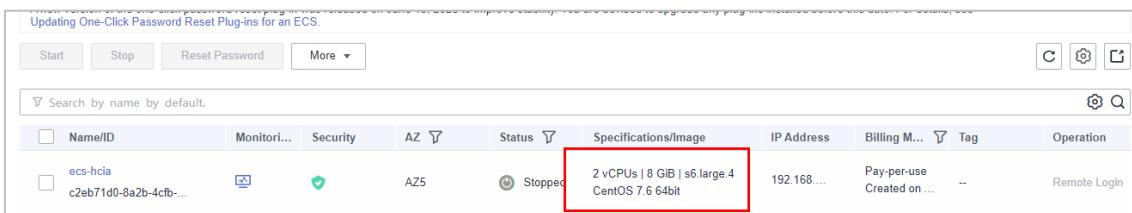
Elastic Cloud Server

The password reset plug-in can now be installed after creating an ECS. Learn how to install the plug-in. A new version of the one-click password reset plug-in was released on June 15, 2023 to improve stability. You are advised to upgrade any plug-ins installed before this date. For details, see Updating One-Click Password Reset Plug-ins for an ECS.

Name/ID	Monitor...	Security	AZ	Status	Specificatio...	IP Address	Billing M...	Tag	Operation
ecs-hcia c2eb71d0-8a2b-4cfb...			AZ5		2 vCPUs   8 ... CentOS 7.6 6...	192.168 ...	Pay-per-use Created on ...	--	Remote Login   More <input type="button" value="?"/>

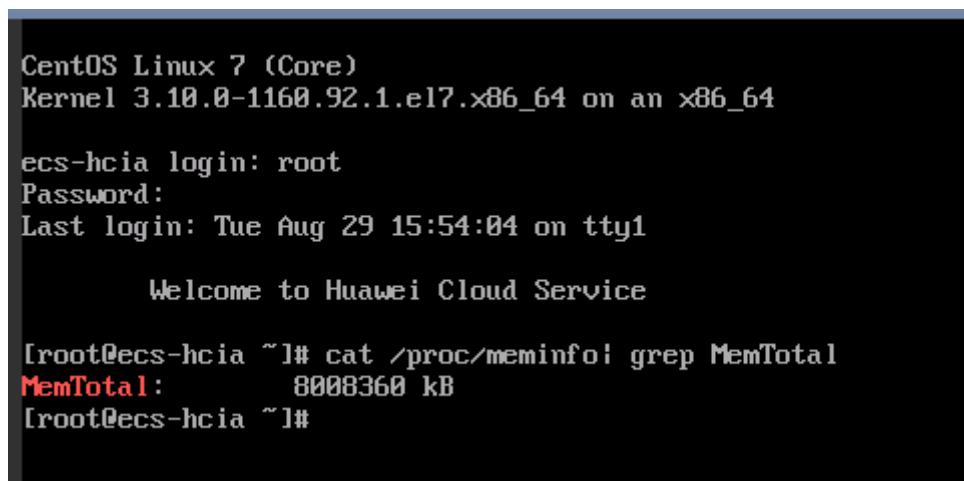
## Figure 2-23 Specifications modifying

Step 6 Start the ECS. The ECS specifications have been modified.



## Figure 2-24 Specifications modified

Step 7 You can also log in to the ECS to check the new specifications, as shown in the following figure.



## Figure 2-25 Confirming new specifications

### 2.2.3 Creating a Linux System Disk Image from an ECS

If you have created and configured a Linux ECS based on your service requirements (for example, by installing software and setting up an application environment), you can create a system disk image based on this configured ECS. Then, all new ECSs created from this image will have the same software and environment preinstalled.

To create a Linux system disk image using an ECS, you need to configure a Linux ECS and then use it to create a system disk image.

#### 2.2.3.1 Configuring a Linux ECS

Take the **ecs-hcia** ECS you created as an example.

Step 1 Remotely log in to the ECS.

Step 2 Check whether DHCP is configured for the ECS NICs. If it is not, configure it.

For CentOS or EulerOS, you can configure DHCP by adding **PERSISTENT\_DHCLIENT="y"** to the **/etc/sysconfig/network-scripts/ifcfg-ethX** configuration file using the vi editor.

```
[root@ecs-hcia ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
```

```
BOOTPROTO="dhcp"
ONBOOT="yes"
TYPE="Ethernet"
PERSISTENT_DHCLIENT="yes"
[root@ecs-hcia ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Step 3 Check whether the one-click password reset plug-in has been installed on the ECS. If it is not, install it.

Note: To ensure that you can reset the passwords of the new ECSs created from a private image, you are advised to install the one-click password reset plug-in (CloudResetPwdAgent) on the ECS used to create the image. For details, see [Installing the One-Click Password Reset Plug-In](#).

- In this exercise, the ECS is created from a public image. Therefore, the one-click password reset plug-in has been installed on it by default. You do not need to manually install it. You can run the following command to check whether CloudResetPwdAgent has been installed.
- If the following information is displayed, the plug-in has been installed:

```
[root@ecs-hcia ~]# ls -lh /Cloud*
/CloudResetPwdUpdateAgent:
total 20K
drwx----- 2 root root 4.0K Jul 22 19:38 bin
drwxr-xr-x 2 root root 4.0K Feb 10 2022 conf
drwx----- 3 root root 4.0K Feb 10 2022 depend
drwx----- 2 root root 4.0K Feb 10 2022 lib
drwx----- 2 root root 4.0K Jul 22 19:38 logs

/CloudrResetPwdAgent:
total 16K
drwx----- 2 root root 4.0K Jul 22 19:38 bin
drwxr-xr-x 2 root root 4.0K Feb 10 2022 conf
drwx----- 2 root root 4.0K Feb 10 2022 lib
drwx----- 2 root root 4.0K Feb 10 2022 logs
[root@ecs-hcia ~]#
```

Step 4 (optional) Check whether Cloud-Init is installed. If it is not, install it.

Note:

- If Cloud-Init is not installed on the ECS, custom information cannot be injected into the new ECSs created from the private image and you can only log in to the ECSs with the password specified in the image.
- For an ECS created from a public image, Cloud-Init has been installed on it by default. You do not need to manually install Cloud-Init for it.
- For an ECS created using an external image file, you need to install Cloud-Init for the ECS before you use it to create a private image. For details, see [Installing Cloud-Init](#) and [Configuring Cloud-Init](#).

In this exercise, the ECS is created from the public image **CentOS 7.6 64bit(40GB)**. Cloud-Init has been installed on it by default. You can run the following command to check whether Cloud-Init has been installed:

```
[root@ecs-hcia ~]# rpm -qa |grep cloud-init  
[root@ecs-hcia ~]#
```

- If information similar to the following is displayed, Cloud-Init has been installed, or use which cloud-init:

```
[root@ecs-hcia ~]# which cloud-init  
/usr/local/bin/cloud-init  
[root@ ecs-hcia ~]#
```

- If no command output is displayed, Cloud-Init is not installed. Run the following commands to install it (before the installation, make sure an EIP is bound to the ECS so that the ECS can access the Internet):

```
[root@ecs-hcia ~]# yum install https://archives.fedoraproject.org/pub/archive/epel/6/x86_64/epel-release-xx-xx.noarch.rpm  
[root@ecs-hcia ~]# yum install cloud-init
```

Run the following commands to enable Cloud-Init to automatically start upon system boot:

```
[root@ecs-hcia ~]# systemctl enable cloud-init-local.service cloud-init.service cloud-config.service  
cloud-final.service  
[root@ecs-hcia ~]# systemctl status cloud-init-local.service cloud-init.service cloud-config.service  
cloud-final.service
```

#### Step 5 Delete files from the network rule directory.

Note: To prevent NIC name drift on the new ECSs created from a private image, you need to delete network rule files of the ECS used to create the image.

Run the following command to check if there is a network rule file on the ESC:

```
[root@ecs-hcia ~]# ls -l /etc/udev/rules.d  
total 0  
[root@ecs-hcia ~]#
```

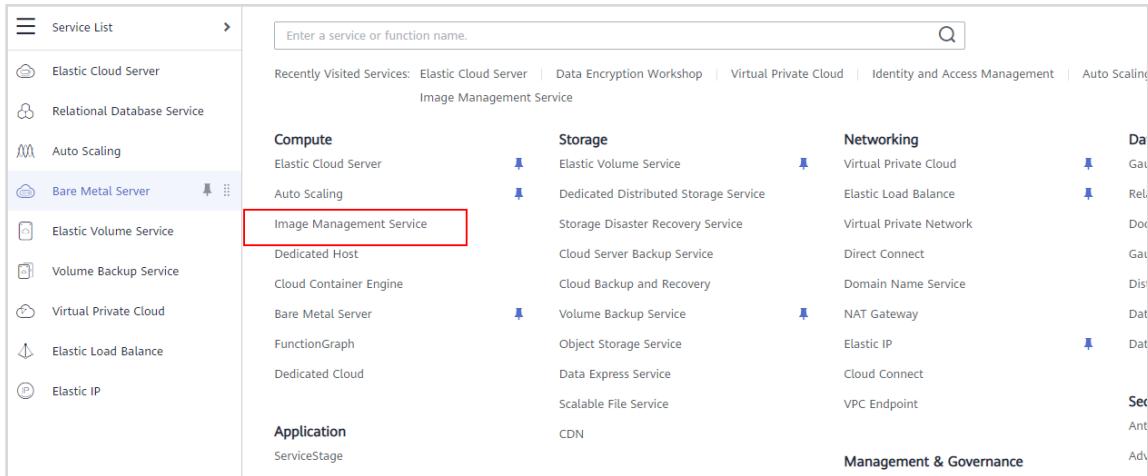
If information similar to the following is displayed, no network rule files exist:

Note:

- An ECS created from a public image does not have network rule files by default.
- An ECS created using an external image file may have network rule files, delete the files by following the instructions provided in [Deleting Files from the Network Rule Directory](#).

## 2.2.3.2 Creating a Linux Private Image

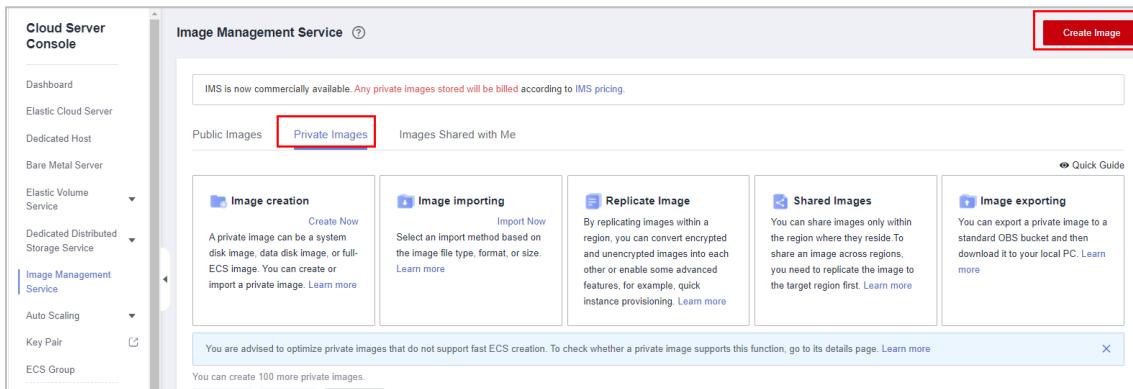
Step 1 Go back to the management console and in **Service List** choose **Compute > Image Management Service**.



The screenshot shows the 'Service List' page in the Huawei Cloud management console. On the left, there's a sidebar with various service icons. In the main area, services are categorized into groups: Compute, Storage, Networking, Application, and Management & Governance. Under the 'Compute' group, 'Image Management Service' is listed and highlighted with a red box. Other services in this group include Elastic Cloud Server, Auto Scaling, Bare Metal Server, Elastic Volume Service, Volume Backup Service, Virtual Private Cloud, Elastic Load Balance, and Elastic IP.

**Figure 2-26 Accessing IMS**

Step 2 On the Image Management Service page, click **Create Image**.



The screenshot shows the 'Image Management Service' page. On the left, there's a sidebar with 'Cloud Server Console' and a list of services like Dashboard, Elastic Cloud Server, Dedicated Host, Bare Metal Server, etc. The 'Image Management Service' option is selected. The main area has tabs for 'Public Images' (selected) and 'Private Images'. Below these tabs are five cards: 'Image creation' (Create Now), 'Image importing' (Import Now), 'Replicate Image', 'Shared Images', and 'Image exporting'. In the top right corner, there's a large red box around the 'Create Image' button.

**Figure 2-27 Creating a private image**

Step 3 Set the following parameters on the **Create Image** page and click **Next**.

- **Type:** System disk image
- **Source:** Select a Linux ECS, for example, **ecs-linux**.
- **Name:** Enter a name, for example, **image-centos7.6**

**Image Type and Source**

\* Region: AP-Singapore

\* Type: Create Image

\* Image Type: System disk image (highlighted with a red box)

\* Source: ECS (highlighted with a red box)

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

**Image Information**

Encryption: Unencrypted

\* Name: image-centos7.6 (highlighted with a red box)

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

**Next**

**Figure 2-28 Setting private image parameters**

Step 4 Confirm the settings. Then, select I have read and agree to the Image Disclaimer and click **Submit**.

Step 5 Switch back to the **Private Images** tab page to view the image status.

The time required for creating an image depends on the image size. Generally, it takes about 10 to 20 minutes. When the image creation completes, its status changes to **Normal**.

Name	Status	OS Type	OS	Image T...	Disk Ca...	Encrypted	Created	Operation
image-centos7.6 0850bad2-fc67-45ff-95f4...	Normal	Linux	CentOS 7.6 ...	ECS system...	40	No		Apply for Server   Modify   More ▾

**Figure 2-29 Viewing the private image status**

### 2.2.3.3 Modifying Image Information

Step 1 Locate the row that contains the image to be modified and click **Modify** in the **Operation** column.

You can create 100 more private images.								
<a href="#">Delete</a> <a href="#">Share</a> <a href="#">Export</a>								
<input type="text"/> Search or filter by keyword.								
Name	Status	OS Type	OS	Image T...	Disk Ca...	Encrypted	Created	Operation
image-centos7.6 085dbad2-fc67-45ff-95f4...	<input checked="" type="checkbox"/> Normal	Linux	CentOS 7.6 ...	ECS system...	40	No		<a href="#">Apply for Server</a> <a href="#">Modify</a> <a href="#">More</a>

**Figure 2-30 Modifying image information**

Step 2 You can modify the image name, memory, and other details.

### Modify Image

★ Name	<input type="text" value="image-centos7.6"/>
Description	<div style="border: 1px solid #ccc; height: 100%; width: 100%;"></div> <p style="margin-top: -20px;">0/1,024</p>
Minimum Memory	<small>Ensure that the minimum memory size of an image is set to its original size before you reinstall OSs of the ECSs that were created using the image.</small>
	<input checked="" type="button" value="Unlimited"/> <input type="button" value="1 GiB"/> <input type="button" value="2 GiB"/> <input type="button" value="4 GiB"/> <input type="button" value="8 GiB"/> <input type="button" value="16 GiB"/> <input type="button" value="32 GiB"/>
	<input type="button" value="64 GiB"/> <input type="button" value="128 GiB"/>
Maximum Memory	<input checked="" type="button" value="Unlimited"/> <input type="button" value="4 GiB"/> <input type="button" value="32 GiB"/> <input type="button" value="64 GiB"/> <input type="button" value="128 GiB"/>
NIC Multi-Queue	<input checked="" type="button" value="Supported"/> <input type="button" value="Not supported"/>
Boot Mode	<input checked="" type="button" value="BIOS"/> <input type="button" value="UEFI"/>
	<small>The boot mode must be the same as that of the OS contained in the image file. Otherwise, ECSs created from this system disk image will fail to start.</small>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Figure 2-31 Parameters for image modification**

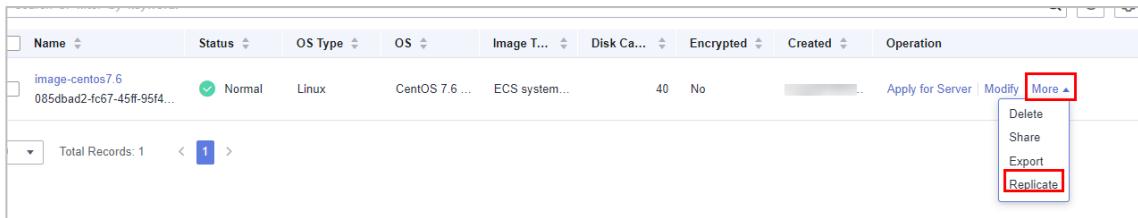
#### 2.2.3.4 Replicating an Image Within a Region

Step 1 On the **Image Management Service** page, click **Private Image** to display the image list.

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. <a href="#">Learn more</a>								
You can create 100 more private images.								
<a href="#">Delete</a> <a href="#">Share</a> <a href="#">Export</a>								
<input type="text"/> Search or filter by keyword.								
Name	Status	OS Type	OS	Image T...	Disk Ca...	Encrypted	Created	Operation
image-centos7.6 085dbad2-fc67-45ff-95f4...	<input checked="" type="checkbox"/> Normal	Linux	CentOS 7.6 ...	ECS system...	40	No		<a href="#">Apply for Server</a> <a href="#">Modify</a> <a href="#">More</a>

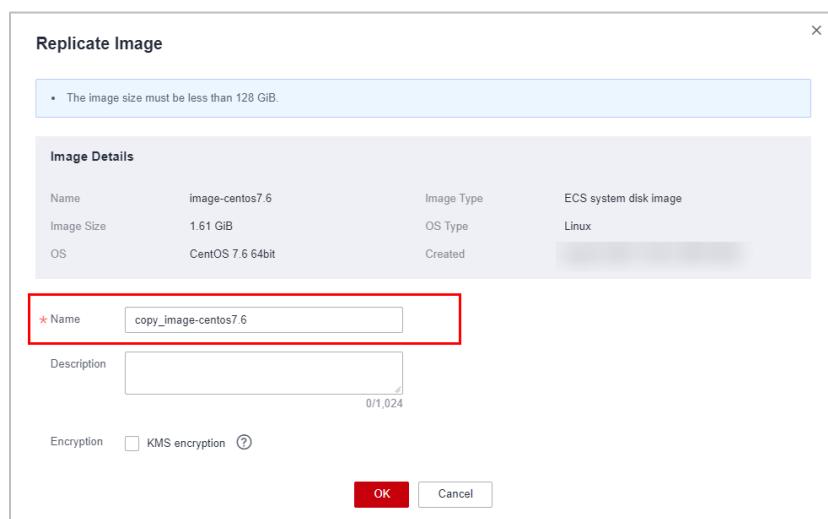
**Figure 2-32 Viewing private images**

Step 2 Locate the row that contains the image to be replicated and in the **Operation** column choose **More > Replicate**.



**Figure 2-33 Replicating a private image**

Step 3 In the displayed **Replicate Image** dialog box, enter a new name for the image and click **OK**. (Do not select **KMS encryption**.)



**Figure 2-34 Parameters for in-region image replication**

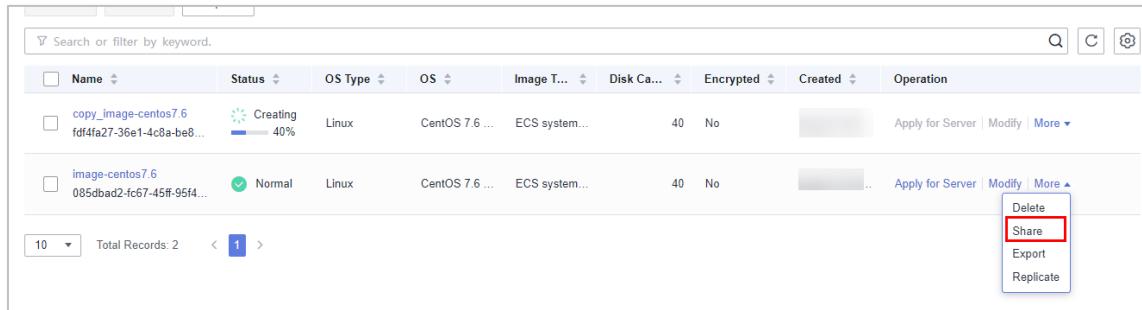


**Figure 2-35 Replicated image**

### 2.2.3.5 Sharing an Image

You can share your images with other users. Before sharing images with a user, you need to obtain their account names (if the user is a DeC or multi-project user, you also need to obtain the project name). You can share a single image or multiple images as needed.

Step 1 On the **Private Images** tab page, select the private image to be shared and in the **Operation** column choose **More > Share**.



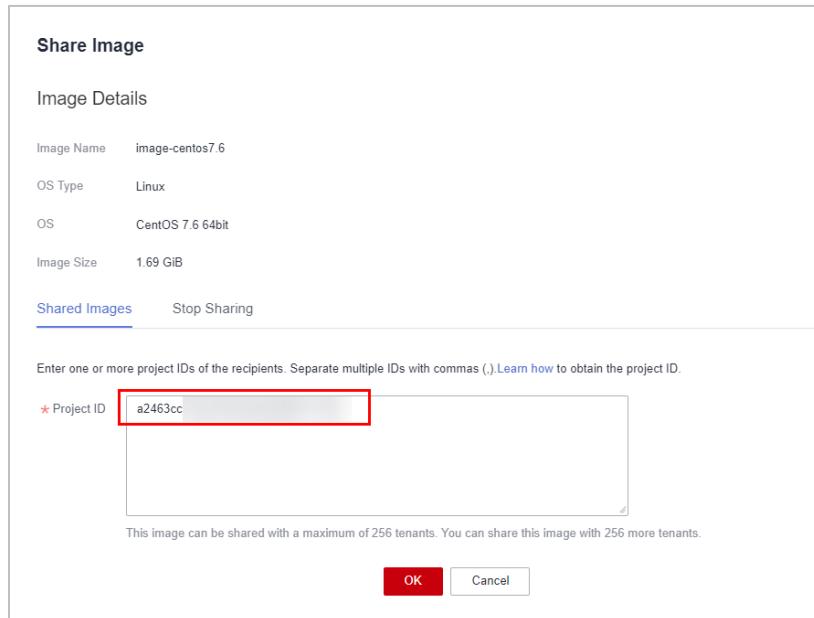
Name	Status	OS Type	OS	Image T...	Disk Ca...	Encrypted	Created	Operation
copy_image-centos7.6 fdf4fa27-36e1-4c8a-be8...	Creating 40%	Linux	CentOS 7.6 ...	ECS system...	40	No		Apply for Server   Modify   More ▾
image-centos7.6 085dbad2-fc67-45ff-95f4 ...	Normal	Linux	CentOS 7.6 ...	ECS system...	40	No		Apply for Server   Modify   More ▾

10 Total Records: 2 < 1 >

**Figure 2-36 Sharing a private image**

Step 2 In the **Share Image** dialog box, enter the Project ID of the target user and click **Add**. Click **OK**.

Before a tenant shares an image with you, you need to provide target project ID. To see How to [Obtaining the Project ID](#).



**Share Image**

**Image Details**

Image Name	image-centos7.6
OS Type	Linux
OS	CentOS 7.6 64bit
Image Size	1.69 GiB

**Shared Images** Stop Sharing

Enter one or more project IDs of the recipients. Separate multiple IDs with commas (,). [Learn how to obtain the project ID](#).

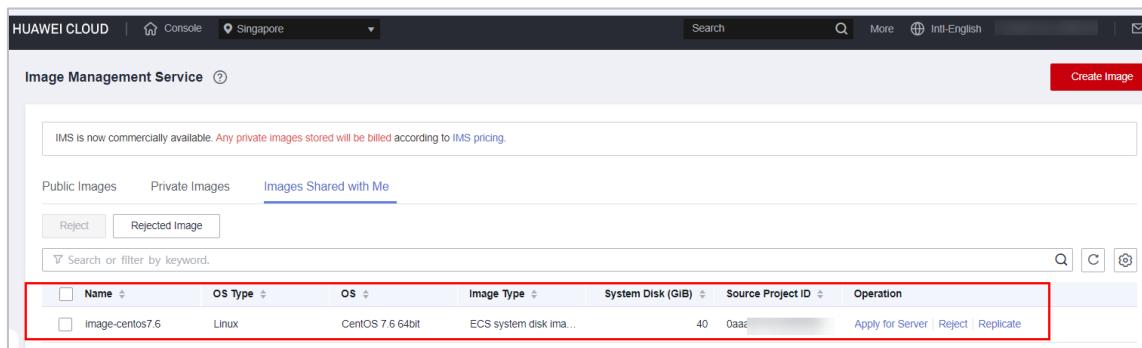
\* Project ID

This image can be shared with a maximum of 256 tenants. You can share this image with 256 more tenants.

OK Cancel

**Figure 2-37 Sharing an image**

Step 3 Log in to the management console using the account of the target user, go to the IMS console, click the **Images Shared with Me** tab, and click **Accept**.



Name	OS Type	OS	Image Type	System Disk (GiB)	Source Project ID	Operation
image-centos7.6	Linux	CentOS 7.6 64bit	ECS system disk ima...	40	0aa6	Apply for Server   Reject   Replicate

**Figure 2-38 Accepting the shared image**

## 2.2.3.6 Adding Tenants Who Can Use Shared Images

Step 1 On the **Image Management Service** page, click **Private Image** to display the image list.

Search or filter by keyword.										
	Name	Status	OS Type	OS	Image T...	Disk Ca...	Encrypted	Created	Operation	
<input type="checkbox"/>	copy_image-centos7.6 fdf4fa27-36e1-4c6a-be8...	<span style="color: green;">Normal</span>	Linux	CentOS 7.6 ...	ECS system...	40	No		<a href="#">Apply for Server</a>   <a href="#">Modify</a>   <a href="#">More</a> ▾	
<input type="checkbox"/>	image-centos7.6 085dbad2-fc67-45ff-95f4...	<span style="color: green;">Normal</span>	Linux	CentOS 7.6 ...	ECS system...	40	No		<a href="#">Apply for Server</a>   <a href="#">Modify</a>   <a href="#">More</a> ▾	

Figure 2-39 Viewing private images

Step 2 Click the name of the image to be shared. On the **Shared with Tenants** tab page, click **Add Tenant**.

image-centos7.6		Apply for Server	
Name	image-centos7.6	ID	085dbad2-fc67-45ff-95f4-24416324c1ce
Image Type	System disk image	Disk Capacity (GiB)	40
OS	CentOS 7.6 64bit	Status	<span style="color: green;">Normal</span>
Minimum Memory	Unlimited	Image Size	1.69 GiB
Maximum Memory	Unlimited	Published	<a href="#">?</a> No
Created		Completed	
Source	ECS ecs-hcia	Description	--
Encrypted	No	OS Type	Linux
NIC Multi-Queue	Supported	Fast ECS Creation	<a href="#">?</a> Supported
<a href="#">Shared with Tenants</a>		Tags	
<a href="#">Delete All</a>		<a href="#">Add Tenant</a> You can add 255 more tenants.	
Project ID		Status	
a24f		Accepted	
		Operation	
		<a href="#">Delete</a>	

Figure 2-40 Adding tenants who can use the shared image

Step 3 In the **Add Tenant** dialog box, enter the project ID of the tenant to be added and click **OK**.

To add multiple tenants, enter their project IDs and separate them with commas. Click **OK**.

**Add Tenant**

! An image can be shared only inside its region.

Enter one or more project IDs of the recipients. Separate multiple IDs with commas (,). [Learn how to obtain the project ID](#).

\* Project ID

This image can be shared with a maximum of 256 tenants. You can share this image with 255 more tenants.

**OK**   **Cancel**

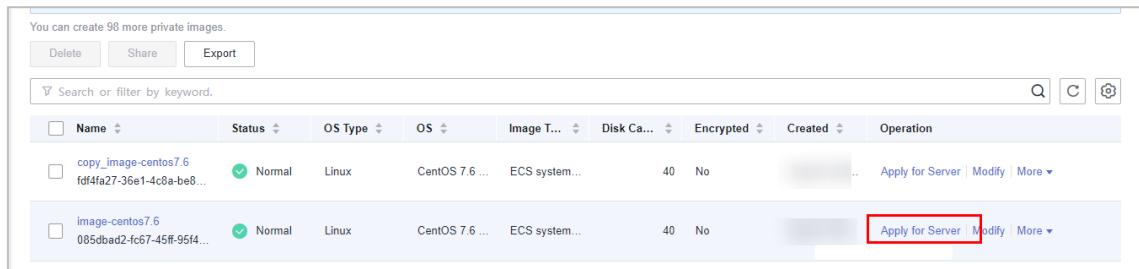
### Figure 2-41 Adding tenants

You can share images only within the region where they reside. To share an image across regions, you need to replicate the image to the target region first.

A project ID uniquely identifies a tenant in a specific region. If you enter a project ID that belongs to a different region from the images, a message will display indicating that the tenant cannot be found.

#### 2.2.3.7 Applying for an ECS Using a Private Image

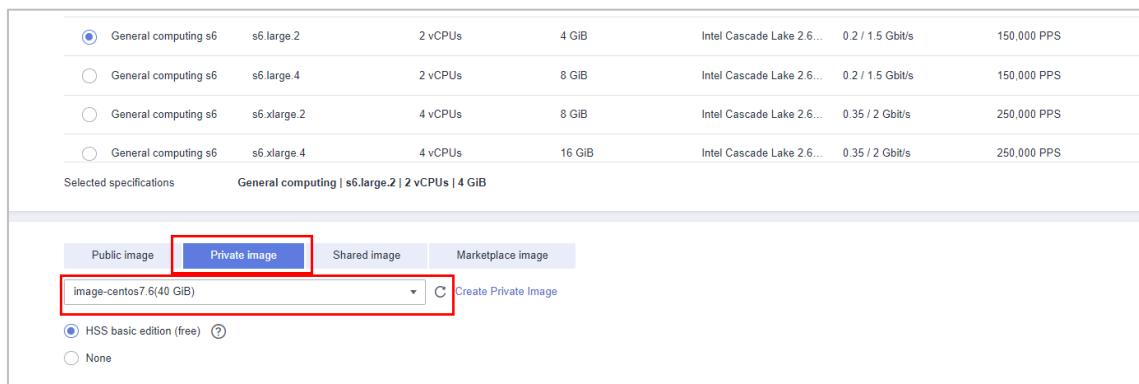
Step 1 On the **Private Images** tab page, locate the image and click **Apply for Server** in the **Operation** column.



Name	Status	OS Type	OS	Image T...	Disk Ca...	Encrypted	Created	Operation
copy_image-centos7.6 fdf4fa27-36e1-4c8a-be8...	Normal	Linux	CentOS 7.6 ...	ECS system...	40	No		<a href="#">Apply for Server</a>   <a href="#">Modify</a>   <a href="#">More</a>
image-centos7.6 085dbad2-fc67-45f-95f4...	Normal	Linux	CentOS 7.6 ...	ECS system...	40	No		<a href="#">Apply for Server</a>   <a href="#">Modify</a>   <a href="#">More</a>

### Figure 2-42 Applying for an ECS

Step 2 On the ECS purchase page, ensure that the private image is selected. Ensure that other configurations are the same as those in **ecs-hcia** and name the new ECS **ecs-new**.



General computing s6	s6.large.2	2 vCPUs	4 GiB	Intel Cascade Lake 2.6...	0.2 / 1.5 Gbit/s	150,000 PPS
General computing s6	s6.large.4	2 vCPUs	8 GiB	Intel Cascade Lake 2.6...	0.2 / 1.5 Gbit/s	150,000 PPS
General computing s6	s6.xlarge.2	4 vCPUs	8 GiB	Intel Cascade Lake 2.6...	0.35 / 2 Gbit/s	250,000 PPS
General computing s6	s6.xlarge.4	4 vCPUs	16 GiB	Intel Cascade Lake 2.6...	0.35 / 2 Gbit/s	250,000 PPS

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

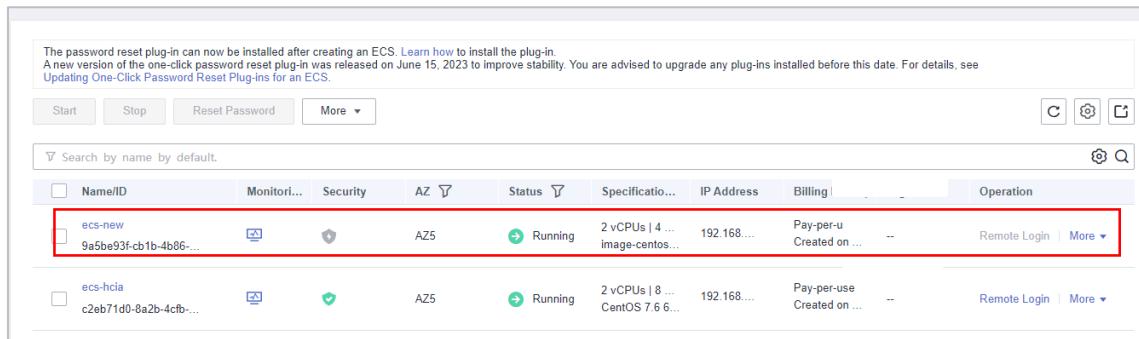
Public image **Private image** Shared image Marketplace image

image-centos7.6 (40 GiB) Create Private Image

HSS basic edition (free) None

### Figure 2-43 Creating an ECS using a private image

Step 3 Go back to the ECS list to view the ECS created using the private image.



Name/ID	Monitori...	Security	AZ	Status	Specificatio...	IP Address	Billing	Operation
ecs-new 9a5be93f-cb1b-4b86...			AZ5	Running	2 vCPUs   4 ... image-centos...	192.168...	Pay-per-u Created on ...	<a href="#">Remote Login</a>   <a href="#">More</a>
ecs-hcia c2eb71d0-8a2b-4cfb...			AZ5	Running	2 vCPUs   8 ... CentOS 7.6 6...	192.168...	Pay-per-use Created on ...	<a href="#">Remote Login</a>   <a href="#">More</a>

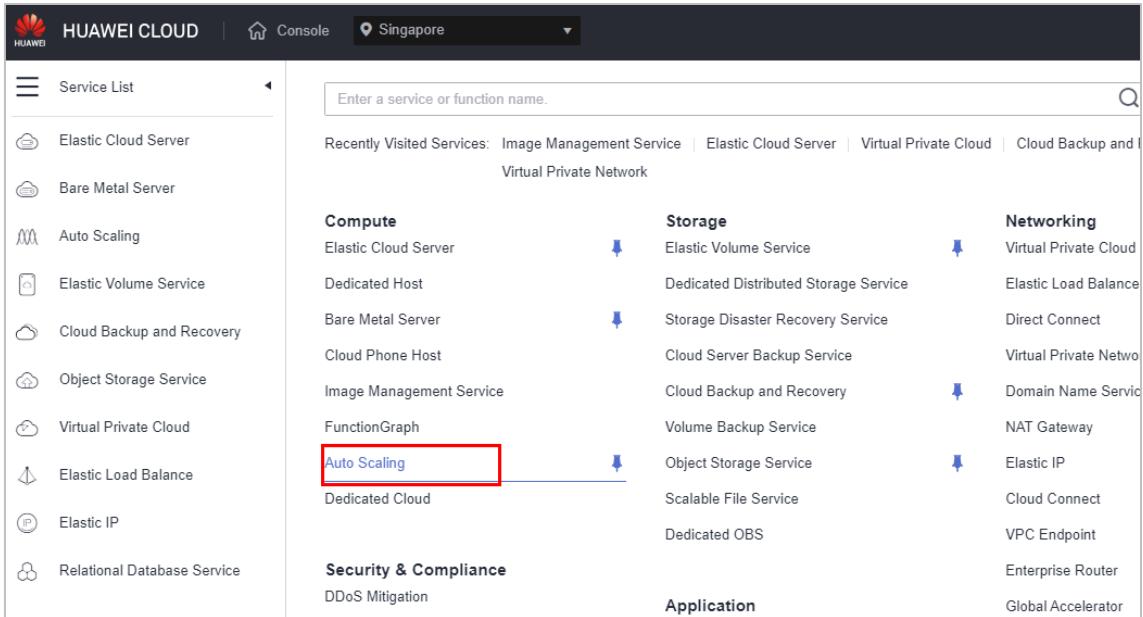
**Figure 2-44 Viewing the ECS**

## 2.2.4 AS Operations

AS automatically adjusts resources based on service demands and pre-configured AS policies. In this section, we will use ECS **ecs-hcia** as an example to describe how to scale ECS and bandwidth resources with AS.

### 2.2.4.1 Creating an AS Configuration

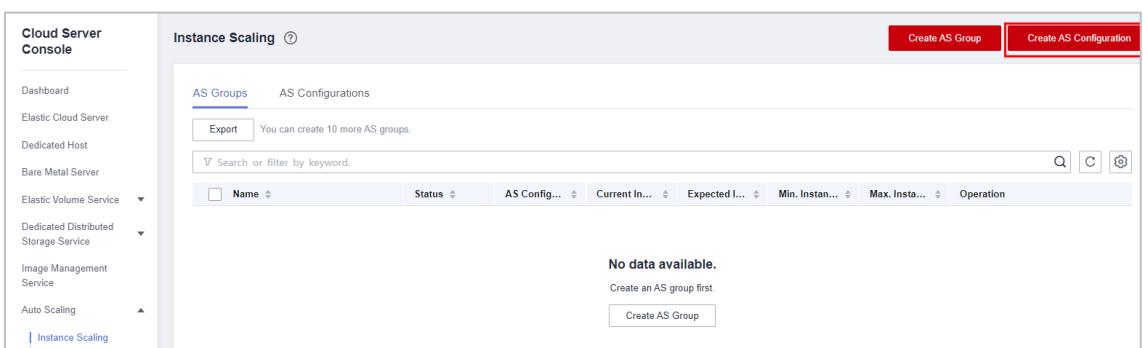
Step 1 Log in to the management console. On the homepage, choose **Service List > Compute > Auto Scaling**.



The screenshot shows the HUAWEI CLOUD Service List interface. The left sidebar lists various services under 'Compute' such as Elastic Cloud Server, Bare Metal Server, Auto Scaling, etc. The 'Auto Scaling' option is highlighted with a red box. The main panel displays a grid of services categorized by Compute, Storage, Networking, and other groups. The 'Auto Scaling' service is located in the Compute group, also highlighted with a red box. Other visible services include Dedicated Host, Bare Metal Server, Cloud Phone Host, Image Management Service, FunctionGraph, and Dedicated Cloud.

**Figure 2-45 Accessing AS**

Step 2 Click Create AS Configuration.



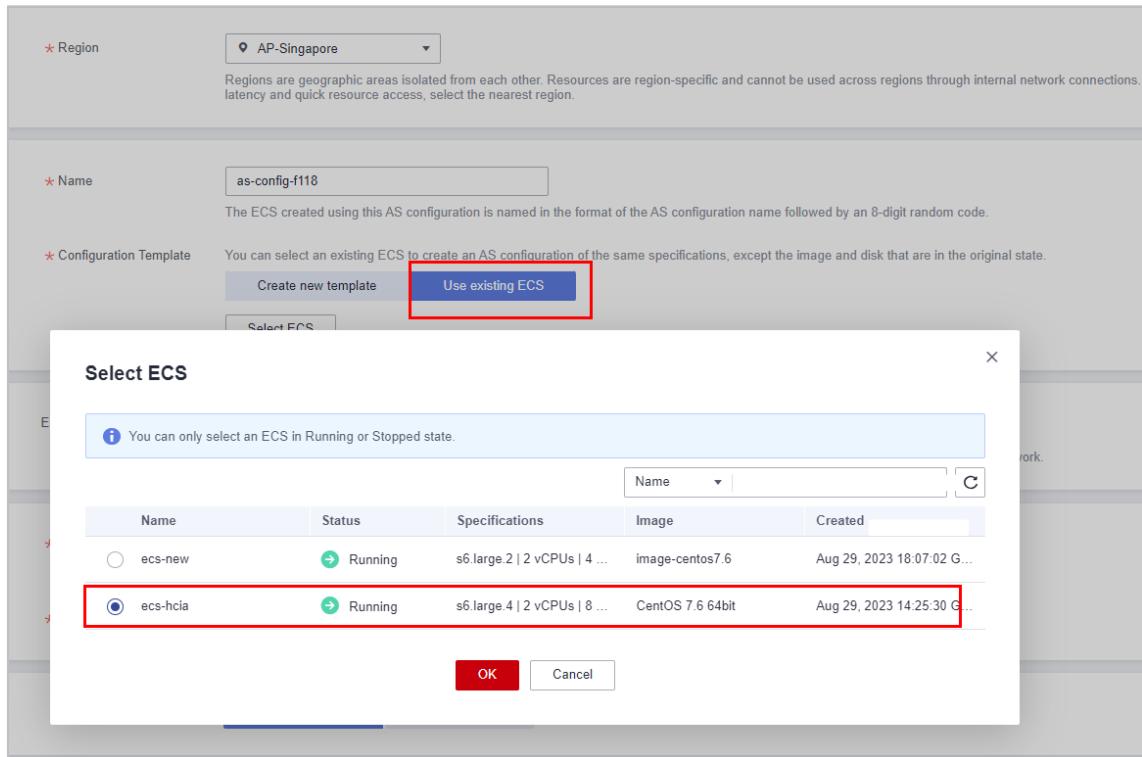
The screenshot shows the 'Instance Scaling - AS Groups' page. The left sidebar includes options like Dashboard, Elastic Cloud Server, Dedicated Host, Bare Metal Server, and Instance Scaling. The main area shows a table for AS Groups with columns for Name, Status, AS Configurations, Current Instances, Expected Instances, Min. Instances, Max. Instances, and Operation. A message at the bottom says 'No data available. Create an AS group first.' A prominent red box highlights the 'Create AS Group' button at the top right of the page.

**Figure 2-46 Creating an AS configuration**

Step 3 Set the following parameters and retain the default settings for other parameters.

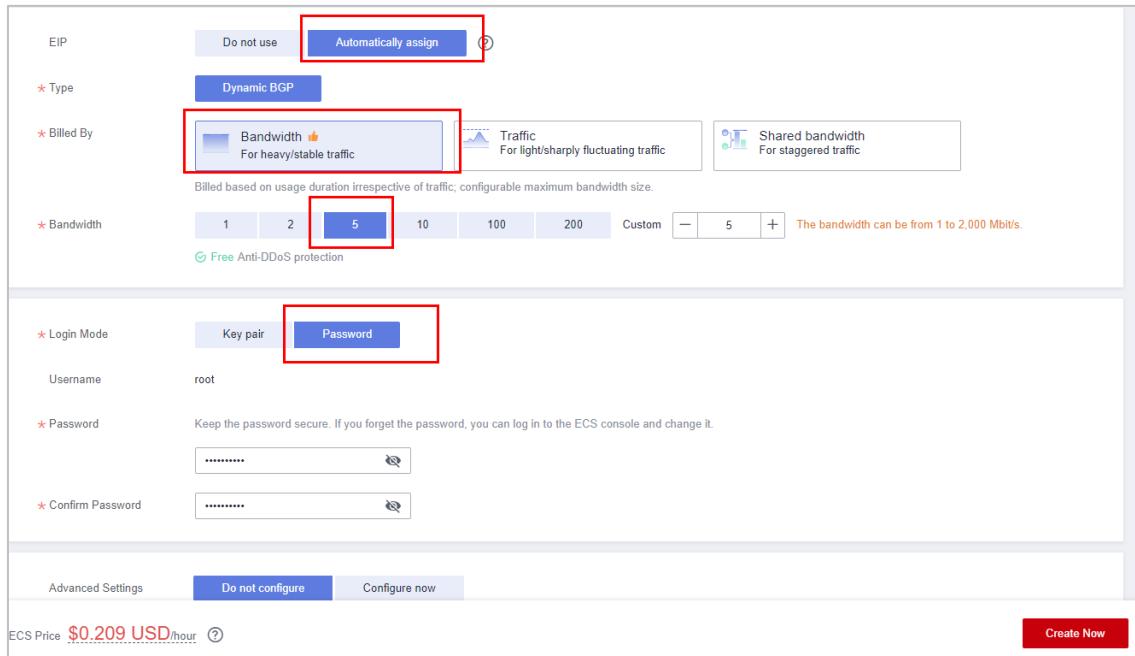
- Region: AP-Singapore
- Name: Use the default name **as-config-822b**.

- **Configuration Template:** Select **Use existing ECS**, and click **Select ECS**. In the **Select ECS** dialog box, select an existing ECS. In this example, **ecs-hcia** is selected.



**Figure 2-47 Selecting a configuration template**

- EIP: Automatically assign
- Type: Dynamic BGP
- Billed By: Bandwidth
- Bandwidth: 5 Mbit/s
- Login Mode: Password
- **Password:** Select the password.



EIP      Do not use      **Automatically assign**

\* Type      Dynamic BGP

\* Billed By      Bandwidth For heavy/stable traffic      Traffic For light/sharply fluctuating traffic      Shared bandwidth For staggered traffic

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

\* Bandwidth      1      2      **5**      10      100      200      Custom      -      5      +      The bandwidth can be from 1 to 2,000 Mbit/s

Free Anti-DDoS protection

\* Login Mode      Key pair      **Password**

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      .....

Advanced Settings      Do not configure      Configure now

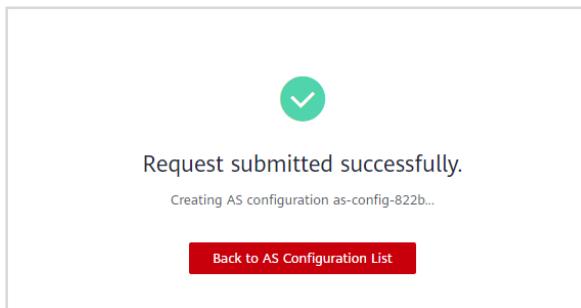
ECS Price **\$0.209 USD/hour**

**Create Now**

**Figure 2-48 Configuring scaling parameters**

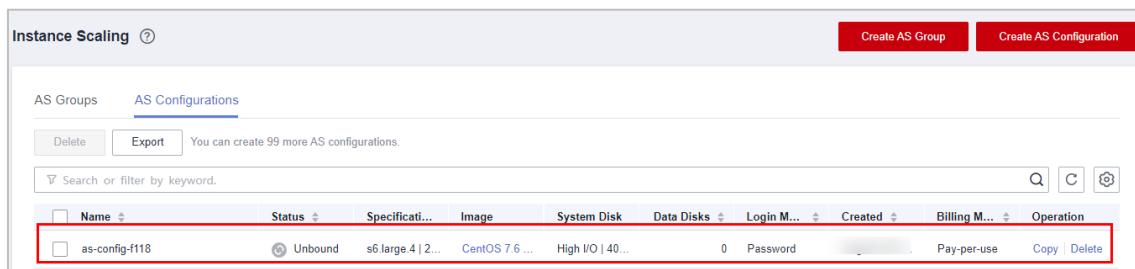
Step 4 Click Create Now.

**Request submitted successfully** is displayed.



**Figure 2-49 AS configuration created**

Step 5 In the AS configuration list, view the created AS configuration **as-config-xxxx**.

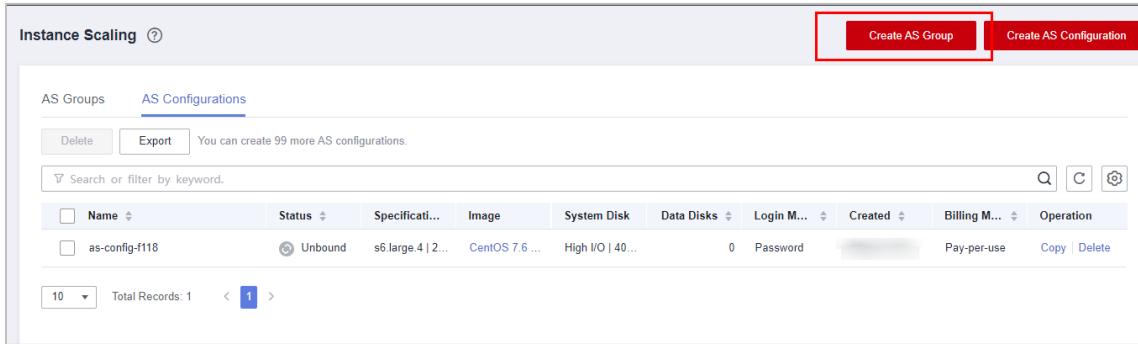


Instance Scaling										<b>Create AS Group</b>	<b>Create AS Configuration</b>	
AS Groups		AS Configurations										
<input type="button"/> Delete	<input type="button"/> Export	You can create 99 more AS configurations.								<input type="button"/> Q	<input type="button"/> C	<input type="button"/> S
Name	Status	Specification	Image	System Disk	Data Disks	Login M...	Created	Billing M...	Operation			
as-config-f118	Unbound	s6 large.4   2...	CentOS 7.6 ...	High I/O   40...	0	Password	...	Pay-per-use	<input type="button"/> Copy	<input type="button"/> Delete		

**Figure 2-50 Viewing the AS configuration**

## 2.2.4.2 Creating an AS Group

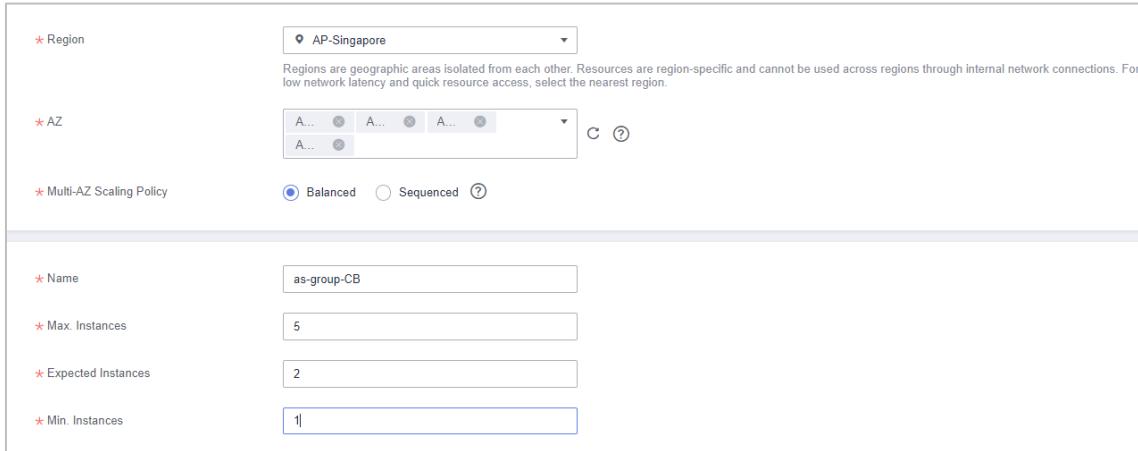
Step 1 On the AS console click **Create AS Group**.



**Figure 2-51 Creating an AS group**

Step 2 Set the following parameters and retain the default settings for other parameters. Then click **Create Now**

- Region: AP-Singapore
- AZ: Select all AZs, including **AZ1**, **AZ2**, and **AZ3**. AZs in the same region can communicate with each other over an intranet.
- Multi-AZ Expansion Policy: Load-balanced
- Name: **as-group-CB** (Change it as needed.)
- Max. Instances: 5
- Expected Instances: 2
- Min. Instances: 1



**Figure 2-52 Configuring AS group parameters**

- **AS Configuration:** Select the created AS configuration **as-config-XXX**.
- **VPC:** Select an existing VPC from the drop-down list. If no VPCs are available, click **Create VPC**. Refresh the list and select the created VPC.
- **Subnet:** Retain the default setting. The system automatically selects a subnet in the VPC.
- **Load Balancing:** Do not use
- **Instance Removal Policy:** Oldest instance created from oldest AS configuration
- **EIP:** Release

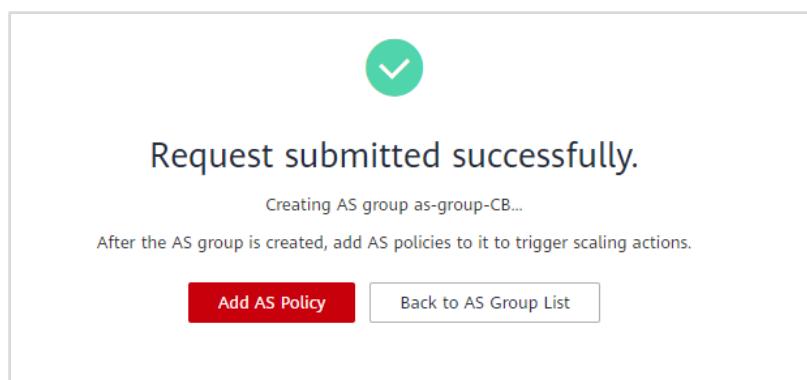
- Health Check Method: ECS health check
- Health Check Interval: 5 minutes
- Health Check Grace Period (s): 600
- Tag: Not required

The selected AS configuration serves as a specifications template for the instances in your AS group. After a subnet is selected, an IP address will be automatically assigned to each instance in the AS group.

<b>* AS Configuration</b>	as-config-f118	[+]
<b>* VPC</b>	vpc-hcia (192.168.0.0/16)	<a href="#">C Create VPC</a> <a href="#">?</a>
<b>* Subnet</b>	subnet-hcia (192.168.0.0/24)	This subnet is used by the primary NIC.
<input checked="" type="checkbox"/> <b>Source/Destination Check</b> <a href="#">?</a>		
<a href="#">+ Add Subnet</a> You can add 4 more subnets. <a href="#">C Create Subnet</a>		
<b>Load Balancing</b> <div style="display: flex; justify-content: space-around;"> <span>Do not use</span> <span>Elastic load balancer</span> </div>		
<b>* Instance Removal Policy</b> <div style="display: flex; justify-content: space-around;"> <span>Oldest instance created from oldest AS config...</span> </div>		
<b>EIP</b> <div style="display: flex; justify-content: space-around;"> <span>Release</span> <span>Do not release</span> </div> <p>Select Release if you want to release ECS EIPs when the ECSSs are removed from the AS group. Select Do not release if you want to unbind EIPs from ECSSs but do not release them. These EIPs will continue to be billed.</p>		
<b>Data Disk</b> <div style="display: flex; justify-content: space-around;"> <span>Delete</span> <span>Do not delete</span> </div> <p>Select Delete if you want to delete ECS data disks when the ECSSs are removed from the AS group. Select Do not delete if you want to detach data disks from ECSSs but do not release them. These data disks will continue to be billed.</p>		
<b>* Health Check Method</b> <div style="display: flex; justify-content: space-between;"> <span>ECS health check</span> <span>[?]</span> </div> <p>If a protected instance is identified as unhealthy in a health check, AS replaces the instance with a new one.</p>		
<b>* Health Check Interval</b> <div style="display: flex; justify-content: space-between;"> <span>5 minutes</span> <span>[?]</span> </div>		
<b>* Health Check Grace Period (s)</b> <div style="display: flex; justify-content: space-between;"> <span>600</span> <span>[?]</span> </div>		
<b>Tag</b> <p>It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. <a href="#">View predefined tags</a> <a href="#">C</a></p>		
ECS Price <b>\$0.209 USD/hour</b> <a href="#">[?]</a>		<a href="#">Create Now</a>

**Figure 2-53 Configuring an AS group**

Step 3 Click Back to AS Group List.



**Figure 2-54 AS group created**

Step 4 In the AS group list, view the created AS group **as-group-CB**.

Instance Scaling									<a href="#">Create AS Group</a>	<a href="#">Create AS Configuration</a>
<a href="#">AS Groups</a>		<a href="#">AS Configurations</a>								
<a href="#">Export</a>		You can create 9 more AS groups.							<a href="#">Search or filter by keyword.</a>	
<input type="checkbox"/>	Name	Status	AS Config...	Current In...	Expected I...	Min. Instan...	Max. Insta...	Operation		
<input type="checkbox"/>	as-group-CB afc694ab-bbca-42f7-87b2-bb21c37...	<span style="color: green;">Enabled</span>	as-config-f118	0	2	1	5	<a href="#">View AS Policy</a>   <a href="#">Disable</a>   <a href="#">More</a> ▾		

Figure 2-55 Viewing the AS group

Step 5 Click **View AS Policy** in the Operation column.

Instance Scaling									<a href="#">Create AS Group</a>	<a href="#">Create AS Configuration</a>
<a href="#">AS Groups</a>		<a href="#">AS Configurations</a>							<a href="#">Search or filter by keyword.</a>	
<a href="#">Export</a>		You can create 9 more AS groups.							<a href="#">Search or filter by keyword.</a>	
<input type="checkbox"/>	Name	Status	AS Config...	Current In...	Expected I...	Min. Instan...	Max. Insta...	Operation		
<input type="checkbox"/>	as-group-CB afc694ab-bbca-42f7-87b2-bb21c37...	<span style="color: green;">Enabled</span>	as-config-f118	0	2	1	5	<a href="#">View AS Policy</a>   <a href="#">Disable</a>   <a href="#">More</a> ▾		

Figure 2-56 View AS Policy

Step 6 On the AS Policies page, click **Add AS Policy**.

as-group-CB											<a href="#">Disable</a>	<a href="#">Modify</a>	<a href="#">C</a>																		
<a href="#">Overview</a>		<a href="#">Monitoring</a>		<a href="#">Instances</a>		<a href="#">Scaling Actions</a>		<a href="#">AS Policies</a>		<a href="#">Notifications</a>		<a href="#">Tags</a>	<a href="#">Lifecycle Hooks</a>																		
An AS policy defines the condition for triggering a scaling action. Learn more																															
<a href="#">Add AS Policy</a>																															
<a href="#">Enable</a> <a href="#">Disable</a> <a href="#">Delete</a> You can add 10 more policies.																															
<table border="1"> <thead> <tr> <th>Name</th> <th>Status</th> <th>Policy Type</th> <th>Monitored Object</th> <th>Trigger Condition</th> <th>Scaling Action</th> <th>Cooldown Period (s)</th> <th>Created</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>No data available.</td> </tr> </tbody> </table>														Name	Status	Policy Type	Monitored Object	Trigger Condition	Scaling Action	Cooldown Period (s)	Created	Operation									No data available.
Name	Status	Policy Type	Monitored Object	Trigger Condition	Scaling Action	Cooldown Period (s)	Created	Operation																							
								No data available.																							

Figure 2-57 Adding an AS policy

Step 7 In the **Add AS Policy** dialog box, configure the following parameters.

In this step, we will configure a policy to add one instance at specified time every day.

- Policy Name: as-policy-test1
- Policy Type: Periodic
- Interval: Day
- Triggered At: 18:00
- Time Range: Retain the default settings.
- Scaling Action: Add 1 instance
- Cooldown Period (s): 900

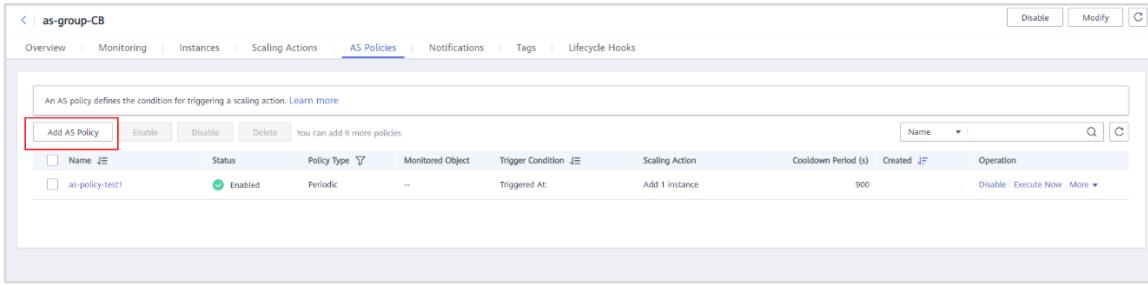
**Add AS Policy**

Policy Name	as-policy-test1		
Policy Type	Alarm	Scheduled	Periodic
Period	Day		
Time Zone	GMT+08:00		
Triggered At	18:00	🕒	
Time Range	📅		
Scaling Action	Add	1	Instances
Cooldown Period (s)	900 ⓘ		
<b>OK</b> <b>Cancel</b>			

**Figure 2-58 Configuring an AS policy**

Step 8 Click **OK**.

Step 9 Click **Add AS Policy** again to create another AS policy.



AS Policies								Disable	Modify	C	
An AS policy defines the condition for triggering a scaling action. Learn more								Name	Search	C	
Add AS Policy		Enable	Disable	Delete	You can add 9 more policies.						
<input type="checkbox"/>	Name	as-policy-test1	<input checked="" type="radio"/>	Enabled	Status	Periodic	Monitored Object	Trigger Condition	Scaling Action	Cooldown Period (s)	Created
						--	--	Triggered At:	Add 1 instance	900	Disable Execute Now More

**Figure 2-59 Adding another AS policy**

Step 10 In the **Add AS Policy** dialog box, configure the following parameters.

In this step, we will configure a policy to remove one instance at specified time every day.

- Policy Name: as-policy-test2
- Policy Type: Periodic
- Interval: Day
- Triggered At: 23:00
- **Time Range:** Retain the default settings.
- Scaling Action: Reduce 1 instances
- Cooldown Period (s): 900

**Add AS Policy**

Policy Name	as-policy-test2		
Policy Type	Alarm	Scheduled	<b>Periodic</b>
Period	Day		
Time Zone	GMT+08:00		
Triggered At	23:00		
Time Range			
Scaling Action	Reduce	1	instances
Cooldown Period (s)	900		
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

**Figure 2-60 Configuring another AS policy**

Step 11 To save time, click **Execute Now** to make the created policy **as-policy-test1** take effect immediately.

as-group-CB								
Overview		Monitoring		Instances		Scaling Actions		AS Policies
An AS policy defines the condition for triggering a scaling action. <a href="#">Learn more</a>								
Name	Status	Policy Type	Monitored Obj...	Trigger Condition	Scaling Action	Cooldown Period (s)	Created	Operation
<input type="checkbox"/> as-policy-test2		Enabled	Periodic	--	Triggered	Reduce 1 instance	900 Aug	<a href="#">Disable</a> <a href="#">Execute Now</a> <a href="#">More</a>
<input type="checkbox"/> as-policy-test1		Enabled	Periodic	--	Triggered At:	Add 1 instance	900 Aug	<a href="#">Disable</a> <a href="#">Execute Now</a> <a href="#">More</a>

**Figure 2-61 Executing an AS policy**

Step 12 After executing the AS policy, click the **Instances** tab to view how the number of instances has changed in response to the periodic AS policy you configured.

The number of instances will change daily at the times configured for the two periodic policies.

as-group-CB								
Overview		Monitoring		Instances	Scaling Actions		AS Policies	Notifications
View instance scaling details								
Name	Lifecycle Status	Health Status	AS Configuration	Instance Added	Instance Protection	Added	Operation	
<input type="checkbox"/> as-config-f118-BP8ON...	Adding to AS group		as-config-f118	Automatically	<input type="checkbox"/>	A	<a href="#">Remove</a> <a href="#">Remove and Delete</a>	
<input type="checkbox"/> as-config-f118-BI6PIIQ	Enabled		as-config-f118	Automatically	<input type="checkbox"/>	A	<a href="#">Remove</a> <a href="#">Remove and Delete</a>	
<input type="checkbox"/> as-config-f118-HZ2P7...	Enabled		as-config-f118	Automatically	<input type="checkbox"/>	A	<a href="#">Remove</a> <a href="#">Remove and Delete</a>	

**Figure 2-62 Viewing instance scaling**

## 2.2.4.3 Creating a Bandwidth Scaling Policy

Step 1 On the management console, choose **Service List > Compute > Auto Scaling**. In the navigation pane on the left, choose **Auto Scaling > Bandwidth Scaling**. Click **Create Bandwidth Scaling Policy**.

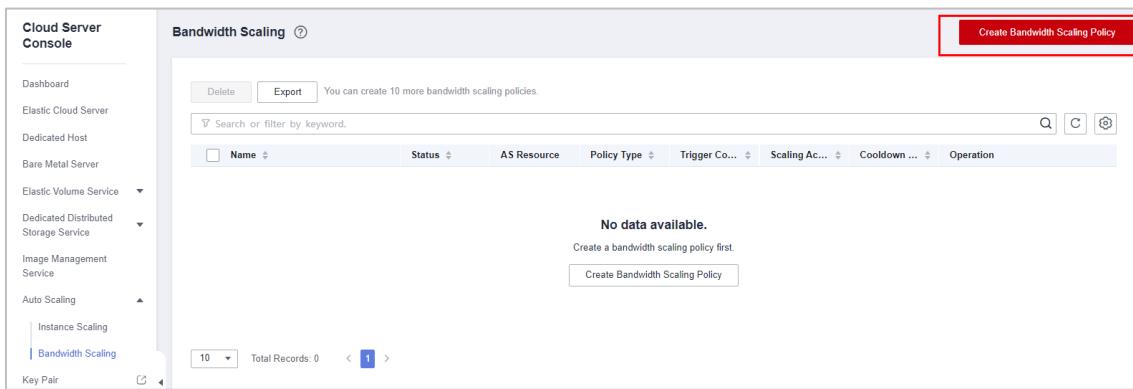
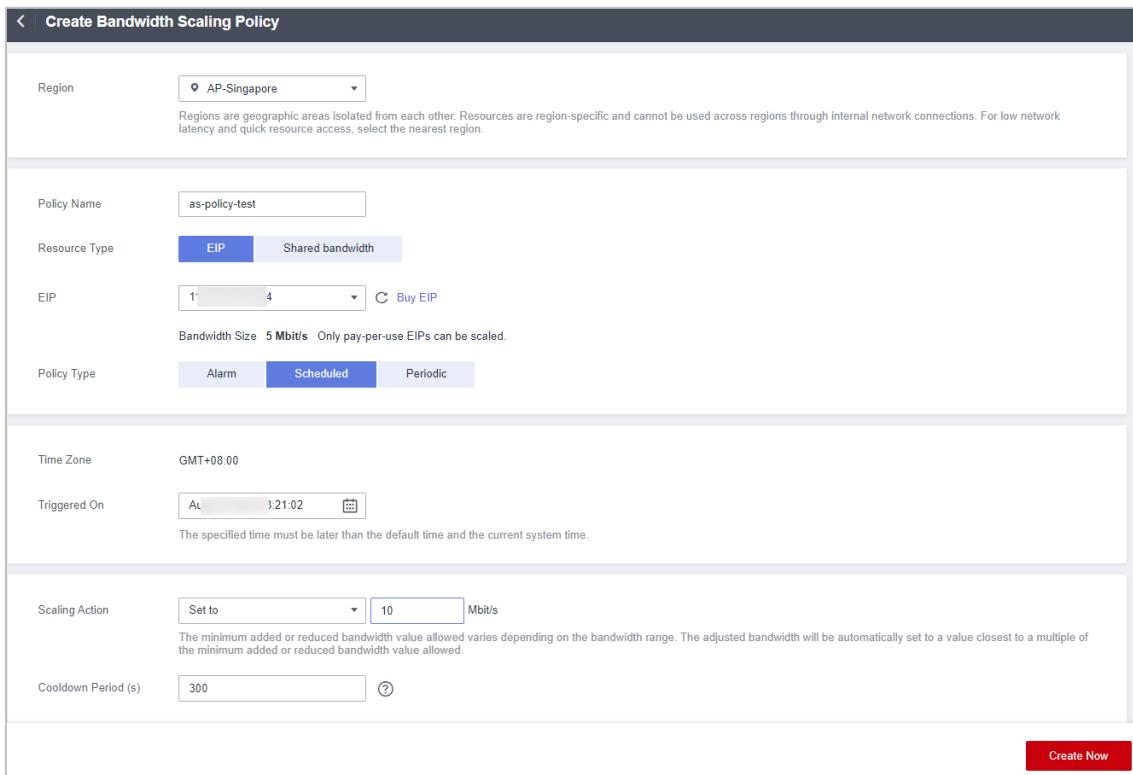


Figure 2-63 Creating a bandwidth scaling policy

Step 2 Set the following parameters:

- Region: AP-Singapore
- Policy Name: as-policy-test
- Resource Type: EIP
- **EIP:** Select an existing EIP or create a new one. After creating an EIP, refresh the EIP list to load it.
- Policy Type: Scheduled
- **Triggered On:** Retain the default settings. Generally, the value is several minutes later than the current time.
- Scaling Action: Set to 10 Mbit/s
- Cooldown Period (s): 300



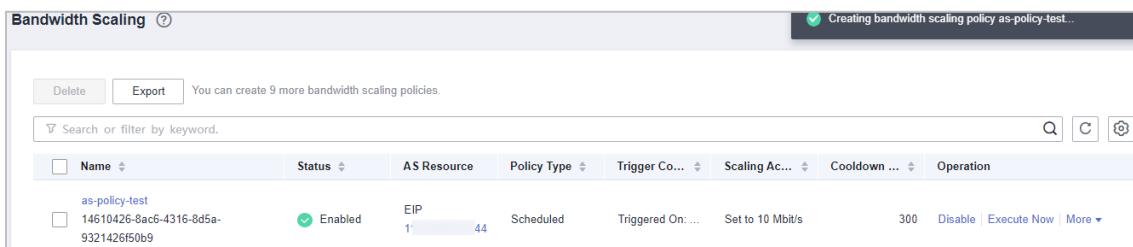
The screenshot shows the configuration of a bandwidth scaling policy. Key settings include:

- Region:** AP-Singapore
- Policy Name:** as-policy-test
- Resource Type:** EIP (selected)
- EIP:** 1 (selected)
- Policy Type:** Scheduled
- Time Zone:** GMT+08:00
- Triggered On:** 3:21:02
- Scaling Action:** Set to 10 Mbit/s
- Cooldown Period (s):** 300

**Figure 2-64 Configuring a bandwidth scaling policy**

Step 3 Click Create Now.

Step 4 Wait for a short while and then return to the page that displays the bandwidth scaling policy list.

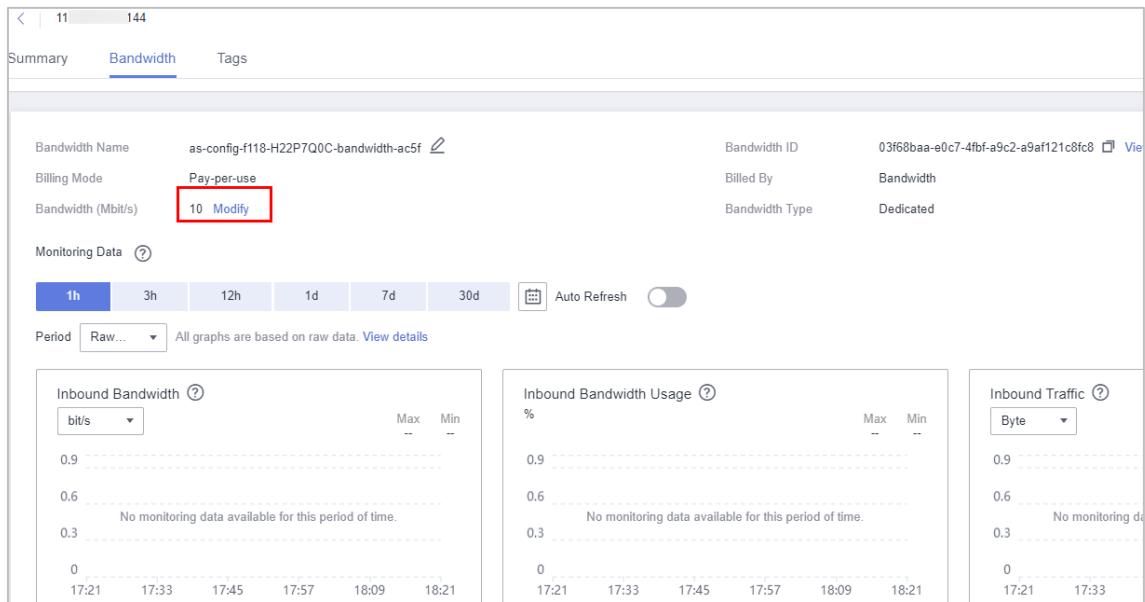


Name	Status	AS Resource	Policy Type	Trigger Co...	Scaling Ac...	Cooldown ...	Operation
as-policy-test	Enabled	EIP 1	Scheduled	Triggered On: ...	Set to 10 Mbit/s	300	Disable   Execute Now   More ▾
14610426-8ac6-4316-8d5a-9321426f50b9							

**Figure 2-65 Viewing the bandwidth scaling policy**

Step 5 In the bandwidth scaling policy list, click the **EIP** (in blue) in the **AS Resource** column of the created policy.

You can see that the bandwidth has been changed to 10 Mbit/s. It means that the bandwidth scaling policy has taken effect.



**Figure 2-66 Viewing the bandwidth**

## 2.2.5 Deleting Resources

- Step 1 Disable AS before deleting resources. Otherwise, resources in the AS group will be scaled based on the expected number of instances.
- Step 2 After the experiment is complete, delete the corresponding ECS resources (select Release EIP and disk resources)
- Step 3 Delete the private images.
- Step 4 Delete the AS group and configuration.
- Step 5 Delete the subnet and then the VPC.
- Step 6 Confirm that all the resources created in the experiment have been deleted. If they have not, delete them.

## 2.3 Exercises

1. Create an AS group to scale Linux ECS instances.
2. Set the expected number of instances to 3.
3. Add an alarm-based AS policy that removes one instance when the average memory usage is lower than 30%, with a cooldown period of 5 minutes.
4. Observe the effectiveness of the AS policy. If the policy does not take effect, explain the possible causes.

# 3 Networking Services

---

## 3.1 Introduction

### 3.1.1 About This Exercise

A Virtual Private Cloud (VPC) is logically isolated, configurable, and manageable virtual network for cloud servers, containers, and databases. It improves resource security and simplifies network deployment on the cloud.

A security group provides access control for ECSs that have the same security requirements within a given VPC. You can define inbound and outbound rules to control traffic to and from the ECSs in a security group, making your ECS more secure.

The Elastic IP (EIP) service enables your cloud resources to communicate with the Internet using static public IP addresses and scalable bandwidths. EIPs can be bound to or unbound from ECSs, BMSs, virtual IP addresses, load balancers, and NAT gateways.

Elastic Load Balance (ELB) automatically distributes incoming traffic across multiple backend servers based on listening rules you configure. ELB expands the service capabilities of your applications and improves their availability by eliminating single points of failure (SPOFs).

A VPC peering connection is a network connection between two VPCs. ECSs in either VPC can communicate with each other if they are in the same region. You can create a VPC peering connection between your own VPCs, or between your VPC and a VPC of another account within the same region. However, you cannot create a VPC peering connection between VPCs in different regions.

A Virtual Private Network (VPN) establishes an encrypted, Internet-based communications tunnel between your network and a VPC. With VPN, you can connect to a VPC and access the resources deployed there.

In this exercise, we will verify that:

- Two ECSs in a VPC can communicate with each other by default.
- Security groups can be used to control communication between ECSs.
- Different VPCs can communicate with each other through VPC peering connections.
- ECSs can access the Internet after an EIP is bound to each of them.
- ELB can distribute traffic across backend servers.

We will also create a VPN connection to enable ECSs in different regions to communicate with each other.

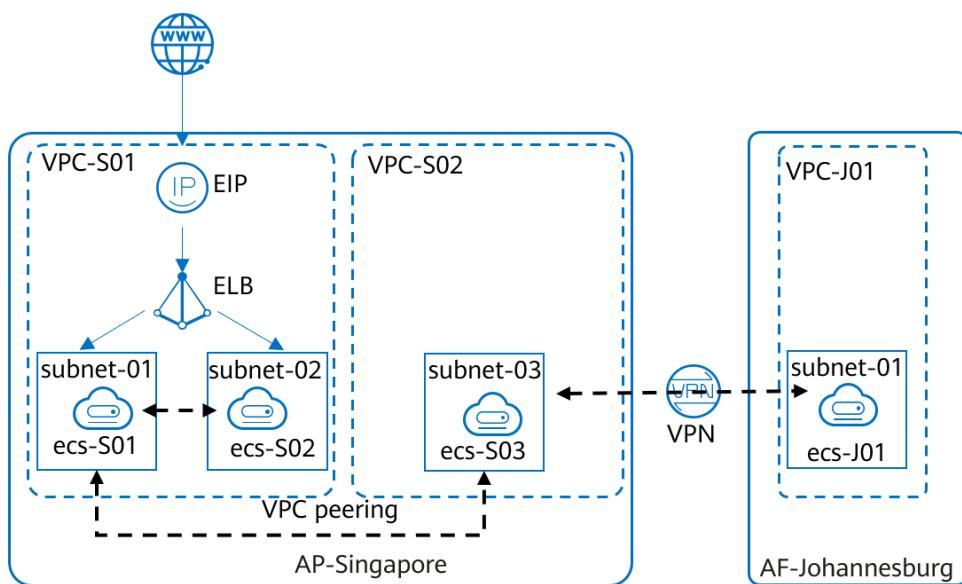
### 3.1.2 Objectives

- Learn how to enable communication between different ECSs in a VPC.
- Learn how to use security groups to control communication between ECSs.
- Learn how to use EIP to allow an ECS to access the Internet.
- Learn how to use ELB to distribute traffic across backend servers.
- Learn how to use a VPC peering connection to enable ECSs in different VPCs in the same region to communicate with each other.
- Learn how to use a VPN connection to enable ECSs in different regions to communicate with each other.

## 3.2 Tasks

### 3.2.1 Roadmap

- Create two VPCs in **AP-Singapore**, one VPC in **AF-Johannesburg**
- Verify that security groups can control communication between ECSs in **AP-Singapore**.
- Verify that an ECS with an EIP bound can access the Internet in **AP-Singapore**.
- Verify that ECSs in different VPCs in the same region (**AP-Singapore**) can communicate with each other through a VPC peering connection.
- Verify that ECSs in different regions (**AP-Singapore** and **AF-Johannesburg**) can communicate with each other through a VPN connection.
- Delete resources.
- Exercises



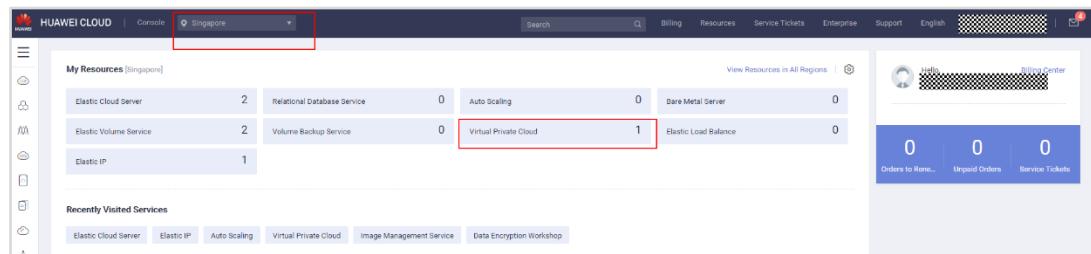
**Figure 3-1 Network topology**

### 3.2.2 Creating VPCs

Tasks:

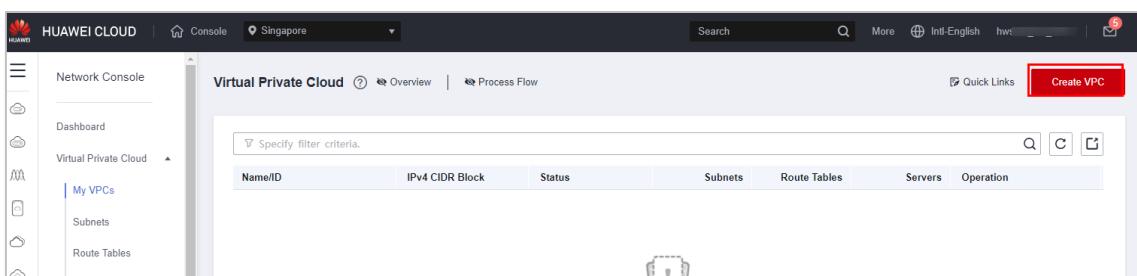
- Create VPC-S01 with subnet-01 and subnet-02, and VPC-S02 with subnet-03 in **AP-Singapore**.
- Create VPC-J01 with subnet-01 in **AF-Johannesburg**.

Step 1 Log in to the management console and select the **AP-Singapore** region. Click **Service List**. Under **Networking**, select **Virtual Private Cloud**.



**Figure 3-2 Switching to VPC console**

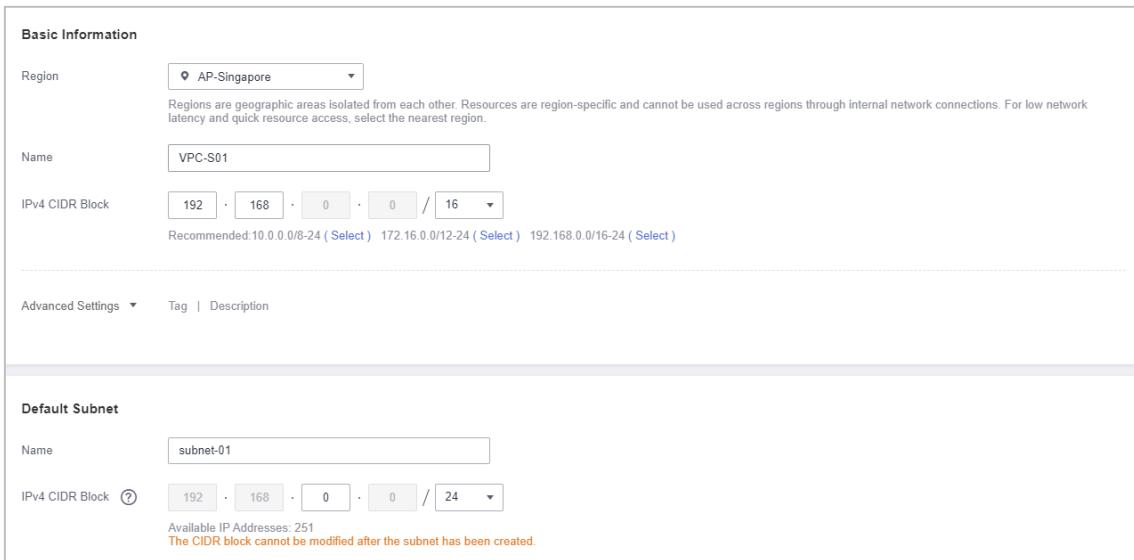
Step 2 Click Create VPC.



### Figure 3-3 Create VPC

Step 3 Configure the VPC parameters as follows and click **Create Now**.

- Region: AP-Singapore
- Name: VPC-S01
- CIDR Block: Use the default CIDR block, for example, 192.168.0.0/16.
- Subnet name: **subnet-01** and **subnet-02**
- Retain the default settings for other parameters.



Basic Information

Region: AP-Singapore

Name: VPC-S01

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

Advanced Settings ▾ Tag | Description

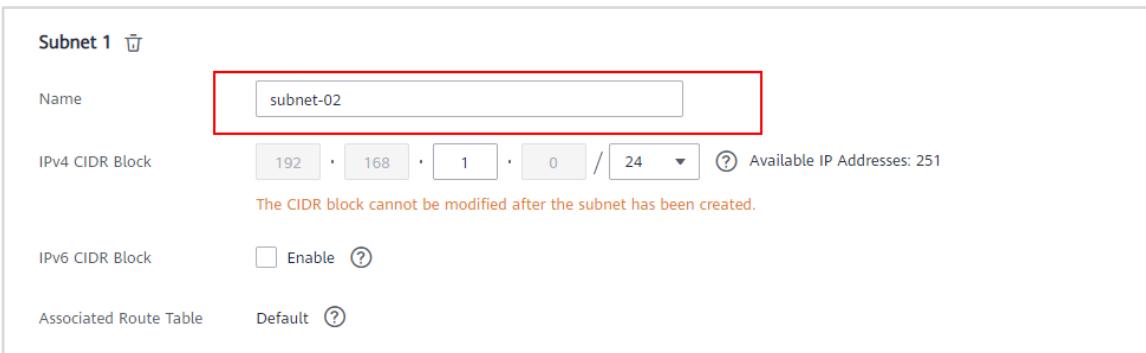
Default Subnet

Name: subnet-01

IPv4 CIDR Block: 192 · 168 · 0 · 0 / 24

Available IP Addresses: 251  
The CIDR block cannot be modified after the subnet has been created.

### Figure 3-4 Configuring the VPC



Subnet 1

Name: subnet-02

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 3-5 Configuring the VPC

Step 4 View the created VPC in the VPC list.

Virtual Private Cloud		Overview	Process Flow	Quick Links	Create VPC		
<input type="checkbox"/> Specify filter criteria. <input type="button" value="Search"/> <input type="button" value="C"/> <input type="button" value="D"/>							
Name/ID	IPv4 CIDR Block	Status	Subnets	Route Tables	Servers	Operation	
VPC-S01 a16fea29-9e3f-4390-b55c-939...	192.168.0.0/16 (Primary Cl...)	Available	2	1	0	<input type="button" value="Edit CIDR Block"/> <input type="button" value="Delete"/>	

Figure 3-6 Viewing the VPC

Step 5 Click **Create VPC** again and configure the VPC parameters as follows.

- Region: AP-Singapore
- Name: VPC-S02
- CIDR Block: Set a CIDR block different from that of VPC-S01, for example, 10.0.0.0/24.
- Default subnet name: **subnet-03**
- Retain the default settings for other parameters.

**Basic Information**

Region	<input type="button" value="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.
Name	<input type="text" value="VPC-S02"/>	
IPv4 CIDR Block	<input type="text" value="10.0.0.0/24"/> / <input type="button" value="16"/>	Recommended: 10.0.0.0/8-24 ( <input type="button" value="Select"/> ), 172.16.0.0/12-24 ( <input type="button" value="Select"/> ), 192.168.0.0/16-24 ( <input type="button" value="Select"/> )
Advanced Settings	<input type="button" value="Tag"/> <input type="button" value="Description"/>	

---

**Default Subnet**

Name	<input type="text" value="subnet-03"/>
IPv4 CIDR Block	<input type="text" value="10.0.0.0/24"/> / <input type="button" value="24"/>
	Available IP Addresses: 251 <small>The CIDR block cannot be modified after the subnet has been created.</small>

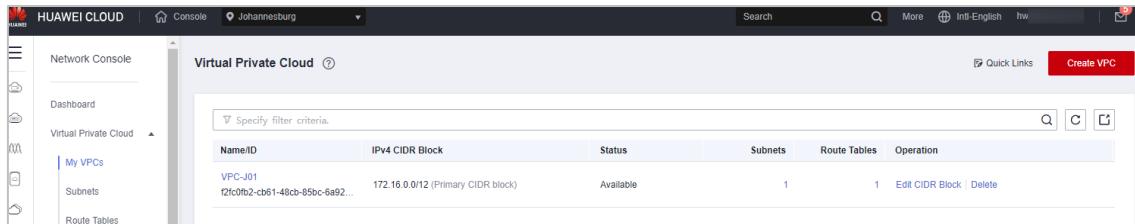
Figure 3-7 Configuring the VPC

Step 6 View the created VPC in the VPC list.

Virtual Private Cloud		Overview	Process Flow	Quick Links	Create VPC		
<input type="checkbox"/> Specify filter criteria. <input type="button" value="Search"/> <input type="button" value="C"/> <input type="button" value="D"/>							
Name/ID	IPv4 CIDR Block	Status	Subnets	Route Tables	Servers	Operation	
VPC-S02 3de841a5-2844-4b0d-9b6f-427...	10.0.0.0/16 (Primary Cl...)	Available	1	1	0	<input type="button" value="Edit CIDR Block"/> <input type="button" value="Delete"/>	
VPC-S01 a16fea29-9e3f-4390-b55c-939...	192.168.0.0/16 (Primar...	Available	2	1	0	<input type="button" value="Edit CIDR Block"/> <input type="button" value="Delete"/>	

Figure 3-8 Viewing the VPC

**Step 7** Create VPC-J01 with subnet-01 in AF-Johannesburg. In subsequent experiments, VPC-S02 and VPC-J01 will be used to test the VPN connection. To prevent connection failures caused by IP address conflicts, the IP address segment of VPC-J01 must be different from that of VPC-S02.



Name/ID	IPv4 CIDR Block	Status	Subnets	Route Tables	Operation
VPC-J01 f2fc0fb2-cb61-48cb-85bc-6a92...	172.16.0.0/12 (Primary CIDR block)	Available	1	1	Edit CIDR Block   Delete

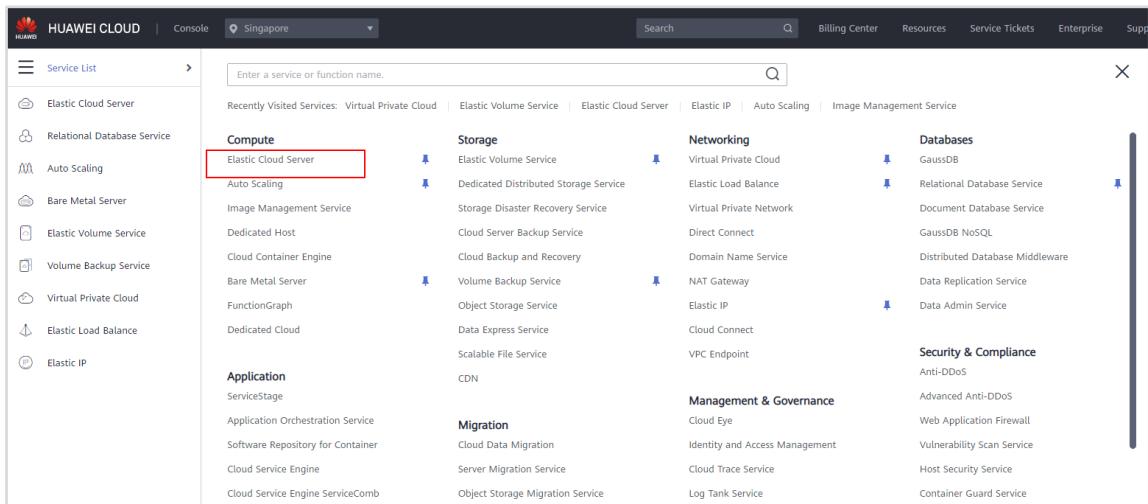
**Figure 3-9 Viewing the VPC**

### 3.2.3 Buying ECSs

Tasks:

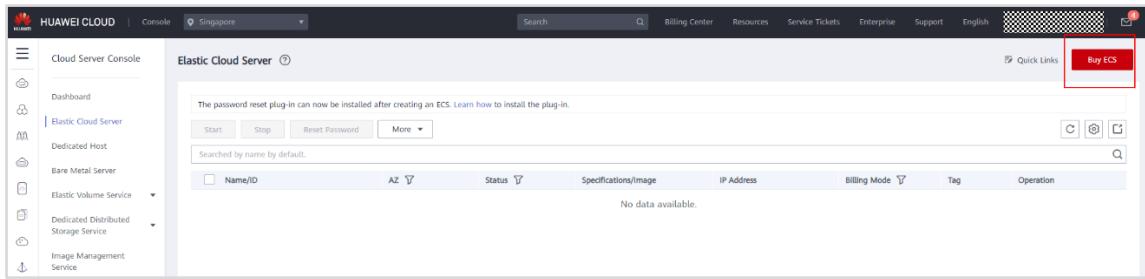
- In the **AP-Singapore** region, create two ECSs in **VPC-S01**, one in **subnet-01** and one in **subnet-02**, and one ECS in **subnet-03** of **VPC-S02**.
- In the **AF-Johannesburg** region, create an ECS in **subnet-01** of **VPC-J01**.

**Step 1** Select the AP-Singapore region, click **Service List**. Under **Compute**, select **Elastic Cloud Server**.



**Figure 3-10 Switching to ECS console**

**Step 2** Click **Buy ECS**.

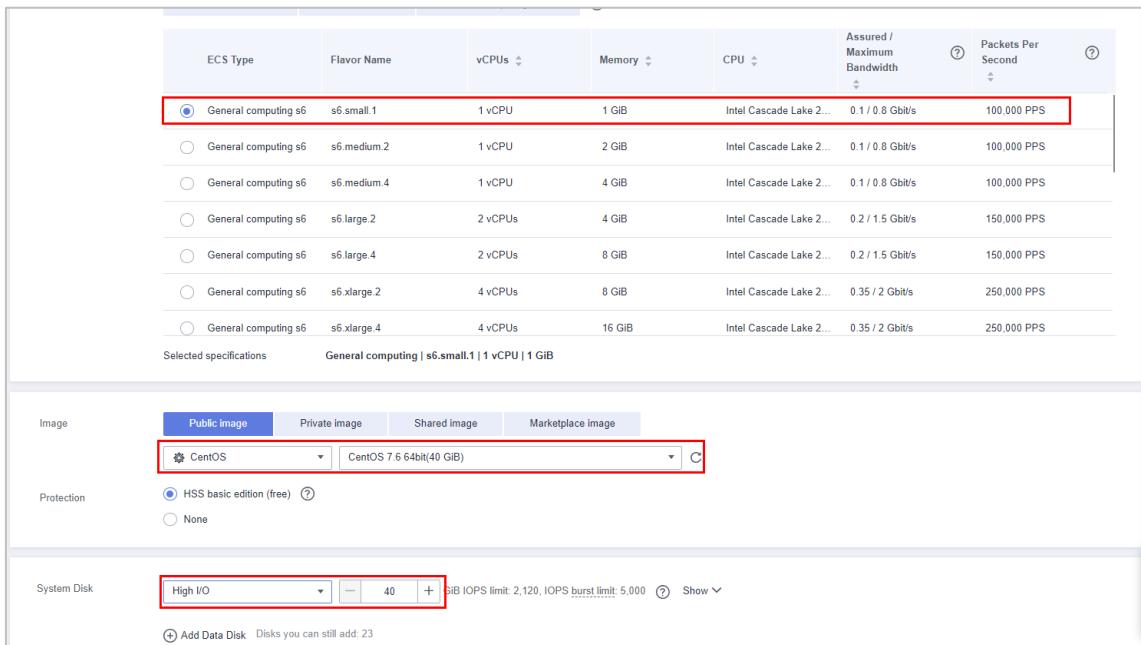


**Figure 3-11 Buy ECS**

Configure the parameters as follows.

Basic settings:

- Region: AP-Singapore
- Billing Mode: Pay-per-use
- AZ: Random
- CPU Architecture: x86
- Specifications: General computing, s6.small.1, 1 vCPUs | 1GB
- Image: Public image, CentOS 7.6 64bit(40GB)
- System Disk: High I/O, 40 GB



ECS Type	Flavor Name	vCPUs	Memory	CPU	Assured / Maximum Bandwidth	Packets Per Second
<input checked="" type="radio"/> General computing s6	s6.small.1	1 vCPU	1 GiB	Intel Cascade Lake 2...	0.1 / 0.8 Gbit/s	100,000 PPS
<input type="radio"/> General computing s6	s6.medium.2	1 vCPU	2 GiB	Intel Cascade Lake 2...	0.1 / 0.8 Gbit/s	100,000 PPS
<input type="radio"/> General computing s6	s6.medium.4	1 vCPU	4 GiB	Intel Cascade Lake 2...	0.1 / 0.8 Gbit/s	100,000 PPS
<input type="radio"/> General computing s6	s6.large.2	2 vCPUs	4 GiB	Intel Cascade Lake 2...	0.2 / 1.5 Gbit/s	150,000 PPS
<input type="radio"/> General computing s6	s6.large.4	2 vCPUs	8 GiB	Intel Cascade Lake 2...	0.2 / 1.5 Gbit/s	150,000 PPS
<input type="radio"/> General computing s6	s6.xlarge.2	4 vCPUs	8 GiB	Intel Cascade Lake 2...	0.35 / 2 Gbit/s	250,000 PPS
<input type="radio"/> General computing s6	s6.xlarge.4	4 vCPUs	16 GiB	Intel Cascade Lake 2...	0.35 / 2 Gbit/s	250,000 PPS

Selected specifications  
General computing | s6.small.1 | 1 vCPU | 1 GiB

Image  
 Public Image  
 Private Image  
 Shared image  
 Marketplace image  
 CentOS  
 CentOS 7.6 64bit(40 GiB)

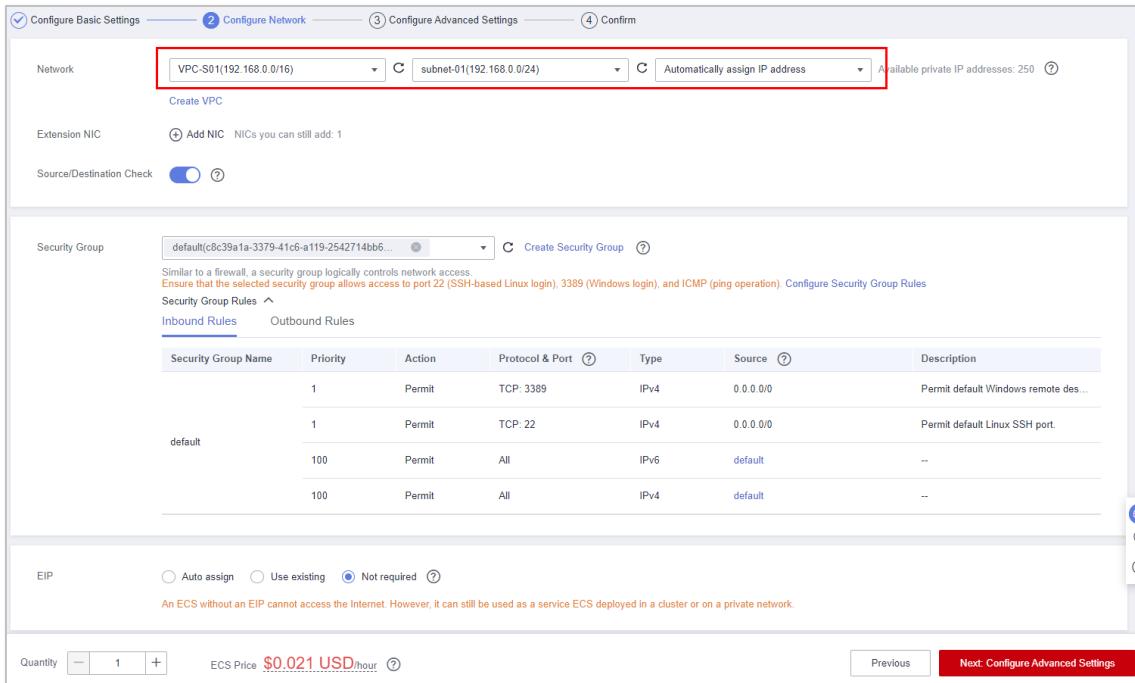
Protection  
 HSS basic edition (free)  
 None

System Disk  
 High I/O  
 40  
 40 GiB IOPS limit: 2,120, IOPS burst limit: 5,000  
 Add Data Disk Disks you can still add: 23

**Figure 3-12 Configuring the ECS**

Network configuration:

- Network: VPC-S01
- subnet-01
- **Security Group:** Select the default security group.
- EIP: Not required



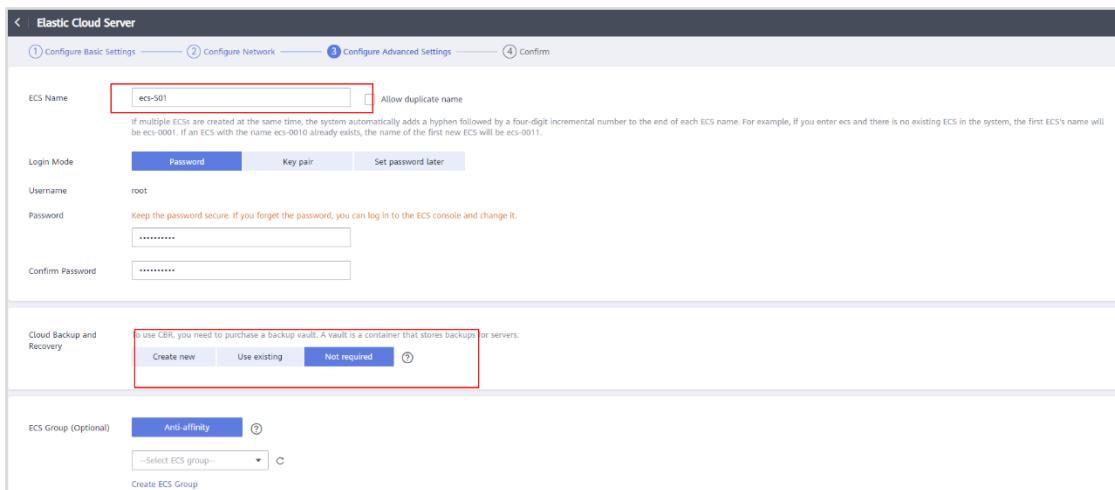
The screenshot shows the 'Configure Basic Settings' step of the ECS creation process. Key fields include:

- Network:** VPC-S01 (192.168.0.0/16) - Subnet: subnet-01 (192.168.0.0/24). The 'Automatically assign IP address' option is selected.
- Security Group:** default (c8c39a1a-3379-41c6-a119-2542714bb6...). It lists security group rules for Inbound and Outbound traffic.
- EIP:** Auto assign (radio button selected).
- Quantity:** 1.
- ECS Price:** \$0.021 USD/hour.

**Figure 3-13 Configuring the ECS**

#### Advanced settings:

- ECS Name: ecs-S01
- Login Mode: Password, for example, Huawei@123!
- Cloud Backup and Recovery: Not required



The screenshot shows the 'Configure Advanced Settings' step of the ECS creation process. Key fields include:

- ECS Name:** ecs-S01. A note indicates that 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.
- Login Mode:** Password (radio button selected).
- Cloud Backup and Recovery:** Options for Create new, Use existing, and Not required. The 'Not required' option is selected.
- ECS Group (Optional):** Anti-affinity (radio button selected).

**Figure 3-14 Configuring the ECS**

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

The screenshot shows the configuration wizard for creating an ECS instance. It includes tabs for Configuration, Basic, Network, and Advanced. The Basic tab shows the following details:

- Billing Mode: Pay-per-use
- Specifications: General computing | s6.small.1 | 1 vCPU... Image: CentOS 7.6 64bit
- System Disk: High I/O, 40 GB
- Region: Singapore
- AZ: AZ5
- Host Security: HSS basic edition (free)

The Network tab shows:

- VPC: VPC-S01(192.168.0.0/16)
- EIP: No EIP bound to the primary network int... Source/Destination Check: Enable
- Primary NIC: subnet-01(192.168.0.0/24)

The Advanced tab shows:

- ECS Name: ecs-S01
- ECS Group: --
- Login Mode: Password
- Cloud Eye: Monitoring details

Other fields include:

- Quantity: 1 (maximum of 20)
- Save as Launch Template: button
- Agreement: A checked checkbox with a red border.
- ECS Price: \$0.021 USD/hour

**Figure 3-15 Confirming the configuration**

**Step 4** Repeat the preceding steps to create **ecs-S02** in **subnet-02**, **ecs-S03** in **subnet-03**. You can create a general computing ECS (**ecs-J01** in **subnet-01**) with flavor c3.large.2, 2 vCPUs, and 4 GB of memory in the **AF-Johannesburg** regions.

The screenshots show the Elastic Cloud Server management interface. The top screenshot displays three ECS instances:

Name/ID	Monitor...	Security	AZ	Status	Specification...	IP Address	Billing Mode	Tag	Operation
ecs-S03 f9d25dec-7cef-420d...	monitor	shield	AZ5	Running	1 vCPU   1 ... CentOS 7.6 ...	10.0.0....	Pay-per-use Created on A...	--	Remote Login   More
ecs-S02 ca01b7dd-8e4f-48b...	monitor	shield	AZ5	Running	1 vCPU   1 ... CentOS 7.6 ...	192.16....	Pay-per-use Created on A...	--	Remote Login   More
ecs-S01 d6e4a353-2696-429...	monitor	shield	AZ5	Running	1 vCPU   1 ... CentOS 7.6 ...	192.16....	Pay-per-use Created on A...	--	Remote Login   More

The bottom screenshot shows one instance:

Name/ID	Monitor...	Security	AZ	Status	Specification...	IP Address	Billing Mode	Tag	Operation
ecs-J01 5c168510-eb8b-4f41-90...	monitor	shield	AZ1	Running	2 vCPUs   4 Gi... CentOS 7.6 64bit	172.16.0....	Pay-per-use Created on A...	--	Remote Login   More

**Figure 3-16 Viewing the ECSs**

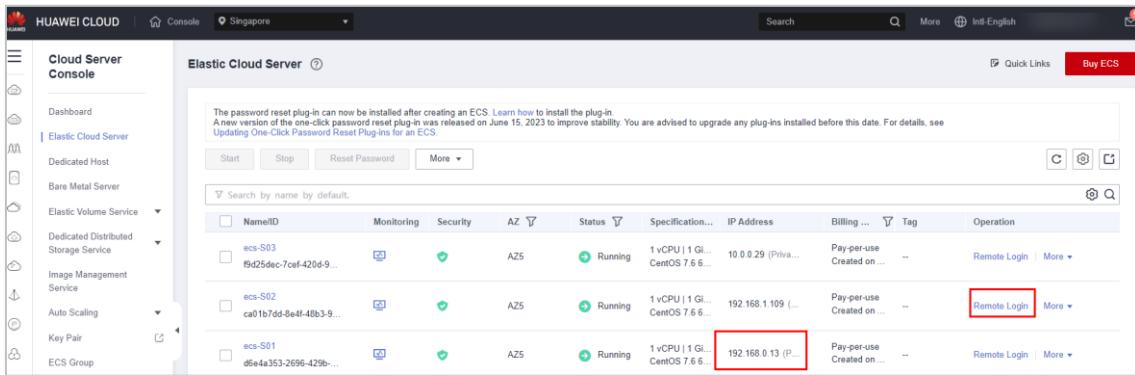
## 3.2.4 Verifying Network Service Functions

Tasks:

- Verify that two ECSs in a VPC can communicate with each other by default.
- Configure security groups to control communication between ECSs.
- Bind an EIP to an ECS to allow the ECS to access the Internet.
- Use ELB to distribute traffic across backend servers.
- Create a VPC peering connection to enable communication between ECSs in different VPCs of the same region.
- Create a VPN to enable ECSs in different regions to communicate with each other.

### 3.2.4.1 Communication Between ECSs

Step 1 On the ECS console, switch to the **AP-Singapore** region, make a note of the private IP address of **ecs-S01**, and log in to **ecs-S02** remotely.



Name/ID	Monitoring	Security	AZ	Status	Specification...	IP Address	Billing ...	Tag	Operation
ecs-S03 f9d25dec-7cef-420d-9...			A25	Running	1 vCPU   1 Gi...	10.0.0.29 (Priva...	Pay-per-use		Remote Login More ▾
ecs-S02 ca01b7dd-8eff-4fb3-9...			A25	Running	1 vCPU   1 Gi...	192.168.1.109 (...	Pay-per-use		Remote Login More ▾
ecs-S01 d6a4a353-2696-429b-...			A25	Running	1 vCPU   1 Gi...	192.168.0.13 (P...	Pay-per-use		Remote Login More ▾

Figure 3-17 Remotely logging in to the ECS

Step 2 Enter the username (**root** for a Linux ECS by default) and password to log in to **ecs-S02**.

```
Welcome to Huawei Cloud Service
[root@ecs-s02 ~]#
```

Step 3 Ping the private IP address of **ecs-S01** from **ecs-S02** to check whether these two ECSs in the same VPC can communicate with each other. The ping is successful, indicating that the two ECSs in a VPC can communicate with each other.

```
[root@ecs-s02 ~]# ping 192.168.0.13
PING 192.168.0.13 (192.168.0.13) 56(84) bytes of data.
64 bytes from 192.168.0.13: icmp_seq=1 ttl=64 time=0.204 ms
64 bytes from 192.168.0.13: icmp_seq=2 ttl=64 time=0.569 ms
64 bytes from 192.168.0.13: icmp_seq=3 ttl=64 time=0.128 ms
64 bytes from 192.168.0.13: icmp_seq=4 ttl=64 time=0.133 ms
```

Step 4 Ping the private IP address of **ecs-S03** from **ecs-S02** to check whether these two ECSs in different VPCs can communicate with each other. The ping fails, indicating that two ECSs in different VPCs cannot communicate with each other.

```
[root@ecs-s02 ~]# ping 10.0.0.29
PING 10.0.0.29 (10.0.0.29) 56(84) bytes of data.
```

### 3.2.4.2 Traffic Control by Security Groups

Step 1 Switch to the network console. In the left navigation pane, choose **Security Groups**.

Name/ID	Security Group R...	Associated Instances	Description	Created	Operation
default c8c39a1a-3379-41c6-a119-25...	6	3	Default security...		<a href="#">Manage Rule</a> <a href="#">Manage Instance</a> <a href="#">Clone</a>

Figure 3-18 Viewing the security group

Step 2 Click the security group name and delete all inbound security group rules on the **Inbound Rules** tab page.

Prio...	Action	Type	Protocol & Port	Source	Description	Last Modified	Operation
<input checked="" type="checkbox"/>	Allow	IPv4	TCP : 22	0.0.0.0/0	Permit default Li...	A	<a href="#">Modify</a> <a href="#">Replicate</a> <a href="#">Delete</a>
<input checked="" type="checkbox"/>	Allow	IPv4	TCP : 3389	0.0.0.0/0	Permit default ...	A	<a href="#">Modify</a> <a href="#">Replicate</a> <a href="#">Delete</a>
<input checked="" type="checkbox"/>	Allow	IPv4	All	default	--	A	<a href="#">Modify</a> <a href="#">Replicate</a> <a href="#">Delete</a>
<input checked="" type="checkbox"/>	Allow	IPv6	All	default	--	A	<a href="#">Modify</a> <a href="#">Replicate</a> <a href="#">Delete</a>

Figure 3-19 Deleting inbound rules

Step 3 Switch to the ECS console, remotely log in to **ecs-S02**, and ping the private IP address of **ecs-S01**. The ping fails, indicating that the two ECSs cannot communicate with each other.

```
[root@ecs-s02 ~]# ping 192.168.0.13
PING 192.168.0.13 (192.168.0.13) 56(84) bytes of data.
```

Step 4 Go back to the **Inbound Rules** tab page of the security group and click **Allow Common Ports**.

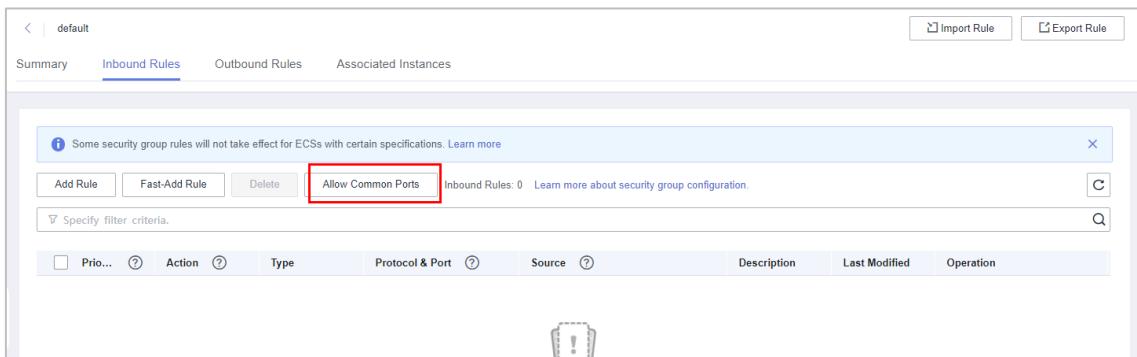


Figure 3-20 Allow Common Ports

Step 5 Switch to the ECS console, remotely log in to **ecs-S02**, and ping the private IP address of **ecs-S01**. The ping is successful, so the two ECSSs can communicate with each other, indicating that the security group can be used to control communication.

```
[root@ecs-s02 ~]# ping 192.168.0.13
PING 192.168.0.13 (192.168.0.13) 56(84) bytes of data.
64 bytes from 192.168.0.13: icmp_seq=1 ttl=64 time=0.301 ms
64 bytes from 192.168.0.13: icmp_seq=2 ttl=64 time=0.569 ms
64 bytes from 192.168.0.13: icmp_seq=3 ttl=64 time=0.128 ms
```

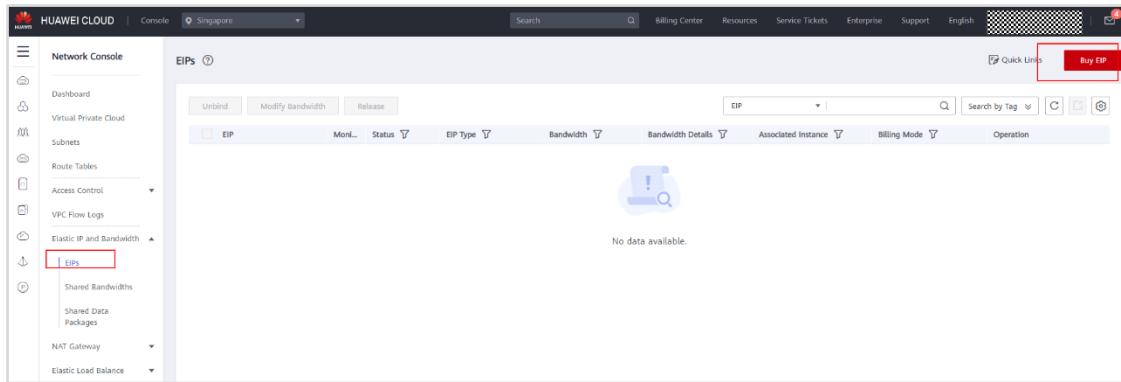
### 3.2.4.3 Access to the Internet with an EIP

Step 1 Ping baidu.com from **ecs-S02**. The ping fails, indicating that **ecs-S02** fails to access the Internet. Then bind an EIP to **ecs-S02** and check whether **ecs-S02** can access the Internet.

```
[root@ecs-s02 ~]# ping baidu.com
PING baidu.com(220.181.38.148) 56(84) bytes of data.
```

If you want to log in to the ECS with an EIP bound using a remote login tool, we recommend you to use a key pair instead of a password for security. If you log in to the ECS through the management console, you can still use a password.

Step 2 Switch to the network console, choose **EIPs**, and click **Buy EIP**.



**Figure 3-21 Buy EIP**

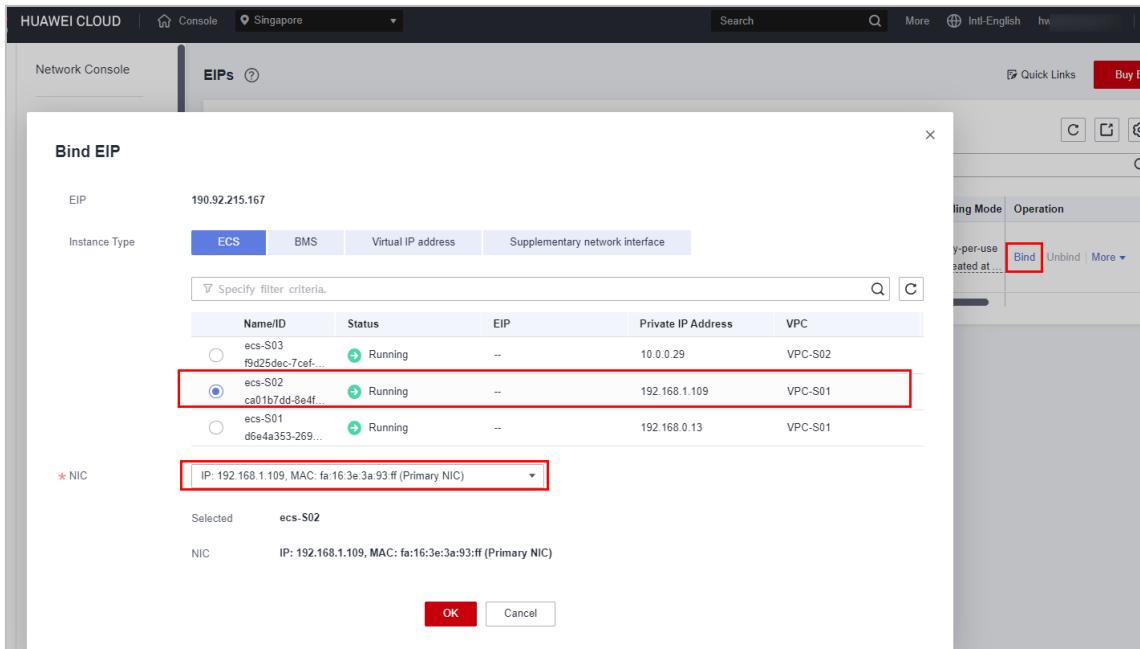
Step 3 Configure the parameters as follows, click **Next**, confirm the parameters, and click **Submit**.

- Billing Mode: Pay-per-use
- Region: AP-Singapore
- EIP Type: Dynamic BGP
- Billed By: Bandwidth
- **Bandwidth:** 1 Mbit/s
- Retain the default settings for other parameters.

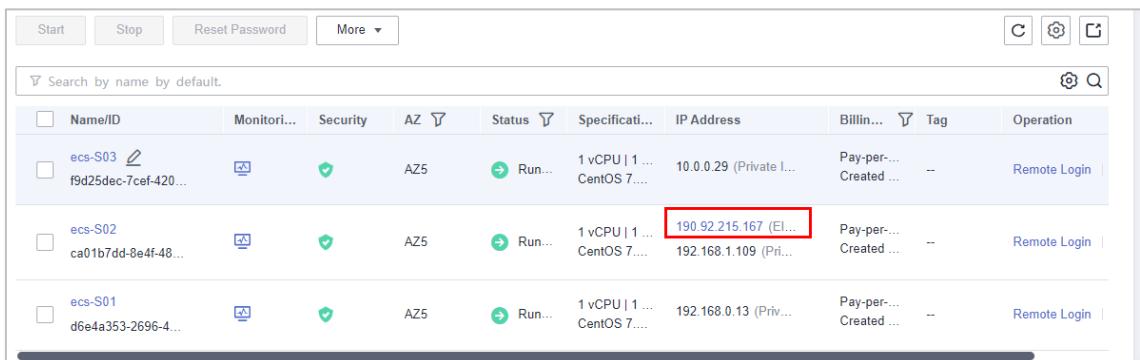
Billing Mode	Yearly/Monthly	Pay-per-use
Region	AP-Singapore	Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.
EIP Type	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
Bandwidth (Mbit/s)	1	The value ranges from 1 to 2,000 Mbit/s.

**Figure 3-22 Configuring EIP**

Step 4 On the **EIPs** page, locate the newly purchased EIP, click **Bind** in the **Operation** column, select **ecs-S02**, and click **OK**.



**Figure 3-23 Binding an EIP**



**Figure 3-24 Viewing the EIP**

Step 5 Remote Login to the **ecs-S02**. Run the **ping baidu.com** command to check whether **ecs-S02** can access the Internet. The ping is successful, indicating that **ecs-S02** can access the Internet through an EIP.

```
[root@ecs-s02 ~]# ping baidu.com
PING baidu.com (39.156.66.10) 56(84) bytes of data.
64 bytes from 39.156.66.10: icmp_seq=1 ttl=64 time=0.301 ms
64 bytes from 39.156.66.10: icmp_seq=2 ttl=64 time=0.569 ms
64 bytes from 39.156.66.10: icmp_seq=3 ttl=64 time=0.128 ms
```

### 3.2.4.4 Using ELB to Distribute Incoming Traffic

Tasks:

- Start the HTTP service on **ecs-S01** and **ecs-S02**.
- Create a load balancer.

- Use the load balancer to route HTTP requests for the web page across two ECSs.

Step 1 Remotely log in to **ecs-S01** and **ecs-S02** and enable port **8889**, which is a default port for HTTP communication.

1. Start the HTTP service on each ECS.

```
[root@ecs-s01 ~]# nohup python -m SimpleHTTPServer 8889 > /dev/null 2>&1 &
[1] 1278
```

2. Verify that port 8889 is enabled.

```
[root@ecs-s01 ~]# curl 127.0.0.1:8889
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a>
<li><a href=".bash_logout">.bash_logout</a>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".bashrc">.bashrc</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
<li><a href=".tcshrc">.tcshrc</a>
</ul>
<hr>
</body>
</html>
[root@ecs-s01 ~]#
```

3. **ecs-S02** and enable port **8889**.

```
[root@ecs-s02 ~]# nohup python -m SimpleHTTPServer 8889 > /dev/null 2>&1 &
[1] 1369
[root@ecs-s02 ~]# curl 127.0.0.1:8889
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a>
<li><a href=".bash_logout">.bash_logout</a>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".bashrc">.bashrc</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
```

```
<li><a href=".tcshrc">.tcshrc</a>
</ul>
<hr>
</body>
</html>
[root@ecs-s02 ~]#
```

Step 2 Use **touch** to create an empty file named **SERVER1** on **ecs-S01** and one called **SERVER2** on **ecs-S02**. Run the **ls** command to confirm the files are there.

ecs-01:

```
[root@ecs-s01 ~]# touch SERVER1
[root@ecs-s01 ~]# ls
SERVER1
```

ecs-02:

```
[root@ecs-s02 ~]# touch SERVER2
[root@ecs-s02 ~]# ls
SERVER2
```

Step 3 Log in to the management console. On the service list page, choose **Networking > Elastic Load Balance**.

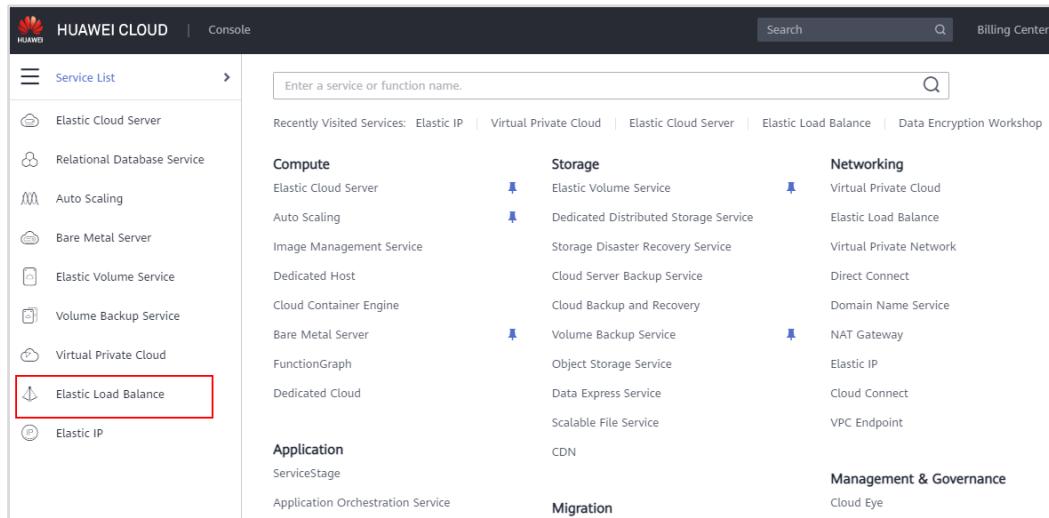
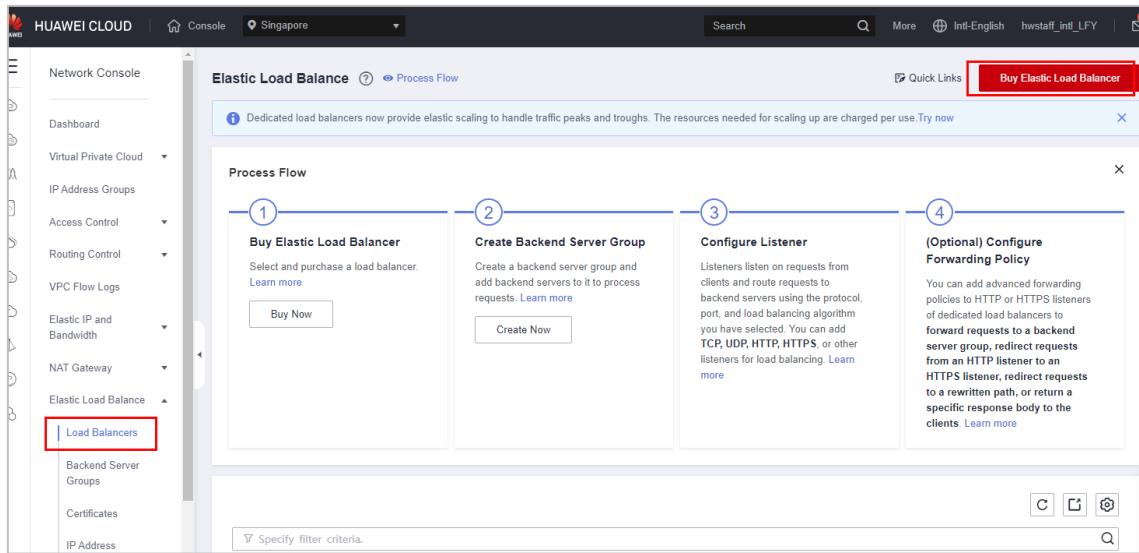


Figure 3-25 Accessing Elastic Load Balance

Step 4 Click Buy Elastic Load Balancer and select Shared for Type.



**Figure 3-26 Buy Elastic Load Balancer**

Step 5 Configure the parameters and click **Next**. Confirm the configuration and click **Submit**.

- Type: Shared
- Region: AP-Singapore
- Network Type: Public Ipv4 network
- **VPC: VPC-S01** (Select a VPC with two ECSs. Select subnet-01 as the subnet.)
- EIP: New EIP
- EIP Type: Dynamic BGP
- Billed By: Bandwidth
- Bandwidth: 1 M/bits
- **Name: elb-name** (Change it as needed.)

**Figure 3-27 Configuring parameters**

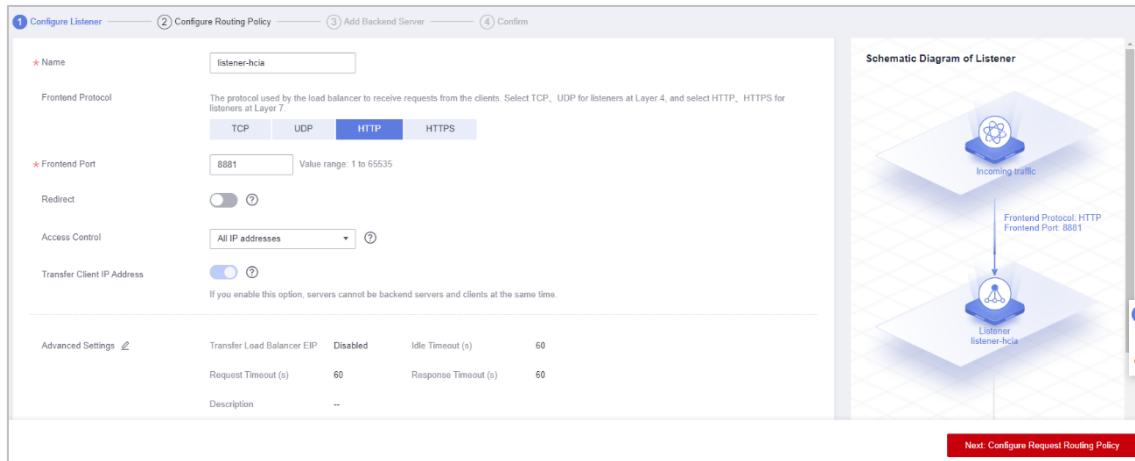
Step 6 Return to the load balancer list, locate the load balancer you just created, and click **Add listener**.

Name/ID	Monit...	Status	Type	Specificati...	IP Address and Netw...	Listener (Frontend Proto...	Bandwidth...	Billing Mode	Operation
elb-name 0573519a-398e-4900-ba40-a2bd1994d9a3		Running	Shared	Guaranteed...	192.168.0.214 (Private... VPC-S01 (VPC)	No listeners added <a href="#">Add now</a>	--	Pay-per-use Created at	<a href="#">Add Listener</a>

**Figure 3-28 Viewing the load balancer**

Click **Add Listener** and configure the following parameters:

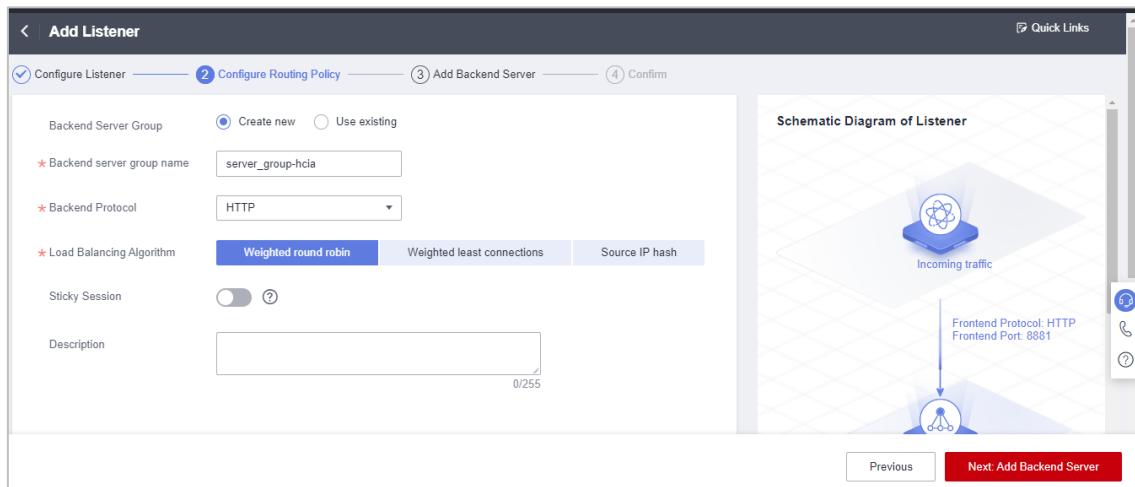
- **Name: listener-hcia** (Change it as needed.)
- Frontend Protocol/Port: HTTP/8881
- **Redirect:** disabled



**Figure 3-29 Configuring a listener**

Click **Next** and configure a backend server group.

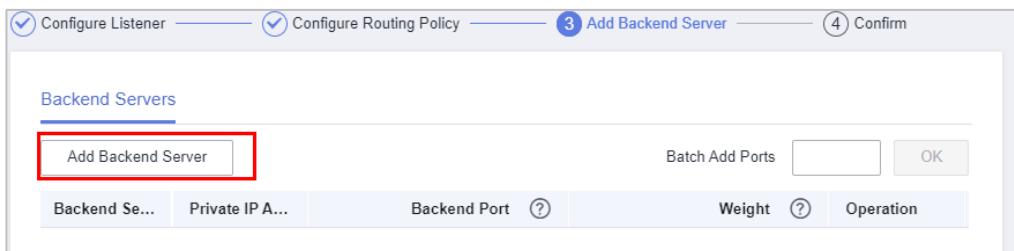
- Backend Cloud Server Group: Create new
- Name: server\_group-hcia** (Change it as needed.)
- Backend Protocol: HTTP
- Load Balancing Algorithm: Weighted round robin



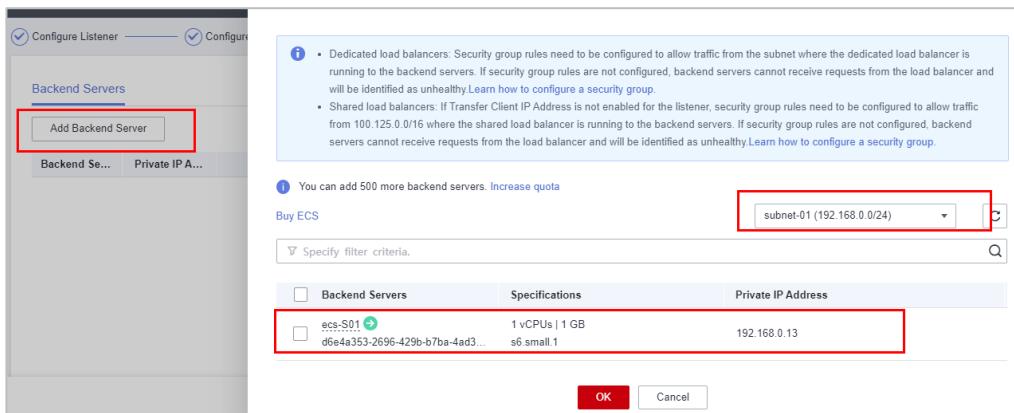
**Figure 3-30 Configuring a backend server group**

Click **Next: Add Backend Server**. Click **Add Backend Server**, and add **ecs-sh-01** and **ecs-sh-02** ECSs to the backend server group. The two ECSs, **ecs-S01** and **ecs-S02**, are in different subnets (**subnet-01** and **subnet-02**). When you add them, each needs to be added separately. When you add **ecs-S01**, select **subnet-01**. When you add **ecs-S02**, select **subnet-02**:

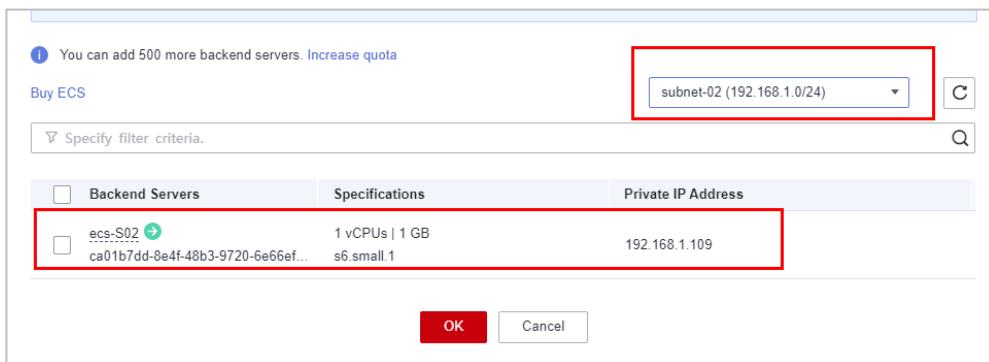
- Back-end port: 8889
- Weight: 1
- Health check: Enabled | Protocol: HTTP



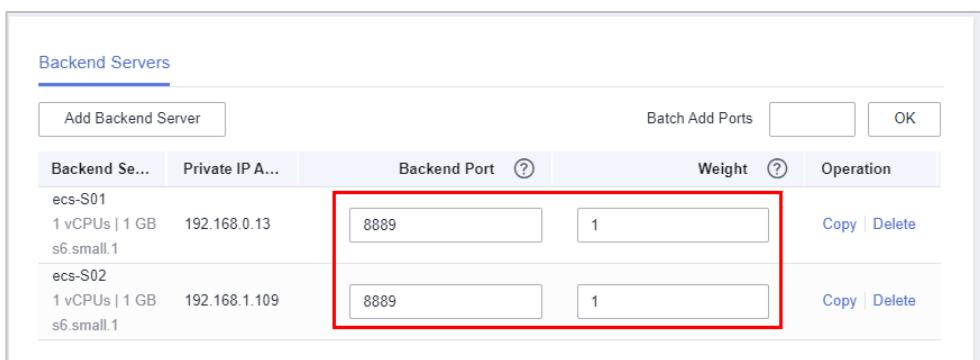
**Figure 3-31 Adding a Backend Server**



**Figure 3-32 Adding ecs-S01**



**Figure 3-33 Adding ecs-S02**



**Figure 3-34 Configuring Ports and Weights**

**Health Check**

Health Check

Health check detects the running of backend servers and ensures that requests are routed only to healthy backend servers. [Learn more](#)

Advanced Settings [/](#)

\* Health Check Protocol [?](#)

Domain Name  Private IP address of the backend server  Specified domain name

Health Check Port  Default backend server port  Specified port

\* Path [?](#)

Start the path with a slash (/). The path can contain 1 to 80 characters, including letters, digits, and the following characters:-/.%?&\_

\* Interval (s) [?](#)

Value range: 1 to 50

\* Timeout (s) [?](#)

Value range: 1 to 50

\* Maximum Retries [?](#)

Value range: 1 to 10

**Figure 3-35 Configuring the Health Check**

Configure Listener  Configure Routing Policy  Add Backend Server  4 Confirm

**Listener** [/](#)

Name	listener-hcia	Frontend Protocol	HTTP
Frontend Port	8881	Access Control	All IP addresses
Transfer Load Balancer EIP	Disabled	Transfer Client IP Address	Enabled
Idle Timeout (s)	60	Request Timeout (s)	60
Response Timeout (s)	60	Description	--

**Configure Routing Policy** [/](#)

Name	server_group-hcia	Backend Protocol	HTTP
Load Balancing Algorithm	Weighted round robin	Sticky Session	Disabled
Description	--		

**Add Backend Server** [/](#)

**Backend Servers**

Backend Servers	Private IP Address	Backend Port <a href="#">?</a>	Weight <a href="#">?</a>
ecs-S01 1 vCPUs   1 GB s6.small.1	192.168.0.13	8889	1
ecs-S02 1 vCPUs   1 GB s6.small.1	192.168.1.109	8889	1

Health Check  Enabled  Health Check Protocol

Domain Name  Private IP address of the bac...  Health Check Port

Path   Interval (s)

Timeout (s)   Maximum Retries

### Figure 3-36 Confirm the configuration.

Step 7 After the preceding configuration is complete, the ELB page is automatically displayed. You can view the status of the backend server through the listener.

Name/ID	Monit...	Status	Type	Specifications	IP Address and Network	Listener (Frontend Proto...	Bandwidth Infor...	Billing Mode	Operation
elb-name 0573519a-390e-4900-ba40-a2bd1994d9a3			Shared	Guaranteed Perfo...	192.168.0.214 (Private IP... 119.8.180.158 (IPv4 EIP) VPC-S01 (VPC)	Listener-hc1a (HTTP/8881)	IPv4 1 Mbit/s Pay-per-use By bandw...	Pay-per-use Created at Aug 31...	<a href="#">Add Listener</a> <a href="#">More</a>

Step 8 In the address box of the browser on your PC, enter **http://Load balancer's EIP:8881** to check whether the ECSs can be accessed.

In the following figure, you can see the **SERVER1** file we created earlier, indicating that **ecs-S01** is the one being accessed.

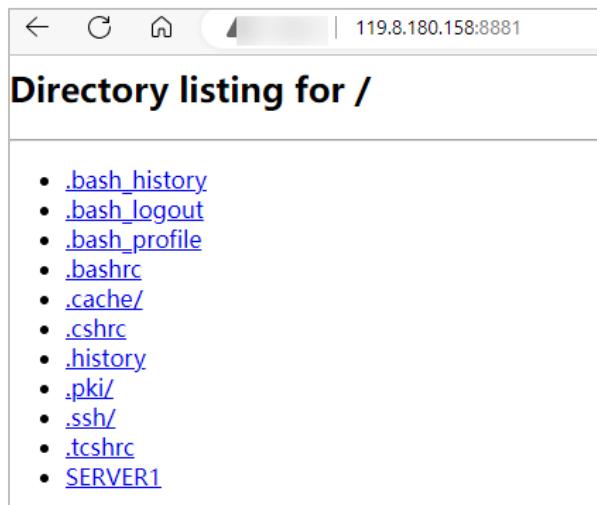


Figure 3-37 Accessing the web page

Step 9 Refresh the browser.

This time **SERVER2** is displayed, indicating that **ecs-S02** is being accessed. As you continue refreshing the browser, the different ECSs are accessed in turn, indicating that the load balancer is balancing the load across the two ECSs.

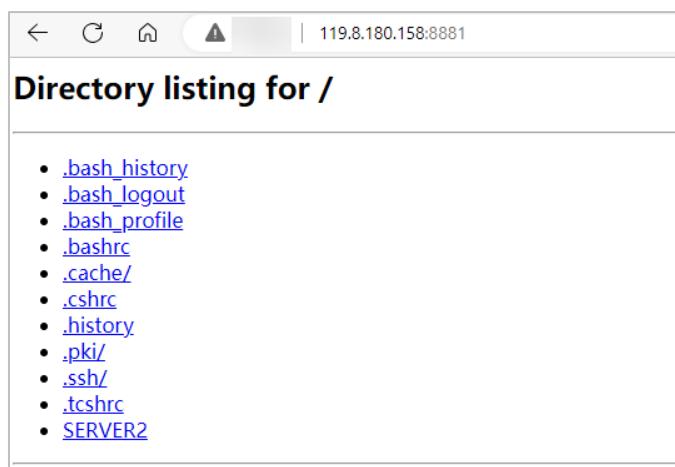


Figure 3-38 Verifying load balancing

You can see from this exercise how ELB automatically distributes incoming traffic across multiple backend servers based on the listening rules you configure.

### 3.2.4.5 Communication Between ECSs in Different VPCs of the Same Region

Tasks:

- Create a VPC peering connection in **AP-Singapore**.
- Configure routes for the two VPCs connected by the VPC peering connection.

Step 1 On the VPC Console, choose VPC Peering and click **Create VPC Peering Connection**.

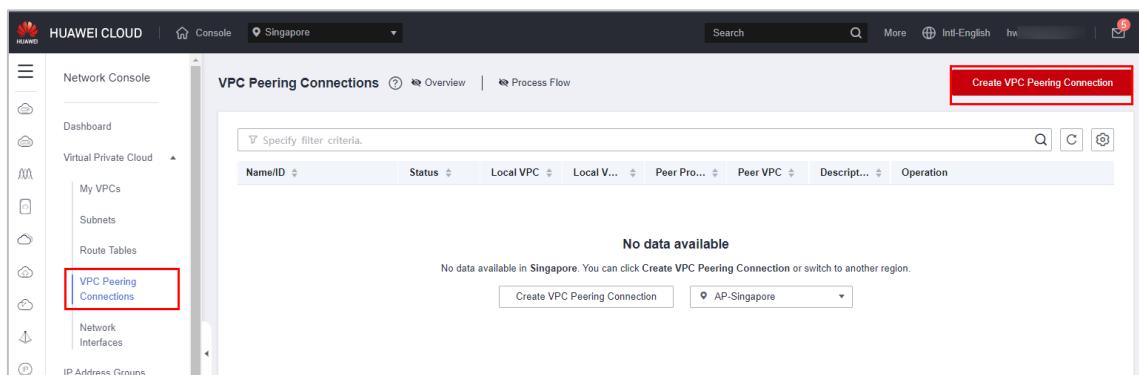


Figure 3-39 Create VPC Peering Connection

Step 2 Configure the VPC peering connection parameters as follows and click **OK**. If the parameters are correct, the status of VPC peering connection will be **Accepted**.

- **Name:** `peering-hcia`(Change it as needed.)
- Choose the local VPC and peer VPC in the same region. Ensure that the CIDR blocks of the two VPCs do not overlap with each other.

**Create VPC Peering Connection**

A VPC peering connection can connect VPCs from the same account or from different accounts as long as they are in the same region.

- Creating a VPC Peering Connection with Another VPC in Your Account
- Creating a VPC Peering Connection with a VPC in Another Account

If you want to connect VPCs in different regions, use Cloud Connect.

★ VPC Peering Connection Name

**Local VPC Settings**

★ Local VPC  C

Local VPC CIDR Block 192.168.0.0/16

**Peer VPC Settings**

★ Account  Another account ?

★ Peer Project  If you select My account, the project is filled in by default.

★ Peer VPC

OK Cancel

**Figure 3-40 Configuring the VPC peering connection**

Name/ID	Status	Local VPC	Local VPC Cl...	Peer Project ID	Peer VPC	Description	Operation
peering-hcia 87a85772-af97-4950-9e73-2b3...	Accepted	VPC-S01	192.168.0.0/16	0aaaa775cc80f 39d2fc3e00326 0f78a4	VPC-S02	--	Modify   Delete

10 Total Records: 1 < 1 >

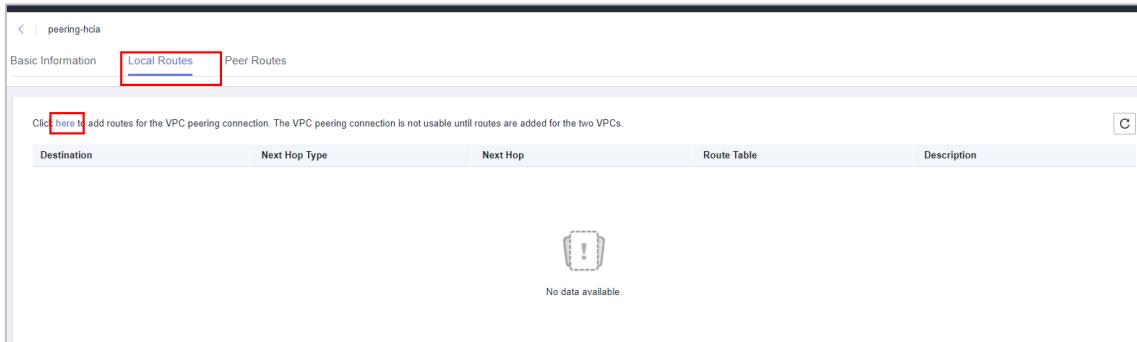
**Figure 3-41 Viewing the VPC peering connection**

Step 3 Click **Add Route** on the **Information** page or click the name of the VPC peering connection and click **Local Routes** to add routes.

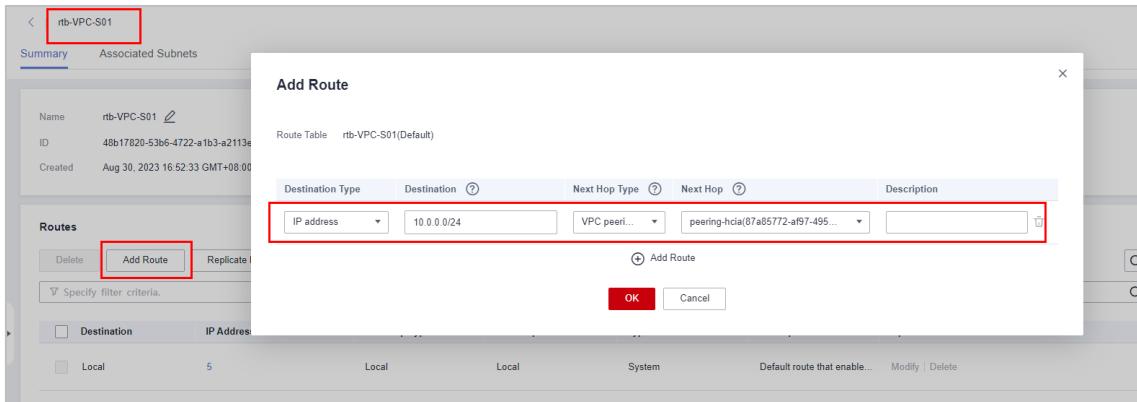
**i Information**

You can now add routes to enable communication between two VPCs.

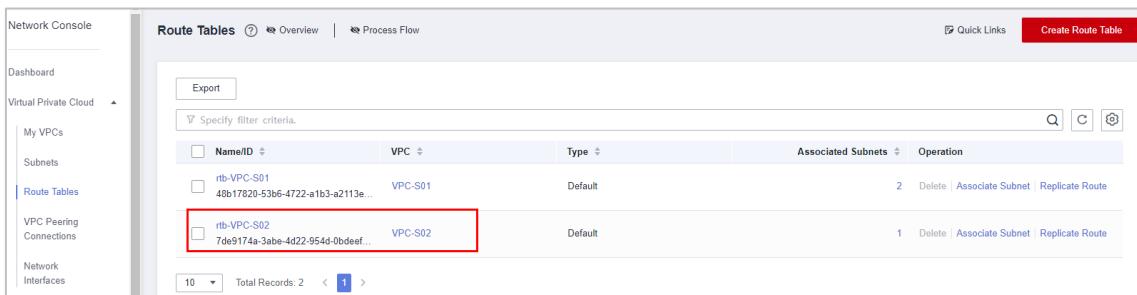
Add Route Add Later

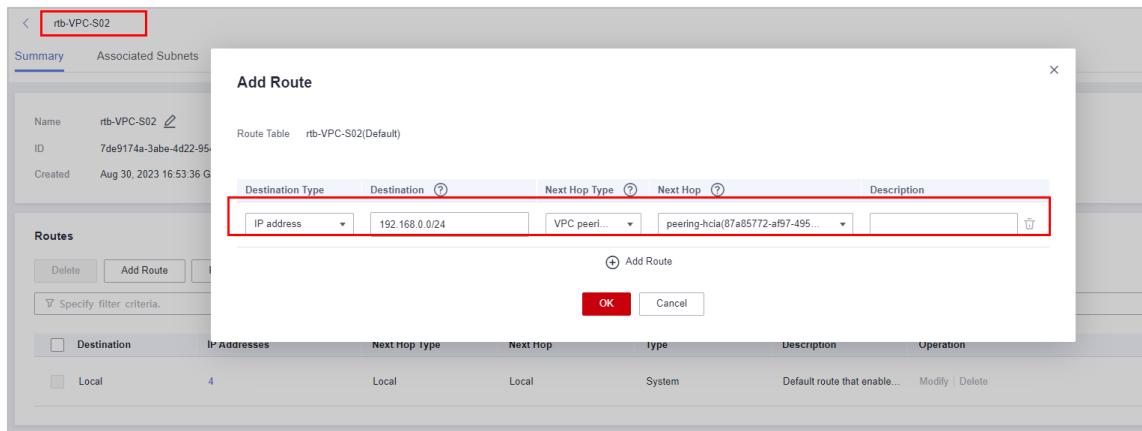
**Figure 3-42 Add Route**

**Figure 3-43 Route Tables**

Step 4 In route table rtb-VPC-S01, click **Add Route**. Set Destination to the CIDR block of VPC-S02, **Next Hop Type** to VPC peering connection, and **Next Hop** to Peering-vivi.


**Figure 3-44 Add Route**

Step 5 Back to Route Tables, in route table rtb-VPC-S02, click **Add Route**. Set Destination to the CIDR block of VPC-S01, **Next Hop Type** to VPC peering connection, and **Next Hop** to Peering-vivi. Click OK.





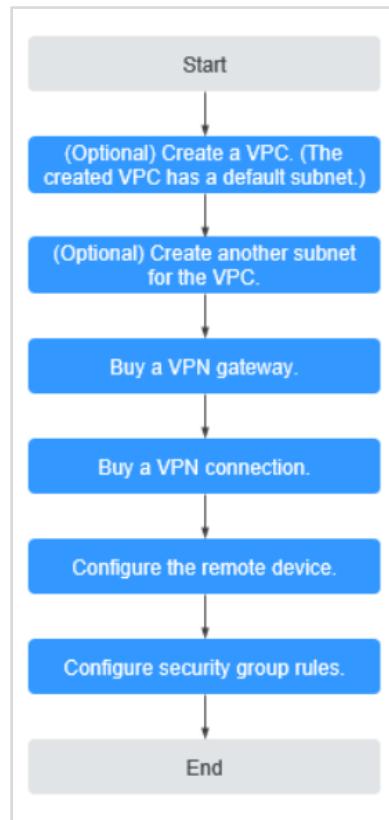
**Figure 3-45 Add Route**

Step 6 Switch to the ECS console, remotely log in to **ecs-S01**, and ping the private IP address of **ecs-S03** in **VPC-S02**. The ping is successful, indicating that ECSs from different VPCs in the same region can communicate with each other over the VPC peering connection.

```
[root@ecs-s01 ~]# ping 10.0.0.29
PING 10.0.0.29 (10.0.0.29) 56(84) bytes of data.
64 bytes from 10.0.0.29: icmp_seq=1 ttl=64 time=0.202 ms
64 bytes from 10.0.0.29: icmp_seq=2 ttl=64 time=0.183 ms
64 bytes from 10.0.0.29: icmp_seq=3 ttl=64 time=0.125 ms
```

### 3.2.4.6 Creating a VPN to Enable Communication Between ECSs in Different Regions

By default, ECSs in a VPC cannot communicate with your local data center or private network. To enable communication between them, use a VPN. The procedure is as follows:



**Figure 3-46 VPN configuration flowchart**

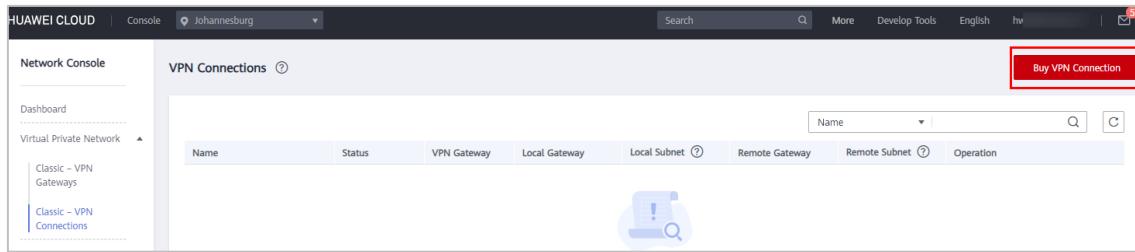
When you configure a VPN connection, note the following:

- The local and remote subnets cannot conflict.
- Different local subnets cannot overlap.
- The local and remote subnets need to use the same IKE and IPsec policies and PSK.
- The local and remote subnet and gateway parameters must be matched pairs.
- The security groups associated with ECSs in the VPC allow traffic to and from your local data center.
- After a VPN is created, its status changes to **Normal** only after the servers on both ends of the VPN communicate with each other.

Tasks:

- Buy VPN gateways in the **AF-Johannesburg** and **AP-Singapore** regions.
- Create a VPN connection.
- Modify security group rules.
- Ping **ecs-J01**, in the **AF-Johannesburg** region, from **ecs-S03**, in the **AP-Singapore** region.
- View the VPN connection status.

Step 1 In the AF-Johannesburg region, access **Network Console**, choose **Virtual Private Network > Classic**, and click **Buy VPN Gateway**.



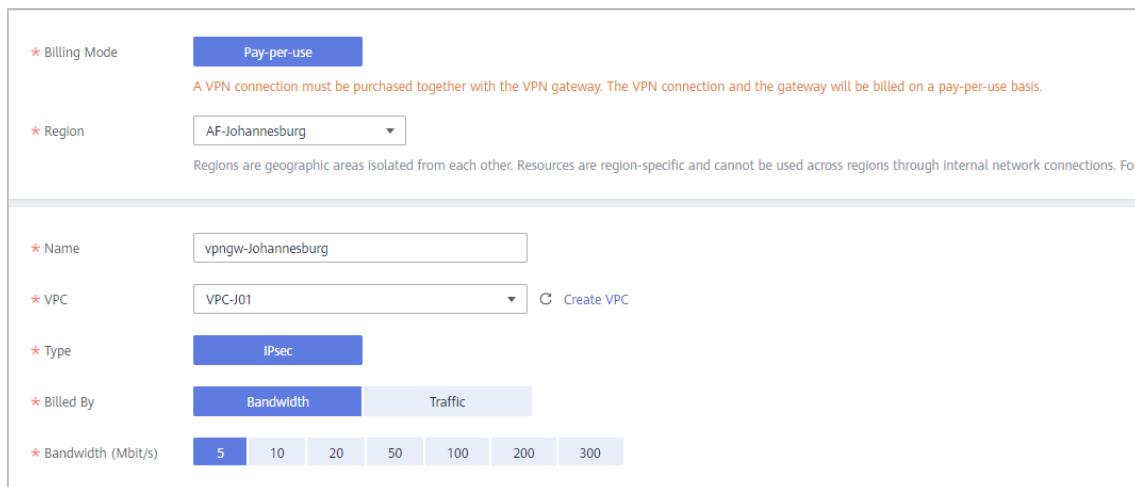
**Figure 3-47 Buy VPN Gateway**

Step 2 Configure VPN gateway parameters and click **Buy Now**.

- Billing Mode: Pay-per-use
- Region: AF-Johannesburg
- Name: vpngw-Johannesburg
- VPC: vpc-J01
- Type: IPsec
- Billed By: Bandwidth
- Bandwidth (Mbit/s): 5

#### VPN connection

- Name: vpn-Johannesburg
- Local Subnet: Select subnet-01 of VPC-J01.
- **Remote Gateway:** Enter an IP address and then replace it with the IP address of the VPN gateway you will create in the **AP-Singapore** region.
- **Remote Subnet:** Enter subnet CIDR blocks of **VPC-S02**.
- **PSK:** Enter a value.
- Advanced Settings: Default



**Figure 3-48 Configuring a VPN gateway**

VPN Connection

\* Name: vpn-Johannesburg

VPN Gateway: vpngw-Johannesburg

\* Local Subnet: Select subnet (subnet-01 (172.16...))

\* Remote Gateway: 1 . 1 . 1 . 1

\* Remote Subnet: 10.0.0.0/24

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

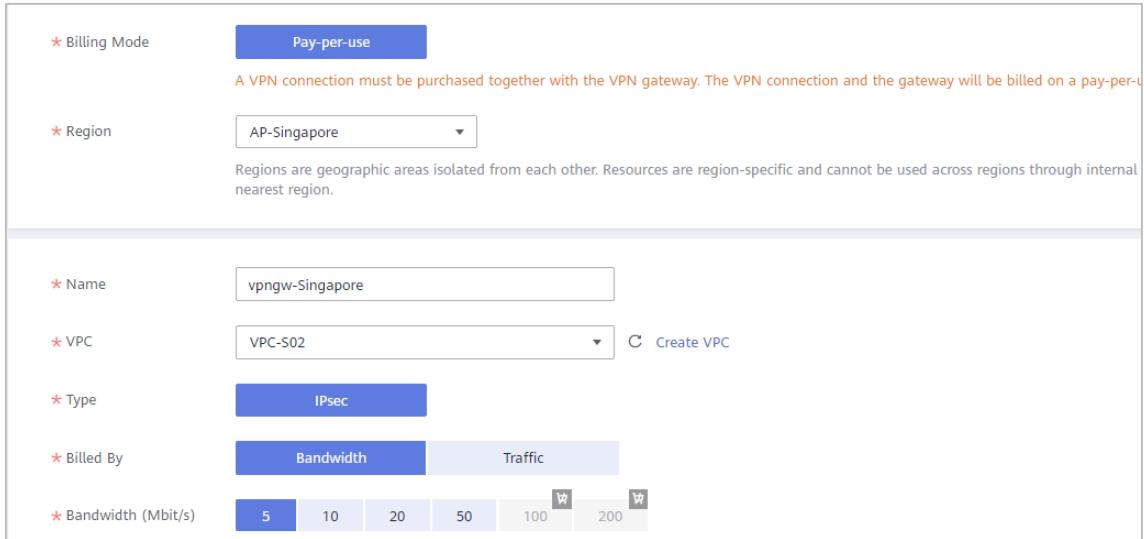
Figure 3-49 Configuring a VPN connection

Step 3 Switch to the AP-Singapore region, go to **Network Console**, choose **Virtual Private Network > Classic**, and click **Buy VPN Gateway**.

- Billing Mode: Pay-per-use
- Region: AP-Singapore
- Name: vpngw-Singapore
- VPC: VPC-S02
- Type: IPsec
- Billed By: Bandwidth
- Bandwidth (Mbit/s): 5

#### VPN connection

- Name: vpn-Singapore
- Local Subnet: Select subnet-03 of VPC-S02.
- **Remote Gateway:** Enter an IP address and then replace it with the IP address of the VPN gateway you created in the **AP-Singapore** region.
- **Remote Subnet:** Enter subnet CIDR blocks of **VPC-J01**.
- **PSK:** Enter the PSK you configured in the **AF-Johannesburg** region.
- **Advanced Settings:** Default



**Billing Mode**

**Region**: AP-Singapore

**Name**: vpngw-Singapore

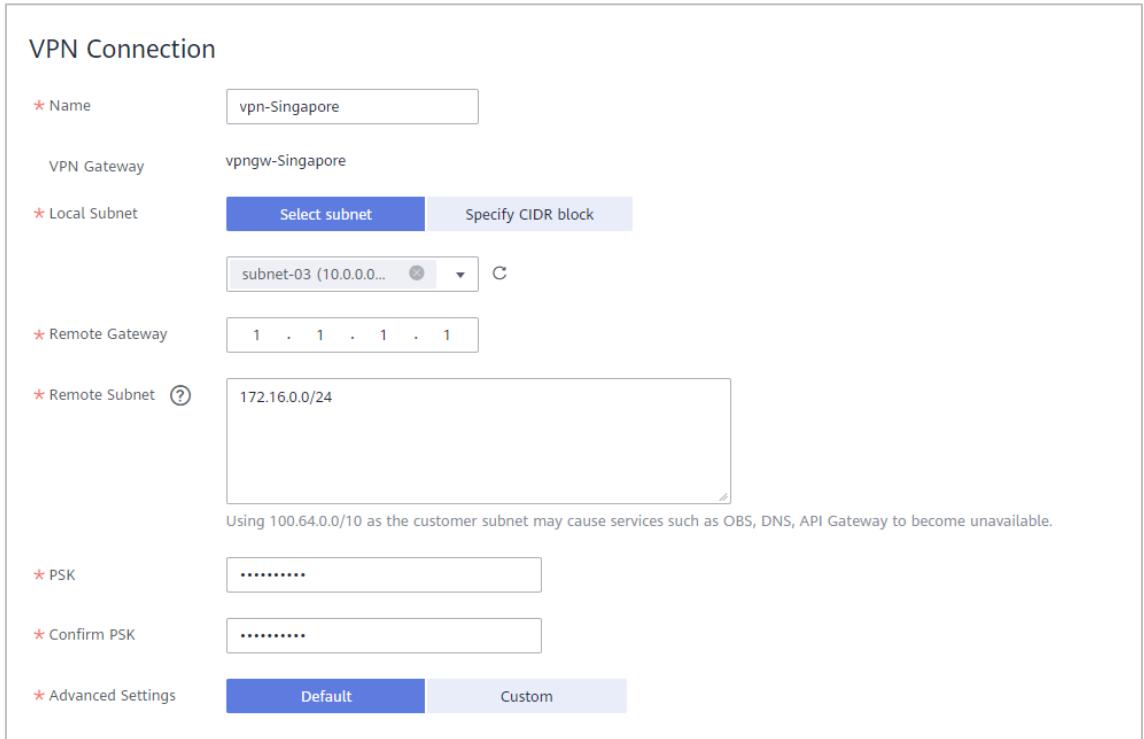
**VPC**: VPC-S02

**Type**: IPsec

**Billed By**: Bandwidth

**Bandwidth (Mbit/s)**: 100

**Figure 3-50 Configuring a VPN gateway**



**VPN Connection**

**Name**: vpn-Singapore

**VPN Gateway**: vpngw-Singapore

**Local Subnet**: Select subnet

**Remote Gateway**: 1.1.1.1

**Remote Subnet**: 172.16.0.0/24

**PSK**: .....

**Confirm PSK**: .....

**Advanced Settings**: Default

**Figure 3-51 Configuring a VPN connection**

Step 4 Go back to the **VPN Gateways** page, locate **vpngw- Singapore**, and record gateway IP address: **159.138.81.127**. Switch to the **AF-Johannesburg** region. Go to the **VPN Connections** page, locate VPN connection **vpn-Johannesburg**, and choose **More > Modify** in the **Operation** column. On the **Modify VPN Connection** page, enter **159.138.81.127** for **Remote Gateway** and click **OK**.

Name	Status	VPC	Type	Gateway IP Address	Bandwidth	Description	Operation
vpngw-Singapore	Not connect...	VPC-502	IPsec	159.138.81.127	5 Mbit/s	--	<a href="#">View Metric</a>   <a href="#">More</a>

Figure 3-52 Viewing a VPN gateway

Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet	Operation
vpn-Johannesburg	Not connected	vpngw-Johannesburg	159.138.161.88	172.16.0.0/24	1.1.1.1	10.0.0.0/24	<a href="#">View Policy</a>   <a href="#">View Metric</a>   <a href="#">More</a>   <a href="#">Modify</a>   <a href="#">Delete</a>

Figure 3-53 Modifying a VPN connection

Basic Information

Name	vpn-Johannesburg	Remote Gateway	159 . 138 . 81 . 127
Local Subnet	Select subnet	Specify CIDR block	10.0.0.0/24
Using 100.64.0.0/10 as the customer subnet may cause services such as OBS, DNS, API Gateway to become unavailable.			

Advanced Settings ▾ PSK IKE Policy IPsec Policy

OK Cancel

Figure 3-54 Changing the remote gateway IP address

Step 5 On the **VPN Gateways** page, locate **vpn-Johannesburg**, and record its IP address: **159.138.161.88**. Switch to the **AP-Singapore** region. Go to the **VPN Connections** page, locate VPN connection **vpn-Singapore**, and choose **More > Modify** in the **Operation** column. On the **Modify VPN Connection** page, enter **159.138.161.88** for **Remote Gateway** and click **OK**.

Name	Status	VPC	Type	Gateway IP Address	Bandwidth	Description	Operation
vpngw-Johannesburg	Normal	VPC-I01	IPsec	159.138.161.88	5 Mbit/s	--	<a href="#">View Metric</a>   <a href="#">More</a>

**Figure 3-55 Changing the remote gateway IP address**

Step 6 Check the VPN connection status. The VPN connection status is **Not connected**.

Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet	Operation
vpn-Singapore	Not connected	vpngw-Singapo...	159.138.81.127	10.0.0.0/24	159.138.161.88	172.16.0.0/24	<a href="#">View Policy</a>   <a href="#">View Metric</a>   More ▾

**Figure 3-56 Viewing a VPN connection**

Step 7 In the **AF-Johannesburg** and **AP-Singapore** regions, configure security groups associated with the ECSs in the VPCs to allow access from and to the peer VPC.

**Figure 3-57 Add Inbound Rule**

Step 8 In the AP-Singapore region, remotely log in to **ecs-S03** in **VPC-S02** and ping **ecs-J01** in **VPC-J01** in the **AF-Johannesburg** region. The result shows that ECSs in different regions can communicate with each other.

```
[root@ecs-s03 ~]# ping 172.16.0.53
PING 172.16.0.53 (172.16.0.53) 56(84) bytes of data.
64 bytes from 172.16.0.53: icmp_seq=1 ttl=64 time=0.210 ms
```

64 bytes from 172.16.0.53: icmp\_seq=2 ttl=64 time=0.190 ms  
 64 bytes from 172.16.0.53: icmp\_seq=3 ttl=64 time=0.136 ms  
 64 bytes from 172.16.0.53: icmp\_seq=4 ttl=64 time=0.134 ms

**Step 9** Go back to the **VPN Connections** page, and refresh the page to check whether status of **vpn-Singapore** is **Normal** and whether status of **vpn- Johannesburg** is **Healthy**.

Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet	Operation
vpn-Singapore	Normal	vpngw-Singapo...	159.138.81.127	10.0.0.0/24	159.138.161.88	172.16.0.0/24	<a href="#">View Policy</a>   <a href="#">View Metric</a>   <a href="#">More</a> ▾

**Figure 3-58 Viewing a VPN connection**

Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet	Operation
vpn-Johannesburg	Normal	vpngw-Johannesbu...	159.138.161.88	172.16.0.0/24	159.138.81.127	10.0.0.0/24	<a href="#">View Policy</a>   <a href="#">View Metric</a>   <a href="#">More</a> ▾

**Figure 3-59 Viewing a VPN connection**

This exercise proves that a VPN can enable communication between ECSs in different regions.

### 3.2.5 Deleting Resources

- Step 1 Delete the ECSs in all regions.
- Step 2 Remove the ECSs from the Backend Server Groups, delete the listener, and then delete the load balancer in the corresponding region.
- Step 3 Delete the VPC peering connection in the corresponding regions.
- Step 4 Delete the VPN connection and gateways in the corresponding regions. If you delete the VPN connection, the gateways will be automatically deleted.
- Step 5 Delete the VPCs and subnets in all regions.

## 3.3 Exercises

1. Create three ECSs in the same VPC, one as the client, and the other two as backend servers to receive requests from the load balancer.
2. Use the client to access the private IP address of the load balancer.  
 If the web page can be accessed and the content changes after you refresh the web page, the configuration was successful. (For details, see the procedure for using a public network load balancer to route requests over the Internet.)
3. Delete the load balancer. If the load balancer cannot be deleted, locate the cause.
4. Verify a VPC peering connection.  
 After you create a VPC peering connection by following the instructions from earlier, create a subnet in the local VPC with the same CIDR block as that of a subnet in the peer VPC. Check network connectivity and explain what you find.
5. Test a VPN connection.



After you establish a VPN connection by following the instructions from earlier, modify the pre-shared key of a VPN gateway and check network connectivity.

# 4 Storage Services

---

## 4.1 EVS

### 4.1.1 Introduction

#### 4.1.1.1 About This Exercise

EVS provides persistent block storage for ECSs and BMSs. With data redundancy and cache acceleration techniques, EVS disks deliver high availability and durability as well as stable, low latency. You can initialize EVS disks, create file systems on them, and store data persistently on them. This exercise describes basic EVS operations, such as purchasing and attaching EVS disks.

#### 4.1.1.2 Objectives

Upon completion of this exercise, you will be able to:

- Purchase EVS disks
- Attach EVS disks
- Initialize EVS disks Linux servers
- Use EVS snapshots

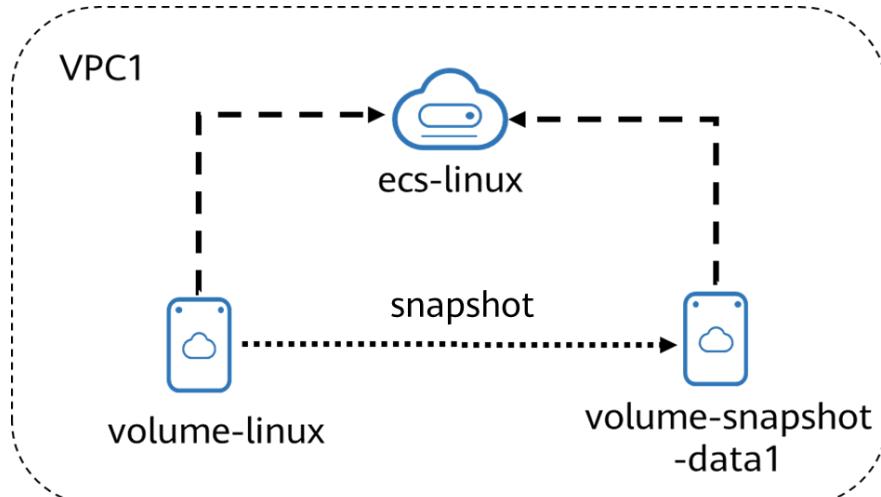
## 4.1.2 Tasks

### 4.1.2.1 Roadmap

EVS disks are usually used to increase user's storage space to meet their business needs. You can buy EVS disks for use, or detach and delete them if they are no longer required. This exercise introduces how to use an EVS disk in Linux.

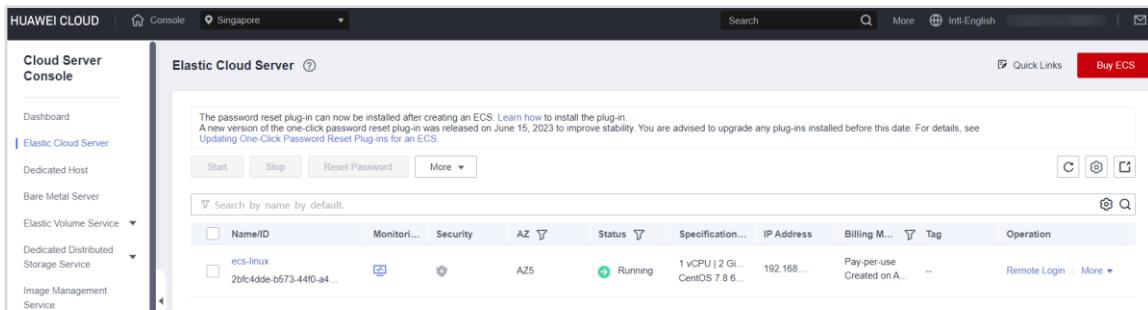
- EVS disks can be used as system disks or data disks for cloud servers. When a cloud server is purchased, a system disk is automatically purchased and attached. You cannot purchase a system disk separately.
- Data disks can be purchased during or after the server purchase. If you add data disks during the server purchase, the system will automatically attach the data disks to the server. If you purchase data disks after the server has been purchased, you need to manually attach the data disks.
- In this exercise, we will buy a Linux ECS **volume-data1** in the **AP-Singapore** region, buy an EVS disk separately and attach it to ECS **ecs-linux**, and log in to ECS **ecs-linux** to check whether the test file exists.

#### 4.1.2.2 Attaching an EVS Disk to a Linux ECS



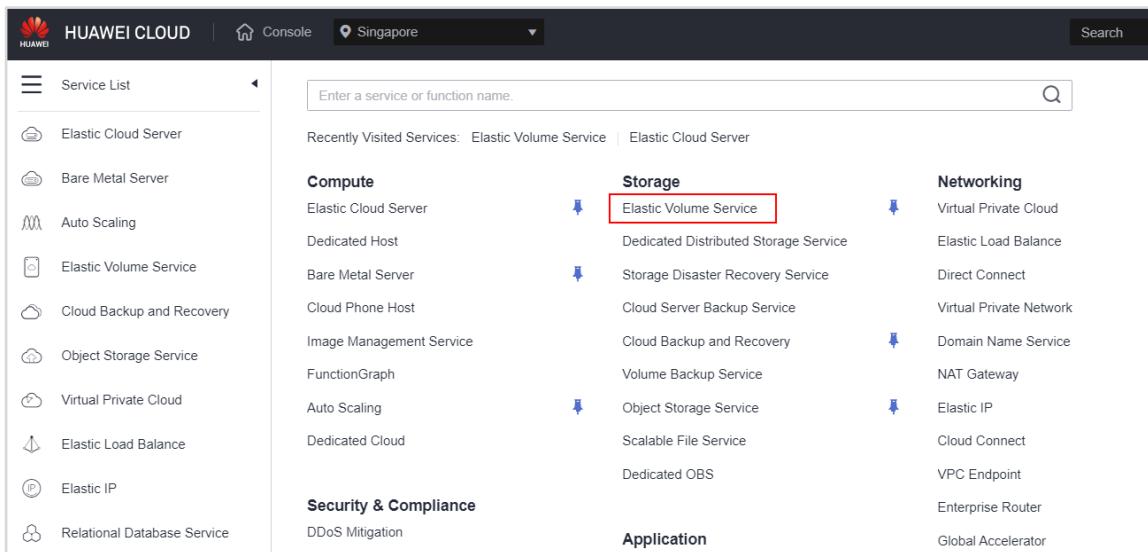
**Figure 4-1 topology diagram**

- Step 1 Repeat the preceding steps to create a VPC, subnet, and security group.
- Step 2 Buy a Linux ECS ( CentOS 7.6 64 bit) by referring to the preceding sections (x86 | General computing | 1 vCPU | 2 GiB | SSD 40 GiB| CentOS 7.8 | Not EIP) .



**Figure 4-2 Creating a Linux ECS**

- Step 3 In the **service list**, choose **Elastic Volume Service** under Storage to go to the **Elastic Volume Service** page.



**Figure 4-3 Selecting the EVS service**

Step 4 On the Elastic Volume Service page, select **Buy Disk**.

- AZ: Select the AZ where your server resides
- Billing Mode: **Pay-per-use**
- Disk Specifications: General Purpose SSD 10 GiB
- Automatic Backup: **by default**
- Disk Name: **volume-linux** (custom)

**Figure 4-4 Buying an EVS disk**

Step 5 Go back to the **disk list** page and view the disk status (10 GiB). When the disk status changes to **Available**, the disk has been purchased.

In the **EVS disk list**, locate the EVS disk to be attached and click **Attach** in the Operation column.

Disk Name	Status	Dis...	Functi...	Serve...	Dis...	De...	En...	AZ	Bill...	Operation
volume-linux a25281ce-5986-468f-9518-5...	Av...	Gener... 10 GiB	Data d...	--	Disabled	VBD	No	AZ5	Pay-p... Create...	<a href="#">Attach</a> <a href="#">Expand Capacity</a> <a href="#">Create Backup</a> <a href="#">More</a>
ecs-linux 2b2bca4b-f52b-49b2-b6c3-4b...	In...	Gener... 40 GiB	Syste...	ecs-linux ECS	Disabled	VBD	No	AZ5	Pay-p... Create...	<a href="#">Attach</a> <a href="#">Expand Capacity</a> <a href="#">Create Backup</a> <a href="#">More</a>

Figure 4-5 Viewing the newly purchased EVS disk

Select the target Linux ECS and select a mount point from the drop-down list. The ECS and EVS disk must be in **the same AZ**. /dev/sdb is used as an example.

### Attach Disk

Disk: volume-linux | Singapore | AZ5 | VBD | Non-shareable

ECss
BMS

Name	Function	Billing Mode	Status	Image	Private IP ...	EIP	AZ
ecs-linux	/dev/vdb	Pay-per-use	Running	CentOS 7....	192.168.1....	--	AZ5

Figure 4-6 Attaching an EVS disk

Step 6 After the attachment is complete, check whether the EVS disk has been attached to ecs-linux.

Disk Name	Status	Dis...	Functi...	Serve...	Dis...	De...	En...	AZ	Bill...	Operation
volume-linux a25281ce-5986-468f-9518-5...	In...	Gener... 10 GiB	Data d...	ecs-linux ECS	Disabled	VBD	No	AZ5	Pay-p... Create...	<a href="#">Attach</a> <a href="#">Expand Capacity</a> <a href="#">Create Backup</a> <a href="#">More</a>
ecs-linux 2b2bca4b-f52b-49b2-b6c3-4b...	In...	Gener... 40 GiB	Syste...	ecs-linux ECS	Disabled	VBD	No	AZ5	Pay-p... Create...	<a href="#">Attach</a> <a href="#">Expand Capacity</a> <a href="#">Create Backup</a> <a href="#">More</a>

Figure 4-7 Viewing attached EVS disks

Step 7 Remotely log in to the Linux ECS and run the following command to view the new data disk.

The command output shows that the ECS has two disks, system disk /dev/vda and data disk /dev/vdb.

```

Welcome to Huawei Cloud Service

[root@ecs-linux ~]# 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: 0x000a952a

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-linux ~]#
```

Step 8 Run the following command to enter fdisk to partition the new data disk.

In this example, run the following command:

```
[root@ecs-linux ~]# fdisk /dev/vdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0xff76a2ae.
```

Step 9 Create partition.

Enter **n** and press Enter to create a partition;

enter **p** and press Enter to create a primary partition;

Enter the partition number of the primary partition and press Enter. Partition number 1 is used in this example;

First sector and Last sector is default.

```
Command (m for help): n
Partition type:
  p  primary (0 primary, 0 extended, 4 free)
  e  extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519):
Using default value 20971519
Partition 1 of type Linux and of size 10 GiB is set
```

Step 10 View and save the partition information.

Enter **p** and press Enter to view details about the new partition;

Enter **w** and press Enter to write the changes into the partition table.

```
Command (m for help): p

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
Disk label type: dos
Disk identifier: 0xff76a2ae

      Device Boot      Start        End      Blocks   Id  System
  /dev/vdb1            2048    20971519     10484736   83  Linux

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

Step 11 Run partprobe command to synchronize the changes in the partition table to the OS.

```
[root@ecs-linux ~]# 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: 0x000a952a

      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
Disk label type: dos
Disk identifier: 0xff76a2ae

      Device Boot      Start        End      Blocks   Id  System
  /dev/vdb1            2048    20971519     10484736   83  Linux
[root@ecs-linux ~]# partprobe
[root@ecs-linux ~]
```

Step 12 Run the following command to set the file system format for the new partition.  
mkfs.system format /dev/vdb1.

In this example, run the following command to set the ext4 file system for the new partition.

```
[root@ecs-linux ~]# mkfs.ext4 /dev/vdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
655360 inodes, 2621184 blocks
131059 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
```

Step 13 Run the following command to create a mount point.

In this example, run the **mkdir** command to create a mount point /mnt/data:

Run the **df** command to check the new folder. Although the folder is created, the file system is not mounted to the mount point.

```
[root@ecs-linux ~]# mkdir /data
[root@ecs-linux ~]# df -Th
Filesystem      Type      Size  Used Avail Use% Mounted on
devtmpfs        devtmpfs  909M    0  909M  0% /dev
tmpfs          tmpfs     919M    0  919M  0% /dev/shm
tmpfs          tmpfs     919M   8.6M  911M  1% /run
tmpfs          tmpfs     919M    0  919M  0% /sys/fs/cgroup
/dev/vda1       ext4      40G   2.4G  35G  7% /
tmpfs          tmpfs    184M    0  184M  0% /run/user/0
[root@ecs-linux ~]#
```

Step 14 Run the following command to mount the new partition on the created mount point.

In this example, run the **mount** command to mount the new partition on /mnt/data, run the **df** command to view the mount result.

```
[root@ecs-linux ~]# mount /dev/vdb1 /data
[root@ecs-linux ~]# df -Th
Filesystem      Type      Size  Used Avail Use% Mounted on
devtmpfs        devtmpfs  909M    0  909M  0% /dev
tmpfs          tmpfs     919M    0  919M  0% /dev/shm
tmpfs          tmpfs     919M   8.6M  911M  1% /run
tmpfs          tmpfs     919M    0  919M  0% /sys/fs/cgroup
/dev/vda1       ext4      40G   2.4G  35G  7% /
tmpfs          tmpfs    184M    0  184M  0% /run/user/0
/dev/vdb1       ext4      9.8G  37M  9.2G  1% /data
```

Step 15 New partition /dev/vdb1 has been mounted on /mnt/sdc. In the new partition, run the **touch** command to create a file. Creating the evs file is used as an example.

```
[root@ecs-linux ~]# cd /data
[root@ecs-linux data]# touch evs
[root@ecs-linux data]# ls
```

```
evs lost+found
```

Step 16 Run the **vi** command to write content in the new file.

Run the **vi** command to access the file page and enter **i** to enter the editing mode. Press **ESC** and enter **:wq** to save the settings and exit.

Run the **cat** command to view the file content.

```
[root@ecs-linux data]# vi evs
[root@ecs-linux data]# cat evs
HUAWEI CLOUD
[root@ecs-linux data]
```

#### 4.1.2.3 Setting Automatic Mounting at System Start

Step 1 In the Linux ECS, The disk mounted using the **mount** command cannot be automatically mounted upon system startup. That is, the mounting becomes invalid after the system restarts. You are advised to configure automatic mounting upon system startup.

```
[root@ecs-linux ~]# vi /etc/fstab
```

Step 2 Edit the configuration file and enter **i** to enter the editing mode. At the bottom of the file, enter the configuration information about the disk to be started.

After editing the file, press **ESC** and enter **:wq** to exit the file editing.

```
# /etc/fstab
# Created by anaconda on Thu Feb 10 07:01:09 2022
#
# 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=6c533615-cacd-47a7-844e-10013da6d35b /           ext4    defaults      1
1
/dev/vdb1      /data    ext4    defaults      0 0
```

Step 3 Run the **umount** command to unmount the mounted partition. Run the **df** command. The information about the mounted disk is not displayed.

```
[root@ecs-linux ~]# umount /dev/vdb1
[root@ecs-linux ~]# df -Th
Filesystem  Type  Size  Used  Avail Use% Mounted on
devtmpfs    devtmpfs 909M   0  909M  0% /dev
tmpfs       tmpfs   919M   0  919M  0% /dev/shm
tmpfs       tmpfs   919M  8.6M  911M  1% /run
tmpfs       tmpfs   919M   0  919M  0% /sys/fs/cgroup
/dev/vda1    ext4   40G  2.4G  35G  7% /
tmpfs       tmpfs  184M   0  184M  0% /run/user/0
```

Step 4 Run the **mount** command to reload all contents in the /etc/fstab file. The information about the mounted disk is displayed again. Verify that the written configuration file is normal.

```
[root@ecs-linux ~]# mount -a
[root@ecs-linux ~]# df -Th
Filesystem      Type      Size  Used Avail Use% Mounted on
devtmpfs        devtmpfs  909M   0  909M  0% /dev
tmpfs           tmpfs     919M   0  919M  0% /dev/shm
tmpfs           tmpfs     919M  8.6M  911M  1% /run
tmpfs           tmpfs     919M   0  919M  0% /sys/fs/cgroup
/dev/vda1        ext4      40G  2.4G  35G  7% /
tmpfs           tmpfs     184M   0  184M  0% /run/user/0
/dev/vdb1        ext4      9.8G  37M  9.2G  1% /data
```

Step 5 Run the **reboot** command to restart the Linux host.

```
[root@ecs-linux ~]# reboot
```

Step 6 After the restart is complete, run the **df** command to check whether the new partition is automatically mounted.

```
Welcome to Huawei Cloud Service

[root@ecs-linux ~]# df -Th
Filesystem      Type      Size  Used Avail Use% Mounted on
devtmpfs        devtmpfs  909M   0  909M  0% /dev
tmpfs           tmpfs     919M   0  919M  0% /dev/shm
tmpfs           tmpfs     919M  8.6M  911M  1% /run
tmpfs           tmpfs     919M   0  919M  0% /sys/fs/cgroup
/dev/vda1        ext4      40G  2.4G  35G  7% /
/dev/vdb1        ext4      9.8G  37M  9.2G  1% /data
tmpfs           tmpfs     184M   0  184M  0% /run/user/0
[root@ecs-linux ~]#
```

#### 4.1.2.4 (Optional) Using Snapshots

Step 1 On the ecs-linux ECS, view the new file.

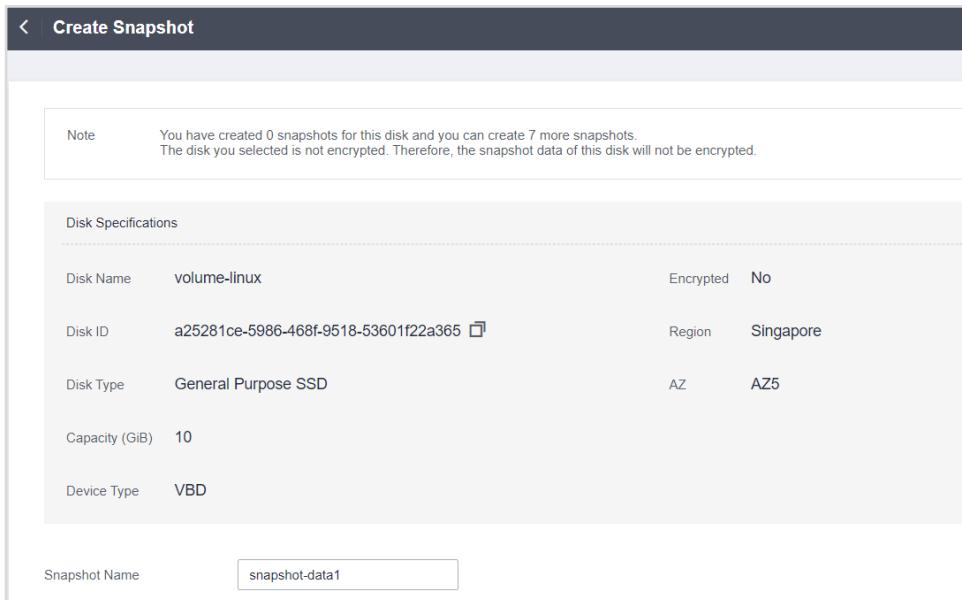
```
[root@ecs-linux ~]# cat /data/evs
HUAWEI CLOUD
[root@ecs-linux ~]#
```

Step 2 On the EVS page, Locate the EVS disk (volume-linux) purchased before and choose More > **Create Snapshot** in the Operation column.

Disk Name	Status	Dis...	Functi...	Serve...	Dis...	De...	En...	AZ	Bill...	Operation
volume-linux a25281ce-5986-468f-9518-5...	● In...	Gener... 10 GiB	Data d...	ecs-linux ECS	Disabled	VBD	No	AZ5	Pay-p... Create...	Attach   Expand Capacity   Create Backup   More ▾
ecs-linux 2b2bca4b-f52b-49b2-b6c3-4b...	● In...	Gener... 40 GiB	System...	ecs-linux ECS	Disabled	VBD	No	AZ5	Pay-p... Create...	Attach   Expand Capacity Create Snapshot Change Billing Mode

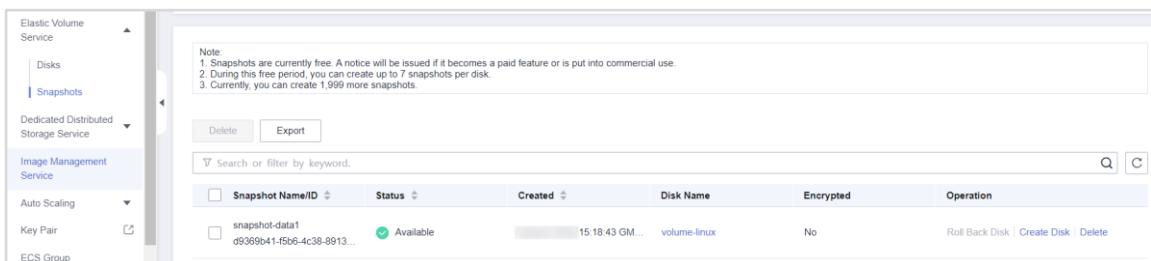
### Figure 4-8 Creating a Snapshot

Step 3 Name the snapshot **volume-data1** and click **Create Now**.



### Figure 4-9 Configuration snapshot

Step 4 Return to the snapshot page and wait until the snapshot is created.



### Figure 4-10 Creating a disk

Step 5 Return to the CLI of the Linux operating system and run the **cat** command to view the file information.

```
[root@ecs-linux ~]# cd /data/
[root@ecs-linux data]# ls
evs  lost+found
[root@ecs-linux data]# cat evs
HUAWEI CLOUD
[root@ecs-linux data]#
```

Step 6 Run the **rm** command to delete the newly created **evs** file and simulate file loss.

```
[root@ecs-linux data]# rm evs
rm: remove regular file 'evs'? y
[root@ecs-linux data]# ls
lost+found
[root@ecs-linux data]#
```

**Step 7** Go back to the **disk list**. Choose Snapshots in the navigation pane on the left, locate the **volume-data1** snapshot, and click **Create Disk** in the Operation column.

Snapshot Name/ID	Status	Created	Disk Name	Encrypted	Operation
snapshot-data1 d6efa855-f74f-49d4-9ab2-...	Available	GM...	volume-linux	No	Roll Back Disk <span style="border: 1px solid red; padding: 2px;">Create Disk</span> Delete

**Figure 4-11 Creating disk**

**Step 8** **Buy a disk** according to the following figure. The name of the new disk is **“volume-snapshot-data1”**. Retain the default values for other parameters. After confirming that the disk is correct, complete the disk purchase.

Region AP-Singapore
 

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

AZ AZ5 (1)
 

There are 1 servers in the current AZ. Select the AZ where your server resides. The AZ cannot be changed after the disk is created.

Attach To Server Now Later
 

When you attach the disk to a server, you can choose to do it now or later. If you choose later, you can attach the disk to a server at any time.

Billing Mode Yearly/Monthly Pay-per-use
 

Pay-per-use billing mode allows you to pay only for the storage capacity you use. You can switch between yearly/monthly and pay-per-use modes at any time.

Data Source (Optional) Source Snapshot: snapshot-data1(d6efa855-f74f-49d4-9ab2-7...)
 

Select a source snapshot to create a new disk. You can also cancel the operation.

Disk Specifications General Purpose SSD - 10 + GiB
 

Configure disk specifications. You can choose a general purpose SSD and specify its size (10 GiB). You can also increase or decrease the size.

Selected Specifications General Purpose SSD | 10 GiB IOPS limit: 1,920, IOPS burst limit: 8,000
 

Summary of selected disk specifications.

Automatic Backup Cloud Backup and Recovery (CBR) allows you to back up and restore the disk data to any backup point. To use CBR, buy a disk backup backups.
 

Configure automatic backup settings. You can choose to use existing or buy new backup services.

Do not use Use existing Buy new

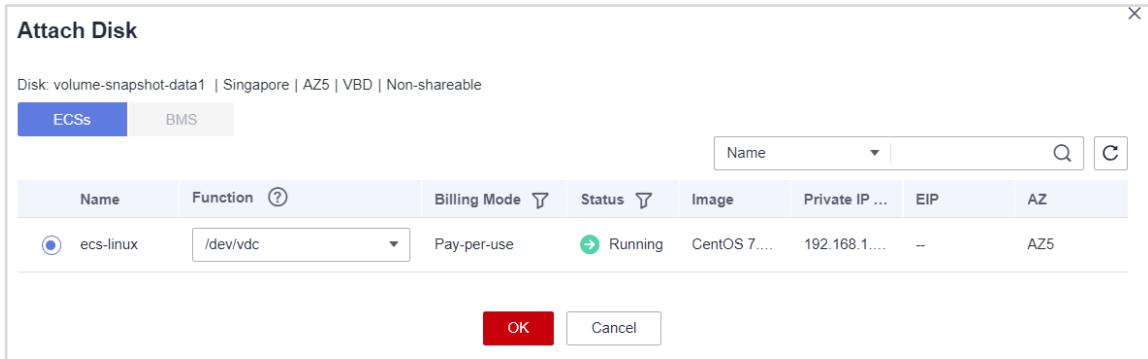
**Figure 4-12 Buying a New Disk**

**Step 9** View the disk(**volume-snapshot-data1**) created from the snapshot.

Elastic Volume Service											Buy Disk
You can create 397 more disks with 32,708 GiB of storage space. To renew multiple disks at a time, switch to the Renewals page.											
Disk Name Status Dis... Funct... Server... Dis... De... En... AZ... Bill... Operation											
volume-snapshot-data1 9cde25c7-47e4-43c1-bdda-8e...	Available	Gener...	Data d...	--	Disabled	VBD	No	A25	Pay-p... Create...	<span style="border: 1px solid red; padding: 2px;">Attach</span> Expand Capacity   Create Backup   More ▾	
volume-linux a25281ce-5986-468f-9518-53...	In use	Gener...	Data d...	ECS	Disabled	VBD	No	A25	Pay-p... Create...	Attach   Expand Capacity   Create Backup   More ▾	
ecs-linux 2b2bca4b-f52b-49b2-b6c3-4b...	In use	Gener...	System...	ECS	Disabled	VBD	No	A25	Pay-p... Create...	Attach   Expand Capacity   Create Backup   More ▾	

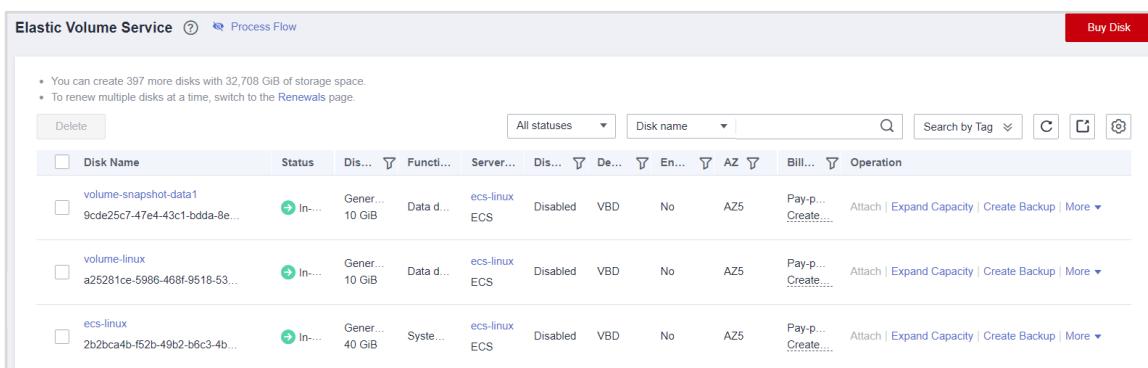
**Figure 4-13 Viewing the new disk**

**Step 10** Select a mount point to mount the disk.



**Figure 4-14 Mounting a disk**

Step 11 Check the disk information.



**Figure 4-15 Configuring Disks**

Step 12 Log in to ECS ecs-linux and view the new data disk. If no disk is added, you are advised to restart the system and check the disk.

The /dev/vdc disk with a capacity of 10 GB is added. This disk is the disk created using the snapshot.

```
[root@ecs-linux ~]# 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: 0x000a952a

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
Disk label type: dos
Disk identifier: 0xff76a2ae

Device Boot      Start         End      Blocks   Id  System
```

```
/dev/vdb1      2048  20971519  10484736  83  Linux

Disk /dev/vdc: 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
Disk label type: dos
Disk identifier: 0xff76a2ae

Device Boot   Start     End   Blocks Id System
/dev/vdc1      2048  20971519  10484736  83  Linux
[root@ecs-linux ~]#
```

Step 13 Create a mount point **/snapshot-data**.

```
[root@ecs-linux ~]# mkdir /snapshot-data
```

Step 14 Run the mount command to mount the newly discovered disk vdc to **/snapshot-data**.

```
[root@ecs-linux ~]# mount /dev/vdc1 /snapshot-data
[root@ecs-linux ~]# df -Th
Filesystem      Type      Size  Used Avail Use% Mounted on
devtmpfs        devtmpfs  909M    0  909M  0% /dev
tmpfs          tmpfs    919M    0  919M  0% /dev/shm
tmpfs          tmpfs    919M  8.6M  911M  1% /run
tmpfs          tmpfs    919M    0  919M  0% /sys/fs/cgroup
/dev/vda1       ext4     40G  2.4G  35G  7% /
/dev/vdb1       ext4     9.8G  37M  9.2G  1% /data
tmpfs          tmpfs   184M    0  184M  0% /run/user/0
/dev/vdc1       ext4     9.8G  37M  9.2G  1% /snapshot-data
[root@ecs-linux ~]#
```

Step 15 Switch to the **/snapshot-data** directory and view the deleted evs file and its content.

```
[root@ecs-linux ~]# cd /snapshot-data/
[root@ecs-linux snapshot-data]# ls
evs  lost+found
[root@ecs-linux snapshot-data]# cat evs
HUAWEI CLOUD
[root@ecs-linux snapshot-data]#
```

## 4.2 OBS

### 4.2.1 Introduction

#### 4.2.1.1 About This Exercise

OBS provides a stable, secure cloud storage with high scalability and ease of use. It allows users to store virtually any amount of unstructured data in any format, and allows them

to access data from anywhere using REST APIs. This exercise describes how to use OBS Browser+ to manage object storage.

### 4.2.1.2 Objectives

Upon completion of this exercise, you will be able to:

- Have a good command of how to use OBS in web mode.
- Understand how to use OBS Browser+.

### 4.2.2 Tasks

#### 4.2.2.1 Roadmap

- To log in to the cloud service console using a browser to access OBS, you need to log in to the console using a HUAWEI CLOUD account or IAM user. In this scenario, OBS uses the account or IAM user information for authentication.
- When you use other methods to access OBS, such as OBS Browser+, obsutil, SDK, or APIs, the access key (AK/SK) of the user is used for authentication. Therefore, before using these methods to access OBS, you need to obtain the access key (AK/SK) in advance.

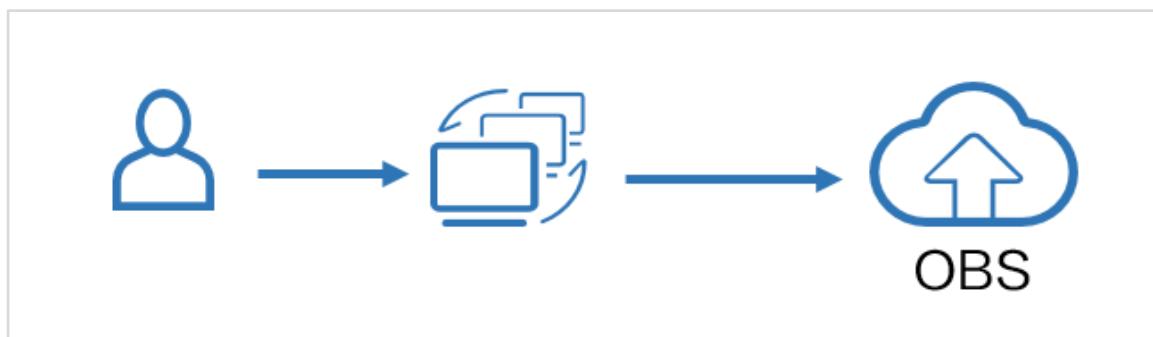
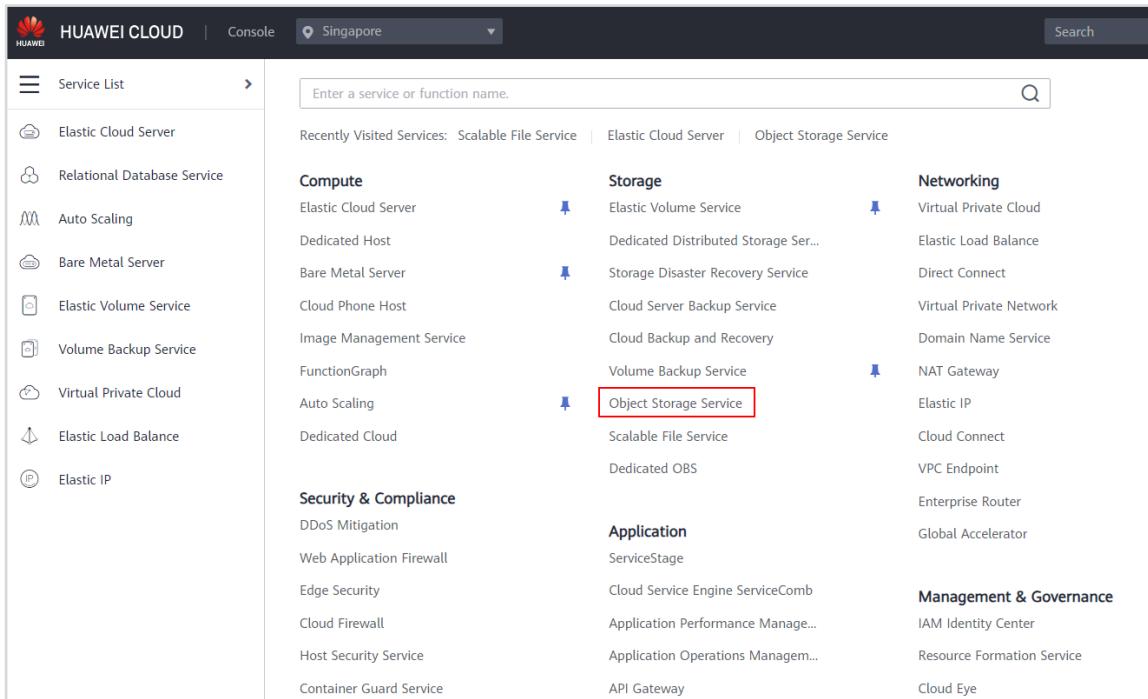


Figure 4-16 Lab Topology

#### 4.2.2.2 Creating a Bucket

Step 1 Log in to the HUAWEI CLOUD console. In the **service list**, choose **Storage > Object Storage OBS**. The Object Storage Service page is displayed.

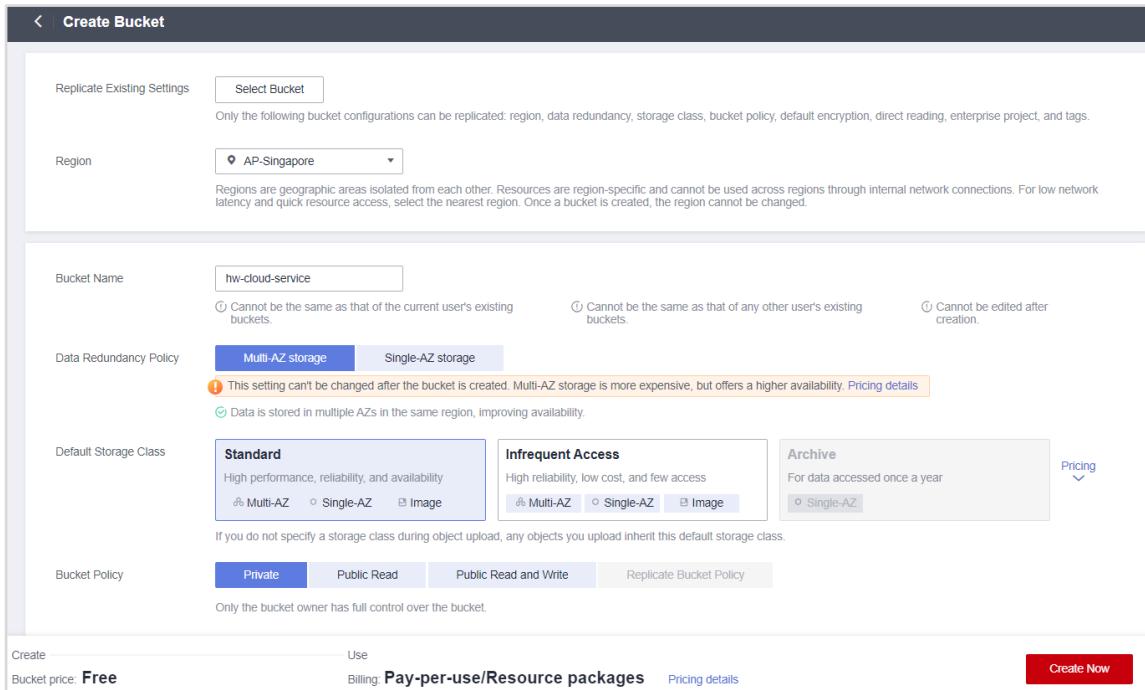


**Figure 4-17 OBS**

**Step 2** On the **Object Storage Service** page, Click **Create Bucket** in the upper right corner of the page to create a bucket. Set the following parameters and click **Create Now**.

- Bucket Name: **hw-cloud-service** ( custom )
- Data Redundancy Policy: **Multi-AZ-storage**
- Default Storage Class: **Standard**
- Bucket Policy: **Private**
- Retain the default values for other parameters

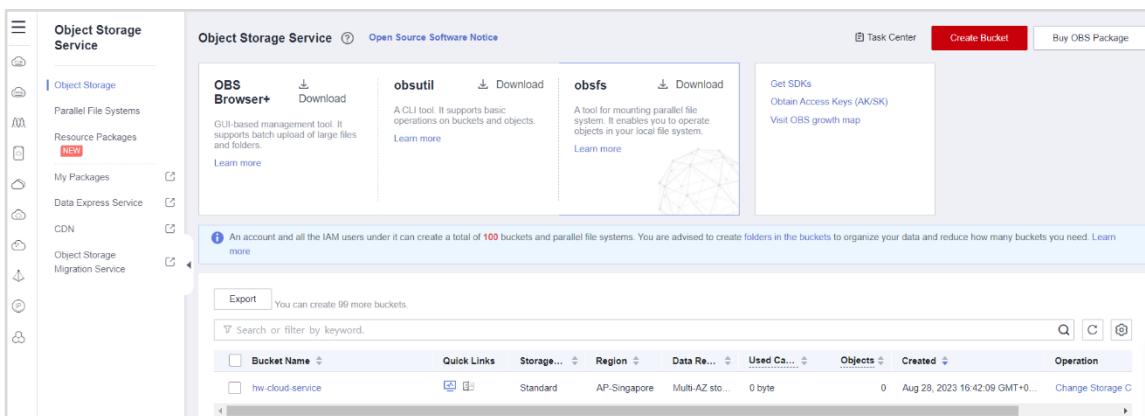
The bucket name must be globally unique and cannot be modified after being created.



The screenshot shows the 'Create Bucket' interface. At the top, there's a 'Replicate Existing Settings' section with a 'Select Bucket' button. Below it is a 'Region' dropdown set to 'AP-Singapore'. The 'Bucket Name' field contains 'hw-cloud-service'. Under 'Data Redundancy Policy', 'Multi-AZ storage' is selected. In the 'Default Storage Class' section, 'Standard' is chosen. The 'Bucket Policy' is set to 'Private'. At the bottom right is a large red 'Create Now' button.

**Figure 4-18 Creating an OBS bucket**

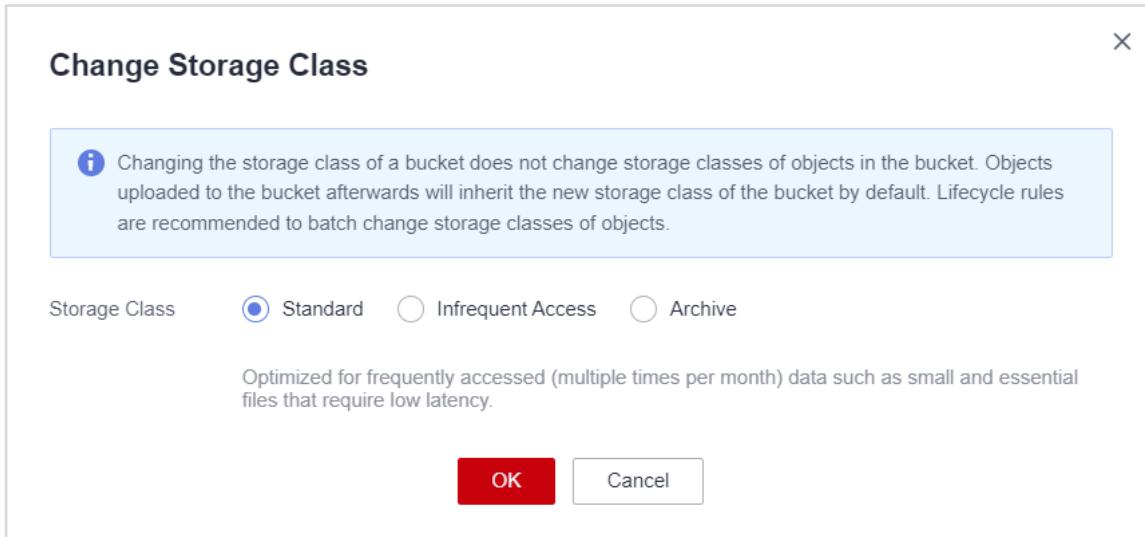
Step 3 After the OBS bucket is created, view the created bucket on the OBS page.



The screenshot shows the OSS service page. On the left, there's a sidebar with various options like Object Storage, Parallel File Systems, Resource Packages, My Packages, Data Express Service, CDN, and Object Storage Migration Service. The main area displays the 'Object Storage Service' with sections for 'OBS Browser', 'obsutil', 'obsfs', and 'Get SDKs'. Below this, there's a note about creating buckets and a 'Create Bucket' button. The main content area shows a table of buckets. One row is highlighted for 'hw-cloud-service', which was just created. The table includes columns for Bucket Name, Quick Links, Storage..., Region, Data Re..., Used Ca..., Objects, Created, and Operation. The 'Operation' column for this row contains a link labeled 'Change Storage C'.

**Figure 4-19 Viewing the newly created bucket**

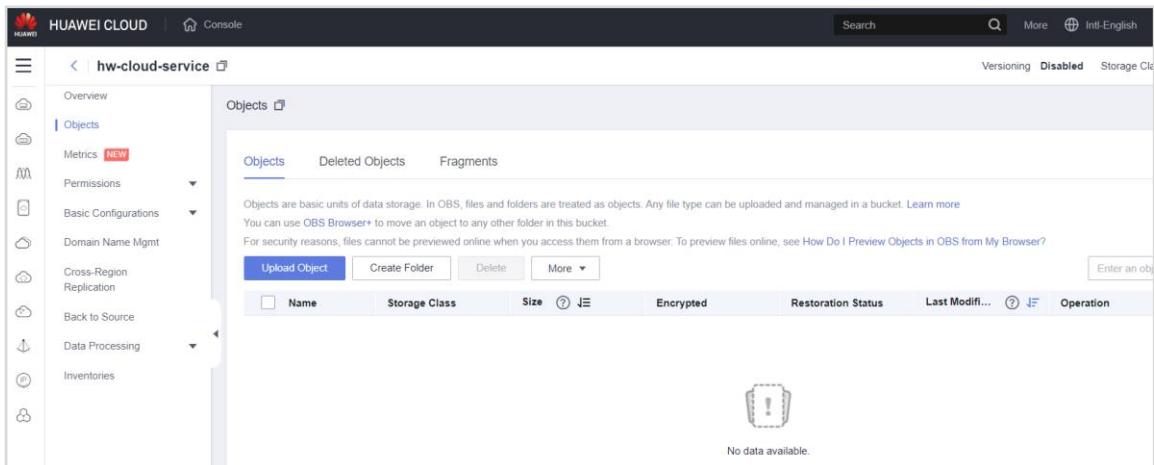
Step 4 (optional) In the Operation column of the bucket list, click **Change Storage Class** to modify the storage class of the bucket.



**Figure 4-20 Bucket Category Information**

#### 4.2.2.3 Uploading a File or Folder

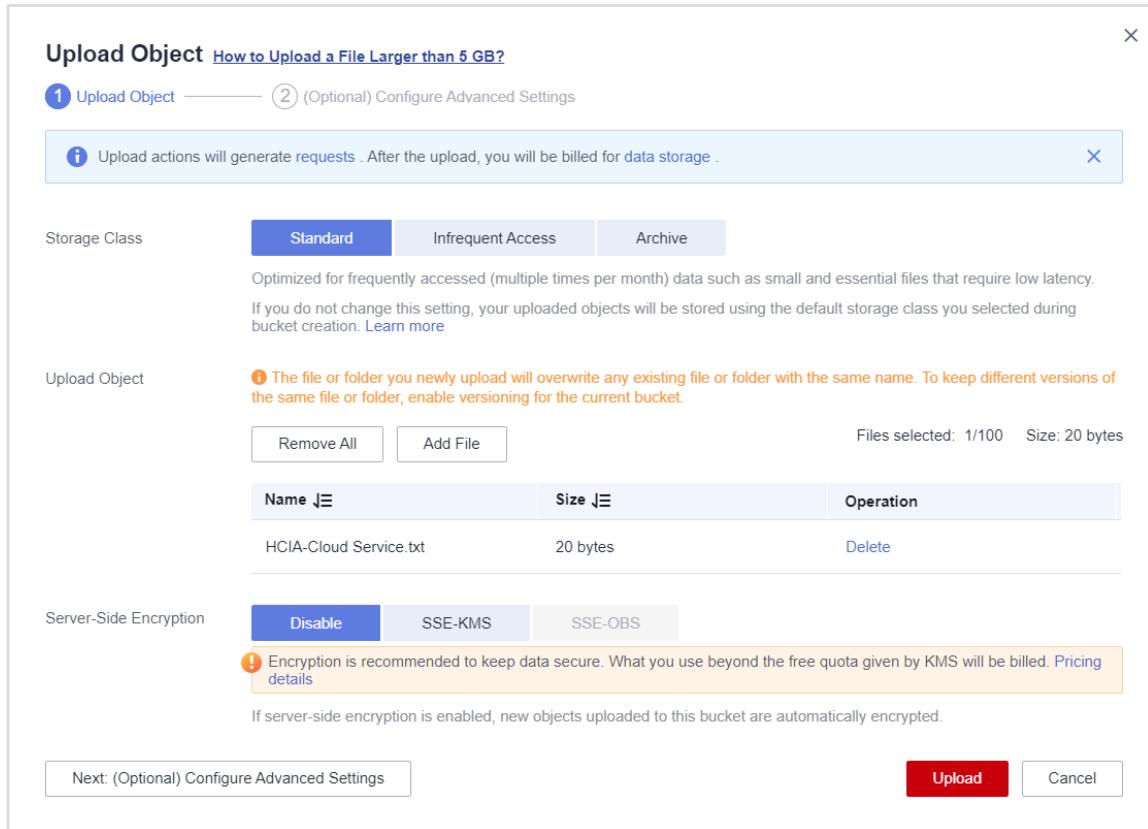
Step 1 Click the **bucket name**, for example, hw-cloud-service. The object list page is displayed.



The screenshot shows the "hw-cloud-service" object list page. The left sidebar has options like Overview, Metrics (NEW), Permissions, Basic Configurations, Domain Name Mgmt, Cross-Region Replication, Back to Source, Data Processing, and Inventories. The main area is titled "Objects" and shows a table with columns: Name, Storage Class, Size, Encrypted, Restoration Status, Last Modifi..., and Operation. A large "Upload Object" button is at the top left of the table area. A message at the bottom says "No data available." with a warning icon.

**Figure 4-21 Object List**

Step 2 Create a text file on the local host, for example, **HCIA-Cloud Service.txt**, and add content, for example, Huawei Cloud Service. Return to the OBS bucket page, click **Upload Object**, drag the created text file to the upload area, and upload the file.



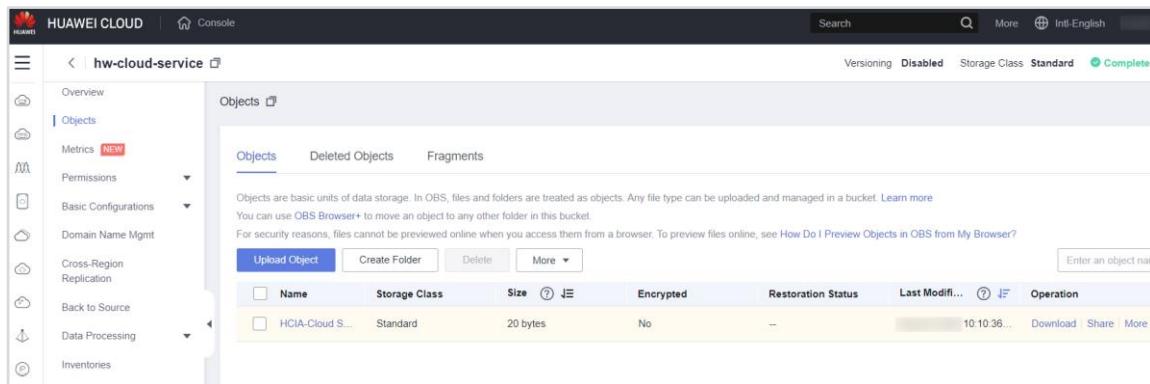
**Figure 4-22 Uploading a file**

Step 3 After you click Upload, the task page is displayed, showing the status of the uploaded task.

Task Center				
ⓘ Refreshing or closing the browser will cancel ongoing tasks and clear all records.				
Upload	Delete	Permanently Delete	Others	
<a href="#">Clear Records</a>	<a href="#">Pause All</a>	<a href="#">Start All</a>		
<a href="#">Specify filter criteria.</a>				
Object Name	Bucket	Size	Status	Operation
HCIA-Cloud Service...	hw-cloud-service	20 bytes	Succeeded	<a href="#">Clear Records</a>

**Figure 4-23 File uploading task**

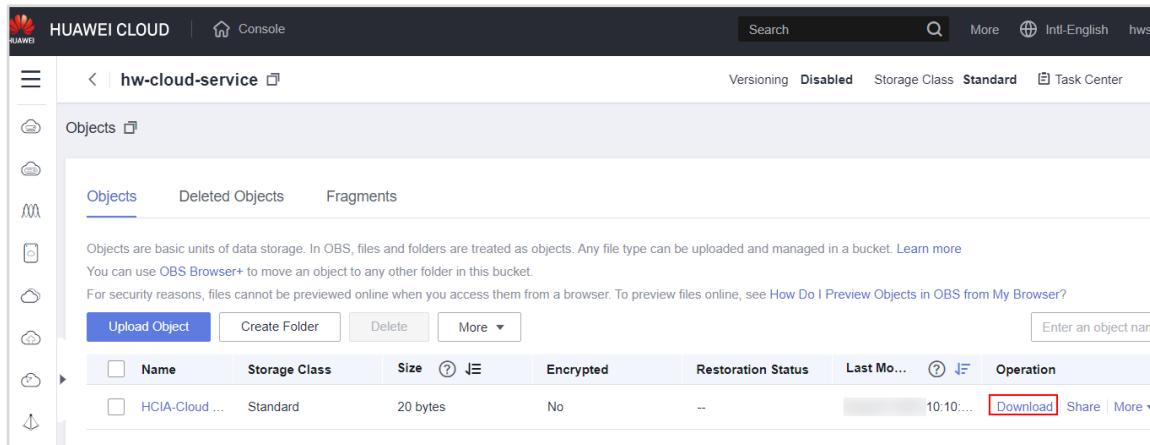
Step 4 After the file is uploaded, you can view the uploaded file on the object page of the bucket.



**Figure 4-24 Viewing uploaded files**

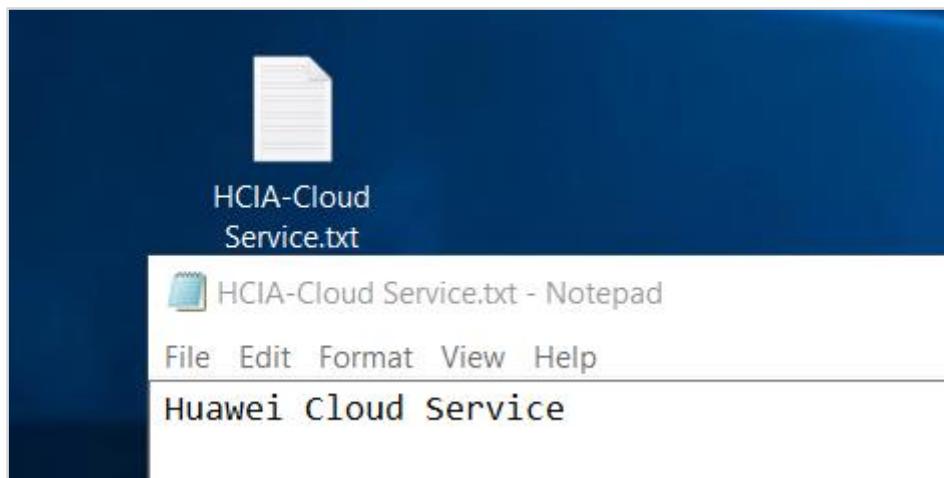
#### 4.2.2.4 File download and sharing

Step 1 On the object list page, select the file to be **downloaded** and click Download to download the file to the local host.



**Figure 4-25 Downloading a file**

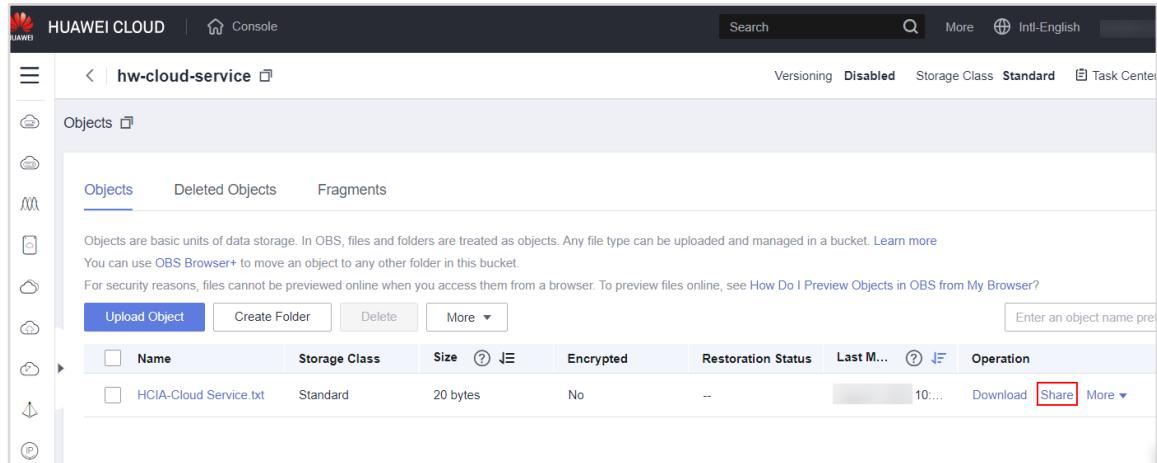
Step 2 Open the downloaded file and view the file content.



**Figure 4-26 Viewing File Contents**

**Step 3** You can easily share files through OBS sharing links. Compress the created local file and upload it to the OBS bucket.

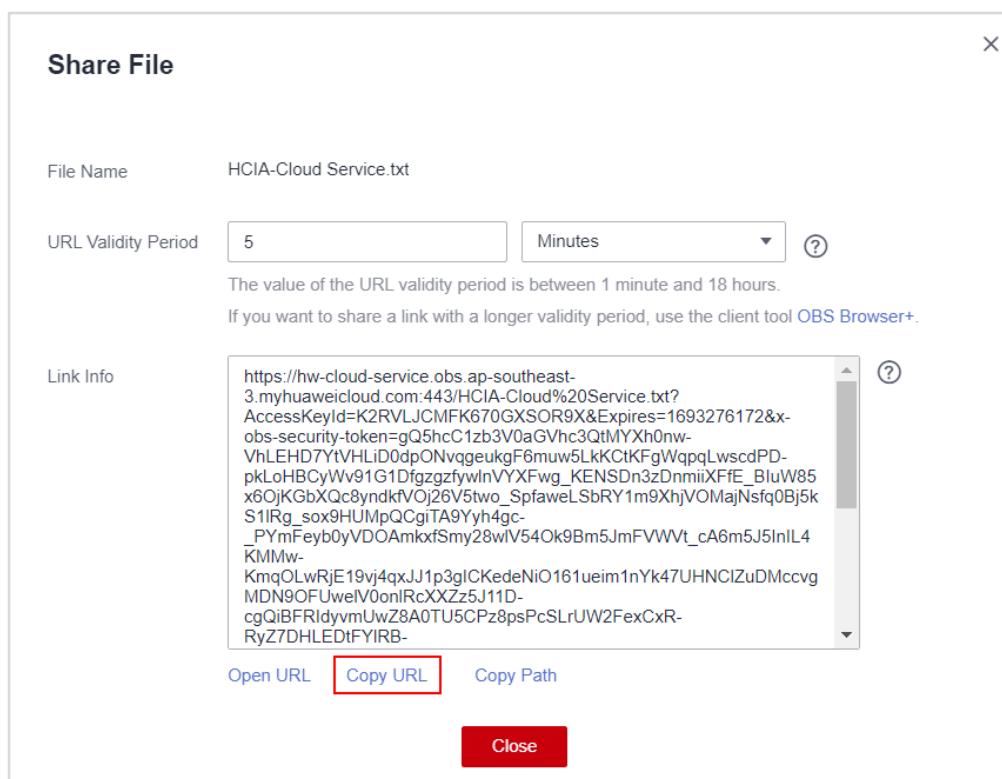
On the object list page of the bucket, select the file to be shared and click **Share**.



Name	Storage Class	Size	Encrypted	Restoration Status	Last M...	Operation
HCIA-Cloud Service.txt	Standard	20 bytes	No	-	10...	<a href="#">Download</a> <a href="#">Share</a> More

**Figure 4-27 File sharing**

**Step 4** Click **Share**. The sharing dialog box is displayed. Set the validity period of the sharing and click **Copy Link** to share the sharing.



File Name	HCIA-Cloud Service.txt
URL Validity Period	5 Minutes
The value of the URL validity period is between 1 minute and 18 hours. If you want to share a link with a longer validity period, use the client tool <a href="#">OBS Browser+</a> .	
Link Info	<pre>https://hw-cloud-service.obs.ap-southeast-3.myhuaweicloud.com:443/HCIA-Cloud%20Service.txt? AccessKeyId=K2RVLJCMFK670GXSOR9X&amp;Expires=1693276172&amp;x-obs-security-token=gQ5hcC1zb3V0aGVhc3QtMYXh0nw-VhLEHD7YtVHLID0dpONvggeukgF6muw5LkCtKFgWqpgLwsqdPD-pkLoHBCyWv91G1DfgzgfywlnVYXFwg_KENSDn3zDnmiiXFfE_BluW85x6OjKGbXQc8yndkfVOj26V5two_SpfaweLSbRY1m9XhjVOMajNsfqOBj5kS1IRg_so9HUMpQCgiTA9Yyh4gc-_PYmFeyb0yVDOAmkxfSmy28wLV54Ok9Bm5JmFVVVt_cA6m5J5InIL4KMMw-KmqOLwRjE19vj4qxJJ1p3glCKedeNiO161ueim1nYk47UHNClZuDMccvgMDN9OFUwe1V0onlRcXXZz5j11D-cgQiBFRldyymUwZ8A0TU5CPz8psPcSlrUW2FexCxRRyZ7DHLEDtFYIRB-</pre>
<a href="#">Open URL</a> <a href="#">Copy URL</a> <a href="#">Copy Path</a>	
<a href="#">Close</a>	

**Figure 4-28 File sharing configuration**

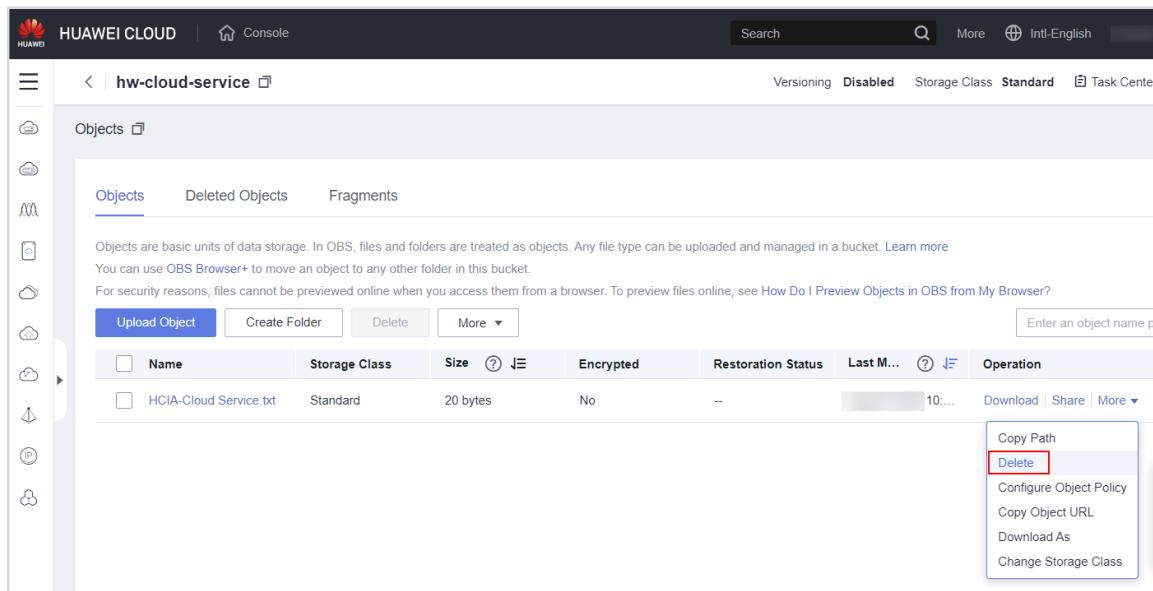
**Step 5** Access the obtained **copy link** in the address box of the browser to download the file.



Figure 4-29 Downloading a file

#### 4.2.2.5 Deleted files

Step 1 On the object list page, select the file or folder to be deleted and choose More > Delete.



The screenshot shows the HUAWEI CLOUD OBS console interface. The left sidebar has icons for Cloud Storage, Cloud Disk, and Cloud Archives. The main area shows the 'hw-cloud-service' bucket under 'Objects'. There are tabs for 'Objects', 'Deleted Objects', and 'Fragments'. Below the tabs, there's a brief description of what objects are. A table lists objects with columns: Name, Storage Class, Size, Encrypted, Restoration Status, Last M..., and Operation. One row is selected: 'HCIA-Cloud Service.txt' (Standard, 20 bytes, No, --, 10...). To the right of the table is a context menu with options: Copy Path, Delete (highlighted with a red box), Configure Object Policy, Copy Object URL, Download As, and Change Storage Class.

Figure 4-30 Deleting a file

Step 2 Click Yes in the Delete Object dialog box.

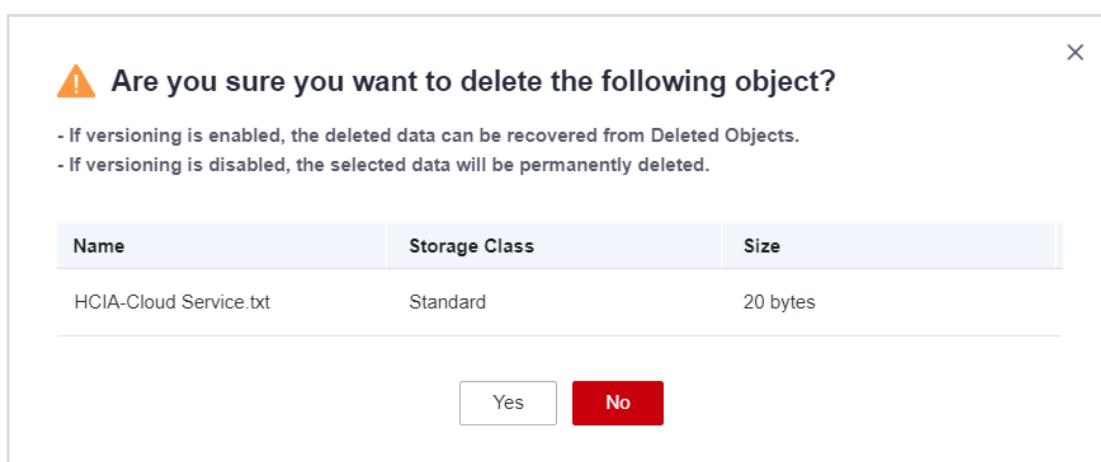
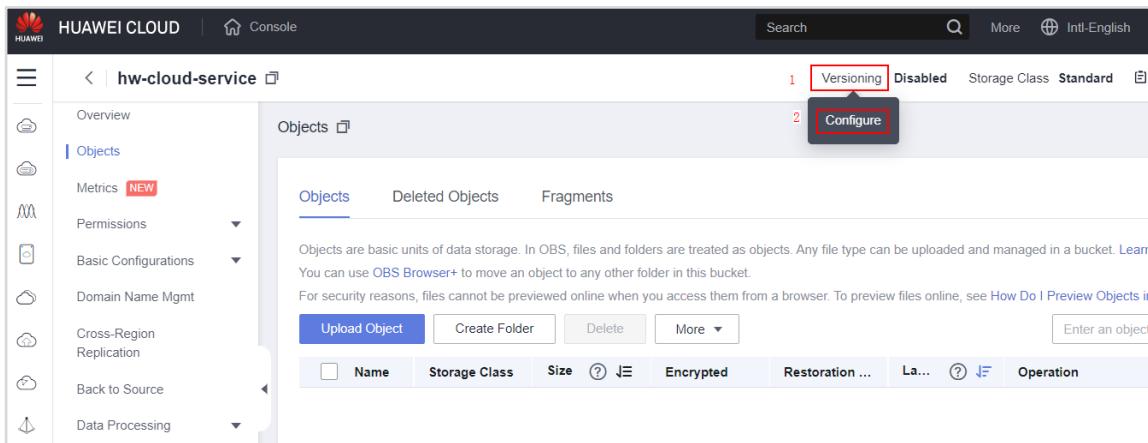


Figure 4-31 Confirming the deletion

#### 4.2.2.6 Versioning

Step 1 Go to the OBS page, select the bucket for which versioning is to be enabled, select **Versioning**, click **Configure**, and enable versioning as prompted.



The screenshot shows the HUAWEI CLOUD OBS console. In the top right corner, there is a 'Versioning' status indicator labeled 'Disabled' with a red box around it. Below it, a 'Configure' button is also highlighted with a red box. The main area shows an 'Objects' list with tabs for 'Objects', 'Deleted Objects', and 'Fragments'. There are buttons for 'Upload Object', 'Create Folder', 'Delete', and 'More'. A search bar at the top right says 'Enter an object'.

Figure 4-32 Bucket Overview

Step 2 In the dialog box that is displayed, select **Enable** and click **OK**. After the configuration is complete, check whether versioning is enabled on the Overview page.

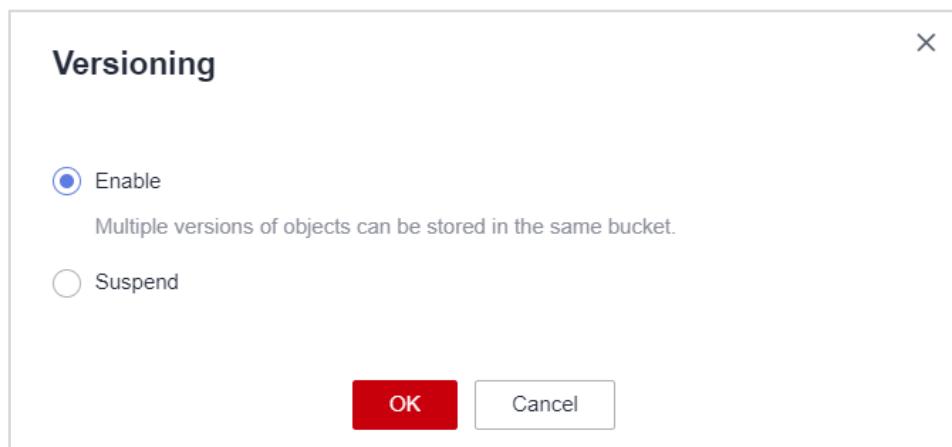
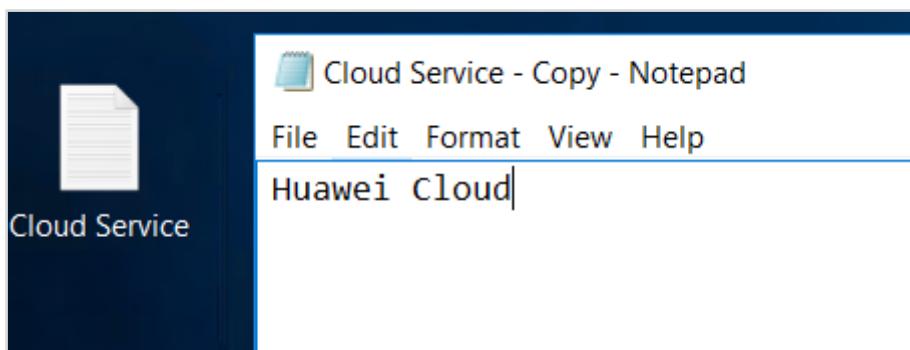


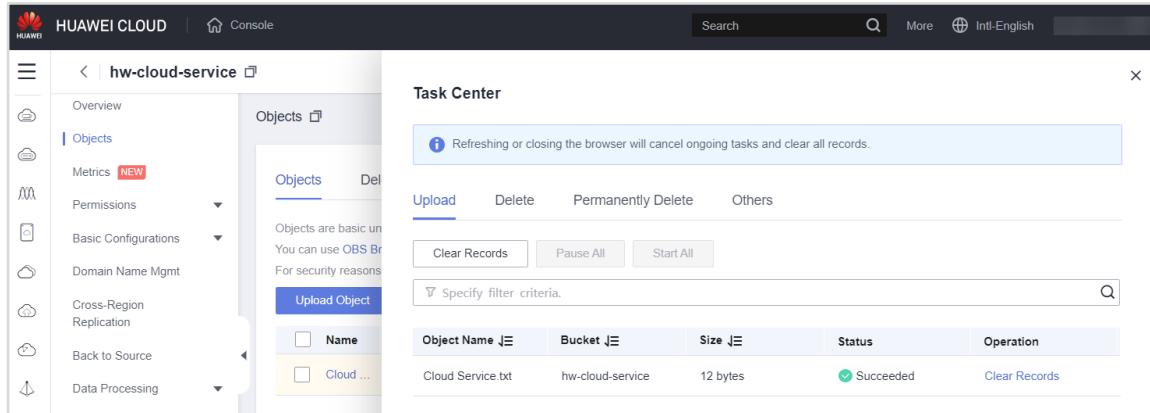
Figure 4-33 Enabling versioning

Step 3 Create a local file, for example, **Cloud Service.txt**, and write the following content to the file "**Huawei Cloud**".



### Figure 4-34 New File

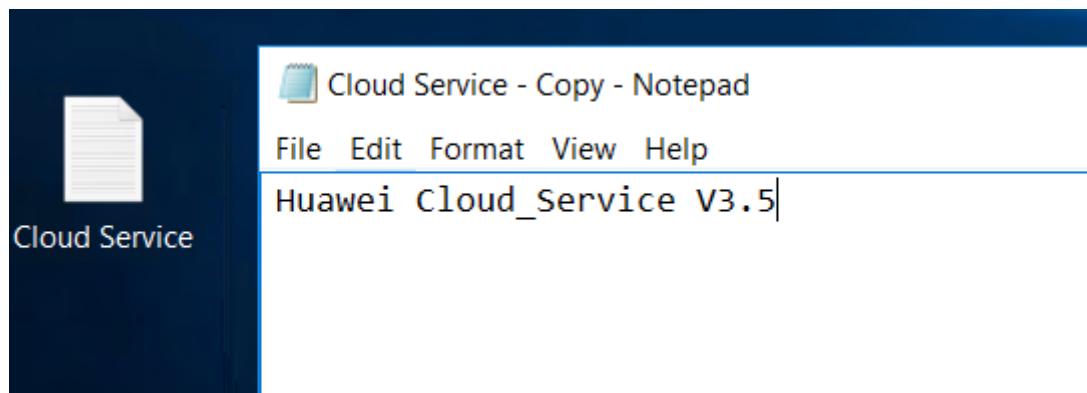
Step 4 On the current page, click Upload Object to upload the new file.



Object Name	Bucket	Size	Status	Operation
Cloud Service.txt	hw-cloud-service	12 bytes	Succeeded	<a href="#">Clear Records</a>

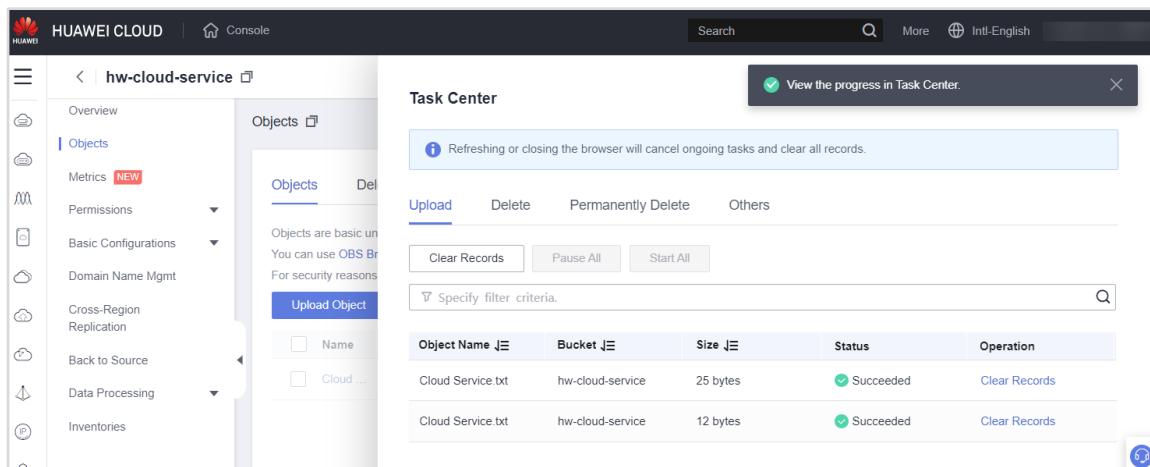
### Figure 4-35 Uploading an object

Step 5 Modify the file content on the local host (the file name remains unchanged), for example, “Huawei Cloud\_Service V3.5”.



### Figure 4-36 Modifying Files

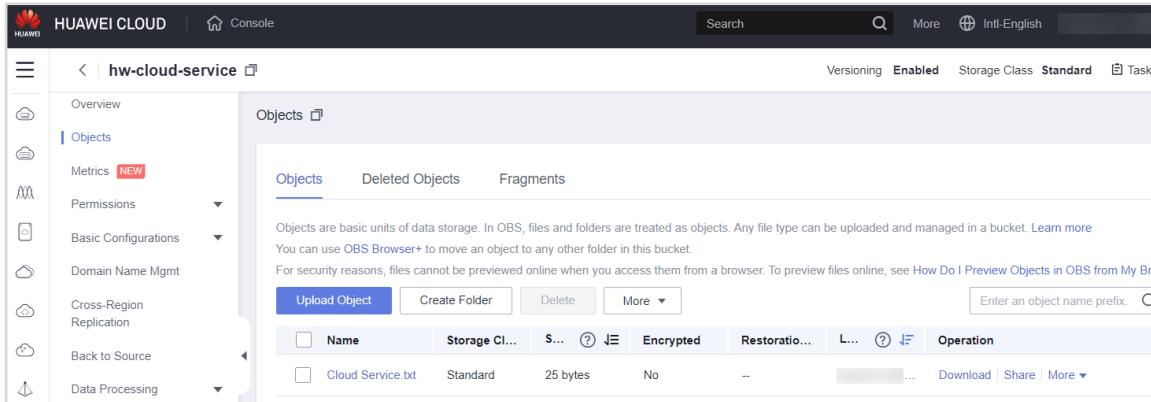
Step 6 Upload the modified file to the OBS bucket again.



Object Name	Bucket	Size	Status	Operation
Cloud Service.txt	hw-cloud-service	25 bytes	Succeeded	<a href="#">Clear Records</a>
Cloud Service.txt	hw-cloud-service	12 bytes	Succeeded	<a href="#">Clear Records</a>

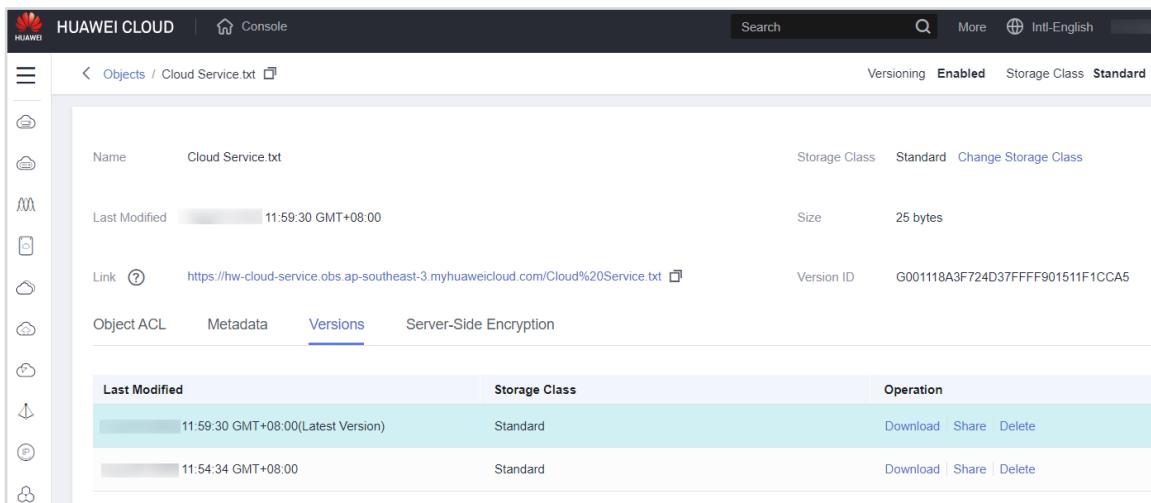
### Figure 4-37 Modifying Files

**Step 7** On the current page, click the **name of the uploaded file**. The file details page is displayed.



**Figure 4-38 Viewing Versions**

**Step 8 Select Versions**, Two versions of the file are displayed. You can perform operations on different versions, such as downloading and sharing.



**Figure 4-39 Document Version**

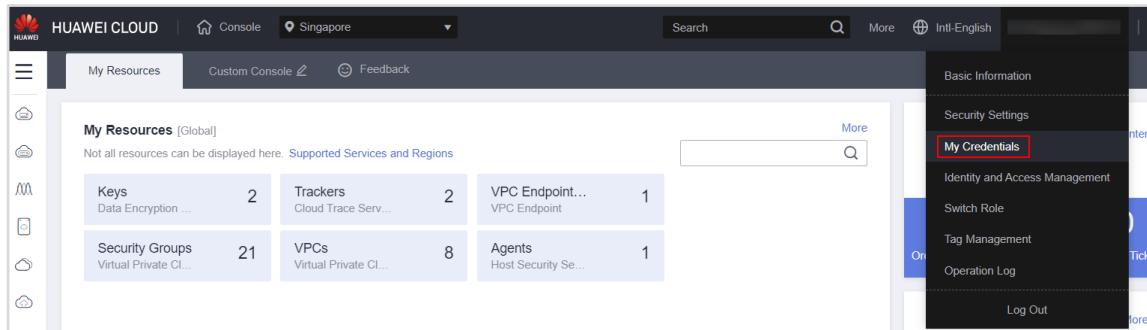
#### 4.2.2.7 ( optional ) OBS Browser+ Usage

OBS Browser+, a GUI tool for managing OBS, provides complete functions for managing your buckets and objects in OBS. With OBS Browser+, you can easily manage OBS resources from a local end.

OBS Browser+ must be installed on Windows.

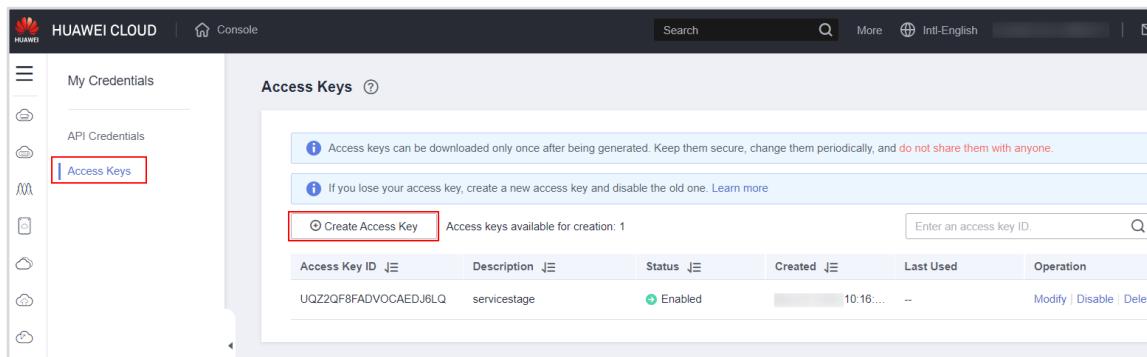
**Step 1** Obtaining AK/SK.

Log in to the **HUAWEI CLOUD console**, click the **username** in the upper right corner of the page, and choose **My Credentials**.



**Figure 4-40 My Credentials**

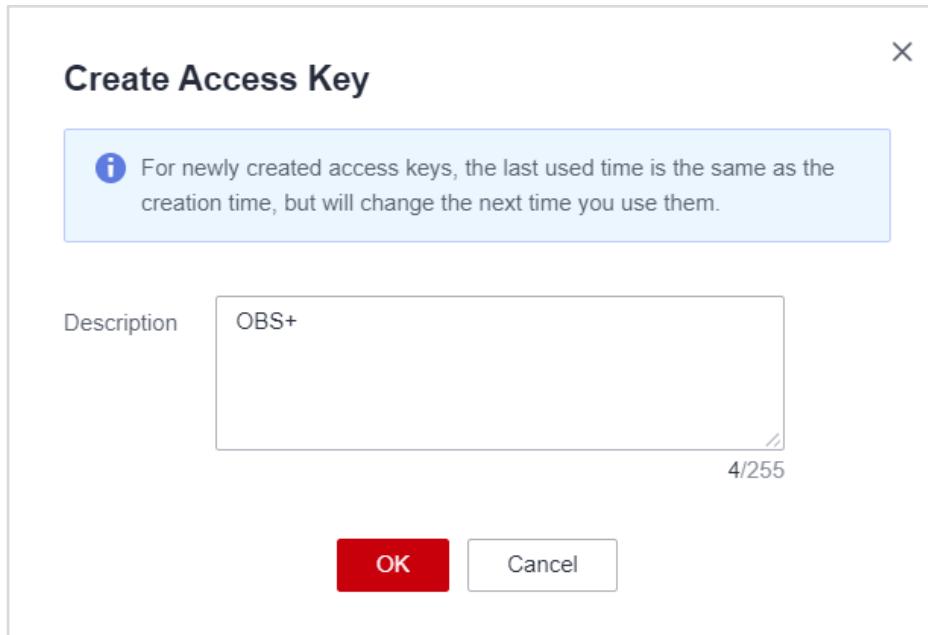
Step 2 In the navigation tree on the left, choose **Access Keys**. Click **Create Access Key**. The Add Access Key page is displayed.



**Figure 4-41 Adding an access key**

Step 3 Enter the key description as required and click **OK** to create an access key and download it.

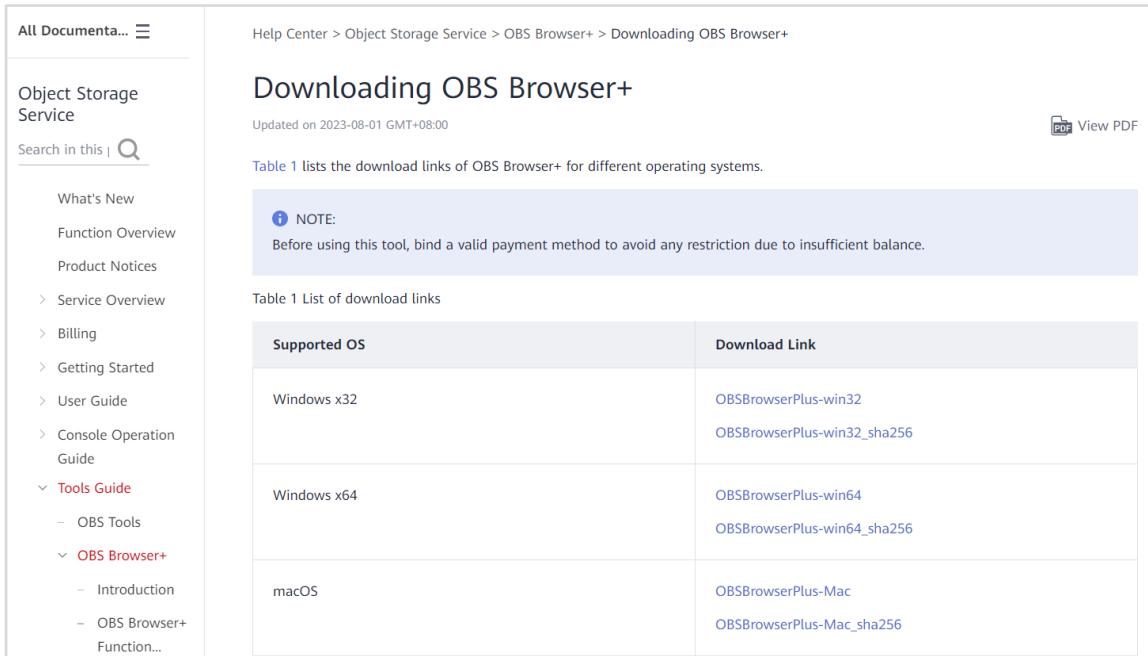
Note: To prevent access keys from being disclosed, you are advised to save them in a secure location.



### Figure 4-42 Create AK/SK

Step 4 Open the downloaded **credentials.csv** key file to obtain the access key (AK/SK).

Step 5 Use a browser to access [https://support.huaweicloud.com/intl/en-us/browsertg-obs/obs\\_03\\_1003.html](https://support.huaweicloud.com/intl/en-us/browsertg-obs/obs_03_1003.html), select the corresponding platform, and download **OBS Browser+ Client**.

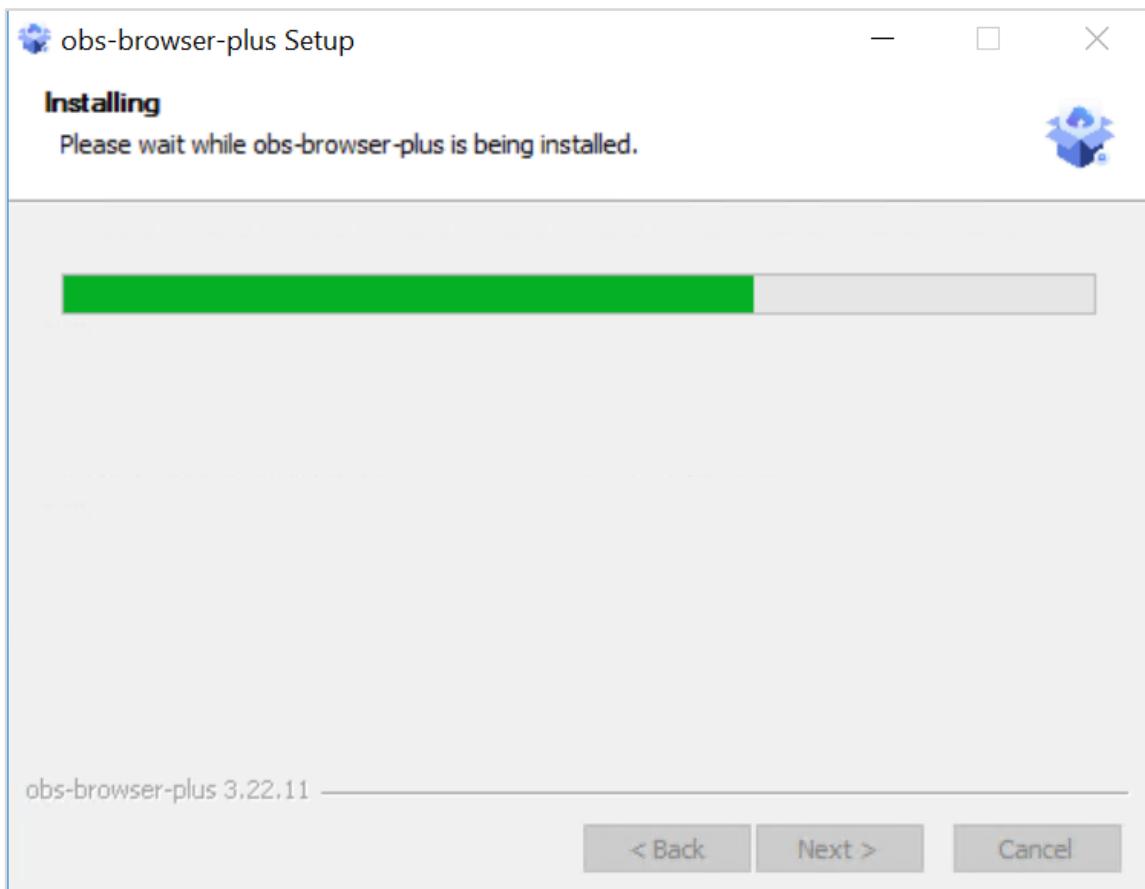


The screenshot shows a web page titled "Downloading OBS Browser+" under the "Object Storage Service" category. The page includes a search bar, a sidebar with navigation links like "What's New", "Function Overview", and "Tools Guide", and a note about binding a payment method. A table lists download links for Windows x32, Windows x64, and macOS.

Supported OS	Download Link
Windows x32	<a href="#">OBSBrowserPlus-win32</a> <a href="#">OBSBrowserPlus-win32_sha256</a>
Windows x64	<a href="#">OBSBrowserPlus-win64</a> <a href="#">OBSBrowserPlus-win64_sha256</a>
macOS	<a href="#">OBSBrowserPlus-Mac</a> <a href="#">OBSBrowserPlus-Mac_sha256</a>

### Figure 4-43 Download OBS Browser+

Step 6 Decompress the downloaded software package to the local PC and complete the installation.



**Figure 4-44 Installing OBS Browser+**

Step 7 After the installation is complete, run OBS Browser+. OBS Browser+ supports login using AK, account, and authorization. In this example, AK is used for login.

- Select AK Login
- Account Name: **Enter the user name**, for example, zhangshan888.
- Service: **HUAWEI CLOUD OBS** ( default ).
- Access Key ID: Obtain the **AK** from the downloaded AK and SK.
- Secret Access Key: Obtain the **SK** from the downloaded AK and SK.
- Access Path: This field is optional.

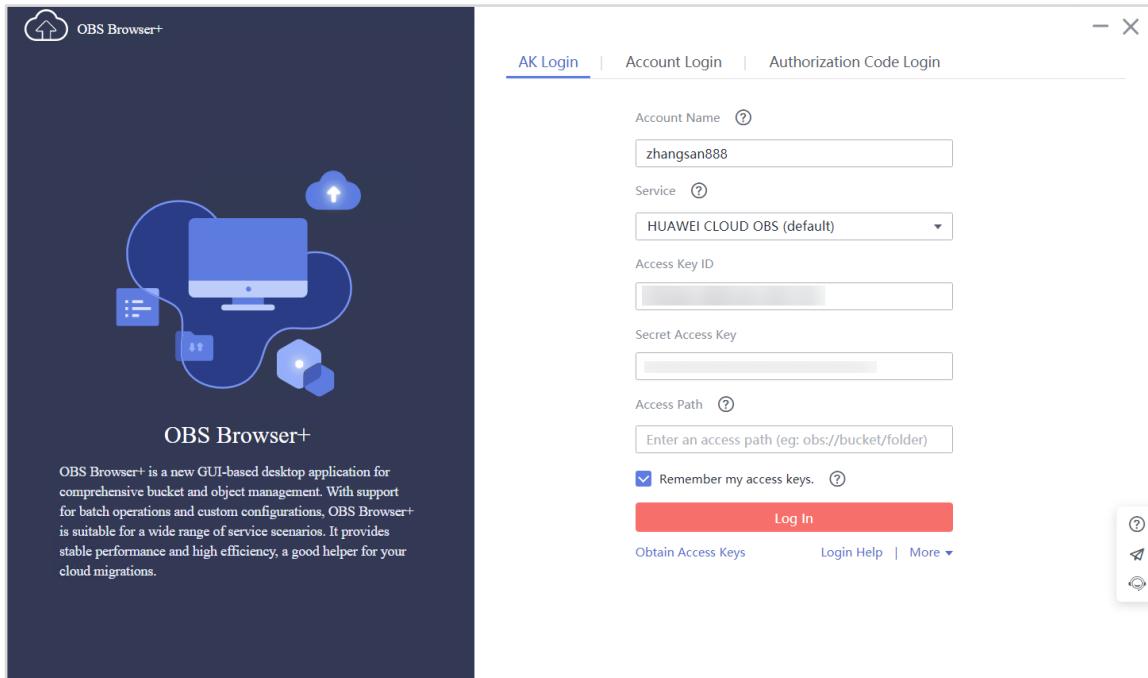


Figure 4-45 Logging in to the OBS client

Step 8 After filling in the information, click **Login**. After login, you can perform operations on the resources under the account.

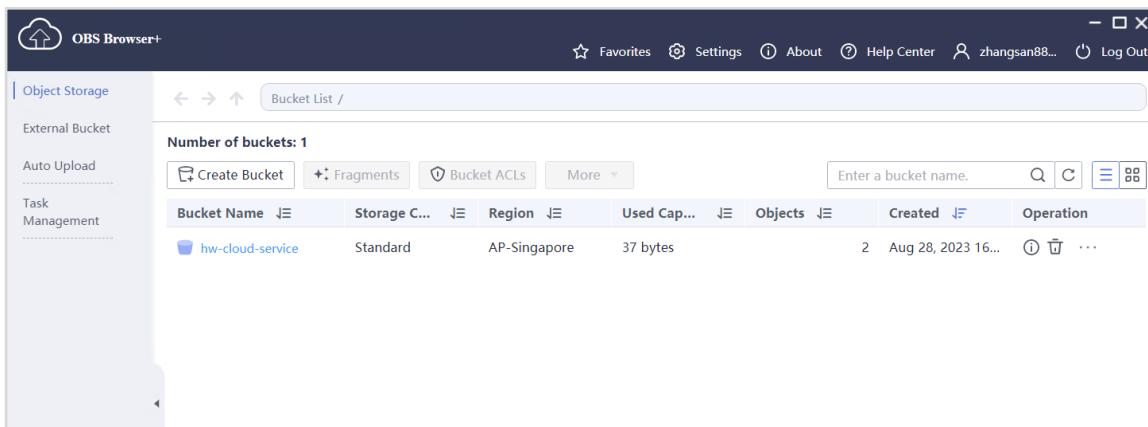


Figure 4-46 OBS Browser+ page

Step 9 Click the **bucket name** to view the uploaded file. You can perform operations on the file using OBS Browser+.

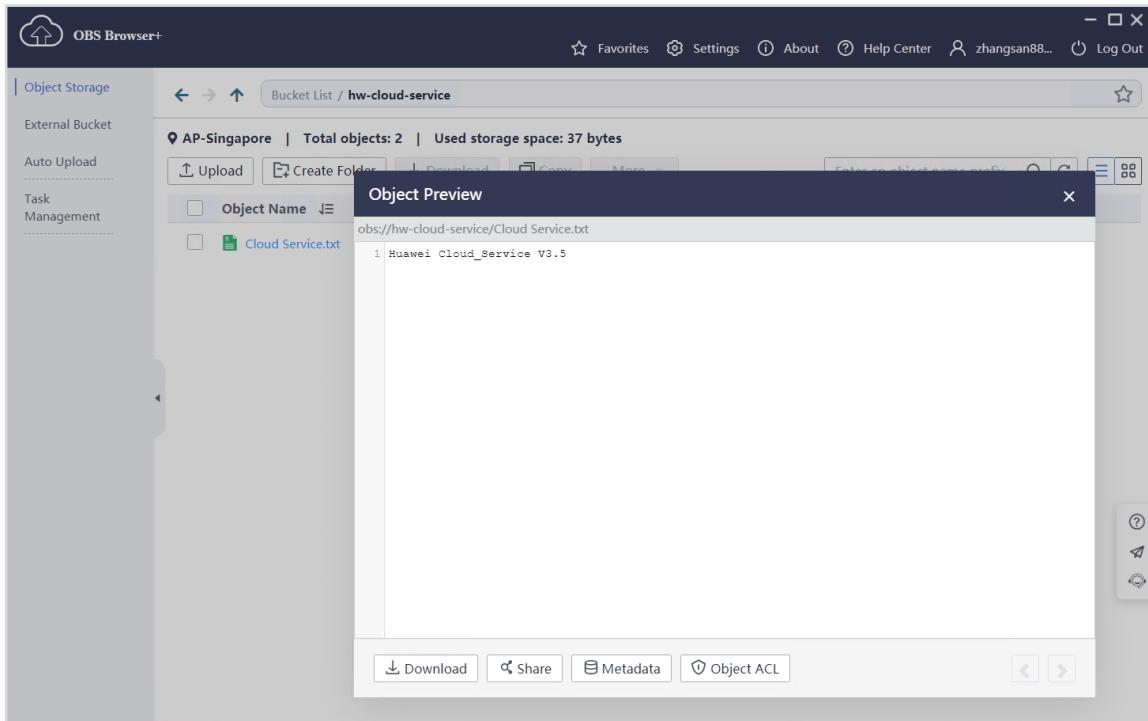


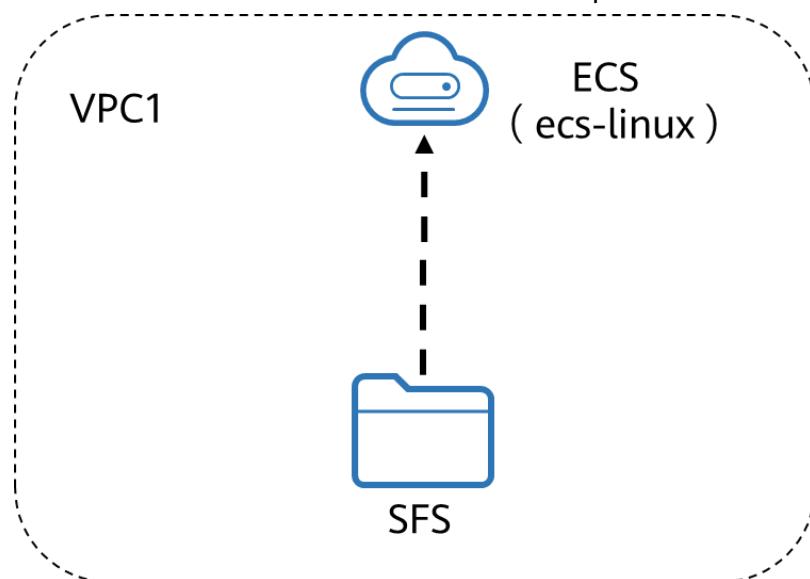
Figure 4-47 Viewing files in a bucket on OBS Browser

## 4.3 SFS

### 4.3.1 Introduction

#### 4.3.1.1 About This Exercise

SFS provides reliable, high-performance shared file storage hosted on HUAWEI CLOUD. With SFS, you can enjoy shared file access spanning multiple ECSS, BMSs, and containers created on CCE and CCI. This exercise describes basic SFS operations.



### Figure 4-48 Lab Topology

#### 4.3.1.2 Objectives

Upon completion of this exercise, you will be able to:

- Create an SFS file system.
- Mount an SFS file system on Linux servers.
- Enable cloud servers in different VPCs to share the same SFS file system.

#### 4.3.2 Tasks

##### 4.3.2.1 Creating an SFS File System

###### 4.3.2.1.1 Creating an ECS

Step 1 Repeat the preceding steps to create a VPC and subnet. For example, select **vpc-1** and **subnet-1** for the network configuration.

Step 2 Apply for an **ECS** bound with an **EIP**. (Dynamic BGP | Charging by Bandwidth | 5 Mbit/s) Linux ECS (ecs-linux | general computing | 1-core | 2 GB | SSD 40 GB | CentOS 7.8) and select **vpc-1** and **subnet-1** in the network configuration.

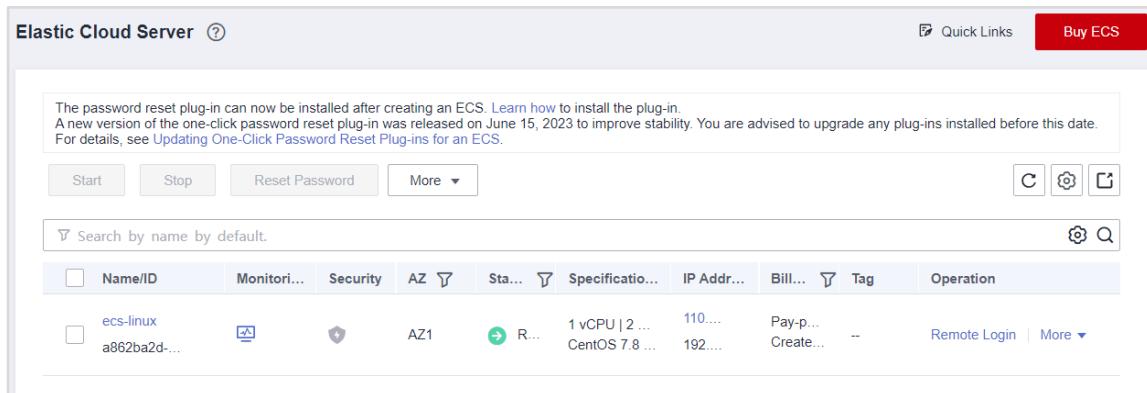
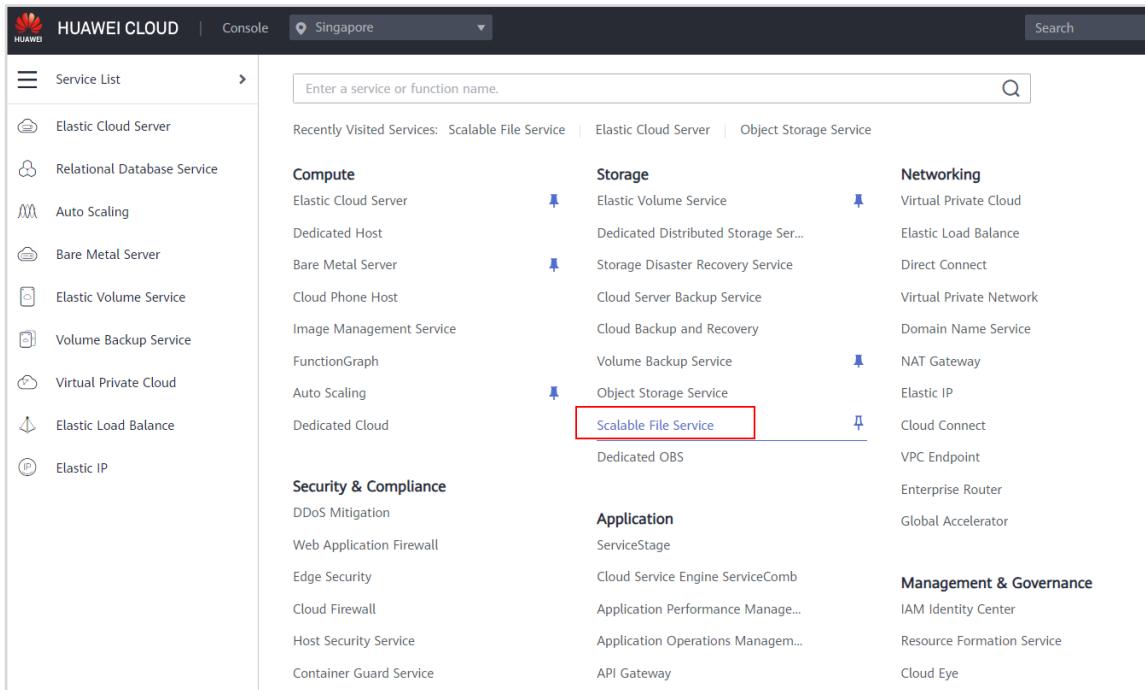


Figure 4-49 Creating a Linux ECS

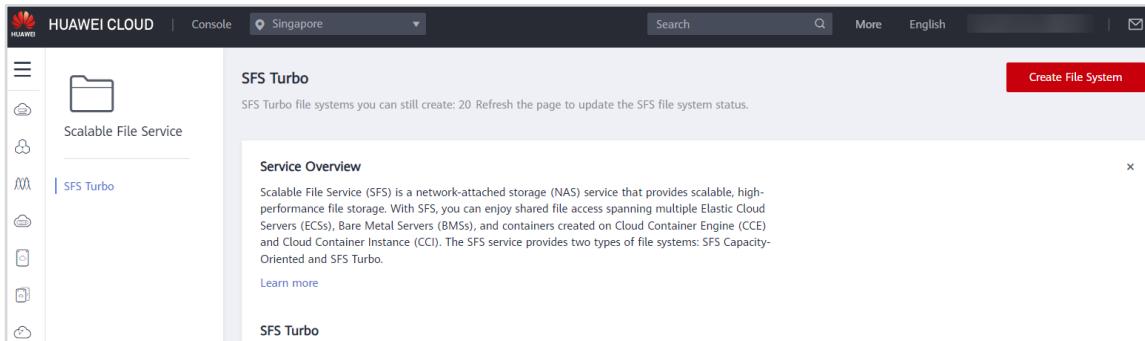
###### 4.3.2.1.2 Creating an SFS

Step 1 On the **HUAWEI CLOUD console**, locate SFS in the **service list** on the home page.



**Figure 4-50 Opening the SFS console**

Step 2 On the SFS page, select **SFS Turbo** and click **Create File System**.

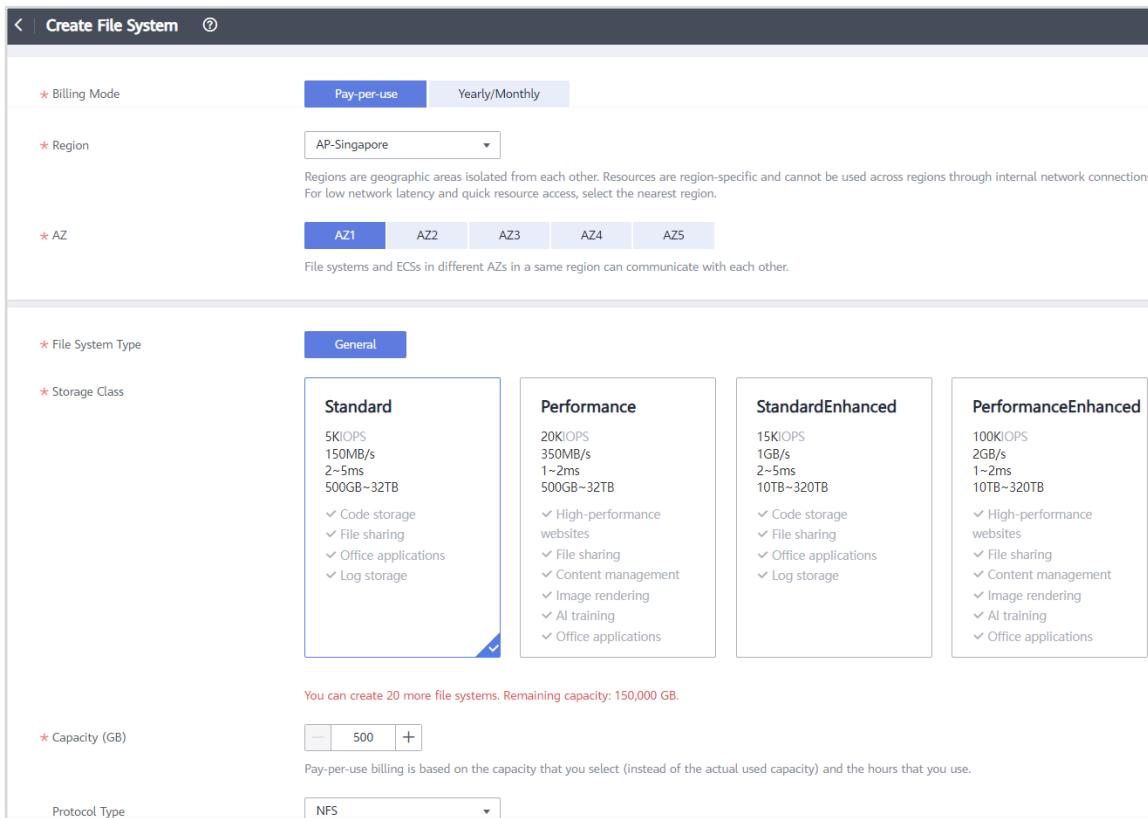


**Figure 4-51 Creating a File System**

Step 3 Enter the following configuration information on the page for creating a file system:

- Billing Mode: **Pay-per-use**
- Region: **AP-Singapore**
- AZ: **Consistent with ECS** ( File systems and ECSS in different AZs in a same region can communicate with each other )
- File System Type: **General**
- Storage Class: **Standard**
- Capacity: **500 GB**
- Protocol Type: **NFS**

- VPC and Security Group: **Consistent with ECS**
- Cloud Backup and Recovery: **Do not use**
- Name: **sfs-turbo-01** ( custom )
- Other default values



The screenshot shows the 'Create File System' interface. At the top, there are tabs for 'Pay-per-use' (selected) and 'Yearly/Monthly'. Below that, fields for 'Region' (set to AP-Singapore) and 'AZ' (set to AZ1) are shown. A note states: '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.' Another note below says: 'File systems and ECSS in different AZs in the same region can communicate with each other.'

In the 'General' tab, there are four storage class options:

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

Below the storage classes, there is a note: 'You can create 20 more file systems. Remaining capacity: 150,000 GB.' A 'Capacity (GB)' input field is set to 500. A note below it says: 'Pay-per-use billing is based on the capacity that you select (instead of the actual used capacity) and the hours that you use.' The 'Protocol Type' is set to NFS.

**Figure 4-52 Configuring the File System**

Step 4 After the configuration is complete, click **Create Now**.

Step 5 Confirm the information and click **Submit**.

Details		
	Product Name	Configuration
SFS Turbo	Region	Singapore
	Name	sfs-turbo-01
	Specifications	Standard
	Capacity (GB)	500
	Encryption	No
	AZ	AZ1
Network	VPC	vpc-1
	Subnet	subnet-1(192.168.1.0/24)
	Security Group	sg-web
Automatic Backup	Do not use	

**Figure 4-53 Confirming the configuration parameters**

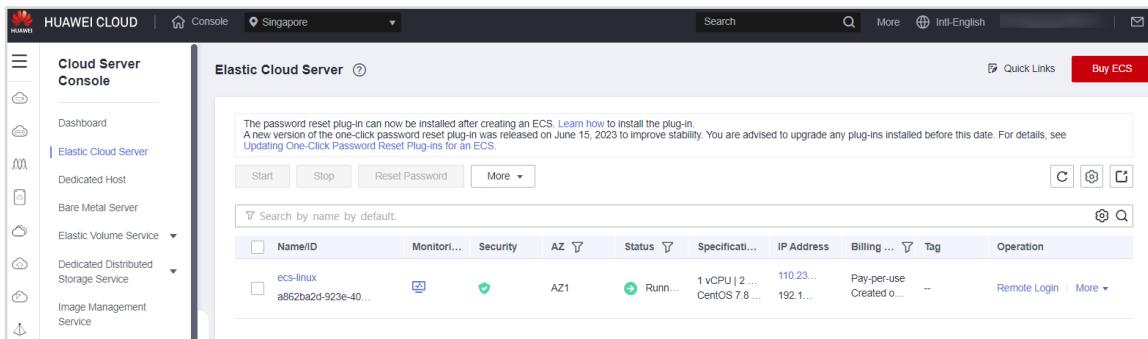
Step 6 Return to the SFS page and view the creation status. Generally, the creation takes 2 to 3 minutes.

SFS Turbo																														
<a href="#">Service Overview</a>   <a href="#">Process</a>																														
SFS Turbo file systems you can still create: 19 Refresh the page to update the SFS file system status.																														
<a href="#">Create File System</a>																														
<table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Status</th> <th>Protocol Type</th> <th>AZ</th> <th>Used Cap...</th> <th>Maximum C...</th> <th>Encrypt...</th> <th>Mount Point</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td>sfs-turbo-01</td> <td>Standard</td> <td>Available</td> <td>NFS</td> <td>AZ1</td> <td>0.00</td> <td>500.00</td> <td>No</td> <td>192.168.1.177:/</td> <td><a href="#">Expand Capacity</a>   ...</td> </tr> </tbody> </table>											Name	Type	Status	Protocol Type	AZ	Used Cap...	Maximum C...	Encrypt...	Mount Point	Operation	sfs-turbo-01	Standard	Available	NFS	AZ1	0.00	500.00	No	192.168.1.177:/	<a href="#">Expand Capacity</a>   ...
Name	Type	Status	Protocol Type	AZ	Used Cap...	Maximum C...	Encrypt...	Mount Point	Operation																					
sfs-turbo-01	Standard	Available	NFS	AZ1	0.00	500.00	No	192.168.1.177:/	<a href="#">Expand Capacity</a>   ...																					

**Figure 4-54 View File System**

#### 4.3.2.2 Attaching an SFS File System to a Linux ECS

Step 1 Go to the ECS page. Locate the row that contains the created ECS, and click **Remote Login**.



**Figure 4-55 Remote login to an ECS**

Step 2 Log in to the ECS as user root. Run the following command to check whether the NFS software package is installed:

```
Welcome to Huawei Cloud Service
[root@ecs-linux ~]# rpm -qa |grep nfs
[root@ecs-linux ~]#
```

Step 3 If no command output is displayed, the is not installed. You need to run different commands to install the NFS software based on the operating system. (In this experiment, CentOS 7.8 bit is used as an example. You need to bind an EIP.) In CentOS, Red Hat, Euler OS, Fedora, or Oracle Enterprise Linux, run the following command:

```
[root@ecs-linux ~]# yum install nfs-utils -y
Loaded plugins: fastestmirror
Determining fastest mirrors
base                                         | 3.6 kB  00:00:00
epel                                         | 4.7 kB  00:00:00
extras                                         | 2.9 kB  00:00:00
updates                                         | 2.9 kB  00:00:00
(1/7): base/7/x86_64/group_gz               | 153 kB  00:00:00
(2/7): epel/x86_64/group_gz                | 99 kB   00:00:00
(3/7): epel/x86_64/updateinfo              | 1.0 MB   00:00:00
(4/7): epel/x86_64/primary_db              | 7.0 MB   00:00:00
(5/7): base/7/x86_64/primary_db            | 6.1 MB   00:00:00
(6/7): extras/7/x86_64/primary_db          | 249 kB   00:00:00
(7/7): updates/7/x86_64/primary_db         | 21 MB    00:00:00
Resolving Dependencies
--> Running transaction check
--> Package nfs-utils.x86_64 1:1.3.0-0.68.el7.2 will be installed
--> Processing Dependency: gssproxy >= 0.7.0-3 for package: 1:nfs-utils-1.3.0-0.68.el7.2.x86_64
--> Processing Dependency: rpcbind for package: 1:nfs-utils-1.3.0-0.68.el7.2.x86_64
--> Processing Dependency: quota for package: 1:nfs-utils-1.3.0-0.68.el7.2.x86_64
The following content is omitted...
Complete!
[root@ecs-linux ~]#
```

Step 4 Run the following command to install the **bind-utils** software package.

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

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
Resolving Dependencies
--> Running transaction check
--> Package bind-utils.x86_64 32:9.11.4-26.P2.el7_9.13 will be installed
--> Processing Dependency: bind-libs-lite(x86-64) = 32:9.11.4-26.P2.el7_9.13 for package: 32:bind-
utils-9.11.4-26.P2.el7_9.13.x86_64
--> Processing Dependency: bind-libs(x86-64) = 32:9.11.4-26.P2.el7_9.13 for package: 32:bind-utils-
9.11.4-26.P2.el7_9.13.x86_64
--> Processing Dependency: liblwres.so.160()(64bit) for package: 32:bind-utils-9.11.4-
26.P2.el7_9.13.x86_64
--> Processing Dependency: libiscfg.so.160()(64bit) for package: 32:bind-utils-9.11.4-
26.P2.el7_9.13.x86_64
--> Processing Dependency: libisc.so.169()(64bit) for package: 32:bind-utils-9.11.4-
26.P2.el7_9.13.x86_64
--> Processing Dependency: libirs.so.160()(64bit) for package: 32:bind-utils-9.11.4-
26.P2.el7_9.13.x86_64
--> Processing Dependency: libdns.so.1102()(64bit) for package: 32:bind-utils-9.11.4-
26.P2.el7_9.13.x86_64
--> Processing Dependency: libbind9.so.160()(64bit) for package: 32:bind-utils-9.11.4-
26.P2.el7_9.13.x86_64
--> Processing Dependency: libGeolP.so.1()(64bit) for package: 32:bind-utils-9.11.4-
26.P2.el7_9.13.x86_64
--> Running transaction check
The following content is omitted...

Installed:
  bind-utils.x86_64 32:9.11.4-26.P2.el7_9.13

Dependency Installed:
  GeolP.x86_64 0:1.5.0-14.el7    bind-libs.x86_64 32:9.11.4-26.P2.el7_9.13    bind-libs-lite.x86_64
  32:9.11.4-26.P2.el7_9.13    bind-license.noarch 32:9.11.4-26.P2.el7_9.13    geoipupdate.x86_64 0:2.5.0-
  1.el7

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

Step 5 Run the following command to check the NFS software package again.

```
[root@ecs-linux ~]# rpm -qa |grep nfs
libnfsidmap-0.25-19.el7.x86_64
nfs-utils-1.3.0-0.68.el7.2.x86_64
[root@ecs-linux ~]#
```

Step 6 Return to the SFS Turbo page and click the **file system name**, for example, sfs-turbo-01.

**Figure 4-56 Viewing the SFS Turbo page**

Step 7 Check the mounting command information of the Linux operating system.

**Figure 4-57 Viewing the mounting parameters**

Step 8 Log in to the ecs-linux ECS and create a mount point.

```
[root@ecs-linux ~]# mkdir /mnt/sfs_turbo
[root@ecs-linux ~]#
```

Step 9 Copy the Linux mounting command on the SFS Turbo page and mount the created shared file system to the local path.

```
[root@ecs-linux ~]# mount -t nfs -o vers=3,nolock 192.168.1.177:/ /mnt/sfs_turbo
[root@ecs-linux ~]#
```

Note: Change the SFS\_turbo IP address based on the site requirements.

Step 10 Run the **df -Th** command to view the mounted file system.

```
[root@ecs-linux ~]# df -Th
Filesystem      Type     Size   Used  Avail Use% Mounted on
devtmpfs        devtmpfs  909M    0    909M  0% /dev
tmpfs           tmpfs    919M    0    919M  0% /dev/shm
tmpfs           tmpfs    919M   8.6M  911M  1% /run
tmpfs           tmpfs    919M    0    919M  0% /sys/fs/cgroup
/dev/vda1        ext4     40G   2.6G  35G  7% /
```

```
tmpfs      tmpfs     184M    0  184M   0% /run/user/0
192.168.1.177:/ nfs      500G    0  500G   0% /mnt/sfs_turbo
[root@ecs-linux ~]#
```

Step 11 Create a file in the newly mounted file path and test that the mounted storage resources can be read and written normally.

```
[root@ecs-linux ~]# cd /mnt/sfs_turbo/
[root@ecs-linux sfs_turbo]# ls
[root@ecs-linux sfs_turbo]# touch huawei_cloud
[root@ecs-linux sfs_turbo]# ls
huawei_cloud
[root@ecs-linux sfs_turbo]#
```

Step 12 Configure automatic mounting upon system startup. The file mounted using the mount command is not automatically mounted upon system startup. You need to write the mounting information to the /etc/fstab file so that the file can be automatically mounted upon system startup. Run the **vi /etc/fstab** command to edit the /etc/fstab file.

```
[root@ecs-linux sfs_turbo]# vi /etc/fstab
```

Press **i** to enter the editing mode and add information about the file system to be mounted to the end of the file. The configuration example is as follows:

```
192.168.1.177:/ /mnt/sfs_turbo nfs     vers=3,nolock 0 0
```

Press **Esc**, enter **:wq**, and press **Enter** to save the file and exit.

Note: Change the SFS\_turbo IP address based on the site requirements.

Step 13 Perform the mounting test. Run the **umount** command to unmount the SFS file system and run the **mount -a** command to test the mounting.

```
[root@ecs-linux sfs_turbo]# cd
[root@ecs-linux ~]# umount /mnt/sfs_turbo/
[root@ecs-linux ~]# mount -a
[root@ecs-linux ~]# df
Filesystem      1K-blocks    Used Available Use% Mounted on
devtmpfs        930352      0    930352   0% /dev
tmpfs          940808      0    940808   0% /dev/shm
tmpfs          940808    8780    932028   1% /run
tmpfs          940808      0    940808   0% /sys/fs/cgroup
/dev/vda1      41152736 2664672  36374580   7% /
tmpfs          188164      0    188164   0% /run/user/0
192.168.1.177:/ 524288000      0  524288000   0% /mnt/sfs_turbo
[root@ecs-linux ~]#
```

Step 14 Restart the server and test the automatic mounting upon startup.

```
[root@ecs-linux ~]# reboot
```

Step 15 Log in to the system again and run the **df** command to view the mounted file system.

```
[root@ecs-linux ~]# df -Th
Filesystem      Type   Size  Used Avail Use% Mounted on
devtmpfs        devtmpfs 909M    0  909M  0% /dev
tmpfs          tmpfs   919M    0  919M  0% /dev/shm
tmpfs          tmpfs   919M   8.6M  911M  1% /run
tmpfs          tmpfs   919M    0  919M  0% /sys/fs/cgroup
/dev/vda1       ext4    40G   2.6G  35G  7% /
192.168.1.177:/ nfs    500G    0  500G  0% /mnt/sfs_turbo
tmpfs          tmpfs   184M    0  184M  0% /run/user/0
[root@ecs-linux ~]#
```

Step 16 Check the created file.

```
[root@ecs-linux ~]# cd /mnt/sfs_turbo/
[root@ecs-linux sfs_turbo]# ls
huawei_cloud
```

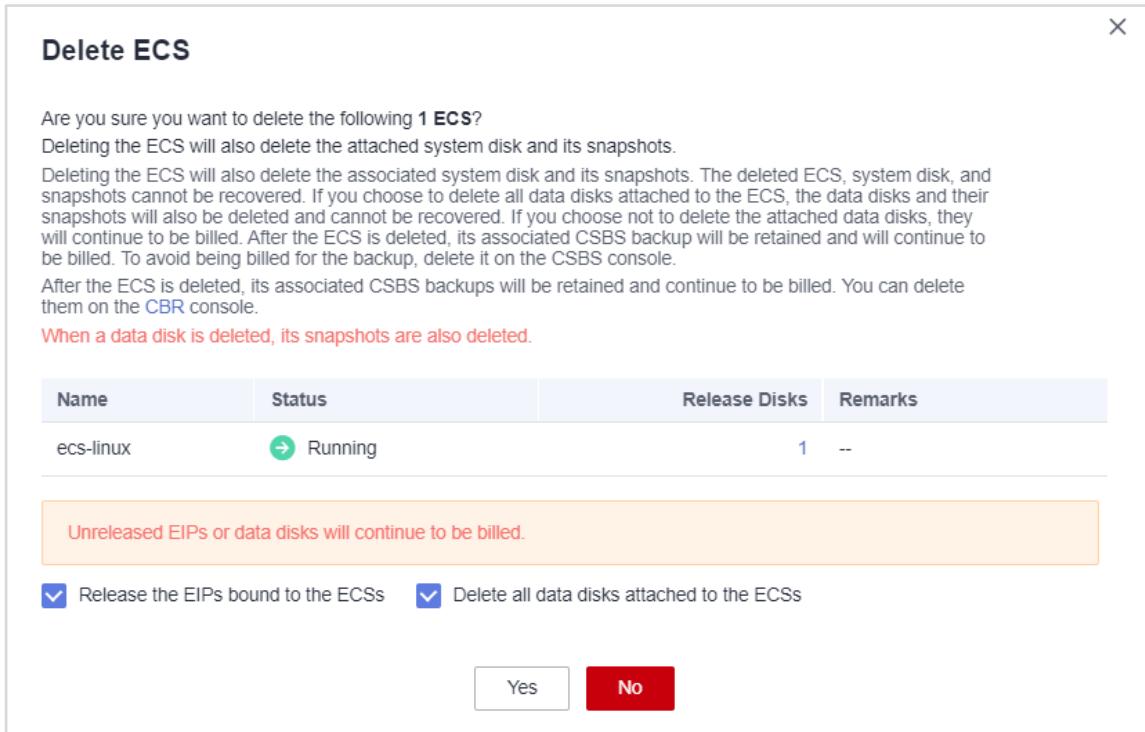
Step 17 Run the **vi** command to write content into the file, for example, “**Hello SFS Turbo**”, and run the **cat** command to view the content.

```
[root@ecs-linux sfs_turbo]# vi huawei_cloud
[root@ecs-linux sfs_turbo]# cat huawei_cloud
Hello SFS Turbo
[root@ecs-linux sfs]
```

### 4.3.3 Deleting Resources

#### 4.3.3.1 Deleting ECSs and EVSs

Step 1 Delete the ECS. Select the ECS to be deleted, choose More > Delete, and select Delete the data disk attached to the ECS.

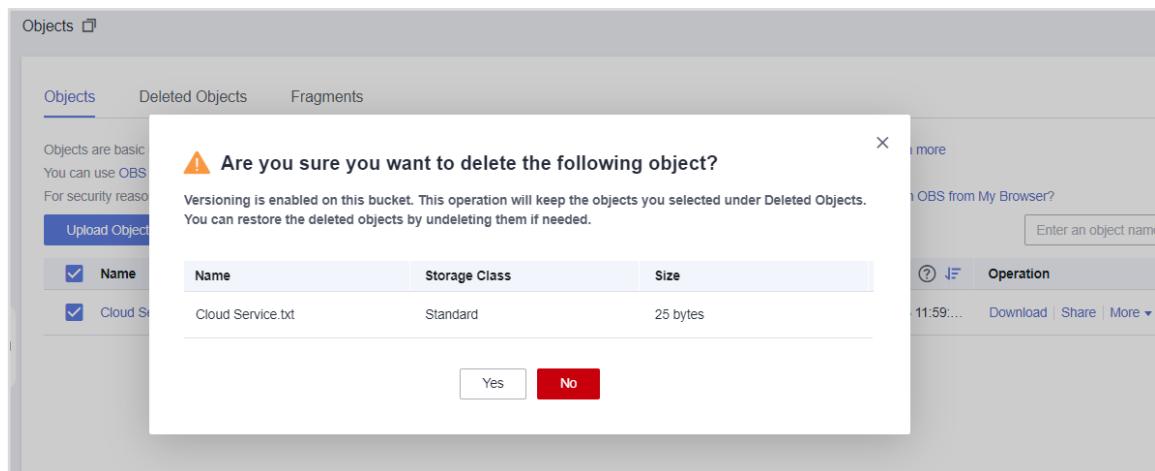


**Figure 4-58 Deleting an ECS and EVS disk**

Step 2 Click Yes to delete the ECS and EVS disk.

## Delete the OBS.

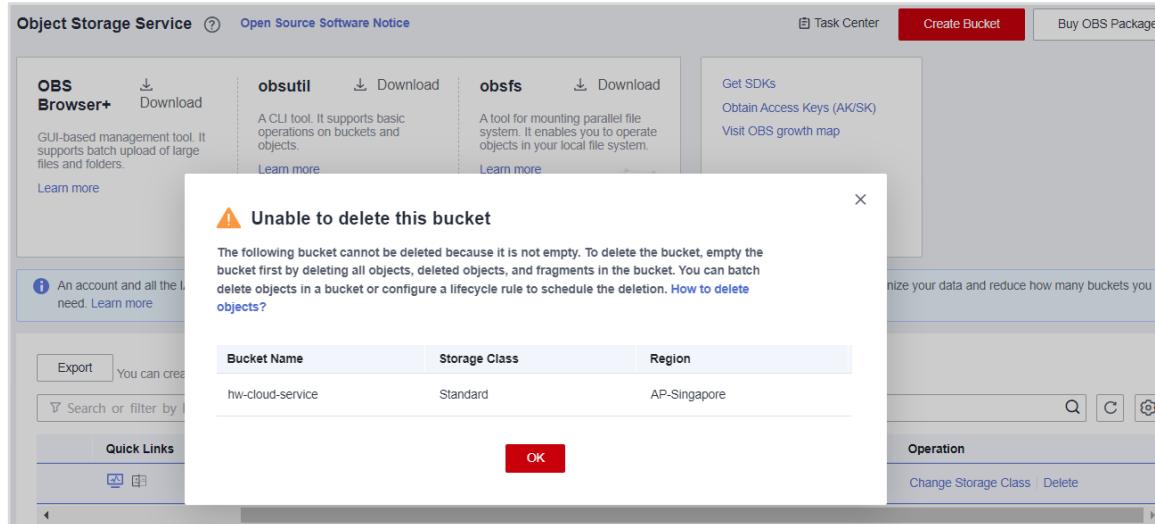
Step 3 Before deleting OBS, delete the files in the bucket.



**Figure 4-59 Deleting a file from a bucket**

Step 4 On the bucket list page, select the bucket to be deleted and click Delete.

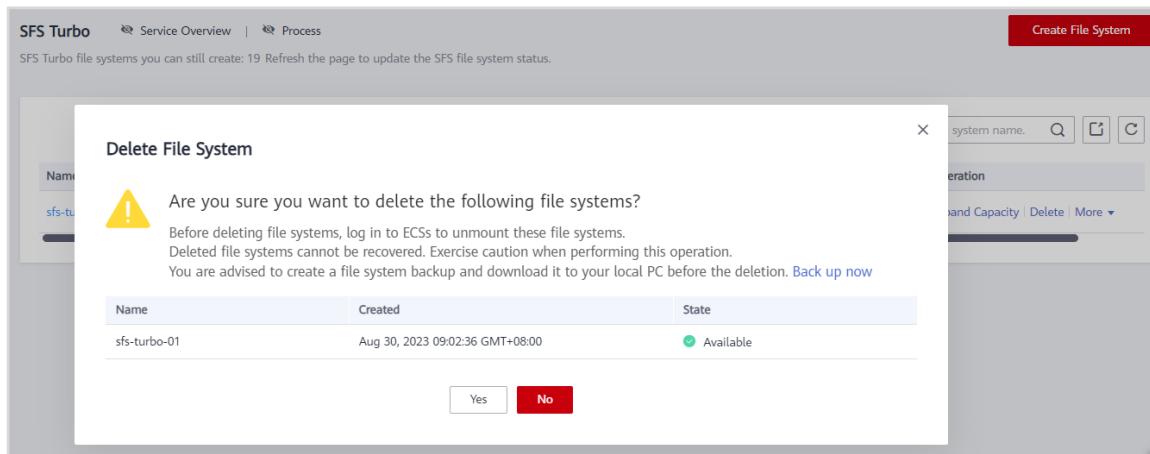
Step 5 Before deleting OBS, delete the files in the bucket.



**Figure 4-60 Deleting a file from a bucket**

#### 4.3.3.2 Delete the SFS file system.

Step 1 On the SFS console, locate the row that contains the created file system, click More, and click Delete.



**Figure 4-61 Deleting a File System**

## 4.4 Self-learning homework

Thinking Questions:

- After the /etc/fstab file has been configured on a Linux ECS, create a private image for the ECS and use the private image to create a same ECS. Check whether the file system is automatically mounted and whether shared files can be accessed.

# 5 O&M Services

## 5.1 Introduction

### 5.1.1 About This Exercise

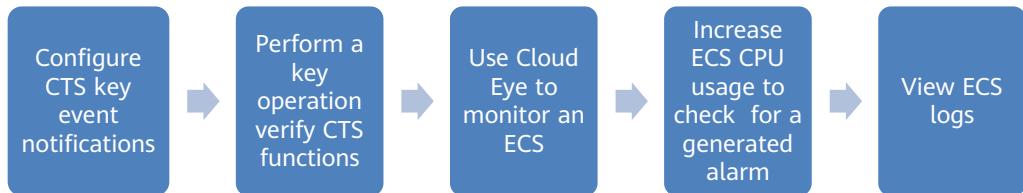
This experiment enables you to get familiar with CTS functions by monitoring key operations. Check ECS alarms on the Cloud Eye service. View ECS logs on LTS.

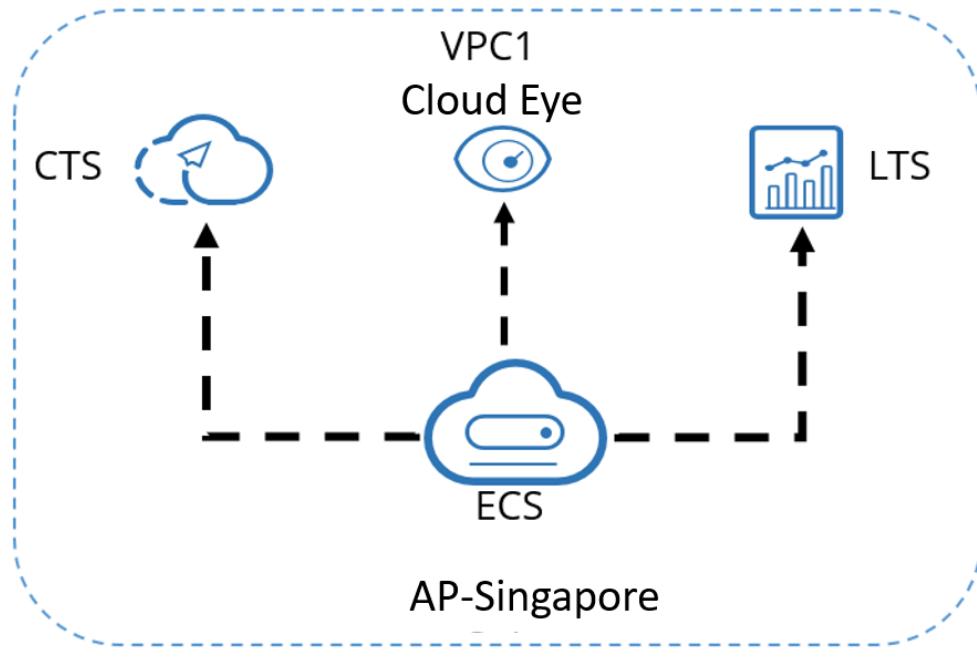
### 5.1.2 Objectives

In this exercise, you will:

- View the CTS console.
- Check ECS alarms on the Cloud Eye service.
- Use LTS to check ECS logs.

## 5.2 Tasks



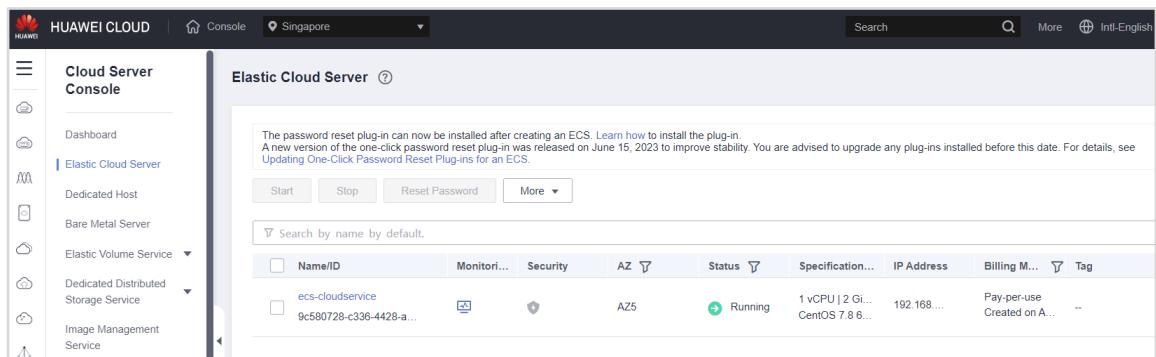


**Figure 5-1 Lab Topology**

## 5.2.2 Configuring CTS - key event notifications

### 5.2.2.1 Enabling a Tracker

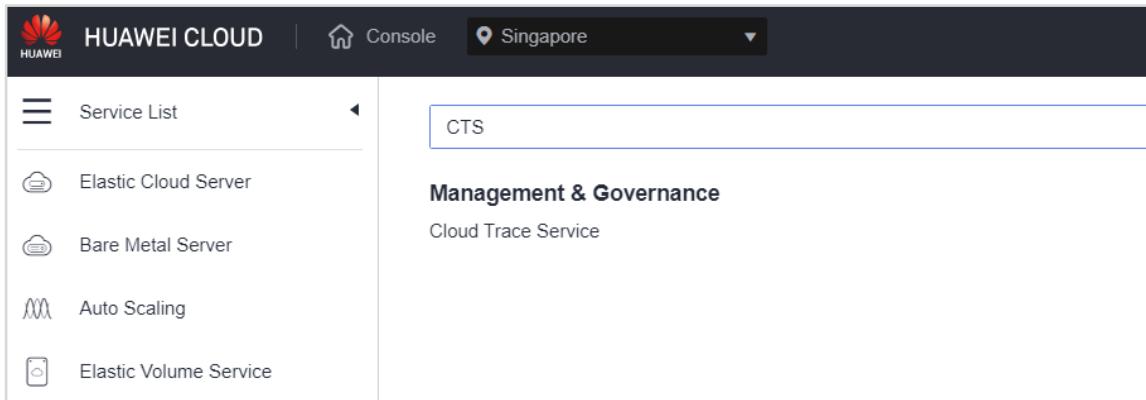
Step 1 Log in to the HUAWEI CLOUD **Cloud Server Console**, Create an **ECS**, for example, **ecs-cloudservice**. (General computing | 1-core | 2 GB | 40 GB | CentOS 7.8).



Name/ID	Monitor...	Security	AZ	Status	Specification...	IP Address	Billing M...	Tag
ecs-cloudservice 9c580728-c39e-4428-a...			AZ5	Running	1 vCPU   2 Gi... CentOS 7.8.8...	192.168...	Pay-per-use Created on A...	--

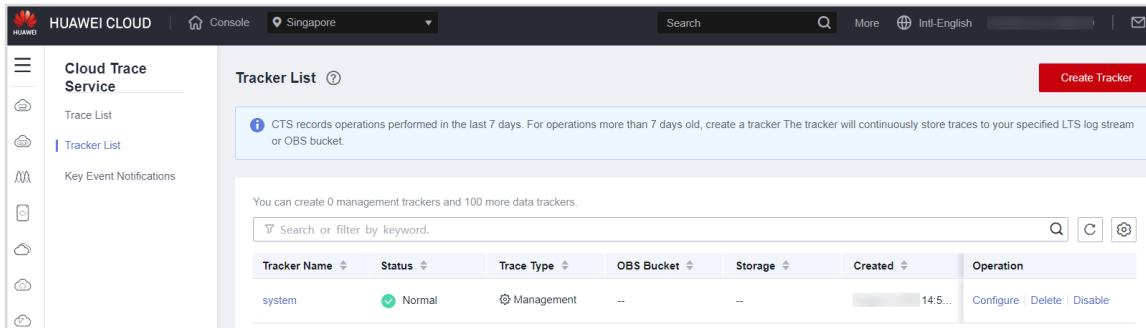
**Figure 5-2 Creating a VM**

Step 2 On the **service list** page, search for **Cloud Trace Service**. The Cloud Trace Service page is displayed.



**Figure 5-3 Enabling CTS**

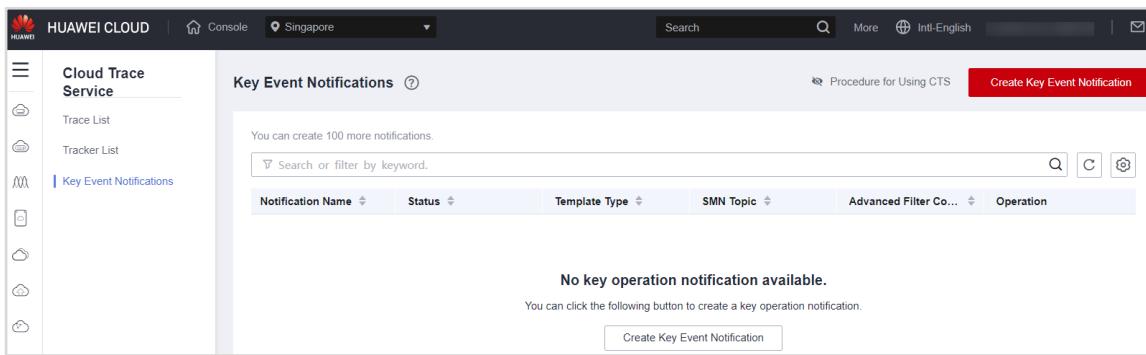
**Step 3 Enable and authorize CTS.** The CTS **tracker** created identifies and associates itself with all cloud services you are using. If the tracker status is Normal, the tracker is successfully applied.



**Figure 5-4 Viewing the default tracker**

### 5.2.2.2 Configuring Key Event Notifications

**Step 1** When a specific operation occurs, the created **SMN topic** can be used to send messages to users' mobile phones and emails. Click **Key Event Notification** in the left pane, and then click **Create Key Event Notification**.

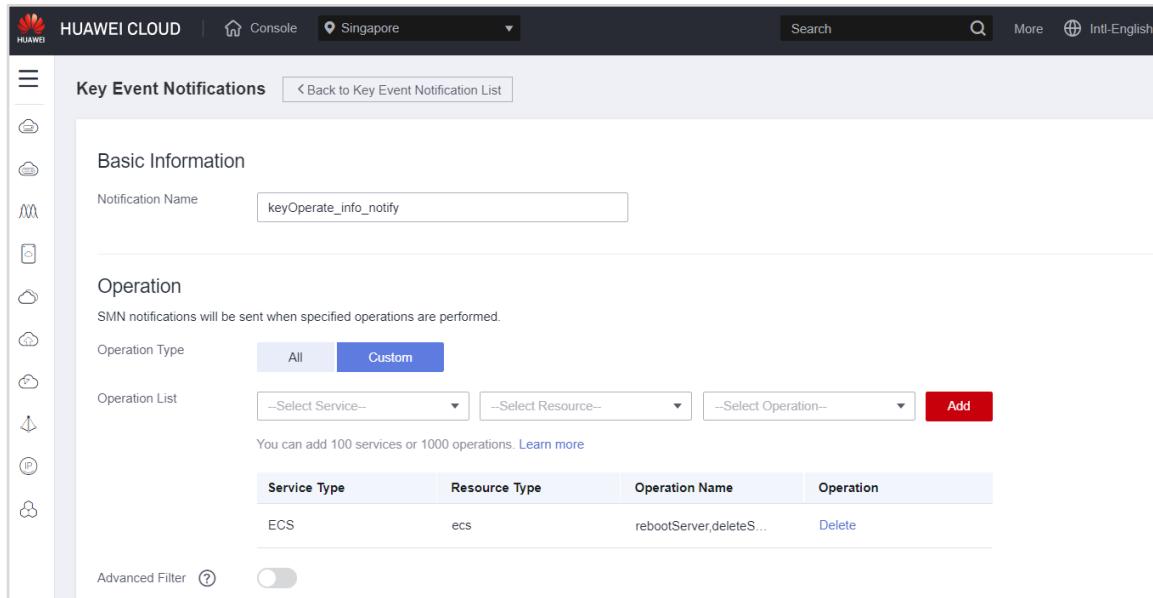


**Figure 5-5 Creating a key operation notification**

**Step 2** Set the following parameters and select **SMN** for the **key event notification**. If there is no topic, click **SMN** to add a **topic**.

- **Notification Name:** `keyOperate_info_notify(custom)`

- Operation Type: **Custom**
- Operation List: ECS – ecs - reboot/delete Server, Click Add
- User Type: **All users**
- Send Notification: **Yes**



**Figure 5-6 Configuration operation**

Step 3 **SMN notification** has not been configured. Therefore, SMN Topic is empty. Click SMN to go to the SMN service page and configure related parameters.

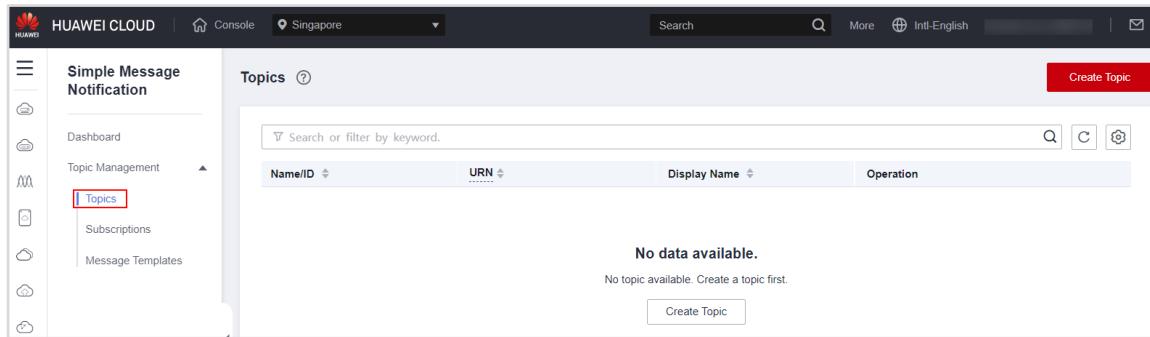
Note: SMN can proactively push notifications based on HUAWEI CLOUD users' requirements. End users can receive notifications through SMS messages, emails, or applications. A **topic** is a specific event type for which a message publication or client subscribes to a notification.



If no topic is available, switch to **SMN** and create a new one

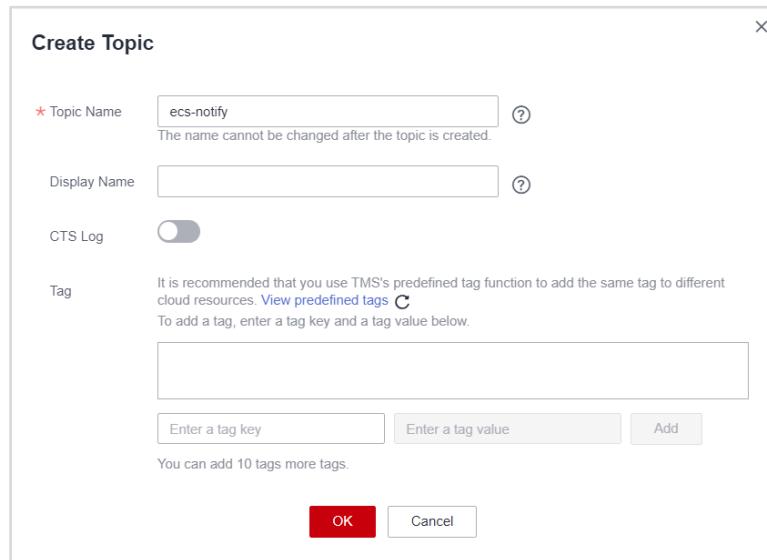
**Figure 5-7 Topic Configuration**

Step 4 In the SMN service, choose **Topic Management > Topic** and click **Create Topic**.



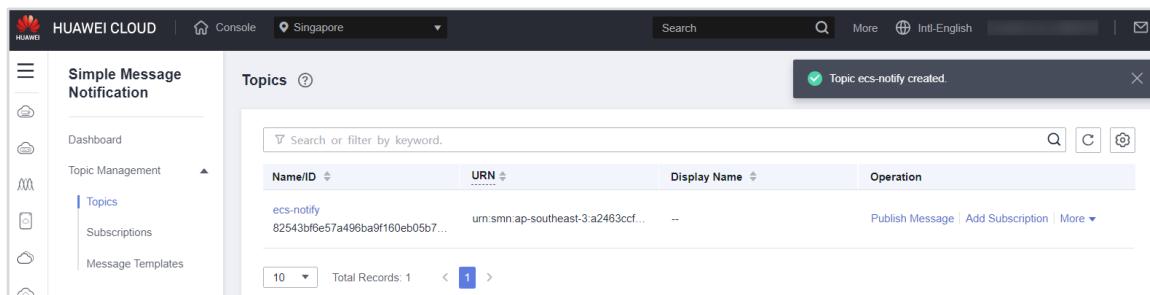
**Figure 5-8 Creating a topic**

Step 5 You can customize the theme **name** and click **OK** to create a theme.



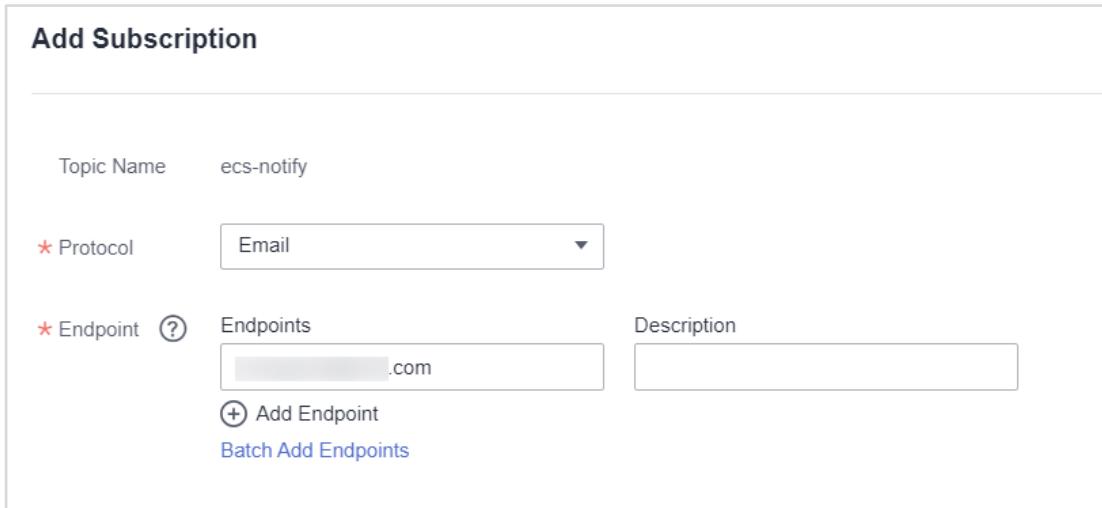
**Figure 5-9 Configuration Topic**

Step 6 The subscriber receives the message notification of the subscription topic through the receiving terminal. Adding a Subscription to a Created Topic.



**Figure 5-10 Adding a subscription**

Step 7 Click **Add Subscription**. You can select multiple subscription protocols, such as SMS and email. Here, select **Email**, enter the email address of the subscription terminal, and click **OK**.



Topic Name ecs-notify

\* Protocol Email

\* Endpoint .com

Description

+ Add Endpoint

Batch Add Endpoints

Figure 5-11 Configuring subscription

Step 8 On the **Topic Management** page, click **Subscription**. The new subscription information is displayed and the status is Unconfirmed. You will receive an SMS message from HUAWEI CLOUD. Click the **link** to **confirm** the subscription. After confirmation, you will receive a message indicating that the subscription is successful.



Subscript...	Protocol	Endpoint	Request H...	Description	Topic Name	Status	Operation
urn:smn:ap...	Email	mengxy32@...	--	--	ecs-notify	Unconfir...	<a href="#">Request Confirmation</a> <a href="#">Delete</a>

Figure 5-12 View Subscription

# SMN-Confirming Your Subscription

今天 15:36



Dear Sir or Madam,

Welcome to Simple Message Notification (SMN) service.

You are invited to subscribe to the topic:

**urn:smn:ap-southeast-3:a2463ccf139a47fba38e2bb890117453:ecs-notify**

After confirmation, you will receive messages posted to this topic via email. Instructions on how to cancel notifications will be included in these messages.

Click the following URL to confirm your subscription: (If you don't want to subscribe to this topic, please ignore this email)

[Confirm Subscription](#)

This URL is valid only within 48 hours.

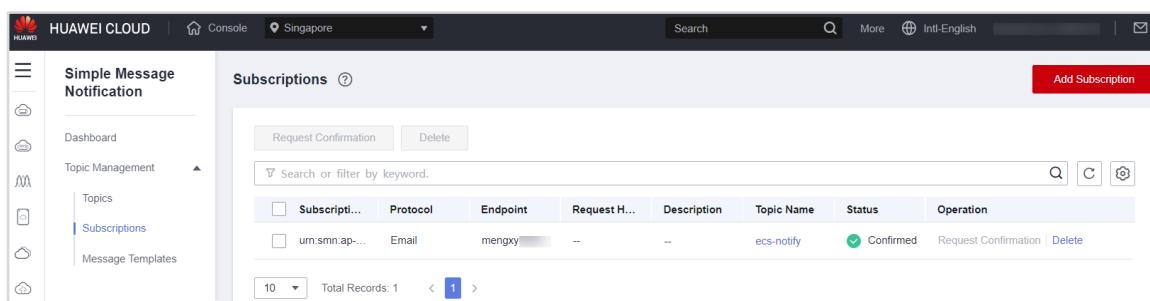
This is an automatically generated email. Please do not reply.

Official Website:

<https://www.huaweicloud.com/intl/en-us>

**Figure 5-13 Succeeded subscription**

Step 9 After the confirmation is complete, refresh the page. The subscription status changes to **Confirmed**.



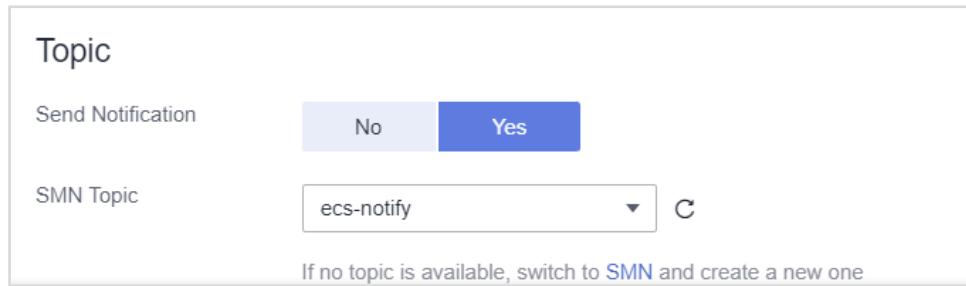
The screenshot shows the 'Subscriptions' page in the Huawei Cloud SMN console. The left sidebar has 'Simple Message Notification' selected under 'Topics'. The main area displays a table of subscriptions. One row is highlighted, showing the following details:

Subscription ID	Protocol	Endpoint	Request H...	Description	Topic Name	Status	Operation
urn:smn:ap-...	Email	mengxy	--	--	ecs-notify	<b>Confirmed</b>	<a href="#">Request Confirmation</a> <a href="#">Delete</a>

At the bottom of the table, it says 'Total Records: 1'.

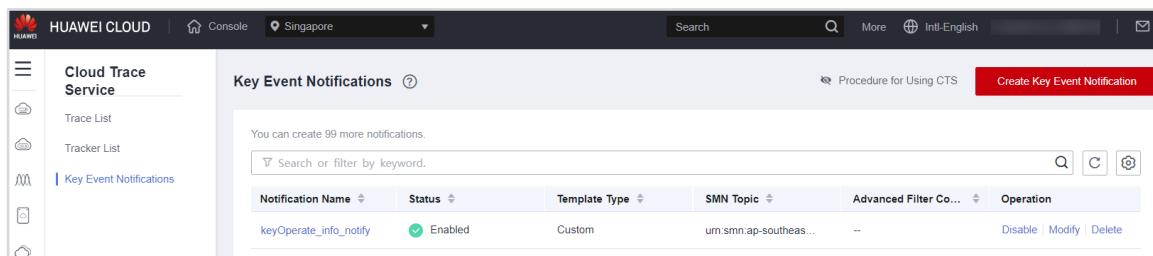
**Figure 5-14 Succeeded subscription configuration**

Step 10 After the SMN configuration is complete, return to CTS. In the **SMN Topic** area, select the **created topic** to create a **key operation notification**.



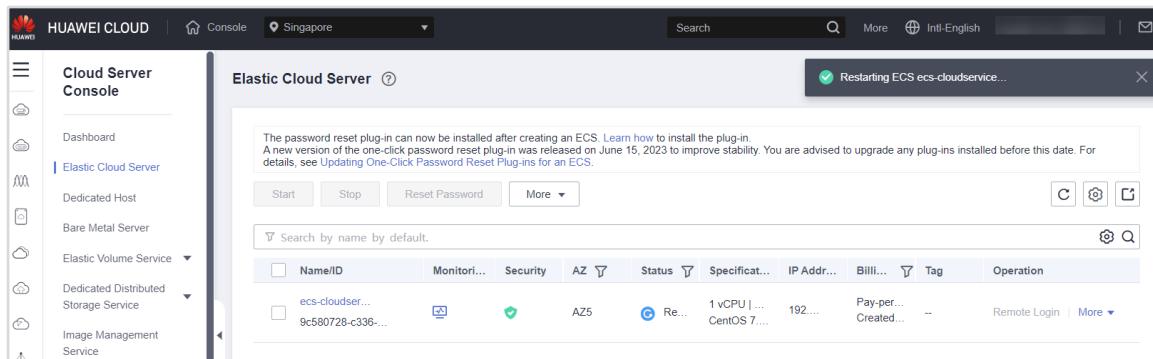
**Figure 5-15 Selecting a Topic**

Step 11 Check the **key operation notification** configuration.



**Figure 5-16 Complete key operation configuration**

Step 12 Return to the ECS page and **restart the ECS**.



**Figure 5-17 Reboot ECS**

Step 13 After the ECS is restarted, you will receive an **email notification** from HUAWEI CLOUD.

# CTS - A Trace Generated for a Performed Operation

16:45



Dear [REDACTED]  
Resource **ecs-cloudservice** was operated at 2023-08-30 16:45:40 GMT+0800. For more information, [log in the CTS console](#)

**Region:** AP-Singapore  
**Operation:** rebootServer  
**Operation Target:** ECS(ecs-cloudservice, 9c580728-c336-4428-ae55-d44a550c2e78)  
//Service name (Resource name, Resource ID)  
**Operation Performed:** 2023-08-30 16:45:40 GMT+0800  
**User:** [REDACTED] ?

**Trace Content:**

```
{  
    "api_version": "1.0",  
    "message": "success",  
    "project_id": "a2463ccf139a47fba38e2bb890117453",  
    "record_time": "[REDACTED] 16:45:40 GMT+0800",  
    "request": {"reboot": {"type": "SOFT", "servers": [{"id": "9c580728-c336-4428-ae55-d44a550c2e78"}]}},  
    "request_id": null,  
    "resource_id": "9c580728-c336-4428-ae55-d44a550c2e78",  
    "resource_name": "ecs-cloudservice",  
    "resource_type": "ecs",  
    "response": "  
        {"job_id": "ff8080828a1da130018a459e5c724ad3", "job_type": "serverActions", "begin_time": "[REDACTED]-  
        08-30T16:45:20.881Z", "end_time": "[REDACTED]-  
        30T16:45:40.100Z", "status": "SUCCESS", "error_code": null, "fail_reason": null, "entities":  
        {"server_id": "9c580728-c336-4428-ae55-d44a550c2e78"}},  
        {"service_type": "ECS",  
        "source_ip": "122.9.169.113",  
        "time": "[REDACTED] 16:45:40 GMT+0800",  
        "trace_id": "991c2a9c-4711-11ee-a42f-4572875480af",  
        "trace_name": "rebootServer",  
        "trace_rating": "normal",  
        "trace_type": "ConsoleAction",  
        "user":  
            {"name": "[REDACTED]", "id": "62e9ab095c8b4229945297b8e0ff927f", "domain": "[REDACTED]"},  
            {"name": "[REDACTED]", "id": "a4a3d32b07e24d4da7ca470b798f3214"}}  
    }  
}
```

Thank you for using HUAWEI CLOUD.

Sincerely,  
HUAWEI CLOUD

This is an automatically generated email. Please do not reply.

Official website: <https://www.huaweicloud.com> (Chinese Mainland)  
<https://intl.huaweicloud.com> (International)

**Figure 5-18 Message notification success**

Step 14 The Trace List displays traces generated in the last 7 days. The traces contain details about operations performed on cloud resources.

Trace Name	Resource ID	Resource Name	Trace Status	Operator	Operation Time	Operation
prepareForStopS...	evs	EVS	--	--	<span style="color: green;">normal</span>	<a href="#">View Trace..</a>
prepareForStopS...	evs	EVS	--	--	<span style="color: green;">normal</span>	<a href="#">View Trace..</a>
rebootServer	ecs	ECS	9c580728-c336-4...	ecs-cloudservice	<span style="color: green;">normal</span>	<a href="#">View Trace..</a>
operateServer	server	ECS	9c580728-c336-4...	--	<span style="color: green;">normal</span>	<a href="#">View Trace..</a>
rebootServer	ecs	ECS	9c580728-c336-4...	ecs-cloudservice	<span style="color: green;">normal</span>	<a href="#">View Trace..</a>
operateServer	server	ECS	9c580728-c336-4...	--	<span style="color: green;">normal</span>	<a href="#">View Trace..</a>

**Figure 5-19 Viewing events**

The configuration of CTS key operation notification is complete.

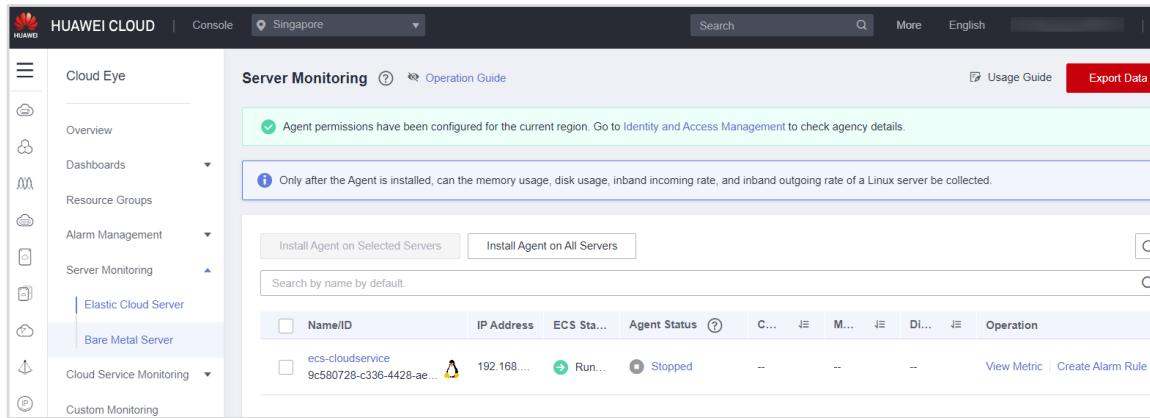
## 5.2.3 Use Cloud Eye - Monitoring ECS

### 5.2.3.1 Monitoring an ECS

Step 1 In the HUAWEI CLOUD service list, search for and select Cloud Eye.

**Figure 5-20 Enabling the Cloud Eye Service**

Step 2 On the CES page, choose **Server Monitoring**. Server Monitoring provides multi-level metrics monitoring for hosts, including basic monitoring, OS monitoring, and process monitoring. The monitoring **plug-in** of the ECS is installed by default. If the plug-in is not installed, you can manually install it.



The screenshot shows the 'Server Monitoring' section of the Huawei Cloud console. The left sidebar has 'Cloud Eye' selected under 'Server Monitoring'. The main area displays a table with one row of data:

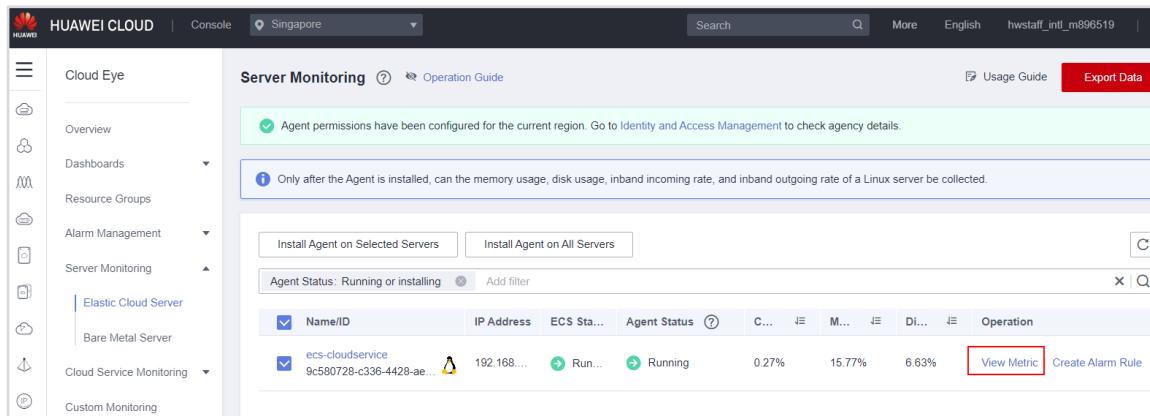
Name/ID	IP Address	ECS Status	Agent Status	C...	M...	D...	Operation
ecs-cloudservice 9c580728-c336-4428-ae...	192.168....	Run...	Stopped	--	--	--	<a href="#">View Metric</a>   <a href="#">Create Alarm Rule</a>

**Figure 5-21 Host Monitoring**

Step 3 (Optional) If the agent has been installed but is not running properly, **log in** to the **ECS** and check the agent status. If the agent status is not running, manually start the agent.

```
Welcome to Huawei Cloud Service
[root@ecs-cloudservice ~]# /usr/local/uniagent/extension/install/telescope/telescopd status
Telescope process is not running.
[root@ecs-cloudservice ~]# /usr/local/uniagent/extension/install/telescope/telescopd start
Starting telescope...
Telescope process starts successfully.
[root@ecs-cloudservice ~]# /usr/local/uniagent/extension/install/telescope/telescopd status
Telescope process is running well.
[root@ecs-cloudservice ~]#
```

Step 4 Click **View Monitoring Indicator** on the server monitoring page to view the running status and performance parameters of the current host.

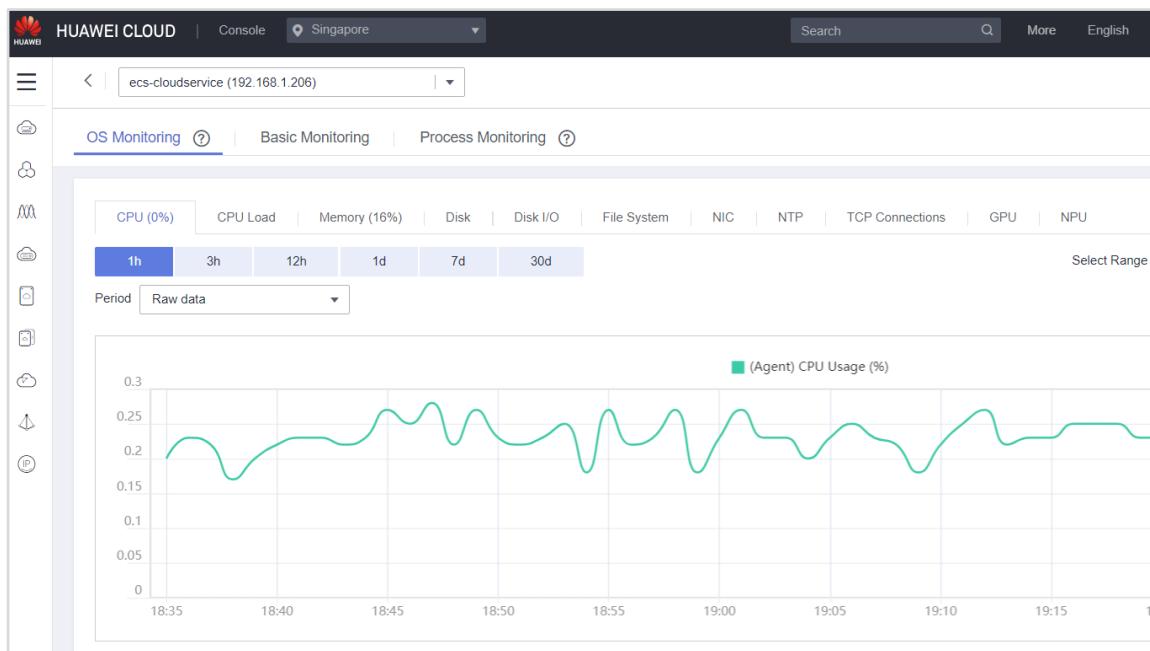


The screenshot shows the 'Server Monitoring' section of the Huawei Cloud console. The left sidebar has 'Cloud Eye' selected under 'Server Monitoring'. The main area displays a table with one row of data, where the 'Agent Status' column is highlighted with a red border:

Name/ID	IP Address	ECS Status	Agent Status	C...	M...	D...	Operation
ecs-cloudservice 9c580728-c336-4428-ae...	192.168....	Run...	Running	0.27%	15.77%	6.63%	<a href="#">View Metric</a>   <a href="#">Create Alarm Rule</a>

**Figure 5-22 Viewing ECS monitoring metrics**

Step 5 You can view the monitoring indicators as required.

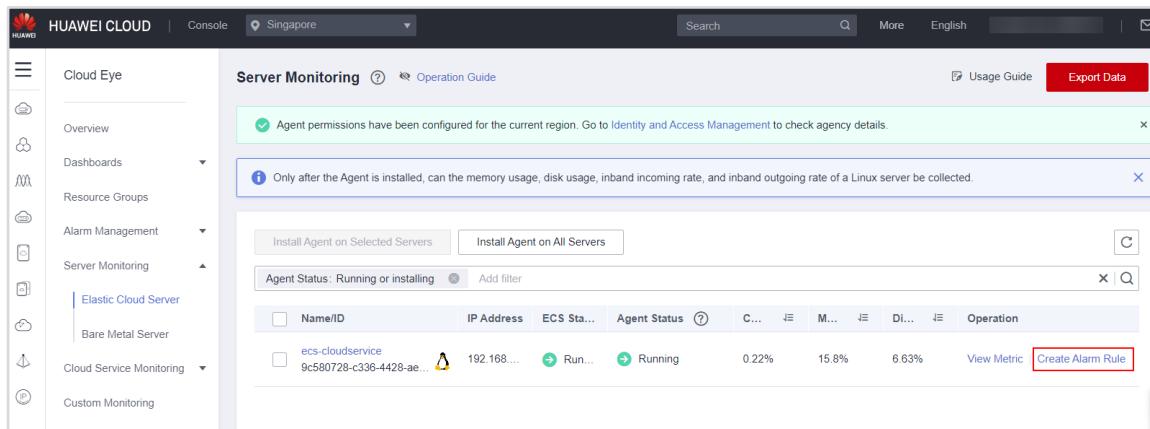


**Figure 5-23 Viewing monitoring indicators**

### 5.2.3.2 Creating an Alarm

Users can flexibly configure alarm rules and notification settings to learn about the running status and performance of instance resources in a timely manner, preventing service loss caused by resource problems.

Step 1 Click **Create Alarm Rule** on the right of the ECS list.

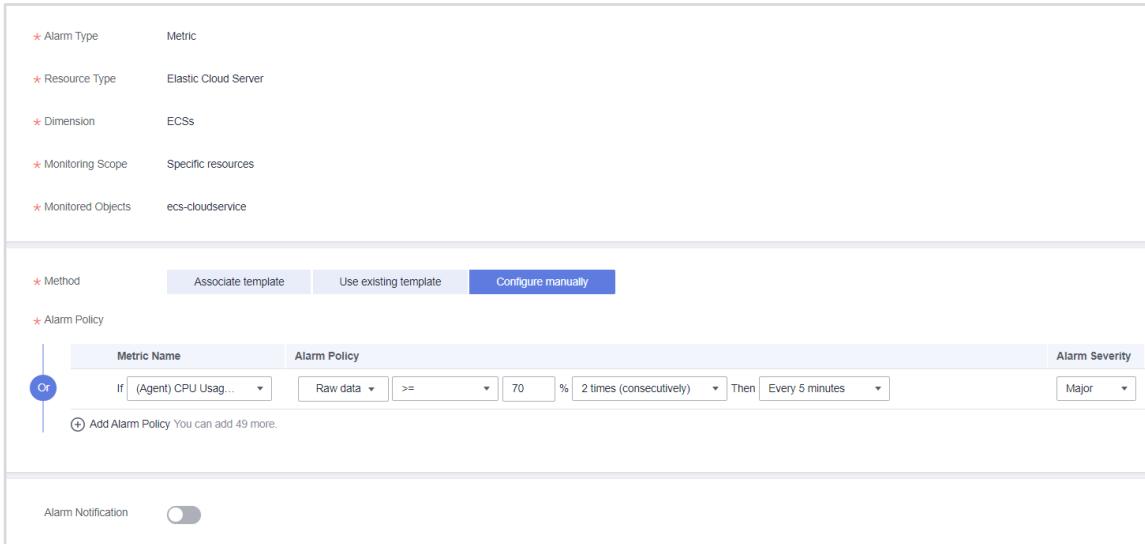


**Figure 5-24 Creating an alarm rule**

Step 2 Set related parameters based on the following information: After the configuration is complete, click **Create Now**.

- Name: **alarm-ecs** (custom)
- Alarm Type: Elastic Cloud Server
- Method: Configure manually

- Alarm Policy: ( Agent ) CPU Usage RAW data  $\geq 70\%$  , 2 times, Every 5 minutes
- Alarm Severity: Major
- Alarm Notification: close

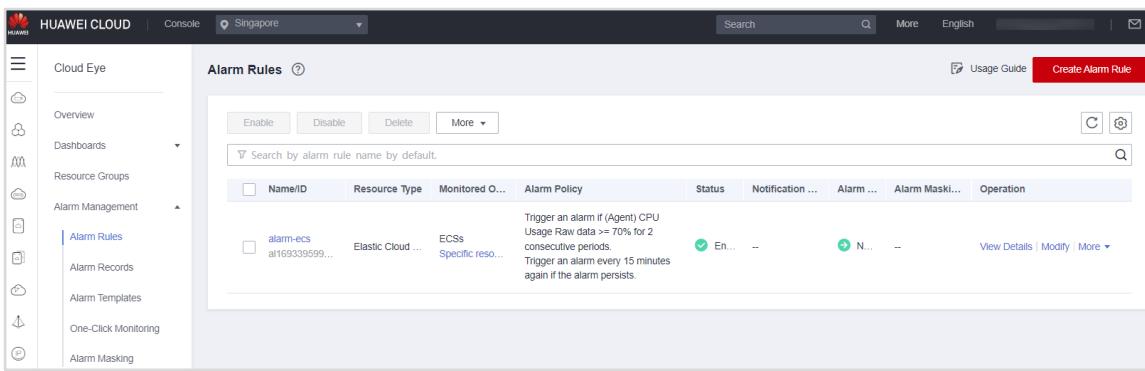


The screenshot shows the configuration of an alarm rule. The configuration details are as follows:

- Metric:** Metric
- Resource Type:** Elastic Cloud Server
- Dimension:** ECSS
- Monitoring Scope:** Specific resources
- Monitored Objects:** ecs-cloudservice
- Method:** Configure manually
- Metric Name:** (Agent) CPU Usag...
- Alarm Policy:**
  - If (Agent) CPU Usag... Raw data  $\geq$  70 % 2 times (consecutively) Then Every 5 minutes
- Alarm Severity:** Major
- Alarm Notification:** close

Figure 5-25 Configuring alarm rules

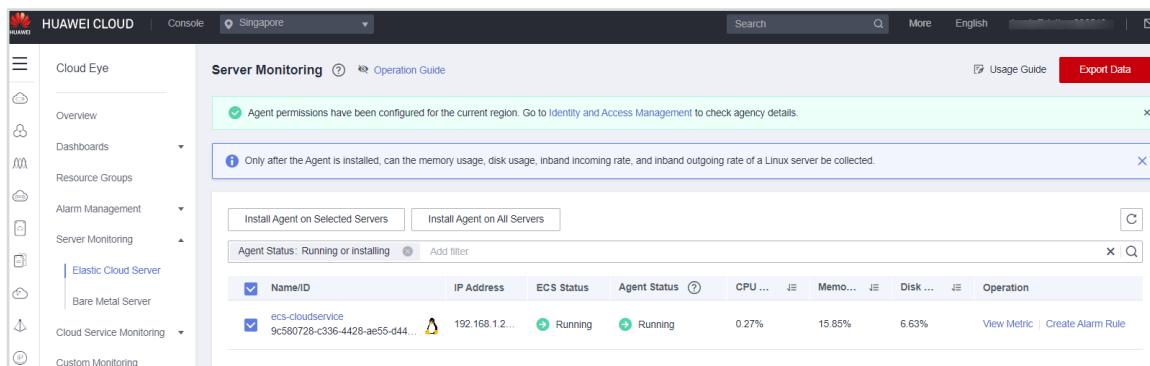
Step 3 After the alarm rule is created, the Alarm Rule page is displayed. If the alarm status of the ECS changes to Enabled on the list page, the alarm rule is successfully created.



Name/ID	Resource Type	Monitored O...	Alarm Policy	Status	Notification ...	Alarm ...	Alarm Maski...	Operation
alarm-ecs ari69339599...	Elastic Cloud ...	ECSS Specific reso...	Trigger an alarm if (Agent) CPU Usage Raw data $\geq 70\%$ for 2 consecutive periods. Trigger an alarm every 15 minutes again if the alarm persists.	En...	N...			<a href="#">View Details</a>   <a href="#">Modify</a>   <a href="#">More</a>

Figure 5-26 Viewing alarm rules

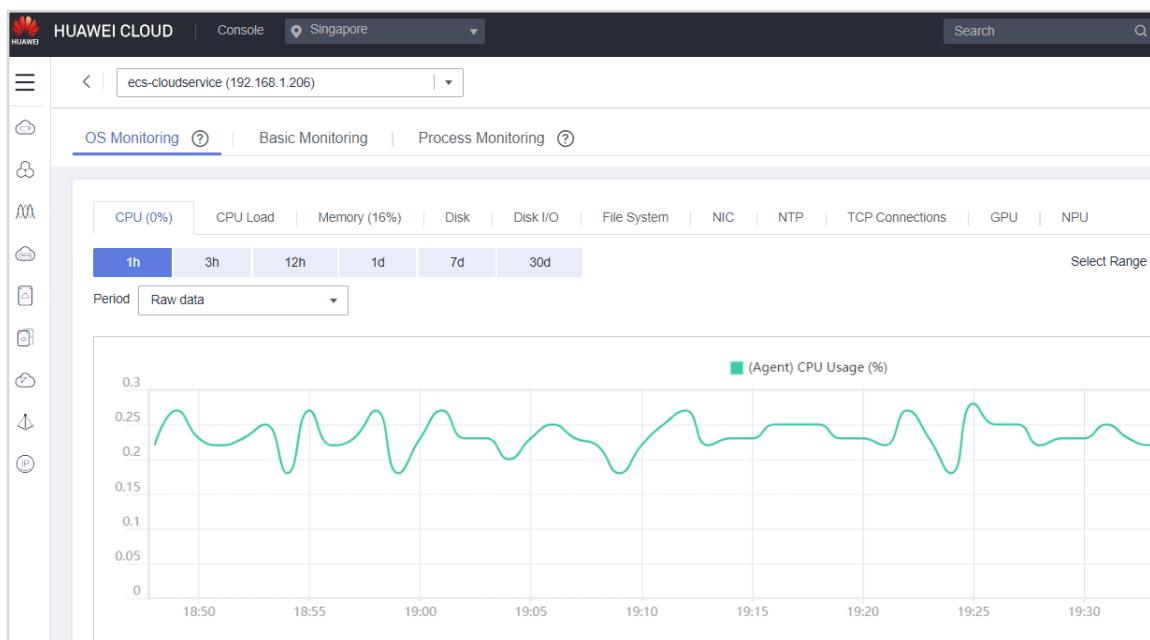
Step 4 Return to the **server monitoring** page and check the CPU usage.



The screenshot shows the HUAWEI CLOUD Server Monitoring page. On the left sidebar, under 'Server Monitoring', 'Elastic Cloud Server' is selected. The main area displays a table of server monitoring data. One row is highlighted for the server 'ecs-cloudservice' with IP address 192.168.1.206. The table includes columns for Name/ID, IP Address, ECS Status, Agent Status, CPU Usage, Memory Usage, Disk Usage, and Operation. A green checkmark indicates agent permissions are configured. Buttons for 'Install Agent on Selected Servers' and 'Install Agent on All Servers' are visible.

**Figure 5-27 Viewing CPU monitoring indicators**

Step 5 You can also view the detailed data on the monitoring metrics page. The current CPU usage is obvious and does not meet the alarm triggering conditions.

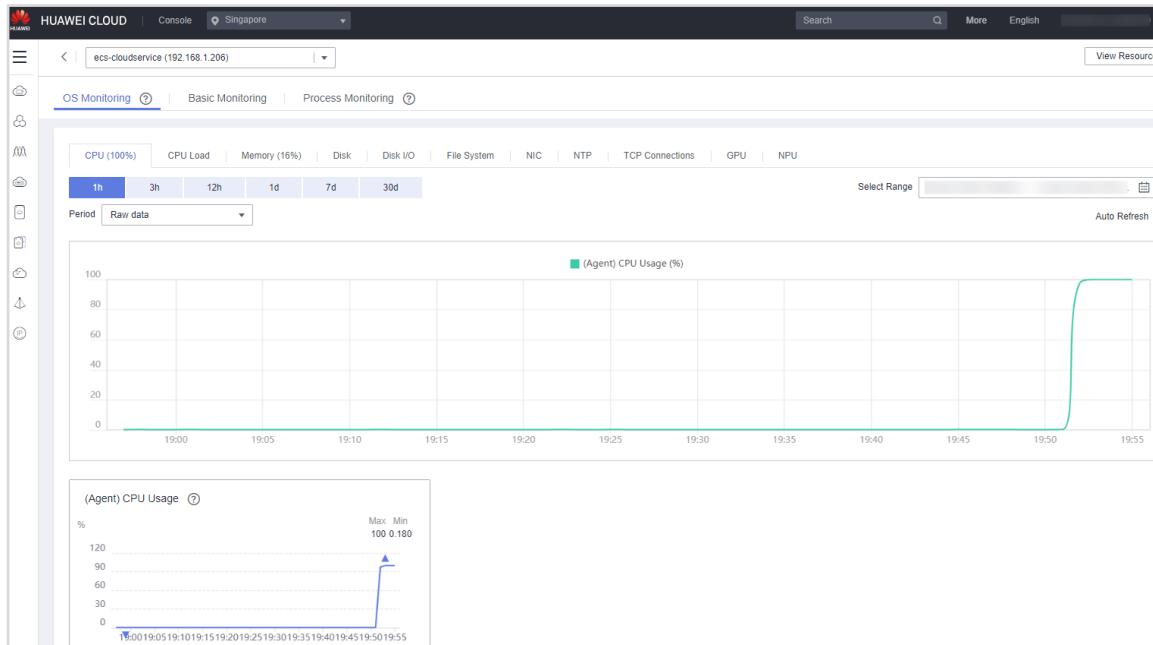


**Figure 5-28 Monitoring Indicator Interface**

Step 6 Log in to the ECS remotely as user root and run the following command to increase the CPU usage of the ECS.

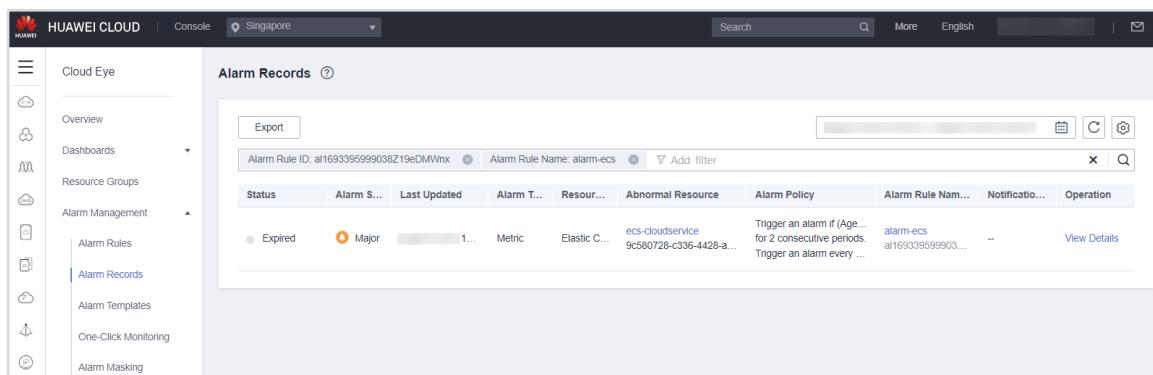
```
Welcome to Huawei Cloud Service
[root@ecs-cloudservice ~]# echo "scale=800000; 4*a(1)" | bc -l -q
```

Step 7 Return to the ECS monitoring page and refresh the data. The CPU usage quickly increases by 100%.



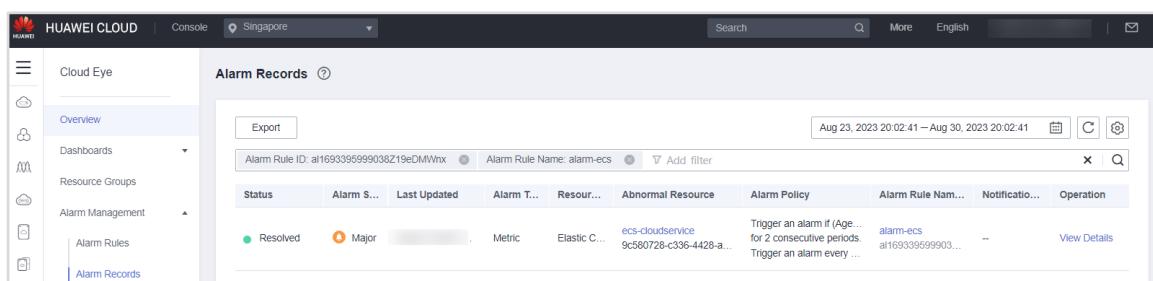
**Figure 5-29 CPU Usage**

Step 8 Choose **Cloud Eye > Alarm > Alarm Records** to view alarm information. The created alarm status changes to Alarming.



**Figure 5-30 Alarm Records Displaying in Alarm**

Step 9 Restart the ECS or press **Ctrl+C** to stop the program. Observe the CPU usage and alarm status.



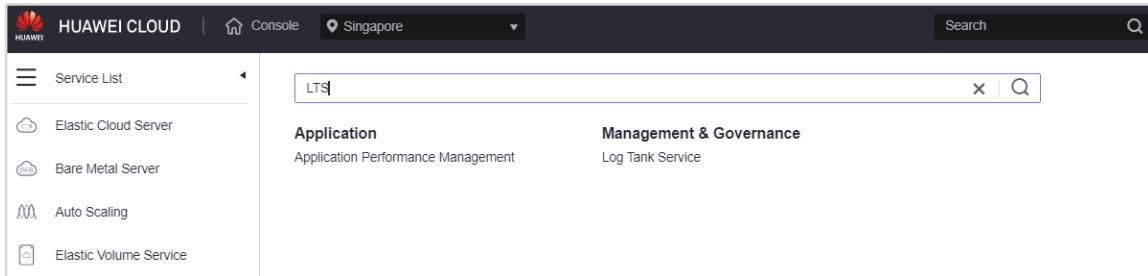
**Figure 5-31 Alarm recovery**

The experiment on using Cloud Eye to monitor ECSs is complete.

## 5.2.4 LTS-Viewing ECS Logs

### 5.2.4.1 Creating a Log Group and Log Stream

Step 1 In the **service list** of HUAWEI CLOUD, search for **LTS** and click LTS to go to the service page.

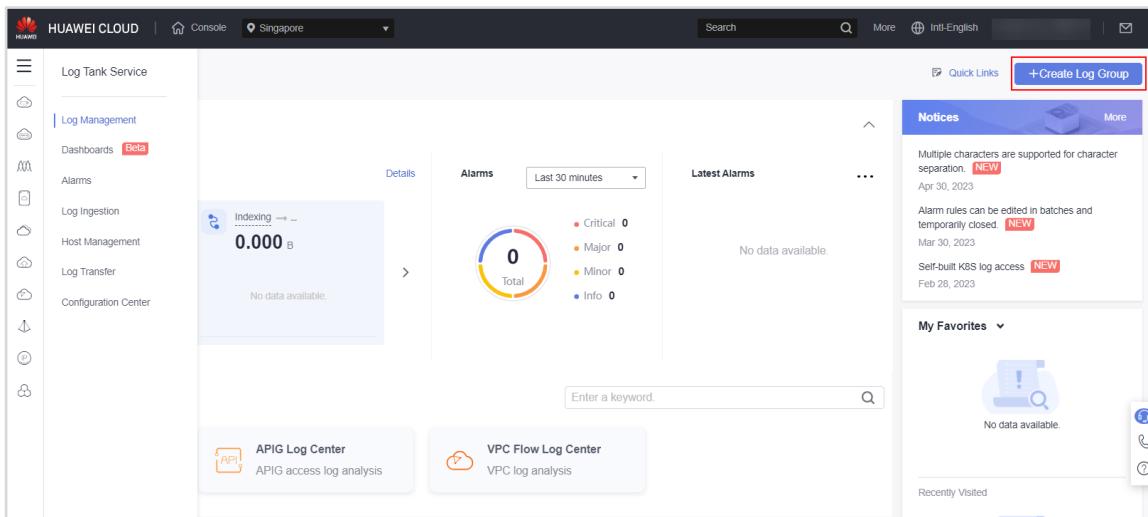


The screenshot shows the HUAWEI CLOUD service list interface. On the left, there's a sidebar with icons for Elastic Cloud Server, Bare Metal Server, Auto Scaling, and Elastic Volume Service. The main area has a search bar at the top with 'LTS' typed in. Below the search bar, there are two sections: 'Application' (containing Application Performance Management) and 'Management & Governance' (containing Log Tank Service). The 'Log Tank Service' section is highlighted.

Figure 5-32 Enabling LTS

Step 2 Log groups and log streams are the basic units for LTS to manage logs. Before using LTS, you need to create a log group and log stream.

On the **Log Management** page, click **Create Log Group**.



The screenshot shows the Log Management page for the Log Tank Service. The left sidebar includes options like Dashboards (Beta), Alarms, Log Ingestion, Host Management, Log Transfer, and Configuration Center. The main area displays indexing status (0.000 B), a circular alarm summary (0 Total), and links to APIG Log Center and VPC Flow Log Center. A prominent red box highlights the '+Create Log Group' button in the top right corner of the main panel.

Figure 5-33 Creating a log group

Step 3 Enter the log group name and log storage duration, and click **OK**.

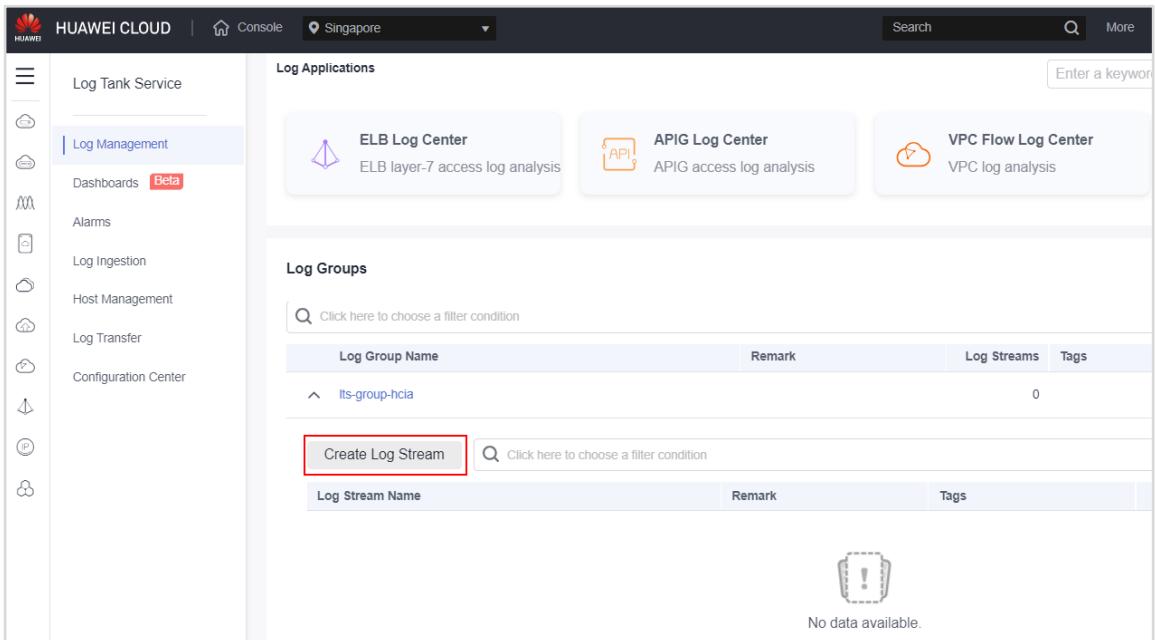
**Create Log Group**

---

Log Group Name	<input type="text" value="Its-group-hcia"/> <span style="font-size: small;">(?)</span>
Log Retention Duration	<input type="text" value="30"/>
You can set the retention duration to 1-365 days (30 days by default). Logs older than the specified duration will be automatically deleted. For long-term storage, you can transfer logs to OBS buckets.	
You can create log groups for free, but charges apply for log read/write, indexing, and storage. <a href="#">Pricing details</a>	
Tag	<input type="text" value="Press Enter after each tag. Example: a=a"/>
You can add 20 more tags. (System tags not included)	

**Figure 5-34 Configuring a log group**

Step 4 On the **Log Management** page, you can see the created log group. On the current page, click **Create Log Stream**.



The screenshot shows the Huawei Cloud Log Management interface. On the left, there's a sidebar with icons for Log Tank Service, Log Management (selected), Dashboards (Beta), Alarms, Log Ingestion, Host Management, Log Transfer, and Configuration Center. The main area has two sections: "Log Applications" and "Log Groups". Under "Log Applications", there are links to ELB Log Center, APIG Log Center, and VPC Flow Log Center. Under "Log Groups", there's a table with one row for "Its-group-hcia". The "Create Log Stream" button is highlighted with a red box. Below the table, it says "No data available." with an exclamation mark icon.

**Figure 5-35 Entering the log group**

Step 5 Enter a log stream **name** and click **OK**.

**Create Log Stream** (?) X

Log Group Name	Its-group-hcia
Log Stream Name	Its-topic-hcia <span>(?)</span>
Log Retention Duration	<input checked="" type="checkbox"/> <span>(?)</span>
Tag	Press Enter after each tag. Example: a=a
Remark	   

**Figure 5-36 Configuring the log flow**

Step 6 Create a combined log stream.

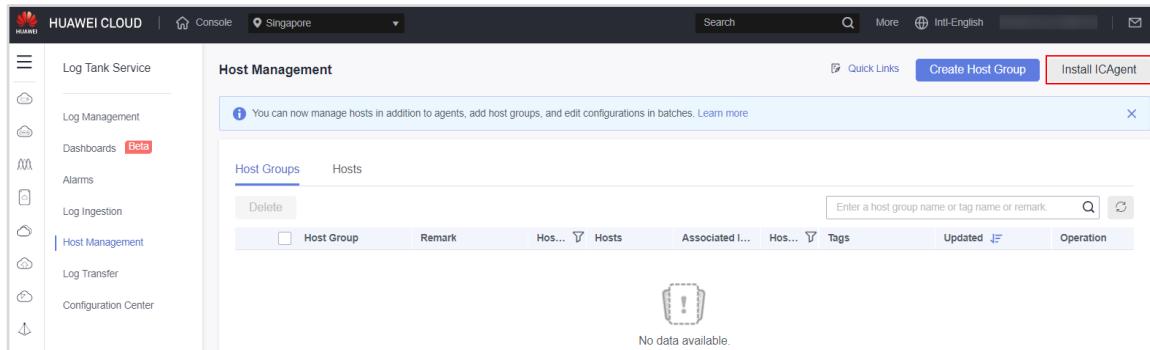
日志组列表				
<input type="text"/> 点击此处添加筛选条件 <span>(?)</span>				
日志组名称	备注	日志流数量	标签	操作
Its-group-IA		1		<a href="#">修改</a>   <a href="#">删除</a>   <a href="#">详情</a>
<a href="#">创建日志流</a> <span>(?)</span> <input type="text"/> 点击此处添加筛选条件 <span>(?)</span> <a href="#">全部企业项目</a> <span>(?)</span>				
日志流名称	备注	企业项目	标签	指标数 操作
Its-topic-ia		default		<a href="#">-</a> <a href="#">编辑</a> <a href="#">星标</a> <a href="#">导出</a> <a href="#">删除</a> <a href="#">更多</a>

**Figure 5-37 Finishing Log Group/Flow Creation**

#### 5.2.4.2 Install ICAgent

Step 1 ICAgent is a tool used by LTS to collect logs. It runs on the host where logs need to be collected to create a combined log stream.

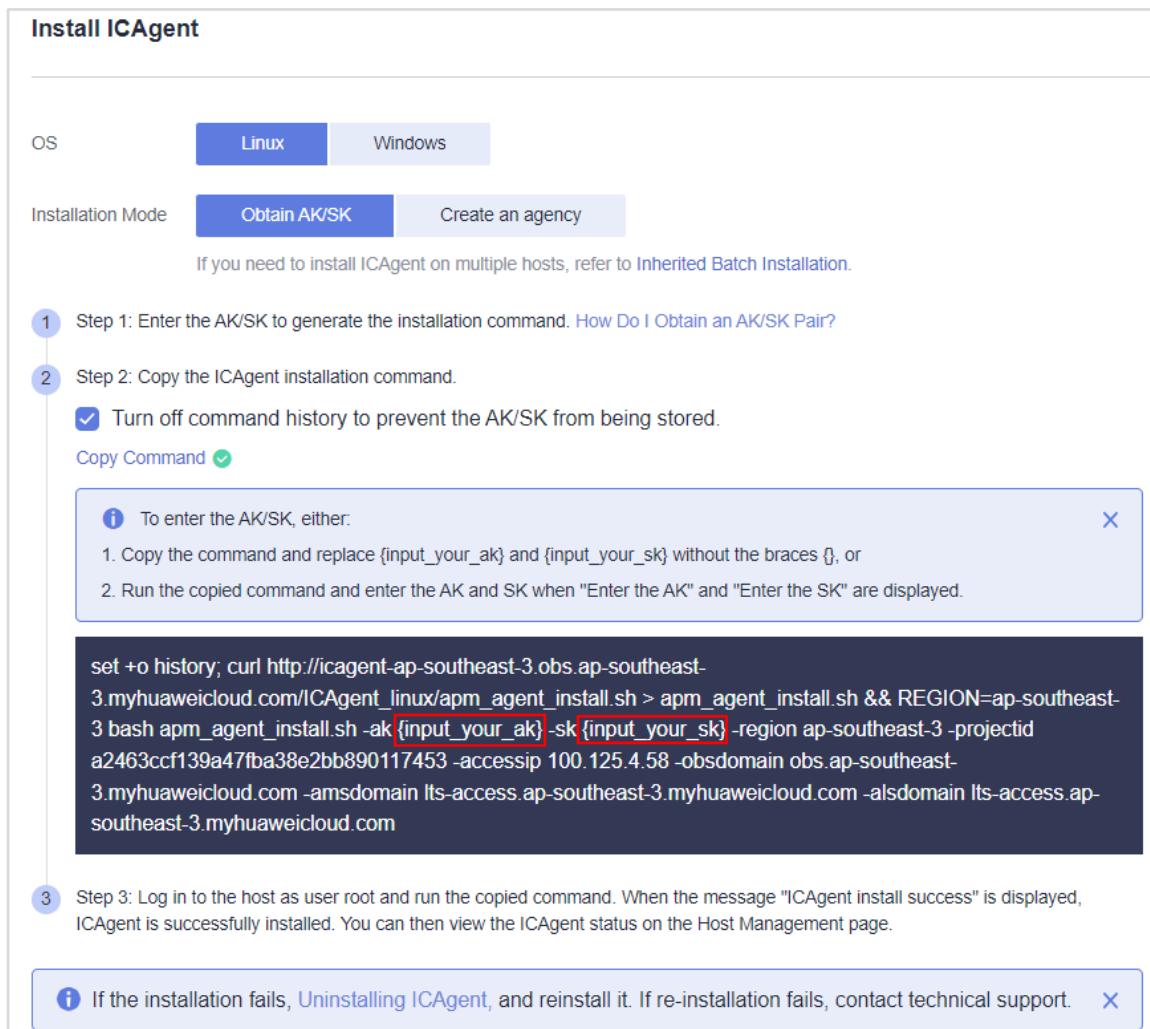
In the left pane of the LTS console, choose **Host Management**. In the upper right corner of the page, click **Install ICAgent**.



**Figure 5-38 Viewing Host Management**

Step 2 Select the host where the ICAgent is to be installed. Replace the AK/SK in the command line with the obtained AK/SK, as shown in the red box in the following figure. Click Copy Command to copy the command.

- OS: Linux
- Installation Mode: **Obtain AK/SK**



```
set +o history; curl http://icagent-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/ICAgent_linux/apm_agent_install.sh > apm_agent_install.sh && REGION=ap-southeast-3 bash apm_agent_install.sh -ak [input_your_ak] -sk [input_your_sk] -region ap-southeast-3 -projectid a2463ccf139a47fba38e2bb890117453 -accessip 100.125.4.58 -obsdomain obs.ap-southeast-3.myhuaweicloud.com -amsdomain lts-access.ap-southeast-3.myhuaweicloud.com -alsdomain lts-access.ap-southeast-3.myhuaweicloud.com
```

**Figure 5-39 Installing the ICAgent**

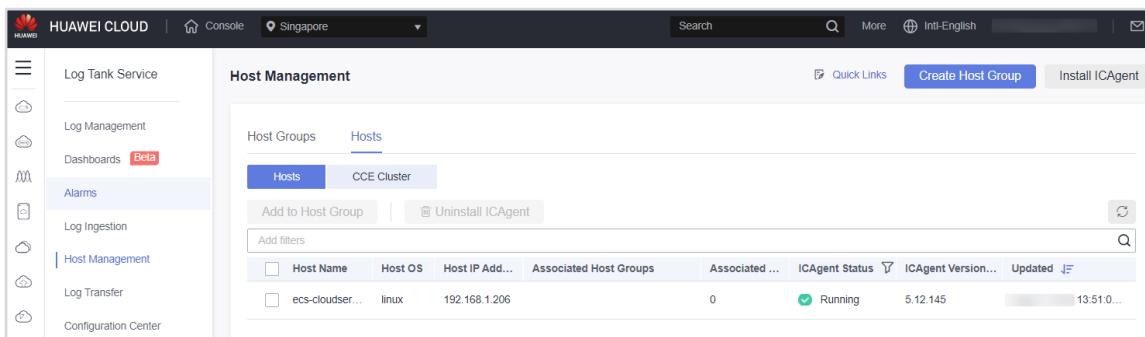
**Step 3 Log in to the ECS as user **root**, copy the commands in the previous step, and run the commands on the CLI. If ICAgent install success is displayed, the installation is successful.**

```
Welcome to Huawei Cloud Service

[root@ecs-cloudservice ~]# set +o history; curl http://icagent-cn-east-3.obs.cn-east-3.myhuaweicloud.com/ICAgent_linux/apm_agent_install.sh > apm_agent_install.sh && REGION=cn-east-3 bash apm_agent_install.sh -ak ***** -sk ##### -region cn-east-3 -projectid 097904e68180f5662fd4c016c9548047 -accessip 100.125.11.177 -obsdomain obs.cn-east-3.myhuaweicloud.com
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          Dload  Upload   Total Spent   Left Speed
100  8465  100  8465    0      0  190k      0 --:--:-- --:--:-- --:--:-- 192k
start to install ICAgent.
begin to download install package from icagent-cn-east-3.obs.cn-east-3.myhuaweicloud.com.
#####
##### 100.0%
#####
##### 100.0%
check sha256 success, start
download success.
start install package.
start install ICAgent...
daemon
start
#####
##### 100.0%
serviceRestart
no crontab for root
starting ICAgent...
ICAgent install success.
[root@ecs-cloudservice ~]#
```

**Step 4 Return to the LTS page. On the **Host Management** page, click **Hosts**. The installed ECS is displayed in the list and the ICAgent status is **Running**.**

Note: If ICAgent has been installed and is running, but the status displayed on the HUAWEI CLOUD page is offline, there is a high probability that the AK/SK is incorrect. Obtain the AK/SK again and reinstall it.



Host Name	Host OS	Host IP Add...	Associated Host Groups	ICAgent Status	ICAgent Version...	Updated
ecs-cloudser...	linux	192.168.1.206	0	Running	5.12.145	13:51:0...

**Figure 5-40 Viewing Hosts**

**Step 5 Return to the **Host Groups** page, click **Create Host Group**, and select Create Host Group.**

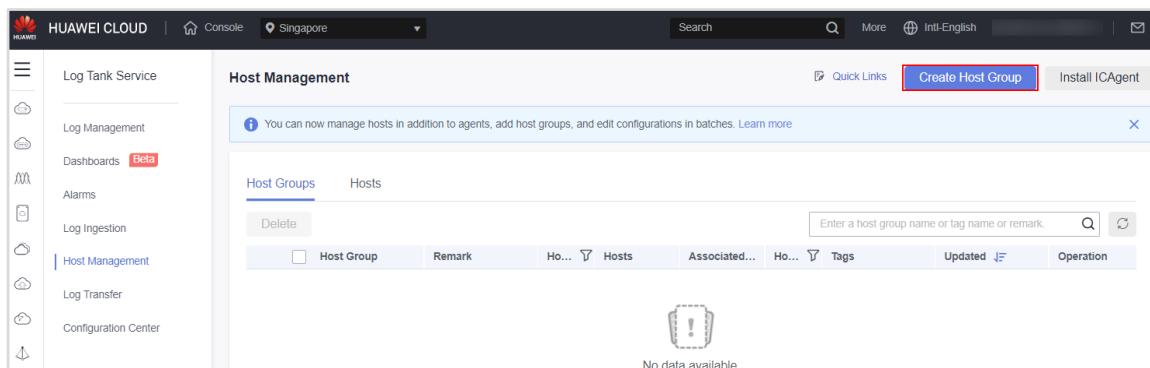
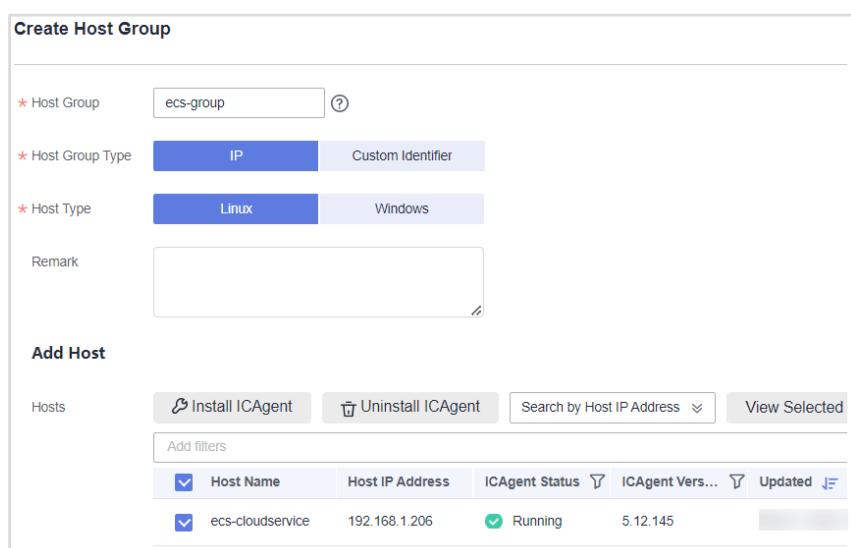


Figure 5-41 Creating a host group

Step 6 Enter the **name** of the host group, for example, ecs-group, **select the ECS** to be added, and click **OK**.



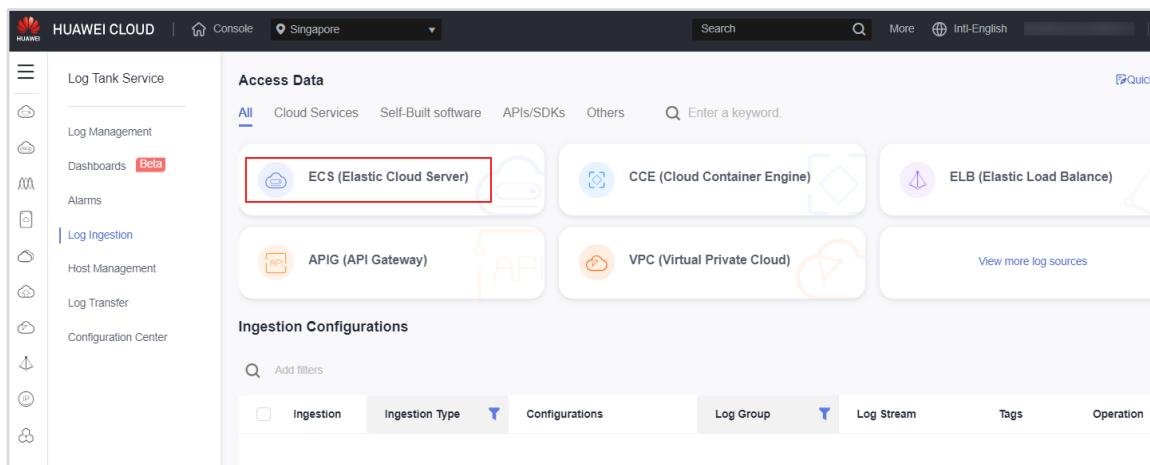
Host Name	Host IP Address	ICAgent Status	ICAgent Vers...	Updated
ecs-cloudservice	192.168.1.206	Running	5.12.145	

Figure 5-42 Adding a host

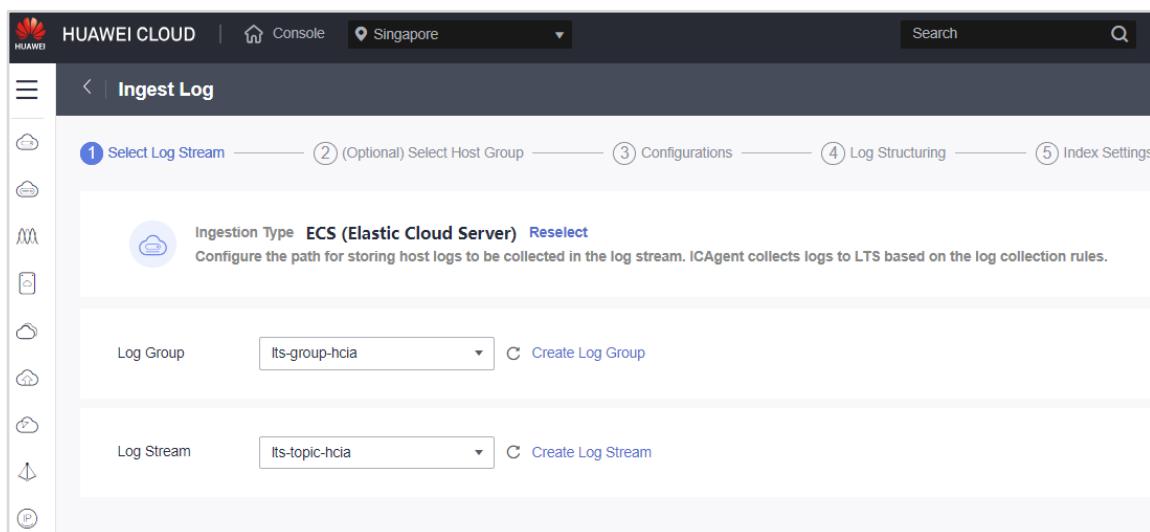
Step 7 After the adding is complete, check whether the status is normal.

#### 5.2.4.3 Configuring Log Ingestion

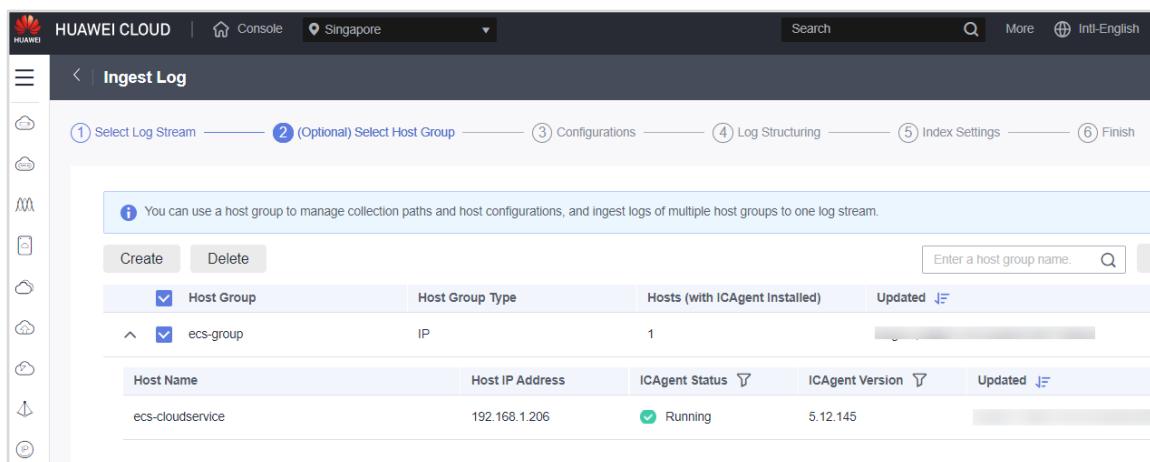
Step 1 Return to the **LTS console** and choose **Access Data > ECS** (Elastic Cloud Server) .


**Figure 5-43 Access Data**

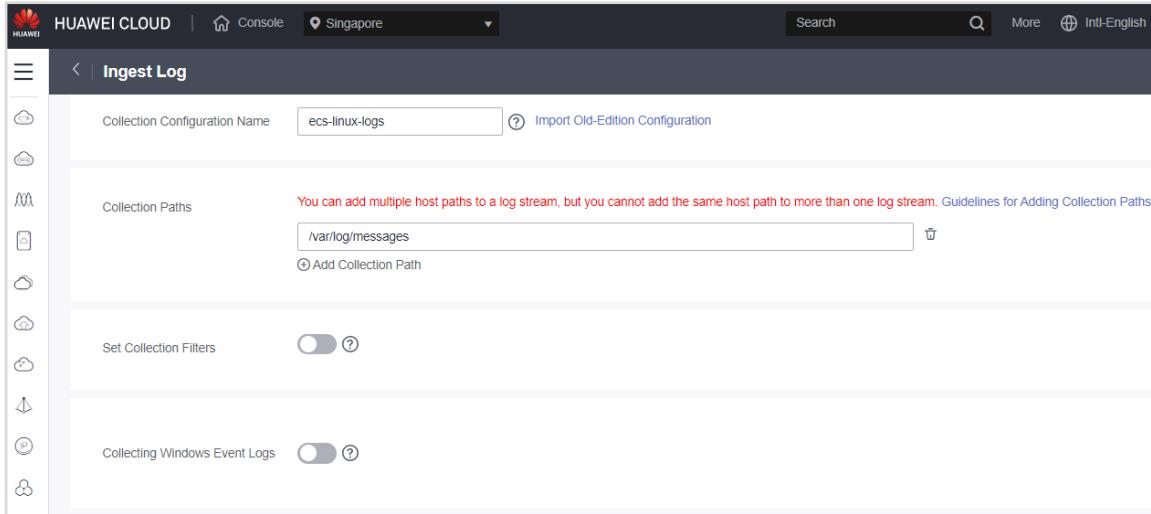
Step 2 Select the created **log group** and **log stream**, and click **Next**.


**Figure 5-44 Configuring the Log Stream**

Step 3 Select the newly created host group and click **Next**.


**Figure 5-45 Creating a host group**

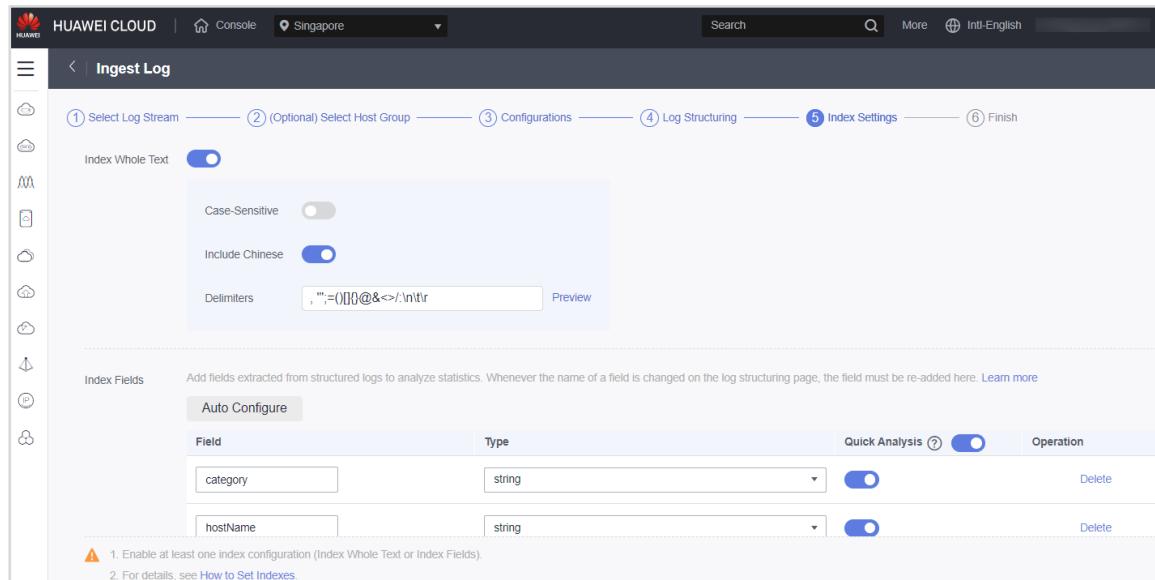
Step 4 Configure the collection information, enter a **log path** (for example, /var/log/messages) of the ECS, retain the default values for other configuration items, and click **Next**.



**Figure 5-46 Collection Configuration**

Step 5 In **Log Structuring** Configuration, retain the default settings and click **Skip**.

Step 6 On the **Index Settings** page, retain the default settings, click **Skip**, and click **Submit**.



**Figure 5-47 Index Settings**

Step 7 Choose **Log Management** and click a **log stream** name, for example, lts-topic-ia. The log stream page is displayed.

The screenshot shows the HUAWEI CLOUD Log Management interface. On the left sidebar, there are several options: Log Tank Service, Log Management (selected), Dashboards (Beta), Alarms, Log Ingestion, Host Management, Log Transfer, and Configuration Center. The main area is titled "Log Applications" and contains three cards: "ELB Log Center" (ELB layer-7 access log analysis), "APIG Log Center" (APIG access log analysis), and "VPC Flow Log Center" (VPC log analysis). Below these is a section titled "Log Groups" with a search bar and a table. The table has columns for "Log Group Name", "Remark", "Log Streams", and "Tags". One entry is visible: "Its-group-hcia" with a remark of "1". Below the table is a "Create Log Stream" button and another search bar. A table for "Log Stream Name", "Remark", and "Tags" is also present, with one entry "Its-topic-hcia" highlighted by a red box.

**Figure 5-48 Viewing logs**

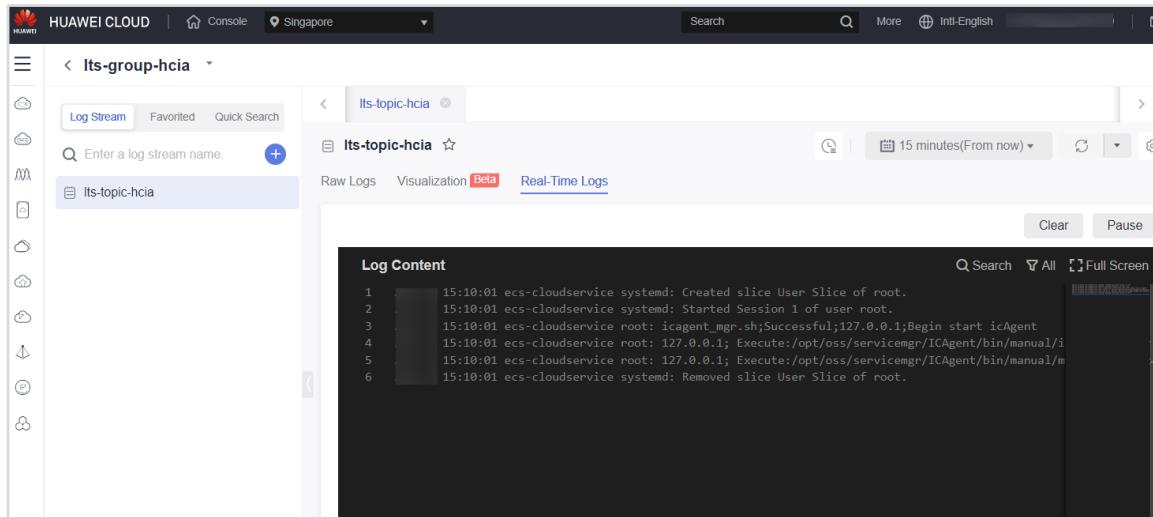
**Step 8** On the current page, wait for several minutes (you are advised to restart the ECS). You can view log information in **Raw logs** and **Real-Time Logs**.

The screenshot shows the HUAWEI CLOUD Log Management interface for the "Its-topic-hcia" log stream. The left sidebar shows "Log Stream" selected. The main area has tabs for "Raw Logs" (selected), "Visualization" (Beta), and "Real-Time Logs". The "Real-Time Logs" tab is currently active. It displays a "Quick Analysis" section with a timeline from 14:56:53 to 15:11:30, showing a total of 10,014 events. Below this is a "Content" section with a table for "Collected" and "Content". Two log entries are shown:

Collected	Content
15:10:01.542 GMT+08:00	192.168.1.206 [ecscloudservice] /var/log/messages LTS 1693465801542 content: ecs-cloudservice systemd: Removed slice Use r Slice of root.
15:10:01.542 GMT+08:00	192.168.1.206 [ecscloudservice] /var/log/messages LTS 1693465801542

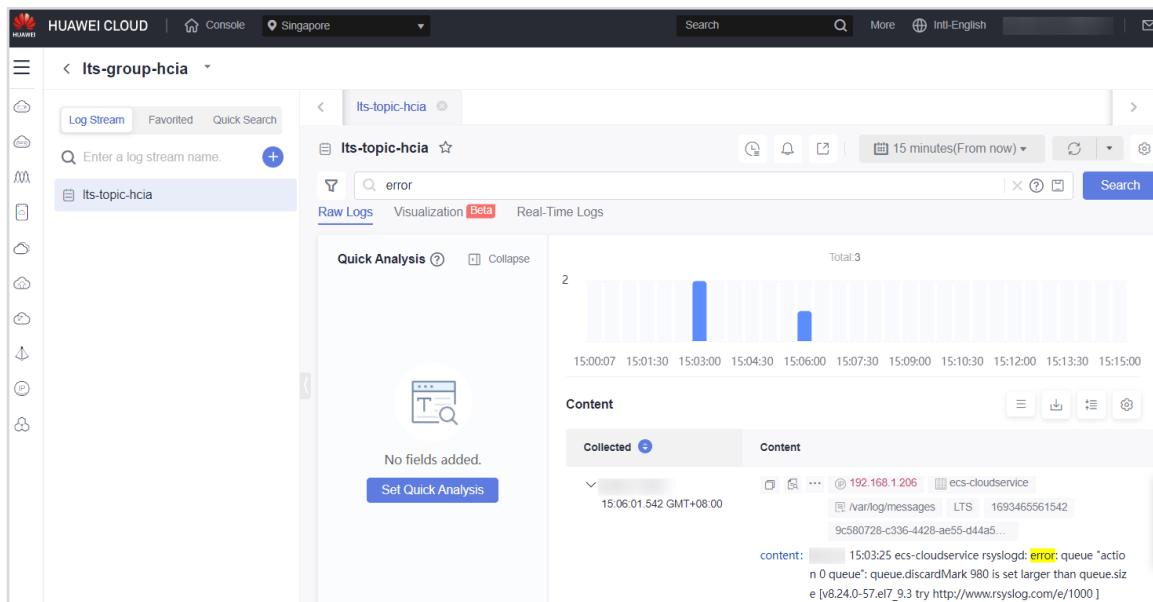
**Figure 5-49 Viewing the Raw logs**

**Step 9** Click **Real-Time Logs** to view the log information.



**Figure 5-50 Viewing real-time logs**

Step 10 On the log flow page, select **Raw Logs** and enter the keyword error to search for logs.



**Figure 5-51 Log keyword search**

The experiment on viewing ECS logs is complete.

## 5.3 Deleting Resources

Step 1 Delete resources, such as ECSSs, ECS monitoring settings, alarm rules, cloud service logs, and VPCs.

Step 2 Check that all resources in the account have been deleted.

## 5.4 Self-learning homework

Thinking Questions:

- 1、Create an ECS.
- 2、Configure the CTS function for the ECS to notify the ECS of cloud service flavor changes.
- 3、Modify ECS specifications.
- 4、View related events on CTS.

# 6

## Comprehensive Exercise: Deploying an Enterprise Website on HUAWEI CLOUD

### 6.1 Background

An enterprise intends to deploy their website on HUAWEI CLOUD and they have the following requirements:

- Database nodes and service nodes are deployed on separate ECSs.
- ECSs are added or removed as incoming traffic changes over time.
- Incoming traffic is automatically distributed across the ECSs.
- Service statuses are monitored and visualized.

### 6.2 Solution

Table 6-1 Solution configuration table

Requirement	Solution	Involved Services
Database nodes and service nodes are deployed on separate ECS instances.	Website setup: Buy ECSs as service nodes and RDS instances as database nodes. Use VPC to provide network resources for ECSs.	ECS VPC RDS
ECSs are scaled in or out as service traffic changes over time.	Feature configuration: Use AS to scale in or out ECSs created from the image of a service node as required to ensure stable, efficient services.	AS, IMS
Service traffic is automatically distributed across the ECSs.	Feature configuration: Use ELB to automatically distribute incoming traffic across the ECSs for better fault tolerance.	ELB
Service statuses are monitored and visualized.	Feature configuration: Use Cloud Eye to monitor services.	Cloud Eye

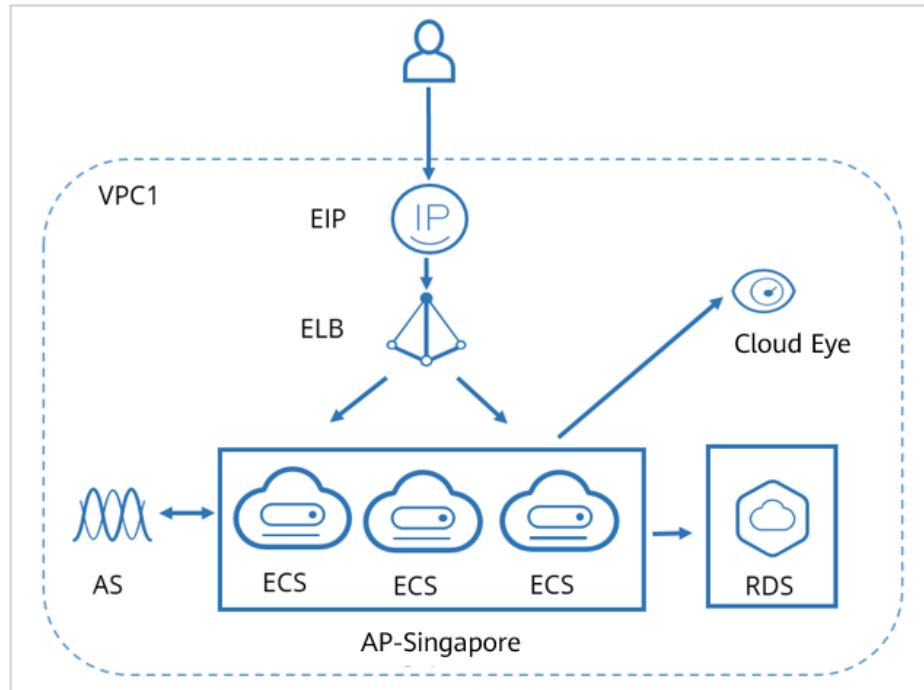


Figure 6-1 Solution topology

## 6.3 Preparations

### 6.3.1 Logging In to HUAWEI CLOUD

Step 1 Visit the [HUAWEI CLOUD official website](#) and click **Log In** in the upper right corner.

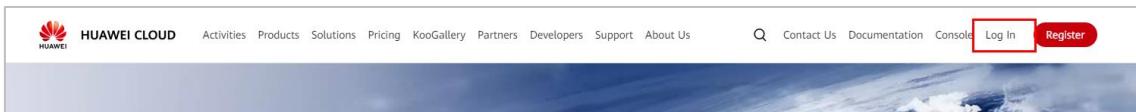
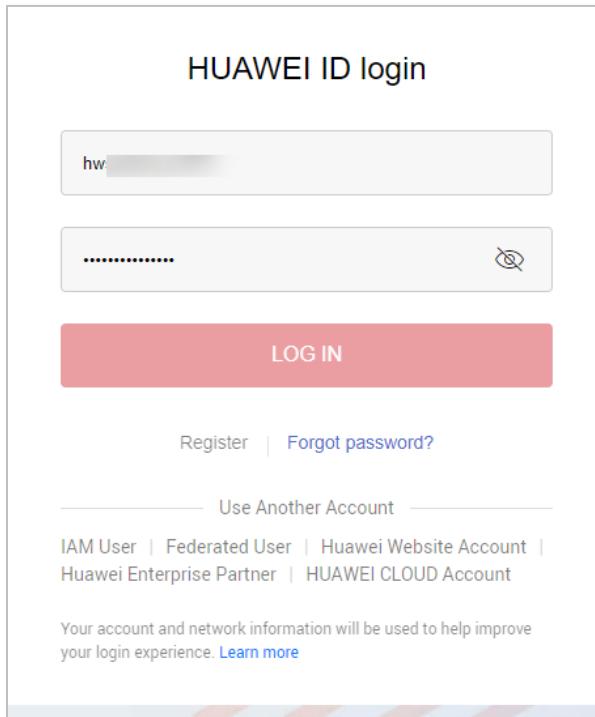


Figure 6-2 Visiting the HUAWEI CLOUD official website

Step 2 On the login page, click **HUAWEI CLOUD Account**, enter your account and password, and then click **Log In**.



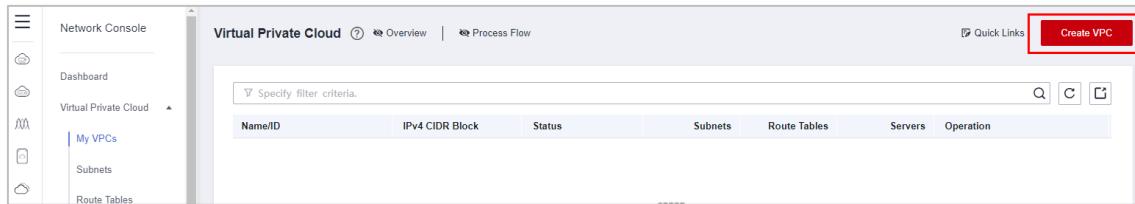
**Figure 6-3 Logging in to the HUAWEI CLOUD official website**

### 6.3.2 Creating a VPC

Step 1 Switch to the management console, and select the **AP-Singapore** region. In the left navigation pane, choose **Service List > Networking > Virtual Private Cloud**.

**Figure 6-4 Switching to the VPC console**

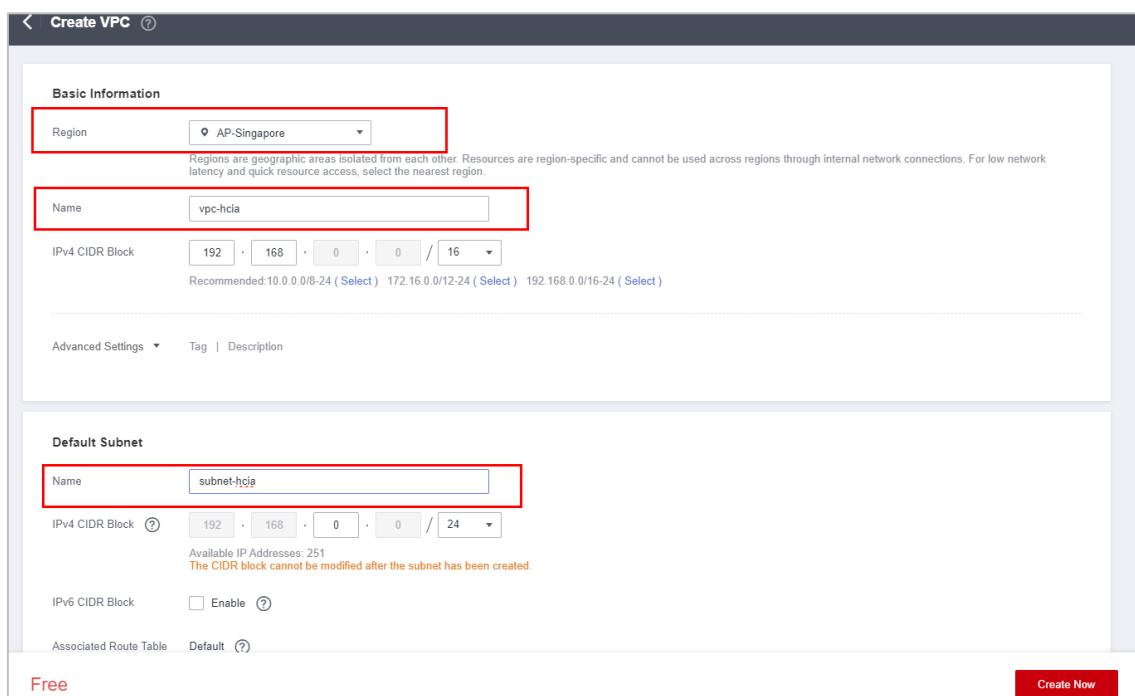
Step 2 Click Create VPC.



**Figure 6-5 Creating a VPC**

Step 3 Configure the parameters as follows, and click **Create Now**.

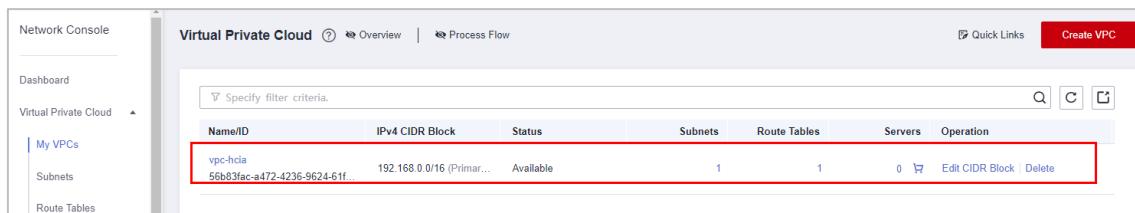
- Region: AP-Singapore
- Name: **vpc-hcia** (Change it as needed.)
- Retain the default settings for other parameters.



Basic Information	
Region	AP-Singapore
Name	vpc-hcia
IPv4 CIDR Block	192 · 168 · 0 · 0 / 16
Advanced Settings Tag   Description	
Default Subnet	
Name	subnet-hcia
IPv4 CIDR Block	192 · 168 · 0 · 0 / 24
Available IP Addresses: 251 The CIDR block cannot be modified after the subnet has been created.	
IPv6 CIDR Block	<input type="checkbox"/> Enable
Associated Route Table	Default
<b>Create Now</b>	

**Figure 6-6 Configuring the VPC**

Step 4 View the created VPC in the VPC list.

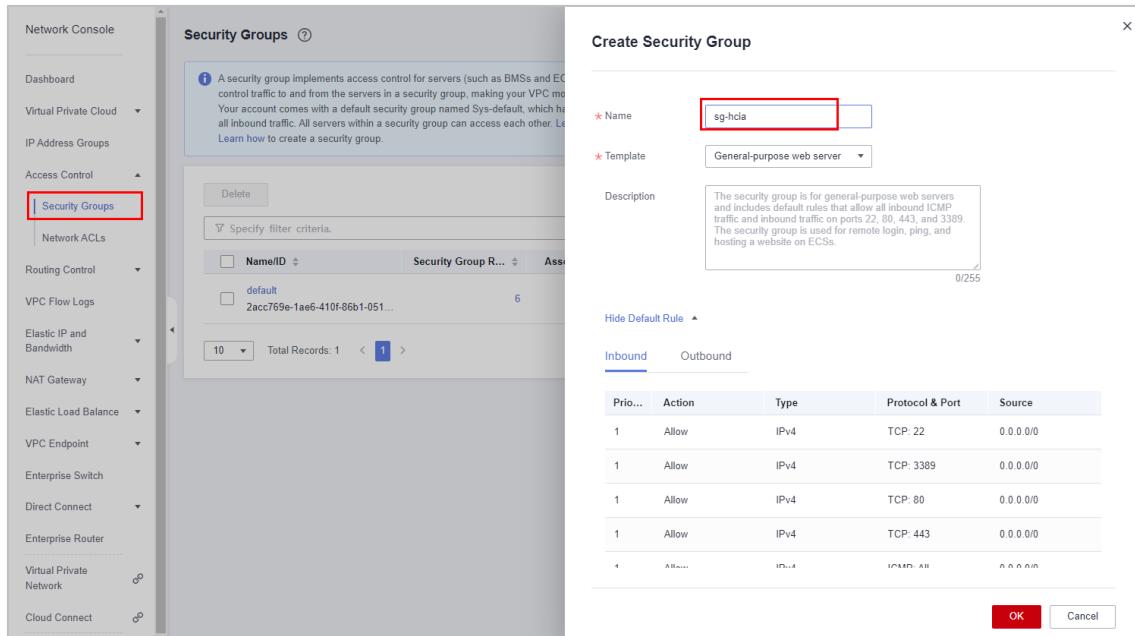


Name/ID	IPv4 CIDR Block	Status	Subnets	Route Tables	Servers	Operation
vpc-hcia 56b83fac-a472-4236-9624-61f...	192.168.0.0/16 (Primar...	Available	1	1	0	<b>Edit CIDR Block</b>   <b>Delete</b>

**Figure 6-7 Viewing the VPC**

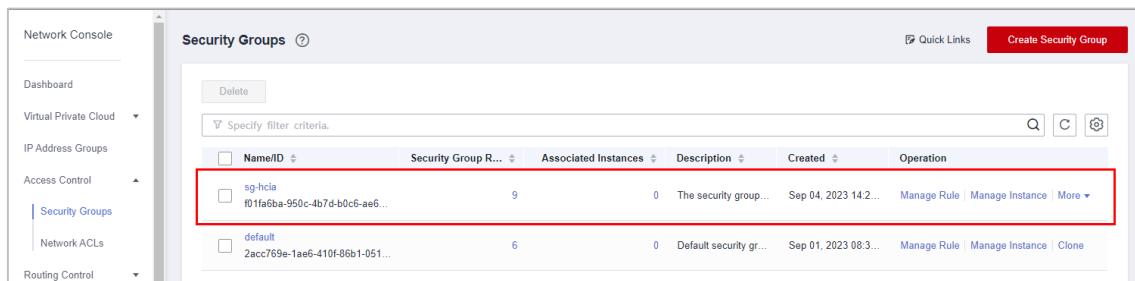
### 6.3.3 Creating and Configuring a Security Group

Step 1 On the **Network Console**, choose **Access Control > Security Groups** and create a security group.



**Figure 6-8 Creating a security group**

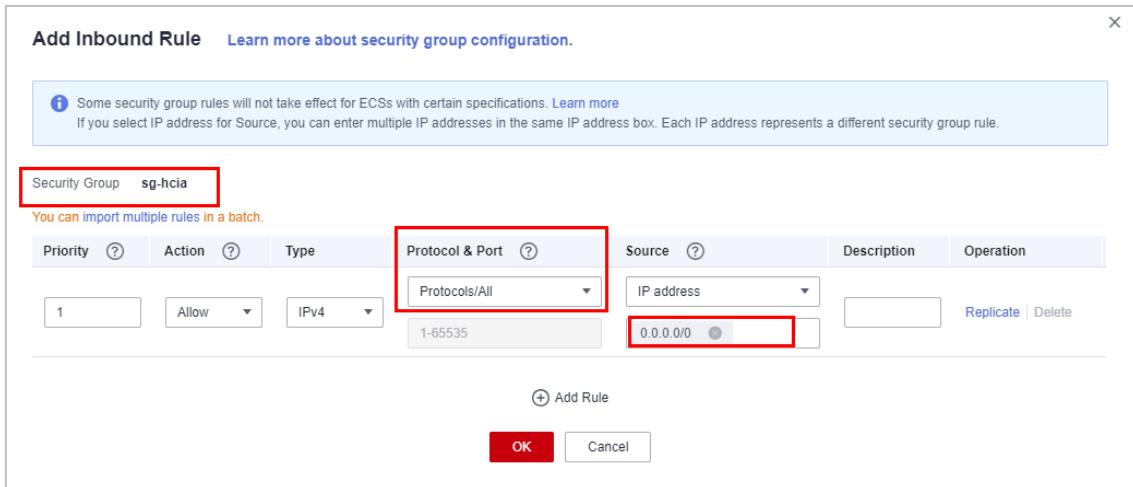
Step 2 Click the security group name.



**Figure 6-9 Viewing the security group**

Step 3 Click **Inbound Rules** and then **Add Rule** to add an inbound rule with the following parameter settings:

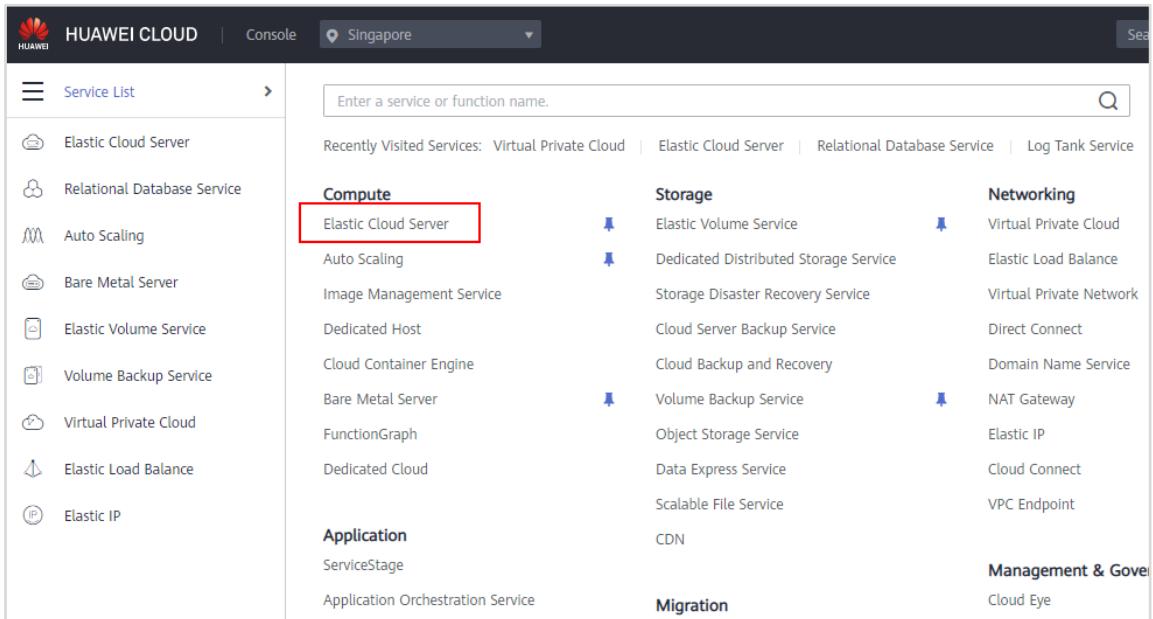
- Protocol & Port: All
- IP address in Source: 0.0.0.0/0



**Figure 6-10 Adding an inbound rule**

### 6.3.4 Buying an ECS

Step 1 In the service list, choose **Compute > Elastic Cloud Server**.



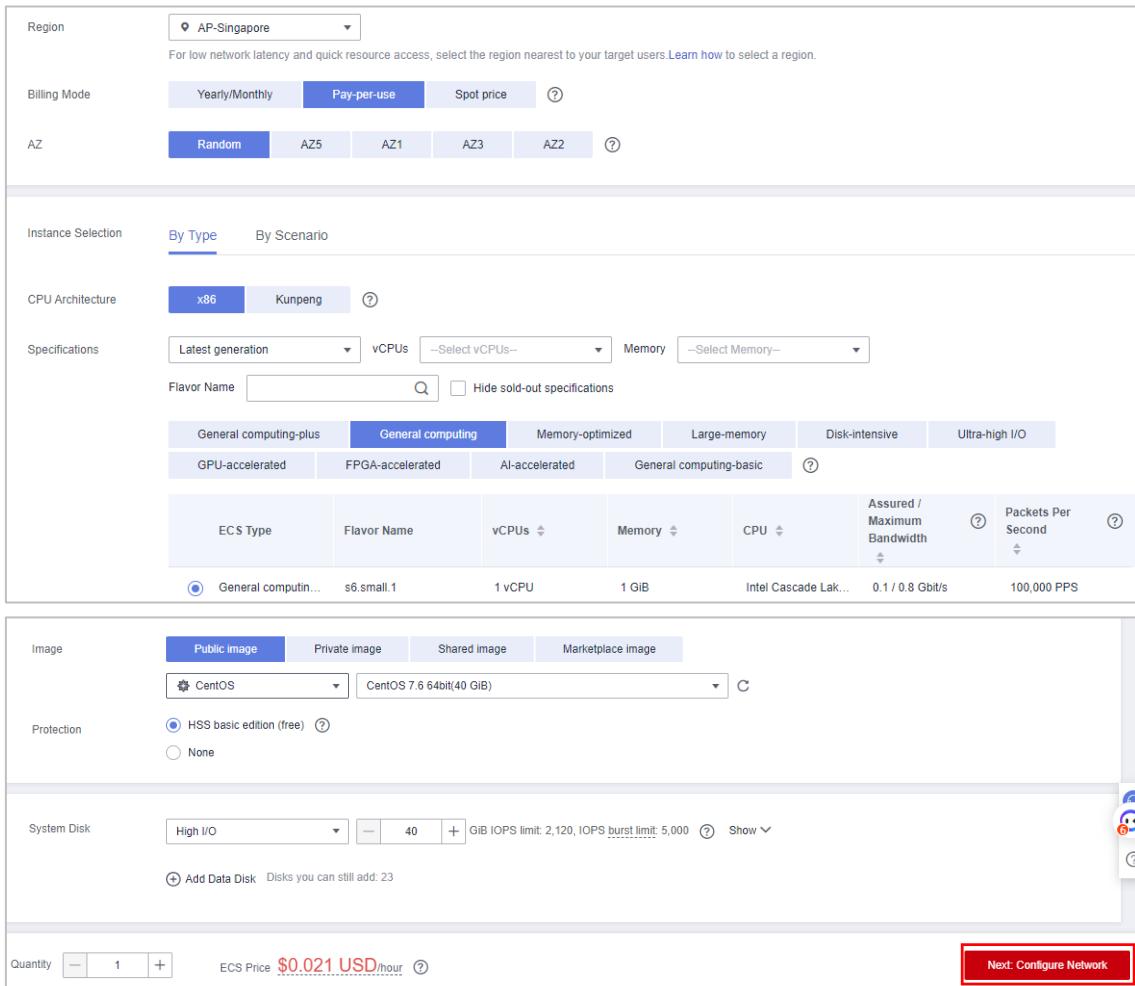
**Figure 6-11 Acessing the ECS console**

Step 2 Click **Buy ECS** and set the following parameters.

Basic settings:

- Billing Mode: Pay-per-use
- Region: AP-Singapore
- AZ: Random
- CPU Architecture: x86
- Specifications: General computing, s6.small.1 1 vCPUs | 1 GB
- Image: Public image, CentOS 7.6 64bit (40 GB)

- System Disk: High I/O, 40 GB



Region: AP-Singapore

Billing Mode: Pay-per-use

AZ: Random

Instance Selection: By Type

CPU Architecture: x86

Specifications: Latest generation, vCPUs: Select vCPUs, Memory: Select Memory

Flavor Name: General computing... (selected)

General computing-plus	General computing	Memory-optimized	Large-memory	Disk-intensive	Ultra-high I/O
GPU-accelerated	FPGA-accelerated	AI-accelerated	General computing-basic		
ECS Type	Flavor Name	vCPUs	Memory	CPU	Assured / Maximum Bandwidth
s6.small.1	1 vCPU	1 GiB	Intel Cascade Lake	0.1 / 0.8 Gbit/s	100,000 PPS

Image: Public image (CentOS 7.6 64bit(40 GiB))

Protection: HSS basic edition (free)

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

Quantity: 1

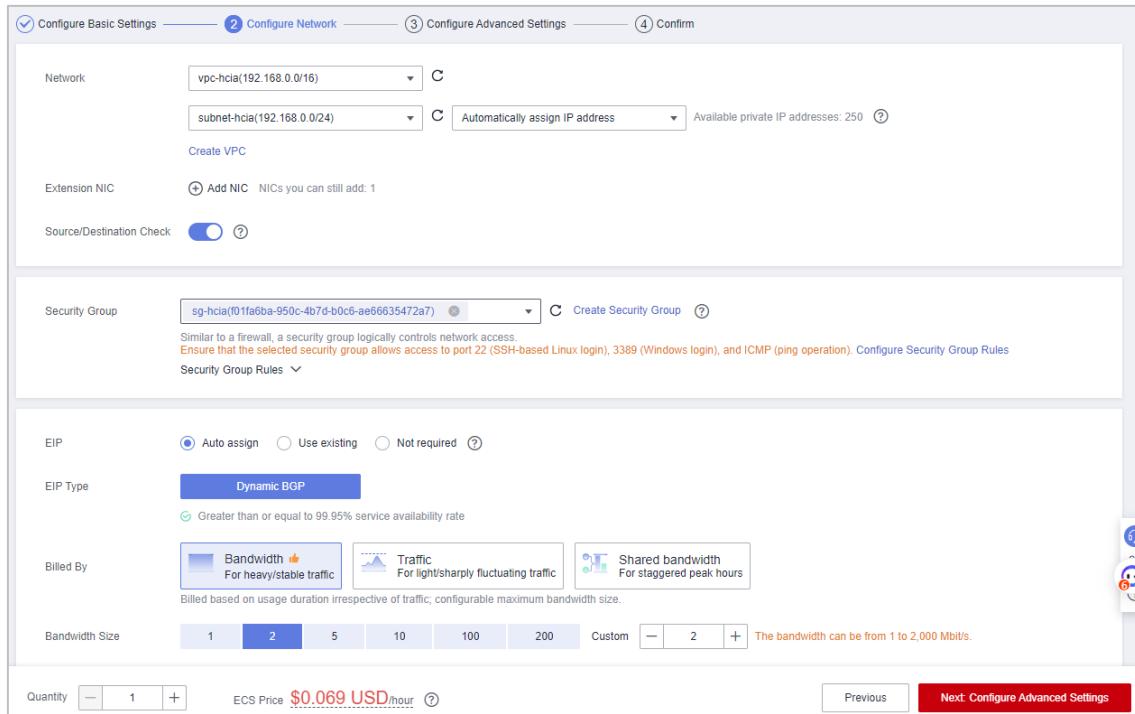
ECS Price: \$0.021 USD/hour

**Next: Configure Network**

**Figure 6-12 Configuring basic settings**

Network configuration:

- **Network:** Select the VPC you have created.
- **Security Group:** Select the security group you have created.
- **EIP:** Auto assign, Dynamic BGP, Billed by Bandwidth, 2 Mbit/s

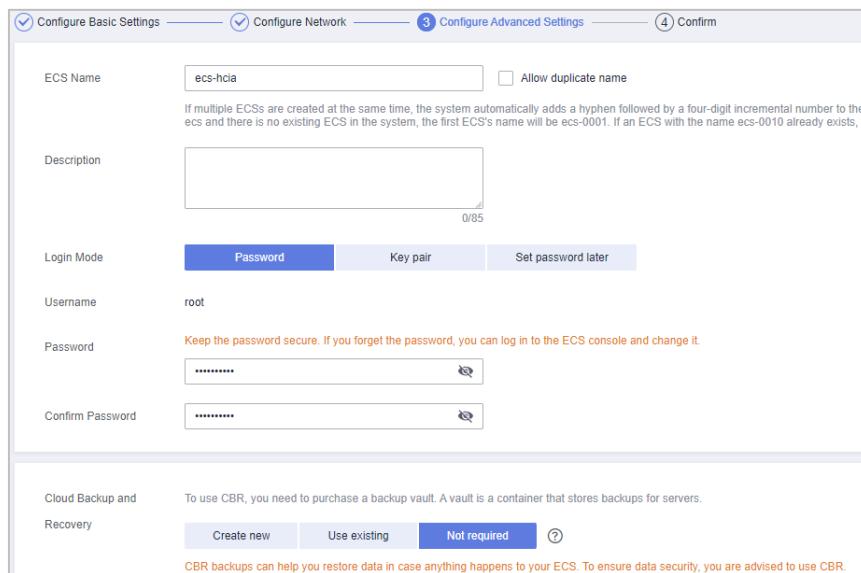


The screenshot shows the 'Configure Network' step of the cloud service setup. It includes fields for Network (vpc-hcia), Subnet (subnet-hcia), Security Group (sg-hcia), and EIP Type (Dynamic BGP). The bandwidth is set to 2 Mbit/s. The ECS price is \$0.069 USD/hour.

**Figure 6-13 Configuring network**

#### Advanced settings:

- **ECS Name:** **ecs-hcia** (Change it as needed.)
- **Login Mode:** Password, for example, **Huawei@123!**
- **Cloud Backup and Recovery:** Not required



The screenshot shows the 'Configure Advanced Settings' step. It includes fields for ECS Name (ecs-hcia), Description, Login Mode (Password selected), Username (root), and Password. It also includes options for Cloud Backup and Recovery (Create new, Use existing, Not required).

**Figure 6-14 Configuring advanced settings**

Step 3 Confirm the configuration, select I have read and agree to the Service Level Agreement and Image Disclaimer, and click Buy Now.

**Figure 6-15 Confirmation**

Step 4 View the purchased ECS in the ECS list.

Name/ID	Monitor...	Security	AZ	Status	Specifications/Im...	IP Address	Billing Mod	Operation
ecs-hcia 55bf6bbf7-f7ad-4971-8806-def...			AZ5	Running	1 vCPU   1 GiB   s... CentOS 7.6 64bit	190.92.207.15... 192.168.0.47 (...)	Pay-per-use Create	<a href="#">Remote Login</a>   <a href="#">More</a>

**Figure 6-16 Viewing the ECS in the list**

Step 5 An EIP has been bound to the ECS. To enhance ECS login security, you are advised to set the ECS login mode to key pair. For details, see [Access to the Internet with an EIP](#).

### 6.3.5 Buying an RDS DB Instance

Step 1 Go back to the service list, and choose **Database > Relational Database Service**.

**Figure 6-17 Acessing the RDS console**

Step 2 Click Buy DB Instance.

**Figure 6-18 Buying a DB instance**

Step 3 Set the parameters as follows and click Next.

- Billing Mode: Pay-per-use
- Region: AP-Singapore
- Instance parameters: **rds-name** (customizable), **MySQL, 8.0, Primary/Standby, Cloud SSD**
- Performance specifications: **Dedicated, 2 vCPUs | 4 GB**. Determine the specifications based on real-world service requirements.
- **VPC, Security Group, and Password**: Select the VPC and security group you have created. Set the password, for example, **Huawei!@#\$**.
- Retain the default settings for other parameters.

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

Region: AP-Singapore

Project: AP-Singapore

DB Instance Name: rds-hcia

DB Engine: MySQL, PostgreSQL

DB Engine Version: 8.0, 5.7, 5.6

DB Instance Type: Primary/Standby, Single

Storage Type: Cloud SSD, Extreme SSD

Primary AZ: AZ2, AZ1, AZ5, AZ3

Standby AZ: AZ2, AZ1, AZ5, AZ3

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Macau, Sanya

Instance Class: Dedicated, General-purpose

vCPUs   Memory	Recommended Connections	TPS   QPS	IPv6
2 vCPUs   4 GB	1,500	580   11,597	Not supported

**Figure 6-19 Configuring a DB instance**

Storage Space: 40 GB

Disk Encryption: Disable, Recommended, Enable

VPC: vpc-hcia, subnet-hcia(192.168.0.0/24), View In-use IP Addresses

Database Port: Default port: 3306

Security Group: sg-hcia

**Figure 6-20 Configuring a DB instance**

Buy DB Instance		
Resource	Configuration	Billing Mode
RDS	Billing Mode Pay-per-use Region AP-Singapore DB Instance Name rds-hcia DB Engine MySQL DB Engine Version 8.0 DB Instance Type Primary/Standby Primary AZ AZ2 Standby AZ AZ1 Instance Specifications rds.mysql.x1.large.2.ha   2 vCPUs   4 GB(Dedicated), Recommended Connections: 1,500, TPS: 580   QPS: 11,597	
	Disk Encryption Disabled Storage Type Cloud SSD Storage Space 40 GB Time Zone UTC+08:00 VPC vpc-hcia Subnet subnet-hcia(192.168.0.0/24) Floating IP Address Automatically assigned Security Group sg-hcia Database Port Default port: 3306 Parameter Template Default-MySQL-8.0 Table Name Case insensitive	Pay-per-use

**Figure 6-21 Confirmation**

Step 4 Confirm the configuration, and click **Submit**. Go to the RDS DB instance list, and wait for the creation to complete, which takes 6 to 10 minutes.

Name/ID	Description	DB Instanc...	DB Engine Version...	Status	Billing Mo...	Floating I...	Storage T...	Operation
rds-hcia 5617e92a3b7b4c96b9512c9...	--	Primary/Standby 2 vCPUs   ...	MySQL 8.0.25	Available	Pay-per-use	--	Cloud SSD	<a href="#">View Metrics</a>   <a href="#">Log In</a>   <a href="#">More</a>
10 Total Records: 1 < 1 >								

**Figure 6-22 Viewing the DB instance**

Step 5 Click the DB instance name to view its floating IP address.

DB Information		Connectivity & Security	
DB Instance Name	rds-hcia	DB Instance ID	5617e92a3b7b4c96b9512c9bfd1129efin01
Description	--	DB Engine Version	MySQL 8.0.25 Upgrade Minor Version
Maintenance Window	02:00 – 06:00 (GMT+08:00)	DB Instance Type	Primary/Standby Switch
Instance Class	rds.mysql.x1.large.2.ha   2 vCPUs   4 GB (Dedicated)	Replication Mode	Semi-synchronous Change
SSL	International	Administrator	root Reset Password
Failover Priority	Reliability Change	Event Scheduler	Off
AZ	AZ2 (Primary AZ), AZ1 (Standby AZ)	ReadWrite Permissions	ReadWrite Change
Connection Information		Storage Space	
Floating IP Address	192.168.0.188	Scale Storage Space	Configure Autoscaling
Database Port	3306	Cloud SSD	Not encrypted
Recommended Max. Connections	1,500	Used/Allocated	2.37/40 GB 5.93%
ReadWrite Splitting Address	Apply	Backup Space	
Other Information			

**Figure 6-23 Viewing the floating IP address of the DB instance**

## 6.4 Setting Up the Linux, Apache, MySQL, PHP (LAMP) Environment

### 6.4.1 Installing LAMP

Step 1 Go back to the ECS console and click **Remote Login** in the **Operation** column of the purchased ECS.

Name/ID	Monitor...	Security	AZ	Status	Specificatio...	IP Address	Billing M...	Tag	Operation
ecs-hcia 55bf6bf7-17ad-4971-8...			AZ5	Running	1 vCPU   1 Gi... CentOS 7.6 ...	190.92.2... 192.168....	Pay-per-us... Created on ...	--	<a href="#">Remote Login</a> <a href="#">More</a>

**Figure 6-24 Remotely logging in to the ECS**

Step 2 In the **VNC** window, enter the username (**root** for Linux ECSs by default) and password for login.

```
Welcome to Huawei Cloud Service  
[root@ecs-hcia ~]#
```

Step 3 Run the following command to install LAMP and enable the services you will need:

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

If **Complete!** is displayed, LAMP has been successfully installed.

```
Installed:  
httpd.x86_64 0:2.4.6-99.el7.centos.1          mariadb.x86_64 1:5.5.68-1.el7          php.x86_64  
0:7.4.33-7.el7.remi      php-fpm.x86_64 0:7.4.33-7.el7.remi      php-mysqld.x86_64 0:7.4.33-  
7.el7.remi  
  
Dependency Installed:  
apr.x86_64 0:1.4.8-7.el7          apr-util.x86_64 0:1.5.2-6.el7_9.1          httpd-tools.x86_64  
0:2.4.6-99.el7.centos.1      libsodium.x86_64 0:1.0.18-1.el7          mailcap.noarch 0:2.1.41-2.el7  
php-cli.x86_64 0:7.4.33-7.el7.remi      php-common.x86_64 0:7.4.33-7.el7.remi      php-json.x86_64  
0:7.4.33-7.el7.remi      php-pdo.x86_64 0:7.4.33-7.el7.remi      php-sodium.x86_64 0:7.4.33-  
7.el7.remi  
  
Complete!
```

Step 4 Configure httpd:

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

Step 5 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 content" ServerName localhost:80":

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

Step 6 Press **Esc** to exit the editing mode, enter **:wq**, and press **Enter** to save and exit the configuration file.

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

Step 7 Run the following command to download the WordPress installation package, If **wordpress-4.9.10.tar.gz** is displayed, the WordPress installation package has been downloaded.

```
[root@ecs-hcia ~]# wget -c https://wordpress.org/wordpress-4.9.10.tar.gz
-- 20:48:41--  https://wordpress.org/wordpress-4.9.10.tar.gz
Resolving wordpress.org (wordpress.org)... 198.143.164.253
Connecting to wordpress.org (wordpress.org)|198.143.164.253|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8744264 (8.3M) [application/octet-stream]
Saving to: ‘wordpress-4.9.10.tar.gz’

100%[=====>] 8,744,264  0.83MB/s  in 12.5s

20:48:50 (0.85 MB/s) - ‘wordpress-4.9.10.tar.gz’ saved [8744264/8744264]
```

Step 8 Run the following command to decompress the WordPress installation package to the **/var/www/html** directory, The command output similar to the following is displayed.

```
[root@ecs-hcia ~]# tar -zxf wordpress-4.9.10.tar.gz -C /var/www/html
...
wordpress/wp-includes/deprecated.php
wordpress/wp-includes/class-wp-http-cookie.php
wordpress/wp-includes/feed-rss2-comments.php
wordpress/wp-includes/class-wp-oembed-controller.php
wordpress/wp-includes/class-walker-comment.php
wordpress/wp-includes/class-feed.php
wordpress/wp-includes/class-wp-list-util.php
...
```

Step 9 Run the following command to grant the read and write permissions to the directory where the file is located:

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

Step 10 Run the following command to enable httpd:

```
[root@ecs-hcia ~]# systemctl start httpd.service
```

Step 11 Run the following command to enable php-fpm:

```
[root@ecs-hcia ~]# systemctl start php-fpm.service
```

Step 12 Run the following command to check the httpd status, which should be **active (running)** and highlighted:

```
[root@ecs-hcia ~]# 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 Sat 20:49:38 CST; 1min 6s ago
    Docs: man:httpd(8)
          man:apachectl(8)
  Main PID: 18708 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"
  CGroup: /system.slice/httpd.service
          └─18708 /usr/sbin/httpd -DFOREGROUND
              ├─18709 /usr/sbin/httpd -DFOREGROUND
              ├─18710 /usr/sbin/httpd -DFOREGROUND
              ├─18711 /usr/sbin/httpd -DFOREGROUND
              ├─18712 /usr/sbin/httpd -DFOREGROUND
              └─18713 /usr/sbin/httpd -DFOREGROUND
20:49:38 ecs-mp systemd[1]: Starting The Apache HTTP Server...
20:49:38 ecs-mp systemd[1]: Started The Apache HTTP Server.
```

Step 13 Run the following command to check the php-fpm status, which should be **active (running)** and highlighted:

```
[root@ecs-hcia ~]# 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 Sat 20:49:48 CST; 1min 55s ago
  Main PID: 18720 (php-fpm)
    Status: "Processes active: 0, idle: 5, Requests: 0, slow: 0, Traffic: 0req/sec"
  CGroup: /system.slice/php-fpm.service
          ├─18720 php-fpm: master process (/etc/php-fpm.conf)
          ├─18721 php-fpm: pool www
          ├─18722 php-fpm: pool www
          ├─18723 php-fpm: pool www
          ├─18724 php-fpm: pool www
          └─18725 php-fpm: pool www
```

```
20:49:48 ecs-mp systemd[1]: Starting The PHP FastCGI Process Manager...
20:49:48 ecs-mp systemd[1]: Started The PHP FastCGI Process Manager
```

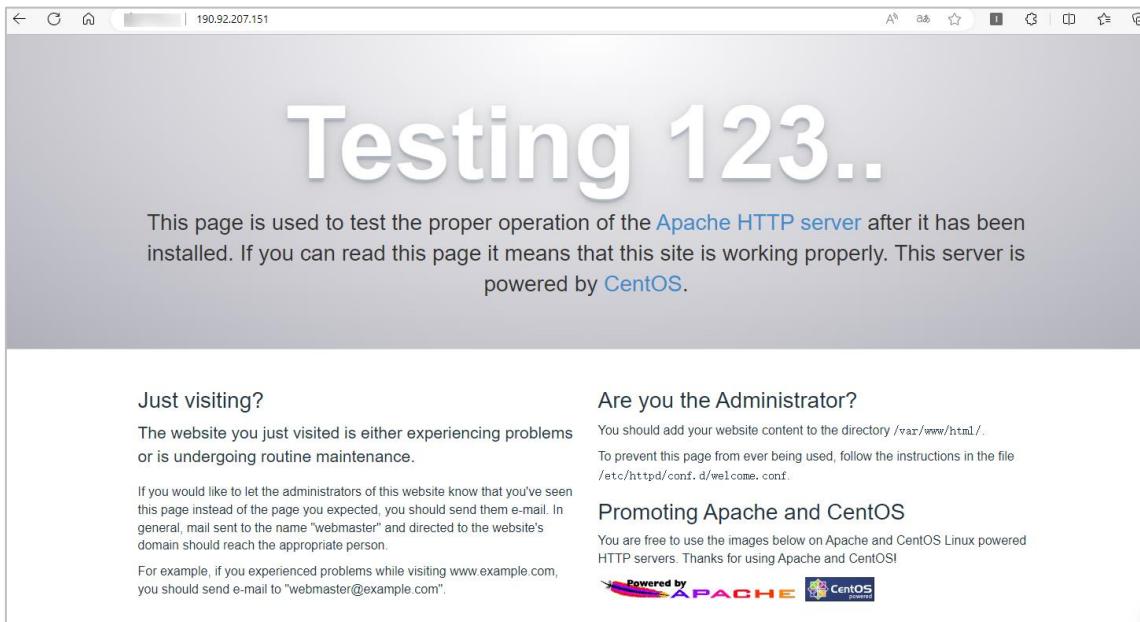
- Step 14 Run the following command to make httpd automatically start at boot. If information similar to what shown in the figure is displayed, httpd has been configured to automatically start at boot.

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

- Step 15 Run the following command to configure php-fpm automatically start upon system boot. If information similar to what shown in the figure is displayed, php-fpm has been configured to automatically start upon system boot.

```
[root@ecs-hcia ~]# 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.
```

- Step 16 In the browser, access the EIP bound to the ECS. If the following figure is displayed, LAMP has been installed.



**Figure 6-25 Checking environment installation**

#### 6.4.2 Creating a Database for WordPress

- Step 1 Go back to the RDS console and click **Log In** in the **Operation** column of the created RDS MySQL database instance.

Name/ID	Description	DB Instance Type	DB Engine Version	Status	Billing Model	Floating IP	Storage Type	Operation
rds-hcia	Primary/Standby	MySQL 8.0.25	Available	Pay-per-Use	192.16...	Cloud SSD	<a href="#">View Metrics</a>	<a href="#">Log In</a>

Figure 6-26 Logging in to the DB instance

Step 2 Enter the username (**root** by default) and password (you set when purchasing the RDS instance). Select **Remember Password**, enable **Collect Metadata Periodically** and **Show Executed SQL Statements**. If the connection test is successful, click **Log In**.

### Instance Login Information

DB Instance Name	rds-hcia	DB Engine Version	MySQL 8.0
* Login Username	<input type="text" value="root"/>		
* Password	<input type="password" value="*****"/> <span style="border: 2px solid red; padding: 2px;">Test Connection</span> <span style="color: green;">Connection is successful.</span>		
<input checked="" type="checkbox"/> Remember Password Your password will be encrypted and stored securely.			
Description	<input type="text" value="created by sync rds instance"/>		
Collect Metadata Periodically	<input type="radio"/> 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	<input type="radio"/> If not enabled, the executed SQL statements cannot be viewed, and you need to input each SQL statement manually.		
<span style="border: 2px solid red; padding: 5px 10px;">Log In</span> <span style="border: 1px solid #ccc; padding: 5px 10px;">Cancel</span>			

Figure 6-27 Instance Login information

Step 3 On the Home page, click **Create Database**.

Home

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

<a href="#">+ Create Database</a>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <input type="text" value="User database"/> <span style="font-size: small;">Enter a database name.</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">C Refresh</span> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Database Name</td> <td style="width: 20%;">Table Quantity</td> <td style="width: 20%;">Table Size</td> <td style="width: 20%;">Index Size</td> <td style="width: 10%;">Character Set</td> <td style="width: 10%;">Operation</td> </tr> <tr> <td><input type="text" value=""/></td> <td><input type="button" value=""/></td> </tr> </table>	Database Name	Table Quantity	Table Size	Index Size	Character Set	Operation	<input type="text" value=""/>	<input type="button" value=""/>				
Database Name	Table Quantity	Table Size	Index Size	Character Set	Operation								
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="button" value=""/>								

Figure 6-28 Creating a database

Step 4 Create a WordPress database, as shown in the following figure.

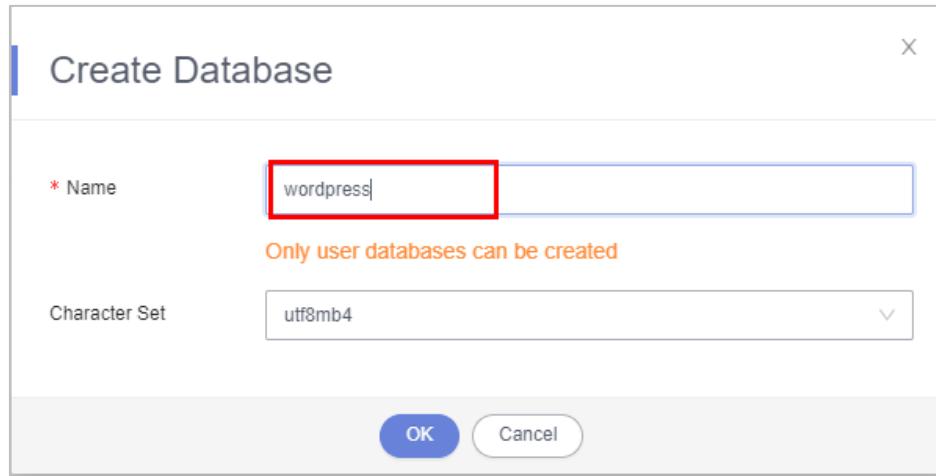


Figure 6-29 Creating a database

### 6.4.3 Installing WordPress

Step 1 In the address box of the browser, enter [http://ECS\\_EIP/wordpress](http://ECS_EIP/wordpress) to access the WordPress installation wizard.

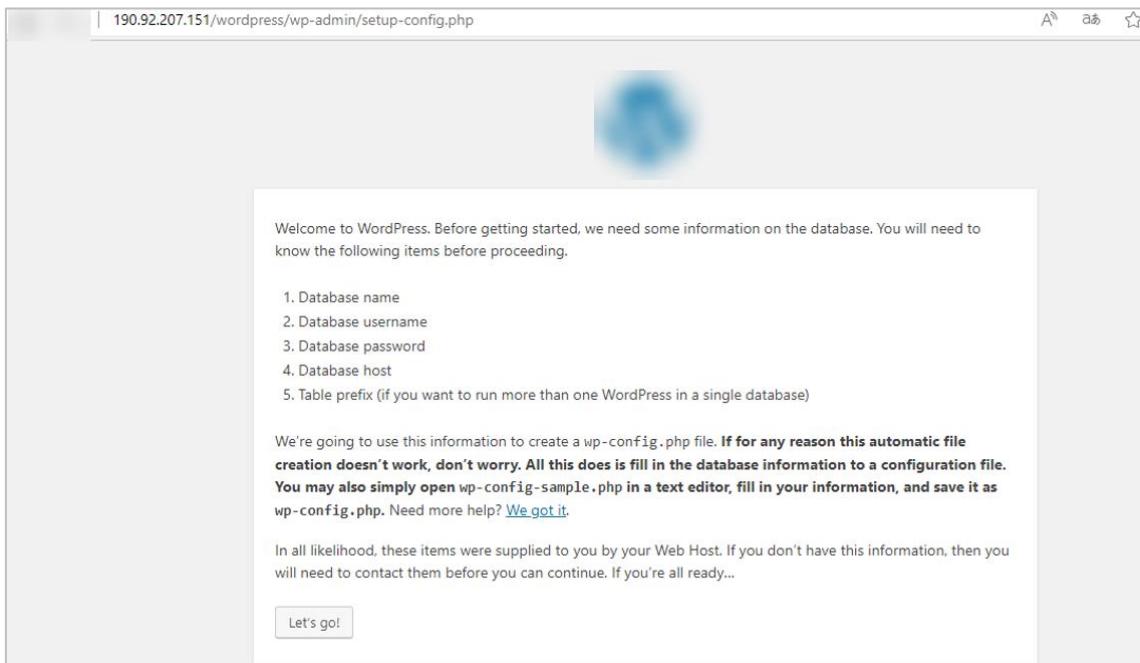
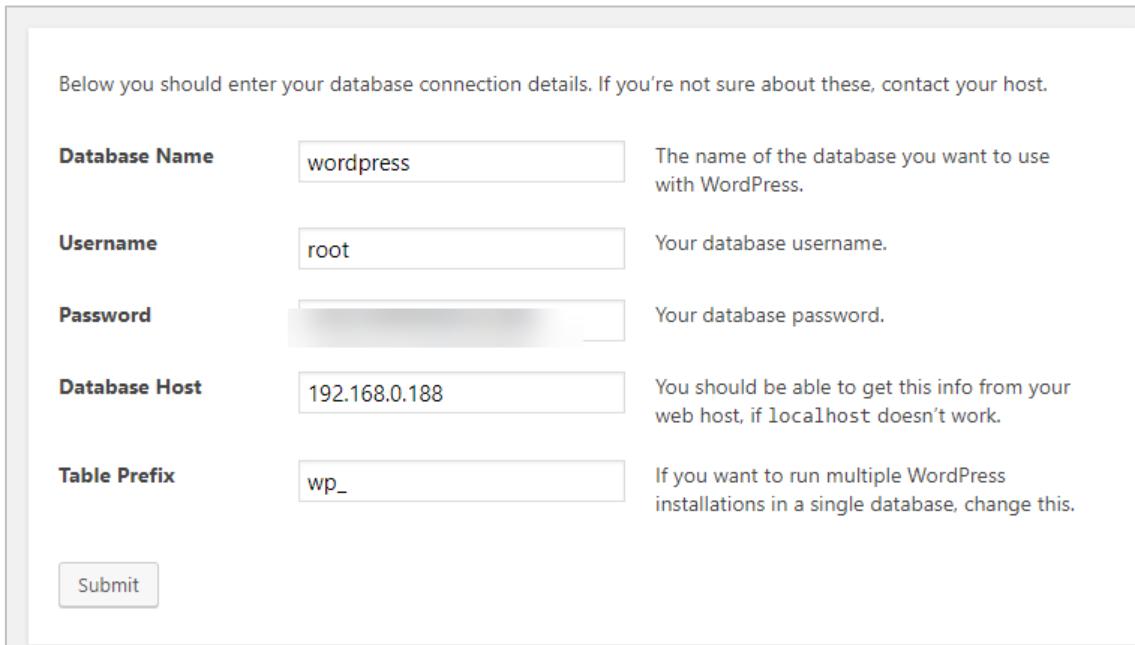


Figure 6-30 Opening the WordPress installation wizard

Step 2 Click **Let's go!**. in the displayed page, enter the database access information, and click **Submit**.

- Database Name: wordpress
- Username: root
- Password: Enter the password you set.
- Database Host: Enter the database floating IP address and port number obtained in step 4 of section [Buying an RDS DB Instance](#).

- **Table Prefix:** Retain the default settings.



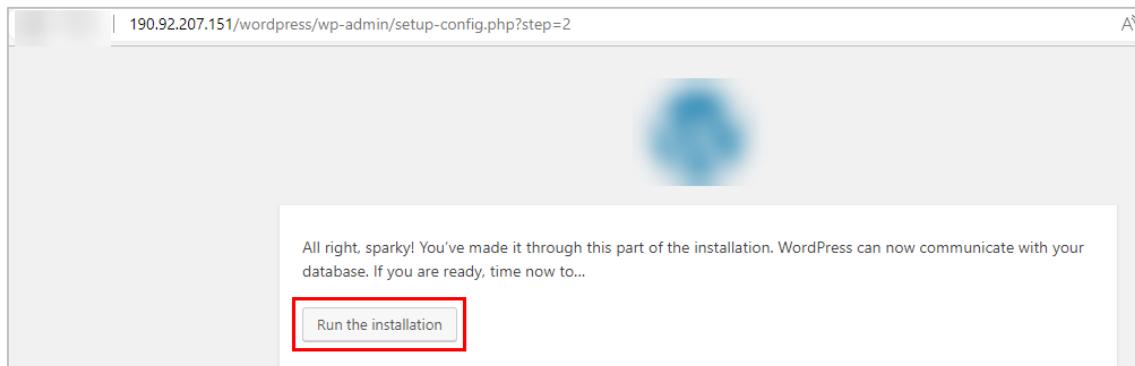
Below you should enter your database connection details. If you're not sure about these, contact your host.

<b>Database Name</b>	<input type="text" value="wordpress"/>	The name of the database you want to use with WordPress.
<b>Username</b>	<input type="text" value="root"/>	Your database username.
<b>Password</b>	<input type="password"/>	Your database password.
<b>Database Host</b>	<input type="text" value="192.168.0.188"/>	You should be able to get this info from your web host, if localhost doesn't work.
<b>Table Prefix</b>	<input type="text" value="wp_"/>	If you want to run multiple WordPress installations in a single database, change this.

**Submit**

**Figure 6-31 Configuring the connection between WordPress and the database**

- Click Run the installation.



**Figure 6-32 Run the installation**

- Set Site Title, Username, Password, and Your Email, and click Install WordPress.

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.

<b>Site Title</b>	<input type="text" value="HCIA-LAB"/>
<b>Username</b>	<input type="text" value="admin"/>
Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.	
<b>Password</b>	<input type="password" value="*****"/> <input type="button" value="Show"/>
Strong	
Important: You will need this password to log in. Please store it in a secure location.	
<b>Your Email</b>	<input type="text"/>
Double-check your email address before continuing.	
<b>Search Engine Visibility</b>	<input type="checkbox"/> Discourage search engines from indexing this site It is up to search engines to honor this request.
<input type="button" value="Install WordPress"/>	

**Figure 6-33 Install WordPress**

Success!

WordPress has been installed. Thank you, and enjoy!

<b>Username</b>	admin
<b>Password</b>	<i>Your chosen password.</i>
<input type="button" value="Log In"/>	

**Figure 6-34 Installation succeeded**

Step 3 Enter the user name and password on the displayed login page. Then, click **Log In**.

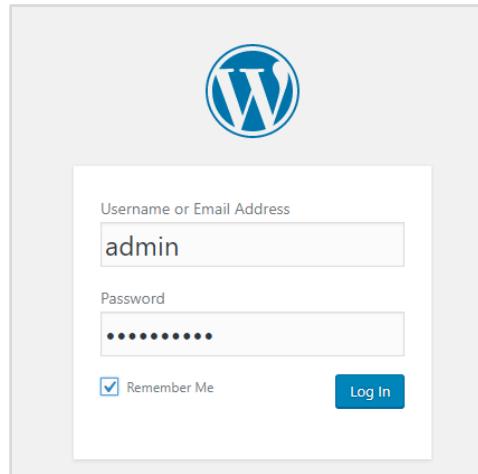


Figure 6-35 Logging in

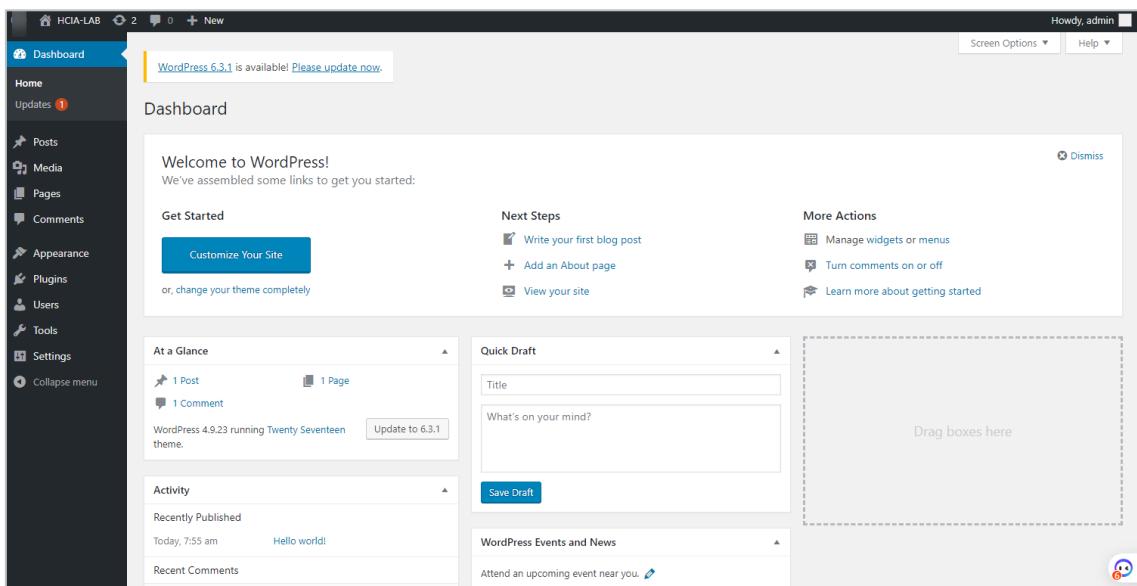
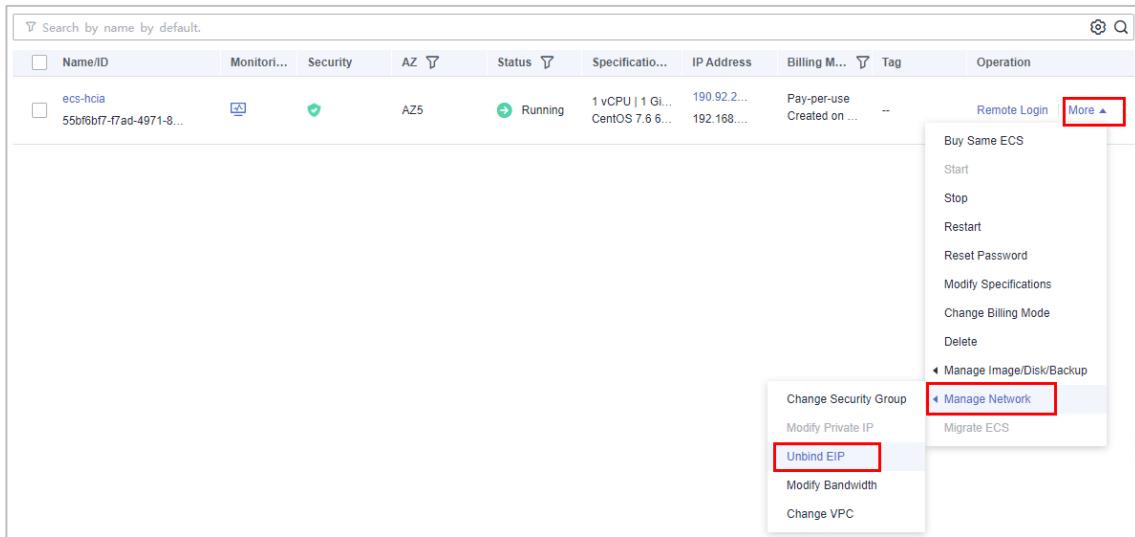


Figure 6-36 Login succeeded

Step 4 The initial configuration of the WordPress website server and backend database instance is complete. Return to the ECS console and unbind the EIP from the ECS where WordPress is installed.



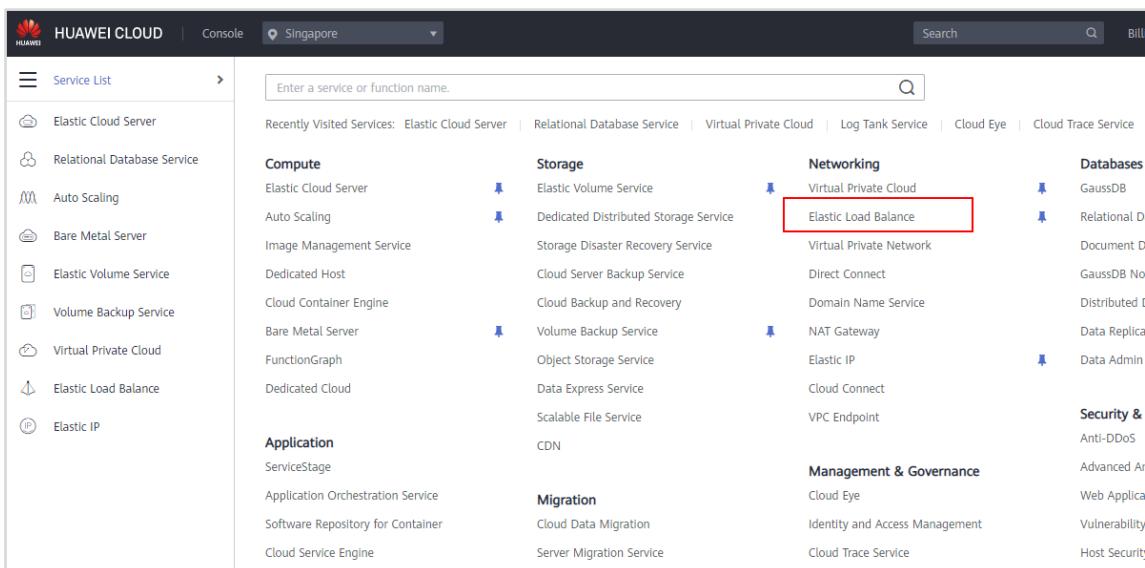
Now the initial configurations of the WordPress website server and its back-end database instance are complete. Next, we will configure ELB and AS for the WordPress website server.

## 6.5 Achieving High Availability for Web Servers

To ensure high availability, enterprises usually deploy their applications on more than one server, use ELB to distribute incoming traffic across these servers, and use AS to scale in or out servers on demand. In this exercise, we will use the website you built in the preceding exercise as an example to describe how you can configure ELB to distribute incoming traffic across the web servers, and we will use AS to improve the availability of the website.

### 6.5.1 Creating a Shared Load Balancer

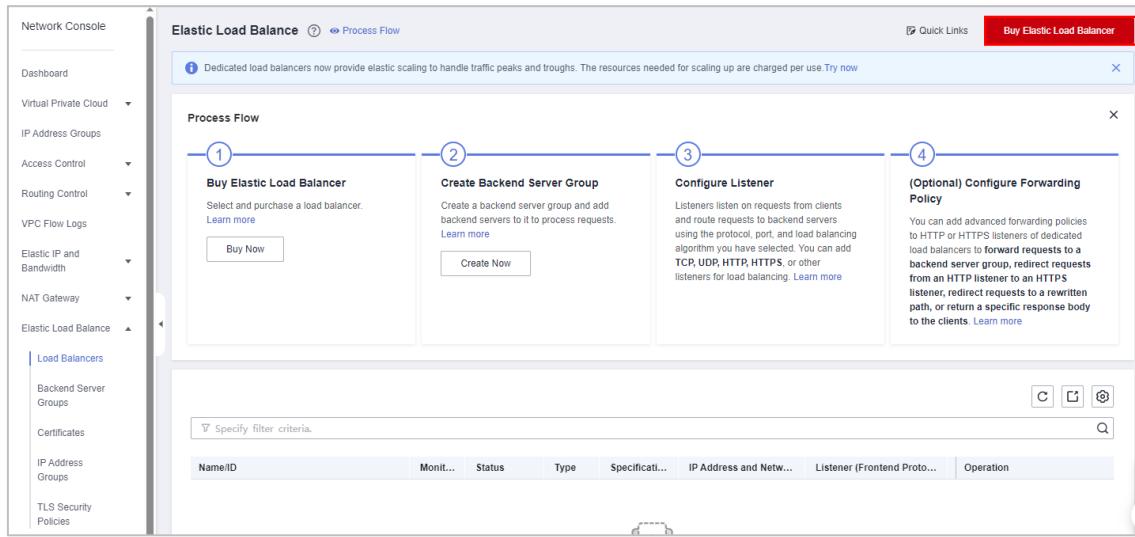
Step 1 On the management console, hover on the upper left to display **Service List** and choose **Networking > Elastic Load Balance**.



Compute		Storage		Networking		Databases	
Elastic Cloud Server	Elastic Cloud Server	Dedicated Distributed Storage Service	Elastic Volume Service	VPC Endpoint	VPC Private Cloud	GaussDB	
Auto Scaling	Auto Scaling	Storage Disaster Recovery Service	Virtual Private Network	NAT Gateway	Relational D		
Bare Metal Server	Image Management Service	Cloud Server Backup Service	Direct Connect	Elastic IP	Document D		
Elastic Volume Service	Dedicated Host	Cloud Backup and Recovery	Domain Name Service	Cloud Connect	GaussDB No		
Volume Backup Service	Cloud Container Engine	Volume Backup Service	NAT Gateway	Scalable File Service	Distributed D		
Virtual Private Cloud	Bare Metal Server	Object Storage Service	Elastic IP	CDN	Data Replica		
Elastic Load Balance	FunctionGraph	Data Express Service	Cloud Connect	Management & Governance	Data Admin		
Elastic IP	Dedicated Cloud	Scalable File Service	VPC Endpoint	Cloud Eye	Security &		
		CDN		Identity and Access Management	Anti-DDoS		
				Cloud Trace Service	Advanced Ar		
					Web Applica		
					Vulnerability		
					Host Securi		

Figure 6-37 Accessing Elastic Load Balance

## Step 2 Click Buy Elastic Load Balancer.



**Figure 6-38 Buy Elastic Load Balancer**

## Step 3 Configure the parameters as follows and click **Next**.

- Type: Shared
- Region: AP-Singapore
- Network type: Public network
- VPC: the VPC and subnet you created
- EIP: Select an existing EIP that has been unbound from the ECS.
- Name: elb-mp (Change it as needed.)

**Basic Information**

* Type	Dedicated	Shared <b>Selected</b>	Learn more
* Billing Mode	Pay-per-use <b>Selected</b>		
* 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.

---

**Network Configuration**

Network Type	<input checked="" type="checkbox"/> Public IPv4 network(Public network traffic)	<input checked="" type="checkbox"/> Private IPv4 network(Private network traffic) <a href="#">?</a>	
* VPC	vpc-hcia	<a href="#">View VPCs</a>	
* Subnet	subnet-hcia (192.168.0.0/24)	<a href="#">View Subnet</a>	
Available private IP addresses: 247			
* IPv4 Address	Automatically assign IP address		
* Guaranteed Performance	<input checked="" type="checkbox"/>		<a href="#">?</a>

---

* Name	elb-hcia
* EIP	<input type="radio"/> New EIP <input checked="" type="radio"/> Use existing <a href="#">?</a>
190.92.207.151 <a href="#">View EIP</a>	
Current bandwidth: 2 Mbit/s	

---

[Advanced Settings](#) [Description](#) | [Tag](#)

**Figure 6-39 Configuring parameters**

Step 4 Confirm the configuration and submit your request.

Resource	Configuration	Billing Mode	Quantity	Price
Elastic load balancer	Region: Singapore			
	Name: elb-hcia			
	Network Type: Public IPv4 network,Private IPv...			
	VPC: vpc-hcia			
	Type: Shared	Pay-per-use	1	\$0.053 USD /hour
	Subnet: subnet-hcia (192.168.0.0/24)			
	Guaranteed Performance: Enabled			
	EIP: 190.92.207.151			
	Tag: --			
	Description: --			

**Figure 6-40 Confirming the configuration**

Step 5 Go back to the load balancer list and ensure that the load balancer is in the **Running** state.

Name/ID	Monit...	Status	Type	Specificati...	IP Address and Netw...	Listener (Frontend Proto...	Bandwid	Operation
elb-hcia 717c1a05-a300-41f1-9117-51c59819ff11d		Running	Shared	Guaranteed...	192.168.0.140 (Private... vpc-hcia (VPC)	No listeners added. Add now	--	Add Listener   More ▾

Figure 6-41 Viewing the load balancer

Step 6 Click the name of the load balancer. Under **Listeners**, click **Add Listener**. Configure the name, protocol, and port for the listener.

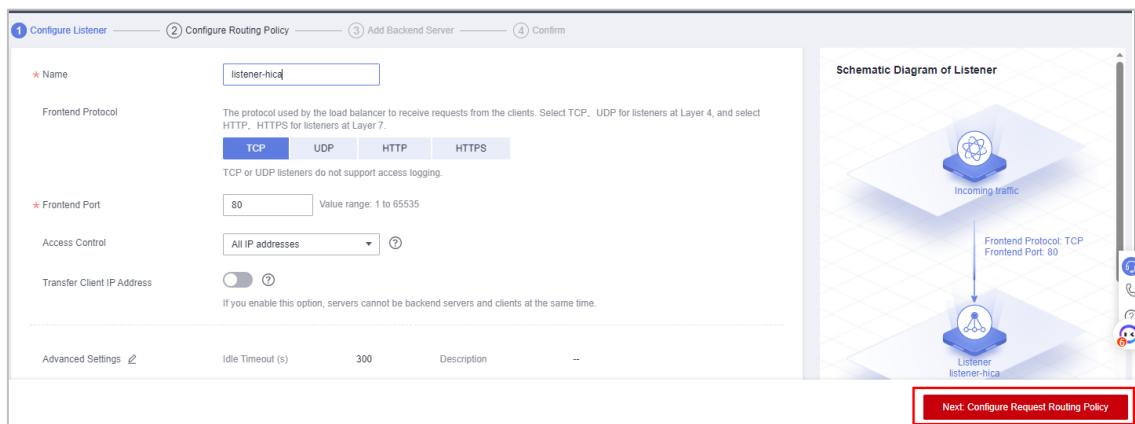


Figure 6-42 Adding a listener

Step 7 Click **Next: Configure Request Routing Policy**, Create a new Backend Server Group.

- Name: server\_group-hcia (Change it as needed.)
- Backend Protocol: TCP
- Load Balancing Algorithm: Weighted round robin
- Remain the default settings for other parameters.

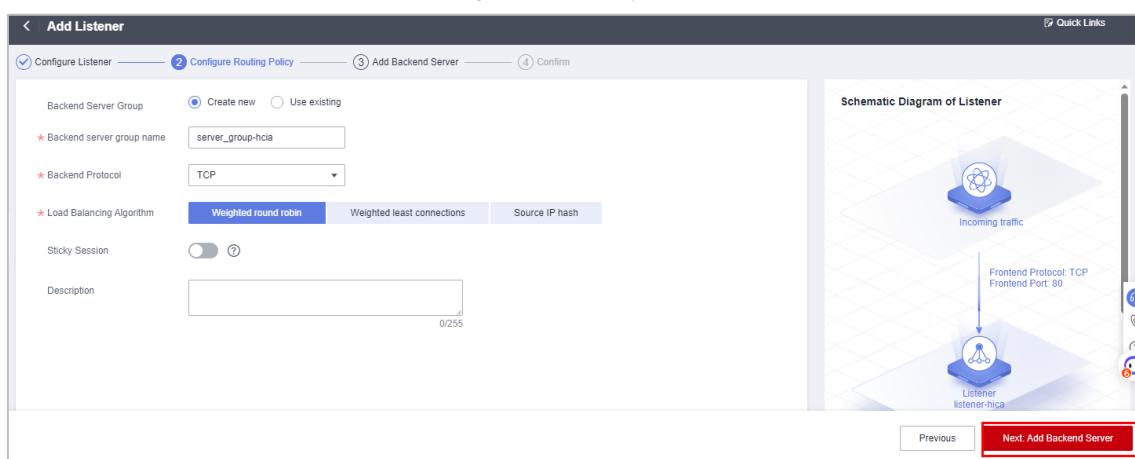
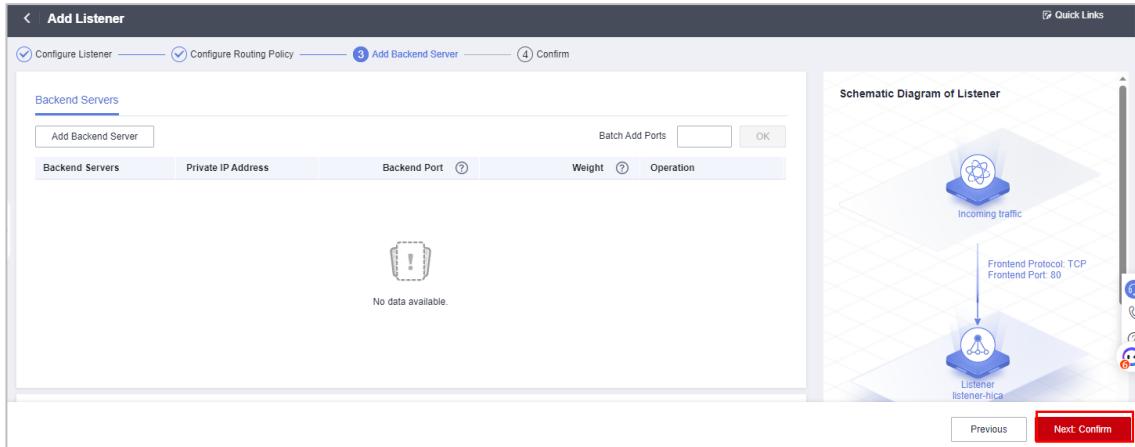


Figure 6-43 Configuring Routing Policy

Step 8 Click Next: Add Backend Server. Do not add the ECS. Click Next: Comfirm, and Submit.

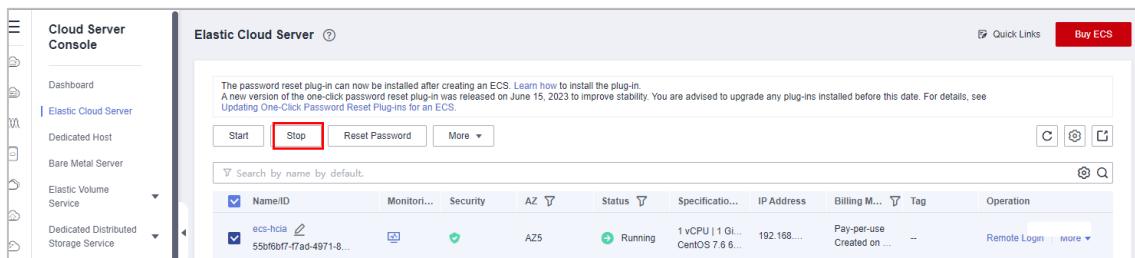


**Figure 6-44 Configuring a backend server group**

Now that the ELB configuration is complete, we need to configure some backend servers for AS. They will be added to or removed from the backend server group based on how much traffic there is. Before you configure AS, create a private image on the IMS console. This image will be used by the system to create these ECSs.

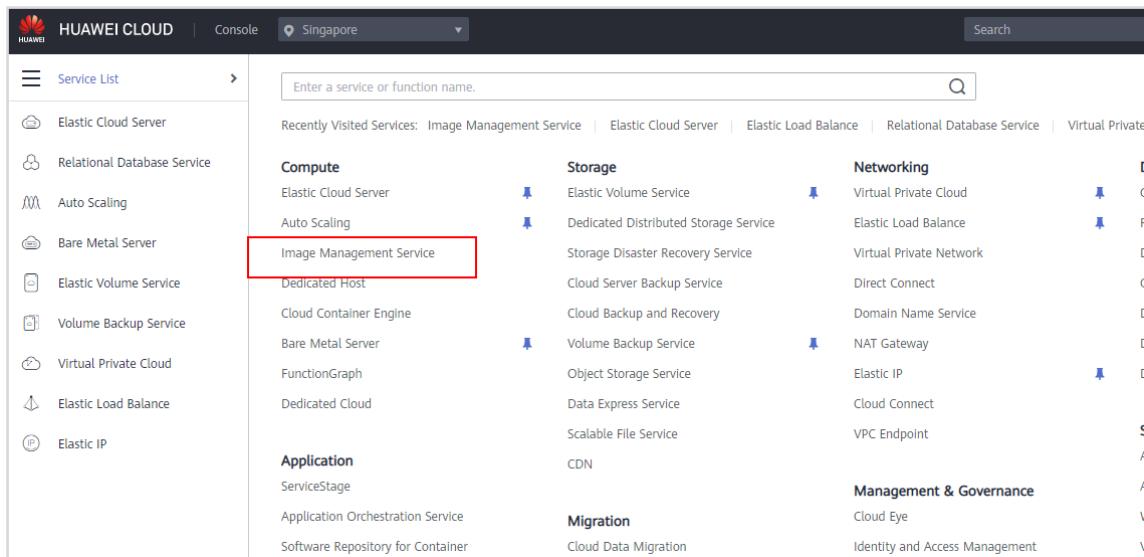
## 6.5.2 Creating an Image

Step 1 Go back to the ECS console, locate the ECS you created, and choose **More > Stop** in the **Operation** column.



**Figure 6-45 Stopping the ECS**

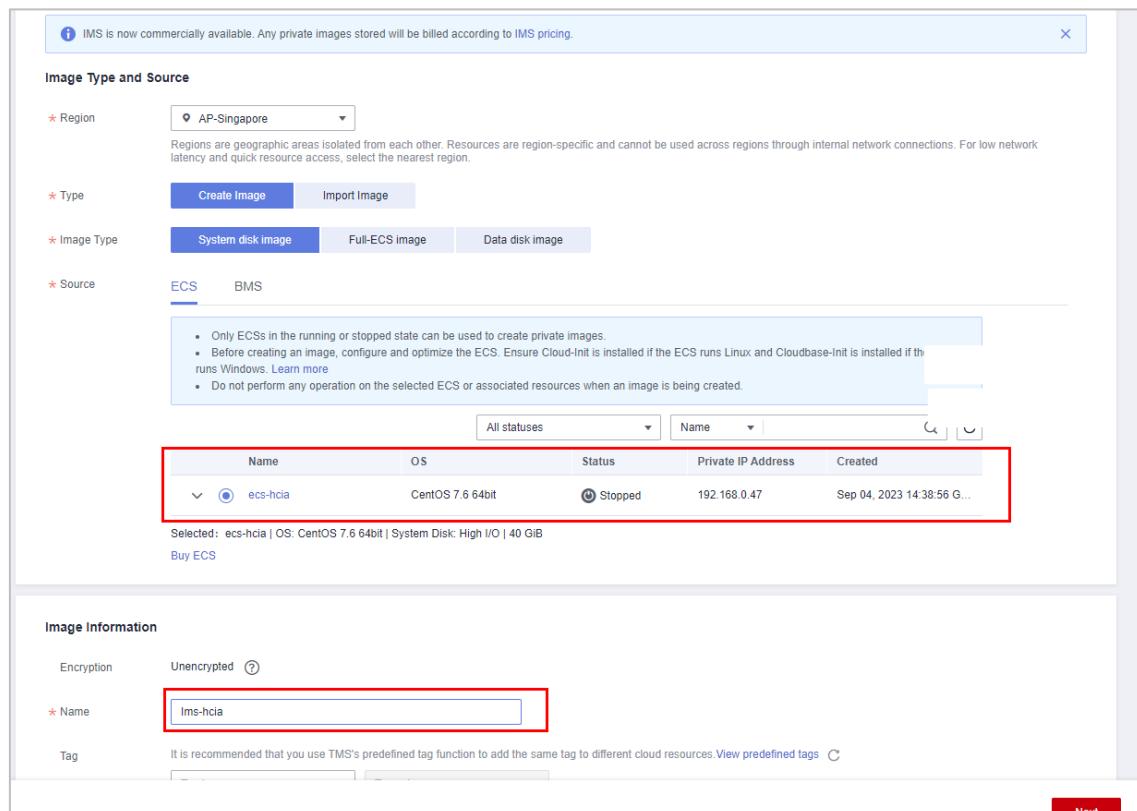
Step 2 Go back to the service list. Under **Compute**, click **Image Management Service**.



**Figure 6-46 Accessing Image Management Service**

Step 3 Click **Create Image** and configure the parameters as follows:

- **Type:** System disk image
- **Source:** the ECS you created
- **Name:** **ims-hcia** (Change it as needed.)



The screenshot shows the 'Create Image' configuration page. It includes fields for Region (AP-Singapore), Type (System disk image selected), and Source (ECS selected). A note indicates that only running or stopped ECSs can be used. The source list shows one ECS named 'ecs-hcia'. The 'Image Information' section shows 'Encryption' as 'Unencrypted' and 'Name' as 'Ims-hcia' (highlighted with a red box). A 'Next' button is at the bottom right.

**Figure 6-47 Configuring parameters**

Step 4 Click **Next**, confirm the configuration, and click **Submit**.

Step 5 Wait until the image status becomes **Normal**. Then, switch back to the ECS console, and start the ECS.

Name	Status	OS Type	OS	Image T...	Disk Ca...	Encrypted	Created	Operation
lms-hcia b218df47-abae-4a4e-beb...	Normal	Linux	CentOS 7.6...	ECS syste...	40	No		<a href="#">Apply for Server</a>   <a href="#">Modify</a>   <a href="#">More</a>

Figure 6-48 Viewing the created image

### 6.5.3 Configuring AS

Step 1 Go back to the service list. Under **Compute**, click **Auto Scaling**.

The screenshot shows the HUAWEI CLOUD service list. The 'Compute' section is expanded, and 'Auto Scaling' is selected, highlighted with a red box. Other services listed under Compute include Elastic Cloud Server, Image Management Service, Dedicated Host, Cloud Container Engine, Bare Metal Server, FunctionGraph, Dedicated Cloud, ApplicationStage, Application Orchestration Service, and Software Repository for Container. The rest of the page displays services from other categories like Storage, Networking, Databases, etc.

Figure 6-49 Accessing Auto Scaling

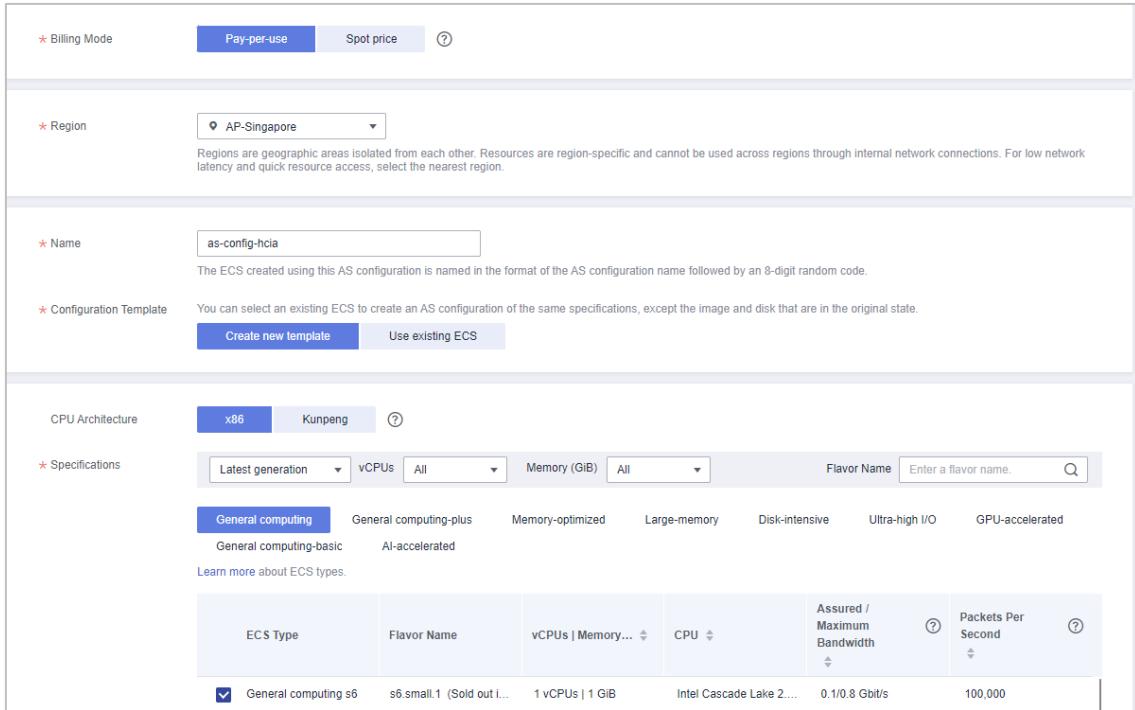
Step 2 Click Create AS Configuration.

The screenshot shows the 'Instance Scaling' configuration page. At the top right, there are two buttons: 'Create AS Group' and 'Create AS Configuration', with 'Create AS Configuration' highlighted by a red box. Below the buttons, there are tabs for 'AS Groups' and 'AS Configurations'. A message indicates you can create 10 more AS groups. The main table has columns for Name, Status, AS Configuration, Current Instances, Expected Instances, Min. Instances, Max. Instances, and Operation. The table currently shows 'No data available.'

Figure 6-50 Create AS Configuration

Step 3 Configure the parameters as shown in the following figures and then click **Create Now**.

Select the system disk image and security group you just created and set **EIP** to **Do not use**.



**Billing Mode:** Pay-per-use (selected), Spot price, ?

**Region:** AP-Singapore

**Name:** as-config-hcia

**Configuration Template:** Create new template (selected), Use existing ECS

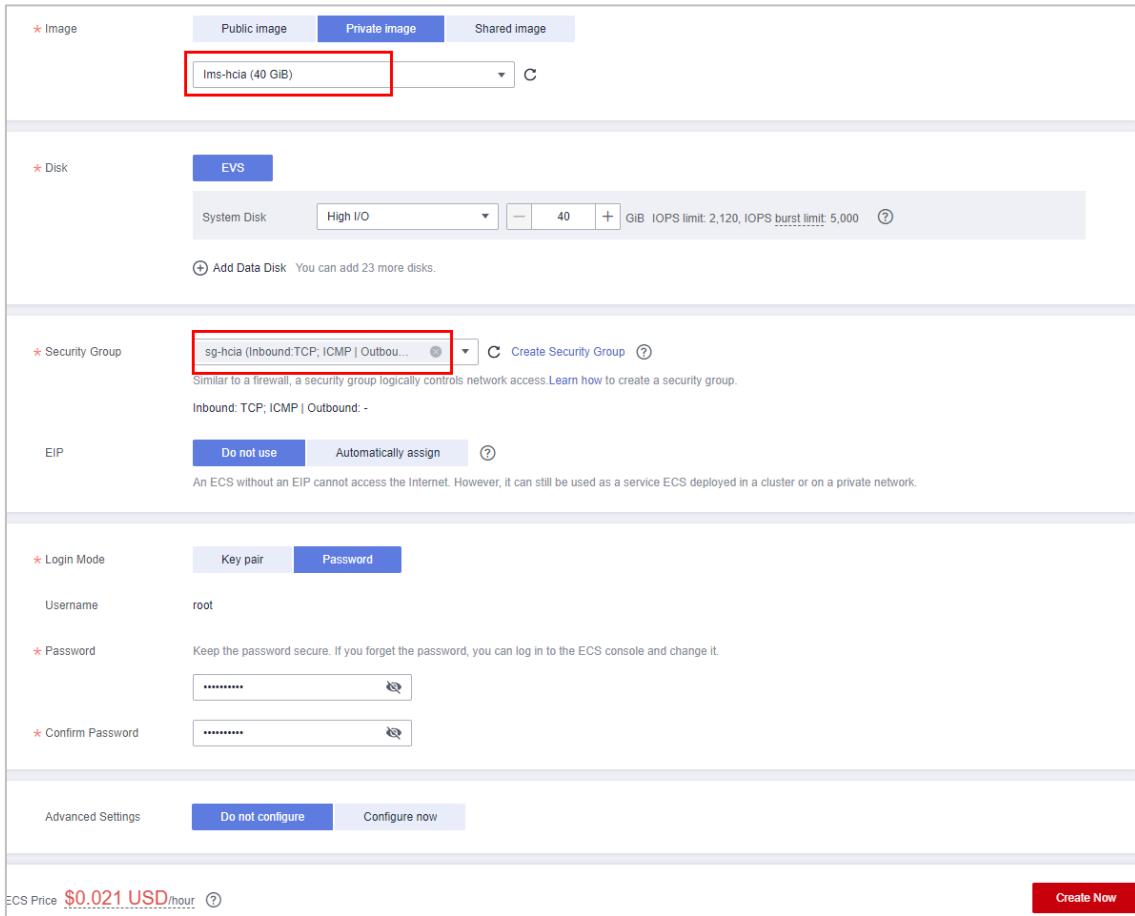
**CPU Architecture:** x86, Kunpeng, ?

**Specifications:**

- Latest generation, vCPUs: All, Memory (GiB): All
- Flavor Name: Enter a flavor name, Search icon
- General computing, General computing-plus, Memory-optimized, Large-memory, Disk-intensive, Ultra-high I/O, GPU-accelerated
- General computing-basic, AI-accelerated
- Learn more about ECS types.

ECS Type	Flavor Name	vCPUs   Memory...	CPU	Assured / Maximum Bandwidth	Packets Per Second
General computing s6	s6.small.1 (Sold out...)	1 vCPUs   1 GiB	Intel Cascade Lake 2...	0.1/0.8 Gbit/s	100,000

Figure 6-51 Configuring parameters



**Image:** Public image, Private image, Shared image, ims-hcia (40 GiB) selected, Create image icon

**Disk:** EVS, System Disk, High I/O, 40 GiB, IOPS limit: 2,120, IOPS burst limit: 5,000, Add Data Disk, Create volume icon

**Security Group:** sg-hcia (Inbound:TCP; ICMP | Outbound: -), Create Security Group, Similar to a firewall, a security group logically controls network access, Learn how to create a security group

**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.

**Login Mode:** Key pair, Password, Key pair selected

**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:** Confirm the password.

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

**ECS Price:** \$0.021 USD/hour, Create Now button

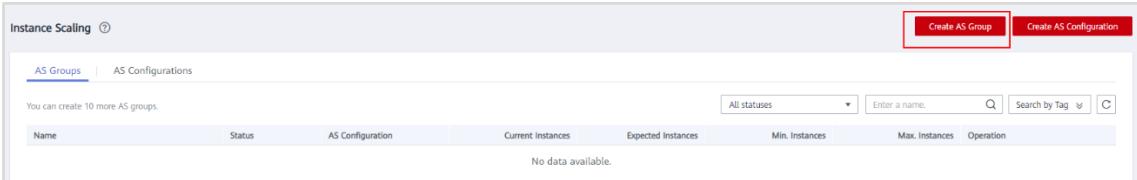
Figure 6-52 Configuring parameters

Step 4 View the created AS configuration.

Name	Status	Specificat...	Image	System Disk	Data Disks	Login M...	Created	Billing M...	Operation
as-config-hcia	Unbound	--	--	--	0	Password		Pay-per-use	<a href="#">Copy</a>   <a href="#">Delete</a>

Figure 6-53 Viewing the AS configuration

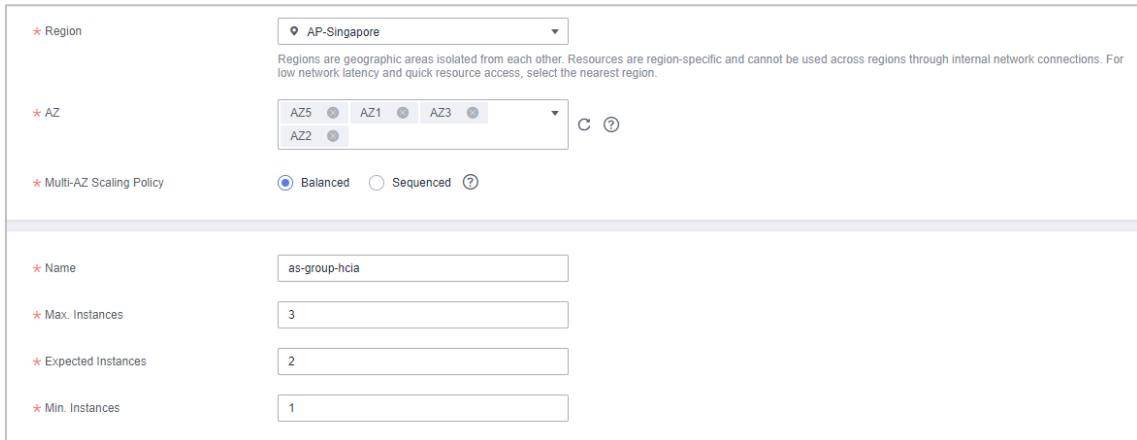
Step 5 Click Create AS Group.



The screenshot shows the 'Instance Scaling' interface with the 'AS Groups' tab selected. It displays a table with columns: Name, Status, AS Configuration, Current Instances, Expected Instances, Min. Instances, Max. Instances, and Operation. A message 'No data available.' is shown below the table. At the top right, there are two buttons: 'Create AS Group' (highlighted with a red box) and 'Create AS Configuration'.

Figure 6-54 Create AS Group

Step 6 Configure the parameters as shown in the following figure.



The screenshot shows the 'Configuring parameters' interface for creating an AS group. It includes fields for Region (set to AP-Singapore), AZ (set to AZ5, AZ1, AZ3, AZ2), Multi-AZ Scaling Policy (set to Balanced), and instance counts (Max. Instances: 3, Expected Instances: 2, Min. Instances: 1). The 'Name' field is set to 'as-group-hcia'.

Figure 6-55 Configuring parameters

Step 7 Select the AS configuration and load balancer you just created. AS will dynamically adjust the number of ECSSs in the backend server group using the image configured or used in the AS configuration.

The selected AS configuration serves as a specifications template for the instances in your AS group. After a subnet is selected, an IP address will be automatically assigned to each instance in the AS group.

<b>* AS Configuration</b>	as-config-hcia	[+]								
<b>* VPC</b>	vpc-hcia (192.168.0.0/16)	C Create VPC ?								
<b>* Subnet</b>	subnet-hcia (192.168.0.0/24)	This subnet is used by the primary NIC.								
<input checked="" type="checkbox"/> Source/Destination Check ?										
<input type="button" value="Add Subnet"/> You can add 4 more subnets. C Create Subnet										
Load Balancing	<input type="radio"/> Do not use <input checked="" type="radio"/> Elastic load balancer C Create ELB									
ECSs in the AS group are automatically bound to the selected load balancer										
<table border="1"> <tr> <td>Load Balancer</td> <td>elb-hcia (717c1a8...)</td> <td>Backend ECS Group</td> <td>server_group-hcia...</td> </tr> <tr> <td>Backend Port</td> <td>80</td> <td>Weight</td> <td>1</td> </tr> </table>			Load Balancer	elb-hcia (717c1a8...)	Backend ECS Group	server_group-hcia...	Backend Port	80	Weight	1
Load Balancer	elb-hcia (717c1a8...)	Backend ECS Group	server_group-hcia...							
Backend Port	80	Weight	1							
<input type="button" value="Add Load Balancer"/> You can add 5 more load balancers.										
<b>* Instance Removal Policy</b>	Oldest instance created from oldest AS config...									
EIP	<input checked="" type="radio"/> Release <input type="radio"/> 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	<input checked="" type="radio"/> Delete <input type="radio"/> 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.										
<b>* Health Check Method</b>	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. <a href="#">Learn more</a>										
<b>* Health Check Interval</b>	5 minutes									
<b>* Health Check Grace Period (s)</b>	600									
Tag	It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. <a href="#">View predefined tags</a> C									
<input type="text"/> Tag key		<input type="text"/> Tag value								

### Figure 6-56 Configuring parameters

Step 8 Locate the AS group you created and click **View AS Policy** in the **Operation** column.

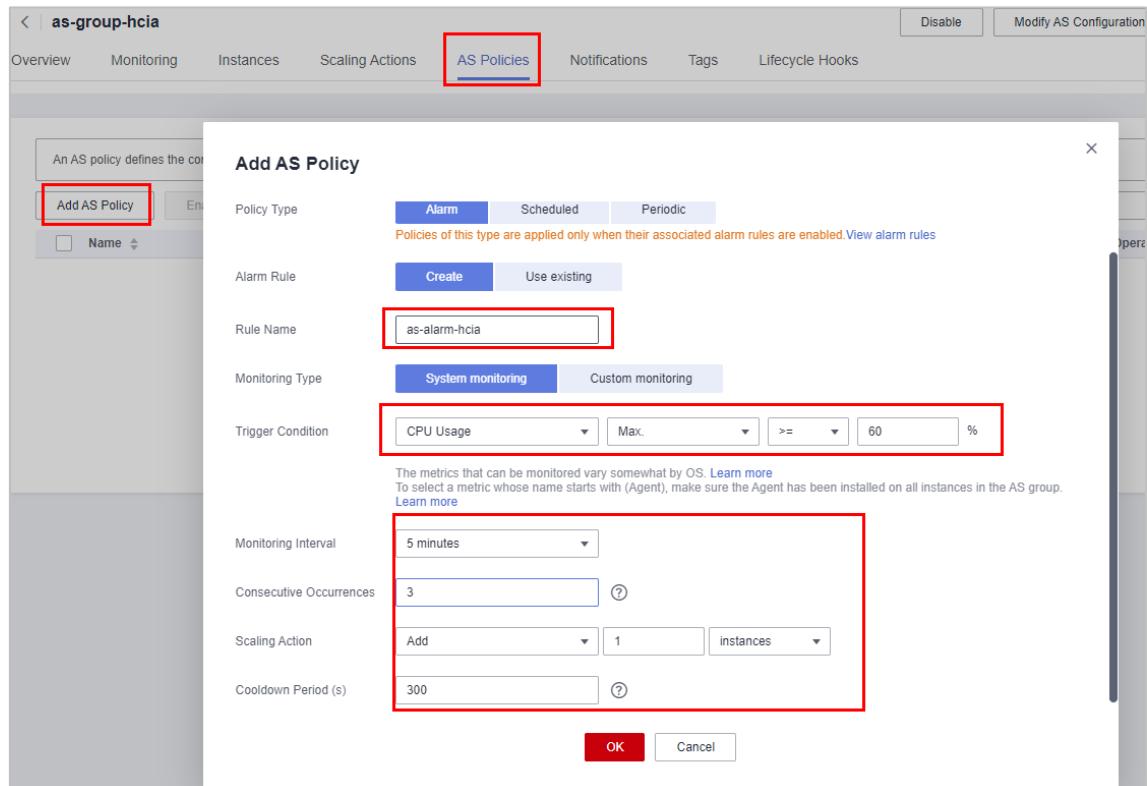
Instance Scaling								<a href="#">Create AS Group</a>	<a href="#">Create AS Configuration</a>
AS Groups		AS Configurations							
<a href="#">Export</a>		You can create 9 more AS groups.							
Name	Status	AS Config...	Current In...	Expected I...	Min. Insta...	Max. Insta...	Operation		
as-group-hcia a18dd24b-5cc9-4...	Enabled	as-config-hcia	0	2	1	3	<a href="#">View AS Policy</a>   Disable   More ▾		

### Figure 6-57 View AS Policy

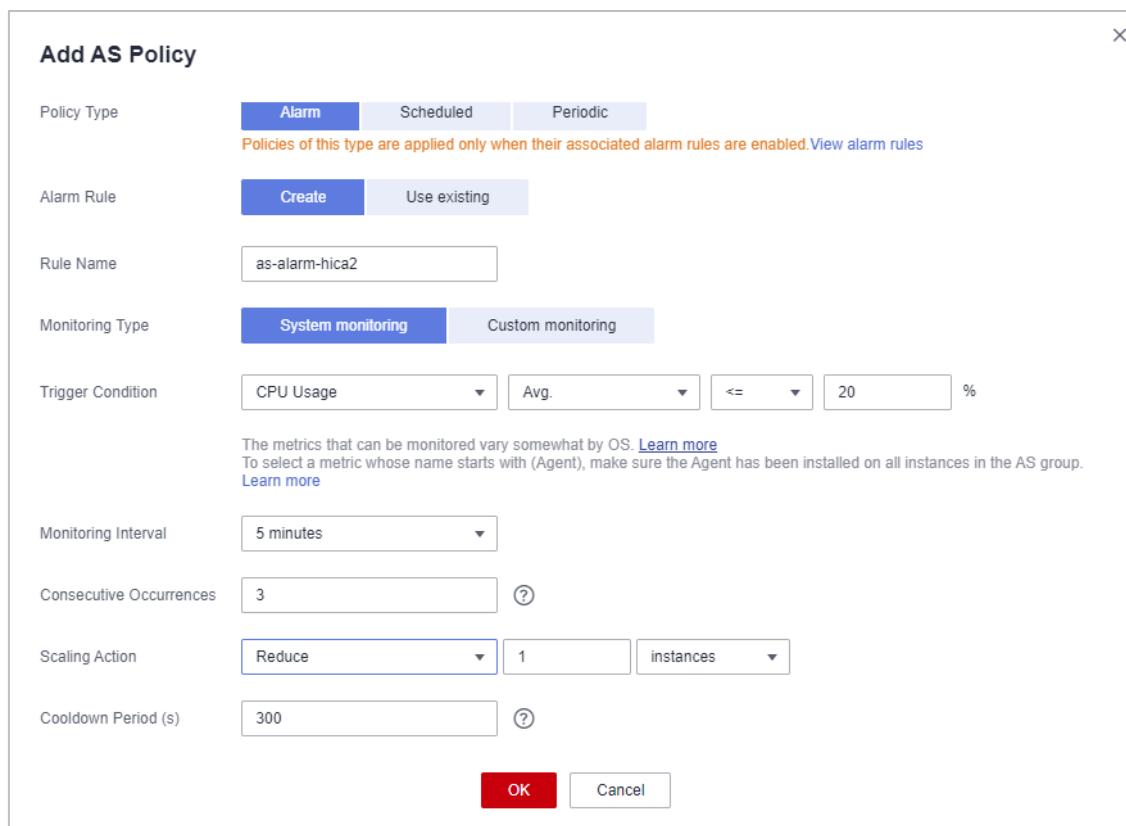
Step 9 Under AS Policies, click **Add AS Policy**.

- Trigger Condition: CPU Usage, Max.,  $\geq$ , 60. Scaling Action: Add, 1, instances

- Trigger Condition: CPU Usage, Avg.,  $\leq$ , 20. Scaling Action: Reduce, 1, instances

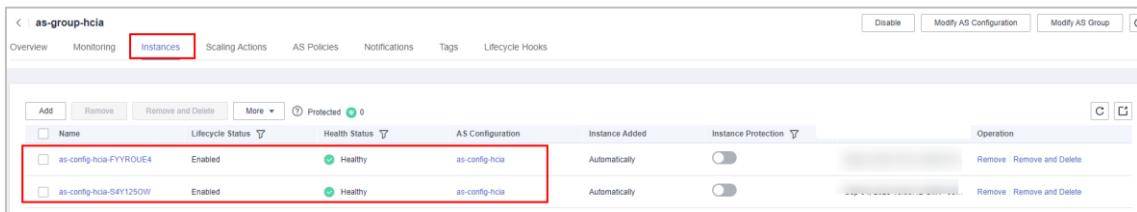


**Figure 6-58 Add AS policy**



**Figure 6-59 Adding an AS policy**

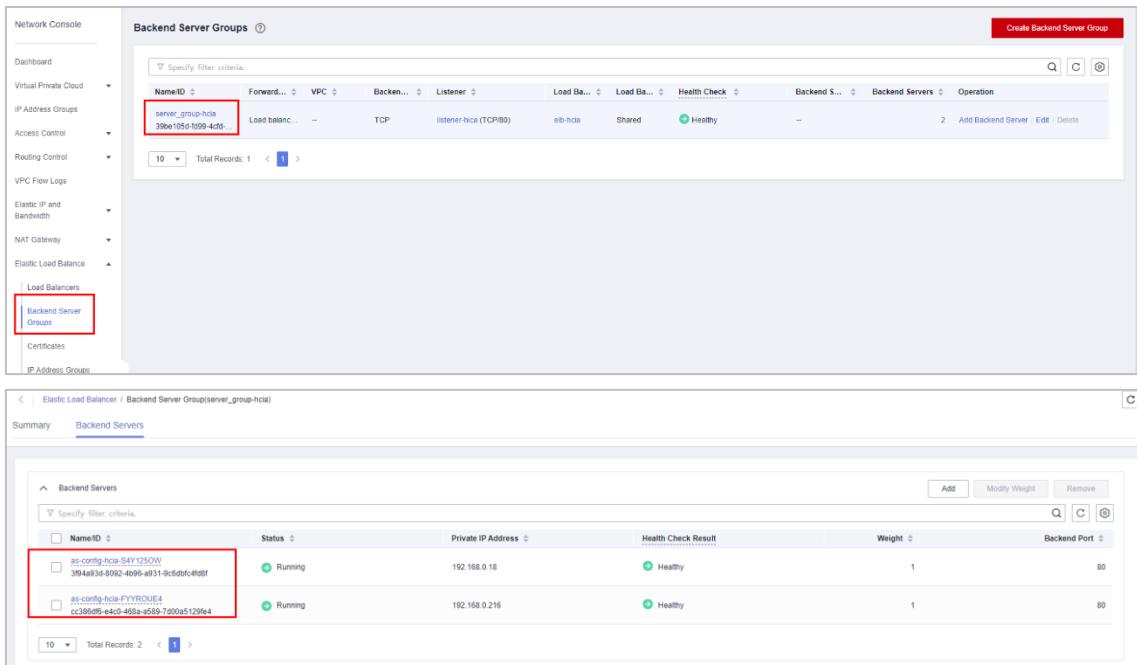
Step 10 Wait for about 2 minutes and check whether the AS policy has taken effect. As we can see in the following figure, two ECSs have been added to the AS group. The AS policy has taken effect.



The screenshot shows the 'Instances' tab of the AS Group 'as-group-hcia'. It lists two instances: 'as-config-hcia-FYYROUTE4' and 'as-config-hcia-S4Y1250W'. Both instances are marked as 'Enabled' and 'Healthy'. They are associated with the AS configuration 'as-config-hcia'. The 'Instance Added' column shows 'Automatically' and the 'Instance Protection' column shows 'Off'. There are 'Remove' and 'Remove and Delete' buttons for each instance.

**Figure 6-60 Viewing instance changes**

Step 11 Switch back to the ELB console and click the load balancer name, **elb-hcia**. Locate the backend server group associated with the load balancer and view the two ECSs added by the AS service.



The screenshot shows the 'Backend Server Groups' section of the ELB console. It lists a single backend server group named 'server\_group-hcia'. The table shows two backend servers: 'as-config-hcia-S4Y1250W' (status: Running, weight: 1, port: 80) and 'as-config-hcia-FYYROUTE4' (status: Running, weight: 1, port: 80). Both servers are marked as 'Healthy'.

**Figure 6-61 Viewing the backend server group**

Step 12 Verify that web servers where the website is deployed can be accessed using the EIP bound to the load balancer. We have finished configuring AS and verified that AS can dynamically adjust the number of ECSs in the backend server group associated with the load balancer based on the configured AS policy.

## 6.6 Visiting the Website

Step 1 View the elastic IP address bound to the Elastic Load Balance load balancer.

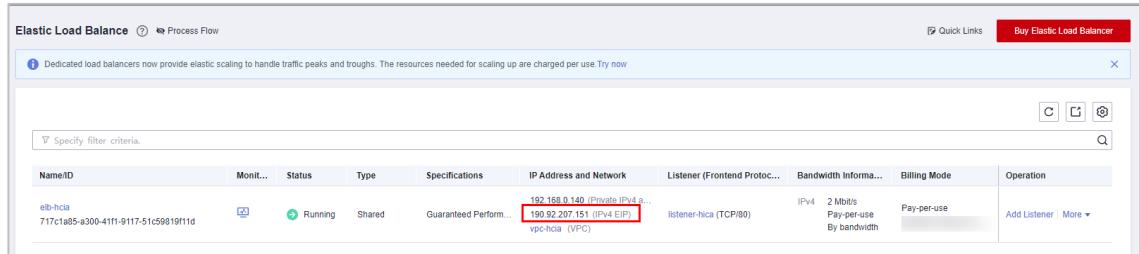


Figure 6-62 Viewing ELB EIP

Step 2 In the address box of the browser on your PC, enter **http://Load balancer's EIP/wordpress/**, and press **Enter**.

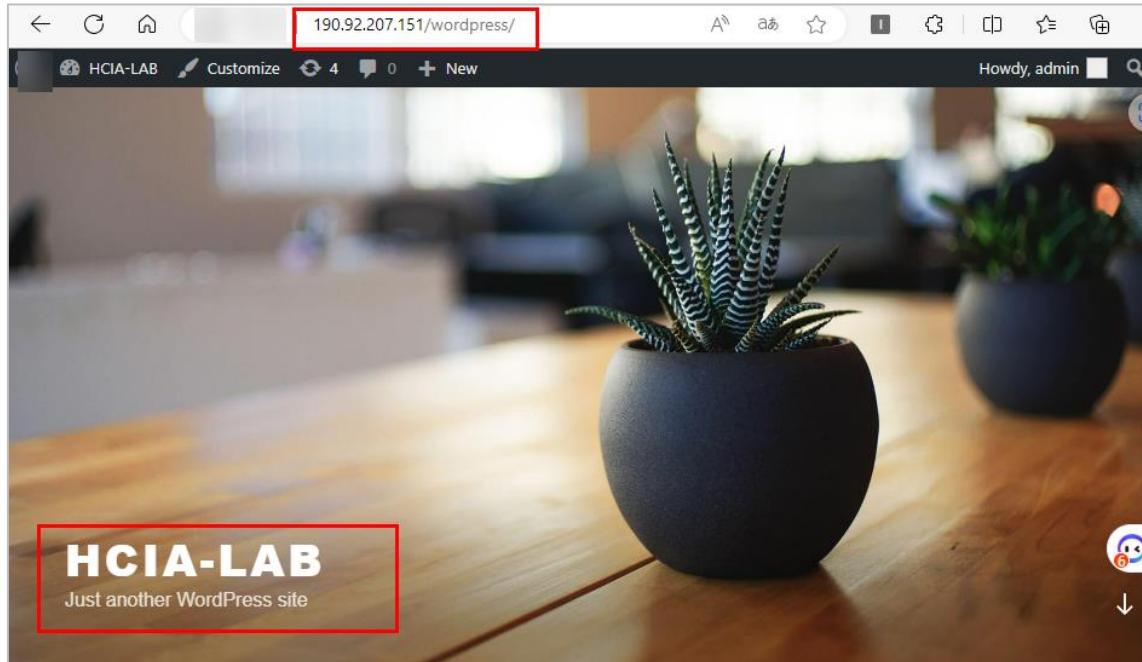
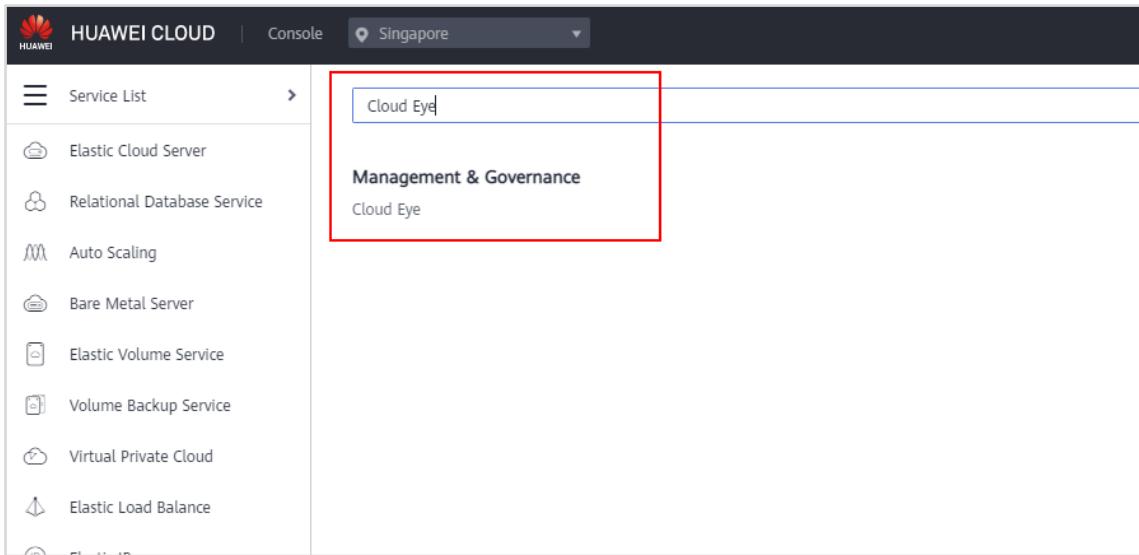


Figure 6-63 Visiting the website

Step 3 Check whether the website can be accessed. If the website can be accessed, web servers where the website is deployed can provide Internet-accessible services using the load balancer's EIP.

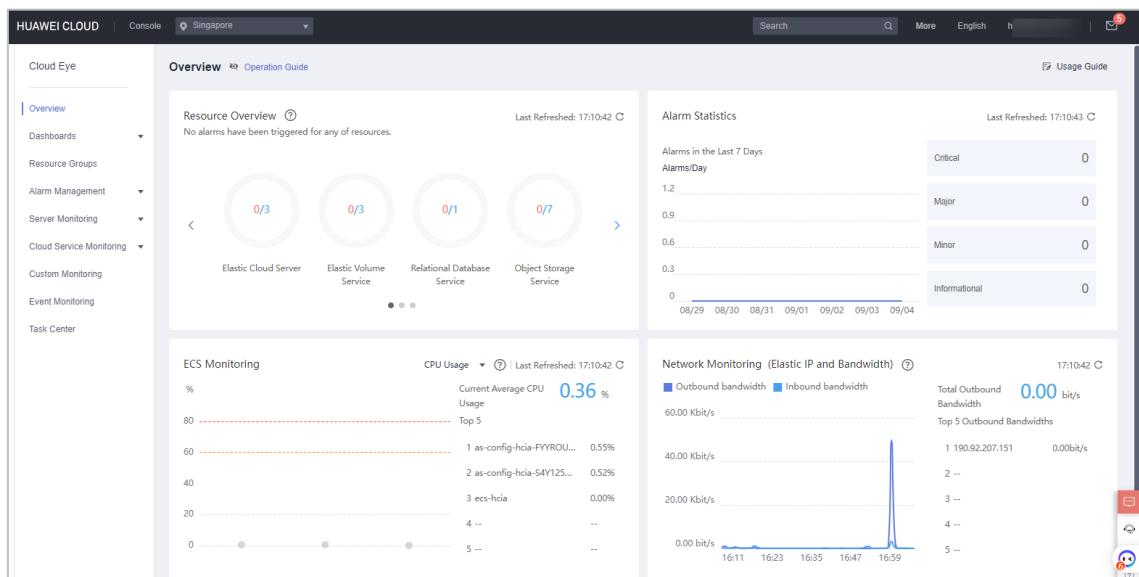
## 6.7 Monitoring Resources

Step 1 On the service list page, choose **Management & Governance > Cloud Eye**.



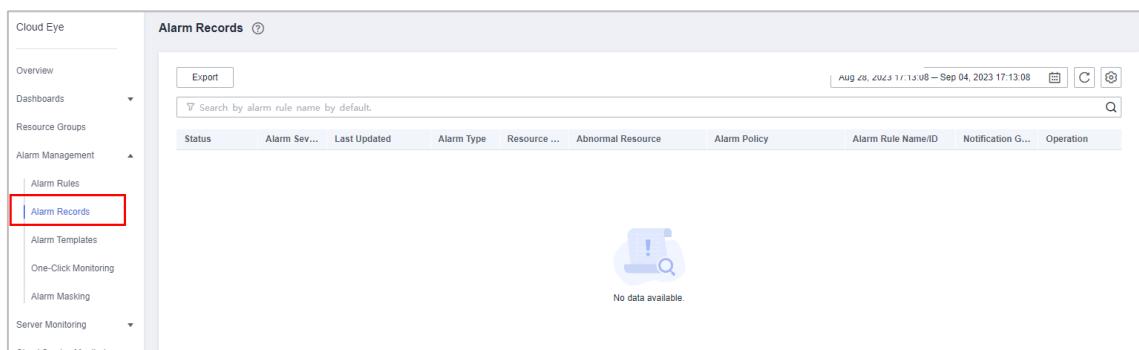
**Figure 6-64 Accessing Cloud Eye**

Step 2 On the **Overview** page, view overall resource information and alarm statistics.



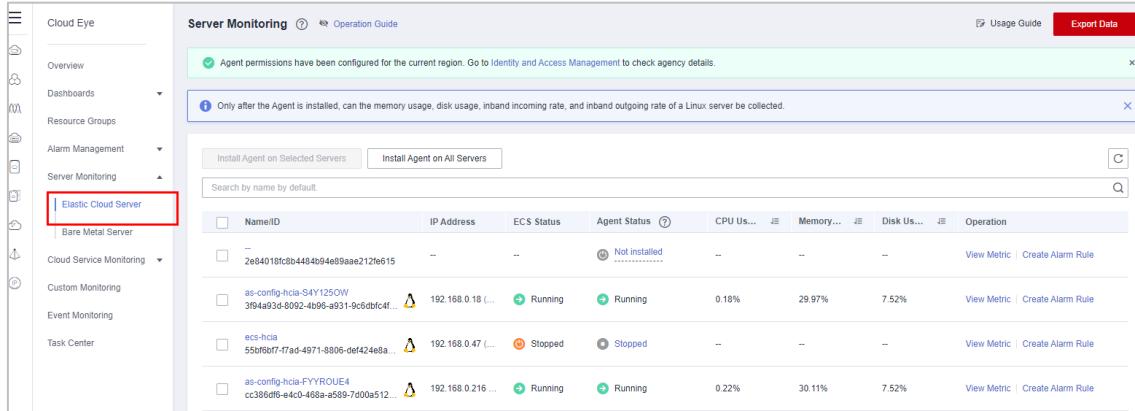
**Figure 6-65 Resource Overview**

Step 3 In the left navigation pane, choose **Alarm Management > Alarm Records**. View service alarms and handle any faults in a timely manner.



**Figure 6-66 Viewing alarm history**

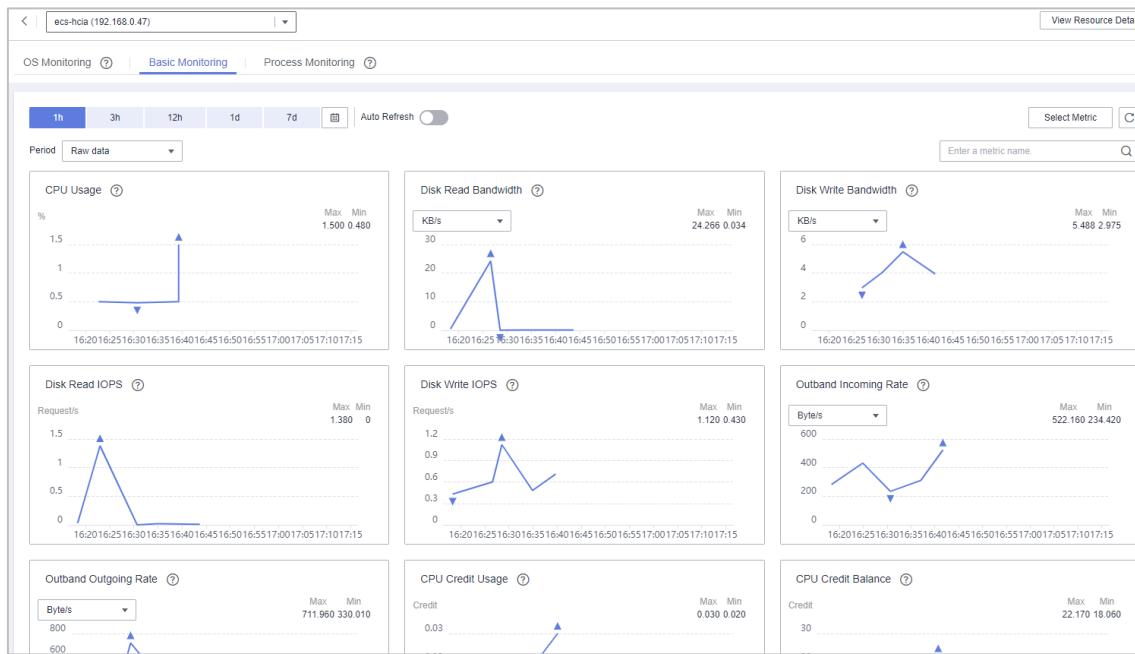
Step 4 In the left navigation pane, choose **Server Monitoring > Elastic Cloud Server** and then view ECS monitoring information.



Name	ID	IP Address	ECS Status	Agent Status	CPU Us...	Memory...	Disk Us...	Operation
2e84018fc8b4484b94e89aae212fe615		—	—	Not installed	—	—	—	<a href="#">View Metric</a>   <a href="#">Create Alarm Rule</a>
as-config-hcia-S4Y1250W	3f94a93d-8092-4b96-a931-9c6bfc4af...	192.168.0.18 (...	Running	Running	0.18%	29.97%	7.52%	<a href="#">View Metric</a>   <a href="#">Create Alarm Rule</a>
ecsi-hcia	550f6bf7-f7ad-4971-8806-def424e8a...	192.168.0.47 (...	Stopped	Stopped	—	—	—	<a href="#">View Metric</a>   <a href="#">Create Alarm Rule</a>
as-config-hcia-FYRROUE4	cc386df8-4c00-468a-a599-7009a512...	192.168.0.216 (...	Running	Running	0.22%	30.11%	7.52%	<a href="#">View Metric</a>   <a href="#">Create Alarm Rule</a>

**Figure 6-67 Server Monitoring**

Step 5 Click the name of an ECS to view its monitoring details.

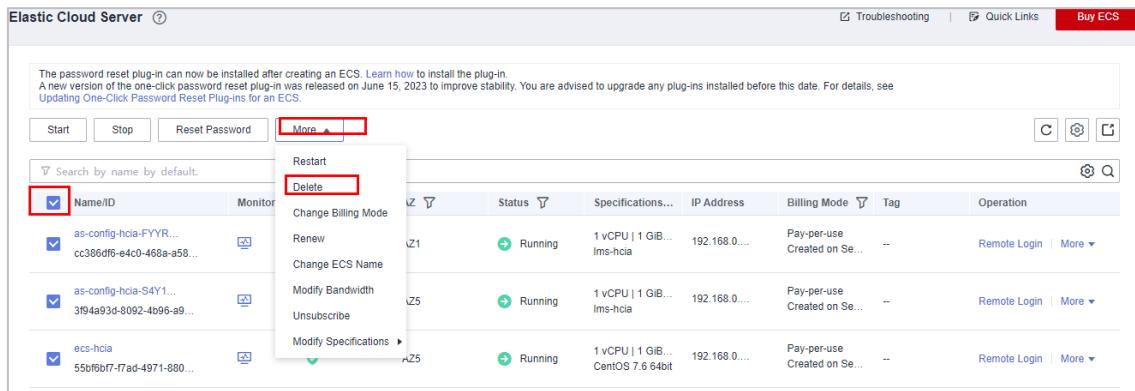

**Figure 6-68 Basic Monitoring**

## 6.8 Deleting Resources

### 6.8.1 Deleting ECSs

Step 1 You need to suspend AS before deleting ECSs. Otherwise, AS automatically creates new ECSs when detecting the expected number of ECSs in the AS group.

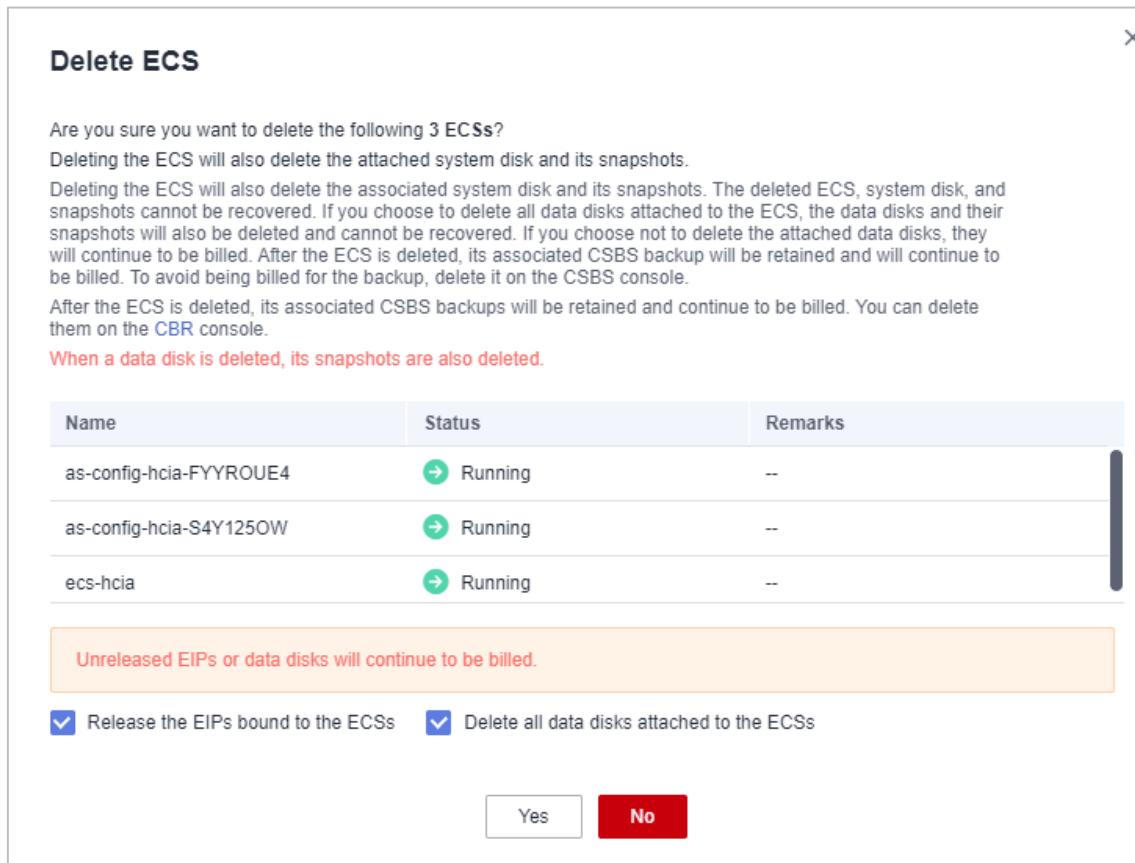
## Step 2 Select the ECSs you want to delete and click **Delete**.



The screenshot shows the 'Elastic Cloud Server' interface. On the left, there's a sidebar with 'Start', 'Stop', 'Reset Password', and a 'More' dropdown. The 'More' dropdown is open, showing options like 'Delete'. Below the sidebar is a search bar with 'Search by name by default.' and a dropdown menu set to 'Name/ID'. The main area displays a table of ECS instances:

	Name/ID	Status	Specifications...	IP Address	Billing Mode	Tag	Operation
<input checked="" type="checkbox"/>	as-config-hcia-FYYR...	Z1	1 vCPU   1 GiB... Ims-hcia	192.168.0....	Pay-per-use	Created on Se...	<a href="#">Remote Login</a>   More
<input checked="" type="checkbox"/>	as-config-hcia-S4Y1...	Z5	1 vCPU   1 GiB... Ims-hcia	192.168.0....	Pay-per-use	Created on Se...	<a href="#">Remote Login</a>   More
<input checked="" type="checkbox"/>	ecs-hcia	AZ5	1 vCPU   1 GiB... CentOS 7.6 64bit	192.168.0....	Pay-per-use	Created on Se...	<a href="#">Remote Login</a>   More

Figure 6-69 Deleting ECSs



**Delete ECS**

Are you sure you want to delete the following 3 ECSs?

Deleting the ECS will also delete the attached system disk and its snapshots.

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	Remarks
as-config-hcia-FYYROUE4	Running	--
as-config-hcia-S4Y125OW	Running	--
ecs-hcia	Running	--

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

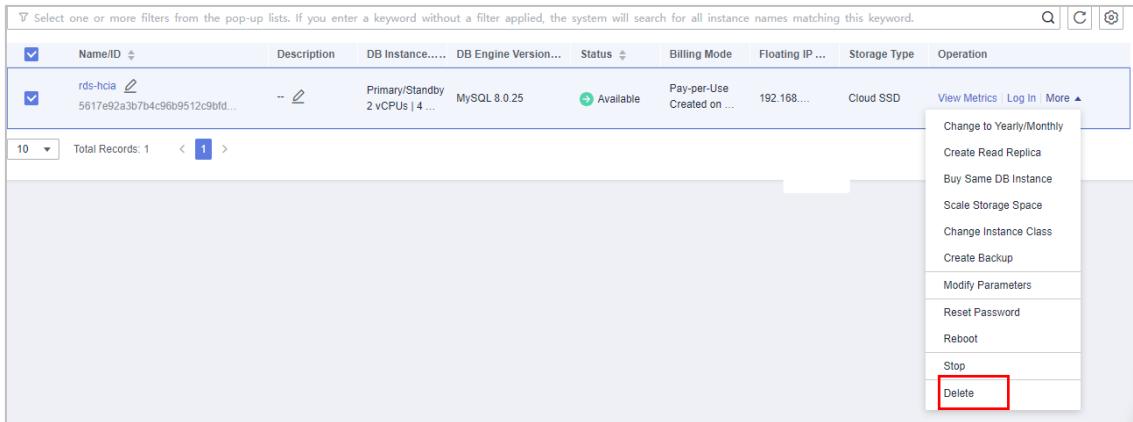
**Yes** **No**

Figure 6-70 Confirming the deletion

## 6.8.2 Deleting the RDS DB Instance

Step 1 On the service list page, choose **Database > Relational Database Service**.

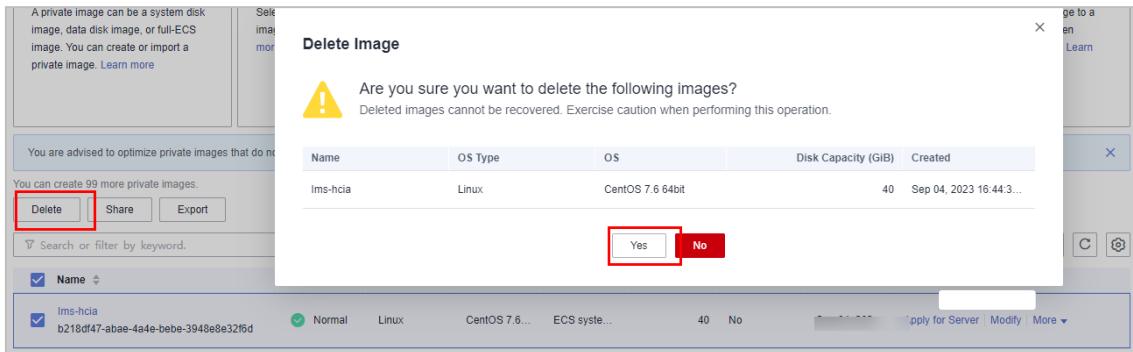
Step 2 Locate the RDS DB instance you want to delete and click **Delete** in the **Operation** column.



**Figure 6-71 Deleting the RDS DB instance**

### 6.8.3 Deleting the Image

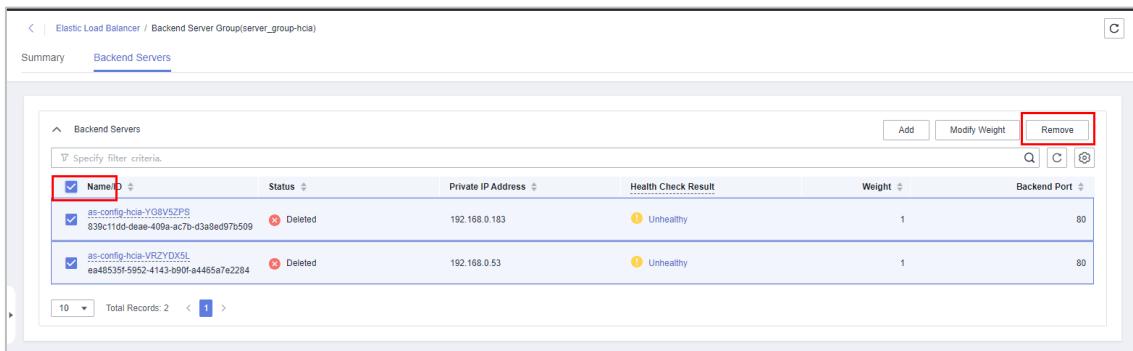
Go to the IMS console. Locate the private image you want to delete and click **Delete**. In the displayed dialog box, click **Yes**.



**Figure 6-72 Deleting the private image**

### 6.8.4 Deleting the Load Balancer

Step 1 Go to the ELB console, click the name of the shared load balancer. Under **Backend Server Groups**, locate the backend server group associated with the load balancer. Remove the ECSs from the group and then delete the listener. Once you have deleted the ECSs added by AS, you can delete the listener.



**Figure 6-73 Deleting the listener**

## Step 2 Delete the listener.

The screenshot shows the 'Listeners' tab of the Elastic Load Balancer interface. It lists a single listener named 'elb-hcfa' with the following details:

Name/ID	Frontend Protocol/Port	Default Backend Server Group	Forwarding Policies	Health Check	Monitoring	Access Control	Operation
elb-hcfa 3cf0030c-23cf-4380-bd87-c346111a841	TCP:80	server_group-hcfa View/Add Backend Server	--	<span style="color: green;">Healthy</span>	<span style="color: blue;">Edit</span>	All IP addresses Configure	<span style="color: red;">Delete</span>

## Step 3 Locate the load balancer and click **Delete**. In the displayed dialog box, click **Yes**.

The screenshot shows the 'Elastic Load Balance' interface with a modal dialog box asking 'Are you sure you want to delete this load balancer?'. The dialog contains two buttons: 'Yes' and 'No'. In the background, the main interface shows a list of load balancers, with one named 'elb-hcfa' selected. A preview pane on the right shows the details for this selected load balancer.

Figure 6-74 Deleting the load balancer

## 6.8.5 Deleting AS Resources

### Step 1 Locate the AS group you want to delete and click **Delete**. In the displayed dialog box, click **Yes**.

The screenshot shows the 'Instance Scaling' interface with the 'AS Groups' tab selected. It lists an AS group named 'as-group-hcfa' with the following details:

Name	Status	AS Config...	Current In...	Expected I...	Min. Insta...	Max. Insta...	Operation
as-group-hcfa a18dd24b-5cc9-4f7b-a94a-de496202718d	Abnormal	as-config-hcfa	0	2	1	3	<span style="color: red;">Delete</span>

Figure 6-75 Deleting the AS group

### Step 2 Locate the AS configuration you want to delete and click **Delete**. In the displayed dialog box, click **Yes**.

The screenshot shows the 'Instance Scaling' interface with the 'AS Configurations' tab selected. It lists an AS configuration named 'as-config-hcfa' with the following details:

Name	Status	Specificatio...	Image	System Disk	Data Disk(s)	Login M...	Created	Billing M...	Operation
as-config-hcfa	Unbound	--	--	--	0	Password	2...	Pay-per-use	<span style="color: red;">Delete</span>

Figure 6-76 Deleting the AS configuration

## 6.8.6 Deleting VPC Resources

### Step 1 In the left navigation pane, choose **Subnets** and then delete the subnet.

Name/ID	VPC	IPv4 CIDR Block	IPv6 CIDR...	Status	Network ACL	Route Table	Operation
subnet-hc1a ec571b7e-9495-4196-8e39-e...	vpc-hc1a	192.168.0.0/24	-- Enable IPv6	Available	--	rtb-vpc-hc1a Default	<a href="#">Change Route Table</a> <a href="#">Delete</a>

Figure 6-77 Deleting the subnet

Step 2 In the left navigation pane, choose **Access Control > Security Groups** and then delete the security group. Then delete the VPC.

Name/ID	Security Group ...	Associated Instances	Description	Created	Operation
sg-hc1a f01fa6ba-950c-4b7d-b0c5-ae6...	10	0	The security group is for...	Sep 04, 2023 14:29:30 ...	<a href="#">Manage Rule</a> <a href="#">Manage Instance</a> <a href="#">More</a> <a href="#">Delete</a>
default 2acc769e-1ae6-410f-86b1-051...	6	0	Default security group	Sep 01, 2023 08:34:58 ...	<a href="#">Manage Rule</a> <a href="#">Manage Instance</a> <a href="#">Clone</a> <a href="#">Delete</a>

Figure 6-78 Deleting the security group

Name/ID	IPv4 CIDR Block	Status	Subnets	Route Tables	Servers	Operation
vpc-hc1a 56b83fac-a472-4236-9624-81f...	192.168.0.0/16 (Primar...	Available	0	1	0	<a href="#">Edit CIDR Block</a> <a href="#">Delete</a>

Figure 6-79 Deleting the VPC

Step 3 On the **Dashboard** page of the **Cloud Server Console** and **Network Console**, and on the IMS console, confirm that all of the purchased resources have been deleted in all regions.

ECs	DeHs	BMs	EVS Disks
0	0	0	0

Dedicated Distributed Storage Services	Images	AS Groups	ECS Groups
0	0	0	0

Figure 6-80 Checking ECS-related resources

**Figure 6-81 Checking network resources**

**Figure 6-82 Viewing private images**

**Step 4** Hover your cursor over **Resources** and click **My Resources**. Check whether there are still billable cloud resources in the corresponding region. If there are such services, delete the resources in that region.

**Figure 6-83 Resources**

**Figure 6-84 My Resources**

# 7

## Acronyms and Abbreviations

---

AS: Auto Scaling  
ACL: access control list  
AK/SK: Access Key ID/Secret Access Key  
AZ: Availability Zone  
BMS: Bare Metal Server  
CES: Cloud Eye Service  
CTS: Cloud Trace Service  
DHCP: Dynamic Host Configuration Protocol  
DNS: Domain Name Service  
EIP: Elastic IP  
Elastic Cloud Server  
ELB: Elastic Load Balance  
EVS: Elastic Volume Service  
I/O: Input/Output  
IAM: Identity and Access Management  
IMS: Image Management Service  
LTS: Log Tank Service  
NAT: network address translation  
NFS: Network File System  
OBS: Object Storage Service  
OS: Operation System  
SFS: Scalable File Service  
SSD: Solid State Disk  
VPC: Virtual Private Cloud  
VPCEP: VPC Endpoint  
VPN: Virtual Private Network