

HCIA Cloud Service Certification Training

HCIA-Cloud Service

Lab Guide for HUAWEI CLOUD Service Engineers

Version: 3.0



Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd. 2021. 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: <http://e.huawei.com>

Huawei Certification System

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

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

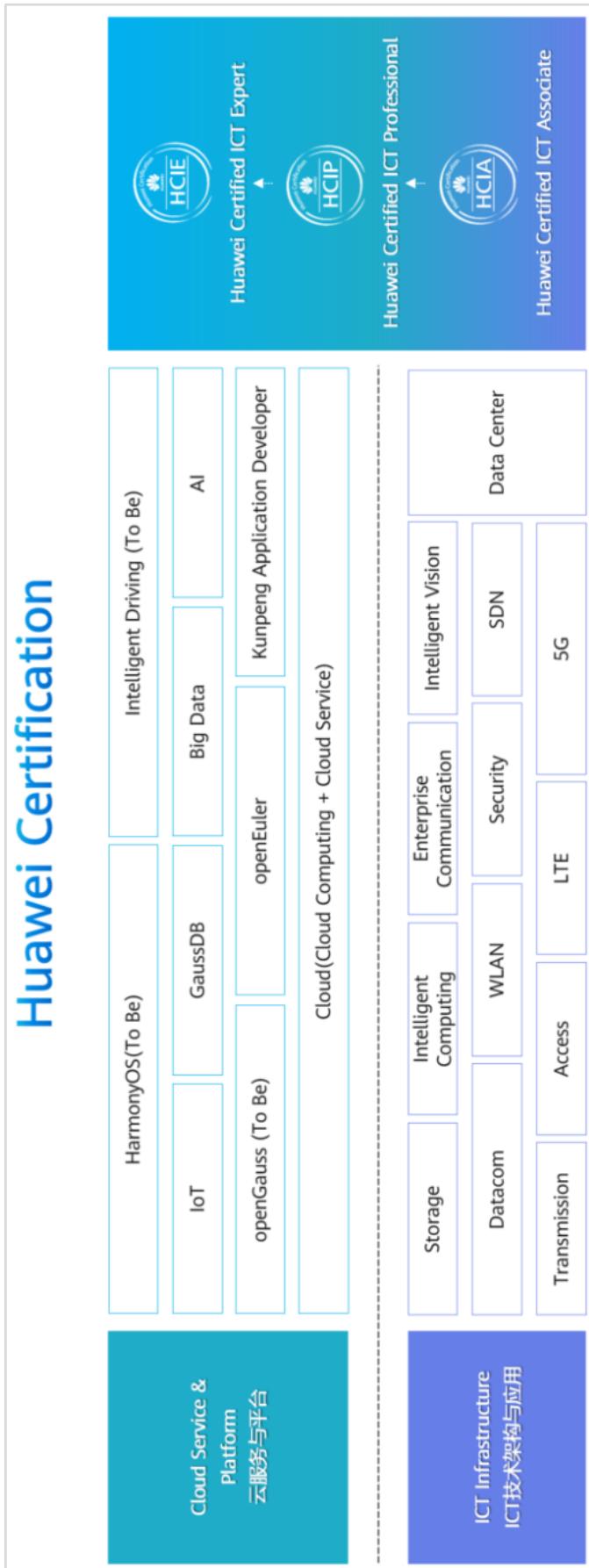
Huawei Certification covers all ICT fields, and it is aligned with the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era and building a sound ICT talent ecosystem.

HCIA-Cloud Service (Huawei Certified ICT Associate-Cloud Service) certification is designed for popularizing cloud computing technologies and basic knowledge and developing engineers who are capable of building enterprise IT architectures with cloud services in fields, such as compute, storage, and network. This document is intended for candidates who take the HCIA-Cloud Service exam or technical personnel who want to understand cloud computing basics and how to use, manage, and maintain HUAWEI CLOUD products. The HCIA-Cloud Service certification covers the basic knowledge of IaaS, PaaS, and SaaS, including the operation and use of HUAWEI CLOUD cloud services, such as compute, storage, network, management & governance, and relational database services.

Passing the HCIA-Cloud Service certification proves that you have a certain understanding of HUAWEI CLOUD products and technologies, and you can independently use HUAWEI CLOUD products.

Enterprises with engineers who have passed HCIA-Cloud Service certification have mastered the scenarios and usage of various HUAWEI CLOUD products, facilitating their cloud transformation in the ICT environment.

Huawei Certification



About This Document

Overview

This document 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.

- Exercise 1: Exercises on HUAWEI CLOUD operations. The exercises include registering a HUAWEI CLOUD account, logging in to the console, configuring IAM, as well as purchasing, trying, and releasing cloud services.
- Exercise 2: 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.
- Exercise 3: Exercises on 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.
- Exercise 4: Exercises on storage services, including using and managing Elastic Volume Service (EVS), Object Storage Service (OBS), and Scalable File Service (SFS).
- Exercise 5: 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.
- Exercise 6: Exercises on using ECS and RDS as service nodes and data nodes, using VPC to provide network resources for ECS, using AS to dynamically add and remove ECS instances to ensure stable running, using ELB to automatically distribute traffic among backend servers to achieve greater levels of fault tolerance in your applications, and using Cloud Eye to monitor cloud services.

Knowledge Required

To better understand this certification course, familiarize yourself with the following knowledge:

- Basic IT knowledge
- Servers and commonly used operating systems (Windows and Linux)
- Fundamentals about storage and network

Lab Environment

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.

All basic security services are configured by default for all exercises.

The following table lists the resources required for the exercises. The actual costs may vary, depending on your use of the cloud services.

**SEMPRE USAR = REGIÃO SÃO-PAULO, BILLING MODE = PAY-PER-USE
(EXCETO NOS CASOS EM QUE O INSTRUTOR SUGERIR OUTRA REGIÃO)**

| Exercise | Cloud Service | Quantity | Specifications |
|-------------------------------|---------------|----------|---|
| Exercises on compute services | ECS | 1 | x86 General computing s3.medium.4 1 vCPU 4 GB, High I/O 40 GB Windows Server 2012 R2 Standard 64-bit English (40 GB) |
| | ECS | 1 | x86 General computing s3.medium.4 1 vCPU 4 GB, High I/O 40 GB, Dynamic BGP Exclusive Billed by bandwidth 1 Mbit/s, Windows Windows Server 2012 R2 Standard 64-bit English |
| | IMS | 1 | Private image |
| | AS | 1 | N/A |
| | VPC | 1 | N/A |
| | HSS | 1 | N/A |
| | DEW | 1 | N/A |

| | | | |
|----------------------------------|-----|---|--|
| Exercises on networking services | ECS | 2 | x86 General computing s3.medium.4 1 vCPU 4 GB, High I/O 40 GB Windows Server 2012 R2 Standard 64-bit English (40 GB) |
| | ECS | 1 | x86 General computing-basic t6.small.1 1 vCPU 1 GB, High IO 40 GB CentOS 7.6 64-bit |
| | EIP | 2 | Dedicated Dynamic BGP Billed by bandwidth 1 Mbit/s |
| | ELB | 1 | Public network Dynamic BGP, 1 Mbit/s |
| | HSS | 1 | N/A |
| | DEW | 1 | N/A |
| Exercises on storage services | ECS | 1 | x86 General computing s3.medium.4 1 vCPU 4 GB; High I/O 40 GB Windows Server 2012 R2 Standard 64-bit English (40 GB) |
| | ECS | 1 | x86 General computing-basic t6.small.1 1 vCPU 1 GB, High IO 40 GB CentOS 7.6 64-bit |
| | EVS | 2 | 40 GB, High I/O |
| | SFS | 1 | 500 GB |
| | OBS | 1 | Pay per use |
| | HSS | 1 | N/A |
| | DEW | 1 | N/A |

| | | | |
|---------------------------|-----------|---|---|
| Exercises on O&M services | IAM | 1 | N/A |
| | Cloud Eye | 1 | N/A |
| | LTS | 1 | N/A |
| | CTS | 1 | N/A |
| Comprehensive exercise | VPC | 1 | N/A |
| | EIP | 2 | Dedicated Dynamic BGP Billed by bandwidth 1 Mbit/s |
| | RDS | 1 | RDS for MySQL 8.0 Active/standby General- enhanced II 1 vCPU 2 GB, Ultra-high I/O 40 GB |
| | ECS | 3 | x86 General computing-basic t6.small.1 1 vCPU 1 GB, High I/O 40 GB, Dynamic BGP Dedicated Billed by bandwidth 1 Mbit/s, CentOS CentOS 7.6 64-bit |
| | IMS | 1 | Private image |
| | AS | 1 | N/A |
| | ELB | 1 | Public network Dynamic BGP, 5 Mbit/s |
| | HSS | 1 | N/A |
| | DEW | 1 | N/A |

Contents

| | |
|---|------------|
| About This Document..... | 3 |
| Overview | 3 |
| Description | 3 |
| Knowledge Required | 3 |
| Lab Environment | 4 |
| 1 Getting Started with HUAWEI CLOUD | 10 |
| 1.1 Introduction..... | 10 |
| 1.1.1 About This Exercise..... | 10 |
| 1.1.2 Objectives | 10 |
| 1.2 Tasks..... | 10 |
| 1.2.1 Roadmap..... | 10 |
| 1.2.2 Registering Your HUAWEI CLOUD Account | 11 |
| 1.2.3 Creating an IAM User and Assigning Permissions..... | 15 |
| 1.2.4 Creating and Configuring a VPC | 21 |
| 2 Compute Services | 24 |
| 2.1 Introduction | 24 |
| 2.1.1 About This Exercise | 24 |
| 2.1.2 Objectives | 24 |
| 2.2 Tasks..... | 24 |
| 2.2.1 Roadmap..... | 24 |
| 2.2.2 ECS Lifecycle Management..... | 25 |
| 2.2.3 Creating a Linux System Disk Image from an ECS..... | 54 |
| 2.2.4 AS Operations..... | 60 |
| 2.2.5 Deleting Resources..... | 70 |
| 3 Networking Services | 71 |
| 3.1 Introduction..... | 71 |
| 3.1.1 About This Exercise | 71 |
| 3.1.2 Objectives | 71 |
| 3.2 Tasks..... | 72 |
| 3.2.1 Roadmap..... | 72 |
| 3.2.2 Creating VPCs | 73 |
| 3.2.3 Buying ECSS | 78 |
| 3.2.4 Verifying Network Service Functions | 81 |
| 3.2.5 Deleting Resources..... | 114 |
| 4 Storage Services | 115 |
| 4.1 EVS | 115 |

| | |
|--|------------|
| 4.1.1 Introduction..... | 115 |
| 4.1.2 Tasks | 115 |
| 4.2 OBS | 141 |
| 4.2.1 Introduction | 141 |
| 4.2.2 Tasks..... | 141 |
| 4.2.3 Deleting Resources..... | 152 |
| 4.3 SFS..... | 153 |
| 4.3.1 Introduction..... | 153 |
| 4.3.2 Tasks..... | 153 |
| 4.3.3 Deleting Resources..... | 170 |
| 5 O&M Services | 172 |
| 5.1 Introduction | 172 |
| 5.1.1 About This Exercise | 172 |
| 5.1.2 Objectives | 172 |
| 5.2 Tasks..... | 173 |
| 5.2.1 Configuring CTS Key Event Notifications..... | 173 |
| 5.2.2 Performing a key operation in VPC and verifying CTS functions | 179 |
| 5.2.3 Use Cloud Eye to Monitor an ECS | 180 |
| 5.2.4 Viewing ECS Logs | 186 |
| 5.3 Deleting Resources..... | 194 |
| 6 Comprehensive Exercise: Deploying an Enterprise Website on HUAWEI CLOUD | 195 |
| 6.1 Background..... | 195 |
| 6.2 Solution | 195 |
| 6.3 Preparations..... | 196 |
| 6.3.1 Logging In to HUAWEI CLOUD | 196 |
| 6.3.2 Creating a VPC | 197 |
| 6.3.3 Creating and Configuring a Security Group..... | 199 |
| 6.3.4 Buying an ECS | 200 |
| 6.3.5 Buying an RDS DB Instance | 203 |
| 6.4 Setting Up the Linux, Apache, MySQL, PHP (LAMP) Environment..... | 205 |
| 6.4.1 Installing LAMP | 205 |
| 6.4.2 Creating a Database for WordPress..... | 211 |
| 6.4.3 Installing WordPress..... | 213 |
| 6.5 Achieving High Availability for Web Servers | 217 |
| 6.5.1 Creating a Shared Load Balancer..... | 217 |
| 6.5.2 Creating an Image | 221 |
| 6.5.3 Configuring AS | 223 |
| 6.6 Visiting the Website | 230 |
| Monitoring Resources..... | 231 |
| 6.7 Deleting Resources..... | 232 |
| 6.7.1 Deleting ECSs..... | 232 |

| | |
|---|------------|
| 6.7.2 Deleting the RDS DB Instance | 234 |
| 6.7.3 Deleting the Image | 234 |
| 6.7.4 Deleting the Load Balancer | 235 |
| 6.7.5 Deleting AS Resources | 235 |
| 6.7.6 Deleting VPC Resources | 236 |
| 7 Acronyms and Abbreviations | 239 |

1

Getting Started with HUAWEI CLOUD

1.1 Introduction

ESTE CAPÍTULO É MERAMENTE INFORMATIVO. AS CONTAS NECESSÁRIAS PARA AS ATIVIDADES DE LABORATÓRIO SERÃO FORNECIDAS PELO INSTRUTOR

1.1.1 About This Exercise

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

- Learn about HUAWEI CLOUD.
- Learn how to register a HUAWEI CLOUD account.
- Learn how to purchase and release HUAWEI CLOUD resources.

1.2 Tasks

1.2.1 Roadmap

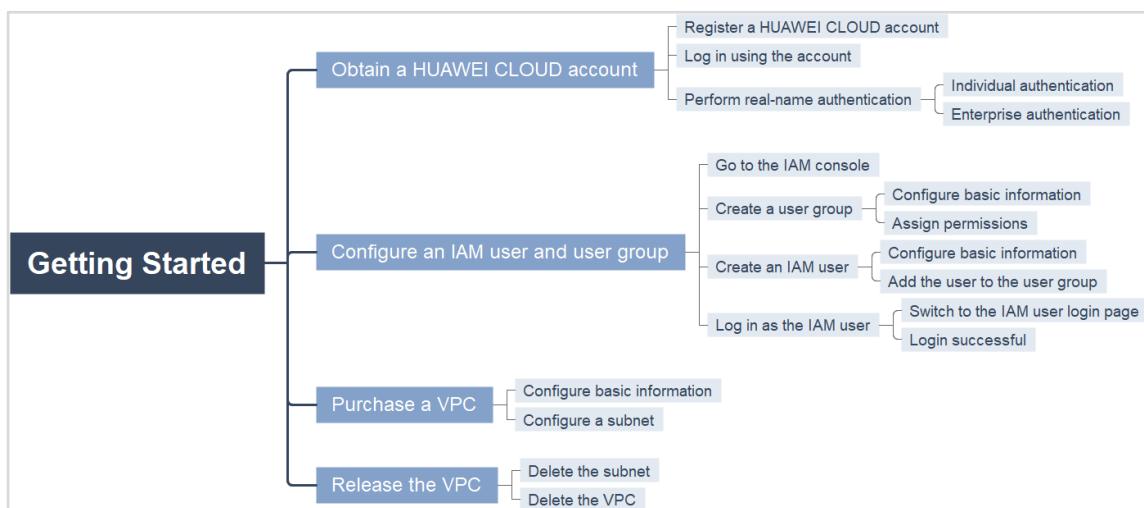


Figure 1-1 Configuration flowchart

1.2.2 Registering Your HUAWEI CLOUD Account

Your account lets you use HUAWEI CLOUD resources and pay for their use.

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

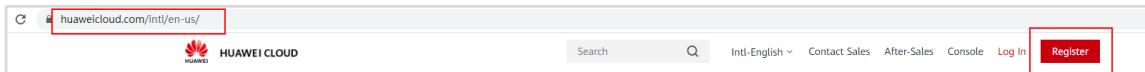


Figure 1-2 Visiting the HUAWEI CLOUD official website

Enter the information required.

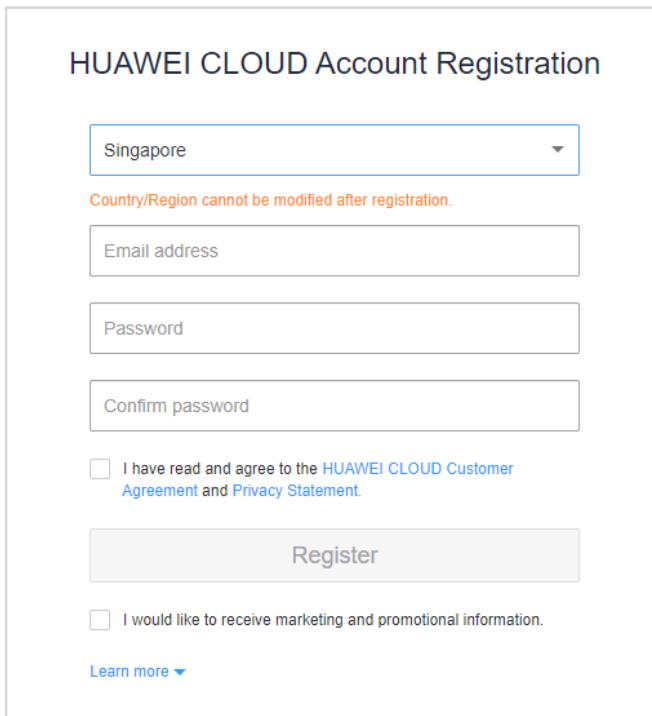
A screenshot of the "HUAWEI CLOUD Account Registration" form. It includes a dropdown menu set to "Singapore", a note about country/region being不可修改 (non-modifiable), and four input fields for "Email address", "Password", "Confirm password", and "Marketing consent". There is also a "Learn more" link and a "Register" button.

Figure 1-3 Registering a HUAWEI CLOUD account

Log in to HUAWEI CLOUD using your new account.

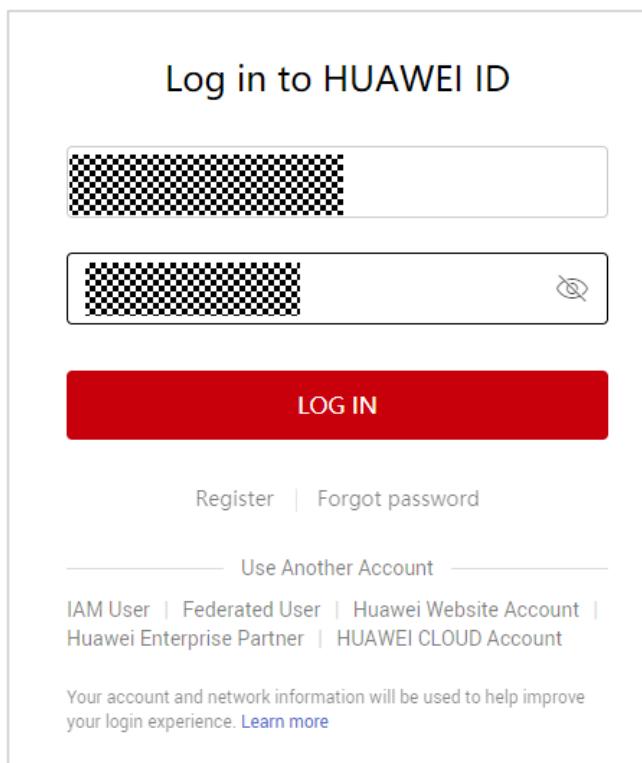


Figure 1-4 Logging in to HUAWEI CLOUD

Click Console in the upper right.

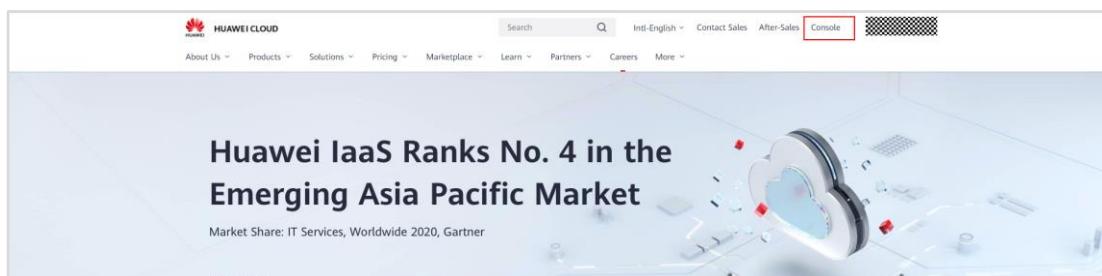


Figure 1-5 Accessing the console

Hover over your username in the upper right and choose Basic Information.

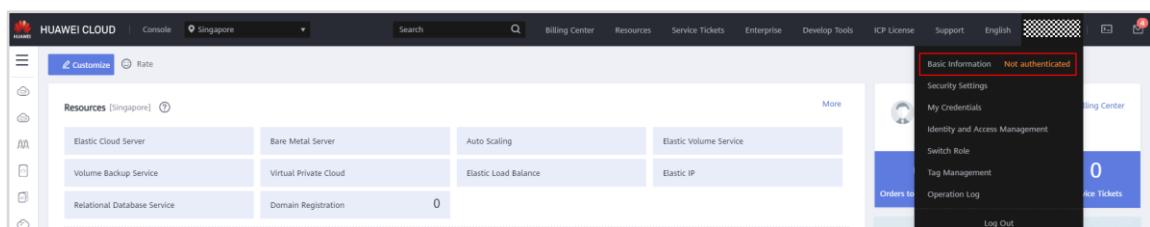
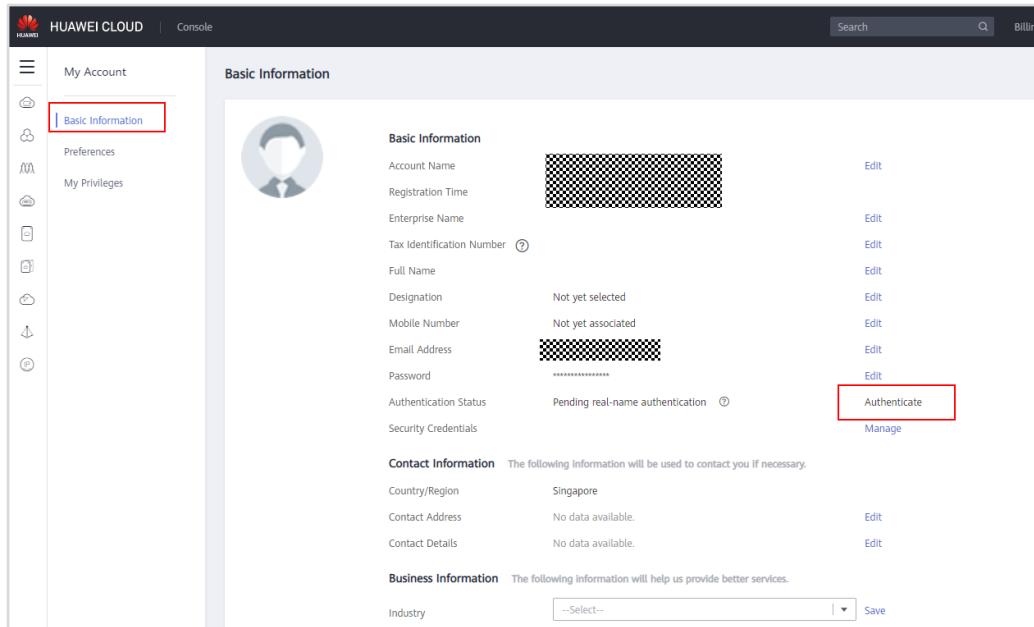


Figure 1-6 Going to My Account

Click Authenticate next to Authentication Status.



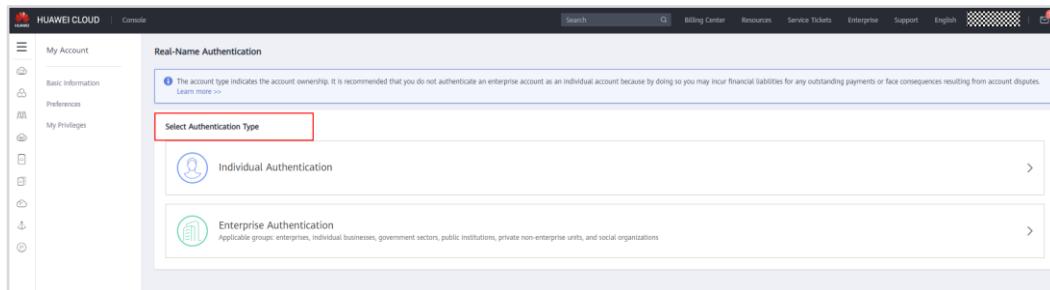
The screenshot shows the HUAWEI CLOUD Console interface. On the left, there's a sidebar with icons for My Account, Basic Information (which is selected and highlighted with a red box), Preferences, and My Privileges. The main content area is titled 'Basic Information' and contains a profile picture placeholder. Below it is a table of account details:

| Basic Information | |
|---------------------------|----------------------------------|
| Account Name | [Placeholder] |
| Registration Time | [Placeholder] |
| Enterprise Name | [Placeholder] |
| Tax Identification Number | [Placeholder] |
| Full Name | [Placeholder] |
| Designation | Not yet selected |
| Mobile Number | Not yet associated |
| Email Address | [Placeholder] |
| Password | [Placeholder] |
| Authentication Status | Pending real-name authentication |
| Security Credentials | [Placeholder] |

Below this, there are sections for 'Contact Information' and 'Business Information'. At the bottom right, there are 'Edit' and 'Manage' buttons for the status, and a 'Save' button. A red box highlights the 'Authenticate' button next to the status field.

Figure 1-7 Clicking Authenticate

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

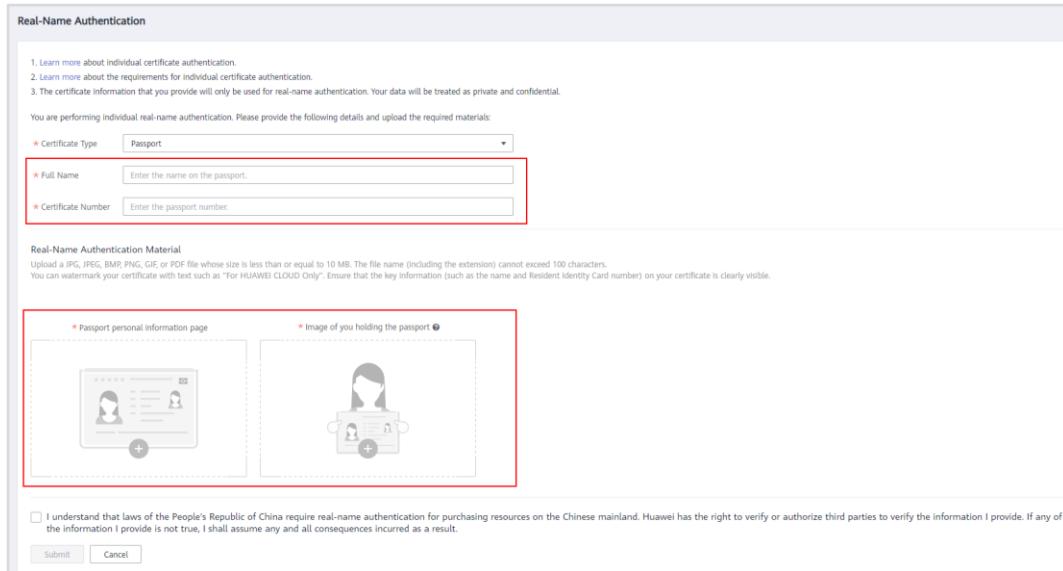


The screenshot shows the 'Real-Name Authentication' page. The sidebar includes 'My Account', 'Basic Information' (highlighted with a red box), 'Preferences', and 'My Privileges'. The main content area is titled 'Real-Name Authentication' and contains a note about account ownership. Below is a section titled 'Select Authentication Type' with two options:

- Individual Authentication** (selected, indicated by a blue background)
- Enterprise Authentication** (applicable groups: enterprises, individual businesses, government sectors, public institutions, private non-enterprise units, and social organizations)

Figure 1-8 Selecting an authentication type

Complete the information required.



The screenshot shows the 'Real-Name Authentication' page. At the top, there are three informational links: 'Learn more about individual certificate authentication.', 'Learn more about the requirements for individual certificate authentication.', and 'The certificate information that you provide will only be used for real-name authentication. Your data will be treated as private and confidential.' Below these, a note says 'You are performing individual real-name authentication. Please provide the following details and upload the required materials:'. A dropdown menu shows 'Certificate Type' set to 'Passport'. Below it, two input fields are shown: 'Full Name' (placeholder: 'Enter the name on the passport.') and 'Certificate Number' (placeholder: 'Enter the passport number.'). A note below the fields specifies file types and size limits. Two large red-bordered boxes are overlaid on the page, highlighting the 'Passport personal information page' and 'Image of you holding the passport' upload fields. At the bottom, a checkbox states: 'I understand that laws of the People's Republic of China require real-name authentication for purchasing resources on the Chinese mainland. Huawei has the right to verify or authorize third parties to verify the information I provide. If any of the information I provide is not true, I shall assume any and all consequences incurred as a result.' Below the checkbox are 'Submit' and 'Cancel' buttons.

Figure 1-9 Individual authentication

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

FIM DO CAPÍTULO INFORMATIVO !!!

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.

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

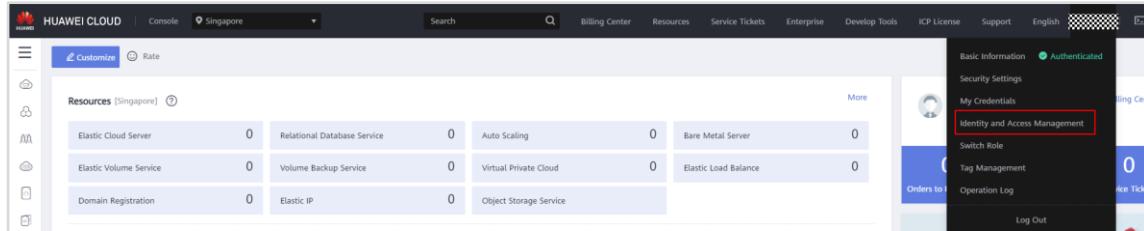


Figure 1-10 Choosing Identity and Access Management

Choose User Groups in the navigation pane and click Create User Group.

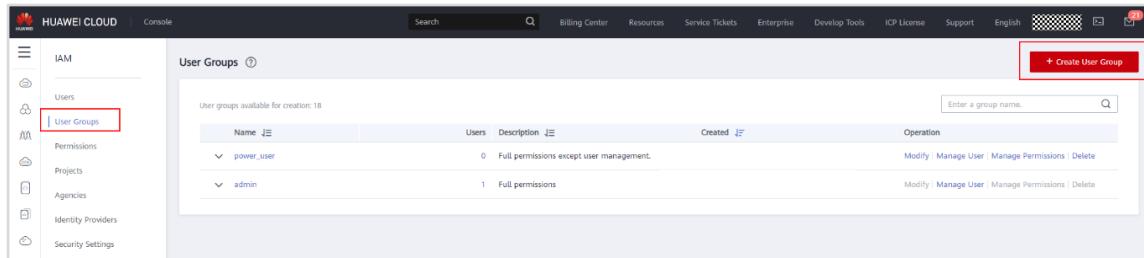


Figure 1-11 Creating a user group

Enter a user group name and click OK.

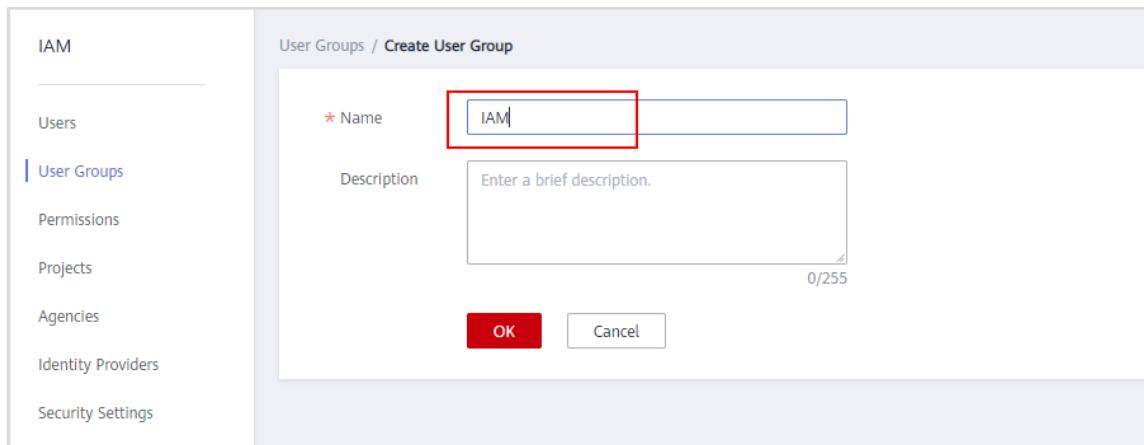


Figure 1-12 Configuring the user group information

Click Manage Permissions for the user group you created.

| Name | Users | Description | Created | Operation |
|------------|-------|--|---------------------|--|
| IAM | 0 | -- | 2023-09-01 10:00:00 | Modify Manage User Manage Permissions Delete |
| power_user | 0 | Full permissions except user management. | 2023-09-01 10:00:00 | Modify Manage User Manage Permissions Delete |
| admin | 1 | Full permissions | 2023-09-01 10:00:00 | Modify Manage User Manage Permissions Delete |

Figure 1-13 Clicking Manage Permissions

Click Assign Permissions.

The screenshot shows the 'Assign Permissions' tab for the 'admin' user group. It includes fields for Policy/Role Name, Type, Description, Project [Region], and Operation. Below the table, it says 'No data available.'

Figure 1-14 Permissions tab page

Under Scope, click Region-specific projects, and select **LA-SaoPaulo. In the Permissions section, search for **IAM**, select **Tenant Guest** and **Tenant Administrator**, and click **OK**.**

The screenshot shows the 'Region-based Authorization' page. Under 'Scope', the 'Region-specific projects' option is selected, with 'ap-southeast-3 [AP-Singapor...]' listed in the dropdown. In the 'Permissions' section, two items are selected: 'Tenant Guest' (Type: System-defined role) and 'Tenant Administrator' (Type: System-defined role).

Figure 1-15 Assigning permissions

Go to the Users page and click Create User in the upper right.

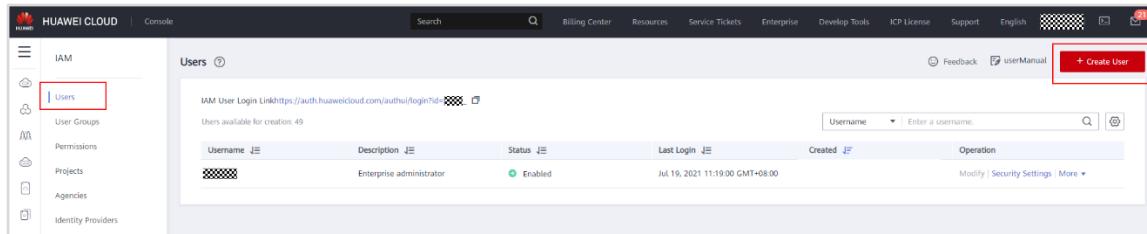


Figure 1-16 Creating a user

Configure the user information and click Next.

- **Username:** a custom username. You can input your name. Here we'll use **yourname** for example.
- **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 1-17 Configuring the basic user information

Select the user group you created and click Create.

Figure 1-18 Adding the user to the created user group

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

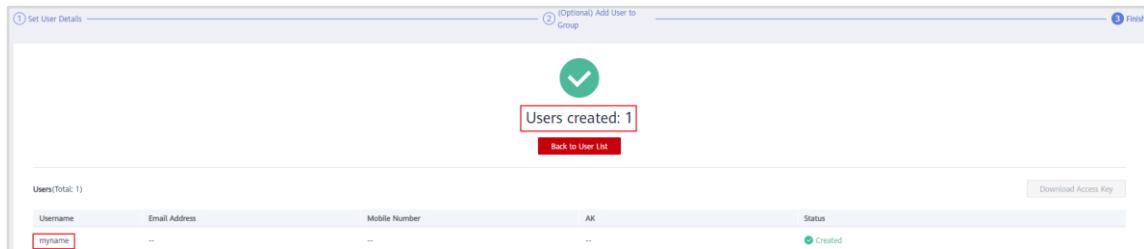


Figure 1-19 User created successfully

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

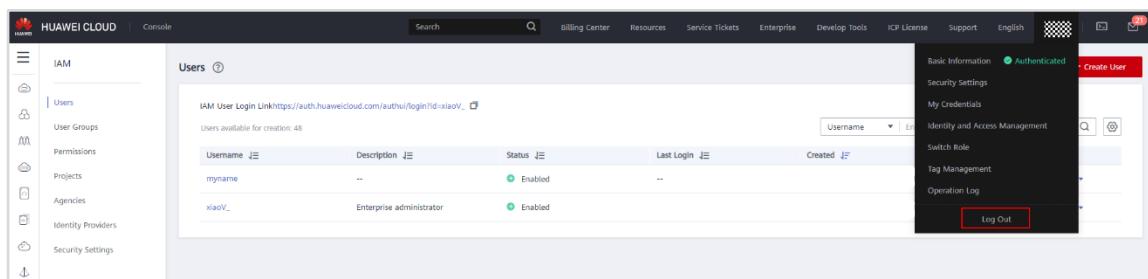


Figure 1-20 Logging out of the account

Click IAM User.

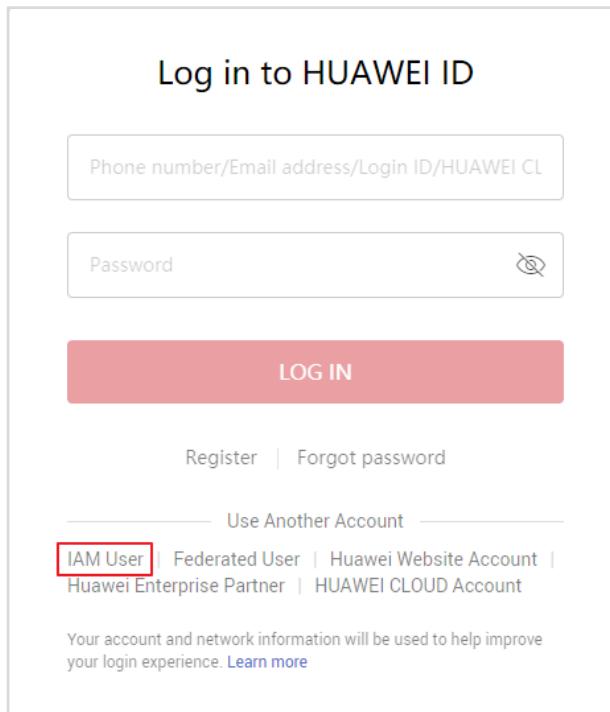
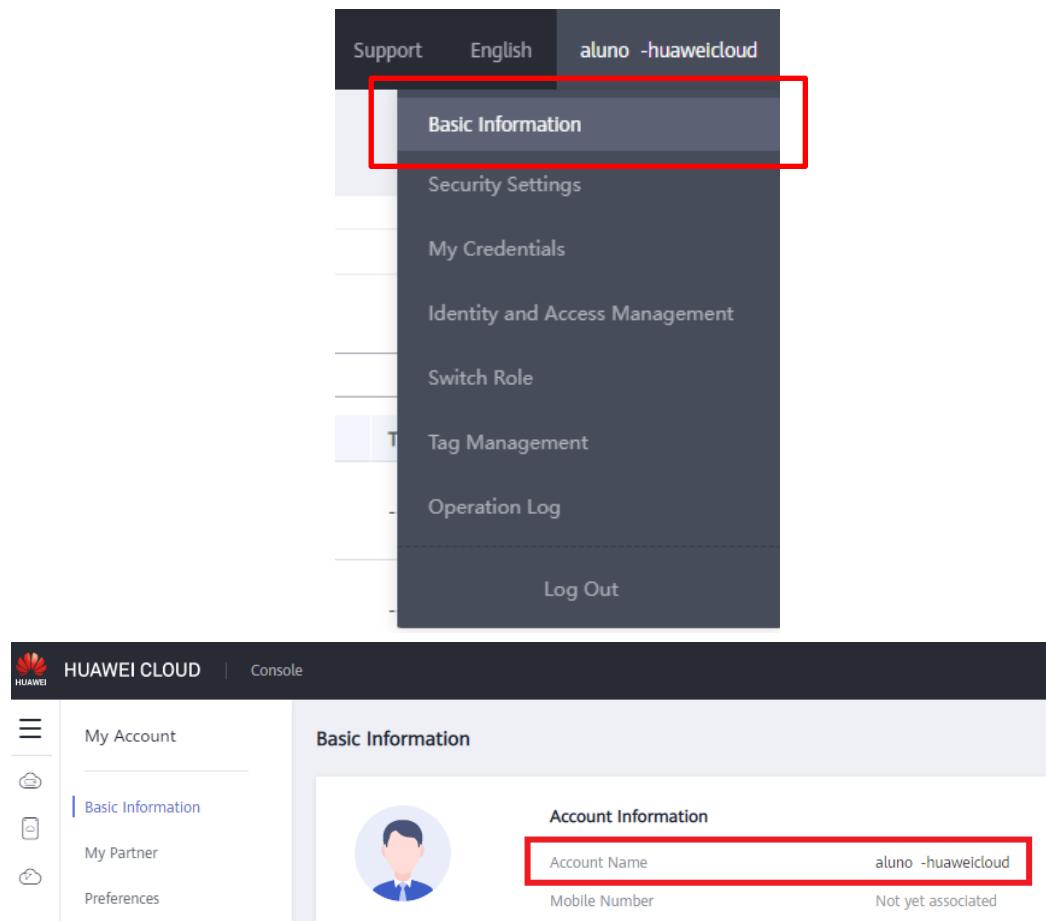


Figure 1-21 Clicking IAM User

Log in as the IAM user you created.

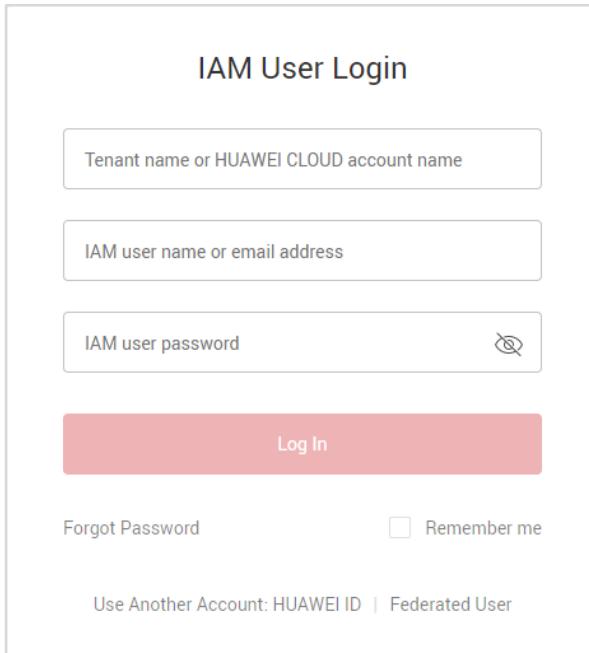
To check this:



The screenshot shows the HUAWEI CLOUD Console interface. At the top, there is a navigation bar with 'Support', 'English', and a user dropdown labeled 'aluno -huaweicloud'. A red box highlights the 'Basic Information' option in the dropdown menu. Below the navigation bar, there is a sidebar with 'My Account' and 'Basic Information' selected. The main content area displays 'Basic Information' with a placeholder profile picture and 'Account Information' table. The 'Account Name' row is highlighted with a red box, showing the value 'aluno -huaweicloud'. The 'Mobile Number' row shows 'Not yet associated'.

| Account Information | |
|---------------------|--------------------|
| Account Name | aluno -huaweicloud |
| Mobile Number | Not yet associated |

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



The image shows the 'IAM User Login' interface. It consists of three input fields: 'Tenant name or HUAWEI CLOUD account name', 'IAM user name or email address', and 'IAM user password' (with a visibility toggle icon). Below these is a large red 'Log In' button. At the bottom left is a 'Forgot Password' link, and at the bottom right is a 'Remember me' checkbox. A note at the bottom center says 'Use Another Account: HUAWEI ID | Federated User'.

Figure 1-22 Logging in as an IAM user

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.

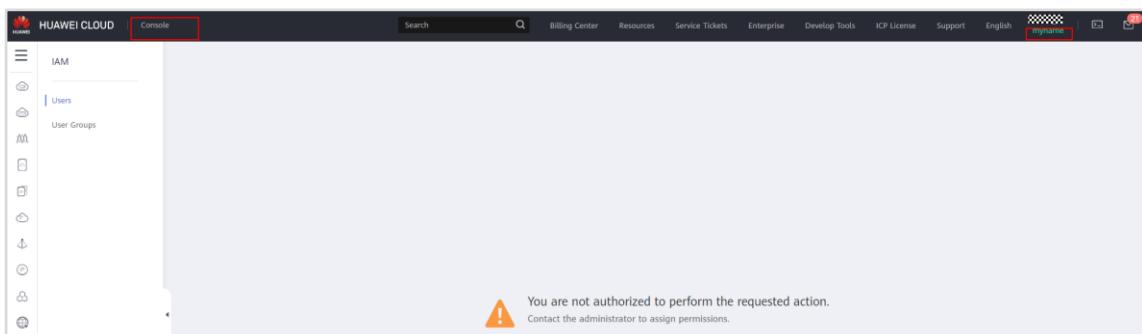


Figure 1-23 IAM user login successful

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.

Log out of the IAM user account.

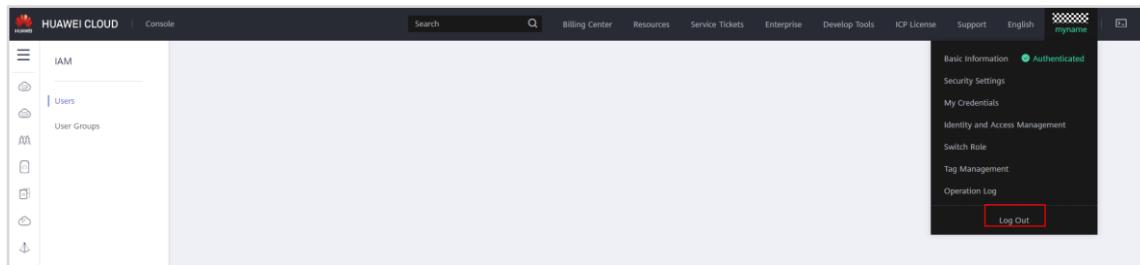


Figure 1-24 Logging out of the IAM user account

Log in with your HUAWEI CLOUD account and choose Virtual Private Cloud in the left pane.

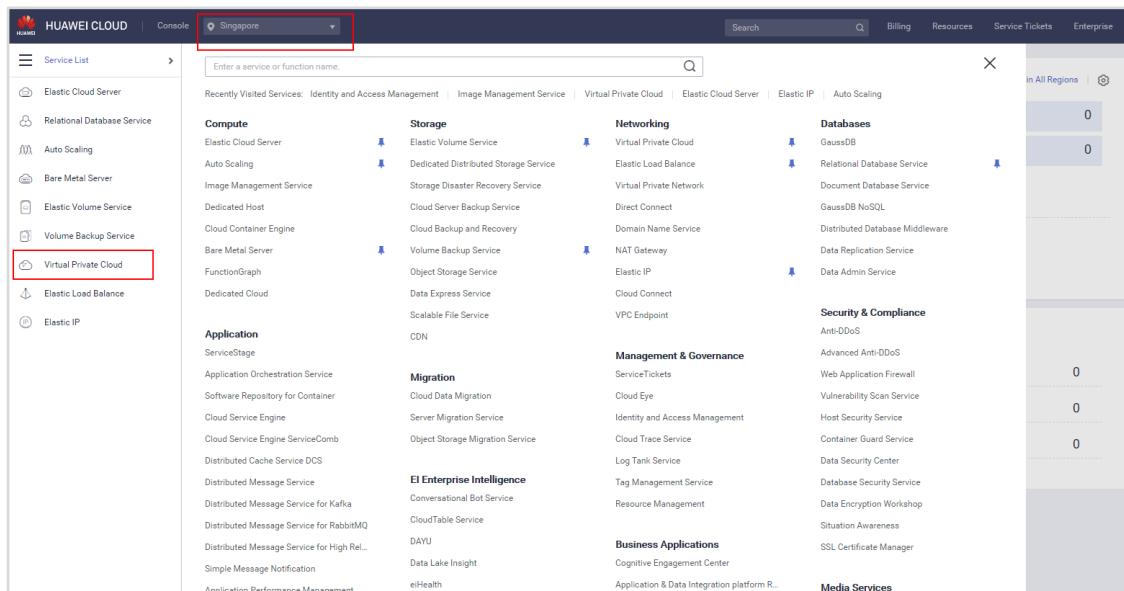


Figure 1-25 Choosing Virtual Private Cloud

Click Create VPC.

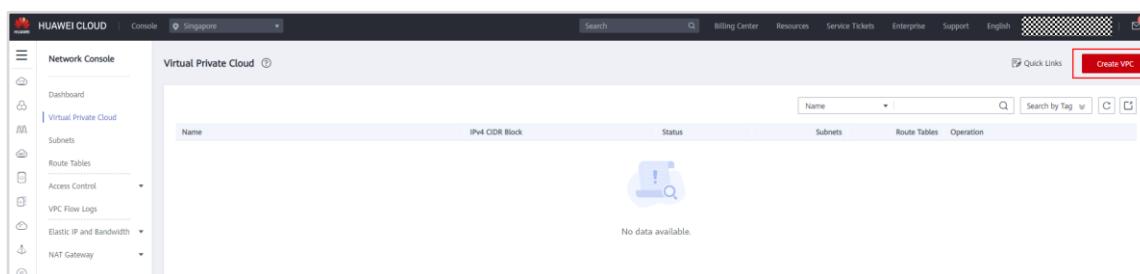
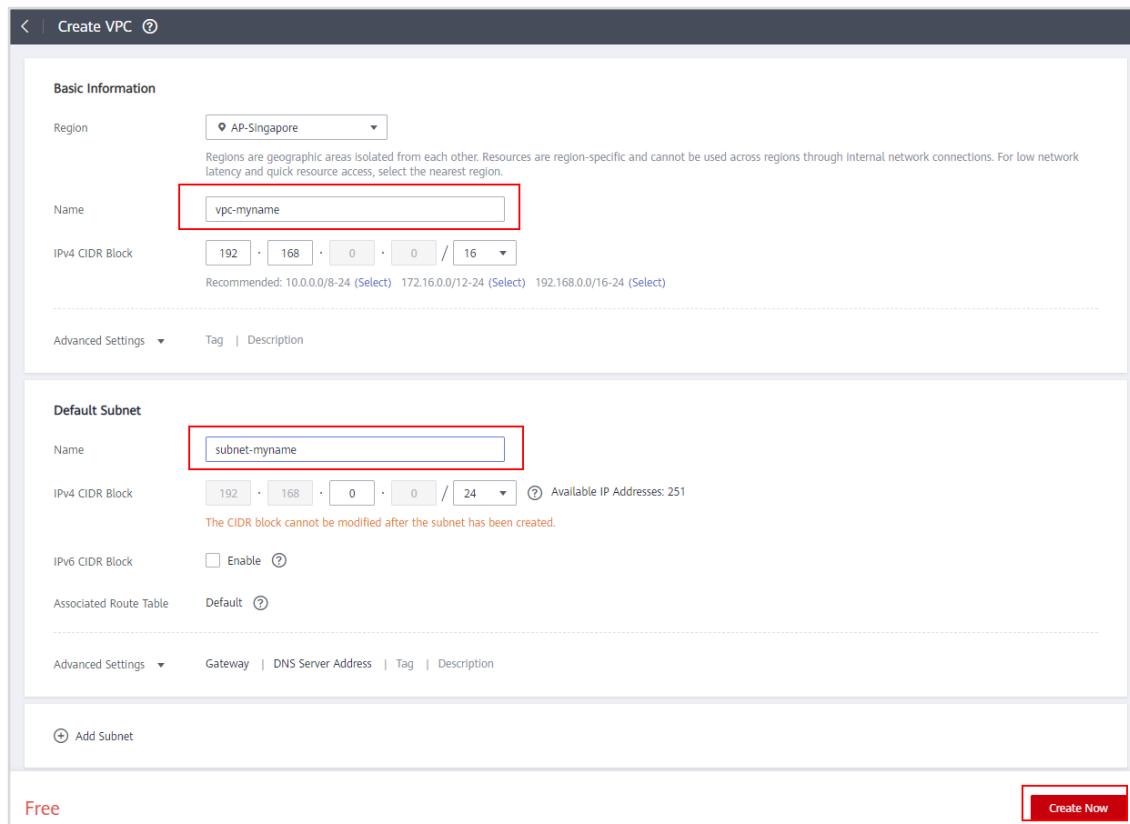


Figure 1-26 Creating a VPC

Configure the VPC parameters and click Create Now.

- **Region:** LA-SaoPaulo
- **Name:** a custom name (exemplo: vpc-production)
- Retain the default settings for other parameters.



The screenshot shows the 'Create VPC' wizard interface. The 'Basic Information' step is active, displaying fields for Region (AP-Singapore), Name (vpc-myname), and IPv4 CIDR Block (192.168.0.0/16). The 'Default Subnet' step is also visible, showing a subnet named 'subnet-myname' with an IPv4 CIDR Block of 192.168.0.0/24. A red box highlights the 'Name' field in both sections. The 'Create Now' button is at the bottom right.

Figure 1-27 Configuring the VPC

Delete the subnet of the VPC.

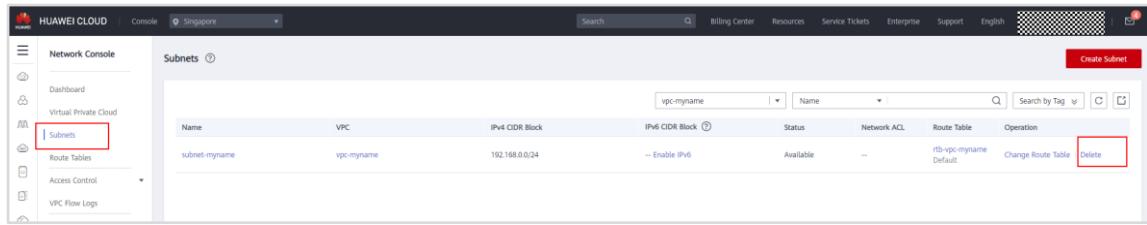


Figure 1-28 Deleting the subnet

Delete the VPC.

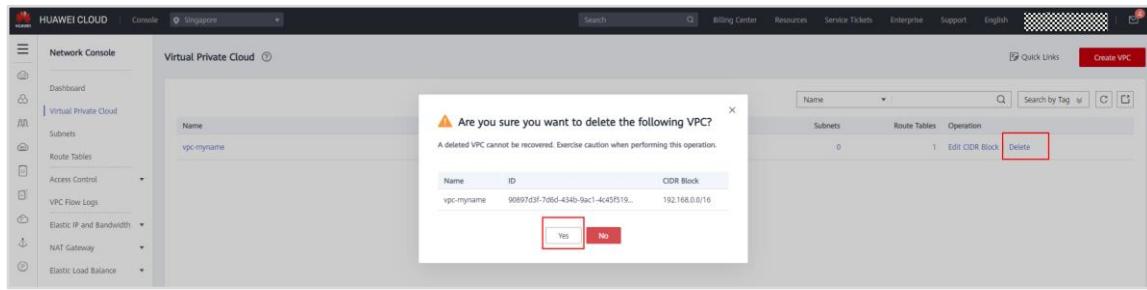


Figure 1-29 Deleting the VPC

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.

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 exercise walks you through how to create and log in to ECSs, modify the ECS specifications, create private Windows and Linux images, create sharable images, and scale resources flexibly.

2.1.2 Objectives

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

- ECS
- IMS
- AS

2.2 Tasks

2.2.1 Roadmap

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

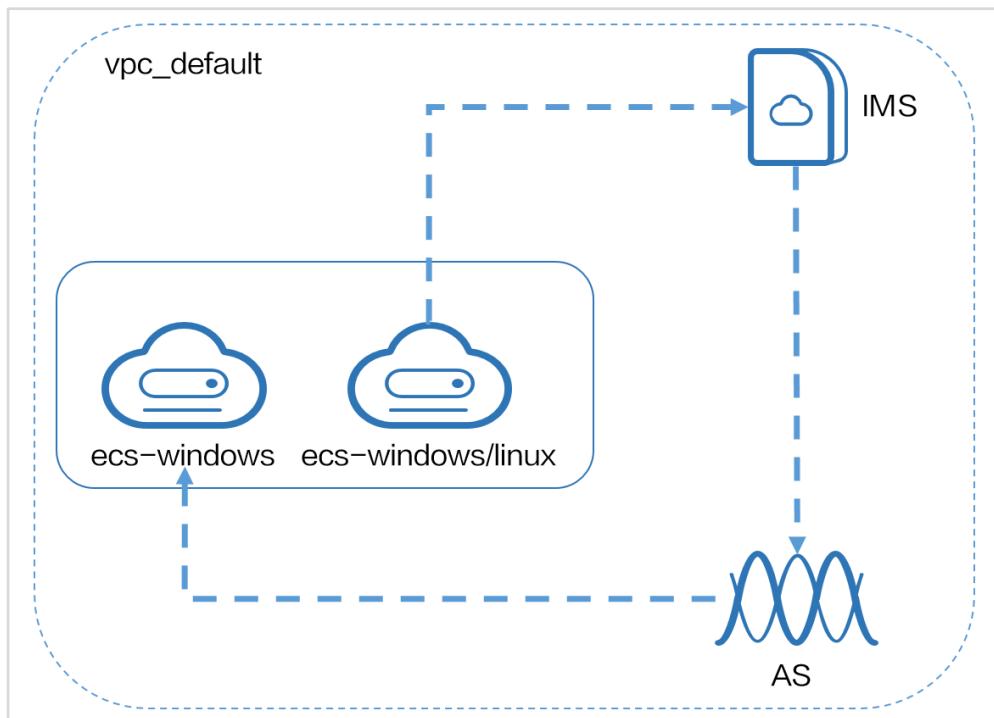


Figure 2-1 Topology

2.2.2 ECS Lifecycle Management

In this exercise, we will create both Windows and Linux ECSSs.

2.2.2.1 Creating Two Types of ECSSs

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

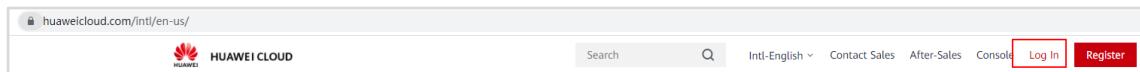


Figure 2-2 Logging in to HUAWEI COULD

Enter your username and password to log in, click Console and choose the **LA-SaoPaulo** region.

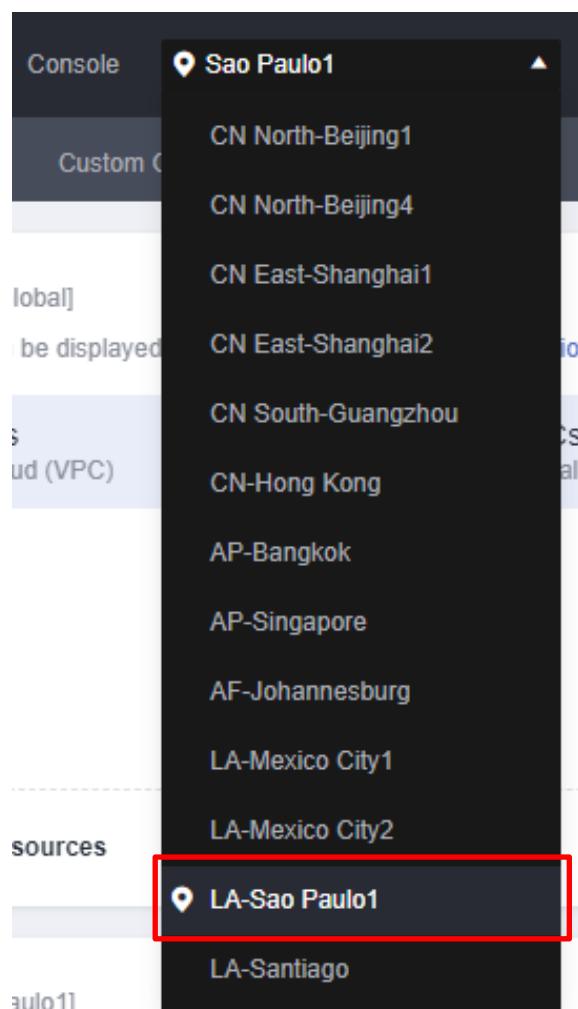


Figure 2-3 Choosing **LA-SaoPaulo**

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

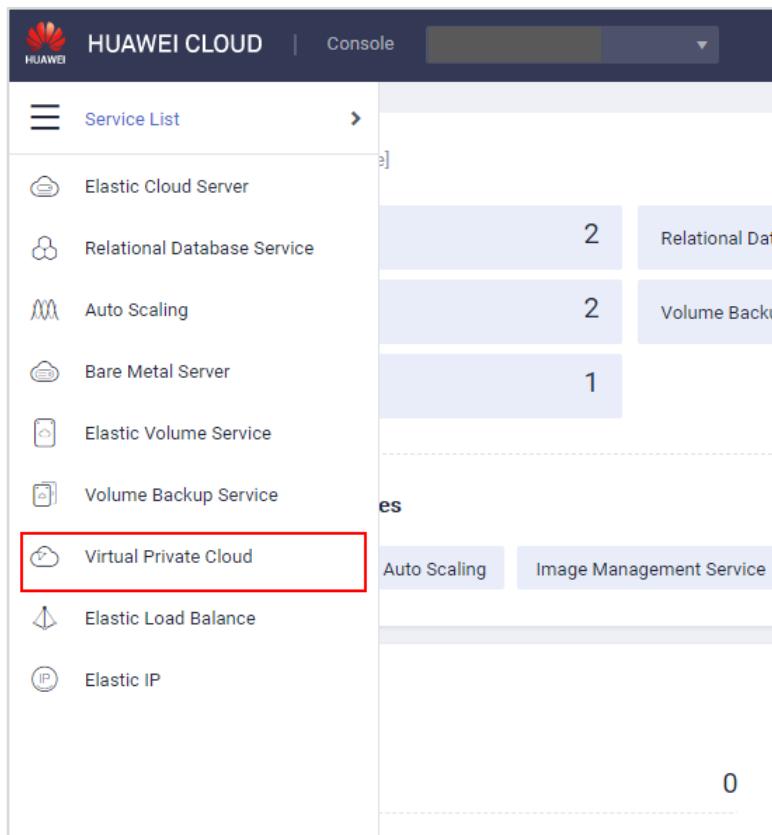


Figure 2-4 Choosing Virtual Private Cloud

Click Create VPC.

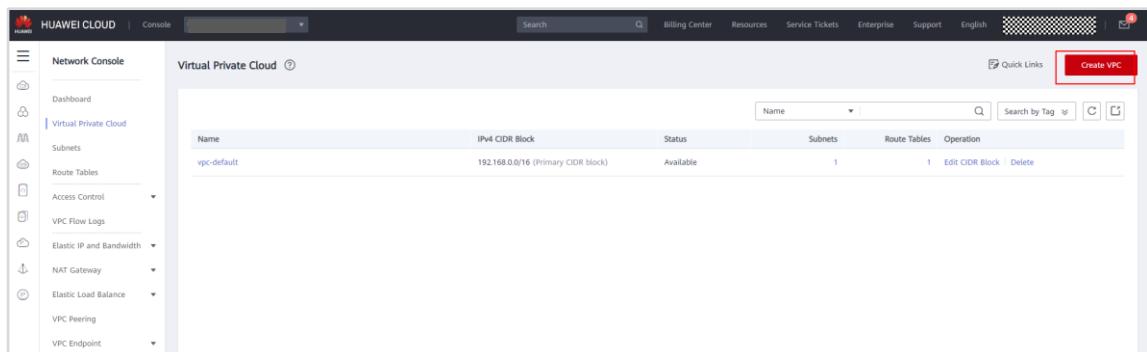


Figure 2-5 Create VPC

Configure the VPC parameters as follows and click Create Now.

- Region: **LA-SaoPaulo**
- Name: Enter a name.
- Retain the default settings for other parameters.

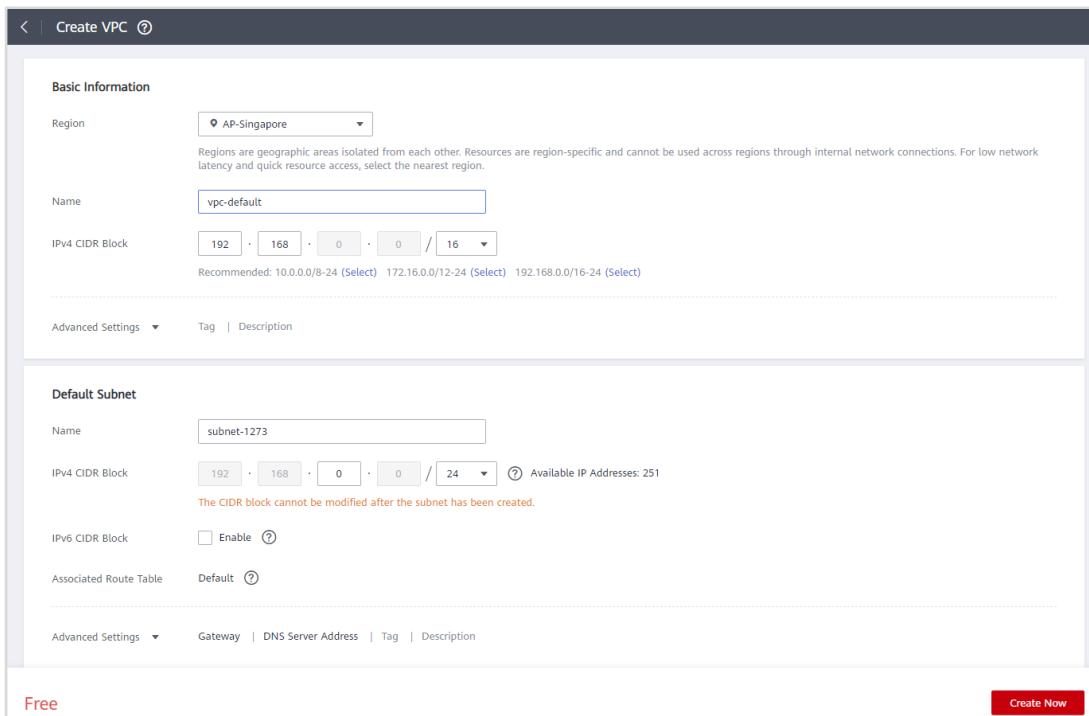


Figure 2-6 Configuring the VPC

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

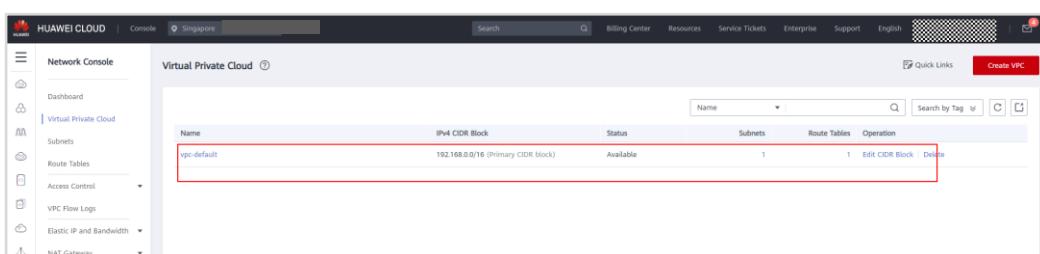


Figure 2-7 Viewing the VPC

Click Service List on the left, and search for Data Encryption Workshop to configure a key pair for the ECS.

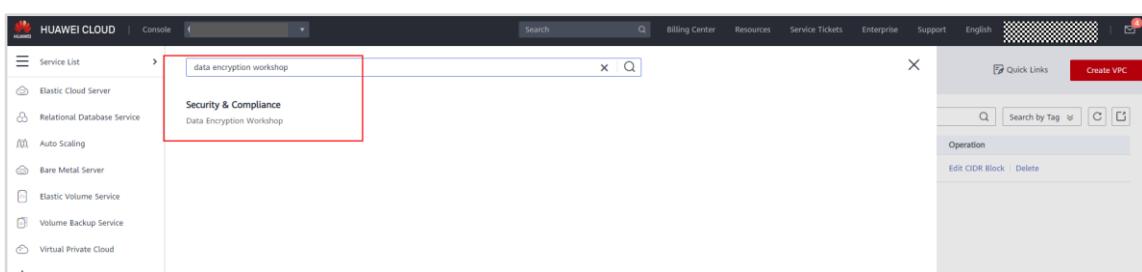
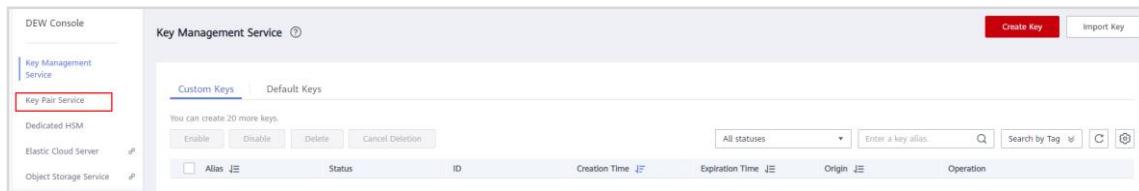


Figure 2-8 Data Encryption Workshop

Choose Key Pair Service on the left.

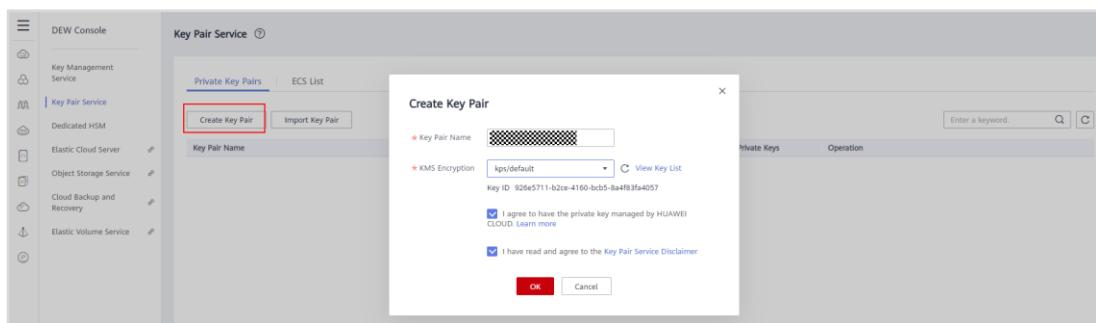


The screenshot shows the HUAWEI CLOUD DEW Console. On the left sidebar, under 'Key Management Service', the 'Key Pair Service' option is highlighted with a red box. The main panel displays the 'Key Management Service' interface with tabs for 'Custom Keys' and 'Default Keys'. It includes buttons for 'Create Key' and 'Import Key', and a search bar. Below the tabs, there are buttons for 'Enable', 'Disable', 'Delete', and 'Cancel Deletion'. A table lists key pairs with columns for 'Alias', 'Status', 'ID', 'Creation Time', 'Expiration Time', 'Origin', and 'Operation'. There are also filters for 'All statuses', 'Enter a key alias', 'Search by Tag', and a refresh button.

Figure 2-9 Key Pair Service

Click Create Key Pair, configure parameters, and click OK.

The key pair file is automatically downloaded to your local PC. The key pair file will be used to obtain the password to log in to the ECS. Keep the file secure.



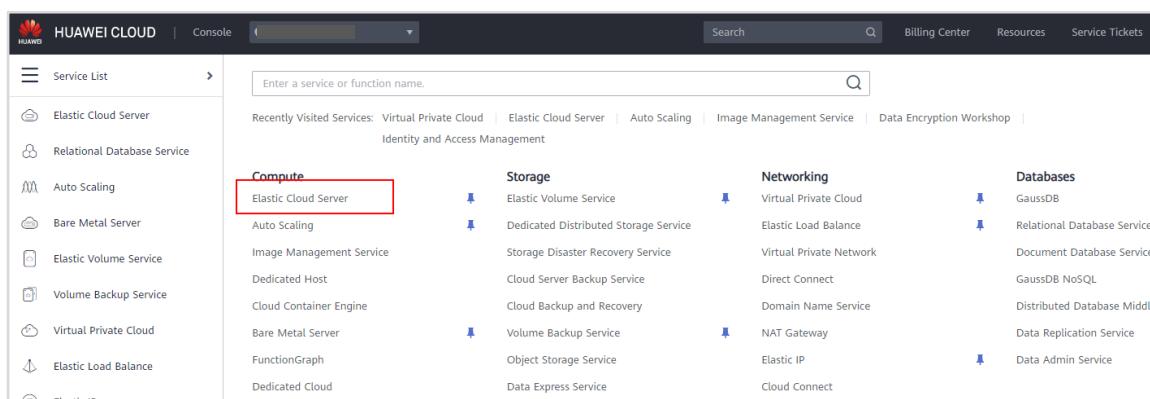
The screenshot shows a 'Create Key Pair' dialog box. On the left, the 'Key Pair Service' interface is visible with the 'Create Key Pair' button highlighted in red. The dialog itself has a title 'Create Key Pair'. It contains fields for 'Key Pair Name' (set to 'kps/default') and 'KMS Encryption' (set to 'kps/default'). There are two checkboxes at the bottom: 'I agree to have the private key managed by HUAWEI CLOUD' and 'I have read and agree to the Key Pair Service Disclaimer'. Both checkboxes are checked. At the bottom right are 'OK' and 'Cancel' buttons.

Figure 2-10 Create Key Pair



Figure 2-11 Downloading the key pair file

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



The screenshot shows the HUAWEI CLOUD DEW Console 'Service List' page. On the left, a sidebar lists various services: Elastic Cloud Server, Relational Database Service, Auto Scaling, Bare Metal Server, Elastic Volume Service, Volume Backup Service, Virtual Private Cloud, and Elastic Load Balance. The 'Compute' section is expanded, showing 'Elastic Cloud Server' highlighted with a red box. Other options in this section include Auto Scaling, Image Management Service, Dedicated Host, Cloud Container Engine, Bare Metal Server, FunctionGraph, and Dedicated Cloud. To the right, there are sections for Storage (Elastic Volume Service, Dedicated Distributed Storage Service, Storage Disaster Recovery Service, Cloud Server Backup Service, Cloud Backup and Recovery, Volume Backup Service, Object Storage Service, Data Express Service), Networking (Virtual Private Cloud, Elastic Load Balance, Virtual Private Network, Direct Connect, Domain Name Service, NAT Gateway, Elastic IP, Cloud Connect), and Databases (GaussDB, Relational Database Service, Document Database Service, GaussDB NoSQL, Distributed Database Middle, Data Replication Service, Data Admin Service).

Figure 2-12 Choosing Elastic Cloud Server

Click Buy ECS.

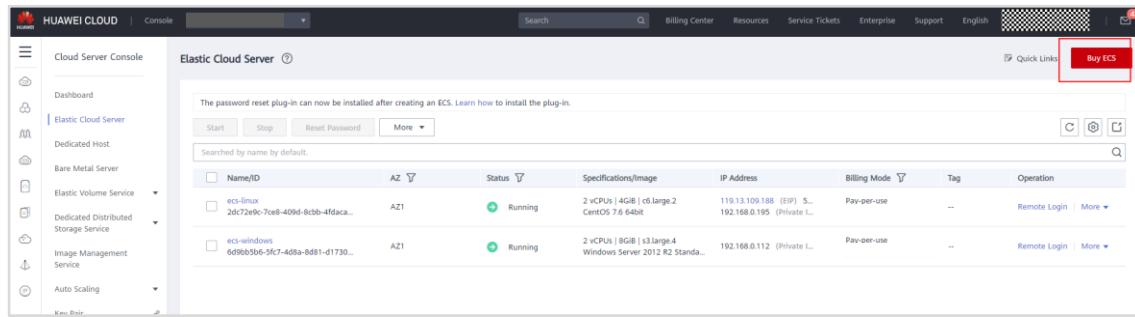


Figure 2-13 Buy ECS

Configure basic settings as follows:

- Billing Mode: Pay-per-use**
- Region: LA-SaoPaulo**
- AZ: Random**
- CPU Architecture: x86**
- Specifications: General computing, s3.medium.4, 1 vCPU | 4 GB (configure based on your requirements)**

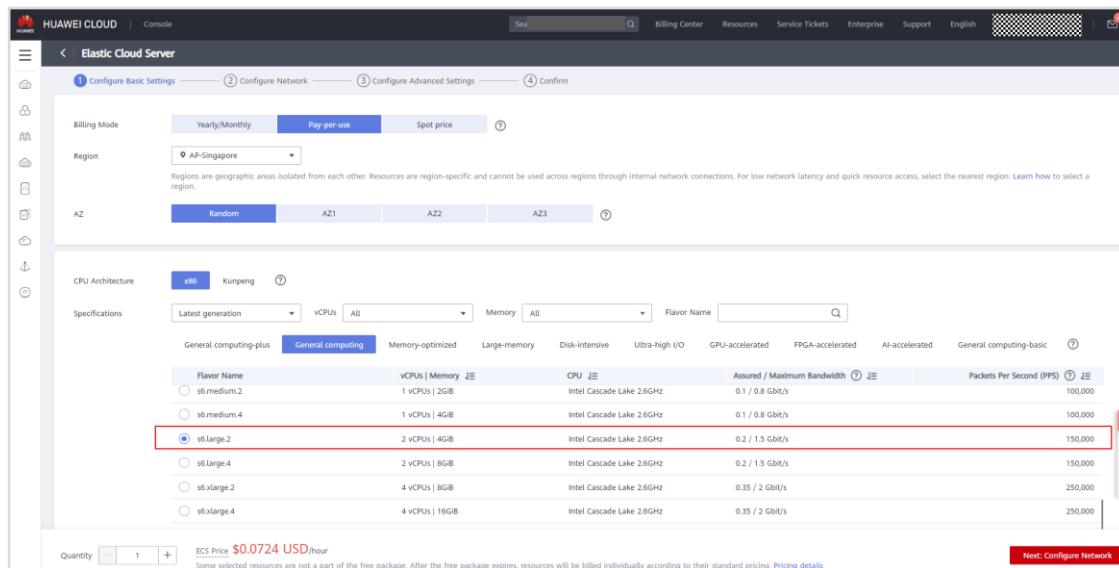


Figure 2-14 Configure Basic Settings

- **Image:** Public Image, Windows, **Windows Server 2012 R2 Standard 64bit English (40 GB)**
- **Host Security:** Select **Enable** (basic edition for this exercise) – if exists.
- **System Disk:** High I/O, 40 GB

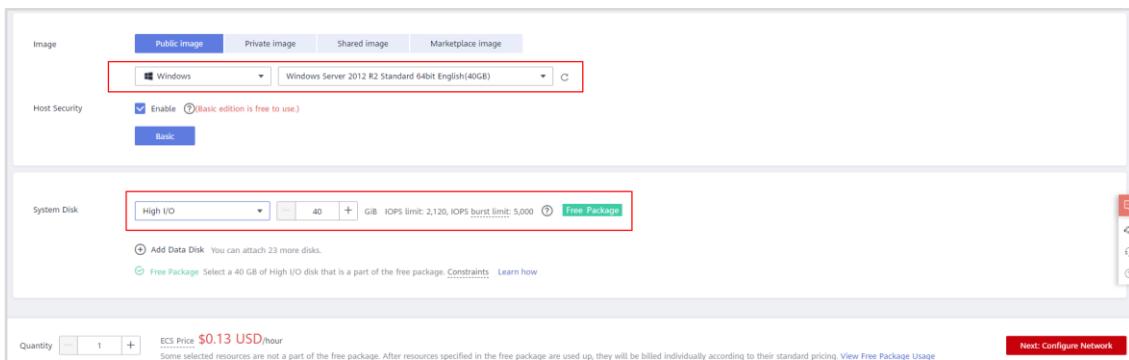


Figure 2-15 Configure Basic Settings

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.

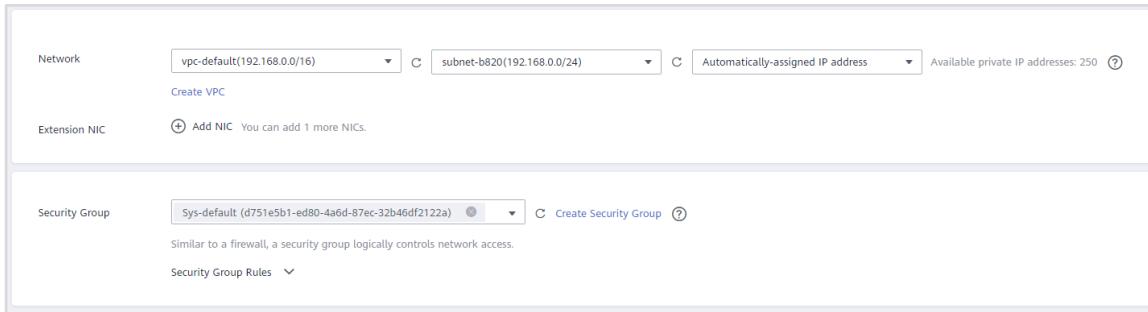


Figure 2-16 Configure Network

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

- ECS Name:** ecs-windows (Change as required.)
- Login Mode:** Key pair
- Key Pair:** Choose the created key pair.
- Cloud Backup and Recovery:** Not required
- ECS Group (Optional):** Retain the default settings.
- Advanced Options:** Retain the default settings.

The screenshot shows the 'Configure Advanced Settings' page. The 'ECS Name' field contains 'ecs-windows'. The 'Login Mode' section has 'Key pair' selected. Under 'Key Pair', there is a dropdown set to 'KeyPair-XXXX' and a checkbox checked with the text: 'I acknowledge that I have the private key file KeyPair-b1fd.pem and that I will not be able to log in to my ECS without this file.' Below this is a note: 'After a Linux ECS is created, use this key pair to log in to the ECS. After a Windows ECS is created, locate the row that contains the ECS in the ECS list, click Get Password in the Operation column, and use this key pair to obtain the ECS login password.' The 'Cloud Backup and Recovery' section has 'Not required' selected. The 'ECS Group (Optional)' section has 'Anti-affinity' selected. At the bottom, there are buttons for 'Create new', 'Use existing', and 'Not required'.

Figure 2-17 Configure Advanced Settings

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.

The screenshot shows the 'Purchase ECS' page. It includes fields for 'Enterprise Project' (a dropdown menu), 'Quantity' (set to 1), and 'Agreement' (a checkbox checked with the text: 'I have read and agree to the Service Level Agreement and Image Disclaimer'). At the bottom, it shows 'ECS Price \$0.13 USD/hour' and 'Submit' button.

Figure 2-18 Purchasing ECS

The screenshot shows the 'Viewing the created ECS' page. On the left is a sidebar with 'Cloud Server Console' and 'Elastic Cloud Server' selected. The main area shows a table with the following data:

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|---|-----|---------|---|-----------------------------|--------------|-----|-------------------|
| ecs-windows 6d90b5b6-5f67-4d8a-8d81-d1730... | AZ1 | Running | 2 vCPUs 4GB s6-large-2 Windows Server 2012 R2 Standard | 192.168.0.112 (Private I... | Pay-per-use | -- | Remote Login More |

Figure 2-19 Viewing the created ECS

Create a Linux ECS. Configure the parameters the same as creating the Windows ECS, except for ECS Name, Image, and Login Mode (choose Password).

Image: Public image, CentOS, CentOS 7.6 64-bit (40 GB)

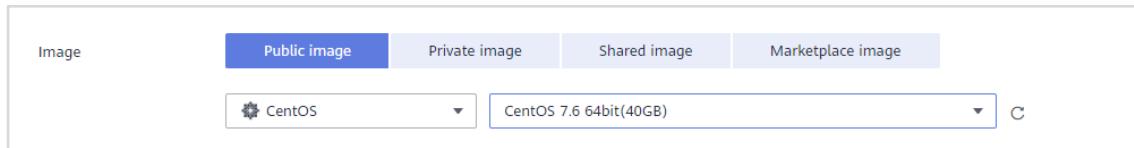


Figure 2-20 Purchasing a Linux ECS

2.2.2.2 Logging In to an ECS

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.

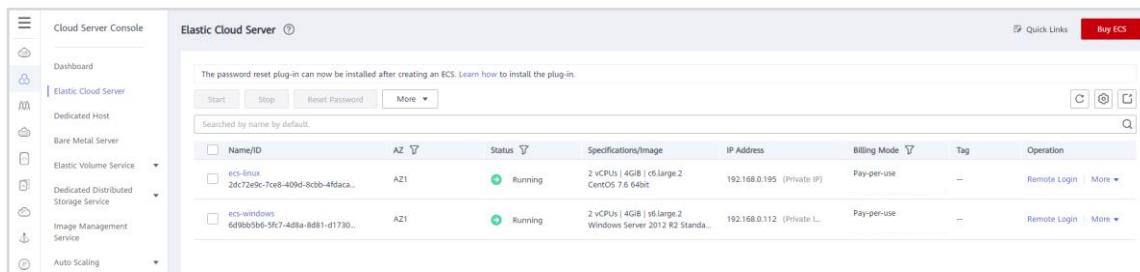


Figure 2-21 Remotely logging in to the ECS

Locate the row containing **ecs-windows**, click **More**, and choose **Get Password**.

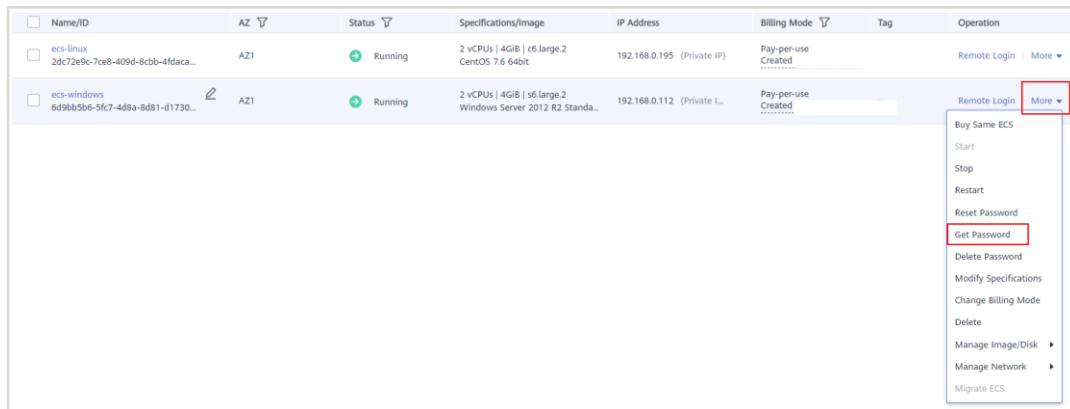


Figure 2-22 Get Password

Click Select File, choose the downloaded key pair file, and click Open.

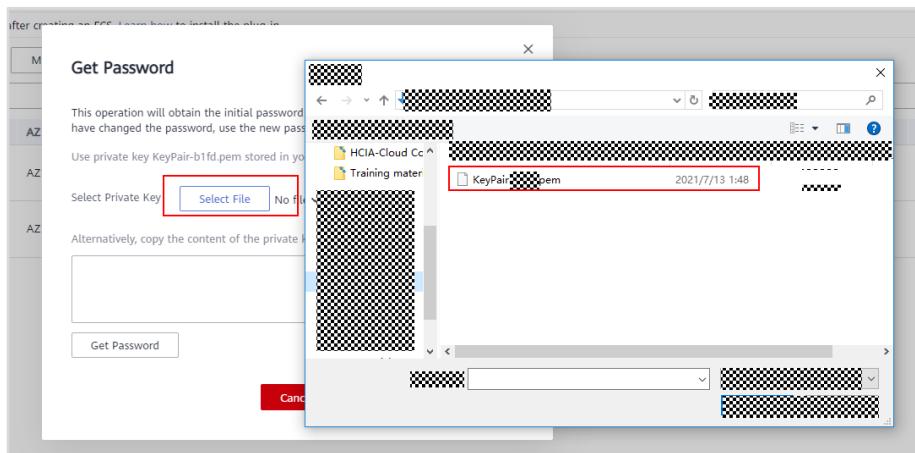


Figure 2-23 Choosing key pair file

Click Get Password, copy the password, and close the window.

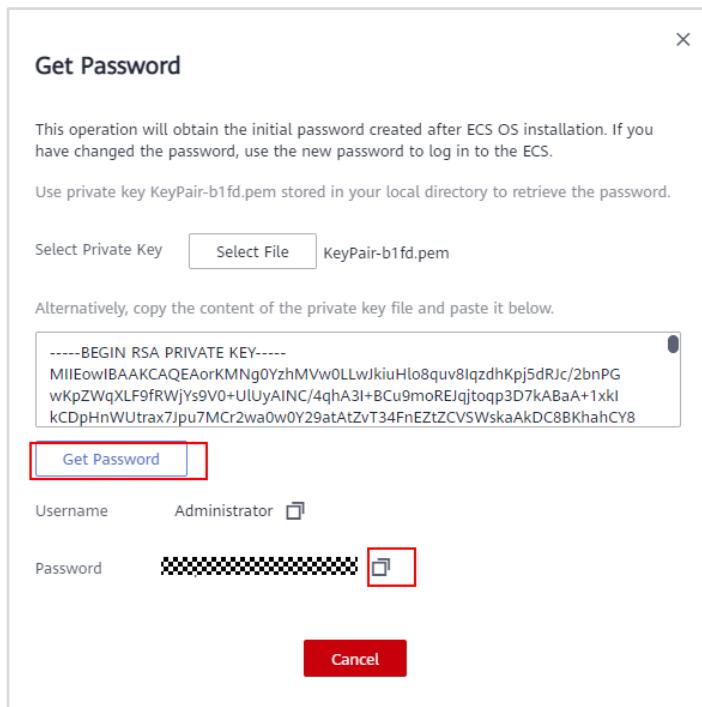


Figure 2-24 Get Password

Locate the row containing **ecs-windows**, click **Remote Login**, and click **Log In**.

If Press **Ctrl+Alt+Delete** to sign in is displayed, click **Send CtrlAltDel** in the upper part of the remote login page.

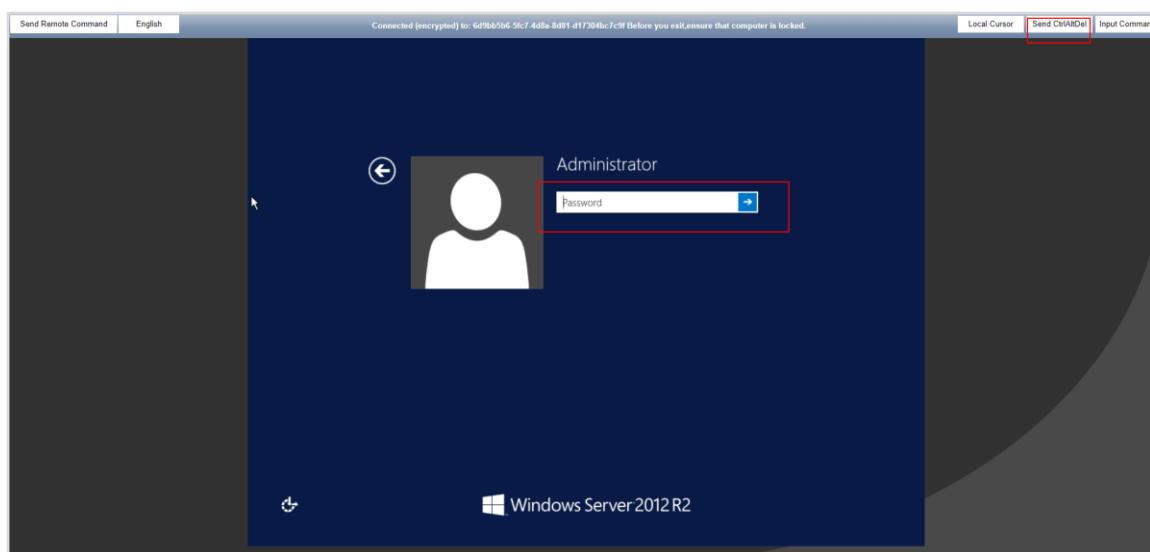


Figure 2-25 Logging In to Windows

Click Input Commands in the upper right corner, paste the copied password, click Send, and then press Enter.

IMPORTANTE: o botão de “Input Command” na console só aparece se o Layout de teclado selecionado for “ENGLISH” (em Português não parece essa opção!!!)

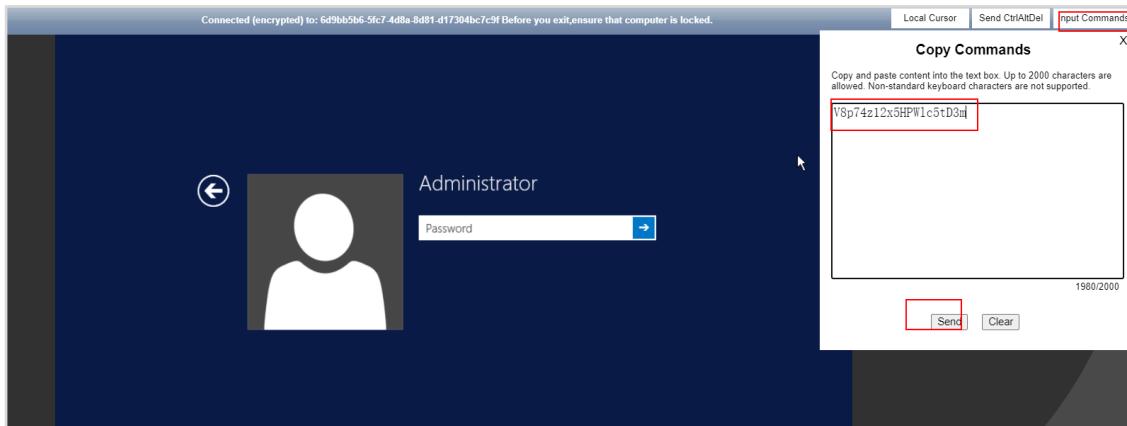


Figure 2-26 Entering the password

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

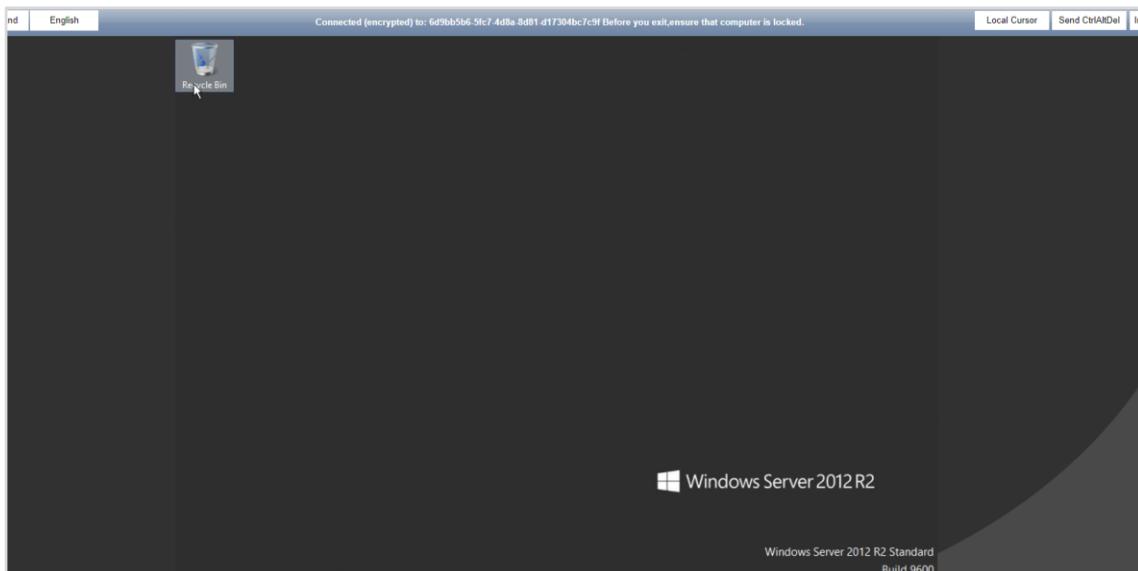


Figure 2-27 Successfully logging in to Windows

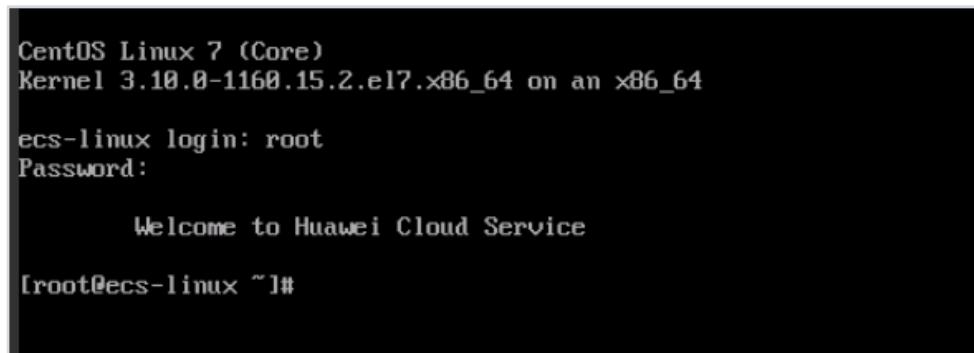
In this exercise, there is no EIP bound to the Linux ECS. Therefore, you cannot use remote login tools (SSH tool) to log in to the ECS. You can choose Remote Login in the row containing ecs-linux, and click Log In to log in to the ECS using VNC.

Linux:

ecs-linux login: root

Password: Enter a password, for example, Huawei@123.

Linux ECSs do not have a GUI. After you log in to 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.



The screenshot shows a terminal window with the following text:
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.15.2.el7.x86_64 on an x86_64

ecs-linux login: root
Password:

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

Figure 2-28 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 Windows ECS Specifications

On the Elastic Cloud Server page, view the status of the target Windows ECS.

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.

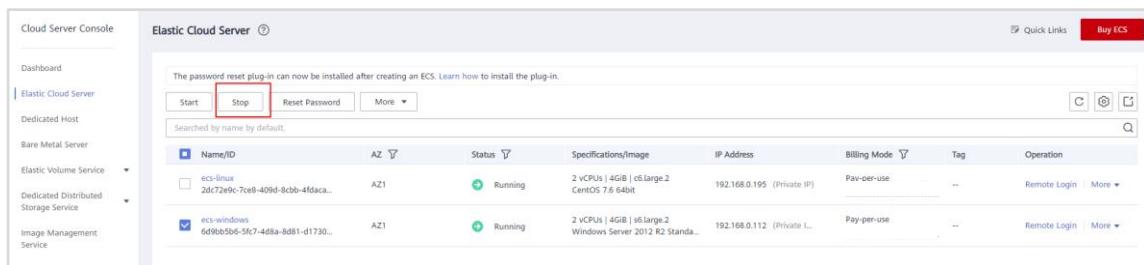


Figure 2-29 Stopping the ECS

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

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|---|-----|---------|---|----------------------------|--------------|-----|-------------------|
| ecs-linux 2dc72e9c-7ce8-409d-8ccb-4fdaca... | AZ1 | Running | 2 vCPUs 4GB sLarge.2 CentOS 7.6 64bit | 192.168.0.195 (Private IP) | Pay-per-use | -- | Remote Login More |
| ecs-windows 6d98b5b6-5fc7-4d8a-8db1-d1730... | AZ1 | Stopped | 2 vCPUs 4GB sLarge.2 Windows Server 2012 R2 Stand... | 192.168.0.112 (Private IP) | Pay-per-use | -- | Remote Login More |

Figure 2-30 Modifying ECS Specifications

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.

| Flavor Name | vCPUs Memory | CPU | Assured / Maximum Bandwidth | Packets Per Second (PPS) |
|-------------------------|-----------------------|----------------------------------|-----------------------------|--------------------------|
| s3.small.1 (Sold Out) | 1 vCPUs 1GiB | Intel SkyLake 6161 2.2GHz | 0.1 / 0.5 Gbit/s | 50,000 |
| s3.medium.2 | 1 vCPUs 2GiB | Intel SkyLake 6161 2.2GHz | 0.1 / 0.5 Gbit/s | 50,000 |
| s3.medium.4 | 1 vCPUs 4GiB | Intel SkyLake 6161 2.2GHz | 0.1 / 0.5 Gbit/s | 50,000 |
| s3.large.2 Free Package | 2 vCPUs 4GiB | Intel SkyLake 6161 2.2GHz | 0.2 / 0.8 Gbit/s | 100,000 |
| s3.large.4 | 2 vCPUs 8GiB | Intel SkyLake 6161 2.2GHz | 0.2 / 0.8 Gbit/s | 100,000 |
| s3.xlarge.2 | 4 vCPUs 8GiB | Intel SkyLake 6161 2.2GHz | 0.4 / 1.5 Gbit/s | 150,000 |
| s3.xlarge.4 | 4 vCPUs 16GiB | Intel SkyLake 6161 2.2GHz | 0.4 / 1.5 Gbit/s | 150,000 |
| s3.2xlarge.2 | 8 vCPUs 16GiB | Intel SkyLake 6161 2.2GHz | 0.8 / 3 Gbit/s | 200,000 |

ECS Price \$0.14 USD/hour **Next**

Figure 2-31 Choosing target specifications

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.

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|-------------|-----|---------|---|----------------------------|--------------|-----|-----------------------|
| ecs-linux | AZ1 | Running | 2 vCPUs 4GiB c6.large.2 CentOS 7.6 64bit | 192.168.0.195 (Private IP) | Pay-per-use | -- | Remote Login More ▾ |
| ecs-windows | AZ1 | Resized | 2 vCPUs 4GiB s6.large.2 Windows Server 2012 R2 Standard | 192.168.0.112 (Private IP) | Pay-per-use | -- | Remote Login More ▾ |

Figure 2-32 Specifications modifying

Start the ECS. The ECS specifications have been modified.

| Name/ID | AZ | Status | Specification/Image | IP Address | Billing Mode | Tag | Operation |
|-------------|-----|---------|---|----------------------------|--------------|-----|-----------------------|
| ecs-linux | AZ1 | Running | 2 vCPUs 4GiB c6.large.2 CentOS 7.6 64bit | 192.168.0.195 (Private IP) | Pay-per-use | -- | Remote Login More ▾ |
| ecs-windows | AZ1 | Stopped | 2 vCPUs 8GiB s3.large.4 Windows Server 2012 R2 Standard | 192.168.0.112 (Private IP) | Pay-per-use | -- | Remote Login More ▾ |

Figure 2-33 Specifications modified

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

Connected (encrypted) to: 6d9bb5b6-5fc7-4d8a-8d81-d17304bc7c9f Before you exit, ensure that computer is locked.

System

View basic information about your computer

Windows edition

Windows Server 2012 R2 Standard © 2013 Microsoft Corporation. All rights reserved.

Windows Server 2012 R2

Processor: Intel(R) Xeon(R) Gold 6161 CPU @ 2.20GHz 2.20 GHz

Installed memory (RAM): 8.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: ecs-windows

Full computer name: ecs-windows

Computer description:

Workgroup: WORKGROUP

Windows activation

Windows is activated Read the Microsoft Software License Terms

Product ID: 00252-70000-00000-AA535

Change product key

Figure 2-34 Confirming new specifications

PARE AQUI: VAMOS INICIAR OUTRO CAPÍTULO TEÓRICO

Creating a Windows System Disk Image from an ECS

If you have created and configured a Windows 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 Windows system disk image using an ECS, you need to configure a Windows ECS and then use it to create a system disk image.

2.2.2.4 Configuring a Windows ECS

Take the ecs-windows ECS you created as an example.

Remotely log in to the ECS.

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

1. Choose Start > Control Panel. (The GUI varies somewhat depending on the OS version.)

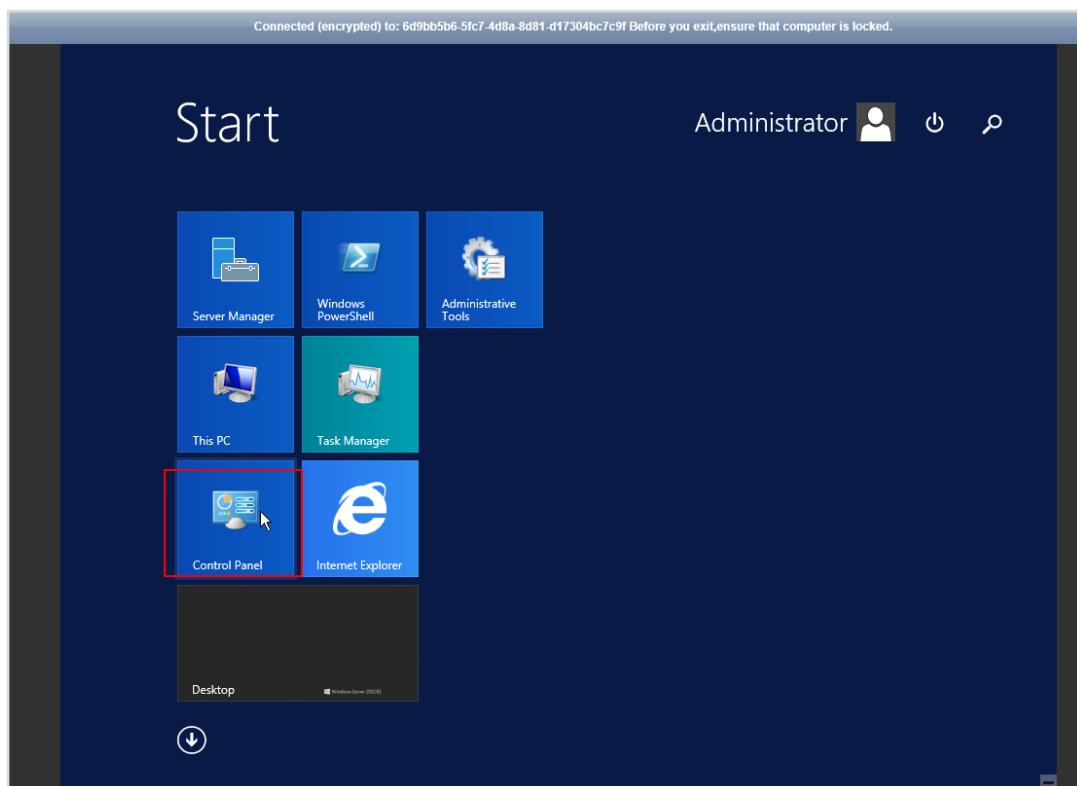


Figure 2-35 Control Panel

2. Click Network and Sharing Center.

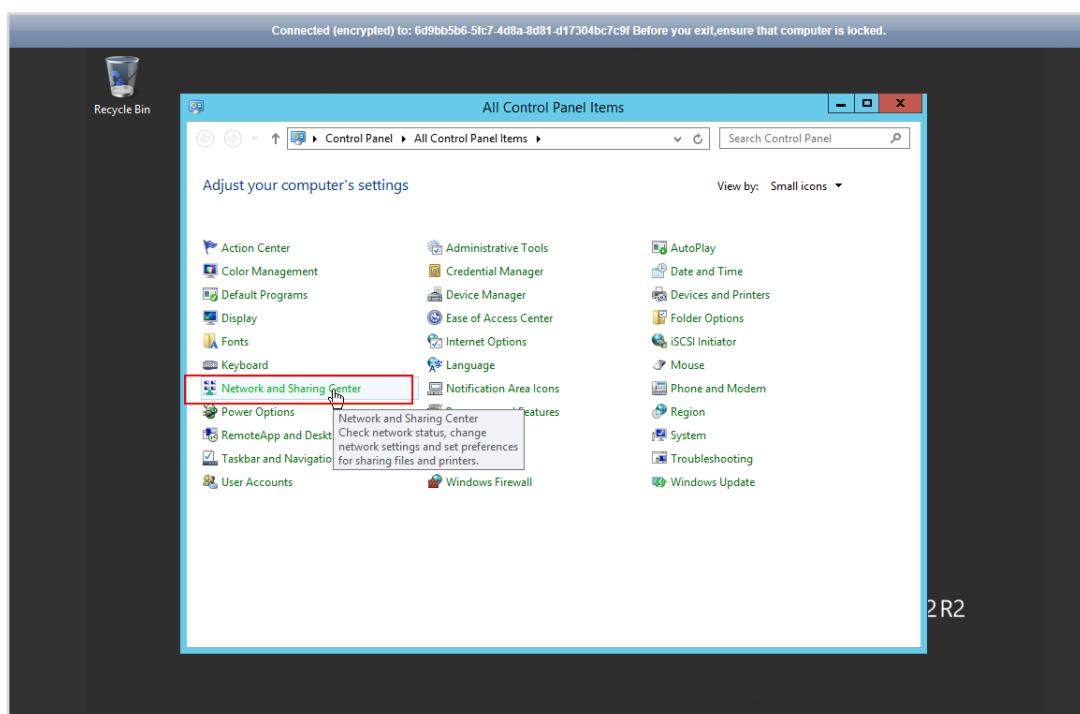


Figure 2-36 Network and Sharing Center

3. Click a network connection, for example, Ethernet 2.

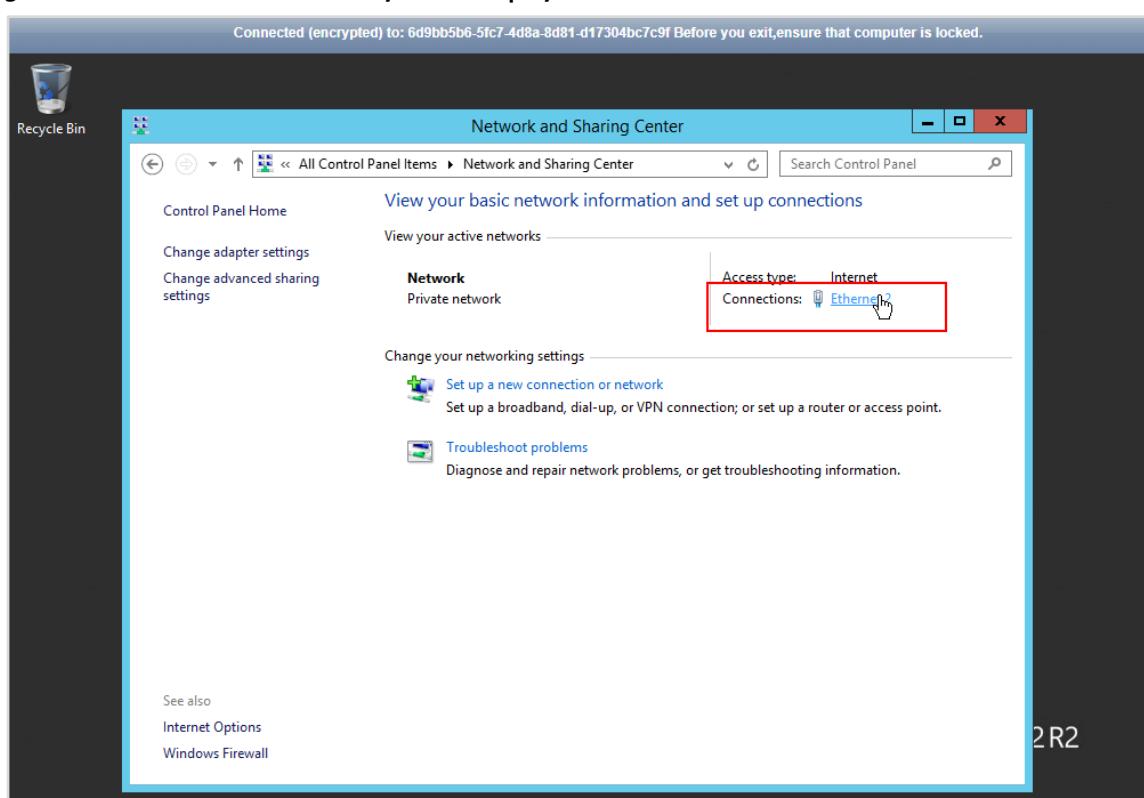


Figure 2-37 NIC

4. Click Properties, select Internet Protocol Version 4 (TCP/IPv4), and click Properties.

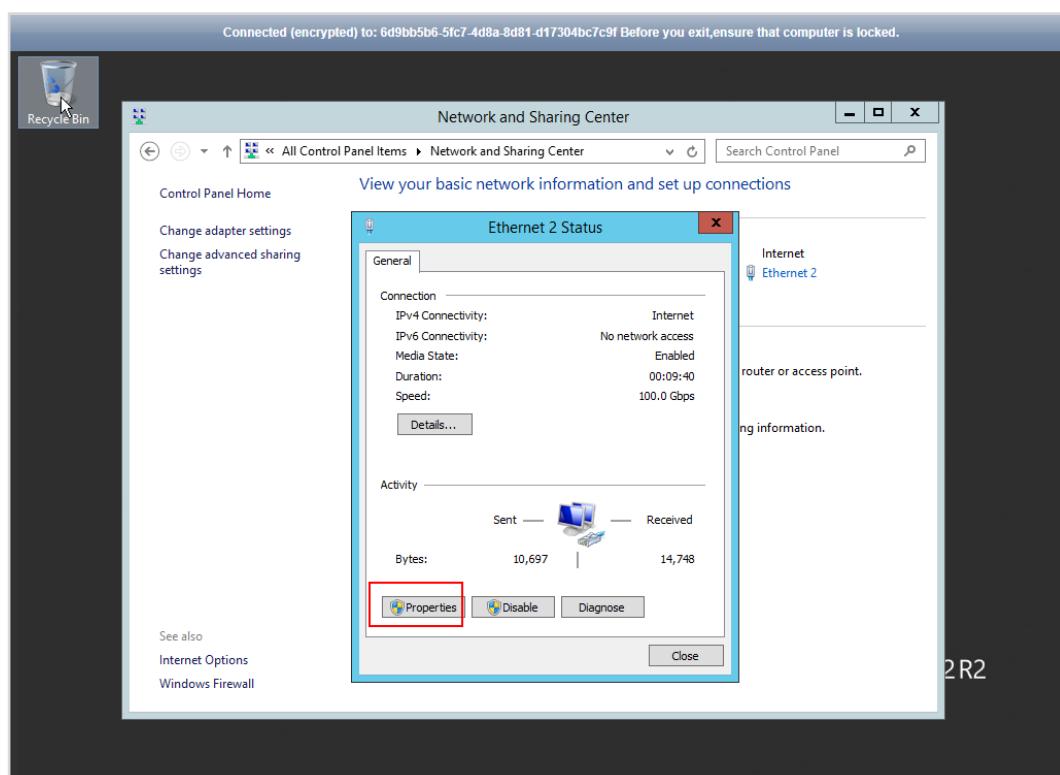


Figure 2-38 NIC properties

5. If Obtain an IP address automatically and Obtain DNS server address automatically are selected, DHCP has been configured. Otherwise, select the two check boxes and click OK.

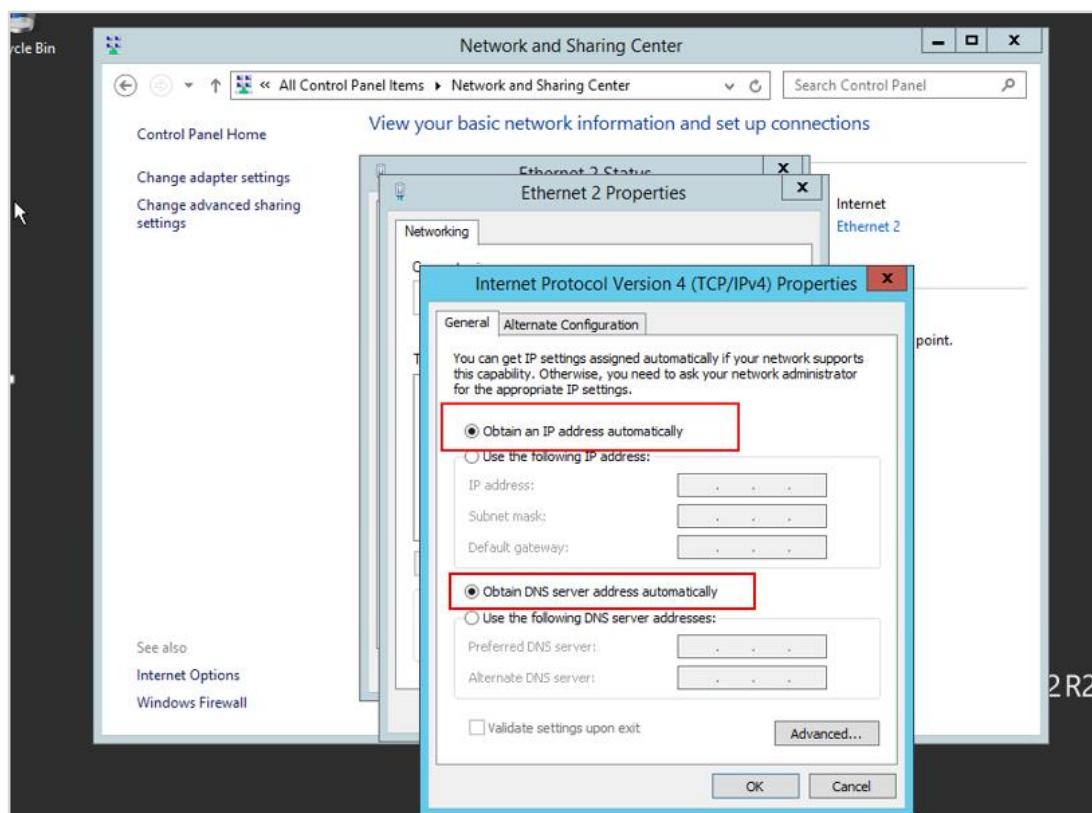


Figure 2-39 Configuring DHCP

Click Start, right-click This PC, and choose Properties. In the navigation pane to the left of the System page, click Remote settings. Select Allow remote connections to this computer. Click OK. (The GUI varies somewhat depending on the OS version.)

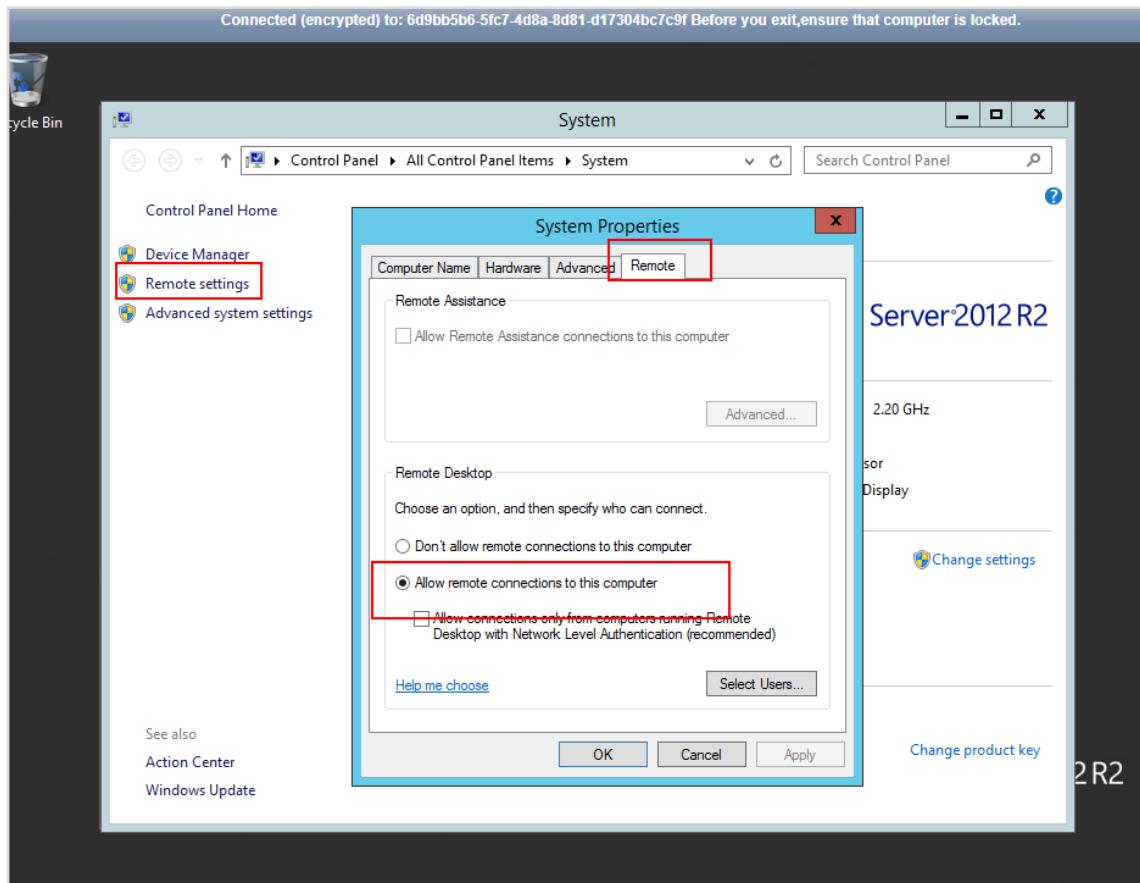


Figure 2-40 Configuring remote desktop

Go to Start > Control Panel and navigate to Windows Firewall. In the left pane, select Allow an app or feature through Windows Firewall. Select apps that are allowed by Windows Firewall for Remote Desktop based on your network requirements and click OK.

In this exercise, both the private and public networks are allowed by the firewall.

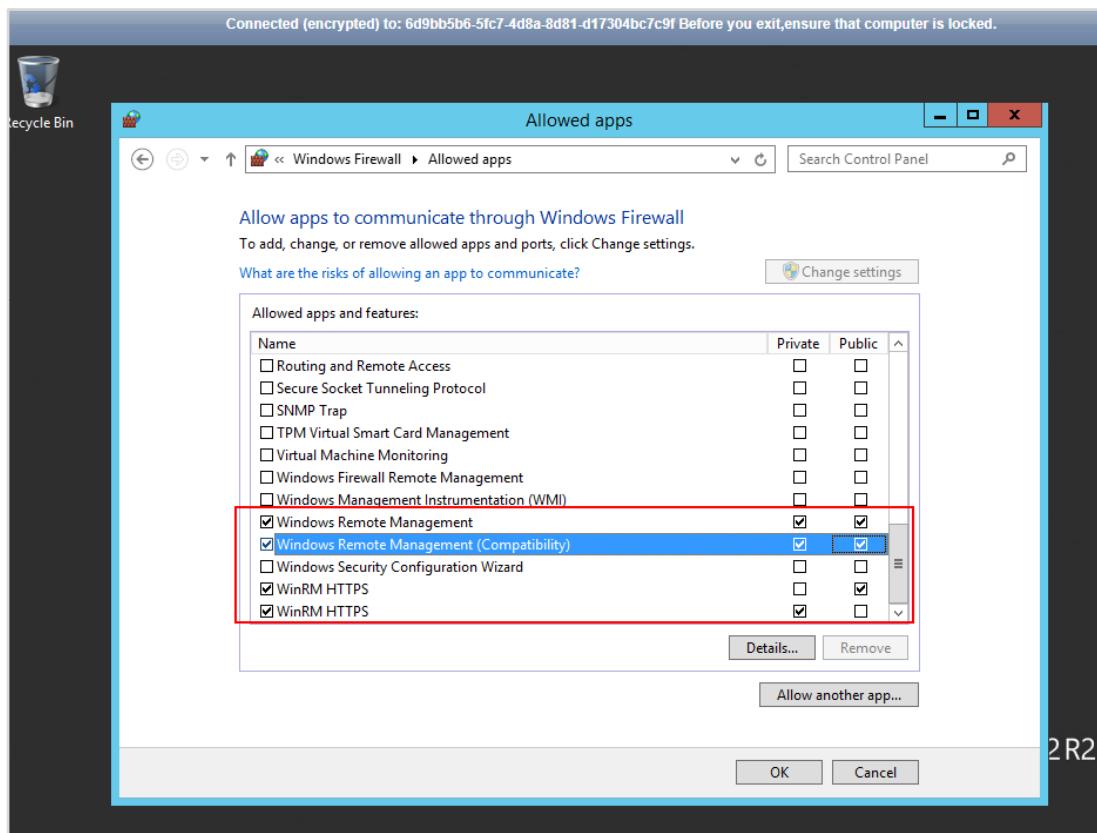


Figure 2-41 Configuring the firewall

Check whether Cloudbase-Init is installed on the ECS. If it is not, install it.

Go to Start > Control Panel > Programs and Features to check whether Cloudbase-Init has been installed on the ECS.

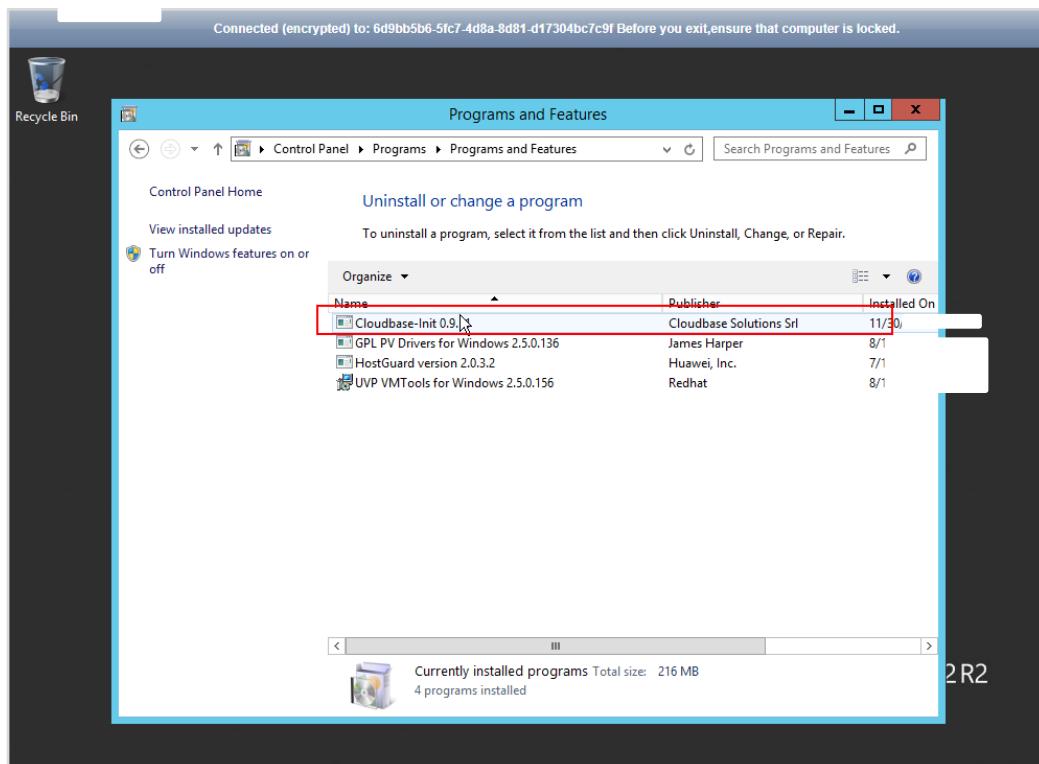


Figure 2-42 Checking whether Cloudbase-Init is installed

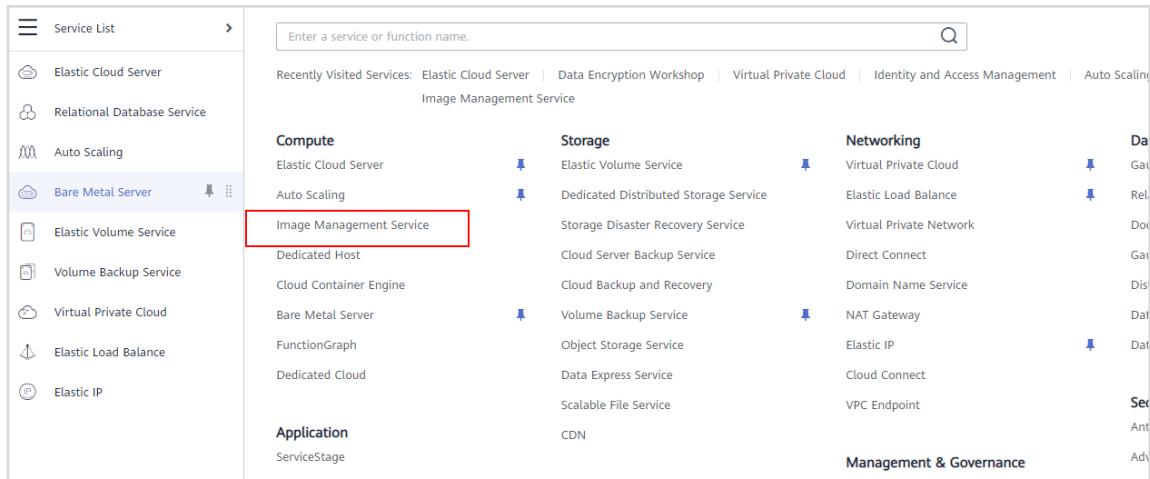
Note:

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

In this exercise, the ECS is created from the public image windows2012 R2, which has Cloudbase-Init installed by default.

2.2.2.5 Creating a Windows Private Image

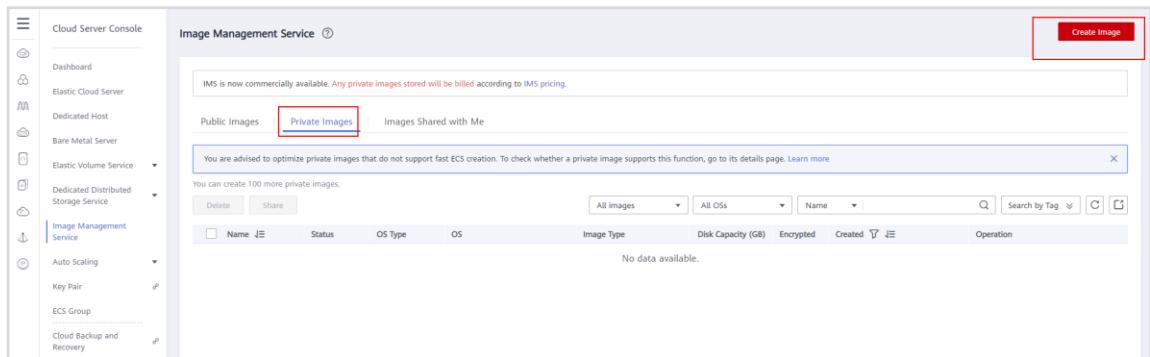
Go back to the management console and in Service List choose Compute > Image Management Service.



The screenshot shows the HUAWEI CLOUD Service List interface. On the left, there is a sidebar with various service icons: Elastic Cloud Server, Relational Database Service, Auto Scaling, Bare Metal Server (selected), Elastic Volume Service, Volume Backup Service, Virtual Private Cloud, Elastic Load Balance, and Elastic IP. The main area is divided into several sections: Compute, Storage, Networking, Application, and Management & Governance. The 'Image Management Service' under the Compute section is highlighted with a red box. At the top right, there is a search bar and a magnifying glass icon.

Figure 2-43 Accessing IMS

On the Image Management Service page, click Create Image.

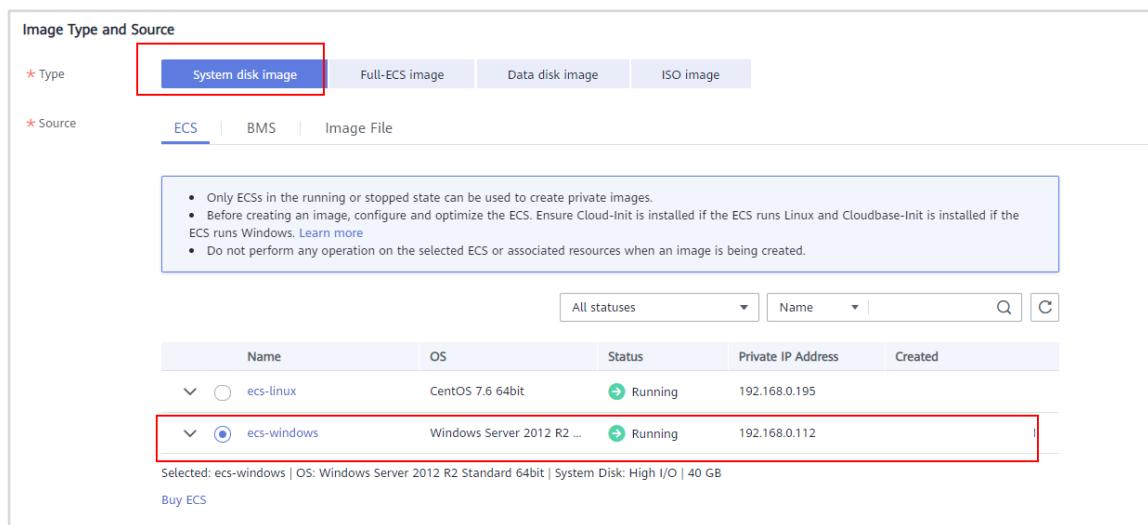


The screenshot shows the Image Management Service page. The left sidebar includes options like Dashboard, Elastic Cloud Server, Dedicated Host, Bare Metal Server, Elastic Volume Service, Dedicated Distributed Storage Service, Image Management Service (selected), Auto Scaling, Key Pair, ECS Group, and Cloud Backup and Recovery. The main content area has tabs for Public Images, Private Images (highlighted with a red box), and Images Shared with Me. A message at the top states: "IMS is now commercially available. Any private images stored will be billed according to IMS pricing." Below this, a note says: "You are advised to optimize private images that do not support fast ECS creation. To check whether a private image supports this function, go to its details page. Learn more." A "Create Image" button is located in the top right corner. The bottom part of the screen shows a table with columns: Name, Status, OS Type, OS, Image Type, Disk Capacity (GB), Encrypted, Created, and Operation. The table currently displays "No data available."

Figure 2-44 Creating a private image

On the Create Image page, set the following parameters and click Next. (Retain the defaults for the rest of the parameters.)

- **Region: LA-SaoPaulo**
- **Type: System disk image**
- **Source:** Select a Windows ECS, for example, **ecs-windows**.
- **Name:** Enter a name, for example, **image-windows2012**.



| Name | OS | Status | Private IP Address | Created |
|-------------|----------------------------|---------|--------------------|---------|
| ecs-linux | CentOS 7.6 64bit | Running | 192.168.0.195 | |
| ecs-windows | Windows Server 2012 R2 ... | Running | 192.168.0.112 | |

Figure 2-45 Setting private image parameters

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

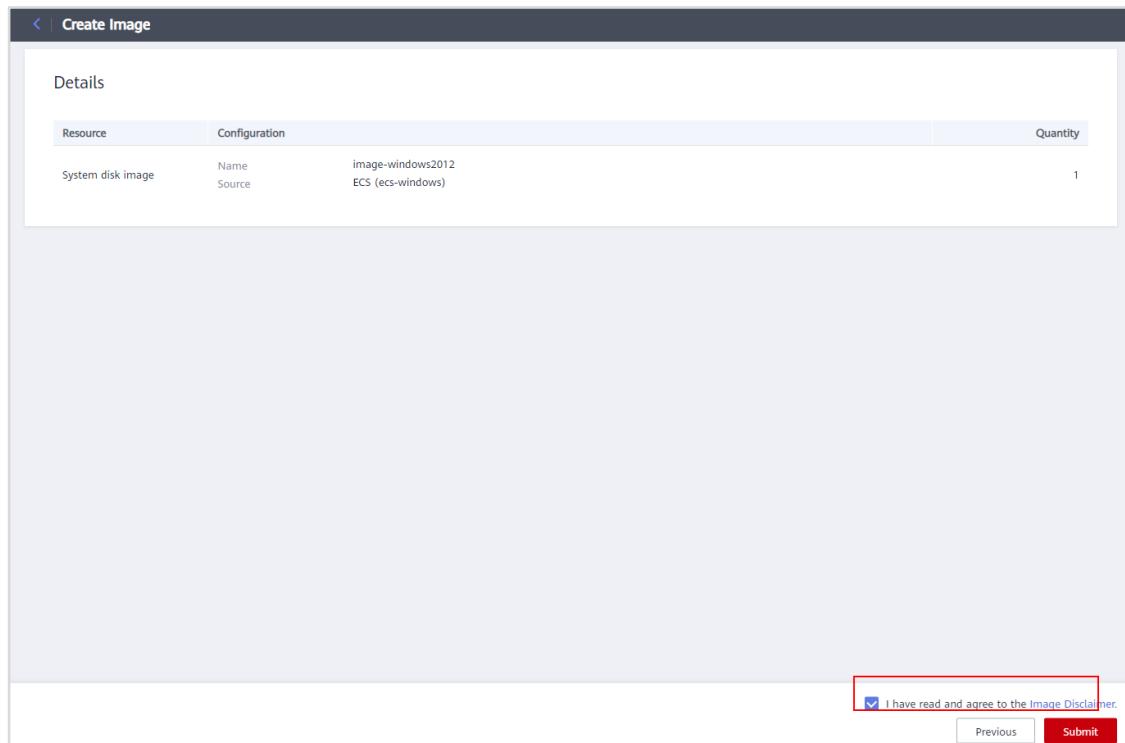


Figure 2-46 Confirming the private image settings

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 Type | Disk Capacity (GB) | Encrypted | Created | Operation |
|---------------|--------|---------|--------------------------------|---------------------------|--------------------|-----------|---------|------------------------|
| image-wind... | Normal | Windows | Windows Server 2012 R2 Stan... | ECS system disk image(x-) | 40 | No | Jul | Modify |

Figure 2-47 Viewing the private image status

2.2.2.6 Modifying Image Information

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

Figure 2-48 Modifying image information

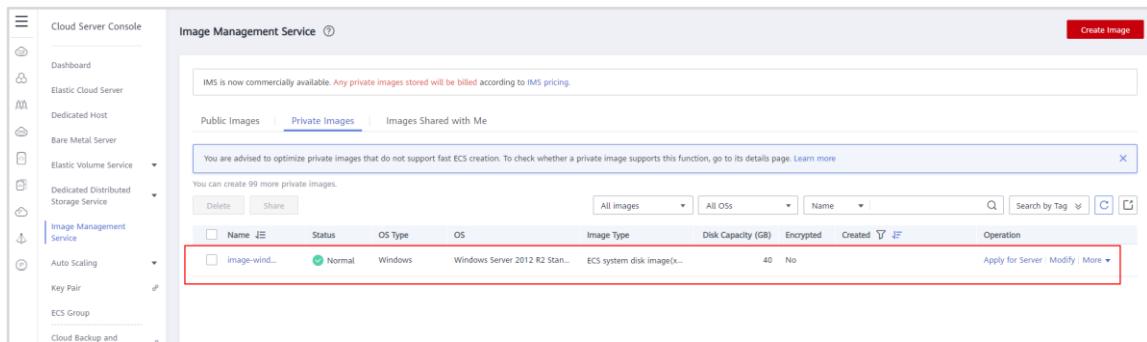
You can modify the image name, memory, and other details.

| | | | | | |
|---|---|---------------|--|--------|------|
| Name | image-windows2012 | | | | |
| Description | 0/1,024 | | | | |
| Minimum Memory | 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. | | | | |
| | Unlimited | 1 GB | 2 GB | 4 GB | 8 GB |
| | 16 GB | 32 GB | 64 GB | 128 GB | |
| Maximum Memory | Unlimited | 4 GB | 32 GB | 64 GB | |
| | 128 GB | | | | |
| NIC Multi-Queue | Supported | Not supported | | | |
| Boot Mode | BIOS | UEFI | The boot mode must be the same as that of the OS contained in the image file. Otherwise, ECSSs created from this system disk image will fail to start. | | |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/> | | | | | |

Figure 2-49 Parameters for image modification

2.2.2.7 Replicating an Image Within a Region

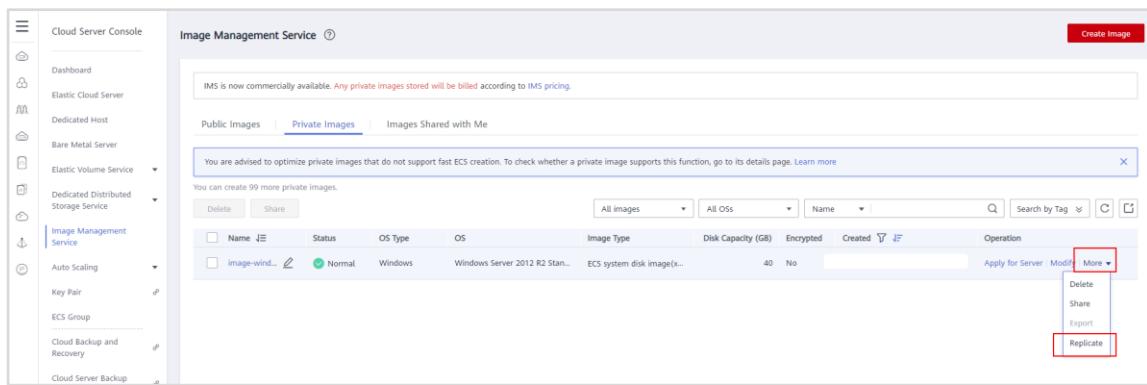
On the Image Management Service page, click Private Image to display the image list.



The screenshot shows the 'Image Management Service' interface. On the left, there's a sidebar with various cloud services like Dashboard, Elastic Cloud Server, Dedicated Host, etc. The 'Image Management Service' is selected. The main area has tabs for 'Public Images', 'Private Images' (which is active), and 'Images Shared with Me'. A message at the top says 'IMS is now commercially available. Any private images stored will be billed according to IMS pricing.' Below the tabs, it says 'You are advised to optimize private images that do not support fast ECS creation. To check whether a private image supports this function, go to its details page. Learn more'. There's a note: 'You can create 99 more private images.' Below this is a table with columns: Name, Status, OS Type, OS, Image Type, Disk Capacity (GB), Encrypted, Created, and Operation. One row is highlighted with a red border: 'image-wind...', Normal, Windows, Windows Server 2012 R2 Stan..., ECS system disk image(x...), 40, No, and 'No'. The 'Operation' column for this row has a dropdown menu with options: 'Apply for Server', 'Modify', 'More', 'Delete', 'Share', 'Export', and 'Replicate' (which is also highlighted with a red box).

Figure 2-50 Viewing private images

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



This screenshot is identical to Figure 2-50, showing the 'Image Management Service' page with the 'Private Images' tab selected. The table displays a single row for 'image-wind...'. In the 'Operation' column for this row, the 'More' option is expanded, and the 'Replicate' button is highlighted with a red box.

Figure 2-51 Replicating a private image

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

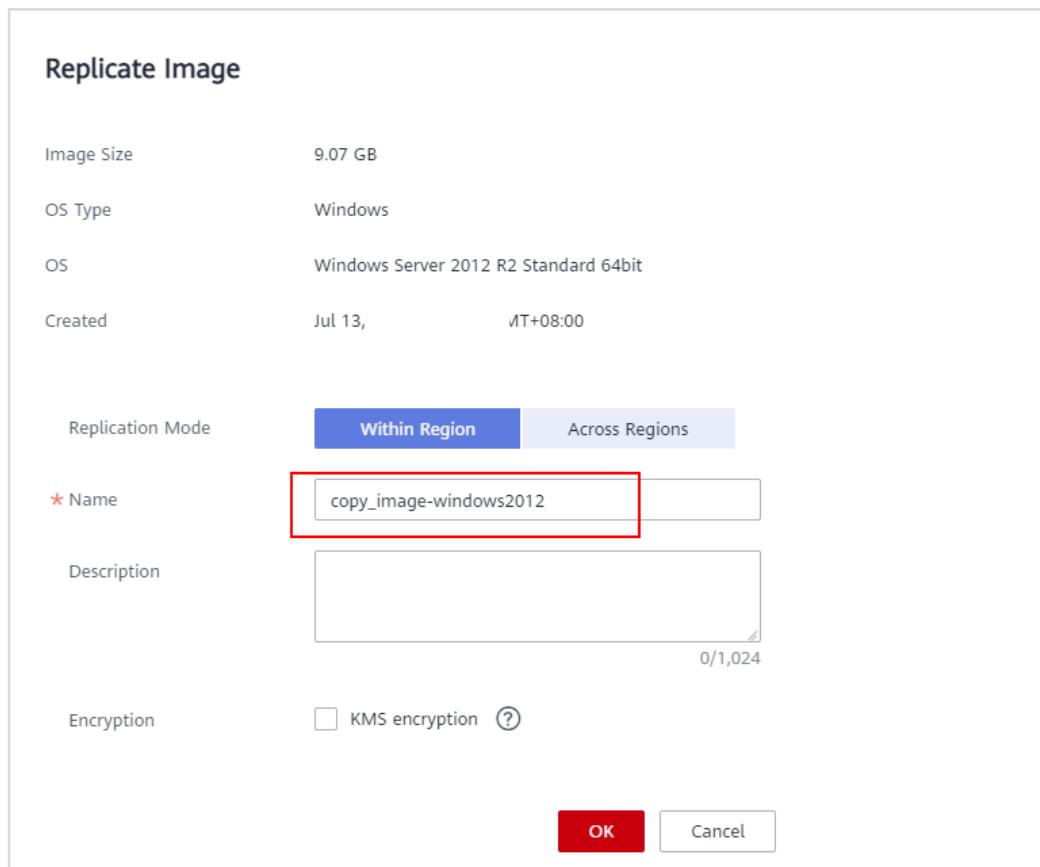


Figure 2-52 Parameters for in-region image replication

| Name | Status | OS Type | OS | Image Type | Disk Capacity (GB) | Encrypted | Created | Operation |
|--------------------|-----------------|---------|--------------------------------|---------------------------|--------------------|-----------|---------------------|--|
| copy_image-wind... | Creating 20% | Windows | Windows Server 2012 R2 Stan... | ECS system disk image | 40 | No | Jul 13, 2018, 08:00 | Apply for Server Modify More |
| image-wind... | Normal | Windows | Windows Server 2012 R2 Stan... | ECS system disk image(x-) | 40 | No | Jul 13, 2018, 08:00 | Apply for Server Modify More |

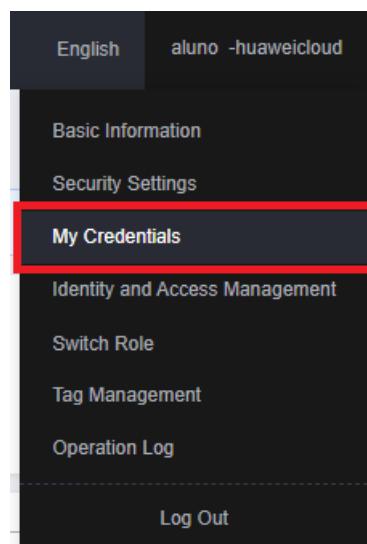
Figure 2-53 Replicated image

2.2.2.8 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.

Talvez essa função de compartilhar Imagens usando diretamente o Account Name ainda não esteja disponível na região de São Paulo (nesse caso, usar o Project ID de cada Huawei Cloud Account na região escolhida para compartilhar as Imagens)

Para obter o Project ID, passe o mouse sobre seu nome de usuário no canto superior direito e escolha "My Credentials".



API Credentials ⓘ

Learn more about HUAWEI CLOUD accounts, IAM users, and projects.

| IAM User Name | aluno -huaweicloud | Account Name | aluno -huaweicloud |
|---------------|----------------------------------|--------------|----------------------------------|
| IAM User ID | 04f2f473fa0025391fbac006a20046cd | Account ID | 04f2f472120025390fafc0063e023480 |

Projects

| Project ID | Project Name | Region |
|----------------------------------|----------------|--------------------|
| 04f302d72b0010422f5dc0066abe0293 | cn-north-1 | CN North-Beijing1 |
| 08022b8f848010d52f3bc006b96648a0 | cn-north-4 | CN North-Beijing4 |
| 06ec4157d40010622f6ac0063677a477 | cn-east-3 | CN East-Shanghai1 |
| 04f302d72b80253a2fc3c00617ffa09e | cn-east-2 | CN East-Shanghai2 |
| 04f302d72980253d2f55c006b28ac9f3 | cn-south-1 | CN South-Guangzhou |
| 04f2f472280025392fb2c0066a7182d2 | ap-southeast-1 | CN-Hong Kong |
| 04f302d72080253f2f37c00621829849 | ap-southeast-2 | AP-Bangkok |
| 04f302d6ca000fca2f25c006bca8c1c5 | ap-southeast-3 | AP-Singapore |
| 04f302d70d80263c2fc0c0067fb3c3c1 | af-south-1 | AF-Johannesburg |
| 06ec4158388010672faec00619b0bdef | na-mexico-1 | LA-Mexico City1 |
| 06ec41581c800ff2f07c006d38db9e2 | sa-brazil-1 | LA-Sao Paulo1 |
| 0632163aac8010e42fbcc00602ca3ee3 | la-south-2 | LA-Santiago |

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

Figure 2-54 Sharing a private image

In the Share Image dialog box, enter the account name (or Project ID, depending of the Region) of the target user and click Add. Click OK.

If the user is a DeC or multi-project user, you also need to enter their project name. To share the image with multiple users, enter their account names (and project names).

Figure 2-55 Sharing an image with an Account name

OU

Figure 2-56 Sharing an image with a Project ID

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.

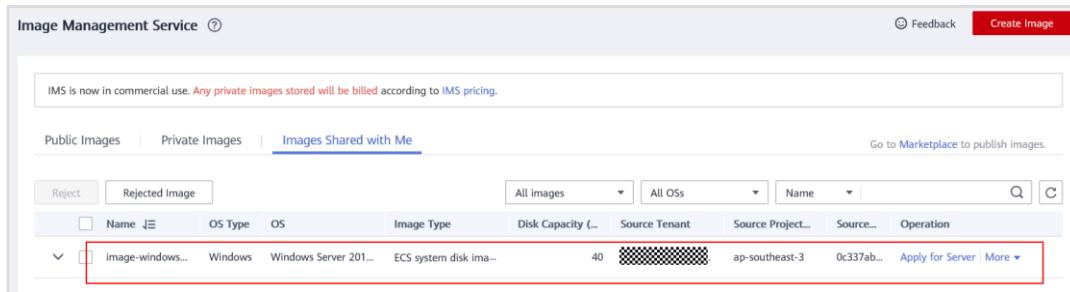


Figure 2-57 Accepting the shared image

2.2.2.9 Applying for an ECS Using a Private Image

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

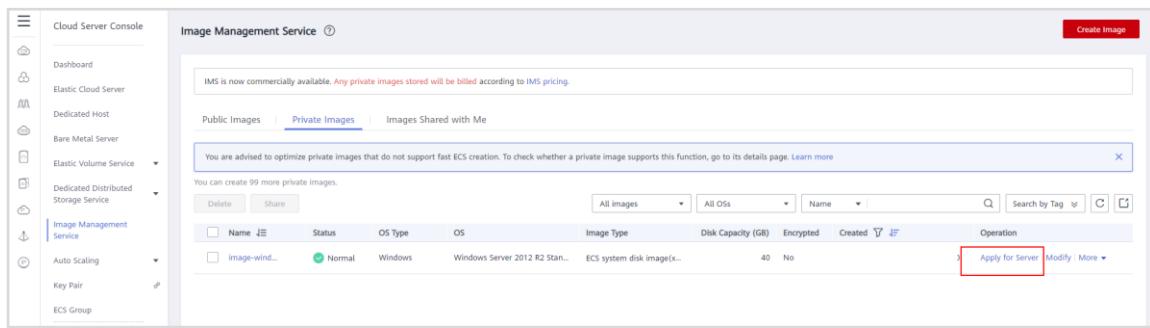


Figure 2-58 Applying for an ECS

On the ECS purchase page, ensure that the private image is selected.

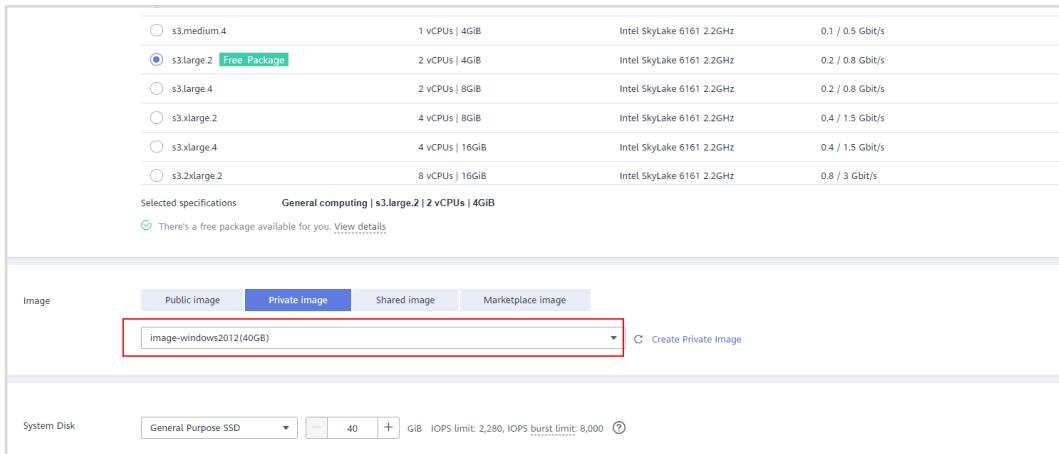


Figure 2-59 Creating an ECS using a private image

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

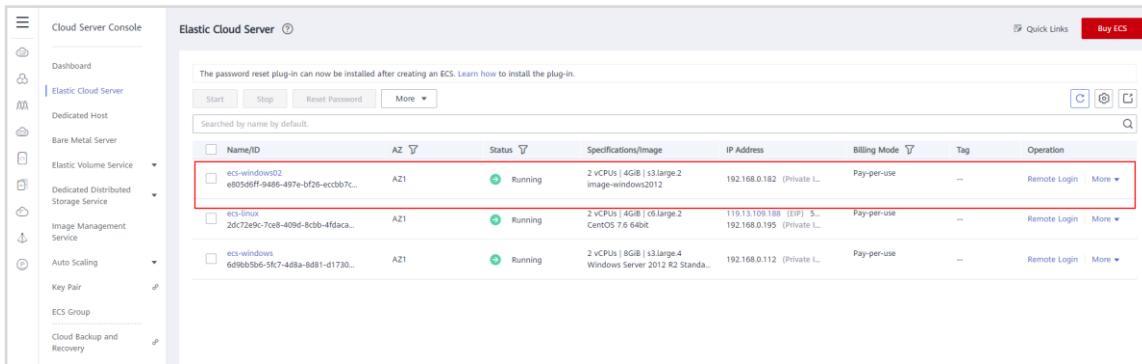


Figure 2-60 Viewing the ECS

2.2.3 Creating a Linux System Disk Image from an ECS

(ATIVIDADE OPCIONAL) – PROCEDIMENTOS SEMELHANTES À CRIAÇÃO DE IMAGENS PRIVADAS COM WINDOWS

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-linux ECS you created as an example.

Remotely log in to the ECS.

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-linux ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Figure 2-61 Opening the NIC configuration file

```
DEVICE="eth0"
BOOTPROTO="dhcp"
ONBOOT="yes"
TYPE="Ethernet"
PERSISTENT_DHCLIENT="yes"
```

Figure 2-62 Checking whether DHCP is configured

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:

```
ls -lh /Cloud*
```

- If the following information is displayed, the plug-in has been installed:

```
[root@ecs-linux ~]# ls -lh /Cloud*
/CloudResetPwdUpdateAgent:
total 20K
drwx----- 2 root root 4.0K Jun 11 09:51 bin
drwxr-xr-x 2 root root 4.0K Feb 26 16:37 conf
drwx----- 3 root root 4.0K Feb 26 16:37 depend
drwx----- 2 root root 4.0K Feb 26 16:37 lib
drwx----- 2 root root 4.0K Jun 11 09:51 logs

/CloudResetPwdAgent:
total 16K
drwx----- 2 root root 4.0K Jun 11 09:51 bin
drwxr-xr-x 2 root root 4.0K Feb 26 16:37 conf
drwx----- 2 root root 4.0K Feb 26 16:37 lib
drwx----- 2 root root 4.0K Jun 11 09:51 logs
[root@ecs-linux ~]# _
```

Figure 2-63 Checking whether CloudResetPwdAgent is installed

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:

```
rpm -qa |grep cloud-init
```

- If information similar to the following is displayed, Cloud-Init has been installed:

```
[root@ecs-linux ~]# rpm -qa |grep cloud-init  
cloud-init-19.4-7.el7.centos.4.x86_64  
[root@ecs-linux ~]# _
```

Figure 2-64 Checking whether Cloud-Init is installed

- 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):

```
yum install https://archives.fedoraproject.org/pub/archive/epel/6/x86_64/epel-release-xx-xx.noarch.rpm  
yum install cloud-init
```

```
root@ecs-linux ~]# yum install https://archives.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release-7-13.noarch.rpm  
Loaded plugins: fastestmirror  
epel-release-7-13.noarch.rpm  
Examining /var/tmp/yum-root-JxR0Za/epel-release-7-13.noarch.rpm: epel-release-7-13.noarch  
/var/tmp/yum-root-JxR0Za/epel-release-7-13.noarch.rpm: does not update installed package.  
Error: Nothing to do  
[root@ecs-linux ~]# yum install cloud-init  
Loaded plugins: fastestmirror  
Determining fastest mirrors  
base  
epel  
extras  
updates  
(1/7): base/7/x86_64/group_gz  
(2/7): epel/x86_64/updateinfo  
(3/7): epel/x86_64/group_gz  
(4/7): extras/7/x86_64/primary_db  
(5/7): base/7/x86_64/primary_db  
51% [=====]  
| 1.5 MB/s | 12 MB 00:00:07 ETA
```

Figure 2-65 Installing Cloud-Init

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:

```
ls -l /etc/udev/rules.d
```

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

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

Figure 2-66 Checking the number of network rule files

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

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

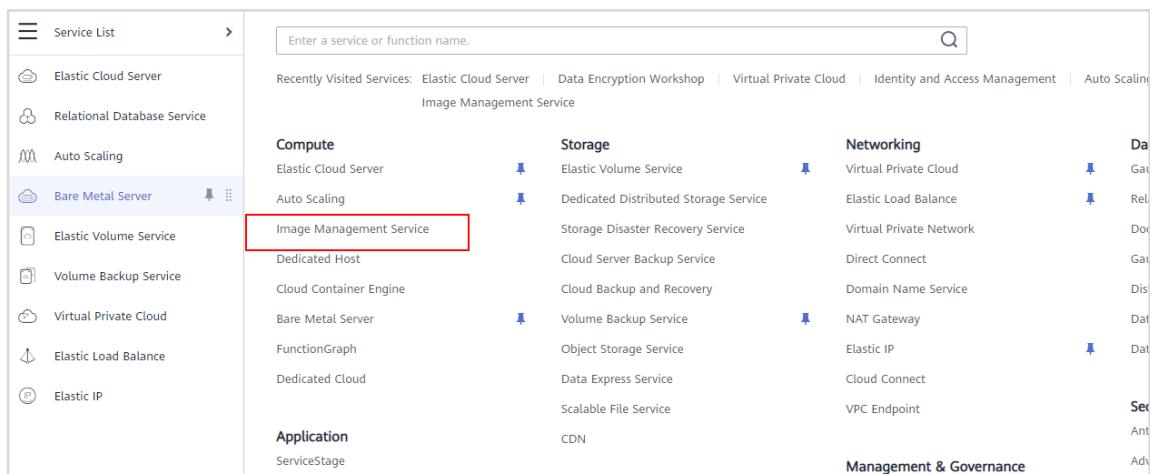


Figure 2-67 Accessing IMS

On the Image Management Service page, click Create Image.

Figure 2-68 Creating a private image

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**

| Name | OS | Status | Private IP Address | Created |
|-------------|----------------------------|---------|--------------------|-------------|
| ecs-linux | CentOS 7.6 64bit | Running | 192.168.0.195 | 19:47 GM... |
| ecs-windows | Windows Server 2012 R2 ... | Stopped | 192.168.0.112 | 1:17 GM... |

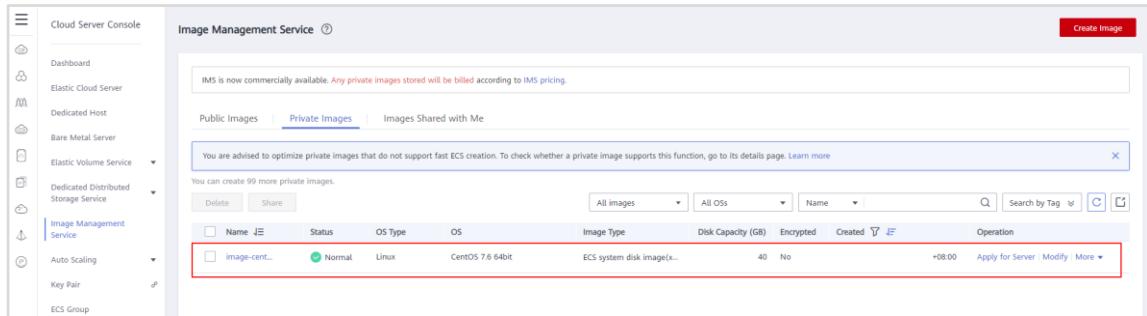
Figure 2-69 Setting private image parameters (1)

Figure 2-70 Setting private image parameters (2)

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

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.



The screenshot shows the 'Image Management Service' interface in the Cloud Server Console. The left sidebar lists various services: Dashboard, Elastic Cloud Server, Dedicated Host, Bare Metal Server, Elastic Volume Service, Dedicated Distributed Storage Service, Image Management Service (selected), Auto Scaling, Key Pair, and ECS Group. The main area is titled 'Image Management Service' with a sub-tab 'Private Images' selected. A message at the top states: 'IMS is now commercially available. Any private images stored will be billed according to IMS pricing.' Below this, a note says: 'You are advised to optimize private images that do not support fast ECS creation. To check whether a private image supports this function, go to its details page. Learn more'. A search bar and filter options ('All images', 'All OSs', 'Name') are present. A table lists one private image: 'image-cent...' (Status: Normal, OS Type: Linux, OS: CentOS 7.6 64bit, Image Type: ECS system disk image(x...), Disk Capacity (GB): 40, Encrypted: No, Created: +08:00). Buttons for 'Apply for Server', 'Modify', and 'More' are shown. A red box highlights the image row in the table.

Figure 2-71 Viewing the private image status

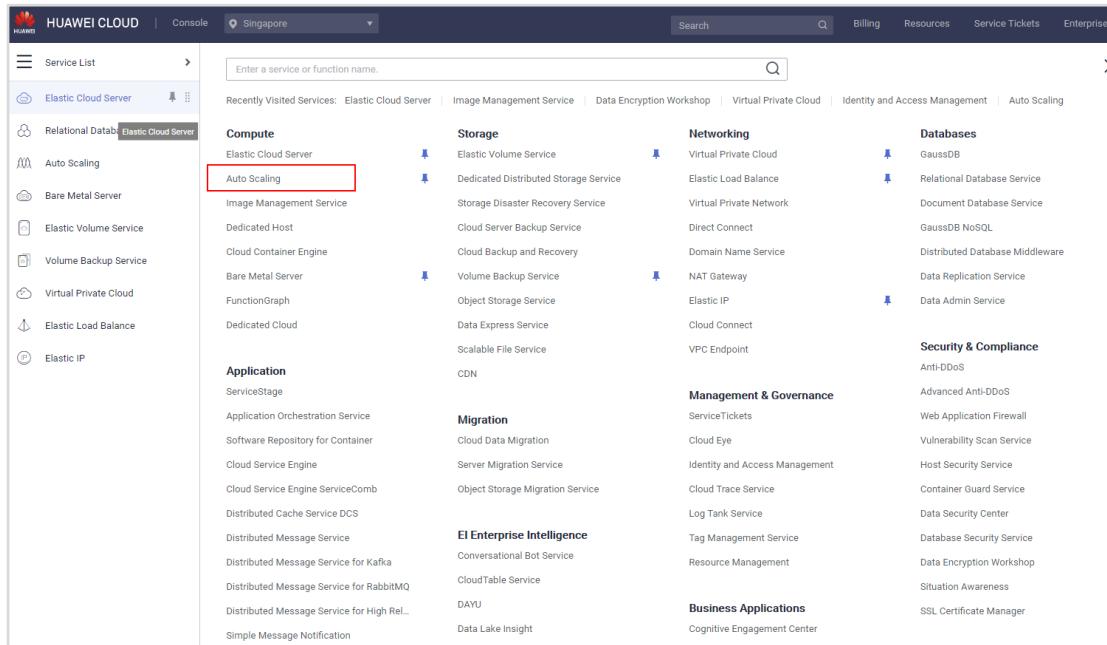
PARE AQUI !!! VAMOS INICIAR OUTRO CAPÍTULO TEÓRICO

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-windows as an example to describe how to scale ECS and bandwidth resources with AS.

2.2.4.1 Creating an AS Configuration

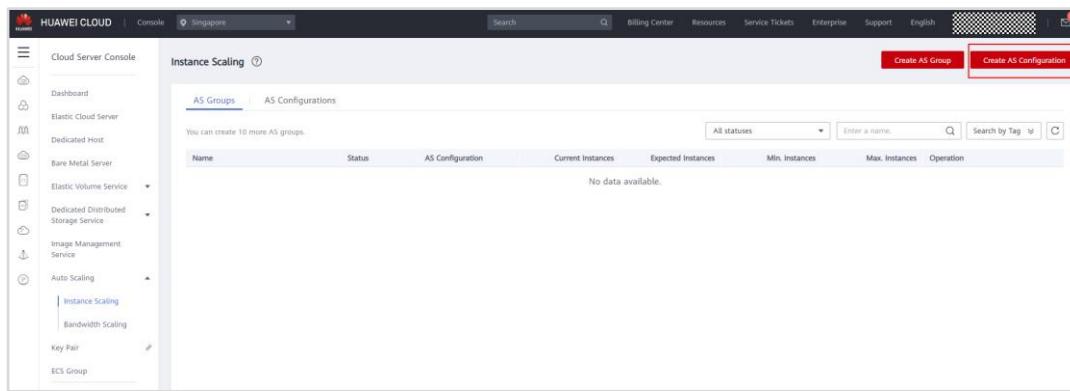
Log in to the management console on Region: LA-SaoPaulo. On the homepage, choose Service List > Compute > Auto Scaling.



The screenshot shows the HUAWEI CLOUD management console interface. The top navigation bar includes 'HUAWEI CLOUD', 'Console', 'Singapore', 'Search', 'Billing', 'Resources', 'Service Tickets', 'Enterprise', and a user icon. Below the navigation is a search bar with placeholder text 'Enter a service or function name.' and a magnifying glass icon. The main content area is divided into several sections: 'Recently Visited Services' (Elastic Cloud Server, Image Management Service, Data Encryption Workshop, Virtual Private Cloud, Identity and Access Management, Auto Scaling), 'Compute' (Elastic Cloud Server, Auto Scaling, Bare Metal Server, Elastic Volume Service, Volume Backup Service, Virtual Private Cloud, Elastic Load Balance, Elastic IP), 'Storage' (Elastic Volume Service, Dedicated Distributed Storage Service, Storage Disaster Recovery Service, Cloud Server Backup Service, Cloud Backup and Recovery, Volume Backup Service, Object Storage Service, Data Express Service, Scalable File Service, CDN), 'Networking' (Virtual Private Cloud, Elastic Load Balance, Virtual Private Network, Direct Connect, Domain Name Service, NAT Gateway, Elastic IP, Cloud Connect, VPC Endpoint), 'Databases' (GaussDB, Relational Database Service, Document Database Service, GaussDB NoSQL, Distributed Database Middleware, Data Replication Service, Data Admin Service), 'Security & Compliance' (Anti-DDoS, Advanced Anti-DDoS, Web Application Firewall, Vulnerability Scan Service, Host Security Service, Container Guard Service, Data Security Center, Database Security Service, Data Encryption Workshop, Situation Awareness, SSL Certificate Manager), 'Management & Governance' (Service Tickets, Cloud Eye, Identity and Access Management, Cloud Trace Service, Log Tank Service, Tag Management Service, Resource Management), 'EI Enterprise Intelligence' (Cloud Data Migration, Server Migration Service, Object Storage Migration Service, Conversation Bot Service, CloudTable Service, DAYU, Data Lake Insight), and 'Business Applications' (Cloud Eye, Identity and Access Management, Cloud Trace Service, Log Tank Service, Tag Management Service, Resource Management, DAYU, Data Lake Insight). The 'Auto Scaling' option under 'Compute' is highlighted with a red box.

Figure 2-72 Accessing AS

Click Create AS Configuration.



The screenshot shows the 'Instance Scaling' page in the HUAWEI CLOUD management console. The left sidebar includes 'Cloud Server Console', 'Dashboard', 'Elastic Cloud Server', 'Dedicated Host', 'Bare Metal Server', 'Elastic Volume Service', 'Dedicated Distributed Storage Service', 'Image Management Service', 'Auto Scaling' (which is expanded to show 'Instance Scaling' and 'Bandwidth Scaling'), 'Key Pair', and 'ECS Group'. The main content area is titled 'Instance Scaling' and shows 'AS Groups' and 'AS Configurations'. A message says 'You can create 10 more AS groups.' Below this is a table with columns: Name, Status, AS Configuration, Current Instances, Expected Instances, Min. Instances, Max. Instances, and Operation. The table currently displays 'No data available.' At the top right of the main area are buttons for 'Create AS Group' and 'Create AS Configuration', with 'Create AS Configuration' highlighted by a red box.

Figure 2-73 Creating an AS configuration

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

- **Region:** LA-SaoPaulo
- **Name:** Use the default name as-config-822b.
- **Configuration Template:** Select **Use specifications of an existing ECS**, and click **Select ECS**. In the **Select ECS** dialog box, select an existing ECS. In this example, **ecs-windows** is selected.

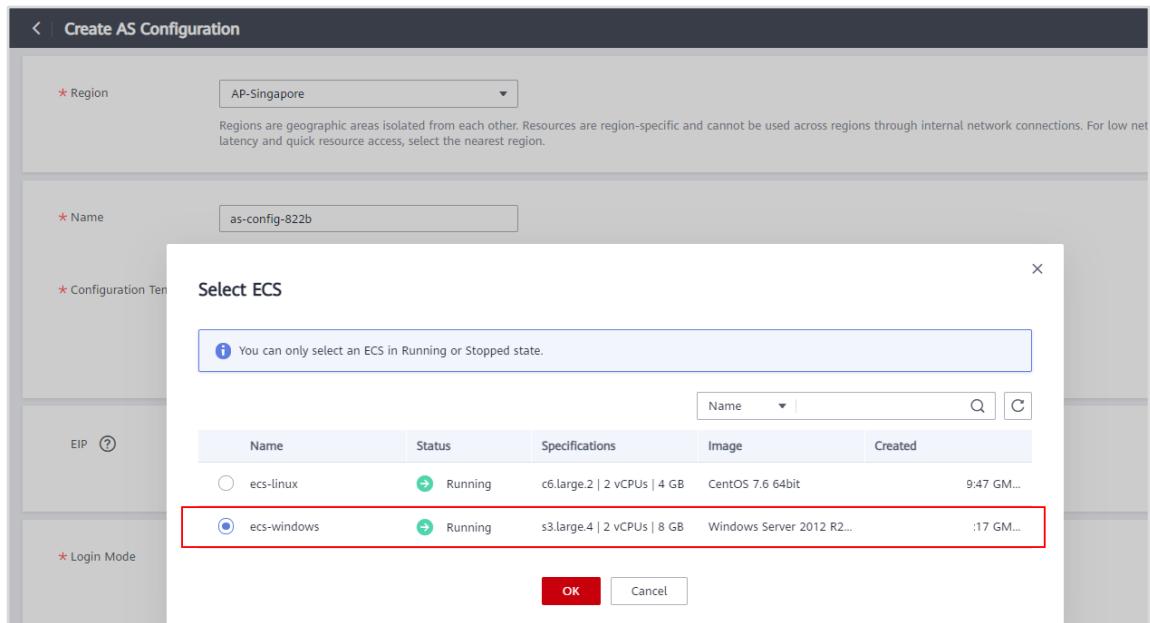


Figure 2-74 Selecting a configuration template

- **EIP: Automatically assign**
- **Type: Dynamic BGP**
- **Billed By: Bandwidth**
- **Bandwidth: 1 Mbit/s**
- **Login Mode: Key pair**
- **Key Pair:** Select the created key pair.

Figure 2-75 Configuring scaling parameters

Click **Create Now**.

Request submitted successfully is displayed.

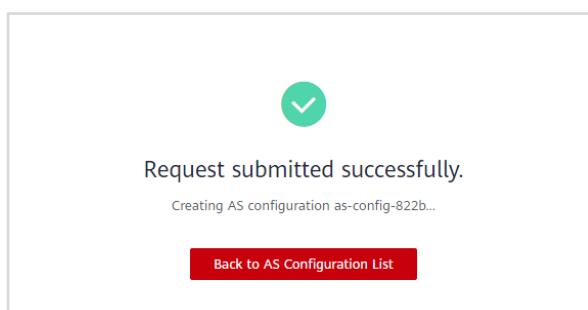


Figure 2-76 AS configuration created

In the AS configuration list, view the created AS configuration as-config-822b.

| AS Groups | | AS Configurations | | | | | | | | | |
|--------------------------|----------------|---|-----------------------------|----------------------------|------------------|-------------|------------|------------|---------|--------------|---|
| | | Name | Status | Specifications | Image | System Disk | Data Disks | Login Mode | Created | Billing Mode | Operation |
| <input type="checkbox"/> | as-config-822b |  Unbound | s3.large.4 2 vCPUs 8 GB | Windows Server 2012 R2 ... | High I/O 40 GB | 0 | Key pair | | | Pay-per-use | Copy Delete |

Figure 2-77 Viewing the AS configuration

2.2.4.2 Creating an AS Group

On the AS console click Create AS Group.

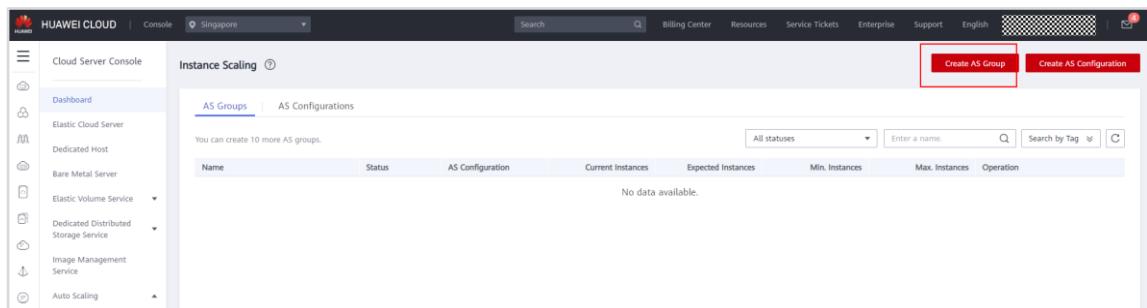
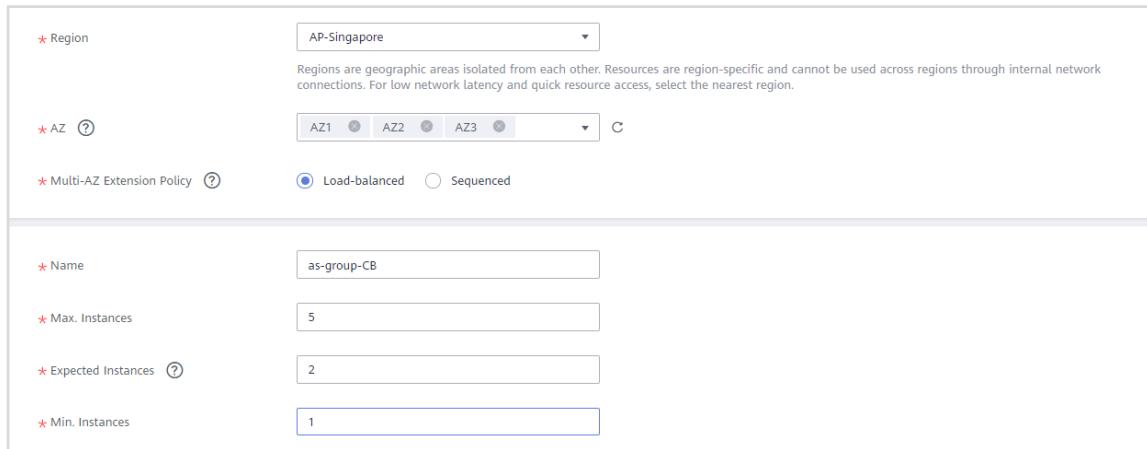


Figure 2-78 Creating an AS group

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

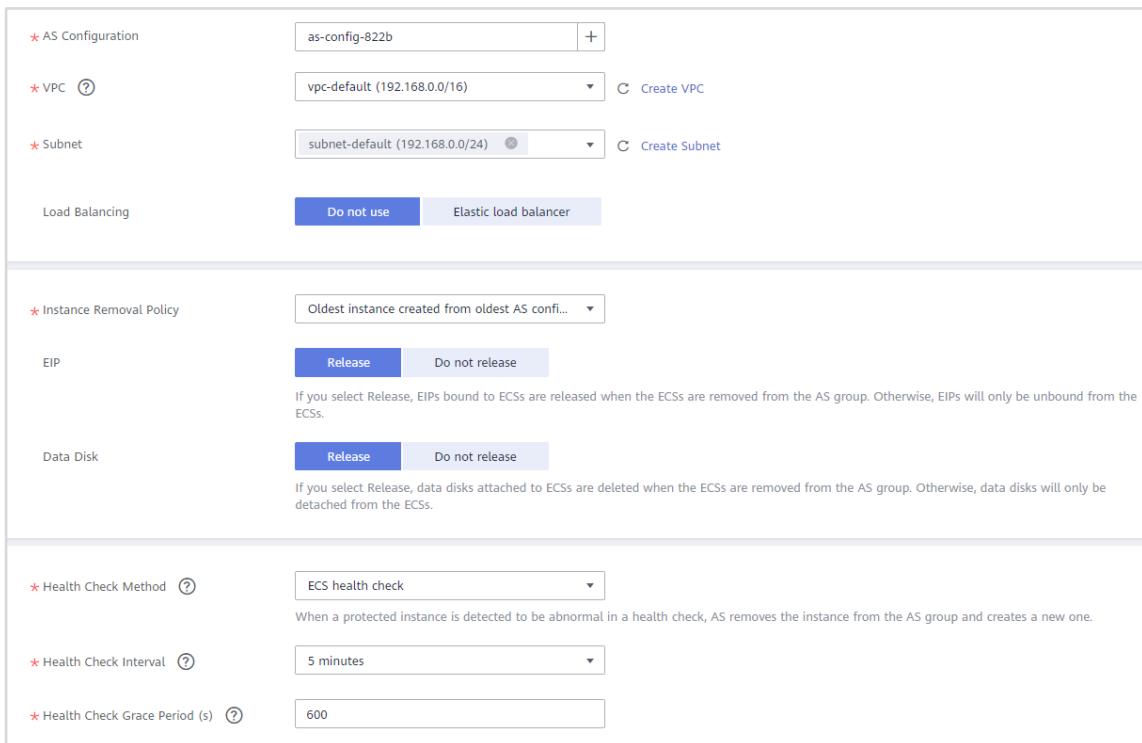
- **Region:** LA-SaoPaulo
- **AZ:** Select all AZs, including AZ1, AZ2, (and AZ3, if exists). AZs in the same region can communicate with each other over an intranet.
- **Multi-AZ Expansion Policy:** Load-balanced (não disponível em LA-SaoPaulo)
- **Name:** as-group-CB (Change it as needed.)
- **Max. Instances:** 5
- **Expected Instances:** 2
- **Min. Instances:** 0 (para poder deletar todas as instâncias criadas pelo AS)



The screenshot shows the configuration page for an AS group. The 'Region' is set to AP-Singapore. Under 'AZ', all three options (AZ1, AZ2, AZ3) are selected. The 'Multi-AZ Extension Policy' is set to 'Load-balanced'. The 'Name' is 'as-group-CB', 'Max. Instances' is 5, 'Expected Instances' is 2, and 'Min. Instances' is 1.

Figure 2-79 Configuring AS group parameters

- **AS Configuration:** Select the created AS configuration **as-config-822b**.
- **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 screenshot shows the configuration page for an AS group. It includes the following fields:

- AS Configuration:** as-config-822b
- VPC:** vpc-default (192.168.0.0/16)
- Subnet:** subnet-default (192.168.0.0/24)
- Load Balancing:** Do not use
- Instance Removal Policy:** Oldest instance created from oldest AS config...
- EIP:** Release
- Data Disk:** Release
- Health Check Method:** ECS health check
- Health Check Interval:** 5 minutes
- Health Check Grace Period (s):** 600

Figure 2-80 Configuring an AS group

Click Back to AS Group List.

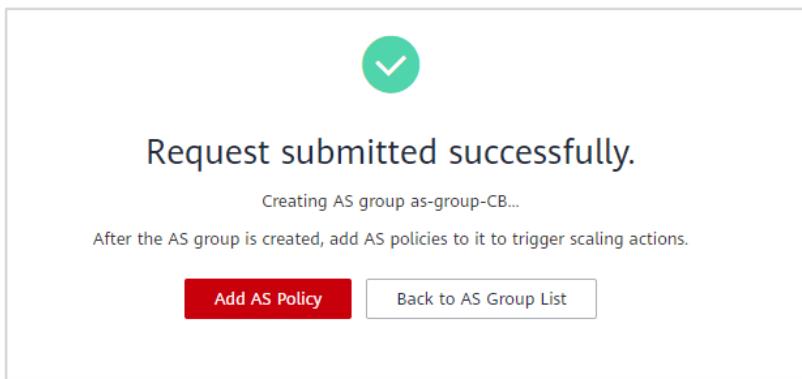
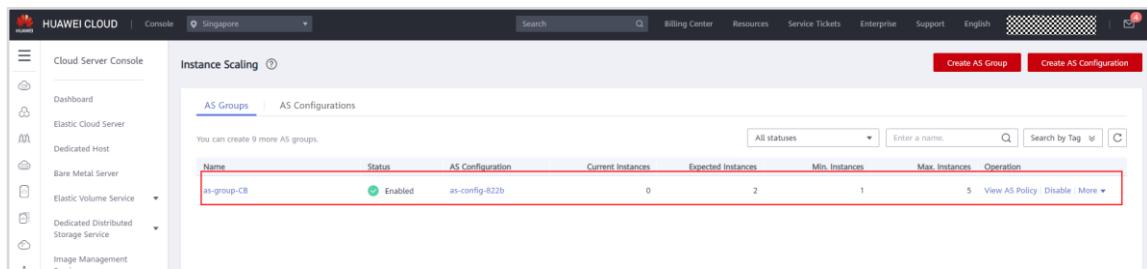


Figure 2-81 AS group created

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

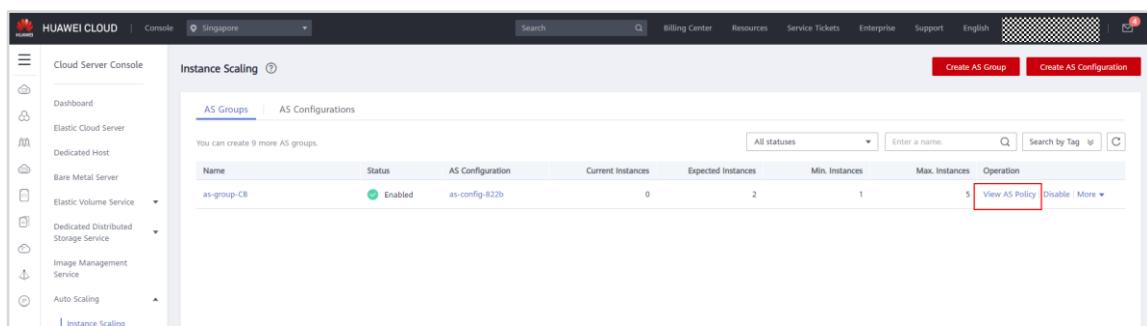


The screenshot shows the 'AS Groups' section of the Instance Scaling service. A single row is listed:

| Name | Status | AS Configuration | Current Instances | Expected Instances | Min. Instances | Max. Instances | Operation |
|-------------|---------|------------------|-------------------|--------------------|----------------|----------------|---|
| as-group-CB | Enabled | as-config-832b | 0 | 2 | 1 | 5 | View AS Policy Disable More |

Figure 2-82 Viewing the AS group

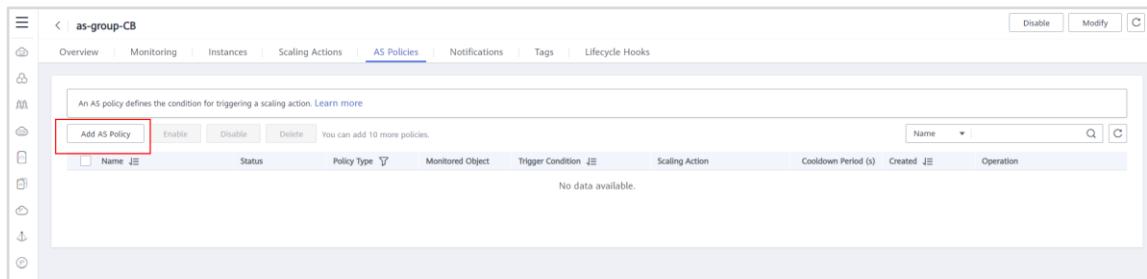
Click View AS Policy in the Operation column.



The screenshot is identical to Figure 2-82, but the 'View AS Policy' link in the 'Operation' column of the 'as-group-CB' row is highlighted with a red box.

Figure 2-83 View AS Policy

On the AS Policies page, click Add AS Policy.



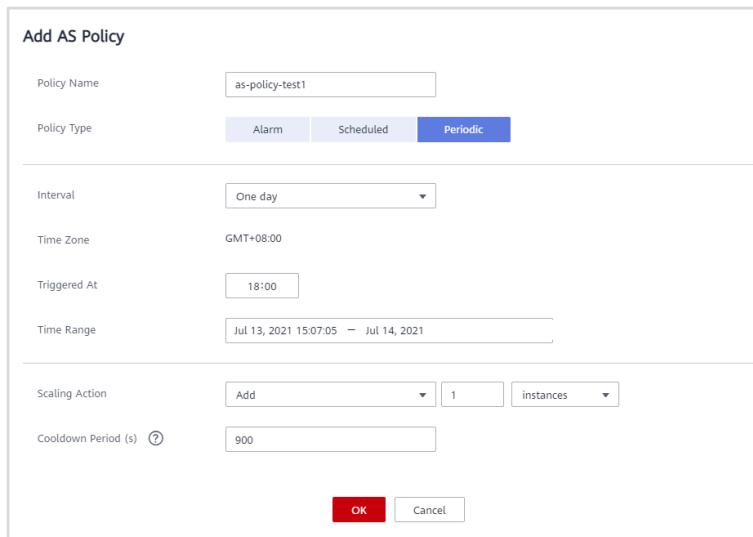
The screenshot shows the 'AS Policies' tab selected in the 'as-group-CB' service. The 'Add AS Policy' button in the top-left corner of the main content area is highlighted with a red box.

Figure 2-84 Adding an AS policy

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:** One 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: Periodic

Interval: One day

Time Zone: GMT+08:00

Triggered At: 18:00

Time Range: Jul 13, 2021 15:07:05 — Jul 14, 2021

Scaling Action: Add 1 instances

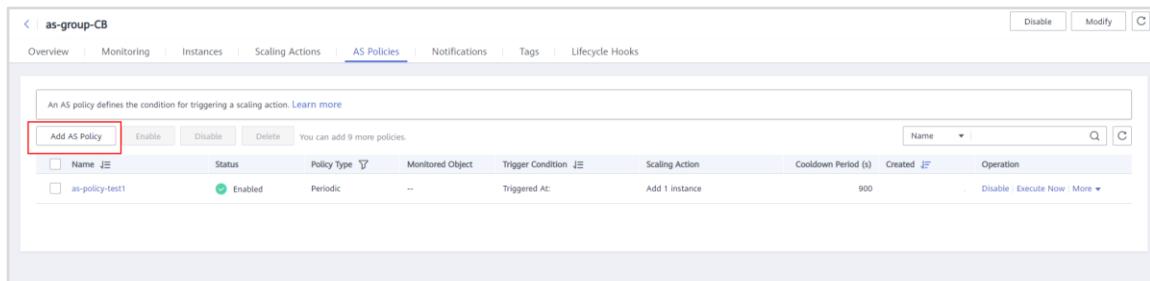
Cooldown Period (s): 900

OK Cancel

Figure 2-85 Configuring an AS policy

Click OK.

Click Add AS Policy again to create another AS policy.



An AS policy defines the condition for triggering a scaling action. Learn more

Add AS Policy

| Name | Status | Policy Type | Monitored Object | Trigger Condition | Scaling Action | Cooldown Period (s) | Created | Operation |
|-----------------|---------|-------------|------------------|-------------------|----------------|---------------------|---------|--------------------------|
| as-policy-test1 | Enabled | Periodic | -- | Triggered At: | Add 1 instance | 900 | ... | Disable Execute Now More |

Figure 2-86 Adding another AS policy

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:** One day
- **Triggered At:** 23:00
- **Time Range:** Retain the default settings.
- **Scaling Action:** Reduce 1 instances
- **Cooldown Period (s):** 900

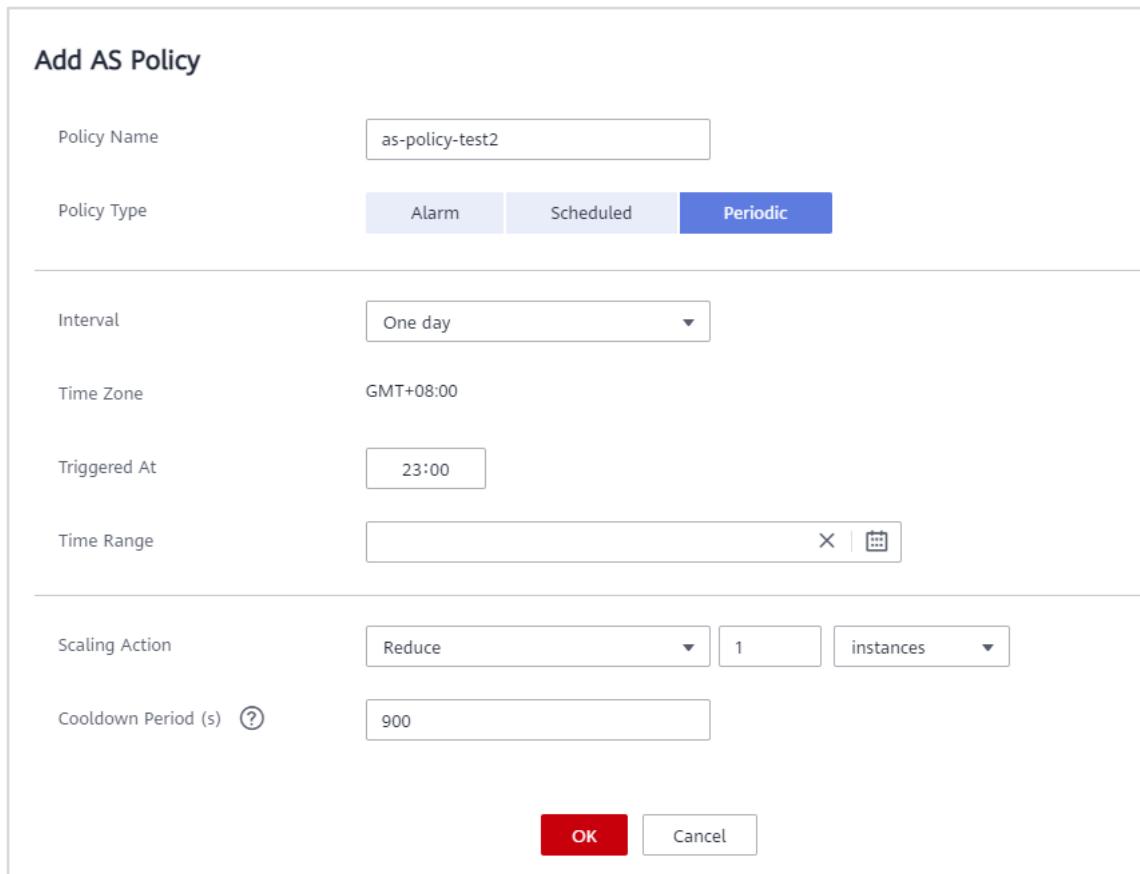


Figure 2-87 Configuring another AS policy

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

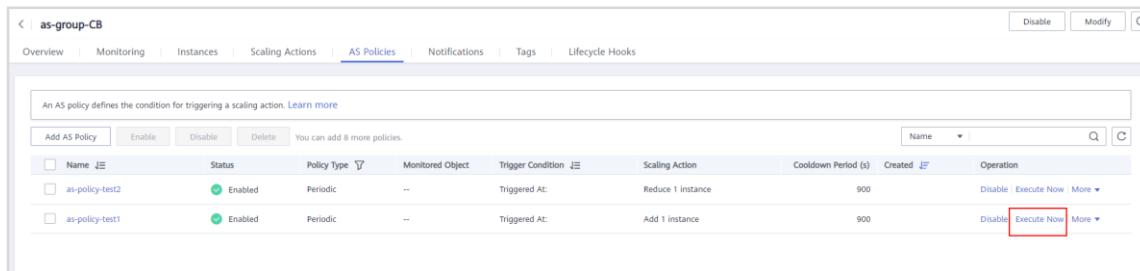


Figure 2-88 Executing an AS policy

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.

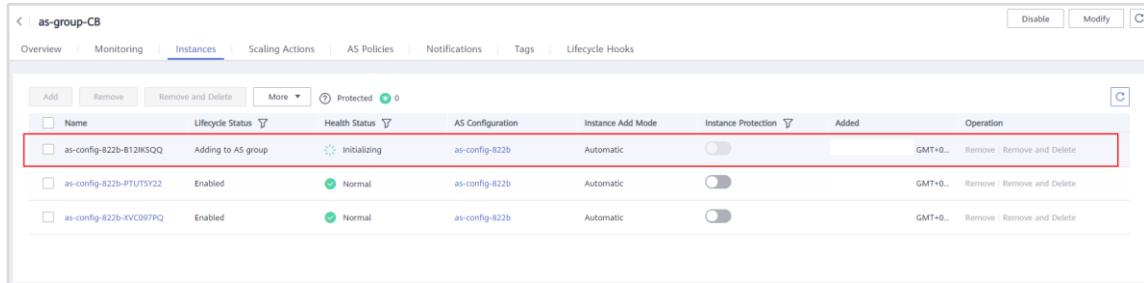


Figure 2-89 Viewing instance scaling

2.2.4.3 Creating a Bandwidth Scaling Policy

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.

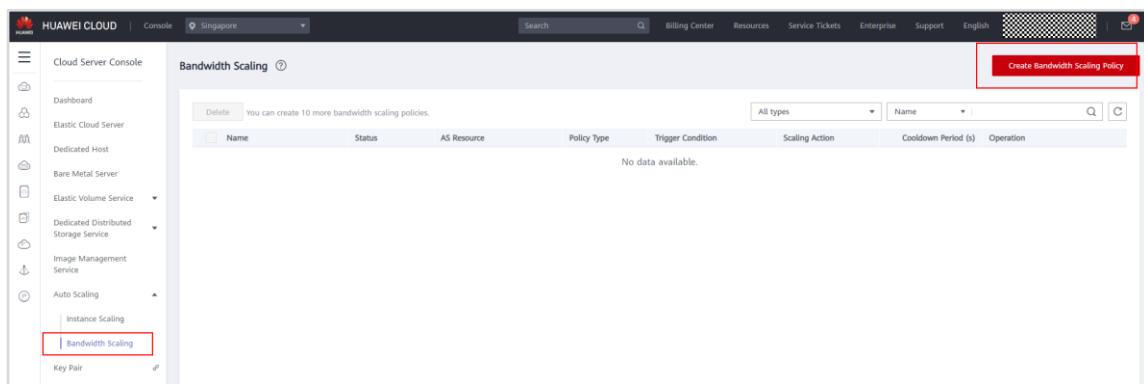
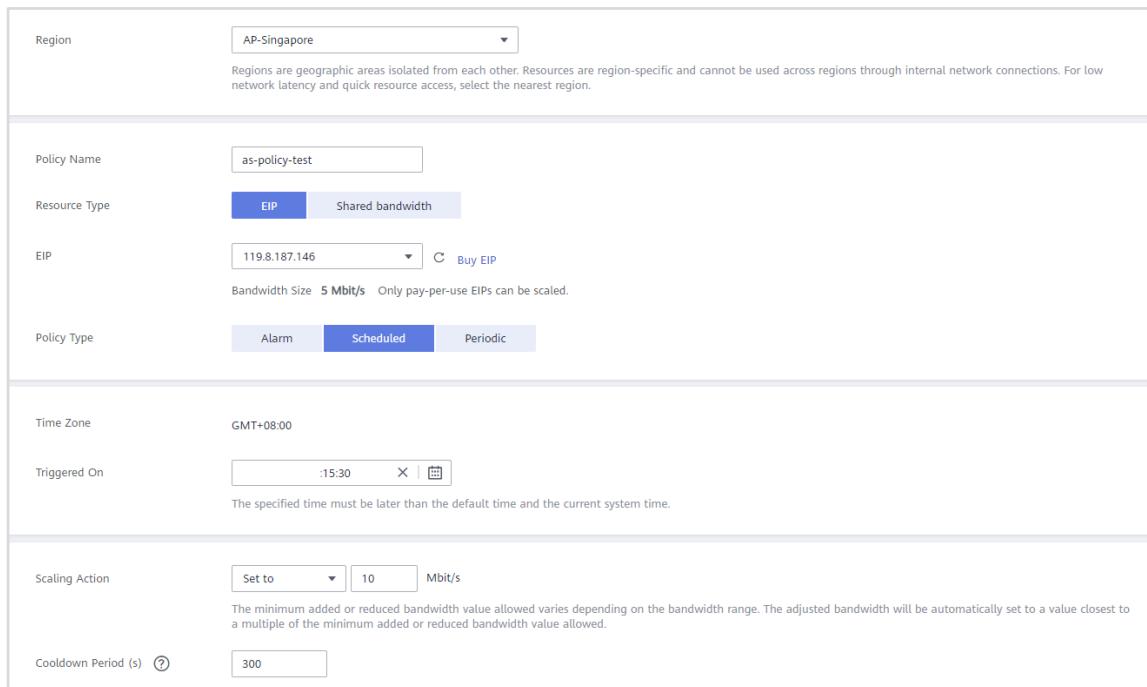


Figure 2-90 Creating a bandwidth scaling policy

Set the following parameters:

- **Region: LA-SaoPaulo**
- **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**



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.

Policy Name: as-policy-test
Resource Type: EIP (selected)
EIP: 119.8.187.146 (Buy EIP)
Policy Type: Alarm, Scheduled (selected), Periodic

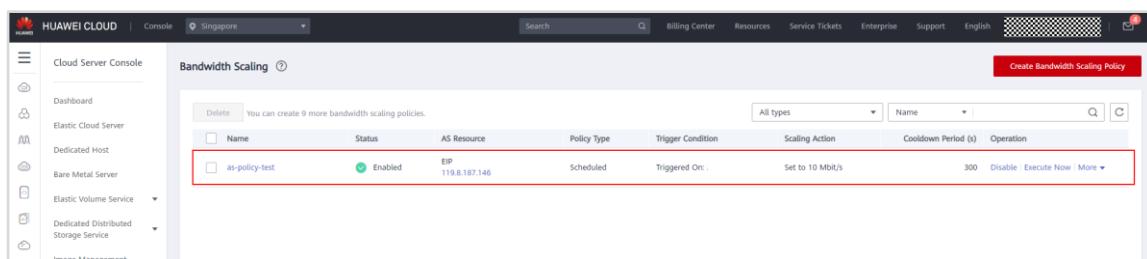
Time Zone: GMT+08:00
Triggered On: 15:30
The specified time must be later than the default time and the current system time.

Scaling Action: Set to 10 Mbit/s
The minimum added or reduced bandwidth value allowed varies depending on the bandwidth range. The adjusted bandwidth will be automatically set to a value closest to a multiple of the minimum added or reduced bandwidth value allowed.
Cooldown Period (s): 300

Figure 2-91 Configuring a bandwidth scaling policy

Click Create Now.

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 Condition | Scaling Action | Cooldown Period (s) | Operation |
|----------------|---------|-------------------|-------------|-------------------|------------------|---------------------|--------------------------------|
| as-policy-test | Enabled | EIP 119.8.187.146 | Scheduled | Triggered On: | Set to 10 Mbit/s | 300 | Disable Execute Now More ▾ |

Figure 2-92 Viewing the bandwidth scaling policy

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.

| Associated Instance | | | |
|---------------------|---|--------------|------------------------|
| Instance Name | as-config-822b-B12IKSQQ | VPC | vpc-default |
| Instance ID | 39da515c-a9be-47dd-9a61-4726f5da1f7c | Subnet | subnet-default |
| Instance Type | ECS | AZ | AZ3 |
| Status | Running | Bound NICs | 192.168.0.66 |
| Bandwidth | | Tags | |
| Bandwidth Name | as-config-822b-B12IKSQQ-bandwidth-815e | Billing Mode | Pay-per-use |
| Bandwidth ID | 765487ca-fcea-4fdb-ad57-d12e1c799a5f | View Metric | Modify |
| Billed By | Bandwidth | | |
| Bandwidth Type | Dedicated | | |

Figure 2-93 Viewing the bandwidth

2.2.5 Deleting Resources

Delete the ECSs.

Delete the private images.

Delete the AS group and configuration.

Delete the subnet and then the VPC.

Confirm that all the resources created in the experiment have been deleted. If they have not, delete them.

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 them.
- 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 VPC peering connection to enable ECSs in different VPCs in the same region to communicate with each other and create a VPN connection to enable ECSs in different regions to communicate with each other.

3.1.2 Objectives

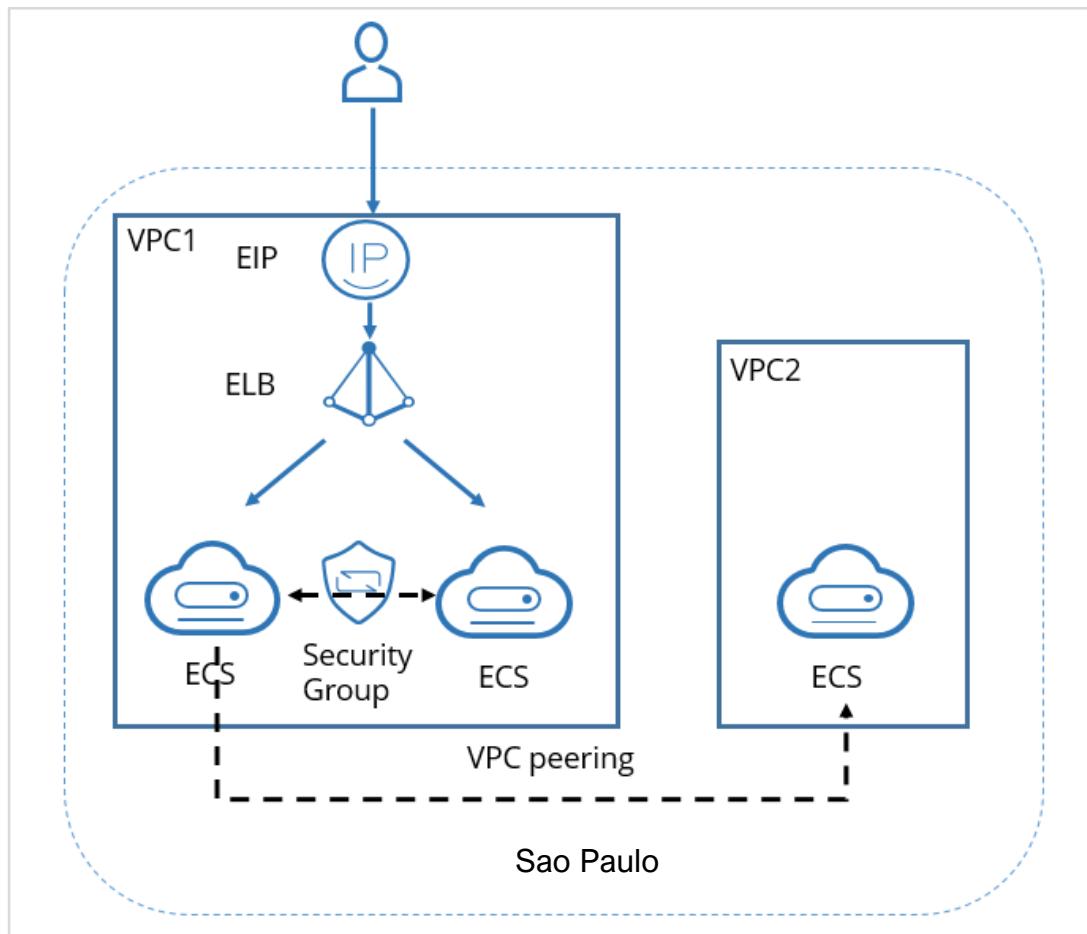
- Learn how to enable communication between different ECSs in a VPC.
- Learn how to use security groups to control communication between ECSs.
- Learn how to use EIP to allow an ECS to access the Internet.

- 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.
- Exercises

3.2 Tasks

3.2.1 Roadmap

- Create two VPCs in **LA-Sao Paulo**, one VPC in **AF-Johannesburg**, and one VPC in **LA-Santiago**.
- Verify that security groups can control communication between ECSs in **LA-Sao Paulo1**.
- Verify that an ECS with an EIP bound can access the Internet in **LA-Sao Paulo1**.
- Verify that ECSs in different VPCs in the same region (**LA-Sao Paulo1**) can communicate with each other through a VPC peering connection.
- Verify that ECSs in different regions (**LA-Santiago** and **AF-Johannesburg**) can communicate with each other through a VPN connection.
- Delete resources.



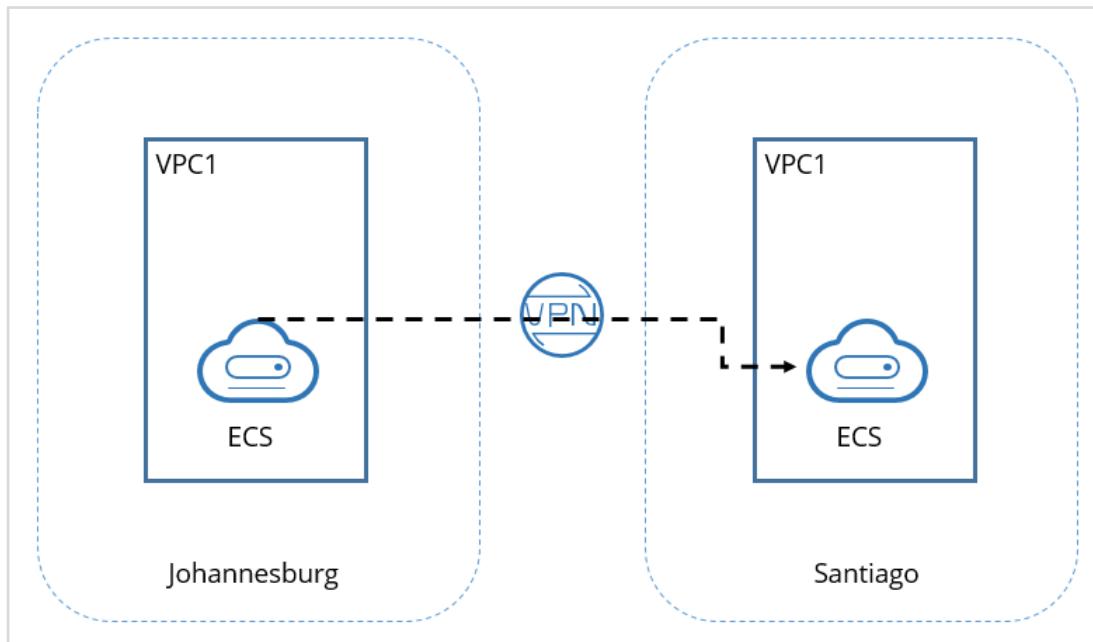


Figure 3-1 Network topology

EXERCÍCIO: ESBOÇAR UM DIAGRAMA DE REDE MAIS DETALHADO (ENDEREÇAMENTO, CONEXÕES, ETC.)

3.2.2 Creating VPCs

Tasks:

- Create VPC-S01 with subnet-01 and subnet-02, and VPC-S02 with subnet-03 in **LA-Sao Paulo**.
- Create VPC-J01 with subnet-01 in **AF-Johannesburg**.
- Create VPC-Sa01 with subnet-01 in **LA-Santiago**.

Use this table as reference:

| REGION | | LA-SaoPaulo1 | | AF-Johannesburg | LA-Santiago |
|--------|----------------|----------------|-------------|-----------------|---------------|
| VPC | Name | vpc-S01 | | vpc-S02 | vpc-J01 |
| CIDR | | 192.168.0.0/16 | | 10.0.0.0/24 | 172.16.0.0/16 |
| SUBNET | subnet-01 | subnet-02 | subnet-03 | subnet-01 | subnet-01 |
| | 192.168.0.0/16 | 192.168.1.0/16 | 10.0.0.0/24 | 192.168.0.0/16 | 172.16.0.0/12 |

Log in to the management console and select the **LA-Sao Paulo** region. Click Service List. Under Networking, select Virtual Private Cloud.

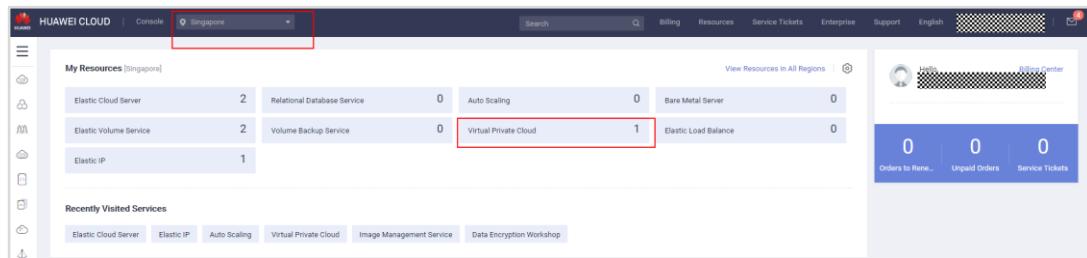


Figure 3-2 Switching to VPC console

Click Create VPC.

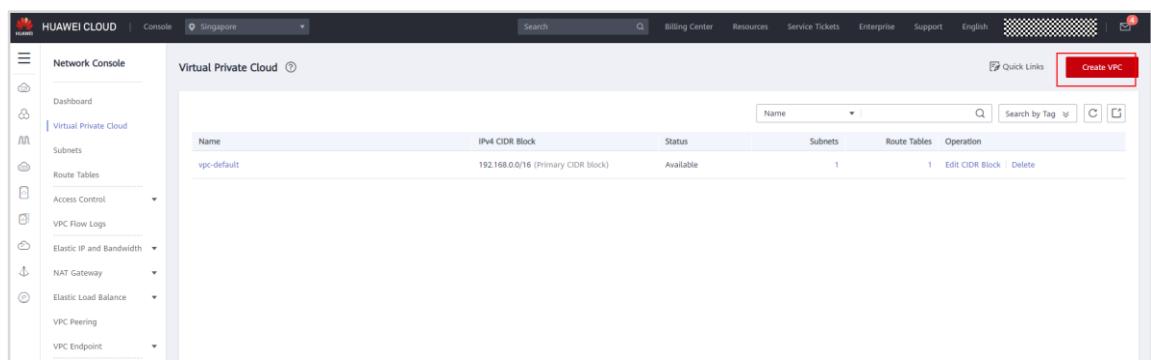
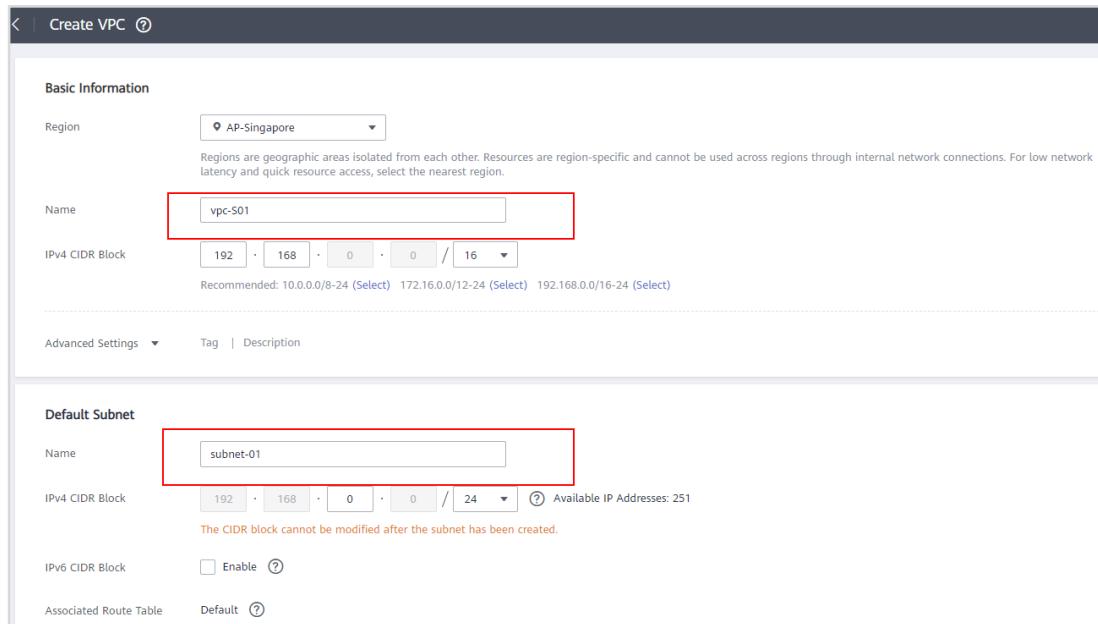


Figure 3-3 Create VPC

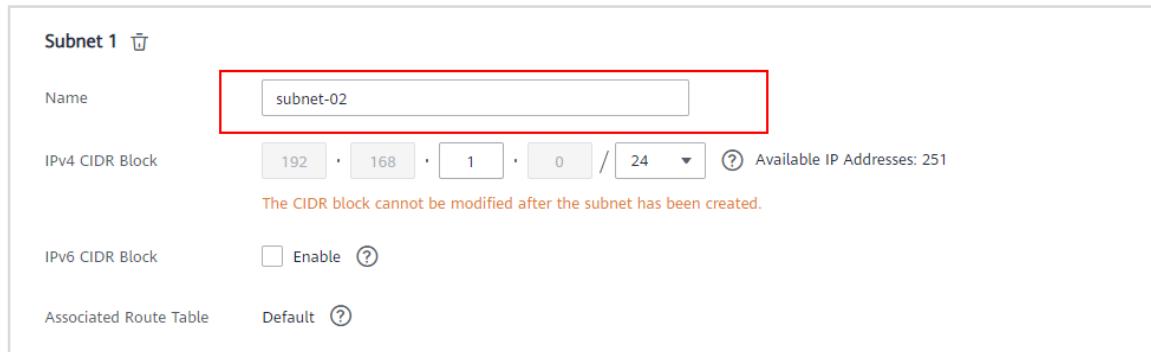
Configure the VPC parameters as follows and click Create Now.

- Region: LA-Sao Paulo
- 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.



The screenshot shows the 'Create VPC' interface. In the 'Basic Information' section, the 'Region' is set to 'AP-Singapore'. The 'Name' field contains 'vpc-S01', which is highlighted with a red box. The 'IPv4 CIDR Block' is set to '192.168.0.0/16', with the prefix length dropdown set to '16'. In the 'Default Subnet' section, the 'Name' field contains 'subnet-01', also highlighted with a red box. The 'IPv4 CIDR Block' is set to '192.168.0.0/24', with the prefix length dropdown set to '24'. The 'Available IP Addresses' is shown as 251. Below this, there are fields for 'IPv6 CIDR Block' (disabled), 'Associated Route Table' (set to 'Default'), and a 'Description' field.

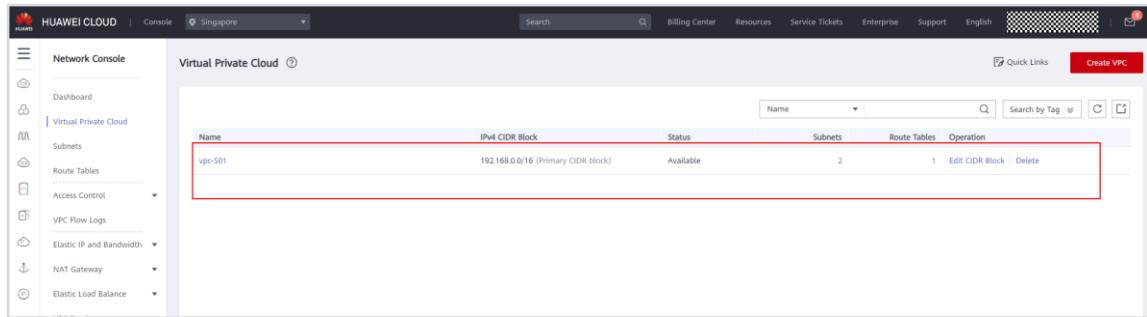
Figure 3-4 Configuring the VPC



The screenshot shows the 'Subnet 1' configuration interface. The 'Name' field contains 'subnet-02', which is highlighted with a red box. The 'IPv4 CIDR Block' is set to '192.168.1.0/24', with the prefix length dropdown set to '24'. A note below states 'The CIDR block cannot be modified after the subnet has been created.' There are fields for 'IPv6 CIDR Block' (disabled), 'Associated Route Table' (set to 'Default'), and a 'Description' field.

Figure 3-5 Configuring the VPC

View the created VPC in the VPC list.

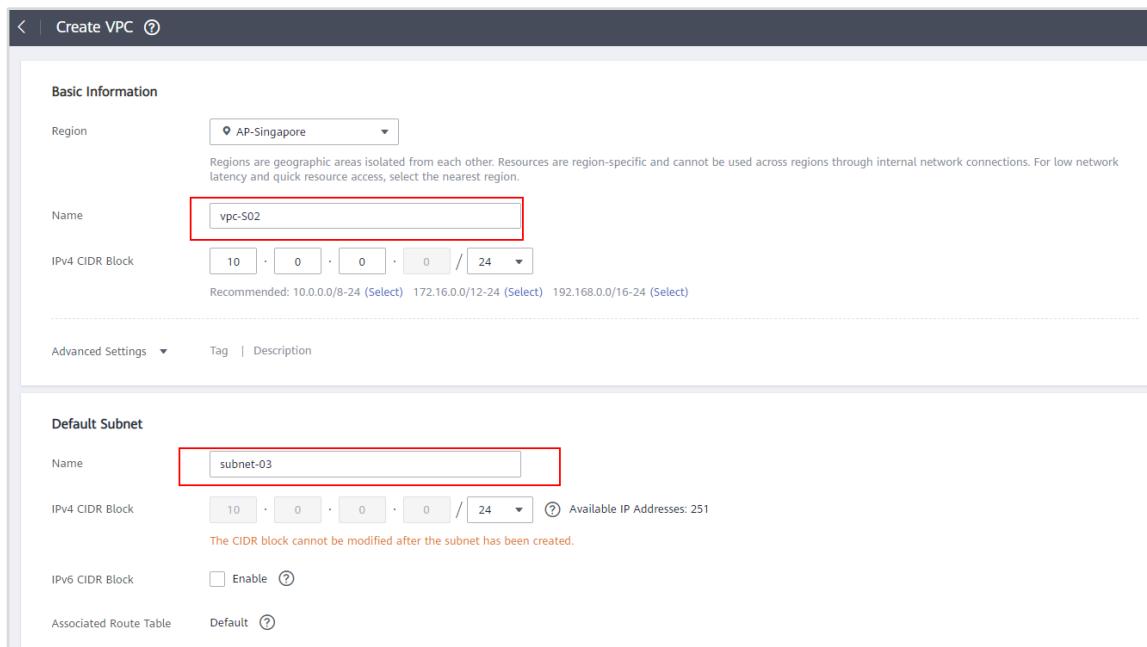


| Name | IPv4 CIDR Block | Status | Subnets | Route Tables | Operation |
|---------|-------------------------------------|-----------|---------|--------------|--|
| vpc-501 | 192.168.0.0/16 (Primary CIDR block) | Available | 2 | 1 | Edit CIDR Block Delete |

Figure 3-6 Viewing the VPC

Click Create VPC again and configure the VPC parameters as follows.

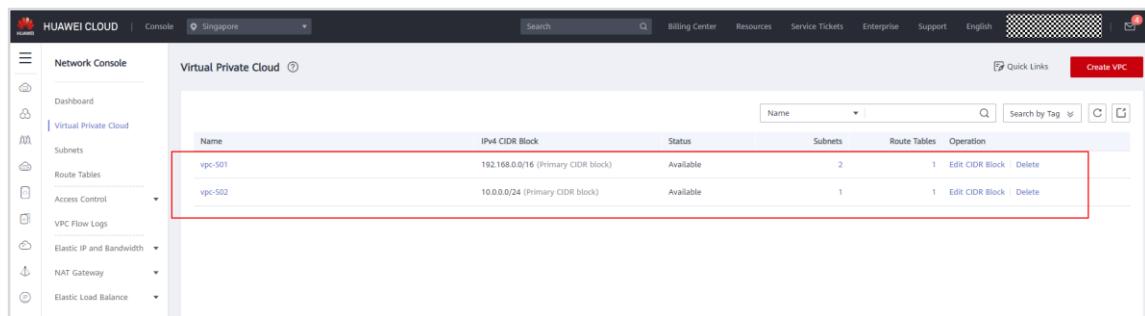
- Region: **LA-Sao Paulo**
- Name: **VPC-So2**
- CIDR Block: Set a CIDR block different from that of VPC-So1, for example, **10.0.0.0/24**.
- Default subnet name: **subnet-03**
- Retain the default settings for other parameters.



| | |
|------------------------|-------------------|
| Region | AP-Singapore |
| Name | vpc-502 |
| IPv4 CIDR Block | 10.0.0.0/24 |
| Advanced Settings | Tag Description |
| Name | subnet-03 |
| IPv4 CIDR Block | 10.0.0.0/24 |
| Associated Route Table | Default |

Figure 3-7 Configuring the VPC

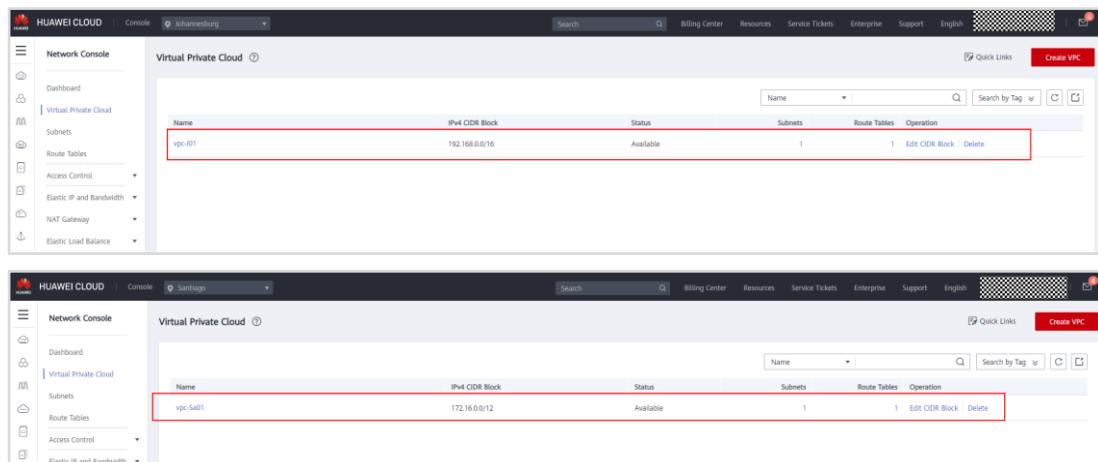
View the created VPC in the VPC list.



| Name | IPv4 CIDR Block | Status | Subnets | Route Tables | Operation |
|---------|-------------------------------------|-----------|---------|--------------|--------------------------|
| vpc-501 | 192.168.0.0/16 (Primary CIDR block) | Available | 2 | 1 | Edit CIDR Block Delete |
| vpc-502 | 10.0.0.0/24 (Primary CIDR block) | Available | 1 | 1 | Edit CIDR Block Delete |

Figure 3-8 Viewing the VPC

Create VPC-Jo1 with subnet-01 in AF-Johannesburg and VPC-Sao1 with subnet-01 in LA-Santiago.



| Name | IPv4 CIDR Block | Status | Subnets | Route Tables | Operation |
|---------|-----------------|-----------|---------|--------------|--------------------------|
| vpc-jo1 | 192.168.0.0/16 | Available | 1 | 1 | Edit CIDR Block Delete |

| Name | IPv4 CIDR Block | Status | Subnets | Route Tables | Operation |
|----------|-----------------|-----------|---------|--------------|--------------------------|
| vpc-sa01 | 172.16.0.0/12 | Available | 1 | 1 | Edit CIDR Block Delete |

Figure 3-9 Viewing the VPC

3.2.3 Buying ECSs

Tasks:

- In the **LA-Sao Paulo01** region, create two ECSs in **VPC-So1**, one in **subnet-01** and one in **subnet-02**, and one ECS in **subnet-03** of **VPC-So2**.
- In the **AF-Johannesburg** region, create an ECS in **subnet-01** of **VPC-Jo1**.
- In the **LA-Santiago** region, create an ECS in **subnet-01** of **VPC-Sao1**.

Select the **LA-Sao Paulo** region, click Service List. Under Compute, select Elastic Cloud Server.

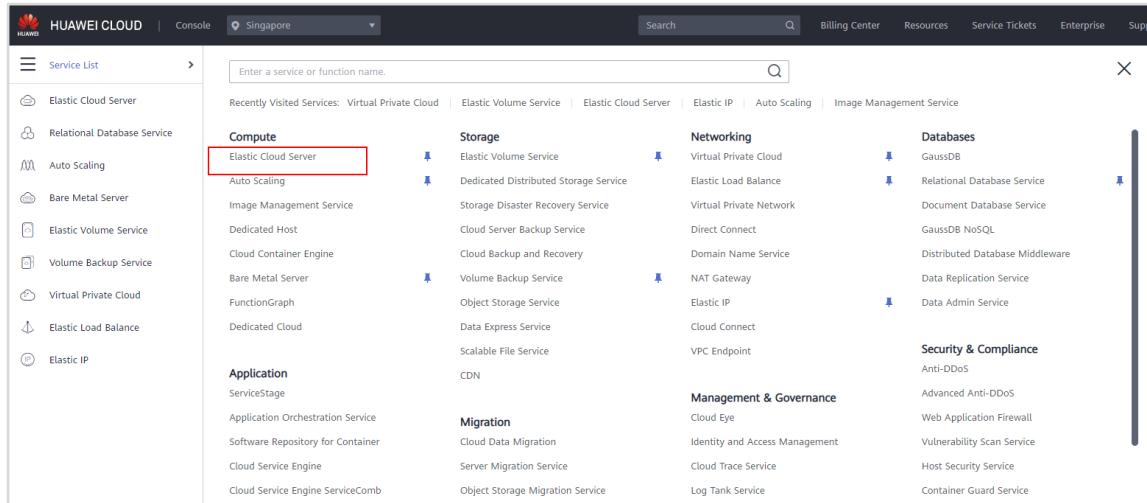


Figure 3-10 Switching to ECS console

Click Buy ECS.

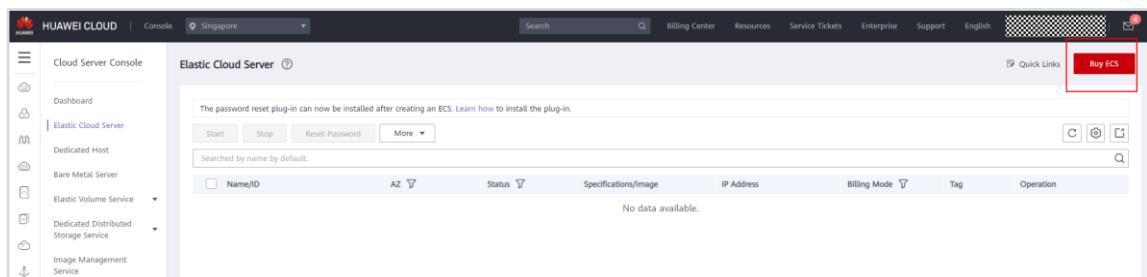
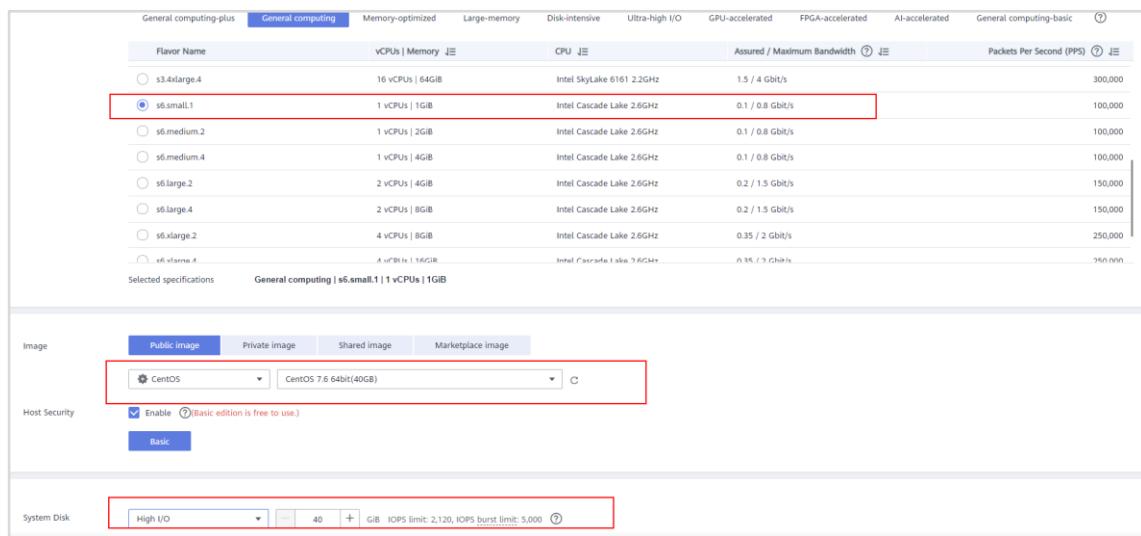


Figure 3-11 Buy ECS

Configure the parameters as follows.

Basic settings:

- **Billing Mode:** Pay-per-use
- **Region:** LA-Sao Paulo
- **AZ:** Random
- **CPU Architecture:** x86
- **Specifications:** General computing-basic, t6.small.1, 1 vCPUs | 1GB
- **Image:** Public image, CentOS 7.6 64bit(40GB)
- **System Disk:** High I/O, 40 GB



The screenshot shows the configuration steps for creating an ECS instance:

- Selected Specifications:** General computing | s6.small.1 | 1 vCPUs | 1GB
- Image:** CentOS 7.6 64bit(40GB) (selected)
- Host Security:** Enable (checkbox checked)
- System Disk:** High I/O, 40 GB

Figure 3-12 Configuring the ECS

Network configuration:

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

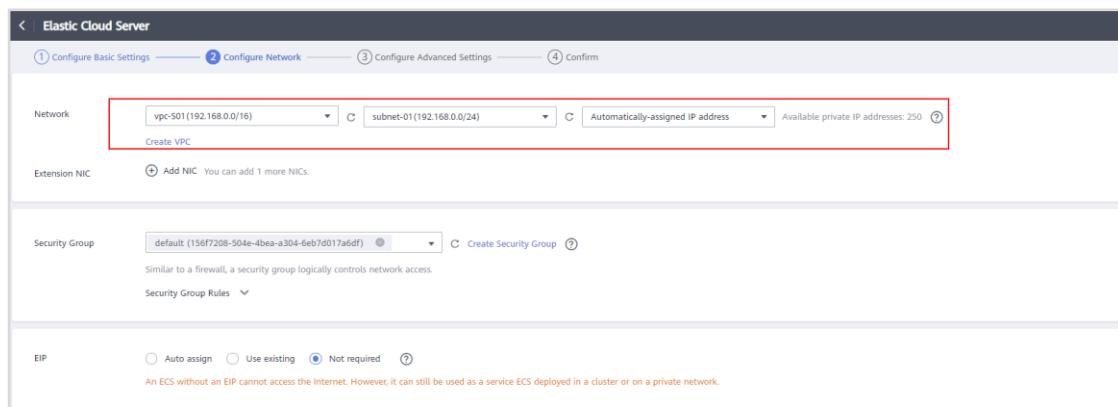


Figure 3-13 Configuring the ECS

Advanced settings:

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

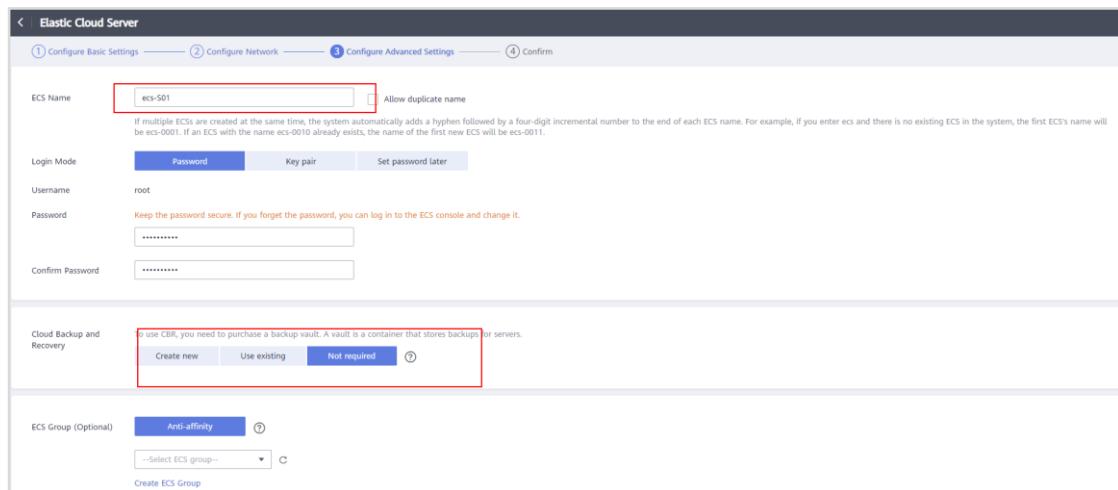


Figure 3-14 Configuring the ECS

Confirm the configuration and click Submit.

Figure 3-15 Confirming the configuration

Repeat the preceding steps to create **ecs-S02** in **subnet-02**, **ecs-S03** in **subnet-03**, **ecs-J01** in **subnet-01**, and **ecs-Sa01** in **subnet-01**. You can create a general computing-basic ECS with flavor t6.small.1 (or s3.small.1), 1 vCPU1, and 1 GB of memory in the LA-Santiago and AF-Johannesburg regions.

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

On the ECS console, switch to the LA-Sao Paulo region, make a note of the private IP address of ecs-So1, and log in to ecs-So2 remotely.

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|--|-----|---------|---|----------------------------|----------------------------------|-----|-----------------------|
| ecs-So1 88c6d9ba-6766-47fb-9309-37dfc9... | AZ1 | Running | 1 vCPU 1GB s6.small.1 CentOS 7.6 64bit | 10.0.0.70 (Private IP) | Pay-per-use Created on Jul... | - | Remote Login More ▾ |
| ecs-So2 e8543722-397c-447f-818a-982f3e... | AZ1 | Running | 1 vCPU 1GB s6.small.1 CentOS 7.6 64bit | 192.168.1.109 (Private IP) | Pay-per-use Created on Jul... | - | Remote Login More ▾ |
| ecs-So3 20f82eb1-5d3c-4a65-ae7f-9c0d86... | AZ1 | Running | 1 vCPU 1GB s6.small.1 CentOS 7.6 64bit | 192.168.0.87 (Private IP) | Pay-per-use Created on Jul... | - | Remote Login More ▾ |

Figure 3-17 Remotely logging in to the ECS

Enter the username (root for a Linux ECS by default) and password to log in to ecs-So2.

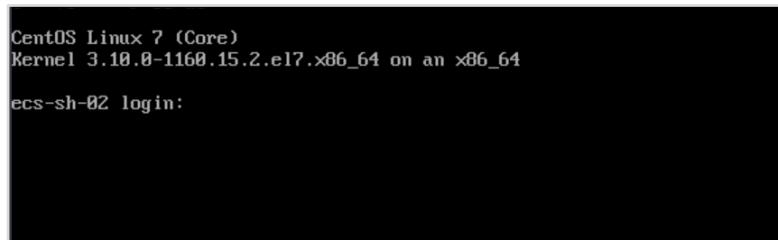


Figure 3-18 Logging in to the Linux ECS

Ping the private IP address of ecs-So1 from ecs-So2 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.

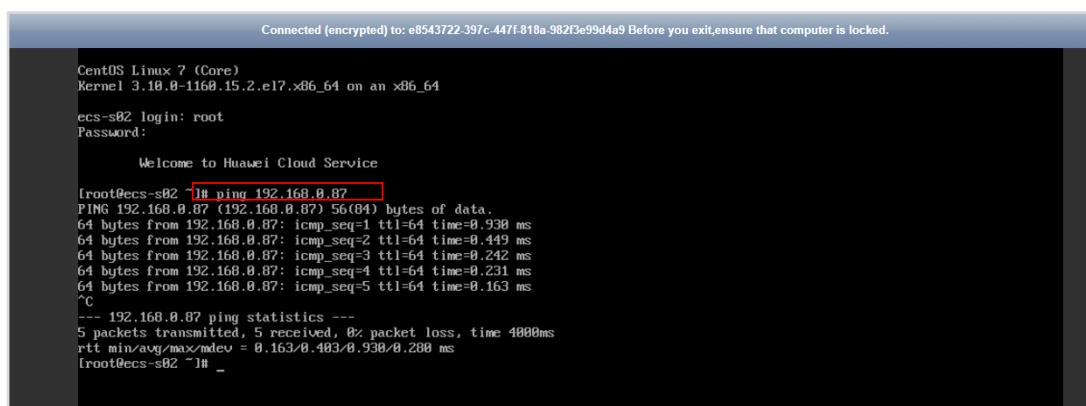


Figure 3-19 Successful ping

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 10.0.0.70
PING 10.0.0.70 (10.0.0.70) 56(84) bytes of data.
```

Figure 3-20 Ping failure

3.2.4.2 Traffic Control by Security Groups

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

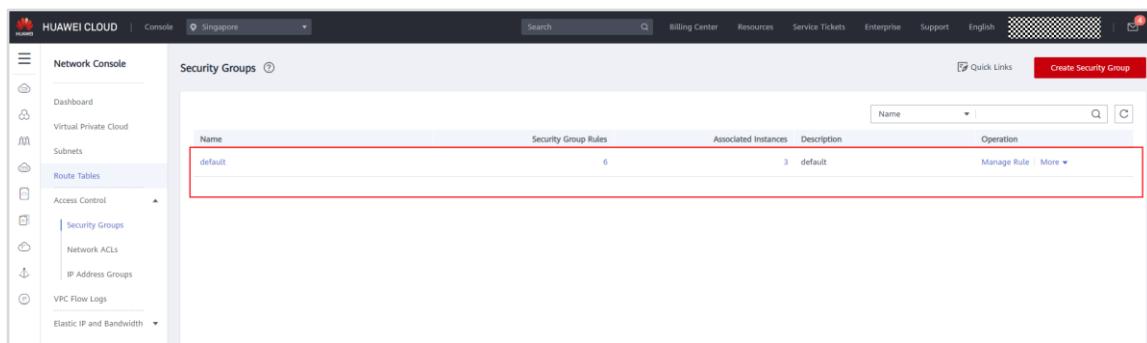


Figure 3-21 Viewing the security group

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

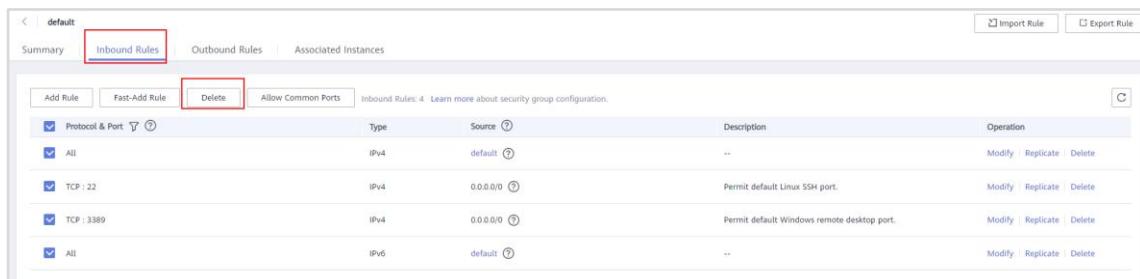
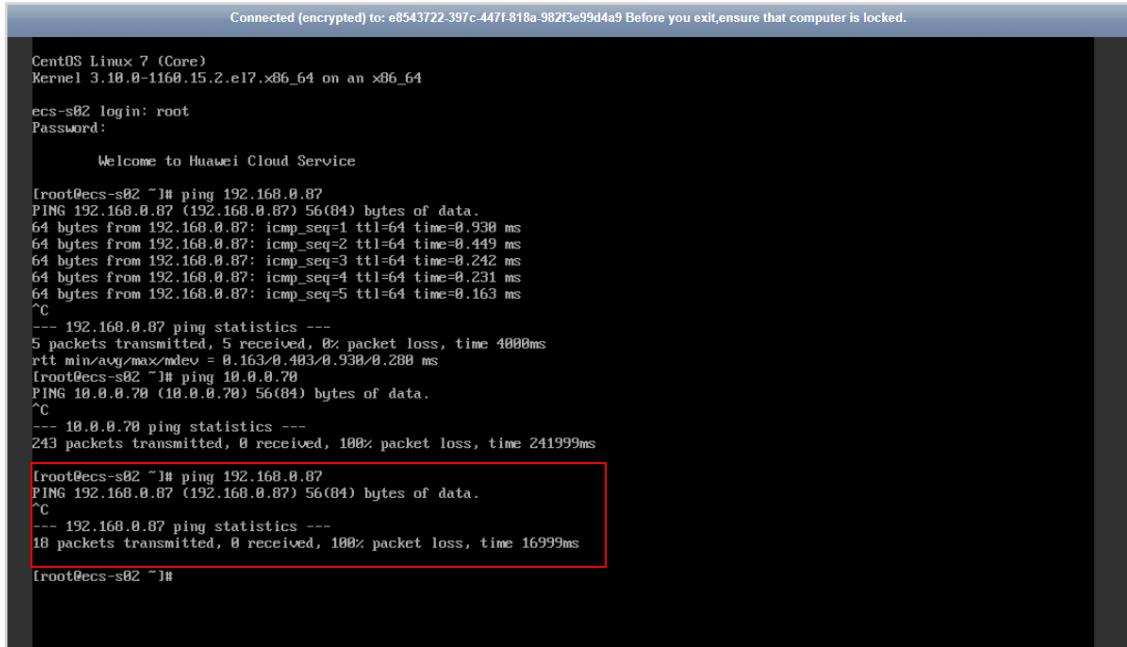


Figure 3-22 Deleting inbound rules

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.



The screenshot shows a terminal session on a CentOS Linux 7 (Core) system. The user logs in as root and runs several ping commands. The first command pings the private IP 192.168.0.87 from the local interface 192.168.0.87, showing successful round-trip times. The second command pings the public IP 10.0.0.70 from the same interface, also showing success. The third command, highlighted with a red box, attempts to ping the private IP 192.168.0.87 from the public interface 10.0.0.70, but fails with 100% packet loss.

```
Connected (encrypted) to e8543722-397c-447f-818a-982f3e99d4a9 Before you exit, ensure that computer is locked.

CentOS Linux 7 (Core)
Kernel 3.10.0-1160.15.2.el7.x86_64 on an x86_64

ecs-s02 login: root
Password:

Welcome to Huawei Cloud Service

[root@ecs-s02 ~]# ping 192.168.0.87
PING 192.168.0.87 (192.168.0.87) 56(84) bytes of data.
64 bytes from 192.168.0.87: icmp_seq=1 ttl=64 time=0.938 ms
64 bytes from 192.168.0.87: icmp_seq=2 ttl=64 time=0.449 ms
64 bytes from 192.168.0.87: icmp_seq=3 ttl=64 time=0.242 ms
64 bytes from 192.168.0.87: icmp_seq=4 ttl=64 time=0.231 ms
64 bytes from 192.168.0.87: icmp_seq=5 ttl=64 time=0.163 ms
^C
--- 192.168.0.87 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.163/0.483/0.930/0.288 ms
[root@ecs-s02 ~]# ping 10.0.0.70
PING 10.0.0.70 (10.0.0.70) 56(84) bytes of data.
^C
--- 10.0.0.70 ping statistics ---
243 packets transmitted, 0 received, 100% packet loss, time 241999ms

[root@ecs-s02 ~]# ping 192.168.0.87
PING 192.168.0.87 (192.168.0.87) 56(84) bytes of data.
^C
--- 192.168.0.87 ping statistics ---
18 packets transmitted, 0 received, 100% packet loss, time 16999ms

[root@ecs-s02 ~]#
```

Figure 3-23 Ping failure

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

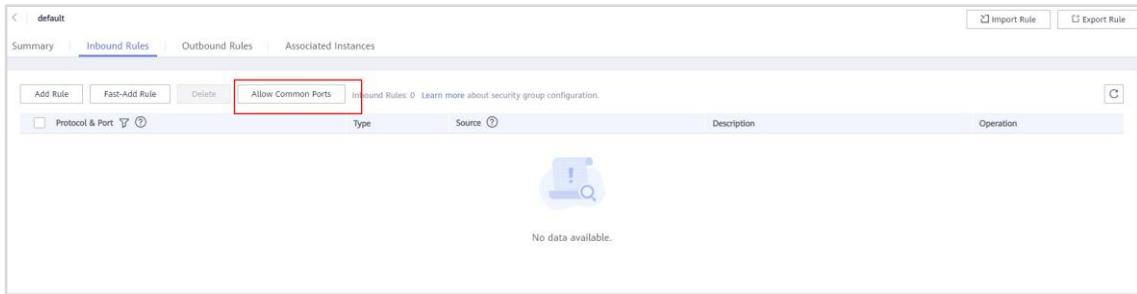
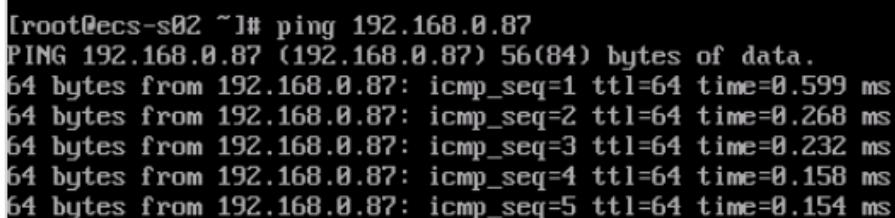


Figure 3-24 Allow Common Ports

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 ECSS can communicate with each other, indicating that the security group can be used to control communication.



The screenshot shows a terminal session on a CentOS Linux 7 (Core) system. The user logs in as root and runs a ping command to the private IP 192.168.0.87. The response shows successful round-trip times for multiple ICMP packets, indicating a successful connection between the two ECS instances.

```
[root@ecs-s02 ~]# ping 192.168.0.87
PING 192.168.0.87 (192.168.0.87) 56(84) bytes of data.
64 bytes from 192.168.0.87: icmp_seq=1 ttl=64 time=0.599 ms
64 bytes from 192.168.0.87: icmp_seq=2 ttl=64 time=0.268 ms
64 bytes from 192.168.0.87: icmp_seq=3 ttl=64 time=0.232 ms
64 bytes from 192.168.0.87: icmp_seq=4 ttl=64 time=0.158 ms
64 bytes from 192.168.0.87: icmp_seq=5 ttl=64 time=0.154 ms
```

Figure 3-25 Successful ping

3.2.4.3 Access to the Internet with an EIP

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 (39.156.69.79) 56(84) bytes of data.
```

Figure 3-26 Verifying Internet access

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. The following steps describe how to use a key pair to log in to the ECS.

Click Service List, search for Data Encryption Workshop, and click Data Encryption Workshop to go to the DEW console.

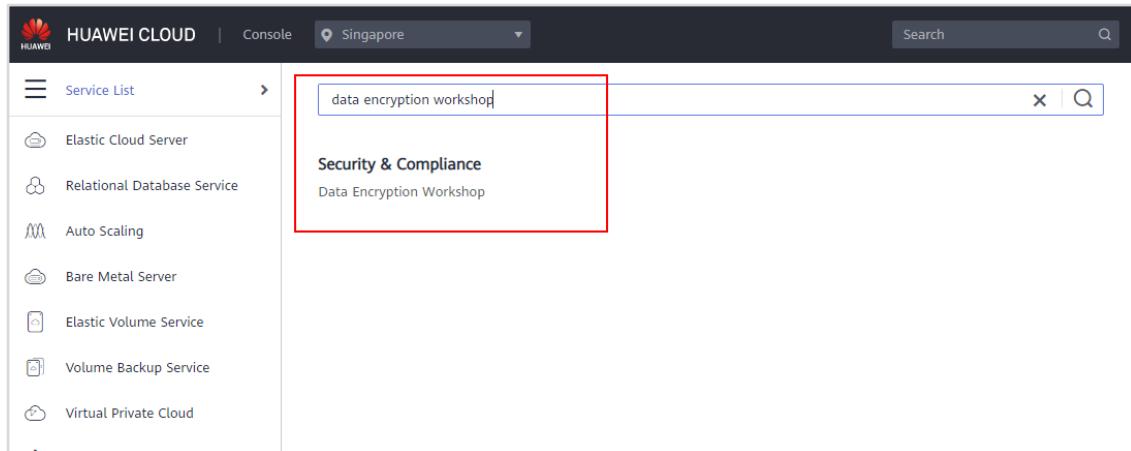


Figure 3-27 Switching to DEW console

In the navigation pane on the left, choose Key Pair Service. On the ECS List tab page, locate the row that contains ecs-S02 and click Bind in the Operation column.

| Key Pair Service | | | | | | |
|---|---------|--------------------|--------------------|---------------------|-----------|--|
| Private Key Pairs | | ECS List | | | | |
| ECS Name/ID | Status | Private IP Address | Elastic IP Address | Associated Key Pair | Operation | |
| ecs-S01 88cd696a-6766-47fb-9309-37dfc96c0497 | Running | 10.0.0.70 | -- | -- | Bind | |
| ecs-S02 e8543722-397c-447f-818a-982f3e99d4a9 | Running | 192.168.1.109 | -- | -- | Bind | |
| ecs-S01 20fb2eb1-5d3c-4a65-aef7-9c0d867b9ef4 | Running | 192.168.0.87 | -- | -- | Bind | |

Figure 3-28 Viewing the ECS list

Select the target key pair, enter the password of user root for logging in to the ecs-S02, and click OK.

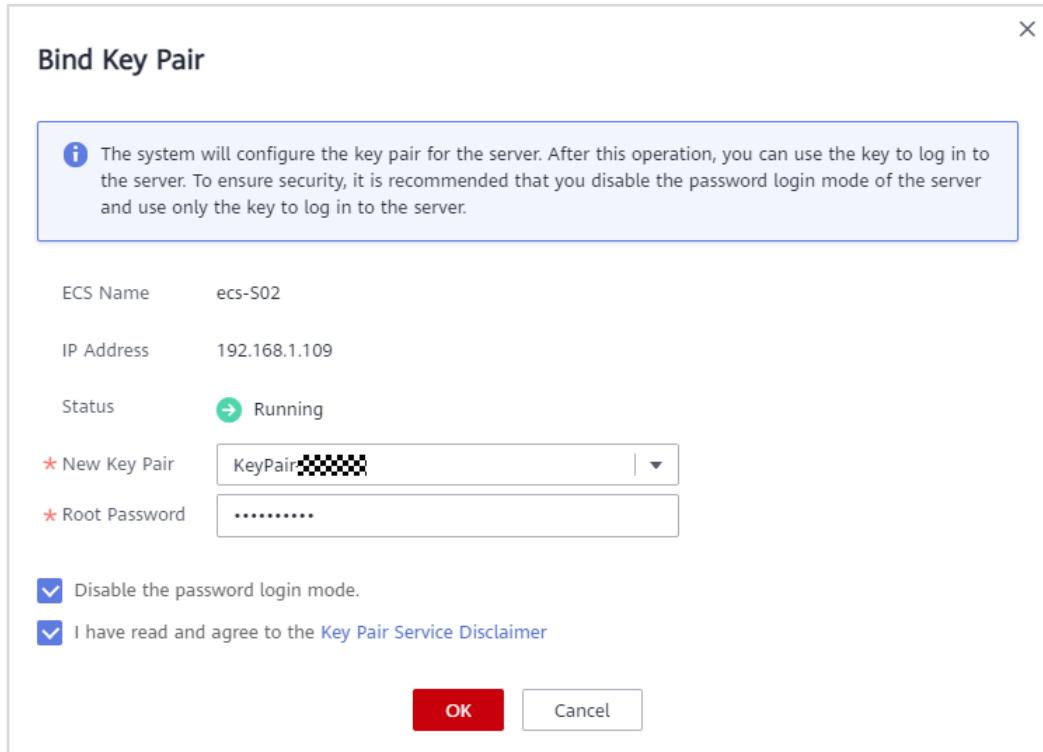
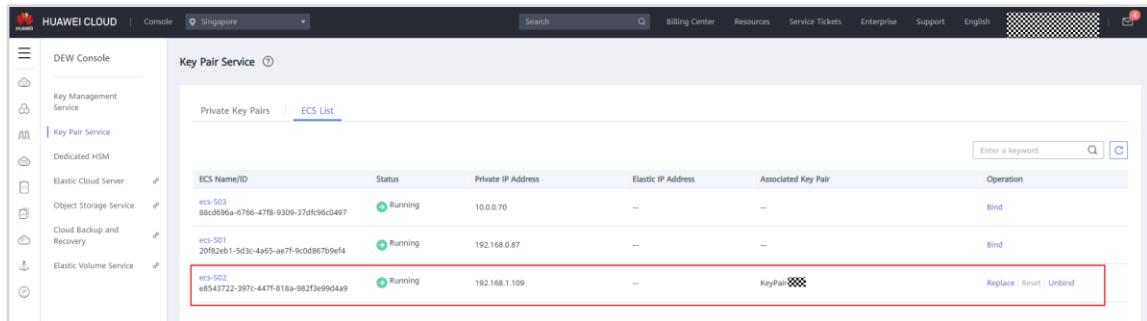


Figure 3-29 Binding a key pair

View the binding result on the ECS List tab page.



| ECS Name/ID | Status | Private IP Address | Elastic IP Address | Associated Key Pair | Operation |
|---|---------|--------------------|--------------------|---------------------|--------------------------|
| ecs-503 88cd96a-6766-47f8-930e-37dfc96cd497 | Running | 10.0.0.70 | -- | -- | Bind |
| ecs-501 2082eb1-5d3c-4a65-ae7f-9c0d887b9ef4 | Running | 192.168.0.87 | -- | -- | Bind |
| ecs-502 e8543722-397c-447f-818a-982f3e99d4a9 | Running | 192.168.1.109 | -- | KeyPair | Replace Reset Unbind |

Figure 3-30 Successful binding

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

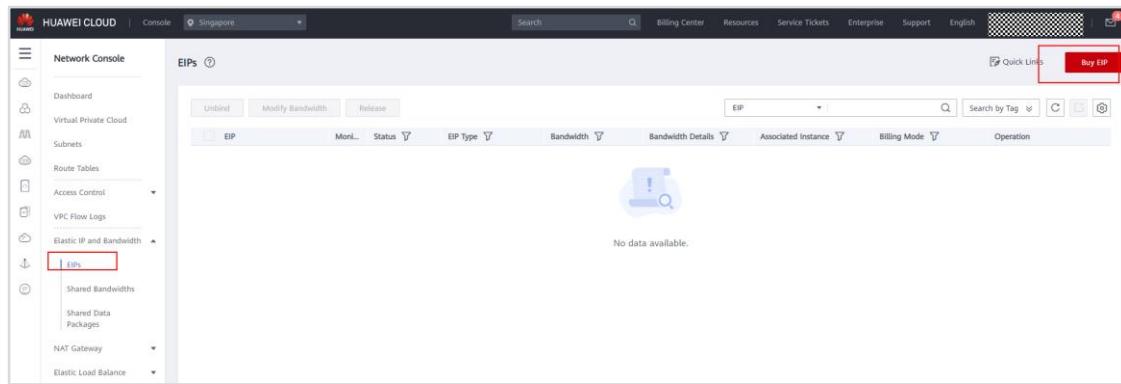
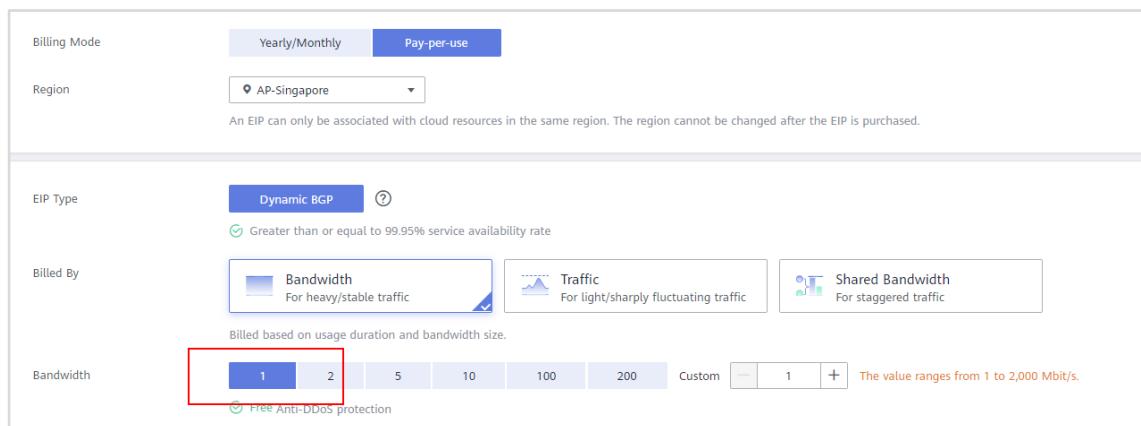


Figure 3-31 Buy EIP

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

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



Billing Mode: Pay-per-use

Region: AP-Singapore

EIP Type: Dynamic BGP

Billed By: Bandwidth

Bandwidth: 1 Mbit/s

Free Anti-DDoS protection

Figure 3-32 Configuring EIP

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

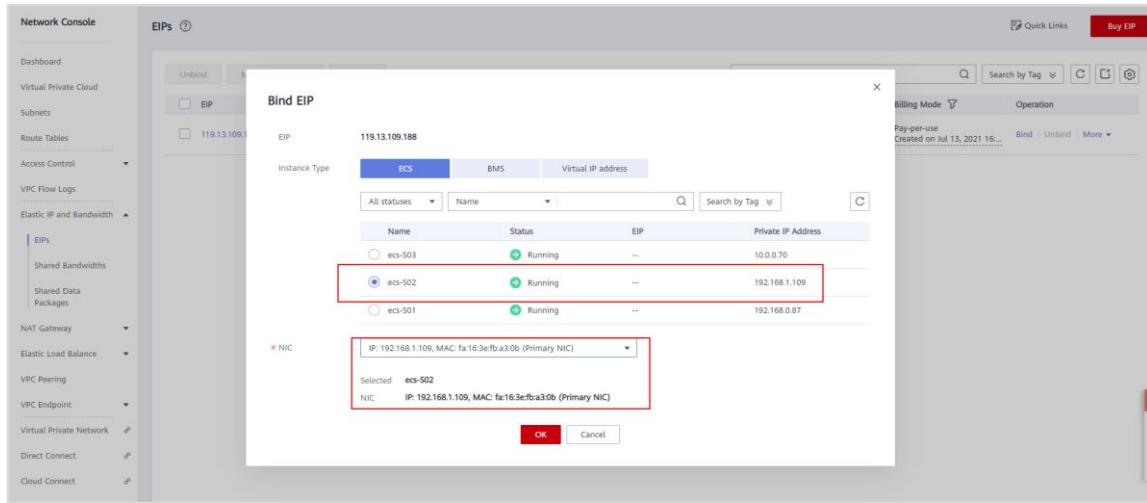


Figure 3-33 Binding an EIP



Figure 3-34 Viewing the EIP

Install PuTTY and PuTTYgen on your local computer. Use PuTTYgen to convert the key pair file format from .pem to .ppk, which is a required format of PuTTY.

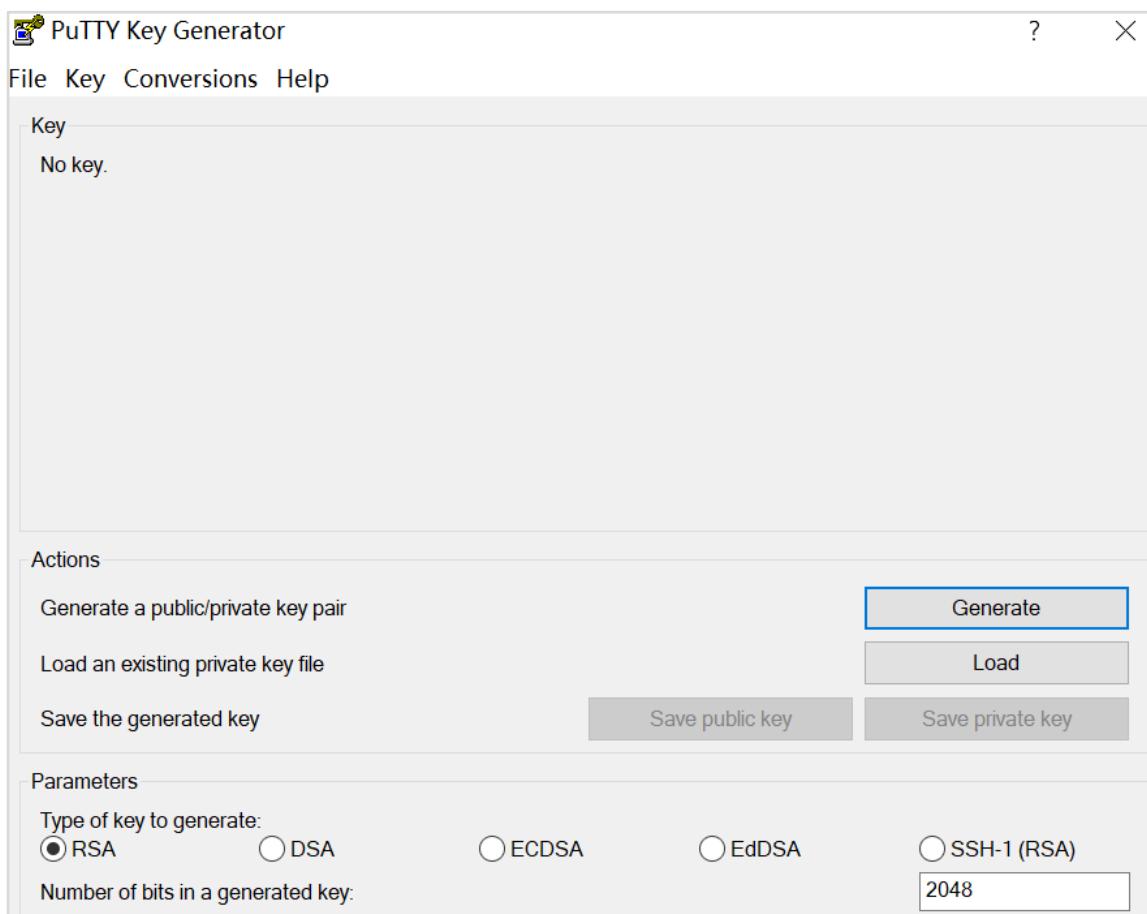


Figure 3-35 Opening the PuTTYgen program

Go to Conversions, and then click Import key to load the key pair file.

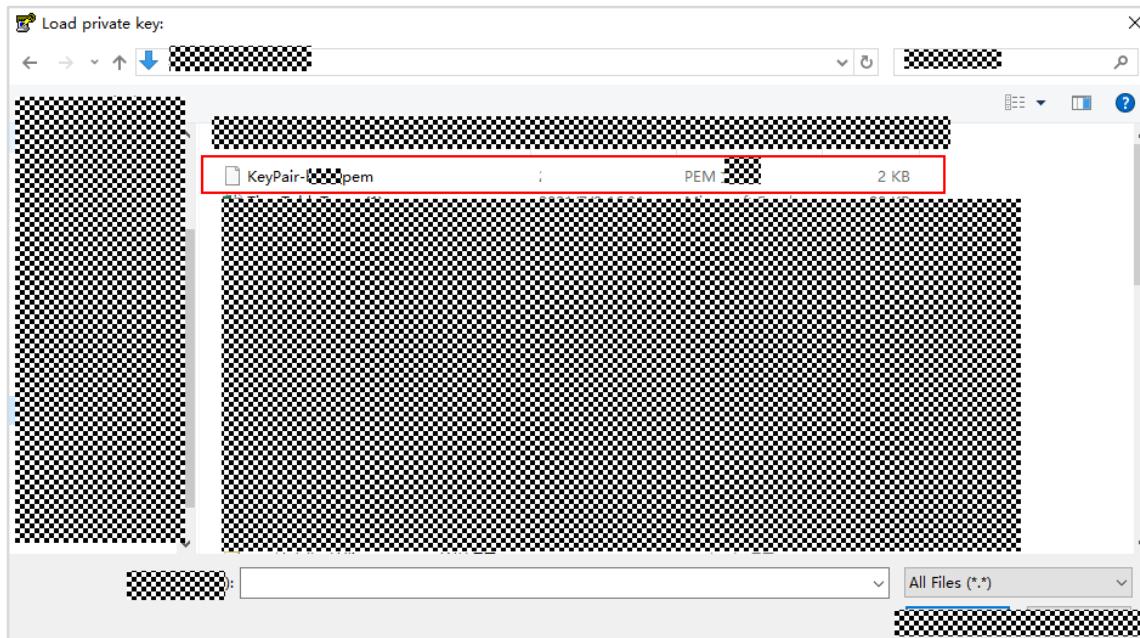


Figure 3-36 Importing the key pair file

Click Save private key to save the key pair file in .ppk format to your local computer.

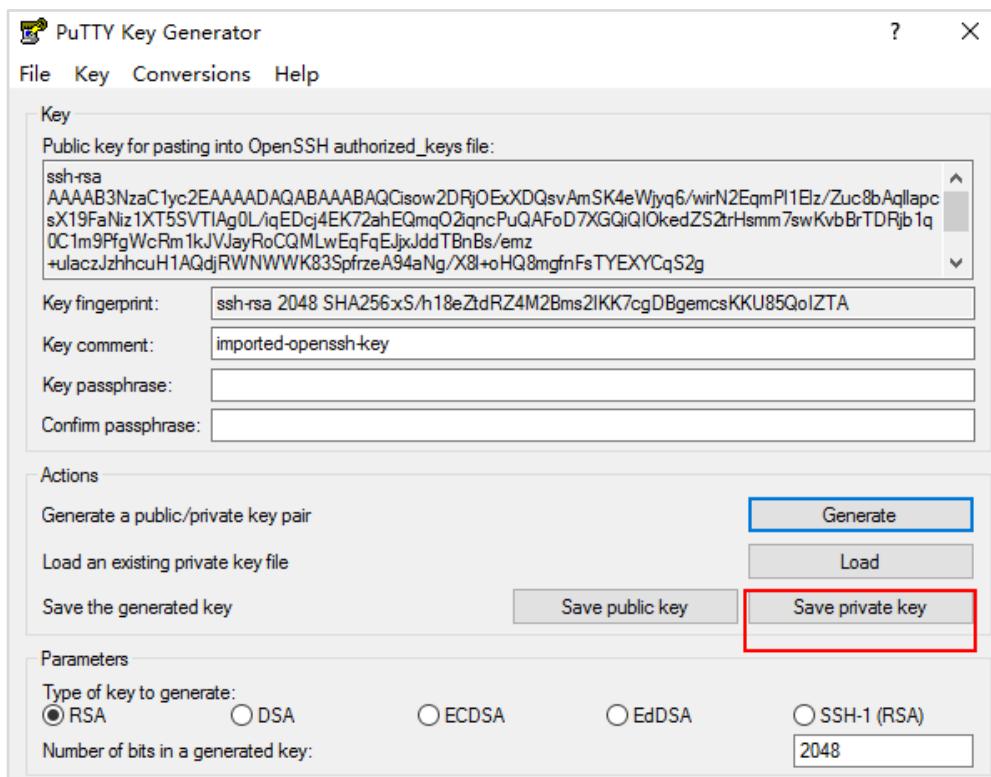


Figure 3-37 Saving the private key file

Open PuTTY, click Connection > Data in the left navigation pane, and set the Auto-login username to root.

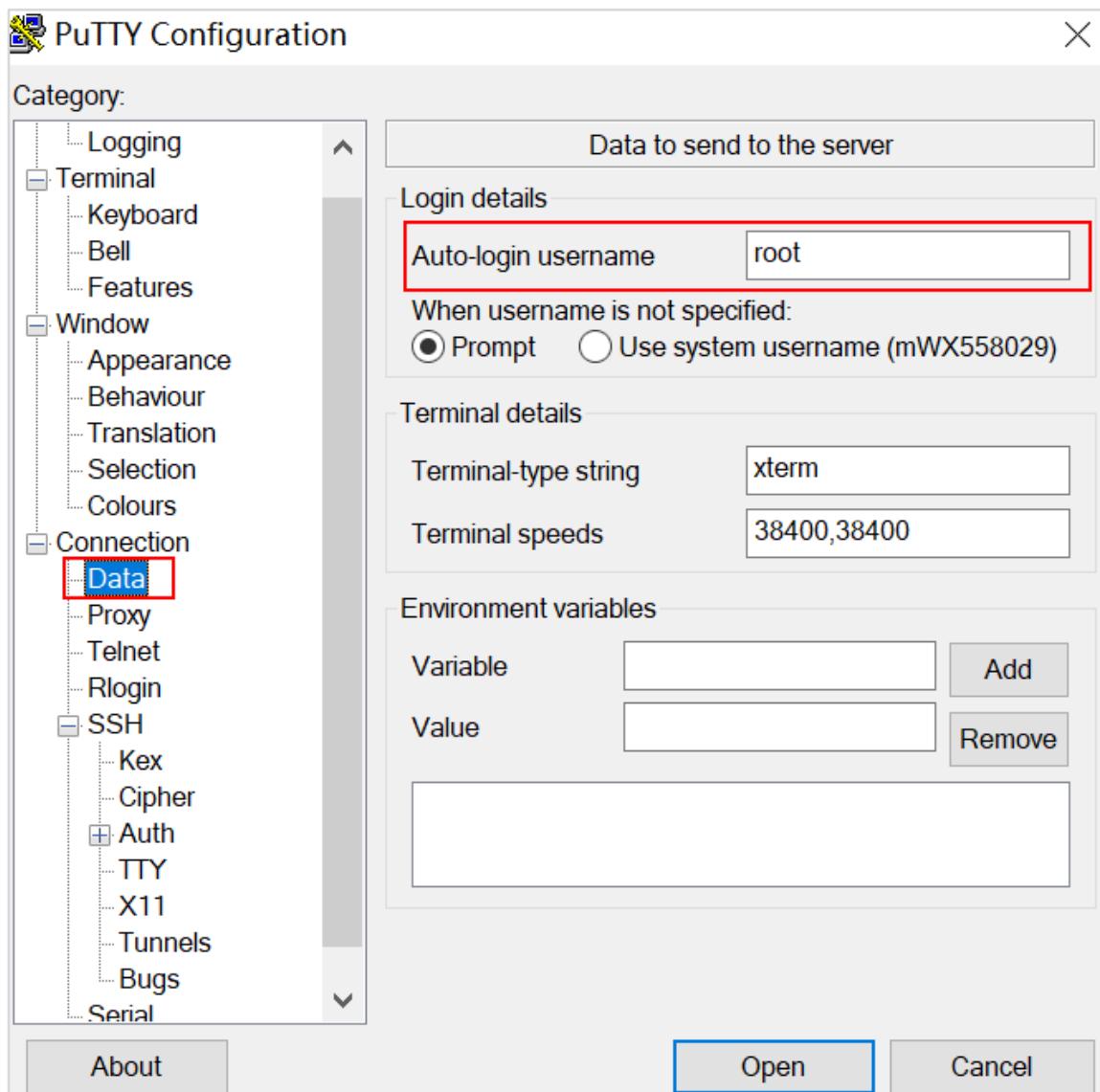


Figure 3-38 Setting the Auto-login username

Click Connection > SSH > Auth in the left navigation pane, click the Browse... button and select your private key file (.ppk file).

Click Session in the left navigation pane, enter the EIP of ecs-S02 in Host Name (or IP address), and click Open.

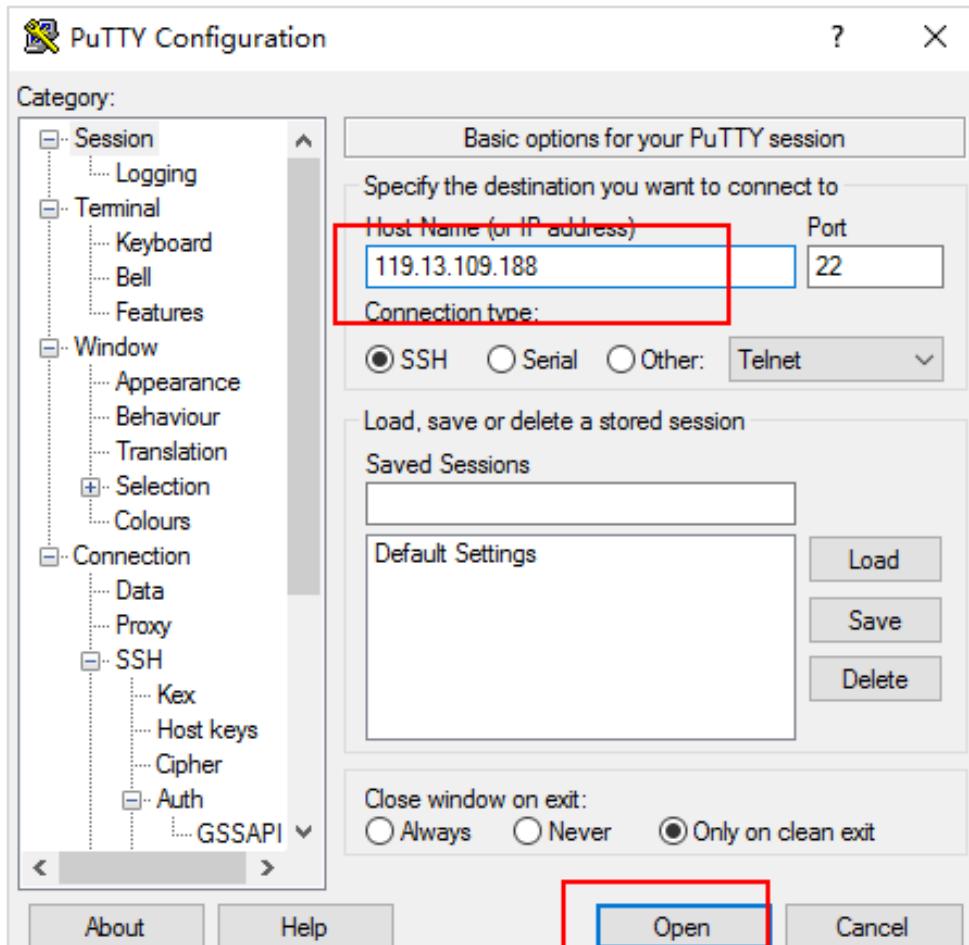
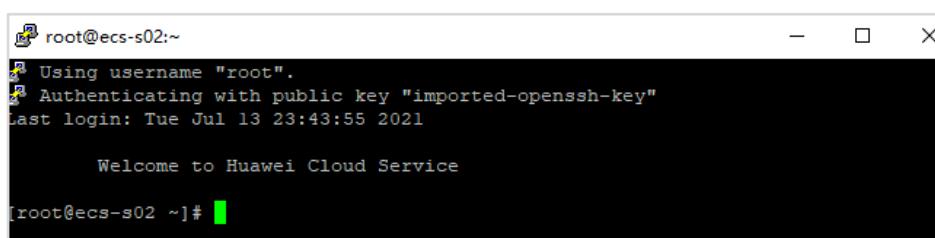


Figure 3-39 Configuring Host Name (or IP address)



```
root@ecs-s02:~  
Using username "root".  
Authenticating with public key "imported-openssh-key"  
Last login: Tue Jul 13 23:43:55 2021  
  
Welcome to Huawei Cloud Service  
[root@ecs-s02 ~]#
```

Figure 3-40 Logging in to ecs-S02 using a key pair

Run the ping baidu.com command to check whether ecs-So2 can access the Internet. The ping is successful, indicating that ecs-So2 can access the Internet through an EIP.

```
[root@ecs-s02 ~]# ping baidu.com
PING baidu.com (39.156.69.79) 56(84) bytes of data.
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1 ttl=40 time=77.8 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=2 ttl=40 time=77.8 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=3 ttl=40 time=77.9 ms
-
```

Figure 3-41 Verifying Internet access

3.2.4.4 Using ELB to Distribute Incoming Traffic

Tasks:

- Start the HTTP service on **ecs-So1** and **ecs-So2**.
- Create a load balancer.
- Use the load balancer to route HTTP requests for the web page across two ECSs.

Remotely log in to **ecs-So1** and **ecs-So2** and enable port 8889, which is a default port for HTTP communication.

- Start the HTTP service on each ECS.

```
nohup python -m SimpleHTTPServer 8889 > /dev/null 2>&1 &
```

- Verify that port 8889 is enabled.

```
curl 127.0.0.1:8889
```

```
[root@ecs-s01 ~]# nohup python -m SimpleHTTPServer 8889 > /dev/null 2>&1 &
[1] 13032
[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 ~]# _
```

Figure 3-42 Port 8899 enabled on **ecs-So1**

```
[root@ecs-s02 ~]# nohup python -m SimpleHTTPServer 8889 > /dev/null 2>&1 &
[1] 13554
[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 ~]# _
```

Figure 3-43 Port 8899 enabled on ecs-S02

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.

```
touch SERVER1
touch SERVER2
```

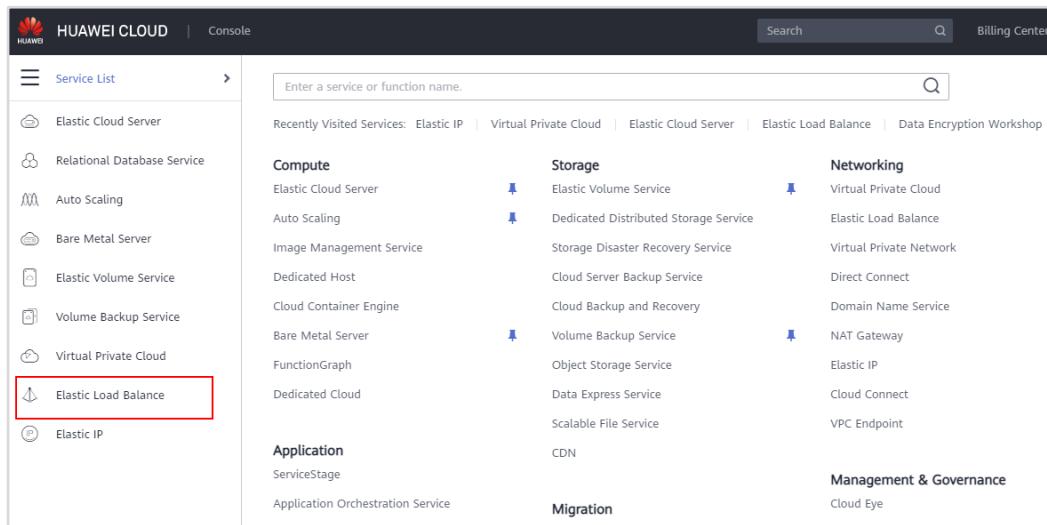
```
[root@ecs-s01 ~]# touch SERVER1
[root@ecs-s01 ~]# ls
SERVER1
[root@ecs-s01 ~]#
```

Figure 3-44 Creating file SERVER1

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

Figure 3-45 Creating file SERVER2

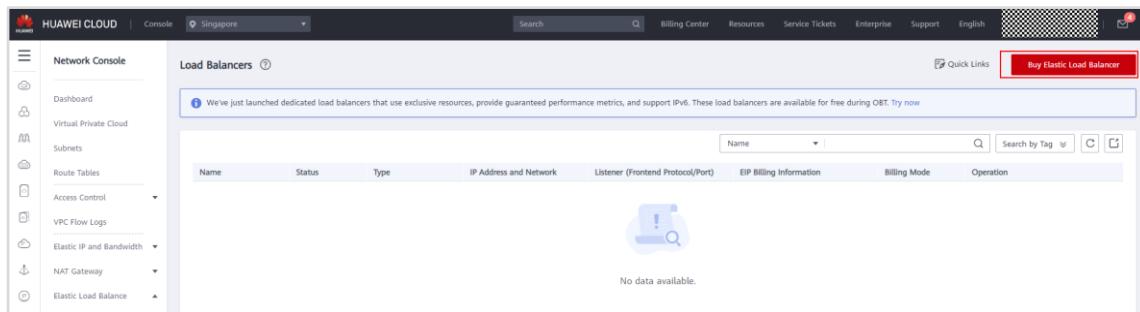
Log in to the management console. On the service list page, choose Networking > Elastic Load Balance.



The screenshot shows the HUAWEI CLOUD Service List interface. The left sidebar lists various services under categories like Compute, Storage, Networking, Application, and Management & Governance. The 'Elastic Load Balance' service is highlighted with a red box. The main area displays a grid of service cards, with the 'Elastic Load Balance' card being the most prominent. It includes icons for Virtual Private Cloud, Auto Scaling, and Bare Metal Server, along with a brief description: 'A highly available and reliable load balancer that distributes traffic across multiple back-end servers based on specific rules.' Below the card are links to 'Create' and 'View Details'.

Figure 3-46 Accessing Elastic Load Balance

Click Buy Elastic Load Balancer and select Shared for Type.



The screenshot shows the Network Console Load Balancers page. The left sidebar lists network-related services. The main area shows a table of existing load balancers with columns for Name, Status, Type, IP Address and Network, Listener (Frontend Protocol/Port), EIP Billing Information, Billing Mode, and Operation. A message at the top says, 'We've just launched dedicated load balancers that use exclusive resources, provide guaranteed performance metrics, and support IPv6. These load balancers are available for free during Q3T. Try now.' A red box highlights the 'Buy Elastic Load Balancer' button in the top right corner of the page.

Figure 3-47 Buy Elastic Load Balancer

Configure the parameters and click Next. Confirm the configuration and click Submit.

- Type: Shared
- Region: LA-Sao Paulo
- Network Type: Public network
- VPC: vpc-S01
- EIP: New EIP
- EIP Type: Dynamic BGP
- Billed By: Bandwidth
- Bandwidth: 1 M/bits
- Name: elb-name (Change it as needed.)

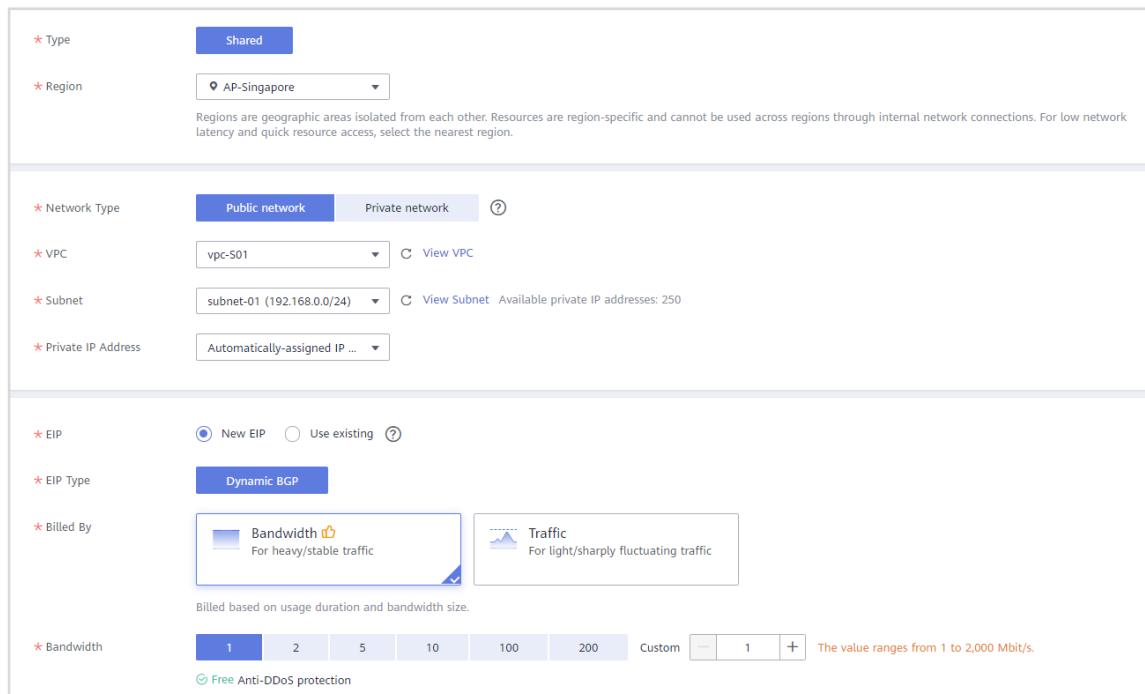


Figure 3-48 Configuring parameters

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

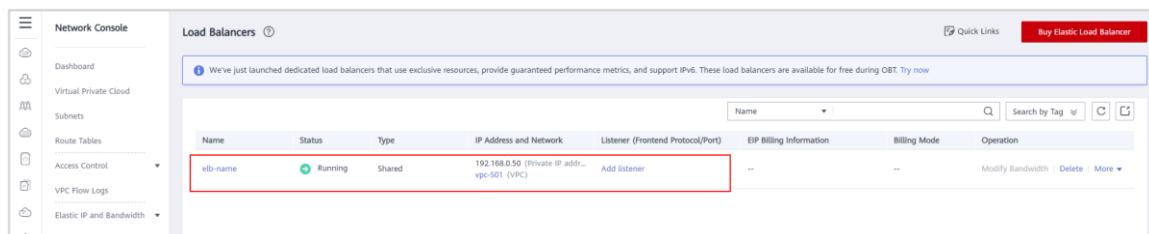
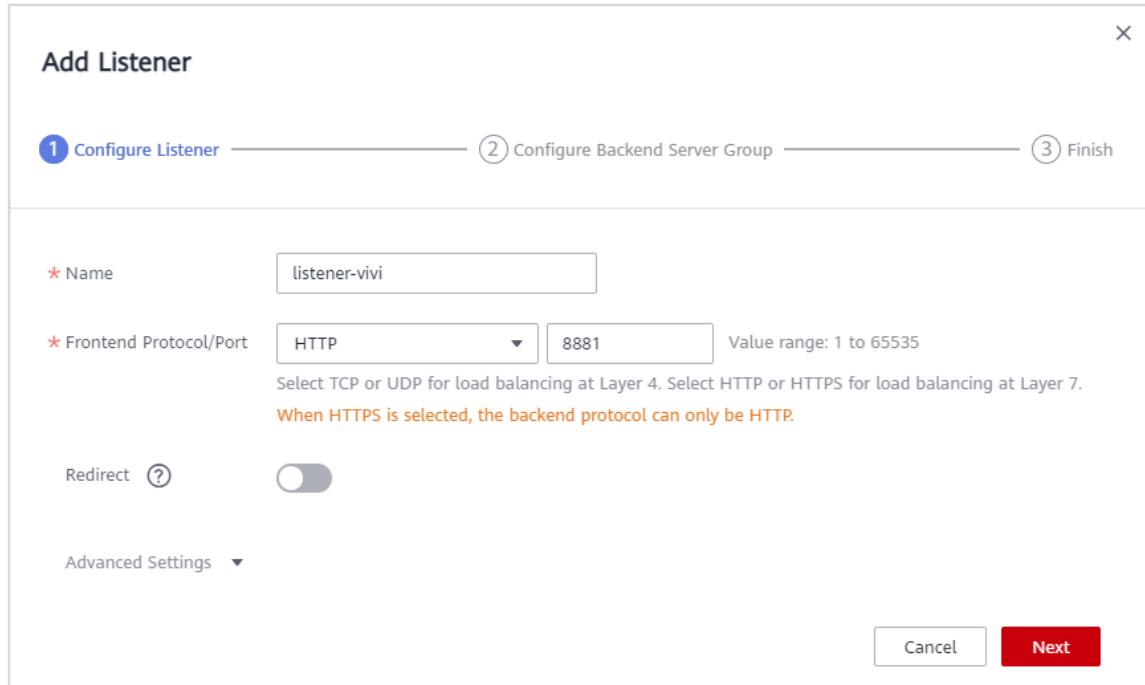


Figure 3-49 Viewing the load balancer

1. Click Add Listener and configure the following parameters:

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



The screenshot shows the 'Add Listener' dialog box. At the top, there are three tabs: ① Configure Listener (highlighted in blue), ② Configure Backend Server Group, and ③ Finish. The main area contains the following fields:

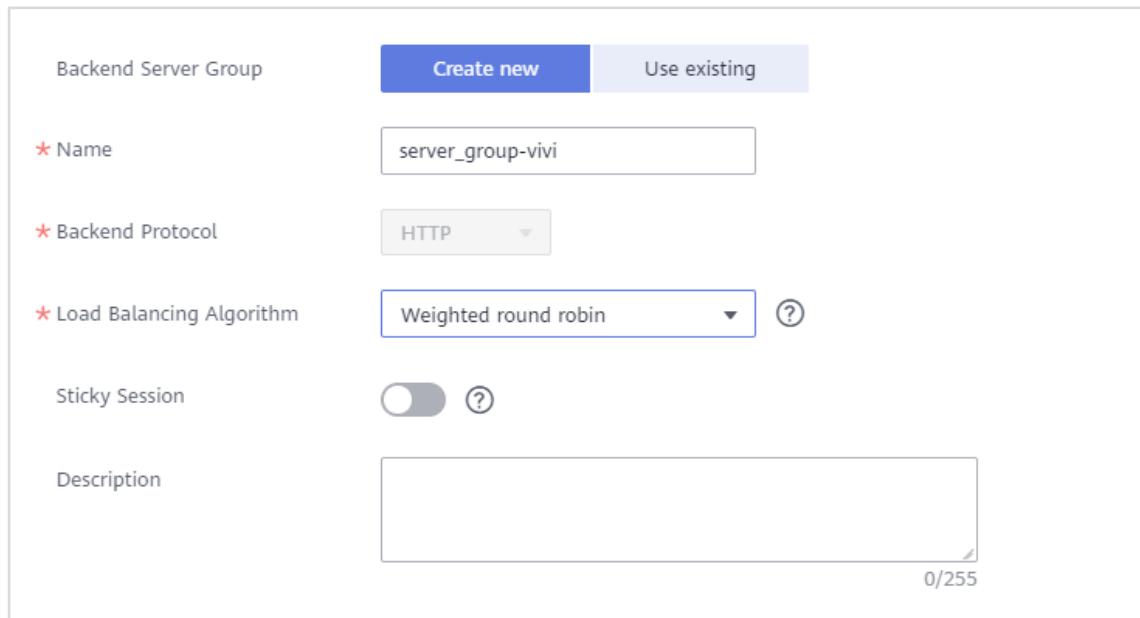
- Name:** listener-vivi
- Frontend Protocol/Port:** HTTP (selected) / 8881 (port number). A note below states: "Select TCP or UDP for load balancing at Layer 4. Select HTTP or HTTPS for load balancing at Layer 7. When HTTPS is selected, the backend protocol can only be HTTP."
- Redirect:** A toggle switch is set to off.
- Advanced Settings:** A dropdown menu.

At the bottom right are 'Cancel' and 'Next' buttons.

Figure 3-50 Configuring a listener

2. Click Next and configure a backend server group.

- Backend Cloud Server Group: Create new
- Name: server_group-vivi (Change it as needed.)
- Load Balancing Algorithm: Weighted round robin
- Health check configuration: enabled, HTTP, 8889



Backend Server Group

Create new Use existing

* Name: server_group-vivi

* Backend Protocol: HTTP

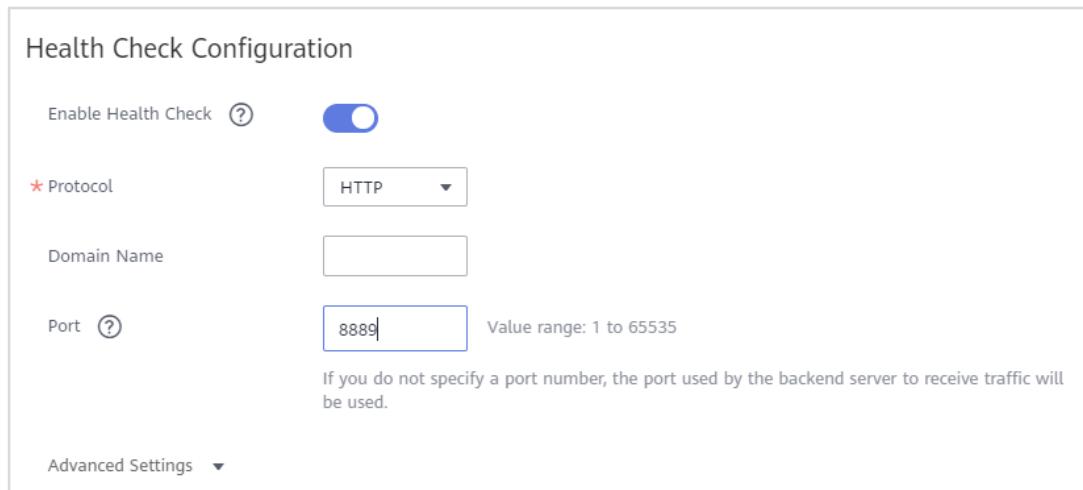
* Load Balancing Algorithm: Weighted round robin

Sticky Session: Off

Description: (empty)

0/255

Figure 3-51 Configuring a backend server group



Health Check Configuration

Enable Health Check: On

* Protocol: HTTP

Domain Name: (empty)

Port: 8889 Value range: 1 to 65535

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

Advanced Settings

Figure 3-52 Configuring a health check

3. Click Finish and then click OK.

Add ecs-S01 and ecs-S02 to the backend server group and set the backend port to 8889.

The two ECSSs, 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.

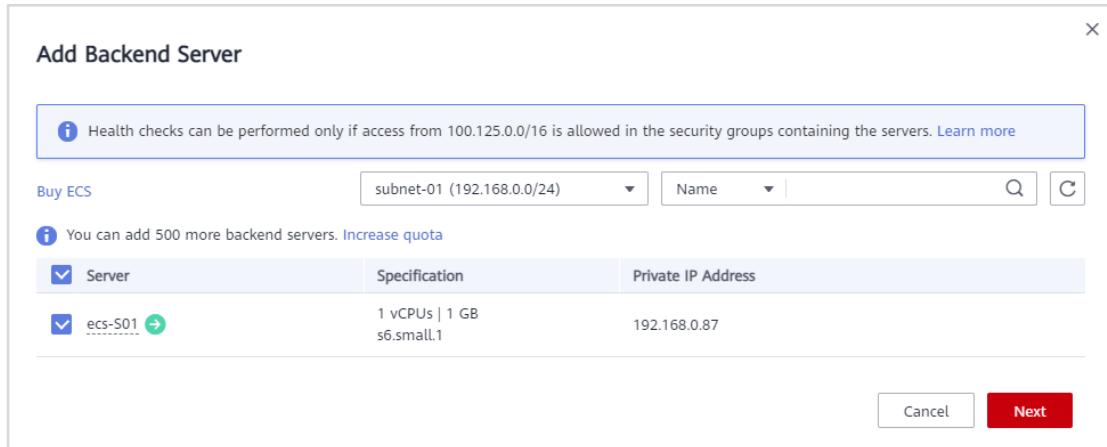


Figure 3-53 Adding ecs-S01 to the backend server group

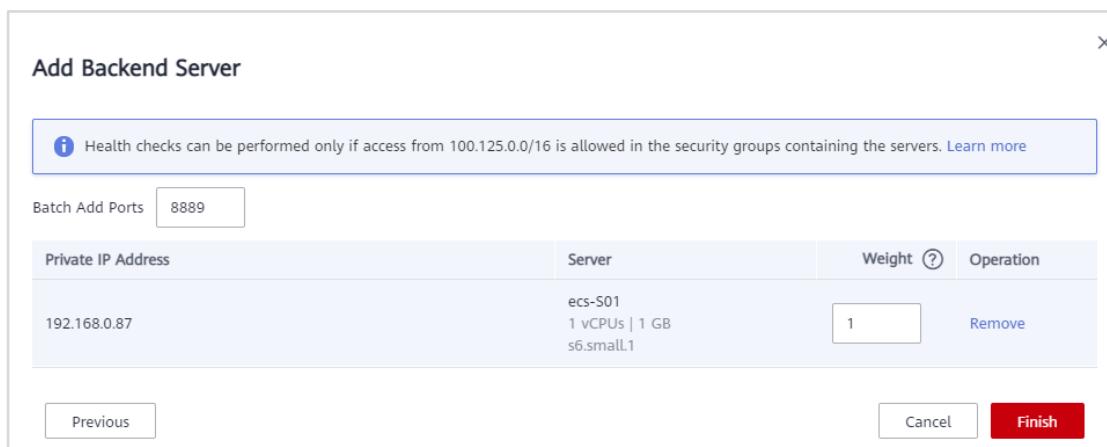


Figure 3-54 Adding ecs-S02 to the backend server group

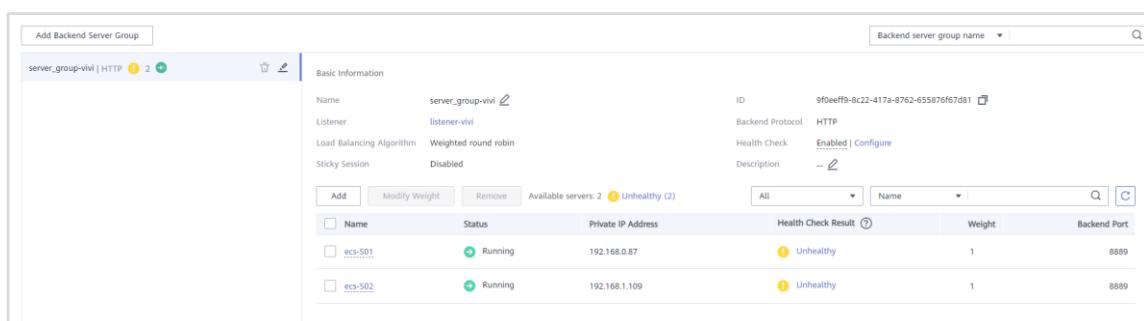


Figure 3-55 Viewing the backend servers

Check the health check results for the two ECSSs.

If the health check result is Unhealthy, security group rules may not have been configured to allow traffic from and to the backend port or the health check configuration is incorrect. Click Unhealthy and rectify the fault by following the instructions in the FAQ. The cause here is that port 8889 is not enabled in the security group. Switch back to the Network Console. In the left navigation pane, choose Access Control > Security Groups, locate the security group that contains the two ECSSs, and add security group rules.

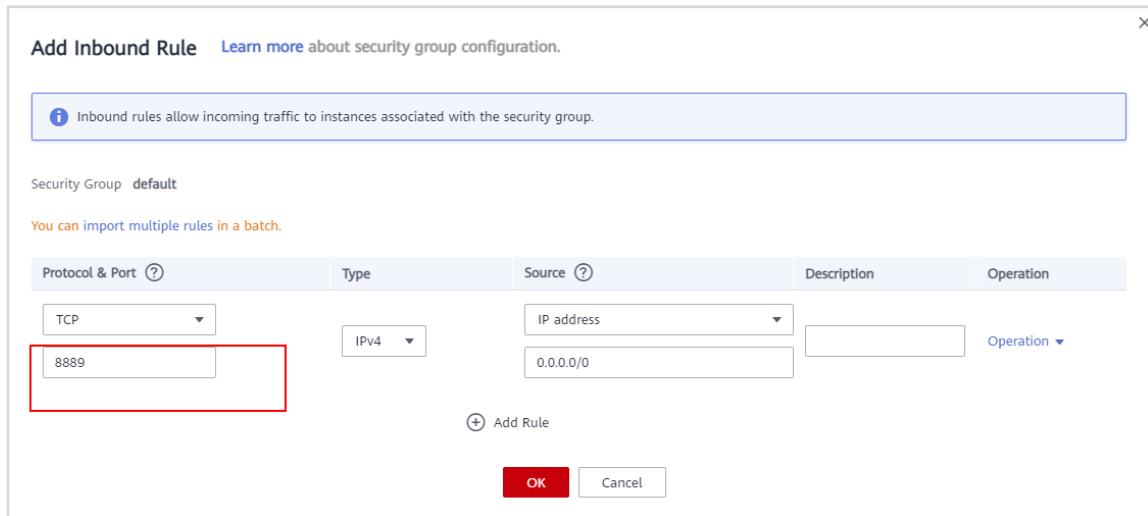


Figure 3-56 Configuring security group rules

Go back to the Backend Server Groups page, **wait for 3 to 5 minutes** and refresh the page.

It takes about 3 to 5 minutes for the system to send heartbeat messages to backend servers to check their health. If the listener has detected the heartbeat messages returned by the backend servers, the health check result becomes Healthy.

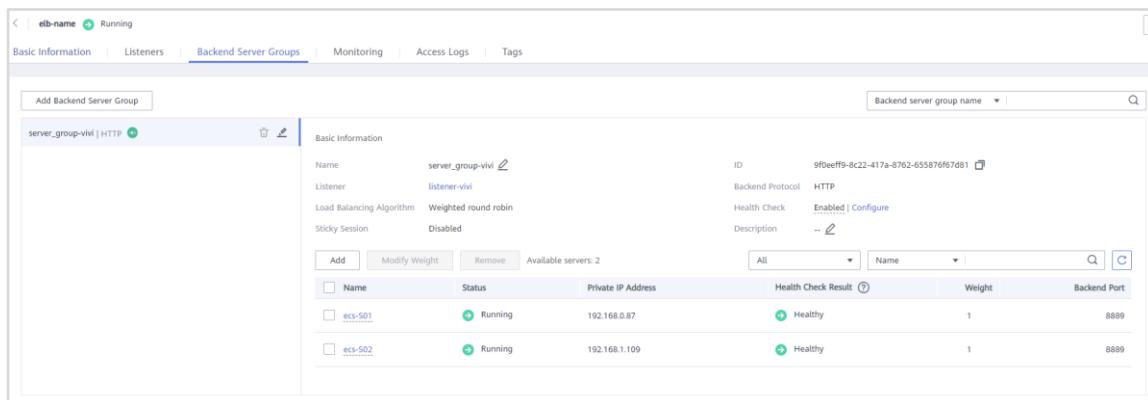


Figure 3-57 Viewing the backend server group

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.

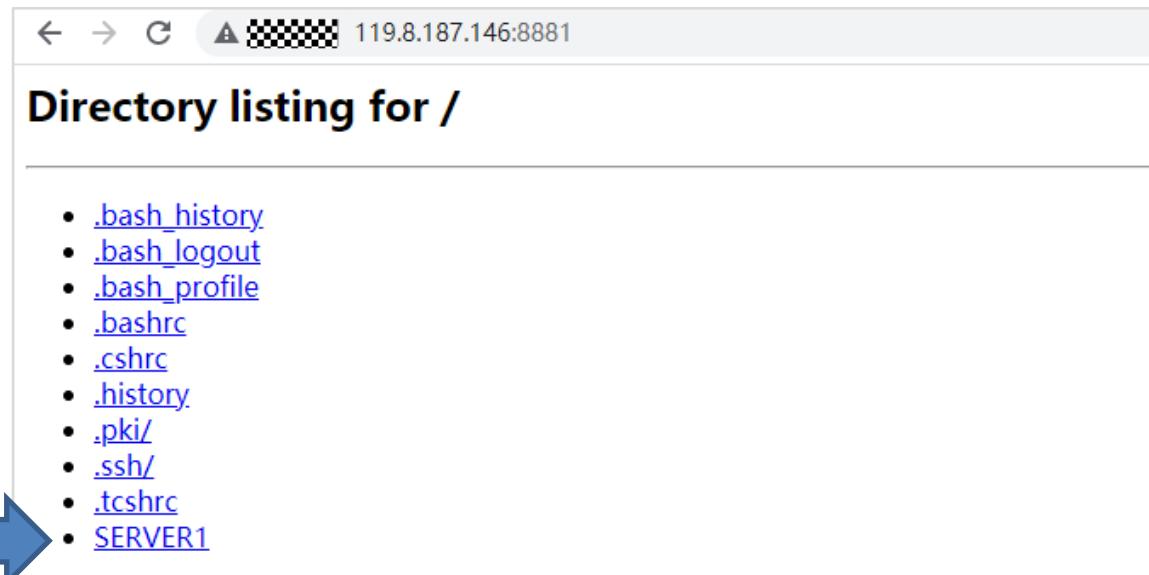


Figure 3-58 Accessing the web page

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 3-59 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 **LA-SaoPaulo**.
- Configure routes for the two VPCs connected by the VPC peering connection.

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

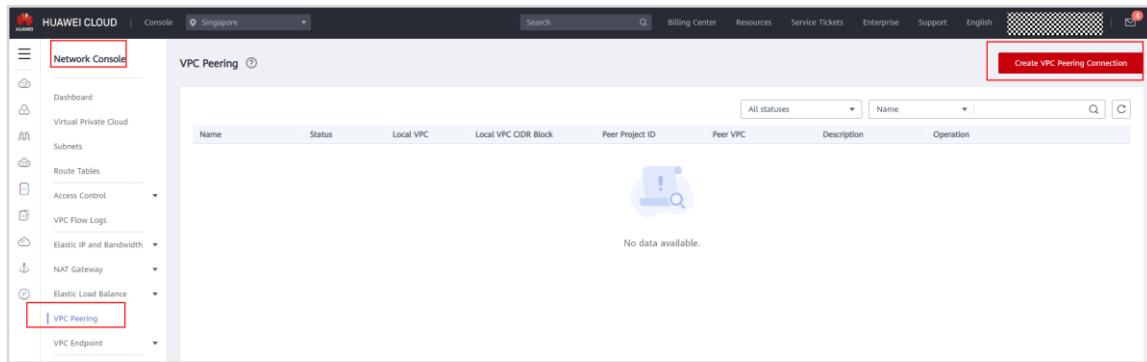


Figure 3-60 Create VPC Peering Connection

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-vivi (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.

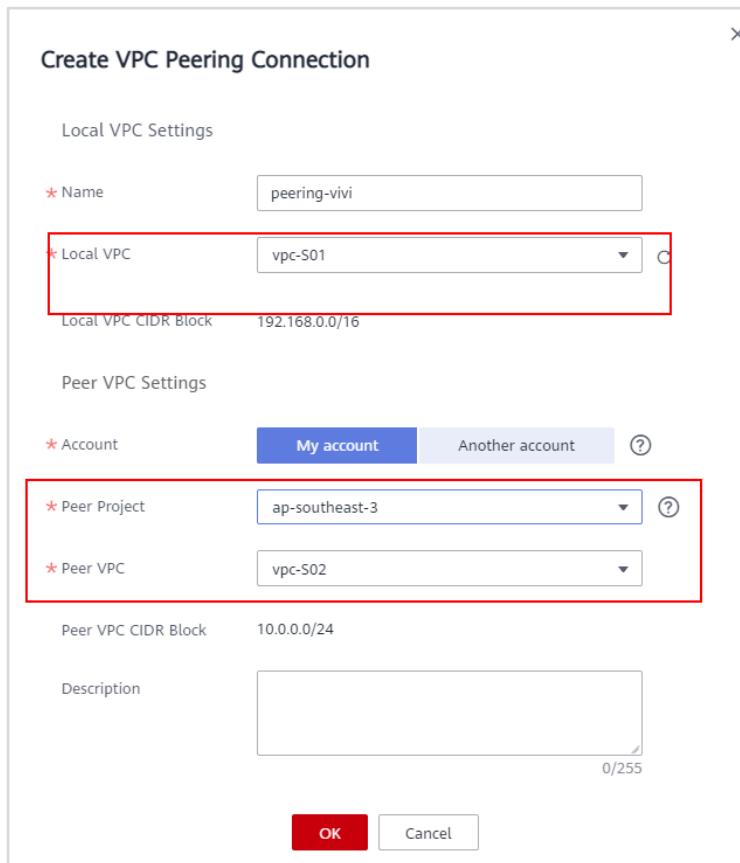


Figure 3-61 Configuring the VPC peering connection

Figure 3-62 Viewing the VPC peering connection

Click Add Route on the Information page or click the name of the VPC peering connection and click Route Tables to add routes.

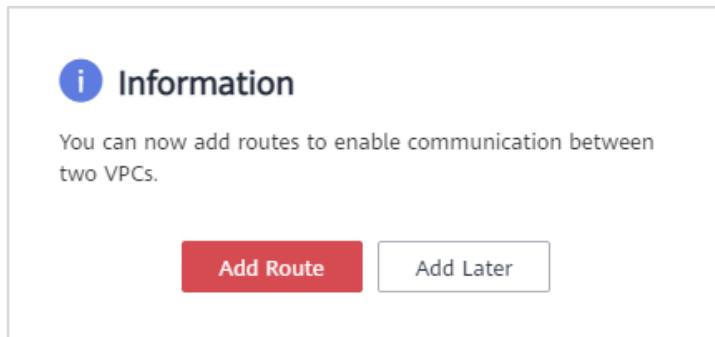


Figure 3-63 Add Route

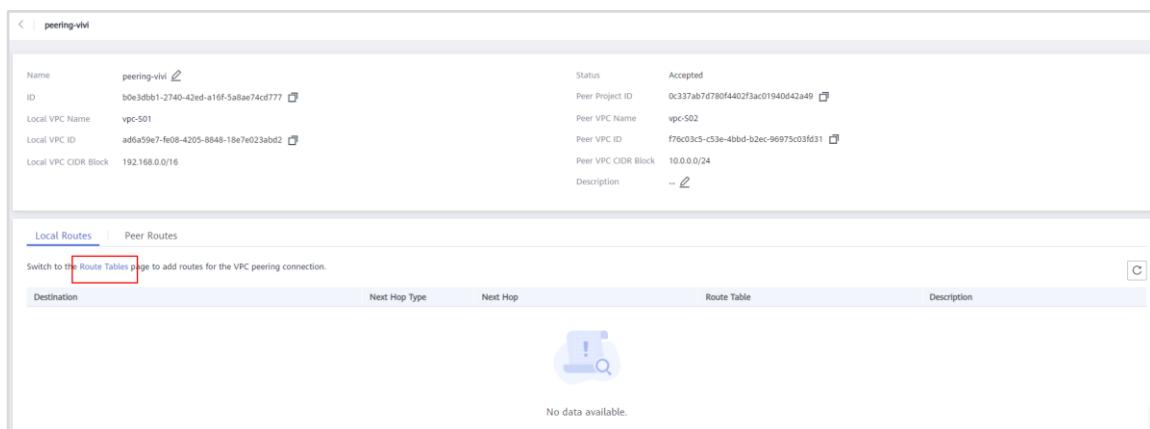


Figure 3-64 Route Tables

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.

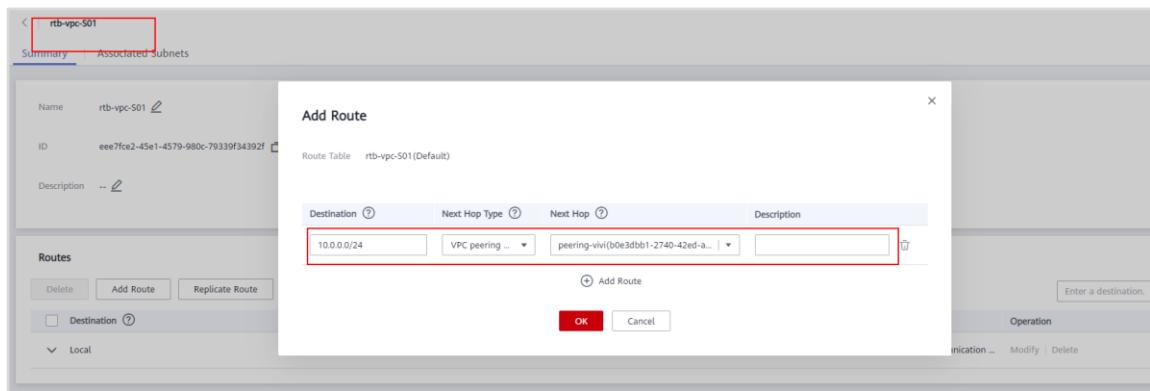


Figure 3-65 Add Route

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.

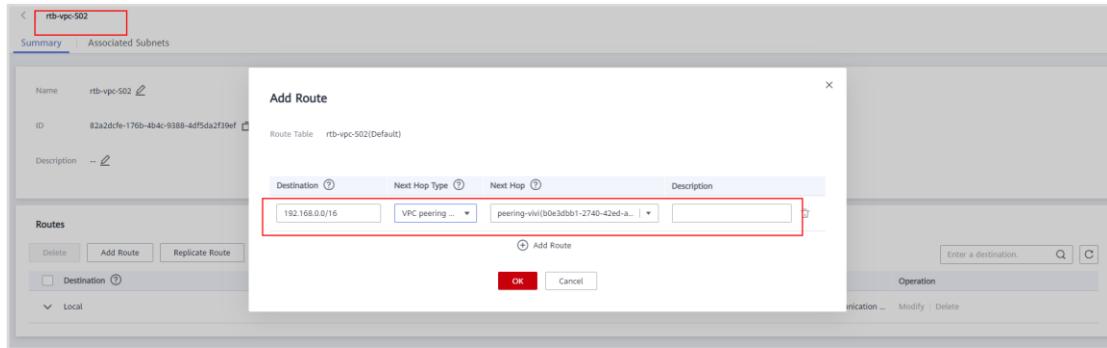


Figure 3-66 Add Route

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 10.0.0.70
PING 10.0.0.70 (10.0.0.70) 56(84) bytes of data.
64 bytes from 10.0.0.70: icmp_seq=1 ttl=64 time=1.06 ms
64 bytes from 10.0.0.70: icmp_seq=2 ttl=64 time=0.378 ms
64 bytes from 10.0.0.70: icmp_seq=3 ttl=64 time=0.313 ms
```

Figure 3-67 Successful ping

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:

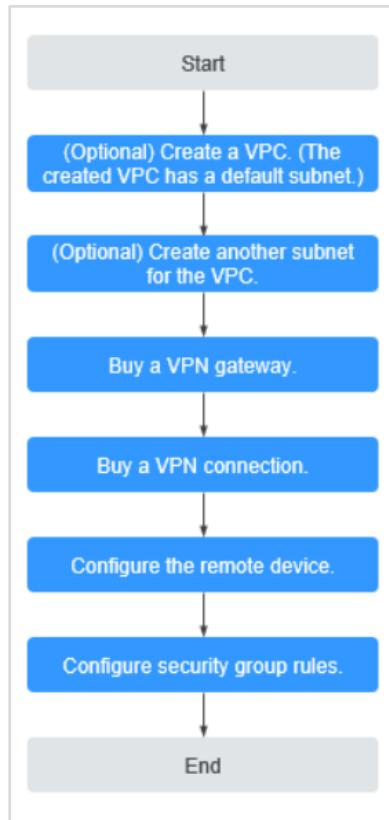


Figure 3-68 VPN configuration flowchart

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 **LA-Santiago** regions.
- Create a VPN connection.
- Modify security group rules.
- Ping **ecs-Jo1**, in the **AF-Johannesburg** region, from **ecs-Sao1**, in the **LA-Santiago** region.
- View the VPN connection status.

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

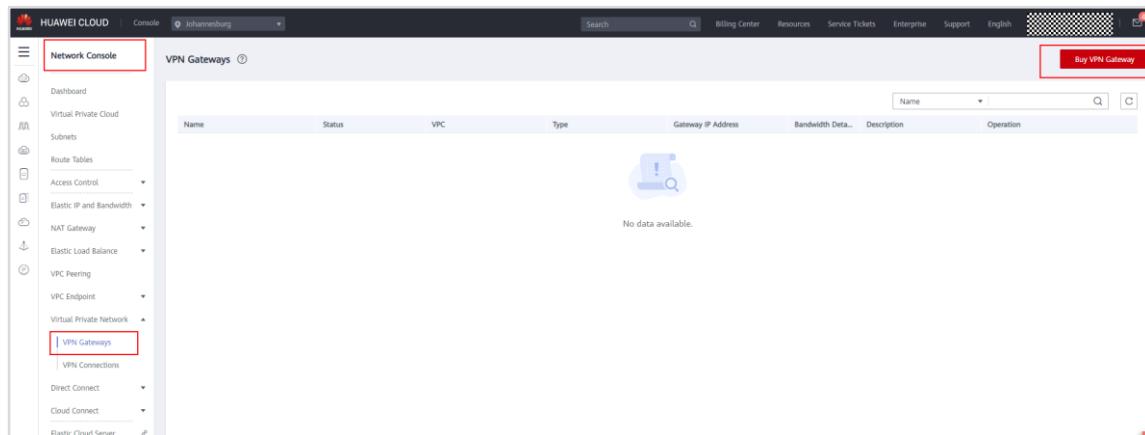


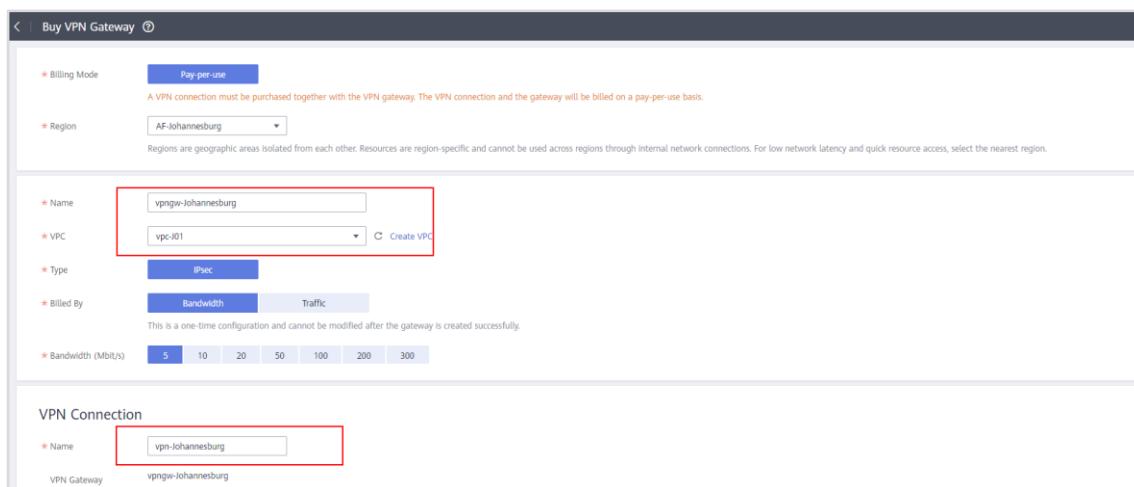
Figure 3-69 Buy VPN Gateway

Configure VPN gateway parameters and click Buy Now.

- **Billing Mode:** Pay-per-use
- **Region:** AF-Johannesburg
- **Name:** vpngw-Johannesburg
- **VPC:** vpc-Jo1
- **Type:** IPsec
- **Billed By:** Bandwidth
- **Bandwidth (Mbit/s):** 5

VPN connection

- **Name:** vpn-Johannesburg
- **Local Subnet:** Select **subnet-01** of **vpc-Jo1**.
- **Remote Gateway:** Enter an IP address and then replace it with the IP address of the VPN gateway you will create in the **LA-Santiago** region.
- **Remote Subnet:** Enter subnet CIDR blocks of **vpc-Sao1**.
- **PSK:** Enter a value.
- **Advanced Settings:** Default



The screenshot shows the 'Buy VPN Gateway' configuration page. The 'Billing Mode' is set to 'Pay-per-use'. The 'Region' is selected as 'AF-Johannesburg'. The 'Name' field contains 'vpngw-Johannesburg', and the 'VPC' dropdown is set to 'vpc-Jo1'. The 'Type' is 'IPsec', and 'Billed By' is 'Bandwidth'. The 'Bandwidth (Mbit/s)' is set to 5. In the 'VPN Connection' section, the 'Name' field is also set to 'vpn-Johannesburg'. The bottom status bar indicates 'VPN Gateway' and 'vpngw-Johannesburg'.

Figure 3-70 Configuring a VPN gateway

VPN Connection

* Name: vpn-Johannesburg

VPN Gateway: vpngw-Johannesburg

* Local Subnet: Select subnet (highlighted with a red box)

172 . 16 . 0 . 1

* Remote Gateway: 172.16.0.12

* Remote Subnet: 172.16.0.0/12 (highlighted with a red box)

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 (highlighted with a red box)

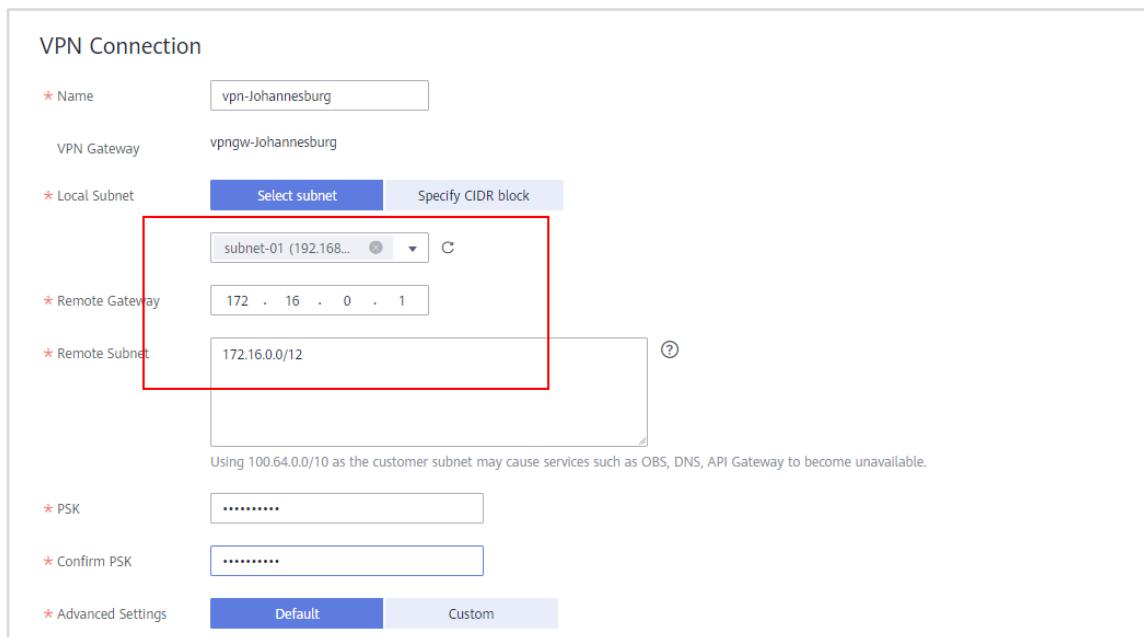


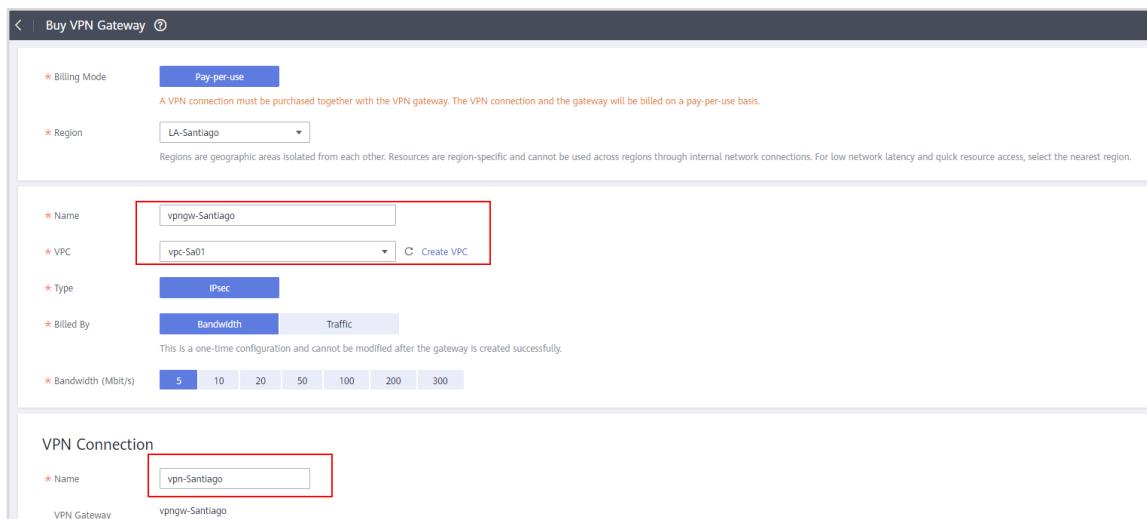
Figure 3-71 Configuring a VPN connection

Switch to the LA-Santiago region, go to Network Console, choose Virtual Private Network > VPN Gateways, and click Buy VPN Gateway.

- **Billing Mode:** Pay-per-use
- **Region:** LA-Santiago
- **Name:** vpngw-Santiago
- **VPC:** vpc-Sao1
- **Type:** IPsec
- **Billed By:** Bandwidth
- **Bandwidth (Mbit/s):** 5

VPN connection

- **Name:** vpn-Santiago
- **Local Subnet:** Select **subnet-01** of **vpc-Sao1**.
- **Remote Gateway:** Enter an IP address and then replace it with the IP address of the VPN gateway you created in the **AF-Johannesburg** region.
- **Remote Subnet:** Enter subnet CIDR blocks of **vpc-Jo1**.
- **PSK:** Enter the PSK you configured in the **AF-Johannesburg** region.
- **Advanced Settings: Default**



The screenshot shows the 'Buy VPN Gateway' configuration interface. At the top, 'Billing Mode' is set to 'Pay-per-use'. The 'Region' is selected as 'LA-Santiago'. In the main configuration area, the 'Name' is 'vpngw-Santiago' and the 'VPC' is 'vpc-Sao1'. The 'Type' is 'IPsec', 'Billed By' is 'Bandwidth', and the 'Bandwidth (Mbit/s)' is set to 5. Below this, the 'VPN Connection' section shows the 'Name' as 'vpn-Santiago' and the 'VPN Gateway' as 'vpngw-Santiago'. A note at the bottom states: 'This is a one-time configuration and cannot be modified after the gateway is created successfully.'

Figure 3-72 Configuring a VPN gateway

VPN Connection

* Name

VPN Gateway vpngw-Santiago

* Local Subnet

subnet-01 (172.16....)

* Remote Gateway

* Remote Subnet

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

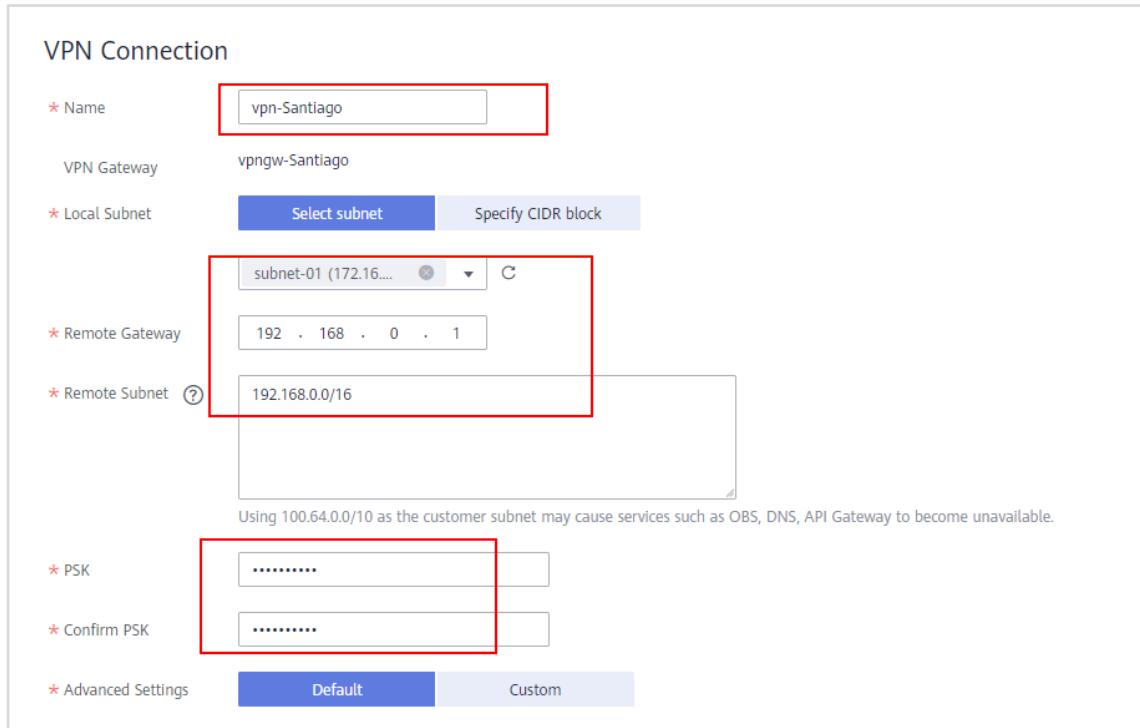


Figure 3-73 Configuring a VPN connection

Go back to the Virtual Gateways page, locate **vpngw-Santiago**, and record gateway IP address: **159.138.113.162**. 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 **159.138.113.162** for Remote Gateway and click OK.

Figure 3-74 Viewing a VPN gateway

Figure 3-75 Modifying a VPN connection

Figure 3-76 Changing the remote gateway IP address

On the Virtual Gateways page, locate vpn-Johannesburg, and record its IP address: 159.138.161.172. Switch to the LA-Santiago region. Go to the VPN Connections page, locate VPN connection vpn-Santiago, and choose More > Modify in the Operation column. On the Modify VPN Connection page, enter 159.138.161.172 for Remote Gateway and click OK.

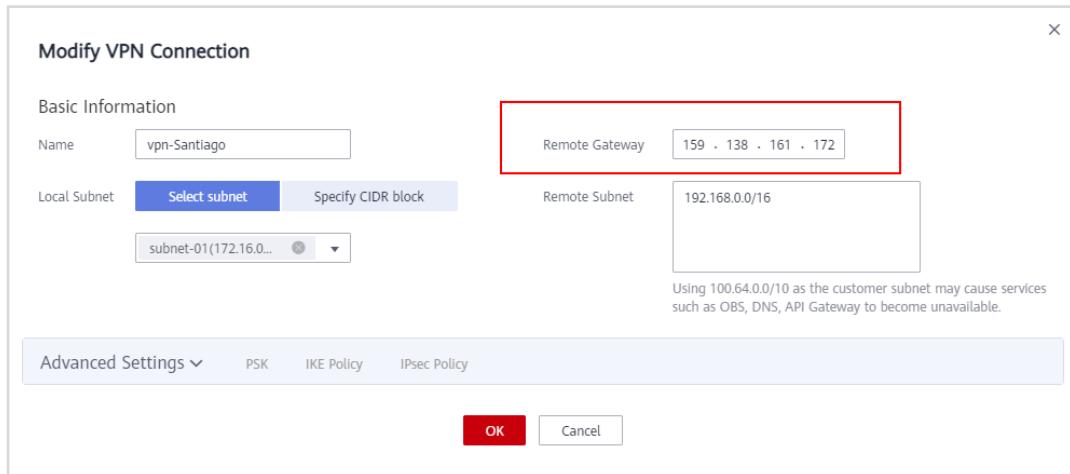


Figure 3-77 Changing the remote gateway IP address

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-Santiago | Not connected | vpngw-Santiago | 159.138.113.162 | 172.16.0.0/24 | 159.138.161.172 | 192.168.0.0/16 | View Policy Modify Delete |

Figure 3-78 Viewing a VPN connection

In the AF-Johannesburg and LA-Santiago regions, configure security groups associated with the ECSs in the VPCs to allow access from and to the peer VPC.

Figure 3-79 Add Inbound Rule

In the LA-Santiago region, remotely log in to ecs-Sao1 in vpc-Sao1 and ping ecs-Jo1 in vpc-Jo1 in the AF-Johannesburg region. The result shows that ECSs in different regions can communicate with each other.

```
[root@ecs-sa01 ~]# ping 192.168.0.44
PING 192.168.0.44 (192.168.0.44) 56(84) bytes of data.
64 bytes from 192.168.0.44: icmp_seq=1 ttl=62 time=391 ms
64 bytes from 192.168.0.44: icmp_seq=2 ttl=62 time=391 ms
64 bytes from 192.168.0.44: icmp_seq=3 ttl=62 time=391 ms
64 bytes from 192.168.0.44: icmp_seq=4 ttl=62 time=391 ms
64 bytes from 192.168.0.44: icmp_seq=5 ttl=62 time=391 ms
```

Figure 3-80 Verifying the network connection

Go back to the VPN Connections page and refresh the page to check whether status of vpn-Santiago is Normal and whether status of vpn-Johannesburg is Healthy.

| Name | Status | VPN Gateway | Local Gateway | Local Subnet | Remote Gateway | Remote Subnet | Operation |
|--------------|--------|----------------|-----------------|---------------|-----------------|----------------|---|
| vpn-Santiago | Normal | vpngw-Santiago | 159.138.113.162 | 172.16.0.0/24 | 159.138.161.172 | 192.168.0.0/16 | View Policy Modify Delete |

Figure 3-81 Viewing a VPN connection

| Name | Status | VPN Gateway | Local Gateway | Local Subnet | Remote Gateway | Remote Subnet | Operation |
|------------------|---------|--------------------|-----------------|----------------|-----------------|---------------|--|
| vpn-Johannesburg | Healthy | vpngw-Johannesburg | 159.138.161.172 | 192.168.0.0/24 | 159.138.113.162 | 172.16.0.0/12 | View Policy View Metric More |

Figure 3-82 Viewing a VPN connection

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

3.2.5 Deleting Resources

Delete the ECSs in all regions.

Remove the ECSs, delete the listener, and then delete the load balancer in the corresponding region.

Delete the VPC peering connection in the corresponding regions.

Delete the VPN connection and gateways in the corresponding regions. If you delete the VPN connection, the gateways will be automatically deleted.

Delete the VPCs and subnets in all regions.

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 on Windows and 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 Windows and 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 two Windows ECSs **ecs-vivi** and **ecs-test** in the **AP-Singapore** region, buy an EVS disk separately and attach it to ECS **ecs-vivi**, and create a test file on the disk. Then, detach this disk and attach it to ECS **ecs-test**, and log in to ECS **ecs-test** to check whether the test file exists.

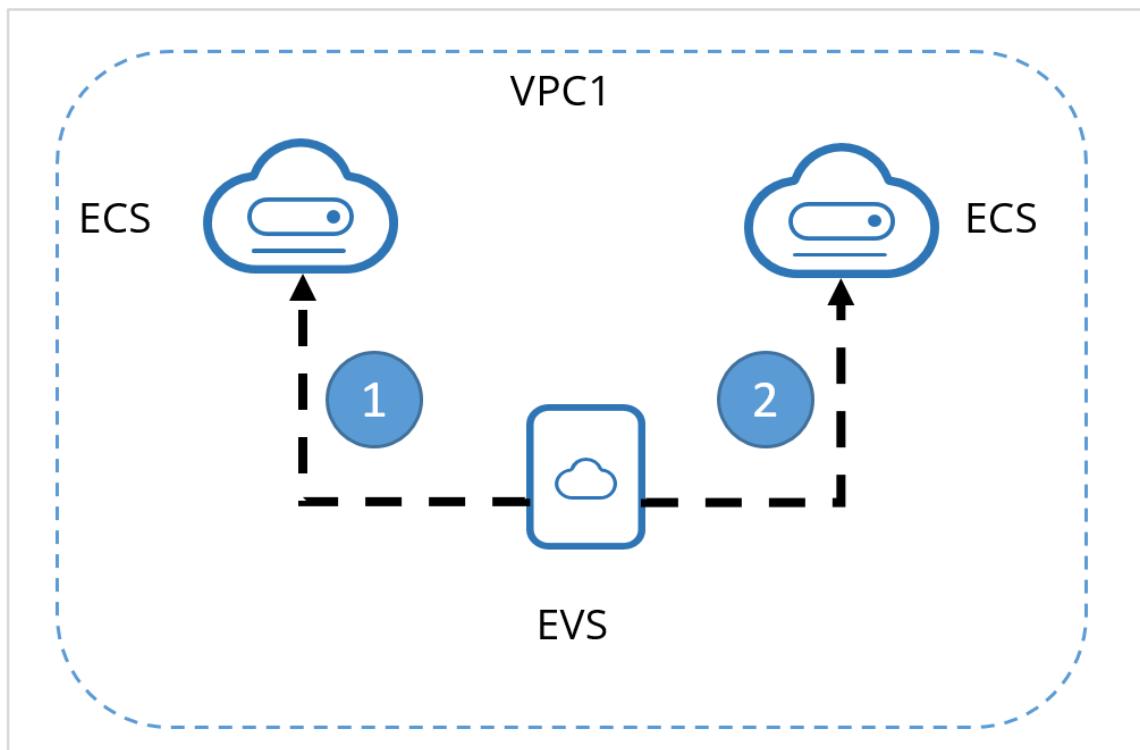
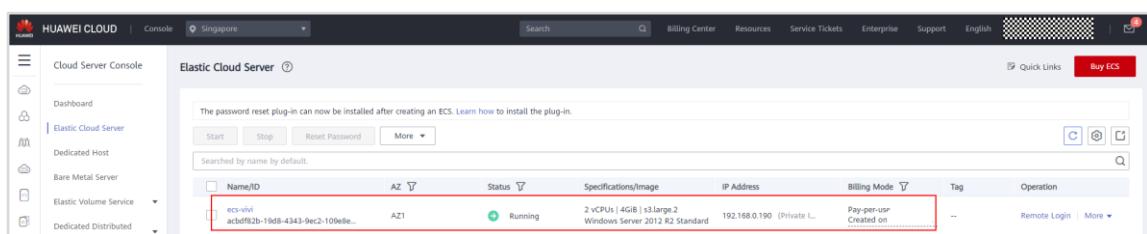


Figure 4-1 Topology

4.1.2.2 Attaching an EVS Disk to a Windows ECS

Purchasing an EVS Disk

Buy a Windows ECS (Windows Server 2012 R2 Standard 64-bit English) by referring to the preceding sections.

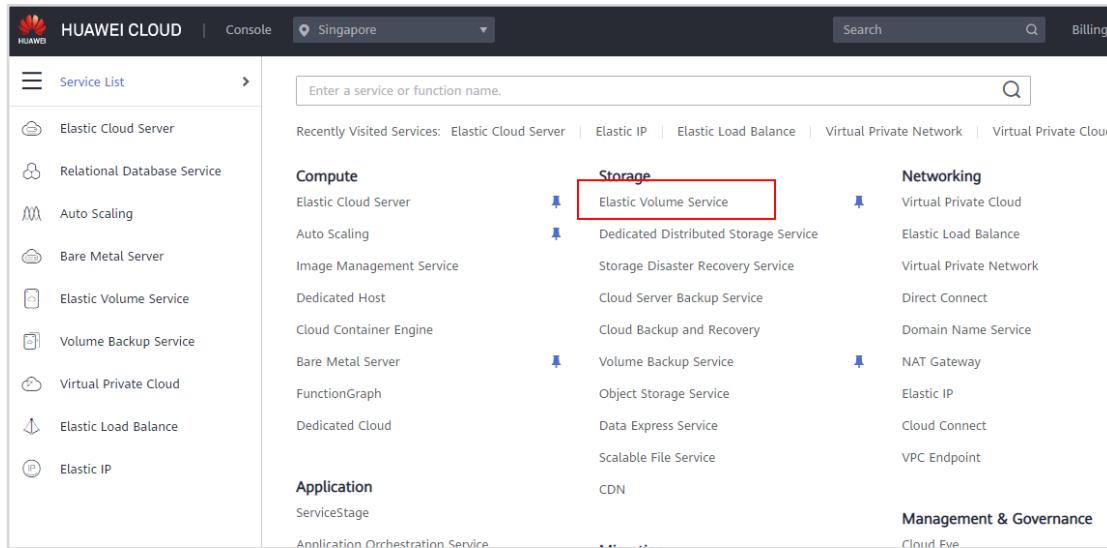


The screenshot shows the "Elastic Cloud Server" page in the Huawei Cloud Console. The left sidebar has a tree view with "Cloud Server Console" selected, followed by "Dashboard", "Elastic Cloud Server" (which is also the active tab), "Dedicated Host", "Bare Metal Server", "Elastic Volume Service" (with a dropdown menu), and "Dedicated Distributed". The main area has a header "Elastic Cloud Server" with a "Buy ECS" button. Below the header is a message about password reset plug-in availability. There are buttons for "Start", "Stop", "Reset Password", and "More". A search bar says "Searched by name by default." A table lists one ECS instance:

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|--|-----|---------|---|----------------------------|---------------------------|-----|---------------------|
| ecs-vn1 acbdf82b-19d8-4343-9ec2-109ebe... | AZ1 | Running | 2 vCPUs 4GB s1-large-2 Windows Server 2012 R2 Standard | 192.168.0.190 (Private IP) | Pay-per-use Created on | -- | Remote Login More |

Figure 4-2 Viewing the ECS

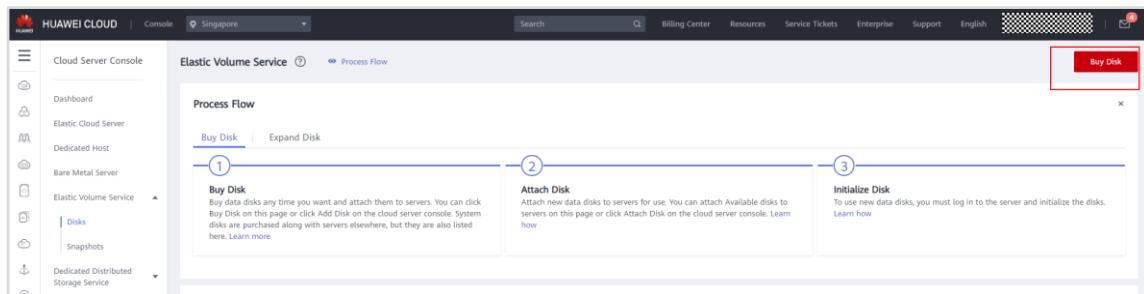
Log in to the management console. In the service list, choose Elastic Volume Service under Storage to go to the Elastic Volume Service page.



The screenshot shows the HUAWEI CLOUD management console interface. At the top, there's a navigation bar with the HUAWEI logo, 'HUAWEI CLOUD', 'Console', 'Singapore', a search bar, and a 'Billing' button. Below the navigation bar is a sidebar titled 'Service List' containing icons and names for various services: Elastic Cloud Server, Relational Database Service, Auto Scaling, Bare Metal Server, Elastic Volume Service, Volume Backup Service, Virtual Private Cloud, Elastic Load Balance, and Elastic IP. To the right of the sidebar is a main content area. At the top of this area is a search bar with the placeholder 'Enter a service or function name.' Below the search bar is a section titled 'Recently Visited Services' with links to Elastic Cloud Server, Elastic IP, Elastic Load Balance, Virtual Private Network, and Virtual Private Cloud. The main content area is organized into several categories: 'Compute' (Elastic Cloud Server, Auto Scaling, Image Management Service, Dedicated Host, Cloud Container Engine, Bare Metal Server, FunctionGraph, Dedicated Cloud), 'Storage' (Elastic Volume Service, Dedicated Distributed Storage Service, Storage Disaster Recovery Service, Cloud Server Backup Service, Cloud Backup and Recovery, Volume Backup Service, Object Storage Service, Data Express Service, Scalable File Service), 'Networking' (Virtual Private Cloud, Elastic Load Balance, Virtual Private Network, Direct Connect, Domain Name Service, NAT Gateway, Elastic IP, Cloud Connect, VPC Endpoint), 'Application' (ServiceStage, Application Orchestration Service), and 'Management & Governance' (Cloud Eye). The 'Storage' category is highlighted with a red box, and the 'Elastic Volume Service' option is also highlighted with a red box.

Figure 4-3 Opening EVS console

Click Buy Disk.



The screenshot shows the 'Elastic Volume Service' process flow. The left sidebar lists services: Cloud Server Console, Dashboard, Elastic Cloud Server, Dedicated Host, Bare Metal Server, Elastic Volume Service (selected), Disks (highlighted), Snapshots, and Dedicated Distributed Storage Service. The main content area shows a 'Process Flow' with three steps: 1. Buy Disk (highlighted with a red box), 2. Attach Disk, and 3. Initialize Disk. Each step has a brief description and a 'Learn more' link. The 'Buy Disk' step describes buying data disks and attaching them to servers. The 'Attach Disk' step describes attaching available disks to servers. The 'Initialize Disk' step describes initializing new data disks after purchase.

Figure 4-4 Buy Disk

Set disk parameters as follows:

- **Billing Mode:** Pay-per-use
- **Region:** LA-SaoPaulo
- **AZ:** AZ1
- **Disk Type:** High I/O (If this type is unavailable, select one available on the console.)
- **Disk Size:** 20 GB
- **More:** Do not configure this parameter.
- **Disk Name:** volume-vivi (customized)

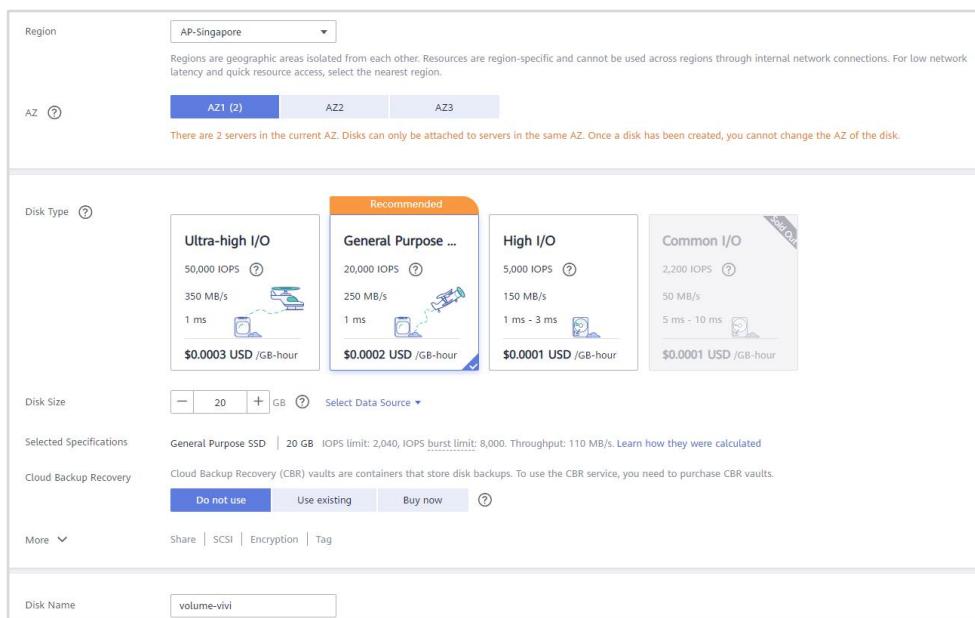


Figure 4-5 Setting disk parameters

Click Next.

On the Details page, confirm the disk configuration. If you need to modify the configuration, click Previous. If not, click Submit.

| Details | | | |
|----------|-----------------|---------------------|----------|
| Resource | Configuration | Billing Mode | Quantity |
| Disk | Region | Singapore | |
| | AZ | AZ1 | |
| | Data Source | Not required | |
| | Capacity (GB) | 20 | |
| | Disk Type | General Purpose SSD | 1 |
| | Disk Encryption | No | |
| | Device Type | VBD | |
| | Disk Sharing | Disabled | |
| | Disk Name | volume-vivi | |

Figure 4-6 Confirming disk parameter settings

Go back to the disk list page and view the disk status. When the disk status changes to Available, the disk has been purchased.

Attaching a Non-shared EVS Disk

Separately purchased EVS disks are data disks. In the EVS disk list, the function of such disks is Data disk, and their status is Available. Data disks need to be attached to servers for use.

System disks are purchased along with servers and are automatically attached. In the EVS disk list, the function of such disks is System disk, and their status is In-use. After a system disk is detached from a server, the disk function changes to Bootable disk, and the disk status changes to Available. (A non-shared EVS disk is similar to a physical SSD or SATA disk. After attached, a non-shared disk can be partitioned into the C, D, and E drives for use.)

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

| You can create 397 more disks. The disks can use up to 32,668 GB of storage space. To renew multiple disks at a time, switch to the Renewals page. | | | | | | | | | |
|---|------------------------|----------------------------|-------------|-----------------|--------------|--------------|-----------|-----|---------------------------------|
| <input type="button" value="Delete"/> | | | | | | | | | |
| Disk Name | Status | Disk Spec... | Function | Server Name | Disk Shar... | Device Ty... | Encrypted | AZ | Billing ... |
| <input type="checkbox"/> volume-vivi | Available | General Purpos... 20 GB | Data disk | -- | Disabled | VBD | No | AZ1 | Pay-per-use Created on Ju... |
| <input type="checkbox"/> ecs-vivi | In-use | General Purpos... 40 GB | System disk | ecs-vivi ECS | Disabled | VBD | No | AZ1 | Pay-per-use Created on Ju... |

Figure 4-7 Viewing the EVS disk

Select the target Windows ECS and select a mount point from the drop-down list. The ECS and EVS disk must be in the same AZ.

Attach Disk

Disk:volume-vivi | Singapore | AZ1 | VBD | Non-shareable

ECSs BMSSs

| Name | Mount Point | Status | Image | Private IP Ad... | EIP | AZ |
|----------|-------------|---------|-----------------|------------------|-----------------|-----|
| ecs-vivi | /dev/vdb | Running | Windows Ser... | 192.168.0.19... | -- | AZ1 |
| ecs-S02 | | Stopped | CentOS 7.6 6... | 192.168.1.10... | 119.13.109.1... | AZ1 |

Figure 4-8 Attach Disk

Go back to the EVS disk list page. The disk status is Attaching, indicating that the disk is being attached to the server. When the disk status changes to In-use, the disk has been attached. You must initialize the disk before using it.

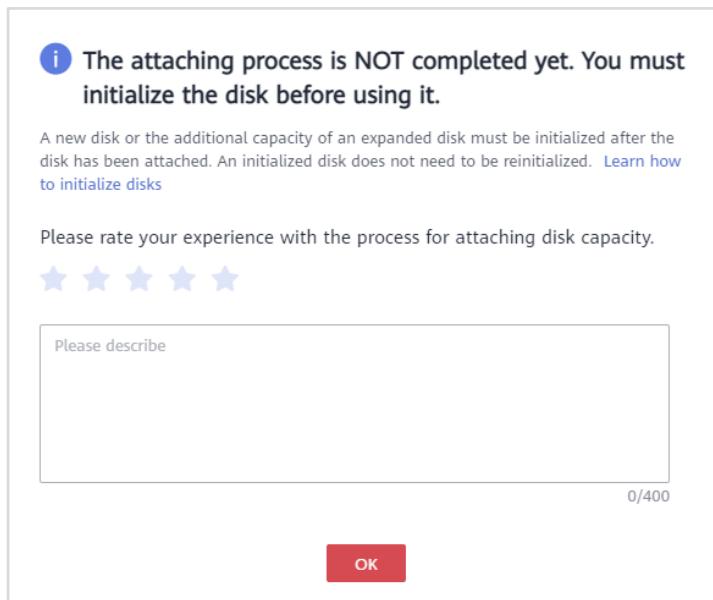


Figure 4-9 Disk attached

Initializing an EVS Disk

After a data disk is attached to an ECS, you must log in to the ECS and initialize the disk before using it.

Locate the row that contains the target ECS and click Remote Login in the Operation column.

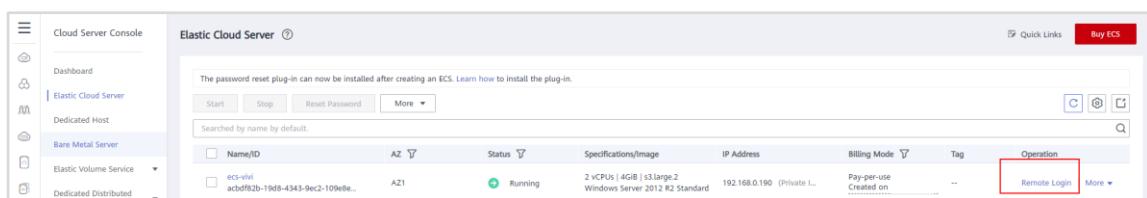


Figure 4-10 Logging in to the ECS

Log in using the RDP file or VNC. On the desktop of the ECS, choose Start > Server Manager. On the dashboard, choose Tools > Computer Management.

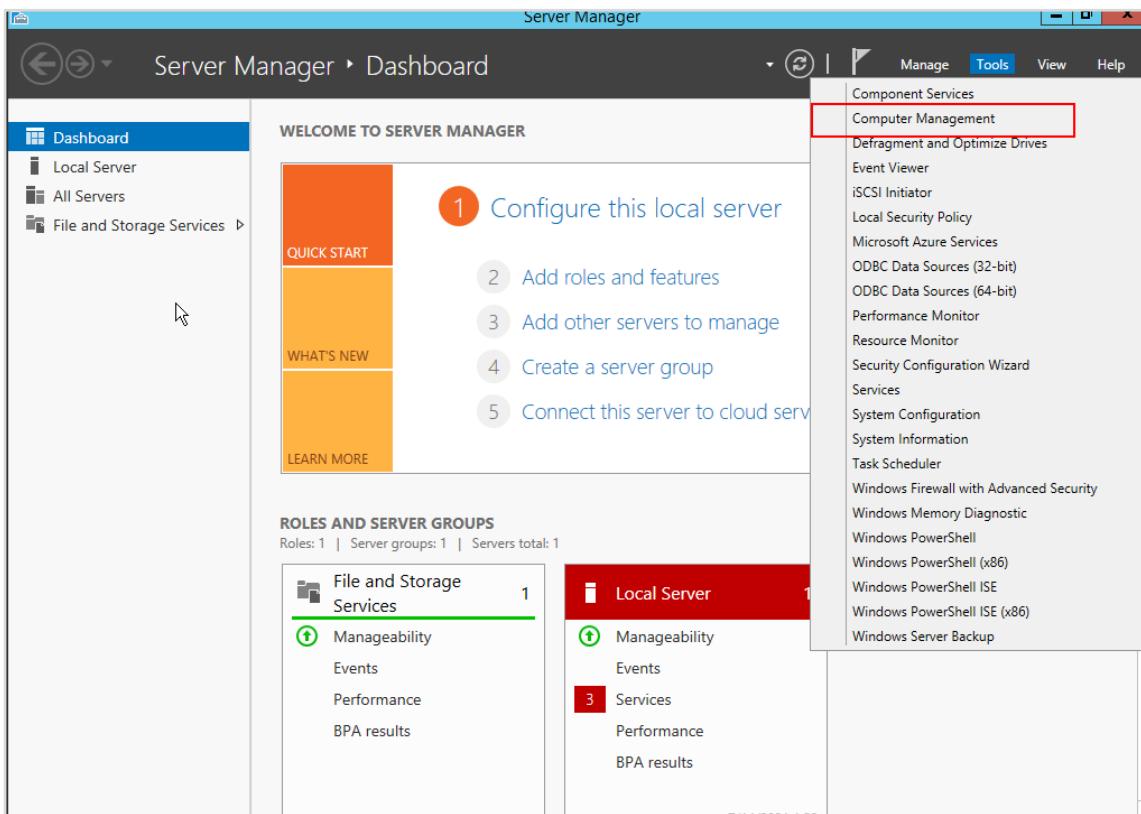


Figure 4-11 Opening Server Manager

In the navigation tree on the left, choose Storage > Disk Management.

On the Disk Management page, if the status of new disk is Offline, right-click Offline and choose Online to online the disk. If the status is Not Initialized, right-click the status and choose Initialize Disk. In the Initialize Disk window, select the target disk, click MBR (Master Boot Record) or GPT (GUID Partition Table), and click OK.

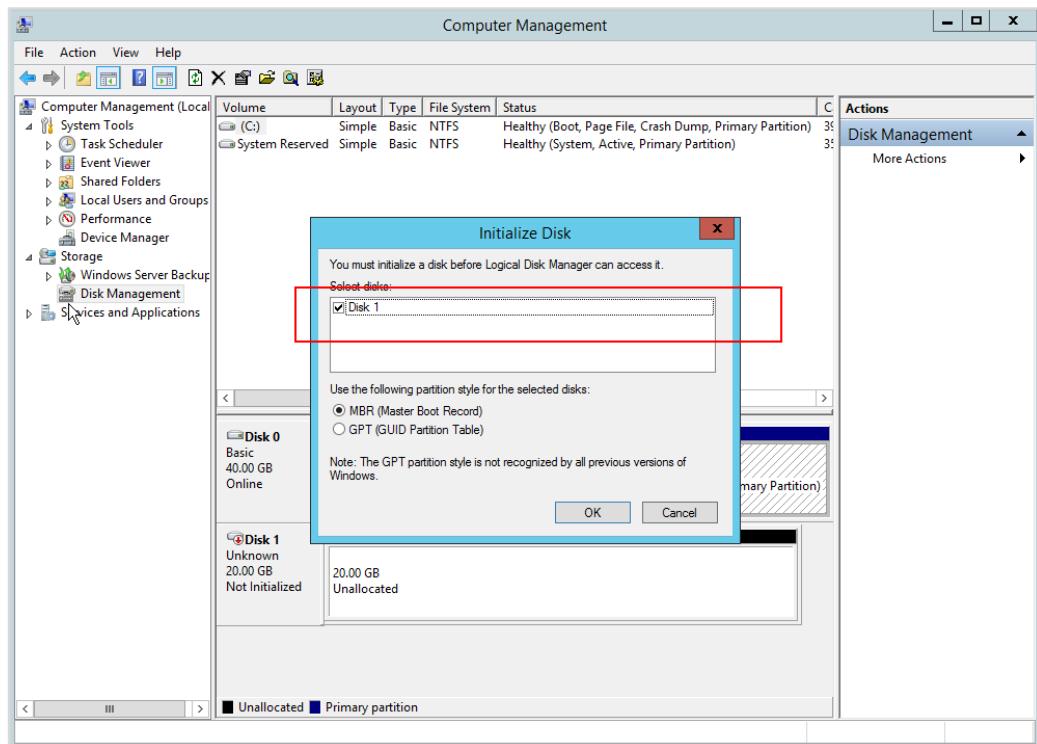


Figure 4-12 Initialize Disk

Right-click the unallocated area and choose New Simple Volume.

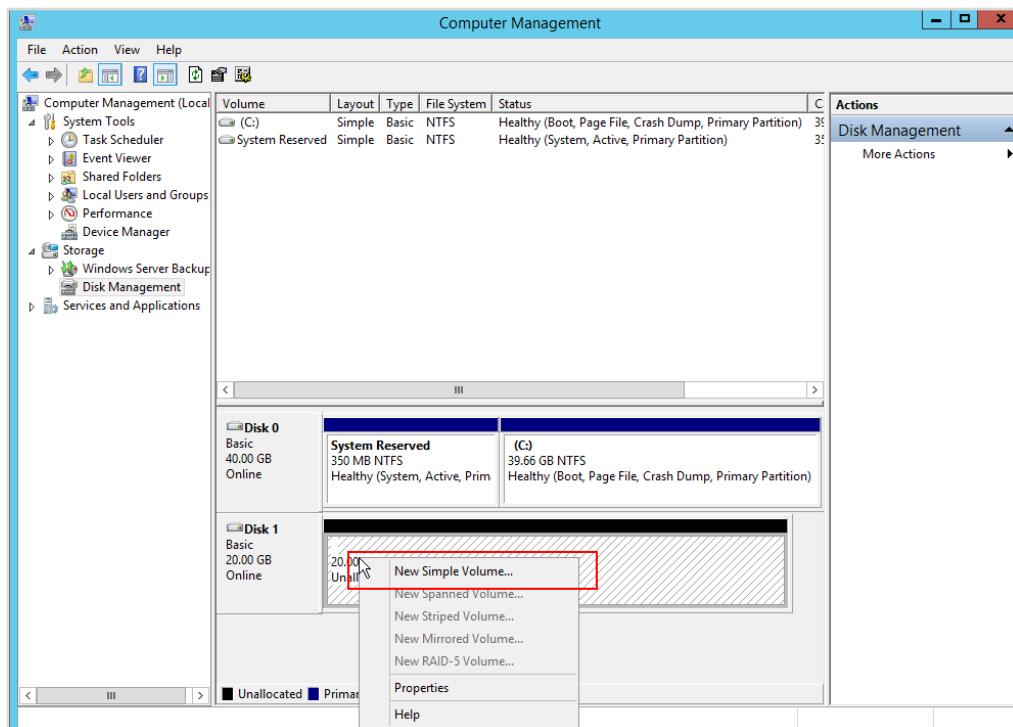


Figure 4-13 New Simple Volume

In the displayed New Simple Volume Wizard window, click Next.

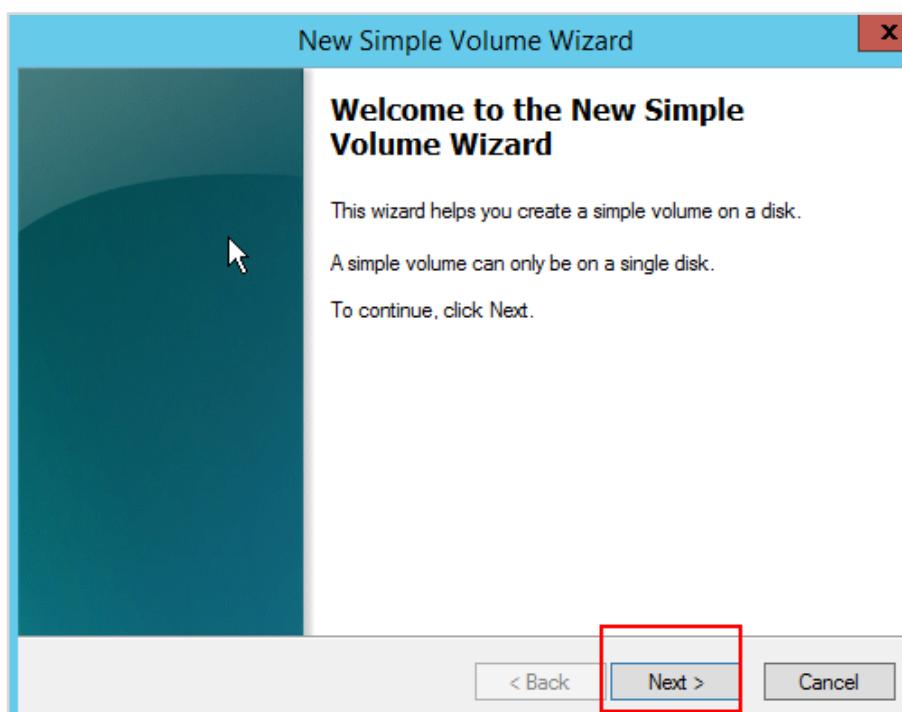


Figure 4-14 New Simple Volume

Specify the volume size and click Next. The default value is the maximum size.

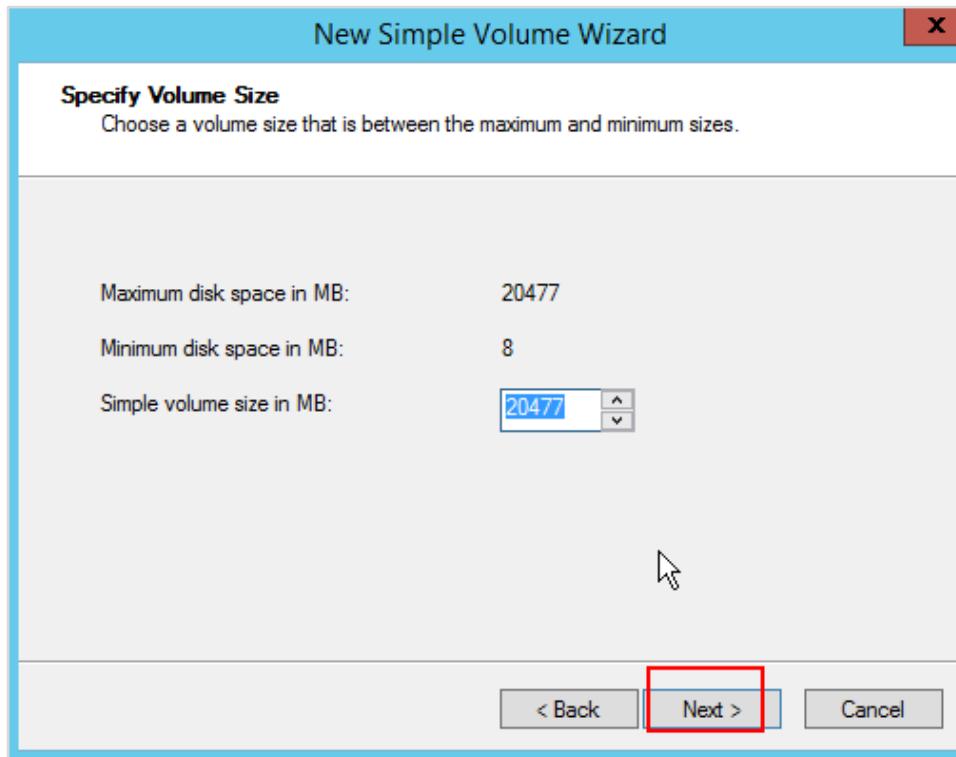


Figure 4-15 Specify Volume Size

Assign a drive letter and click Next.

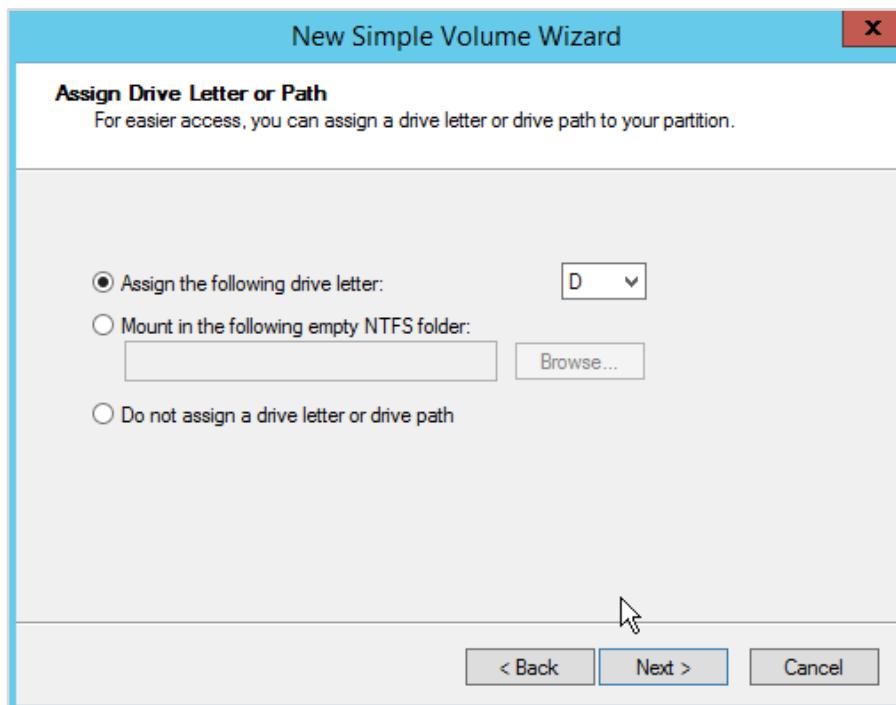


Figure 4-16 Assign Driver Letter or Path

Select Format this volume with the following settings, set parameters based on the requirements, and select Perform a quick format. Then, click Next.

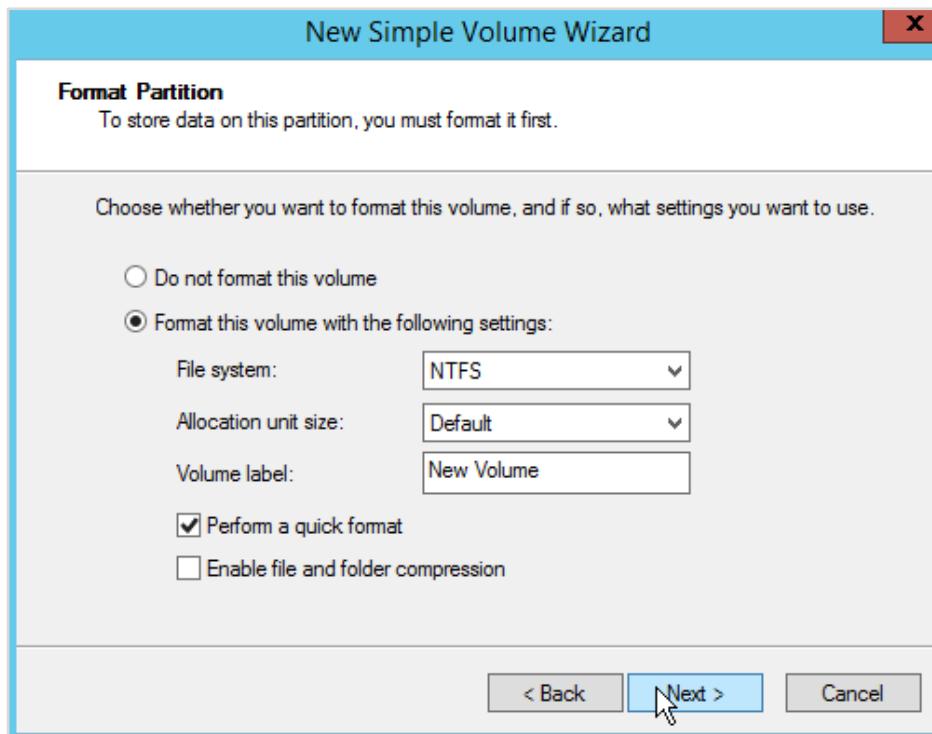


Figure 4-17 Formatting the partition

Click Finish. Wait for the initialization to complete. When the volume status changes to Healthy, the initialization is complete.

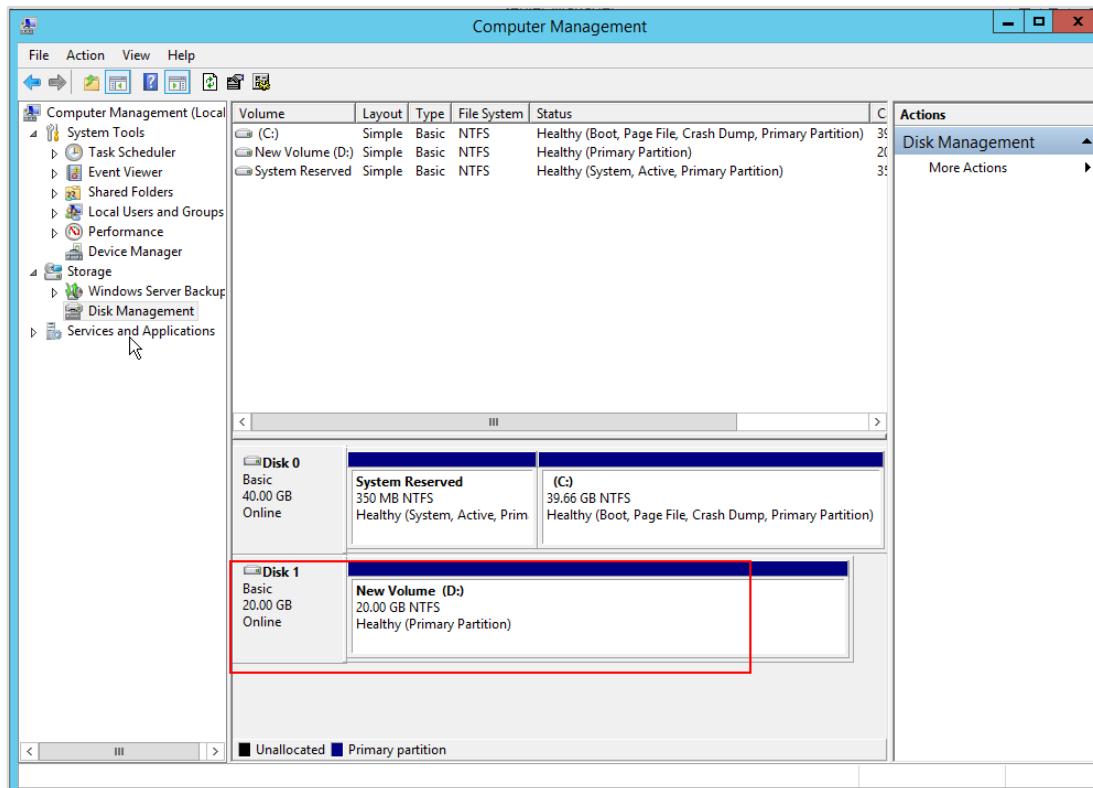


Figure 4-18 Viewing the initialized disk

Open This PC. If a new volume appears, the disk has been attached.

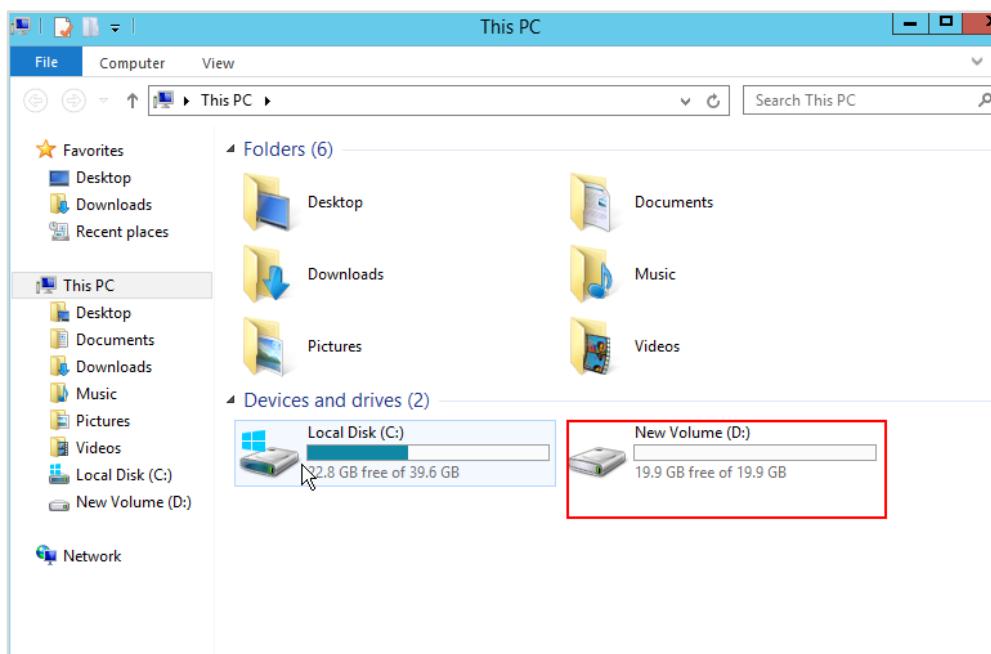


Figure 4-19 Viewing the new volume

Detaching an EVS Disk and Performing Verification

Before you detach an EVS disk on the console, log in to the ECS and unmount the disk. To verify that data on a detached EVS disk can still be used, we will detach the disk and then attach it to another ECS for verification.

Locate the row that contains the target ECS and click **Remote Login** in the Operation column.

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|--|-----|---------|--|----------------------------|---------------------------------|-----|----------------------------|
| ecs-vivi acbd82b-19d8-4343-9ec2-109e8e... | AZ1 | Running | 2 vCPUs 4GiB s3.large.2 Windows Server 2012 R2 Standard | 192.168.0.190 (Private IP) | Pay-per-use Created on Ju... | -- | Remote Login More ▾ |

Figure 4-20 Remotely logging in to the ECS

Create a test file **test.txt** on the attached EVS disk.

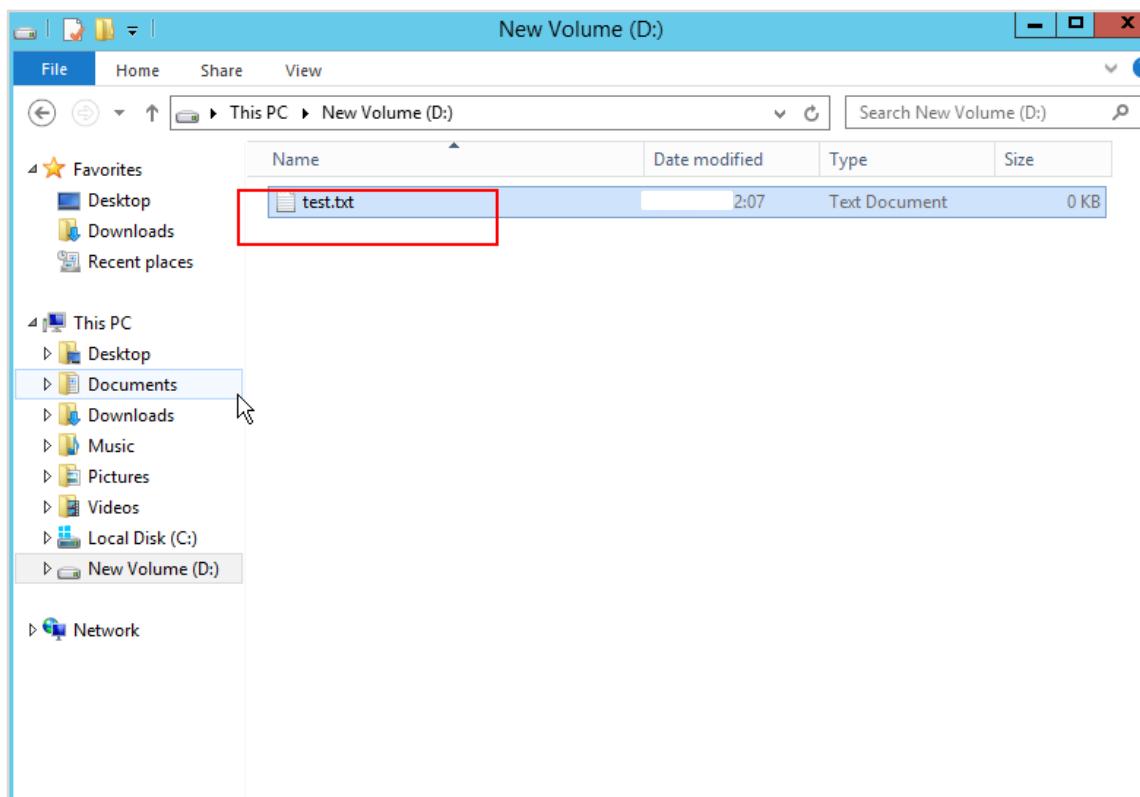


Figure 4-21 Creating the test file

Open the Disk Management window and bring the EVS disk offline.

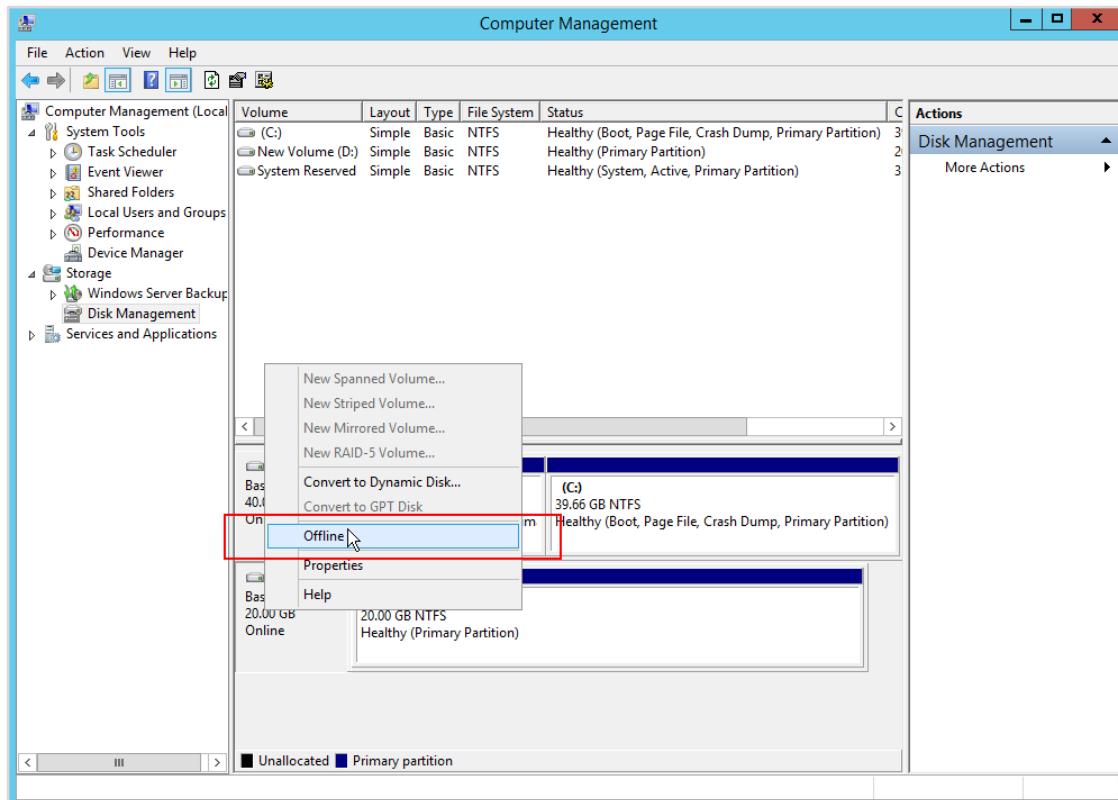


Figure 4-22 Bringing the new disk offline

Open This PC and check that volume D disappears.

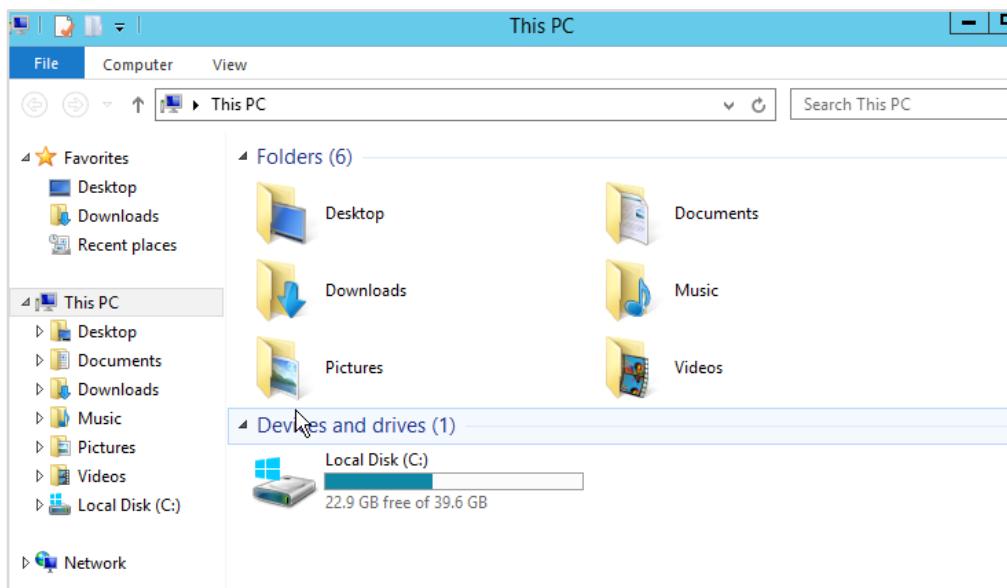


Figure 4-23 Checking whether the disk is offline

Buy another Windows ECS (Windows Server 2012 R2 Standard 64-bit English) by referring to the preceding sections.

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|--|-----|---------|--|----------------------------|---------------------------------------|-----|---------------------|
| ecs-test 25e18c04-bfe6-4456-8b13-826b46... | AZ1 | Running | 2 vCPUs 4GiB s3.large.2 Windows Server 2012 R2 Standard | 192.168.0.150 (Private IP) | Pay-per-use Created on Jul 1, 2023 | | Remote Login More ▾ |
| ecs-vivi acbdff82b-19d8-4343-9ec2-109e8e... | AZ1 | Running | 2 vCPUs 4GiB s3.large.2 Windows Server 2012 R2 Standard | 192.168.0.190 (Private IP) | Pay-per-use Created on Jul 1, 2023 | | Remote Login More ▾ |

Figure 4-24 Purchasing an ECS

Detach the EVS disk from ECS ecs-vivi and attach it to ECS ecs-test, the newly purchased ECS.



Figure 4-25 Detach Disk

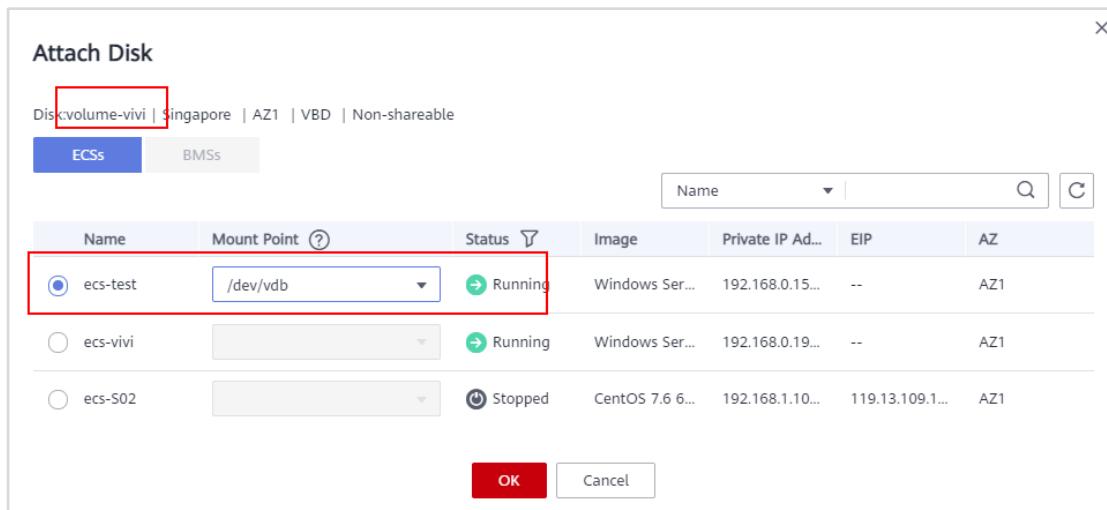


Figure 4-26 Attach Disk

Log in to the ECS console, find ECS ecs-test, and click Remote Login.

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|--|-----|---------|--|----------------------------|----------------------------------|-----|---------------------------------------|
| ecs-test 25e18cb4-bfe6-4456-8b13-826b46... | AZ1 | Running | 2 vCPUs 4GiB s3.large.2 Windows Server 2012 R2 Standard | 192.168.0.150 (Private IP) | Pay-per-use Created on J..... | -- | Remote Login More ▾ |
| ecs-vivi acbdff82b-19d8-4343-9ec2-109e8e... | AZ1 | Running | 2 vCPUs 4GiB s3.large.2 Windows Server 2012 R2 Standard | 192.168.0.190 (Private IP) | Pay-per-use Created on J..... | -- | Remote Login More ▾ |

Figure 4-27 Remotely logging in to the ECS

Open the Disk Management window and check that the EVS disk is online.

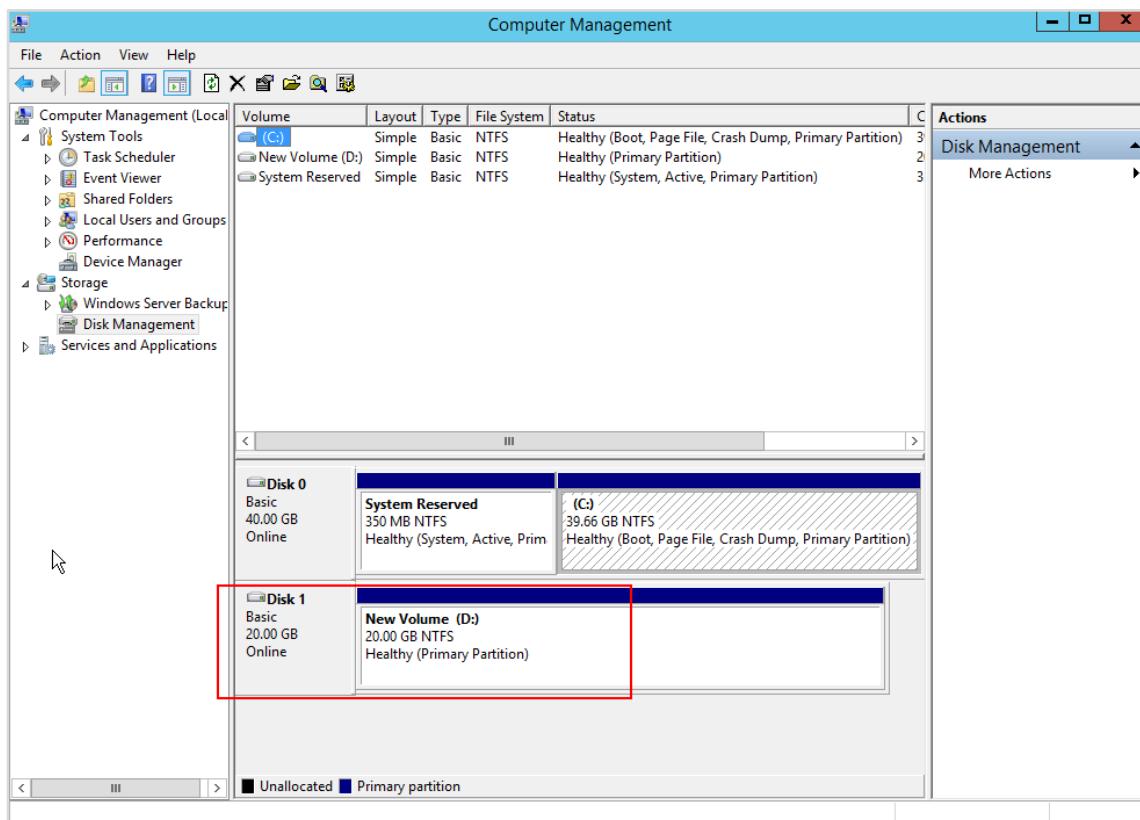


Figure 4-28 Viewing the disk status

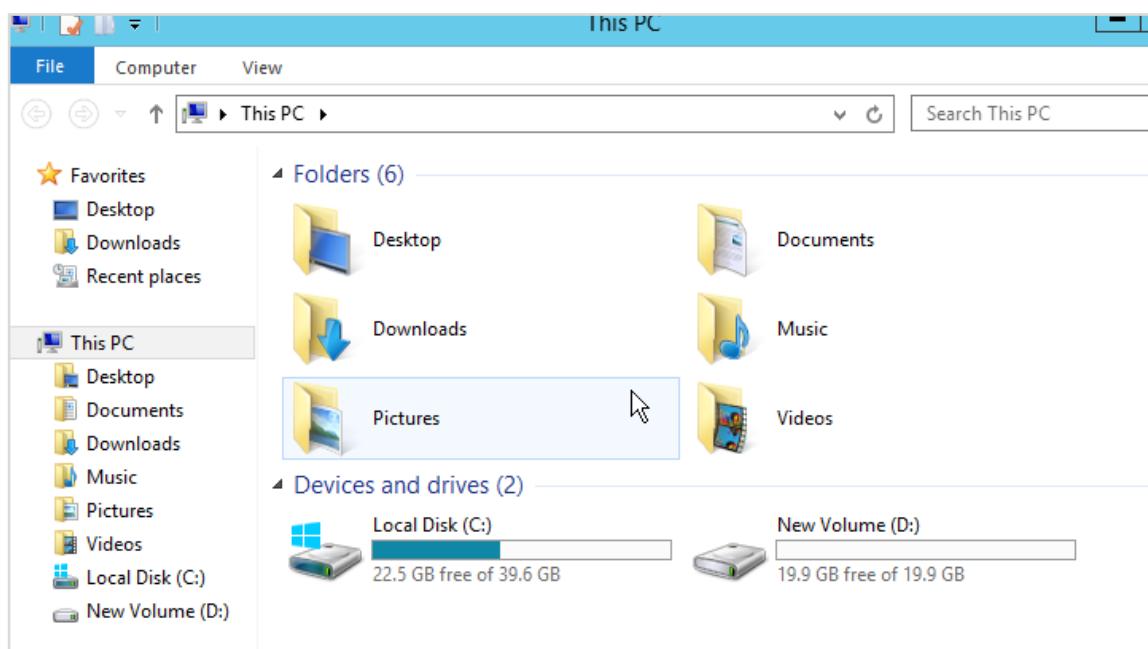


Figure 4-29 Checking whether a new volume appears

Check whether test file test.txt exists.

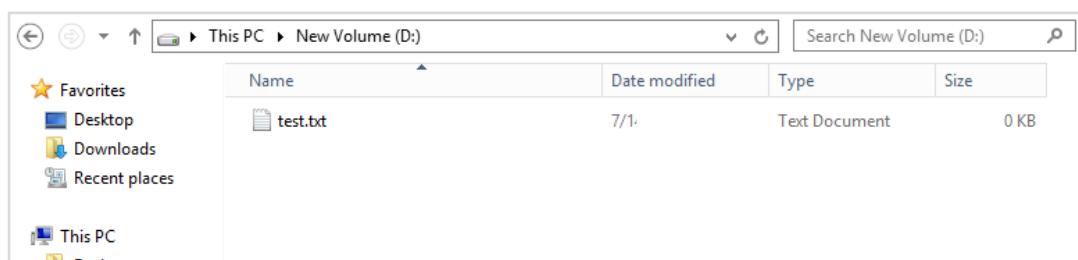


Figure 4-30 Viewing the test file

The file exists, verifying that this exercise succeeds.

4.1.2.3 Attaching an EVS Disk to a Linux ECS

Buy a Linux ECS (CentOS 7.6 64 bit) by referring to the preceding sections.

Purchase a non-shared EVS disk and name it volume-linuxadd by referring to the preceding section, and attach the disk to the purchased ECS. (When purchasing the disk, select the AZ where the Linux ECS resides for the disk.)

Remotely log in to the Linux ECS and run the following command to view the new data disk:

```
fdisk -l
```

```
[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: 0x0002af06

      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
```

Figure 4-31 Viewing the disk

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

Run the following command to enter fdisk to partition the new data disk:

In this example, run the following command:

```
fdisk /dev/vdb
```

```
[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 0x35a056c7.

Command (m for help):
```

Figure 4-32 Initializing the disk

Enter n and press Enter to create a partition.

```
Command (m for help): n
Partition type:
  p  primary (0 primary, 0 extended, 4 free)
  e  extended
```

Figure 4-33 Creating a partition

In this example, a primary partition is created. Therefore, 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.

```
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048):
```

Figure 4-34 Assigning a partition name

First sector indicates the start sector. The value ranges from 2048 to 20971519, and the default value is 2048.

Press Enter. The default first sector 2048 is used.

```
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):
```

Figure 4-35 Allocating the disk space

Last sector indicates the end sector. The value ranges from 2048 to 20971519, and the default value is 20971519.

Press Enter. The default last sector 20971519 is used.

```
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
Command (m for help):
```

Figure 4-36 Initialization completed

A primary partition has been created for a 10-GB data disk.

Enter p and press Enter to view details about the new partition.

```
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: 0x35a056c7

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

Command (m for help):
```

Figure 4-37 Viewing partition information

Details about the /dev/vdb1 partition are displayed.

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

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

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

Figure 4-38 Save and Exit

In case that you want to discard the changes made before, you can exit fdisk by entering q.

Run the following command to synchronize the changes in the partition table to the OS:

```
partprobe
```

Run the following command to set the file system format for the new partition:

```
mkfs -t File system format /dev/vdb1
```

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

```
mkfs -t ext4 /dev/vdb1
```

```
[root@ecs-linux ~]# mkfs -t 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
```

Figure 4-39 Formatting the partition

The formatting takes a period of time. Wait until the task status changes to done.

Run the following command to create a mount point:

In this example, run the following command to create a mount point /mnt/sdc:

```
mkdir /mnt/sdc
```

Run the following command to mount the new partition on the created mount point:

In this example, run the following command to mount the new partition on /mnt/sdc:

```
mount /dev/vdb1 /mnt/sdc
```

Run the following command to view the mount result:

```
df -TH
```

```
[root@ecs-linux ~]# df -TH
Filesystem      Type   Size  Used Avail Use% Mounted on
devtmpfs        devtmpfs 509M    0  509M  0% /dev
tmpfs          tmpfs   520M    0  520M  0% /dev/shm
tmpfs          tmpfs   520M  7.1M 513M  2% /run
tmpfs          tmpfs   520M    0  520M  0% /sys/fs/cgroup
/dev/vda1       ext4    43G  2.2G 38G  6% /
tmpfs          tmpfs   104M    0  104M  0% /run/user/0
/dev/vdb1       ext4    11G  38M  9.9G 1% /mnt/sdc
```

Figure 4-40 Viewing mount result

New partition /dev/vdb1 has been mounted on /mnt/sdc.

4.1.2.4 (Optional) Setting Automatic Mounting at System Start

In the Linux ECS, run the command to query the UUID of the disk partition.

In this example, run the following command to obtain the UUID of /dev/vdb1:

```
blkid /dev/vdb1
```

```
[root@ecs-linux ~]# blkid /dev/vdb1
/dev/vdb1: UUID="8493dccb-1a8c-4225-8e9c-84eb1243cf23" TYPE="ext4"
```

Figure 4-41 Setting automatic mounting

Run the following command to open the fstab file:

```
vi /etc/fstab
```

Press i to enter editing mode and add the following content (replace the UUID with what you have obtained):

```
UUID=8493dccb-1a8c-4225-8e9c-84eb1243cf23 /mnt/sdc ext4 defaults 0 2
```

Press Esc, enter :wq, and press Enter to exit editing mode.

Run the command to unmount the partition. In this example, run the following command:

```
umount /dev/vdb1
```

Run the following command to reload all the content in the /etc/fstab file:

```
mount -a
```

Run the following command to query the file system mounting information:

```
mount | grep /mnt/sdc
```

```
[root@ecs-linux ~]# mount | grep /mnt/sdc  
/dev/vdb1 on /mnt/sdc type ext4 (rw,relatime,data=ordered)
```

Figure 4-42 Querying mounting information

4.1.2.5 (Optional) Using Snapshots

On the ECS ecs-linux, run the following commands to create a test file:

```
mkdir /mnt/sdc/snapshot  
cd /mnt/sdc/snapshot  
echo "snapshot test">> test.file  
cat test.file
```

```
[root@ecs-linux snapshot]# cat test.file  
snapshot test
```

Figure 4-43 Creating the test file

Locate the EVS disk purchased before and choose More > Create Snapshot in the Operation column.

| Disk Name | Status | Disk Spec... | Function | Server Name | Disk Shar... | Device Ty... | Encrypted | AZ | Billing ... | Operation |
|----------------|--------|----------------------------|-------------|------------------|--------------|--------------|-----------|-----|---------------------------------|---|
| volume-diskadd | In-use | General Purpos... 10 GB | Data disk | ecs-Linux ECS | Disabled | VBD | No | AZ1 | Pay-per-use Created on Ju... | Attach Expand Capacity More Detach |
| ecs-Linux | In-use | General Purpos... 40 GB | System disk | ecs-Linux ECS | Disabled | VBD | No | AZ1 | Pay-per-use Created on Ju... | Attach Create Snapshot Create Backup |
| ecs-S02 | In-use | General Purpos... 40 GB | System disk | ecs-S02 ECS | Disabled | VBD | No | AZ1 | Pay-per-use Created on Ju... | Attach Change Billing Mode Delete |

Figure 4-44 Create Snapshot

Name the snapshot volume-linuxdata and click Create Now.

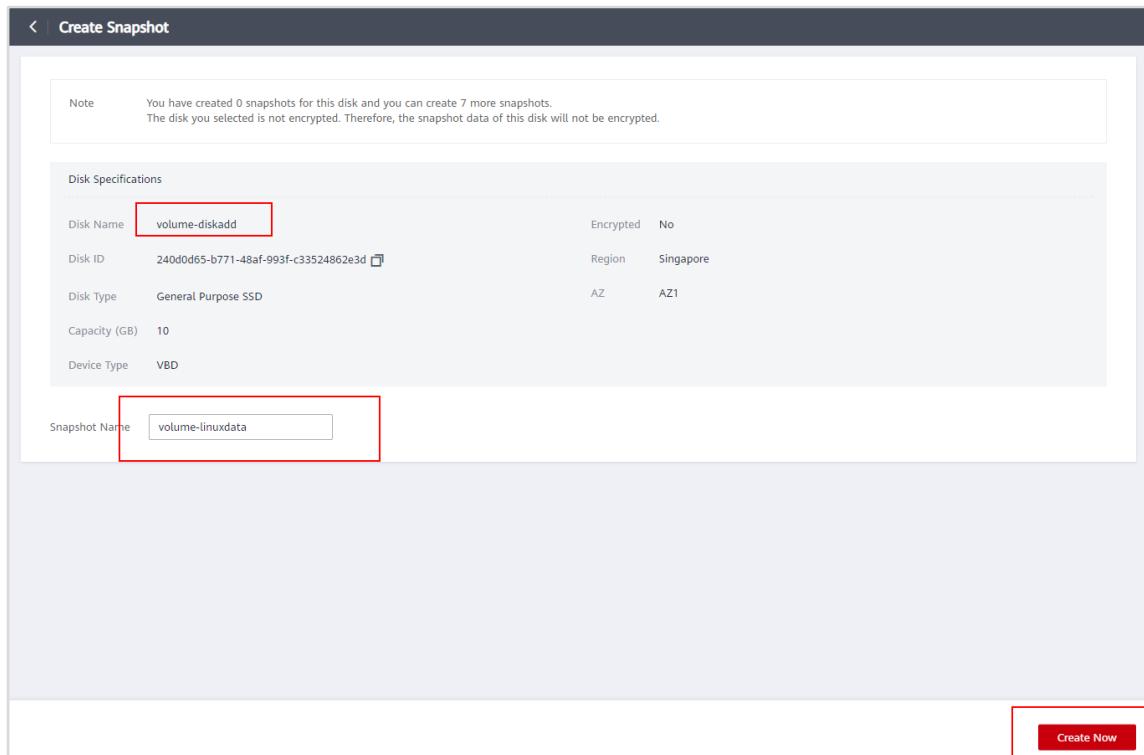


Figure 4-45 Setting snapshot parameters

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

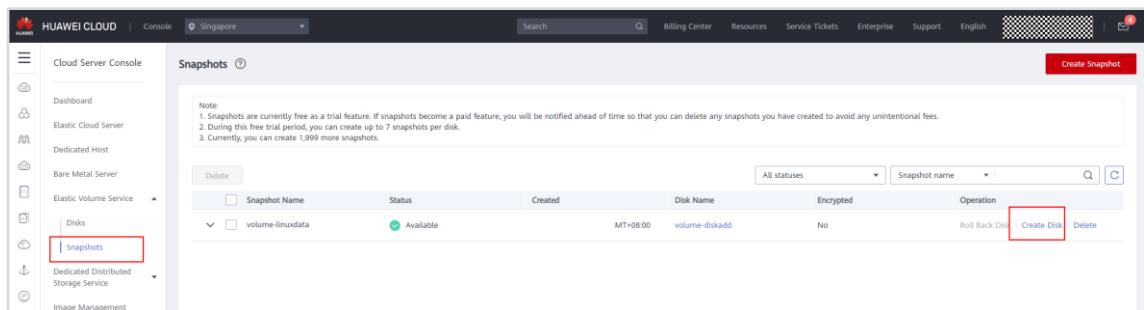


Figure 4-46 Create Disk

Buy a disk according to the following figure.

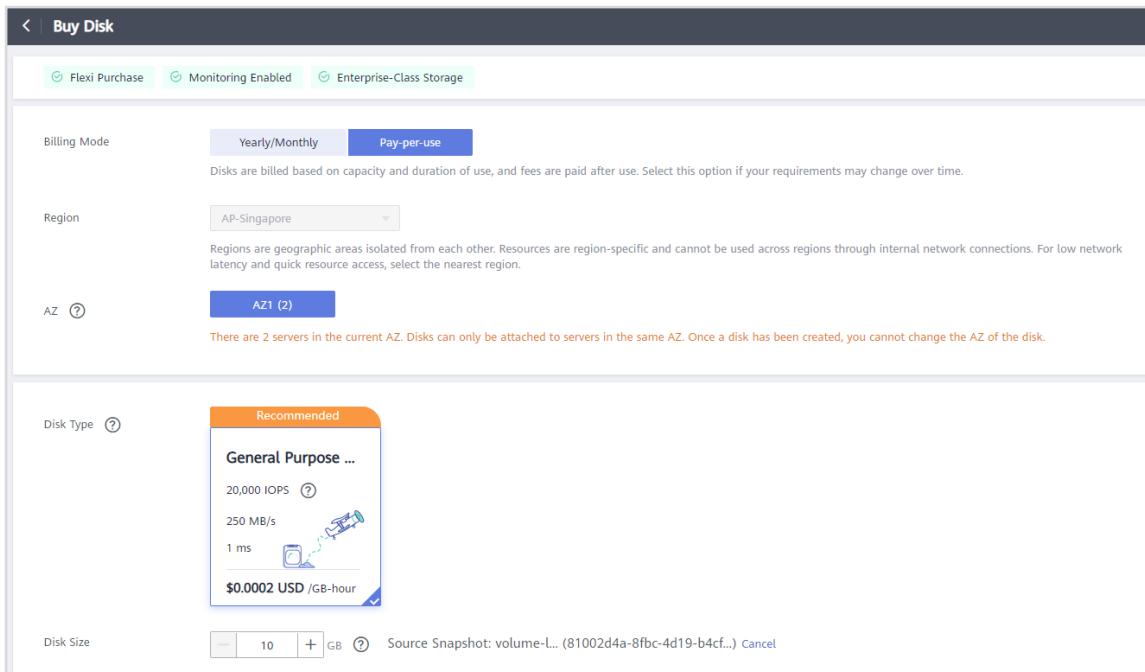


Figure 4-47 Setting disk parameters

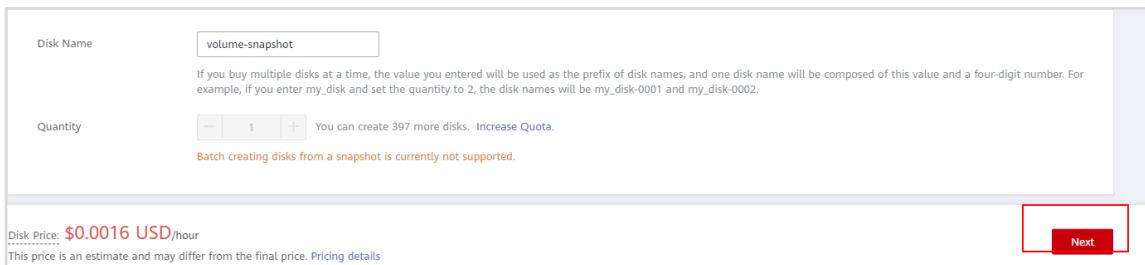


Figure 4-48 Setting disk parameters

View the disk created from the snapshot.



Figure 4-49 Viewing the disk

Attach the disk to ECS ecs-linux.

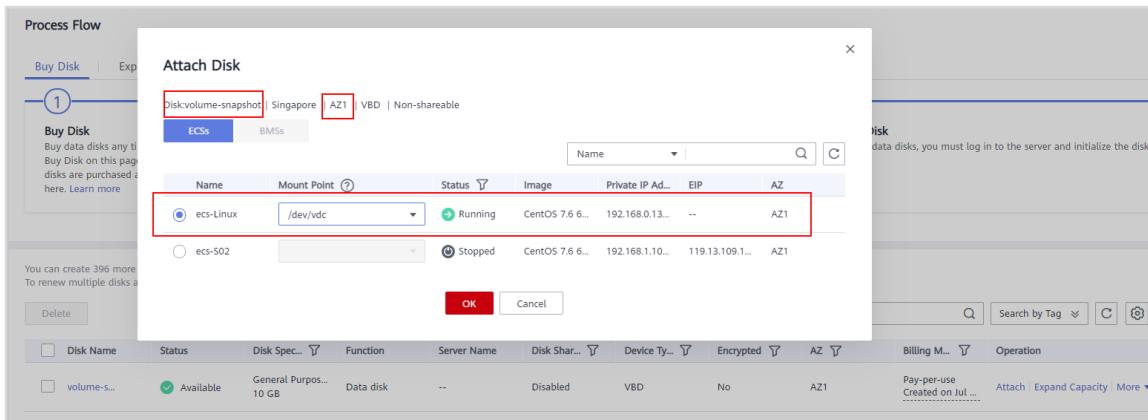


Figure 4-50 Attach Disk

Log in to ECS ecs-linux and view the new data disk.

```
fdisk -l
```

```
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: 0x6e6f062a

Device Boot      Start         End      Blocks   Id  System
/dev/vdc1          2048    20971519   10484736   83  Linux
```

Figure 4-51 Viewing the disk

Run the following command to create a mount point:

```
mkdir /mnt/mdc
```

Run the following command to mount the new partition /dev/vdc1 on /mnt/mdc:

```
mount /dev/vdc1 /mnt/sdc
```

Switch to /mnt/sdc and check whether the snapshot file has been synchronized.

```
cd /mnt/sdc/snapshot
ls
cat test.file
```

```
[root@ecs-linux snapshot]# cat test.file
snapshot test
```

Figure 4-52 Checking whether snapshot file has been synchronized

If the preceding command output is returned, the snapshot file has been synchronized.

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:

- Install OBS Browser+.
- Use basic OBS Browser+ functions, such as creating buckets and folders, uploading, downloading, and deleting files or folders, and deleting buckets.

4.2.2 Tasks

4.2.2.1 Roadmap

- When users log in to OBS Console using their HUAWEI CLOUD account or as an IAM user, OBS authenticates their account or IAM user credentials.
- When users access OBS using the tools (OBS Browser+ or obsutil), SDKs, or APIs, OBS requires access keys (AK and SK) for authentication. Therefore, users need to obtain the access keys (AK and SK) before they access OBS using any methods other than OBS Console.

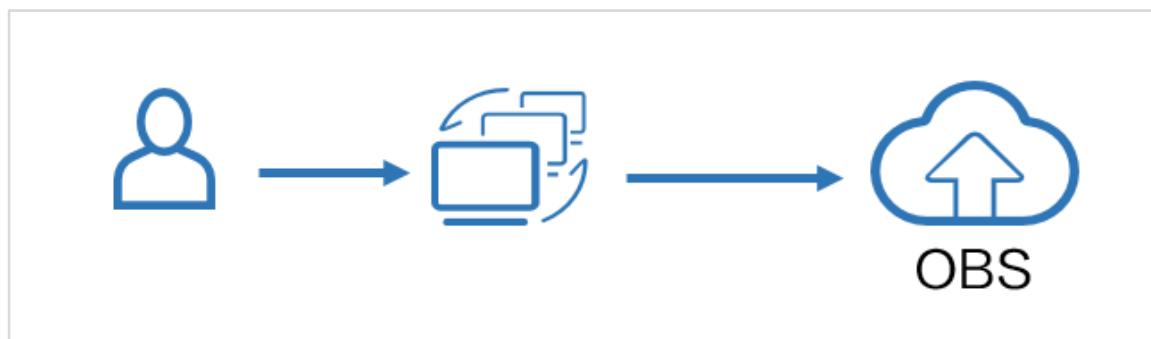


Figure 4-53 Topology

4.2.2.2 Using OBS Browser+

Obtaining Access Keys (AK and SK)

On the homepage of HUAWEI CLOUD console, hover your cursor over your username and choose My Credentials.

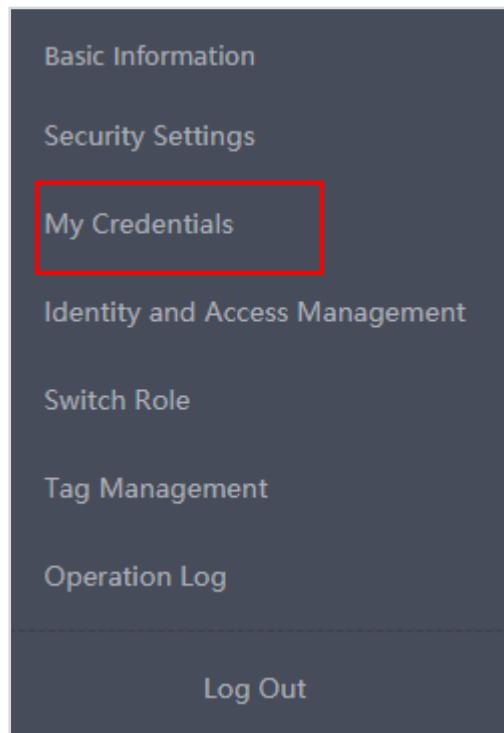
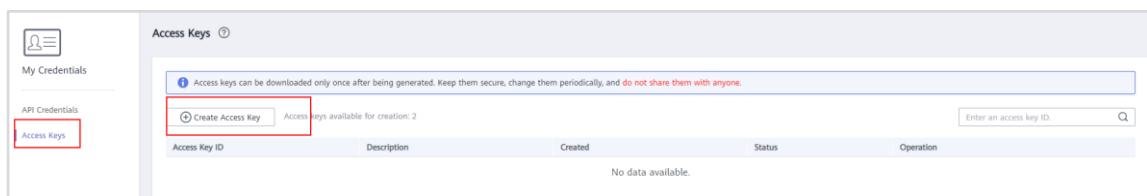


Figure 4-54 My Credentials

In the navigation pane, choose Access Keys. Click Create Access Key.



The image shows the 'Access Keys' page in the HUAWEI CLOUD console. On the left, there's a sidebar with 'My Credentials' and 'API Credentials' sections, with 'Access Keys' highlighted by a red box. The main area has a header 'Access Keys' with a note about keeping keys secure. Below is a table with columns: Access Key ID, Description, Created, Status, and Operation. A button labeled 'Create Access Key' is highlighted with a red box. The table shows 'No data available.'

Figure 4-55 Create Access Key

In the displayed dialog box, enter the email or SMS verification code.

(NÃO SE APLICA A TODAS AS REGIÕES)

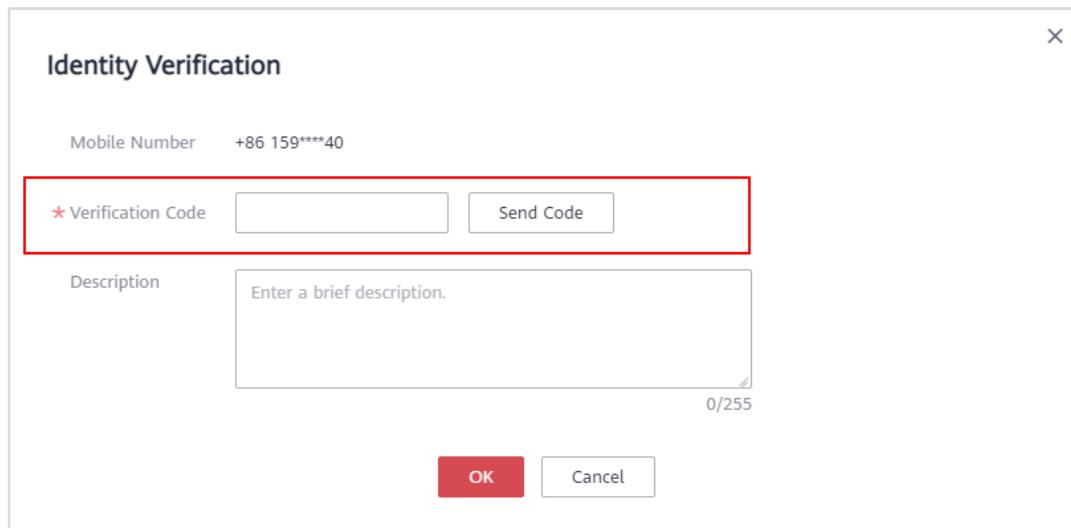


Figure 4-56 Identity Verification

Click OK to download the key file.

Save the key file when prompted.

Keep the access keys properly.

Open the downloaded file credentials.csv to obtain the AK and SK pair.

Downloading and Initializing OBS Browser+

On the console homepage, choose Service List > Storage > Object Storage Service.

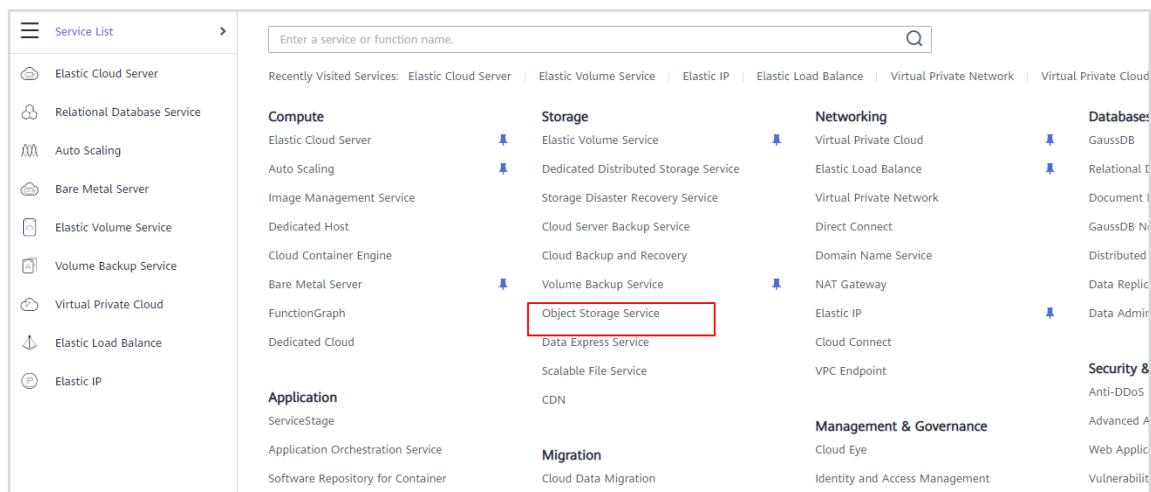


Figure 4-57 Accessing OBS Console

Open https://support.huaweicloud.com/intl/en-us/browsertg-obs/obs_03_1003.html on a new tab and download the OBS Browser+ package corresponding to the OS of your local PC.

Table 1 List of download addresses

| Supported OS | Download Link |
|--------------|---|
| Windows x32 | OBSBrowserPlus-win32 OBSBrowserPlus-win32_sha256 |
| Windows x64 | OBSBrowserPlus-win64 OBSBrowserPlus-win64_sha256 |
| Mac | OBSBrowserPlus-Mac OBSBrowserPlus-Mac_sha256 |

Figure 4-58 Downloading OBS Browser+

Decompress the downloaded software package and install it.

Log in to OBS Browser+ using access keys.

- **Account Name:** `obs_test` is used as an example.
- **Service:** Select **HUAWEI CLOUD OBS (default)**. Once selected, OBS Browser+ automatically sets the server domain name to the OBS service domain name.
- **Access Key ID:** Obtain it from the downloaded key file.
- **Secret Access Key:** Obtain it from the downloaded key file.
- **Access Path:** Leave it blank.

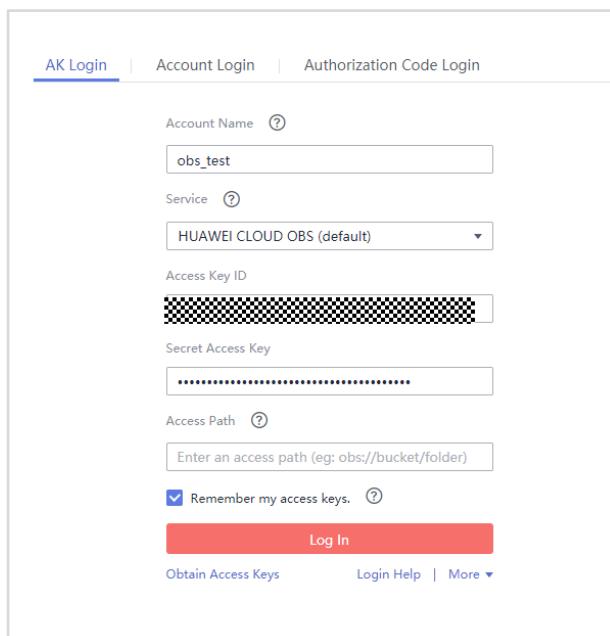


Figure 4-59 Logging in to OBS Browser+

OBS Browser+ saves the login details for a maximum of 100 accounts. If a proxy is required to access your network environment, configure the network proxy under More > Settings > Network before login.

Creating a Bucket

In the upper left corner of OBS Browser+ homepage, click Create Bucket.

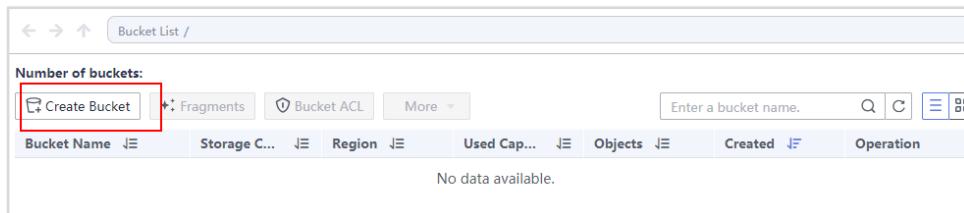


Figure 4-60 Creating a bucket

In the Create Bucket dialog box, configure the following parameters:

- **Region:** LA-SaoPaulo
- **Storage Class:** Select Standard.
- **Bucket ACL:** Private
- **Multi-AZ Mode:** It is disabled by default.
- **Bucket Name:** test-obs is used as an example. You can hover your cursor over the tooltip to view the bucket naming rules.

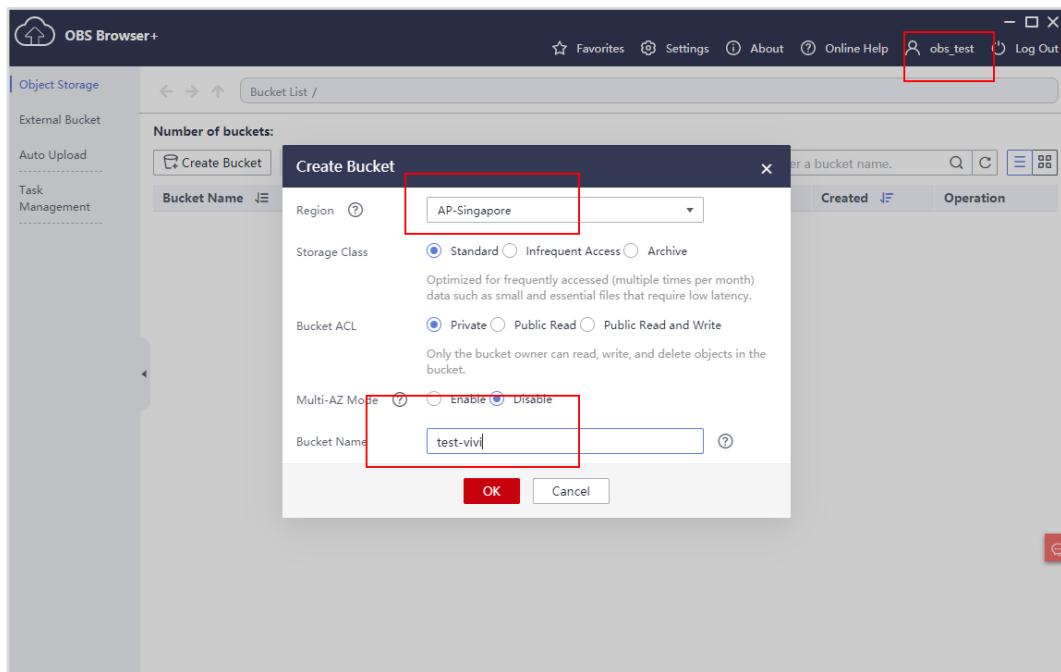


Figure 4-61 Configuring bucket information

Click OK. A dialog box is displayed, indicating whether the bucket is created.

4.2.2.3 Uploading a File or Folder

Click the name of the created bucket to go to the object list page.

Click Upload.

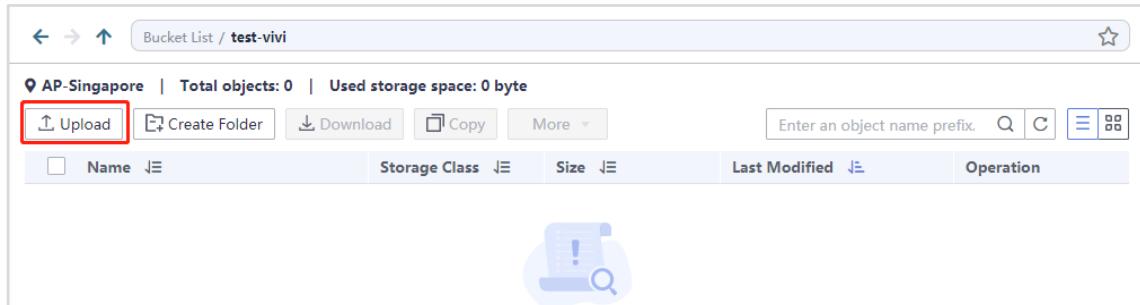


Figure 4-62 Uploading a file

In the Upload dialog box, click File.

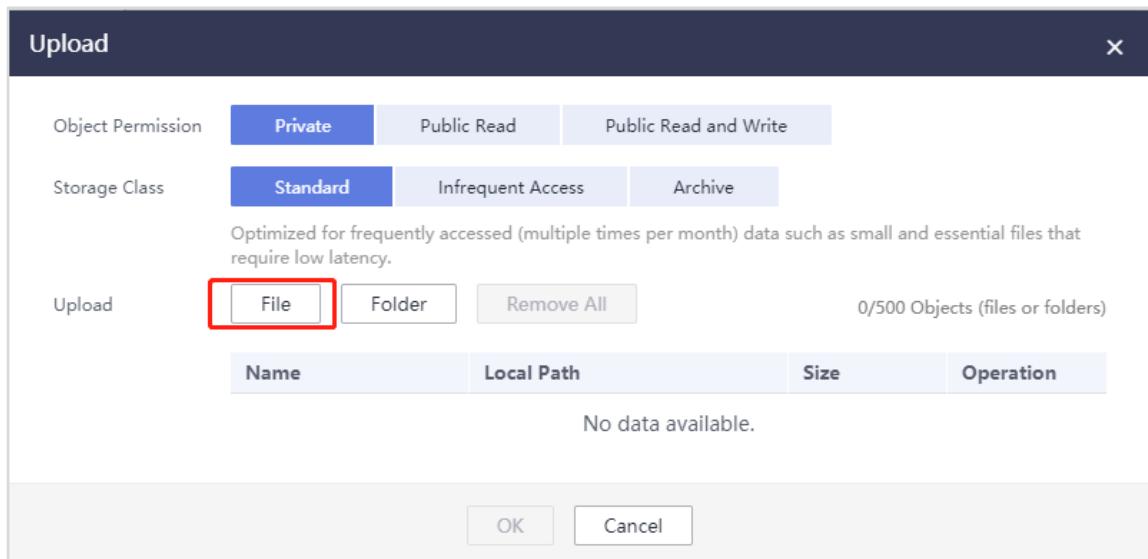


Figure 4-63 Adding a file

Select the files to be uploaded and click OK.

(Optional) Click Task Manager in the upper right corner of the page to go to the task management page. The upload progress is displayed. You can suspend, run, or cancel upload tasks as needed.

View the uploaded file or folder in the list.

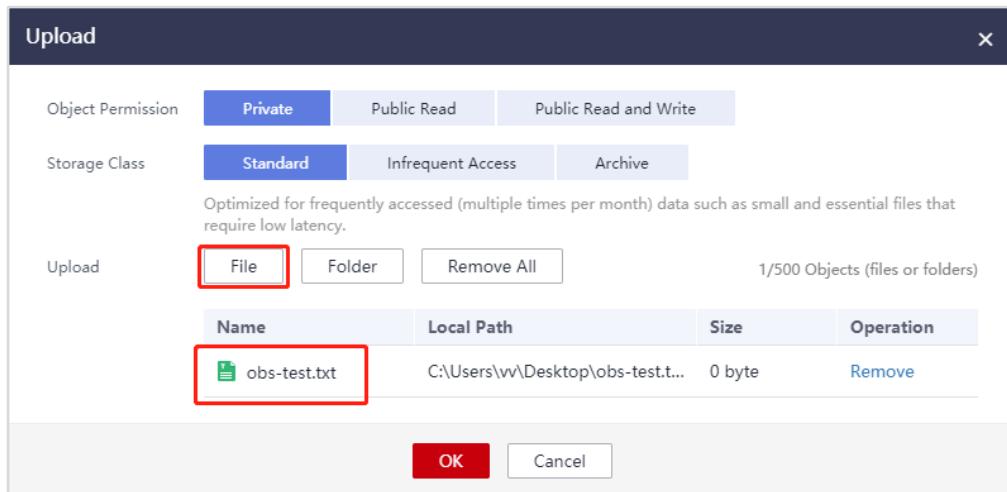


Figure 4-64 Viewing the uploaded file

4.2.2.4 Downloading a File or Folder

In the object list, select the file or folder to be downloaded and click Download.

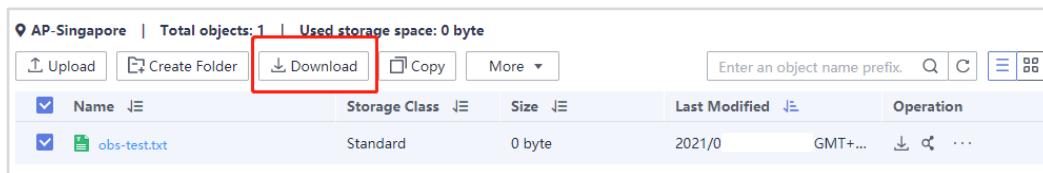


Figure 4-65 Downloading a file

In the dialog box, select a path for saving the downloaded file on your local PC.

(Optional) In the navigation pane, click Task Management. The download progress of the file or folder is displayed. You can suspend, run, or cancel download tasks as needed.

4.2.2.5 Deleting a File or Folder

In the object list, select the file or folder to be deleted, and choose More > Delete in the Operation column.

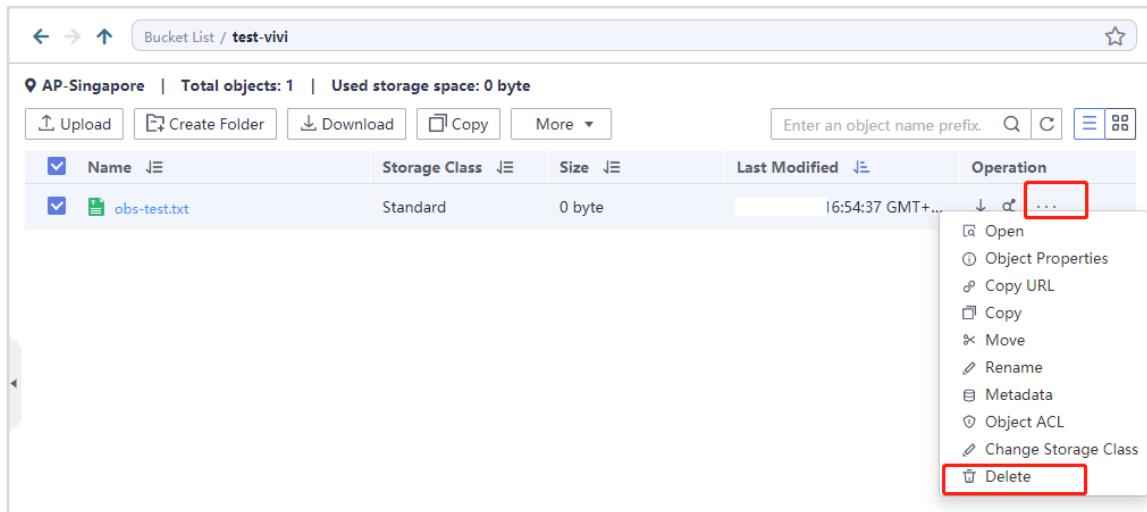


Figure 4-66 Deleting a file

In the Delete Object dialog box, click Yes.

(Optional) Go to the Task Management page. The deletion progress of a file or folder is displayed. You can suspend, run, or cancel deletion tasks as needed.

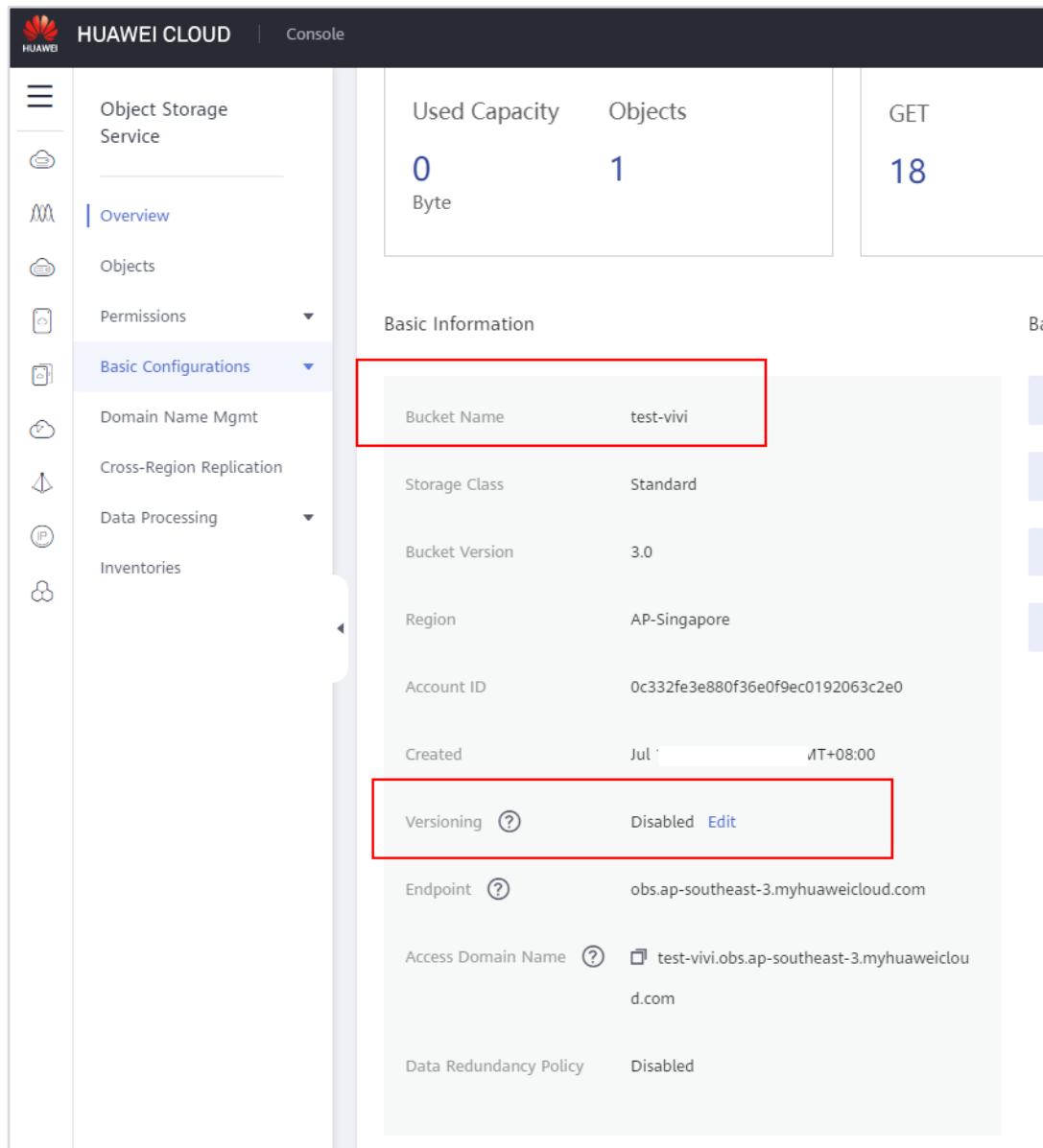
4.2.2.6 Managing Versioning

Log in to OBS Console and find the created bucket from the bucket list.

| Bucket Name | Storage Class | Region | Used Capacity | Objects | Created | Operation |
|-------------|---------------|--------------|---------------|---------|----------|---|
| test-vivi | Standard | AP-Singapore | 0 Byte | 1 | MT+08:00 | Change Storage Class Delete |

Figure 4-67 Logging in to OBS Console

Click the bucket name to go to the Overview page. In the Basic Information area, move your cursor next to Versioning to view its status.



The screenshot shows the HUAWEI CLOUD OSS console. On the left, there's a sidebar with various service icons and a dropdown menu for 'Basic Configurations'. The main area displays basic statistics: Used Capacity (0 Byte), Objects (1), and GET requests (18). Below this is a 'Basic Information' table with the following details:

| | |
|------------------------|--|
| Bucket Name | test-vivi |
| Storage Class | Standard |
| Bucket Version | 3.0 |
| Region | AP-Singapore |
| Account ID | 0c332fe3e880f36e0f9ec0192063c2e0 |
| Created | Jul 1 2023 11:47:11 AM +08:00 |
| Versioning | Disabled |
| Endpoint | obs.ap-southeast-3.myhuaweicloud.com |
| Access Domain Name | test-vivi.obs.ap-southeast-3.myhuaweicloud.com |
| Data Redundancy Policy | Disabled |

A red box highlights the 'Bucket Name' field and the 'Versioning' row, which shows 'Disabled' with an 'Edit' link. The 'Versioning' link has a question mark icon above it.

Figure 4-68 Viewing versioning status

Click Edit next to Versioning. In the Versioning dialog box, select Enable and then OK.

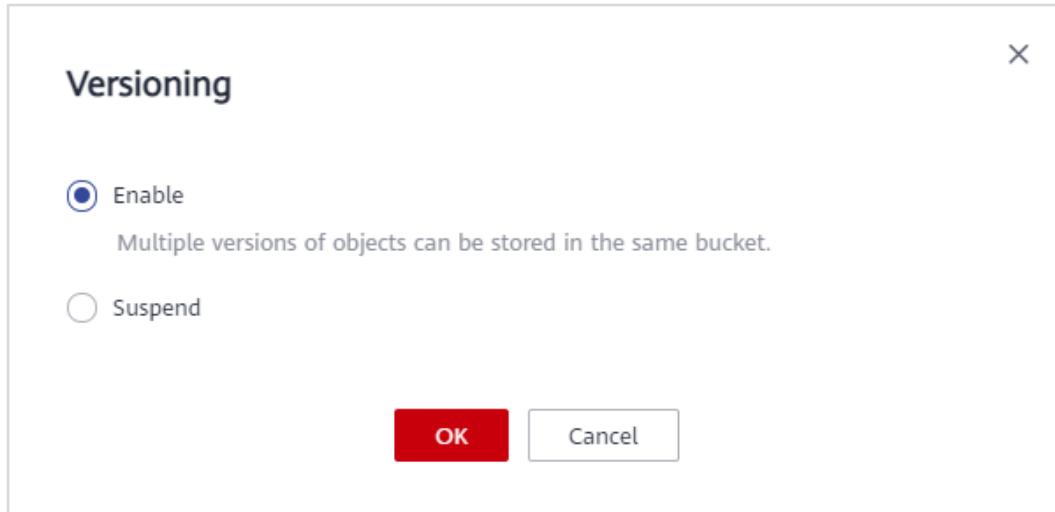


Figure 4-69 Enabling versioning

In the navigation pane, choose Objects. On the displayed page, click Upload Object to upload two objects with the same name.

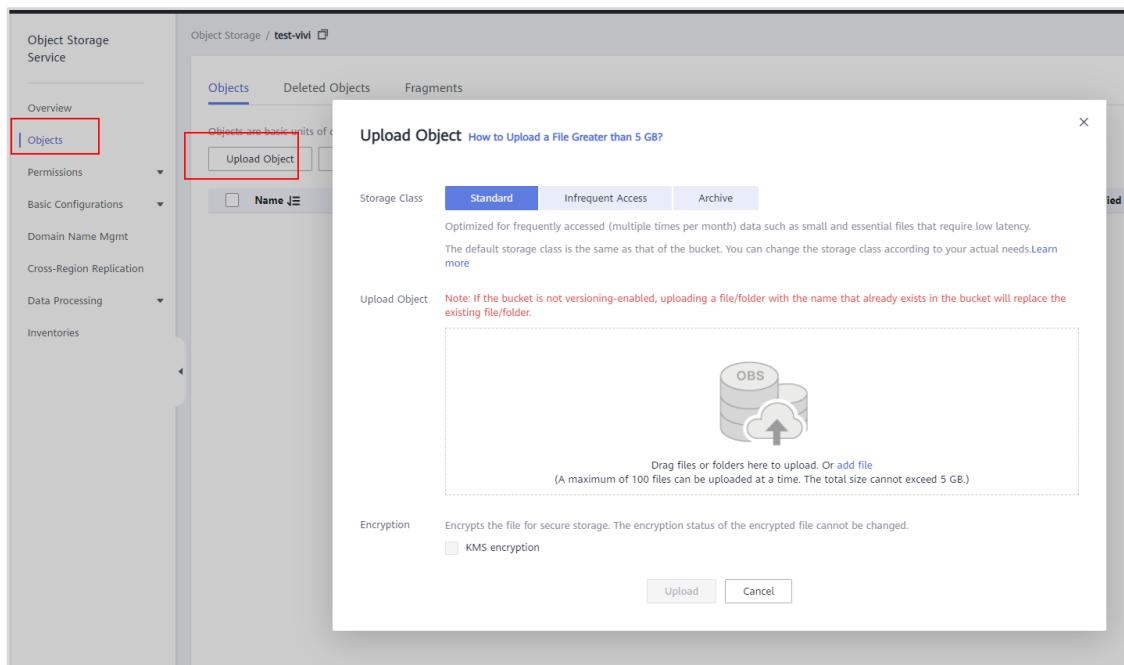


Figure 4-70 Uploading objects

Click the name of the uploaded object to view its properties.

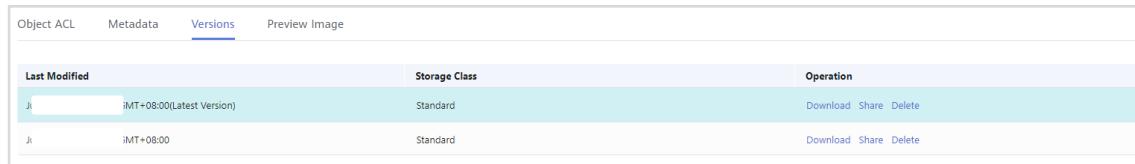


The screenshot shows the 'Objects' tab in the OBS console. A single file, '1.png', is listed. The table columns include Name, Storage Class, Size, Encrypted, Restoration Status, Last Modified, and Operation. The '1.png' row is highlighted with a red border. The 'Operation' column for this row contains the 'Share' link.

| Name | Storage Class | Size | Encrypted | Restoration Status | Last Modified | Operation |
|-------|---------------|-----------|-----------|--------------------|-----------------------|-----------------------|
| 1.png | Standard | 137.39 KB | No | -- | Jul 17, 2021 17:09:36 | Share |

Figure 4-71 Viewing the uploaded objects

On the Versions page, view the different object versions.

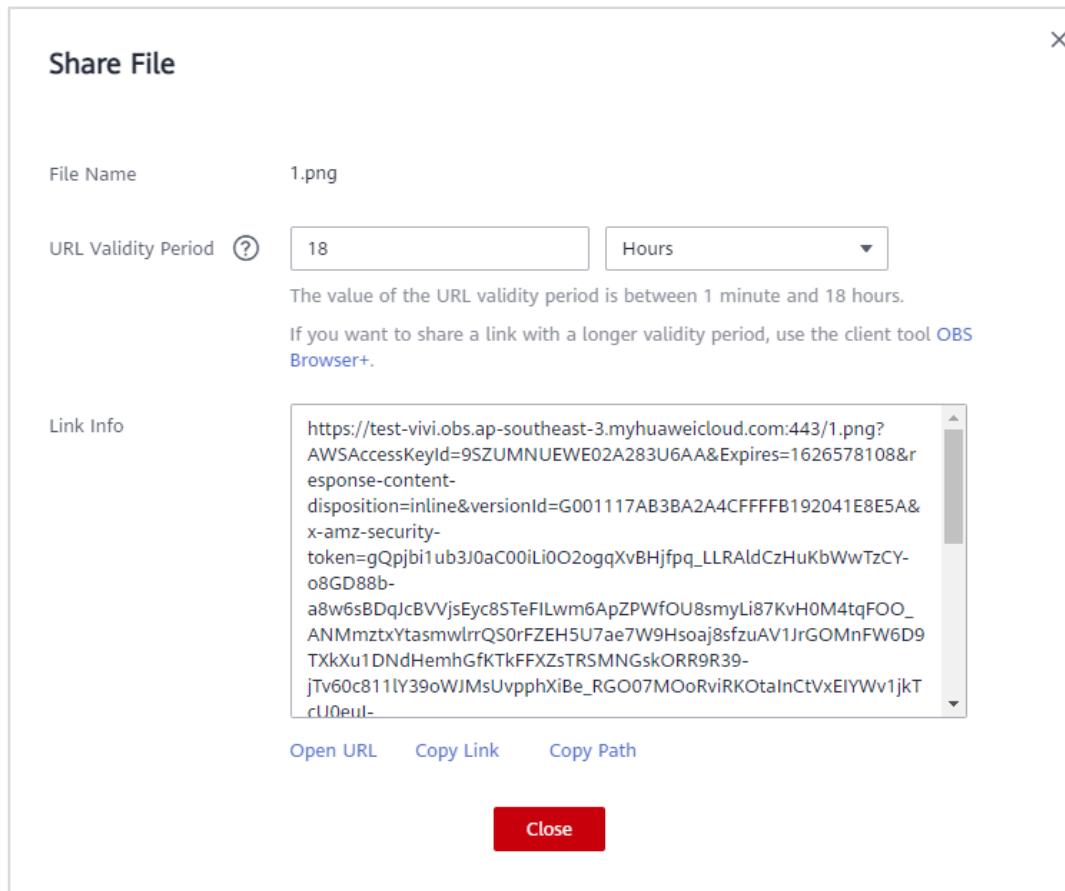


The screenshot shows the 'Versions' tab in the OBS console for the '1.png' object. It lists two versions. The first version is the latest, with a timestamp of 'Ji iMT+08:00(Latest Version)'. The second version is older, with a timestamp of 'Ji iMT+08:00'. Both versions have the same storage class, 'Standard'. The 'Operation' column for each version includes 'Download', 'Share', and 'Delete' links.

| Last Modified | Storage Class | Operation |
|------------------------------|---------------|---|
| Ji iMT+08:00(Latest Version) | Standard | Download Share Delete |
| Ji iMT+08:00 | Standard | Download Share Delete |

Figure 4-72 Viewing object versions

Click Share in the Operation column of the row containing the object to be shared. In the Share File dialog box, enter a URL validity period, and copy the link for sharing.



The screenshot shows the 'Share File' dialog box for the '1.png' file. The 'File Name' field is set to '1.png'. The 'URL Validity Period' field shows '18 Hours'. A note below states: '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 OBS Browser+'. The 'Link Info' section displays a long URL starting with 'https://test-vivi.obs.ap-southeast-3.myhuaweicloud.com:443/1.png?'. At the bottom, there are 'Open URL', 'Copy Link', and 'Copy Path' buttons, and a 'Close' button.

Figure 4-73 Sharing a file

A shared file can be valid for 18 hours at most.

View the two different object versions with the same name through each shared link.

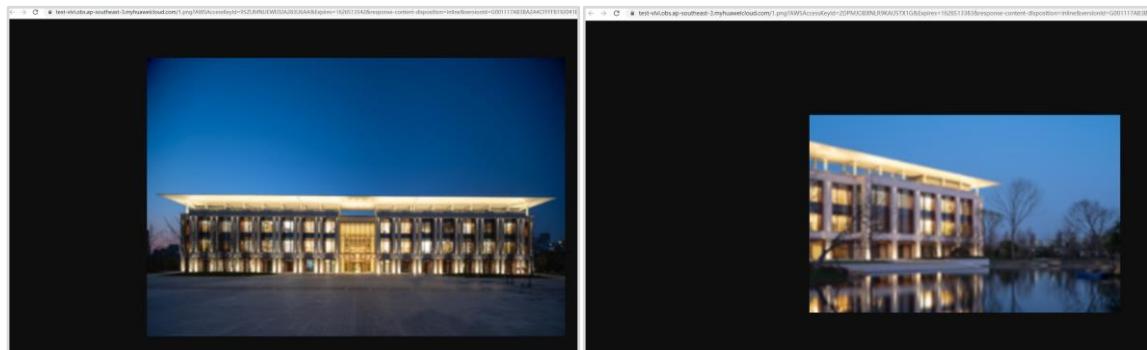


Figure 4-74 Viewing shared files

4.2.3 Deleting Resources

On OBS Console, delete the created OBS resources. Before deleting a bucket, you must delete all files in it.

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.

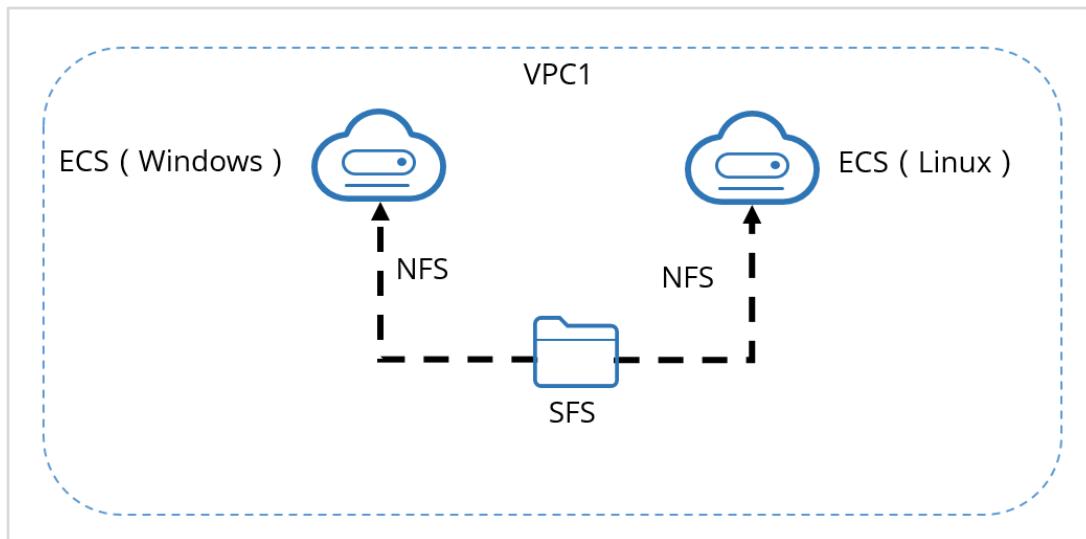


Figure 4-75 Topology

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 and Windows servers.
- Enable cloud servers in different VPCs to share the same SFS file system.

4.3.2 Tasks

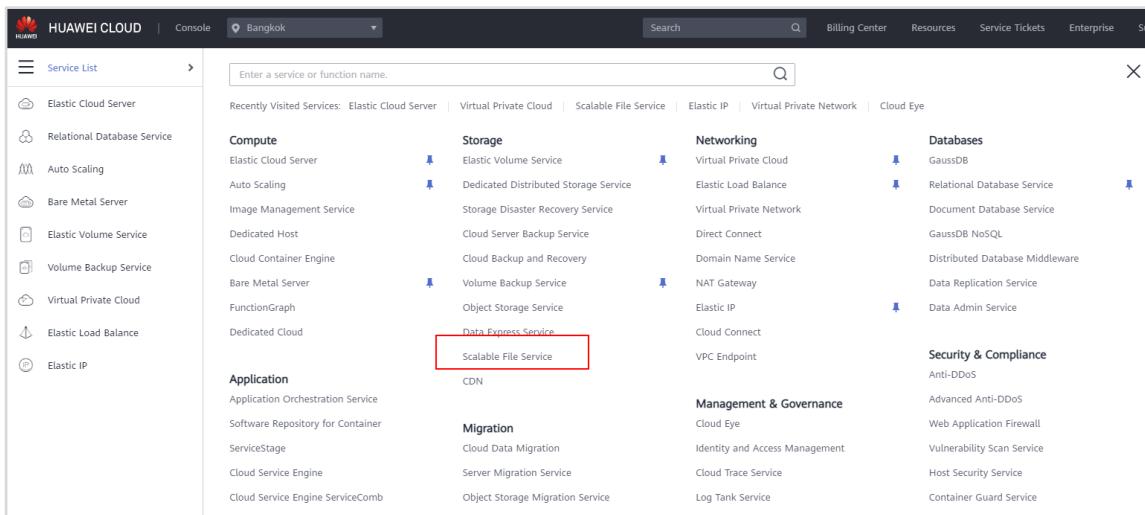
4.3.2.1 Creating an SFS File System

Prerequisites

- A VPC **vpc-mp** has been created.
- A Linux ECS **ecs-linux** running CentOS 7.6 has been purchased (**t6.small.1**). An EIP has been bound to the ECS, and the ECS locates in VPC **vpc-mp**.
- A Windows ECS **ecs-windows** running Windows Server 2012 (**s3.large.2**) has been purchased. An EIP has been bound to the ECS, and the ECS locates in VPC **vpc-mp**.

Creating an SFS File System

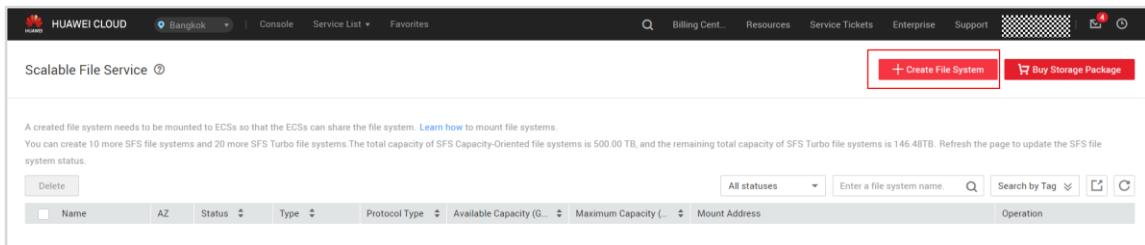
Log in to the HUAWEI CLOUD console on **LA-SaoPaulo** region and choose **Scalable File Service** in the service list.



The screenshot shows the HUAWEI CLOUD Service List interface. The left sidebar has a 'Service List' section with various cloud services like Elastic Cloud Server, Relational Database Service, Auto Scaling, Bare Metal Server, etc. The main area is a grid of services categorized into Compute, Storage, Networking, Databases, Application, Migration, Management & Governance, and Security & Compliance. A red box highlights the 'Scalable File Service' under the Storage category. The top navigation bar shows 'Console' and 'Bangkok'. The top right has links for Billing Center, Resources, Service Tickets, Enterprise, and Support.

Figure 4-76 Opening the SFS console

Click Create File System.

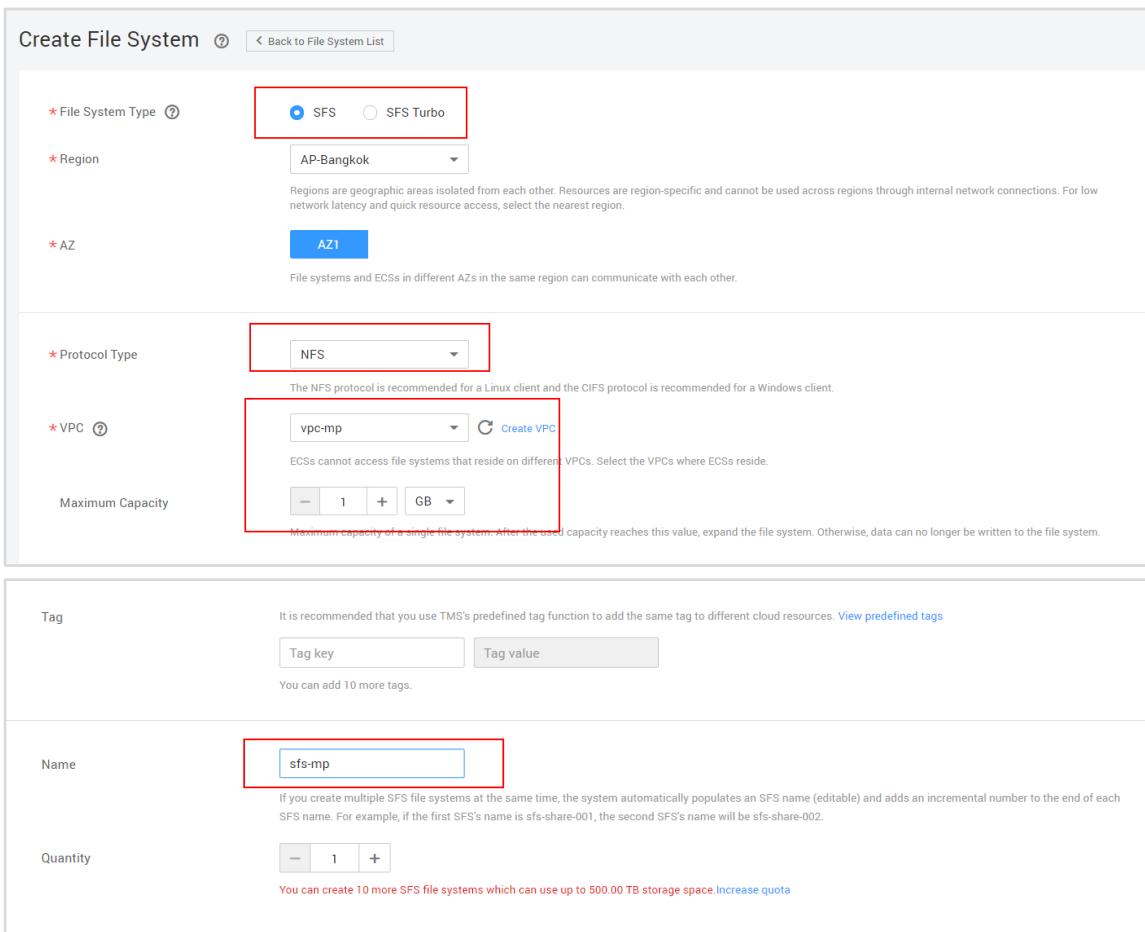


The screenshot shows the 'Scalable File Service' creation page. It features a large red box around the '+ Create File System' button at the top right. Below it is a message about mounting file systems to ECSS. The main area has a table for listing file systems with columns for Name, AZ, Status, Type, Protocol Type, Available Capacity, Maximum Capacity, and Mount Address. There are filters for 'All statuses', 'Enter a file system name', 'Search by Tag', and 'Operation'.

Figure 4-77 Create File System

On the displayed page, set the name, file system type, and VPC for the file system you are creating.

- **File System Type:** SFS
- **Region:** LA-SaoPaulo1
- **AZ:** AZ1
- **Protocol Type:** NFS
- **VPC:** Select an existing VPC or create one.
- **Maximum Capacity:** 1 GB
- **Name:** sfs-mp
- **Quantity:** 1
- Retain the default settings for other parameters.



The screenshot shows the 'Create File System' interface. The 'File System Type' is selected as 'SFS'. The 'Region' is set to 'AP-Bangkok'. The 'AZ' is set to 'AZ1'. The 'Protocol Type' is set to 'NFS'. The 'VPC' dropdown shows 'vpc-mp' and a 'Create VPC' button. The 'Maximum Capacity' is set to 1 GB. In the 'Tag' section, there is a 'Tag key' input field and a 'Tag value' input field. The 'Name' is set to 'sfs-mp'. The 'Quantity' is set to 1. A note at the bottom says 'You can create 10 more SFS file systems which can use up to 500.00 TB storage space. Increase quota'.

Figure 4-78 Setting file system parameters

Click Next.

On the Details page, confirm the configuration and click Submit.

| Details | | |
|----------|---|----------|
| Resource | Configuration | Quantity |
| SFS | Region: AP-Bangkok Name: sfs-mp AZ: AZ1 Protocol Type: NFS VPC: vpc-mp Tag: -- | 1 |

Figure 4-79 Confirming parameter settings

A message is displayed indicating that the request has been submitted.

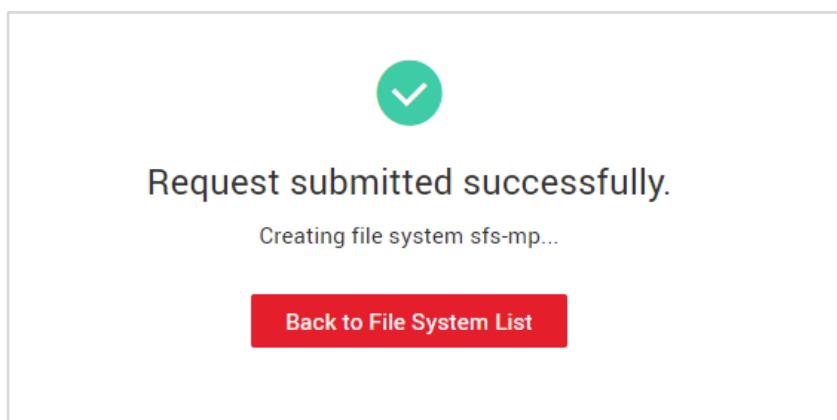


Figure 4-80 File system created

Go back to the SFS console and view the result.

| Name | AZ | Status | Type | Protocol Type | Available Capacity (G...) | Maximum Capacity (G...) | Mount Address | Operation |
|--------|-----|-----------|--------------------|---------------|---------------------------|-------------------------|--|---|
| sfs-mp | AZ1 | Available | SFS Capacity-Or... | NFS | 1.00 | 1.00 | sfs-nas01.ap-southeast-2a.myhuaweicloud.com/share-c343b993 | Resize Delete |

Figure 4-81 Viewing the file system

4.3.2.2 Mounting an SFS File System to a Linux ECS

Procedure

Go to the ECS console. Locate the row that contains the purchased ECS and click Remote Login.

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|--|-----|---------|--|---|----------------------------------|-----|---------------------------------------|
| ecs-windows 5e3be3fd-3ce0-44c2-90b4-e9ae72... | AZ1 | Running | 2 vCPUs 4GiB s3.large.2 Windows Server 2012 R2 Datacent | 159.138.235.195 (EIP) ... 192.168.0.98 (Private IP...) | Pay-per-use Created on: | -- | Remote Login More ▾ |
| ecs-linux aeca144-8e85-4c9c-84d6-3742fe6... | AZ1 | Running | 1 vCPUs 1GiB s3.small.1 CentOS 7.6 64-bit | 94.74.118.115 (EIP) 5 ... 192.168.0.53 (Private IP...) | Pay-per-use Created on: | - | Remote Login More ▾ |

Figure 4-82 Remotely logging in to the ECS

Log in the ECS as user root.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.15.2.el7.x86_64 on an x86_64

ecs-linux login: root_
Password:

      Welcome to Huawei Cloud Service

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

Figure 4-83 Logging in to Linux

Run the following command to check whether the NFS software package has been installed in the operating system (generally available in the operating system):

```
rpm -qa |grep nfs
```

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

Figure 4-84 Checking whether NFS software package is installed

If information similar to the preceding figure is returned, the NFS software package has been installed. The command output varies with the operating system.

If no command output is returned, the NFS software package is not installed. Run the respective command to install the NFS software package. In this exercise, CentOS 7.6 bit is used as an example.

- In CentOS, Red Hat, EulerOS, Fedora, or Oracle Enterprise Linux, run the following command:

```
sudo yum -y install nfs-utils
```

```
Installed:
  nfs-utils.x86_64 1:1.3.0-0.66.el7

Dependency Installed:
  gsproxy.x86_64 0:0.7.0-28.el7
  libcollection.x86_64 0:0.7.0-32.el7
  libnfsidmap.x86_64 0:0.25-19.el7
  libtirpc.x86_64 0:0.2.4-0.16.el7
  quota-nts.noarch 1:4.01-19.el7

  keyutils.x86_64 0:1.5.8-3.el7
  libevent.x86_64 0:2.0.21-4.el7
  libpath_utils.x86_64 0:0.2.1-32.el7
  libverto-libevent.x86_64 0:0.2.5-4.el7
  rpcbind.x86_64 0:0.2.0-49.el7

  libbasicobjects.x86_64 0:0.1.1-32.el7
  libini_config.x86_64 0:1.3.1-32.el7
  libref_array.x86_64 0:0.1.5-32.el7
  quota.x86_64 1:4.01-19.el7
  tcp_wrappers.x86_64 0:7.6-77.el7

Complete!
```

Figure 4-85 Installing the NFS software package

- In Debian or Ubuntu, run the following command:

```
sudo apt-get install nfs-commonSUSE
```

- In OpenSUSE, run the following command:

```
zypper install nfs-client
```

Run the following command to install the bind-utils software package:

```
yum install bind-utils
```

```
Installed:  
bind-utils.x86_64 32:9.11.4-16.P2.el7_8.6  
  
Dependency Installed:  
bind-libs.x86_64 32:9.11.4-16.P2.el7_8.6  
  
Dependency Updated:  
bind-libs-lite.x86_64 32:9.11.4-16.P2.el7_8.6  
bind-license.noarch 32:9.11.4-16.P2.el7_8.6  
  
Complete!
```

Figure 4-86 Installing the NFS software package

Log in to the SFS console, click the file system to be mounted, and view the mount address.

| Name | AZ | Status | Type | Protocol Type | Available Capacity (G...) | Maximum Capacity (G...) | Mount Address | Operation |
|--------|-----|-----------|--------------------|---------------|---------------------------|-------------------------|---|---|
| sfs-mp | AZ1 | Available | SFS Capacity-Or... | NFS | 1.00 | 1.00 | sfs-nas01.ap-southeast-2a.myhuaweicloud.com:/share-c343b993 | Resize Delete |

Figure 4-87 Viewing the mount address

Note that information in the red box is the domain name of the file system.

Run the following command to check whether the file system domain name can be resolved into corresponding IP addresses: (Replace the mount address with the one you have obtained.)

```
nslookup sfs-nas01.ap-southeast-2a.myhuaweicloud.com
```

If information similar to the following is displayed, IP addresses have been mapped to the file system domain name.

```
[root@ecs-linux ~]# nslookup sfs-nas01.ap-southeast-2a.myhuaweicloud.com
Server: 100.125.1.250
Address: 100.125.1.250#53

Non-authoritative answer:
Name: sfs-nas01.ap-southeast-2a.myhuaweicloud.com
Address: 100.125.96.34
Name: sfs-nas01.ap-southeast-2a.myhuaweicloud.com
Address: 100.125.96.42
Name: sfs-nas01.ap-southeast-2a.myhuaweicloud.com
Address: 100.125.96.38
Name: sfs-nas01.ap-southeast-2a.myhuaweicloud.com
Address: 100.125.96.41
Name: sfs-nas01.ap-southeast-2a.myhuaweicloud.com
Address: 100.125.96.43
Name: sfs-nas01.ap-southeast-2a.myhuaweicloud.com
Address: 100.125.96.47
Name: sfs-nas01.ap-southeast-2a.myhuaweicloud.com
Address: 100.125.96.49
Name: sfs-nas01.ap-southeast-2a.myhuaweicloud.com
Address: 100.125.96.35
```

Figure 4-88 Resolving the mount address

Run the **#mkdir /local path** command to create a local directory for mounting the file system.

```
mkdir /localfolder
```

Run the following command to mount the file system on the local path:

```
mount -t nfs -o vers=3,timeo=600,nolock Mount address of the SFS file system /local path
```

In this example, run the following command:

```
mount -t nfs -o vers=3, timeo=600, nolock nslookup sfs-nas01.ap-southeast-2a.myhuaweicloud.com:/share-c343b993 /localfolder
```

```
[root@ecs-linux ~]# mount -t nfs -o vers=3,timeo=600,nolock sfs-nas01.ap-southeast-2a.myhuaweicloud.com:/share-c343b993 /local
lder
[root@ecs-linux ~]# _
```

Figure 4-89 Mounting the file system in the Linux

Run the following command to view the mounted file system:

```
mount -l
```

```
[root@ecs-linux ~]# mount -l
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
devtmpfs on /dev type devtmpfs (rw,nosuid,size=496768k,nr_inodes=124192,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=008)
tmpfs on /run type tmpfs (rw,nosuid,nodev,mode=755)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/usr/lib/systemd/systemd-cgr
ps-agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/net_cls.net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_prio,net_cls)
cgroup on /sys/fs/cgroup/cpu.cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpuacct,cpu)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
configfs on /sys/kernel/config type configfs (rw,relatime)
/dev/vda1 on / type ext4 (rw,relatime,data=ordered)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=26,pgroup=1,timeo=8,minproto=5,maxproto=5,direct,pipe_ino=18
9)
mqueue on /dev/mqueue type mqueue (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
hugepages on /dev/hugepages type hugepages (rw,relatime)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=101432k,mode=700)
sfs-nas01.ap-southeast-2a.myhuaweicloud.com:/share-c343b993 on /localfolder type nfs (rw,relatime,vers=3,rsize=1048576,wsize=1
8576,namlen=255,hard,nolock,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=100.125.96.39,mountvers=3,mountport=2050,mountprot
ldp_local_lock_all,addr=100.125.96.39)
[root@ecs-linux ~]#
```

Figure 4-90 Viewing the mounted file system

Run the following command to edit the /etc/fstab file:

```
vi /etc/fstab
```

Press “i” to enter editing mode. At the end of the file, add the file system information. In this example, add the following content:

```
sfs-nas01.ap-southeast-2a.myhuaweicloud.com:/share-c343b993 /localfolder nfs vers=3, timeo=600, nolock o o
```

Press “Esc”, enter “:wq”, and press Enter to save and exit.

Replace **Mount address** and **/localfolder** with those used in your environment.

Run the following command to view the changes of fstab:

```
cat /etc/fstab
```

```
# 
# /etc/fstab
# Created by anaconda on [REDACTED]
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=1cf0b662-ebd1-44a2-bbd2-0a6e58aec5fa /          ext4    defaults        1 1
sfs-nas01.ap-southeast-2a.myhuaweicloud.com:/share-c343b993 /localfolder nfs vers=3, timeo=600, nolock 0 0
[REDACTED]
```

Figure 4-91 Setting automatic mounting

Restart the ECS.

```
reboot
```

Log in to the system and run the following command to view the mounted file system:

```
mount -l
```

```
sfs-nas01.ap-southeast-2a.myhuaweicloud.com:/share-c343b993 on /localfolder type nfs (rw,relatime,vers=3,rsize=1048576,wsiz=1048576,namlen=255,hard,noexec,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=100.125.96.37,mountvers=3,mountport=2050,mountproto=udp,local_lock=all,addr=100.125.96.37)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=101432k,mode=700)
[root@ecs-linux ~]#
```

Figure 4-92 Viewing the mounted file system

Create file new.

```
cd /localfolder
vim new
```

Press "i" to enter editing mode. Enter "Hello HuaweiCloud SFS", press "Esc", and enter ":wq" to exit editing mode and save the change.

```
Hello HuaweiCloud SFS
```

Figure 4-93 Creating the test file

Run the following command to view the file content:

```
cat /localfolder/new
```

```
[root@ecs-linux localfolder]# cat /localfolder/new
Hello HuaweiCloud SFS
[root@ecs-linux localfolder]#
```

Figure 4-94 Viewing the test file

Now that the file system has been mounted to the ECS and can be used.

4.3.2.3 Mounting an SFS File System to a Windows ECS

Logging In to a Windows ECS

Log in to the ECS console. Locate the row that contains the purchased Windows ECS and click Remote Login.

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|--|-----|---------|--|---|----------------------------------|-----|---|
| ecs-windows 5e3be3fd-3ce0-44c2-90b4-e9ae72... | AZ1 | Running | 2 vCPUs 4GiB s3.large.2 Windows Server 2012 R2 Datacent | 159.138.235.195 (EIP) ... 192.168.0.98 (Private IP...) | Pay-per-use Created on J..... | | Remote Login More ▾ |

Figure 4-95 Viewing the Windows ECS

Installing the NFS Client

Open Server Manager by clicking the icon in the lower left corner.

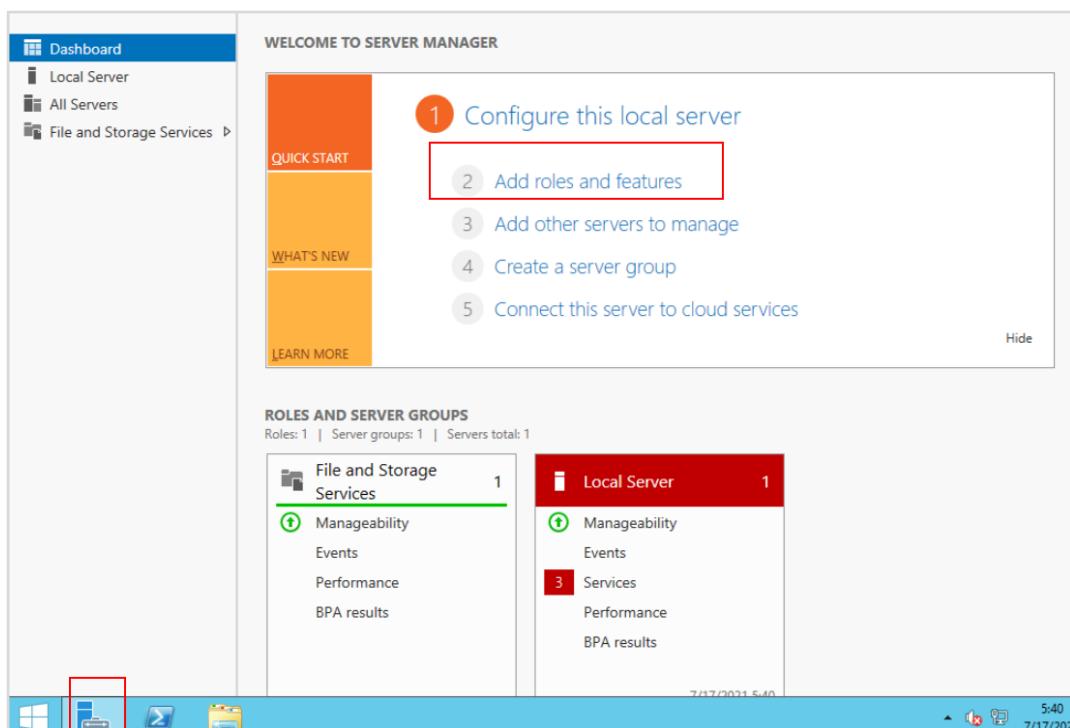


Figure 4-96 Opening Server Manager

Click Add Roles and Features and click Next for three consecutive times to go to the Server Roles page.

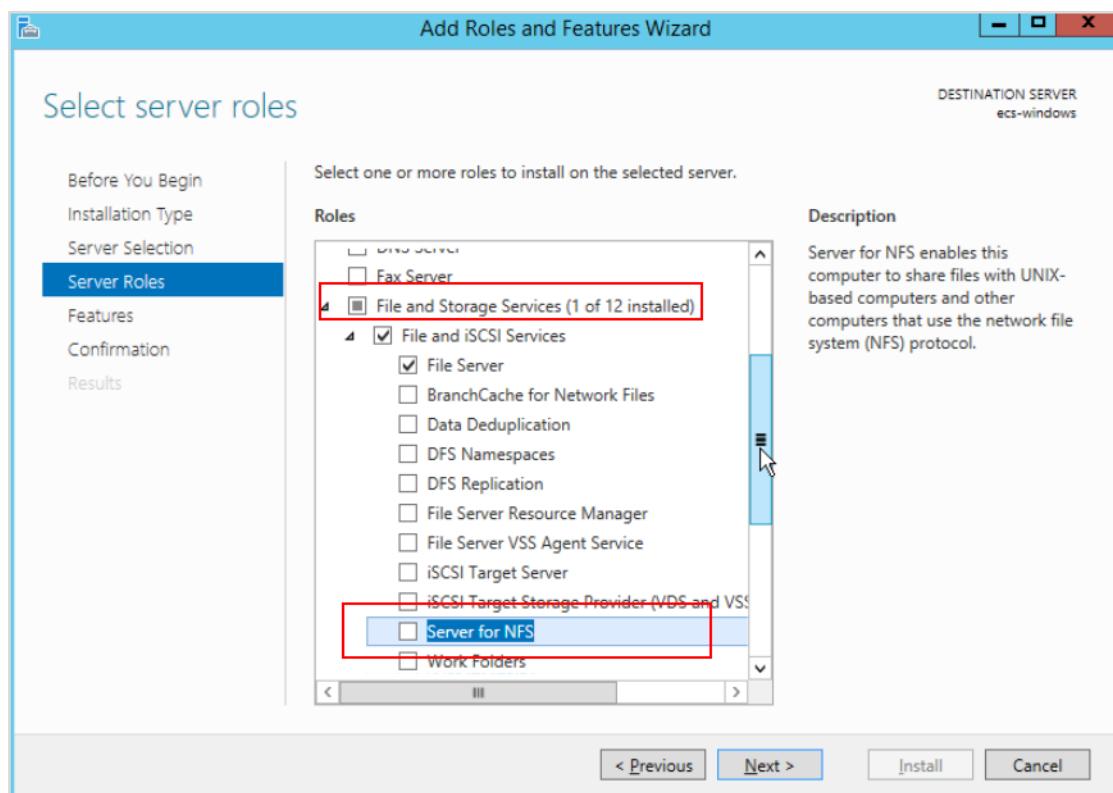


Figure 4-97 Selecting the server role

Under File and Storage Services, click Server for NFS. In the displayed window, click Add Features.

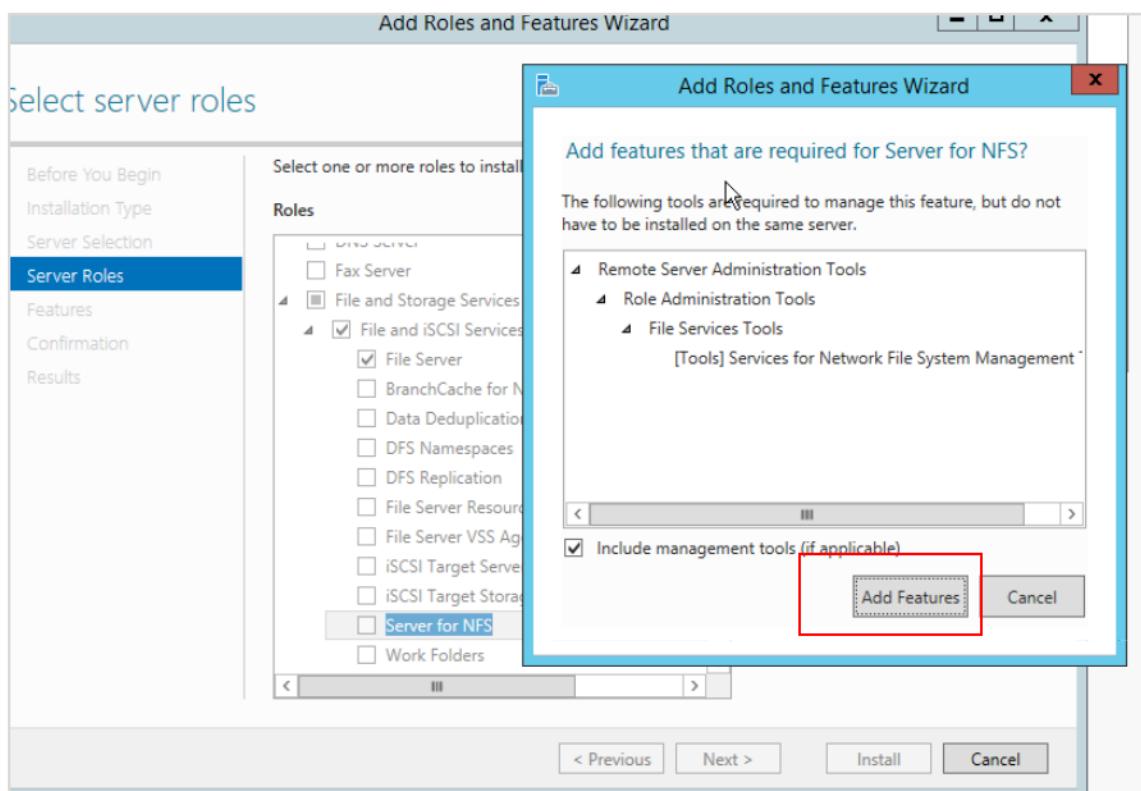


Figure 4-98 Clicking Server for NFS

Click Next. On the Features page, click Client for NFS.

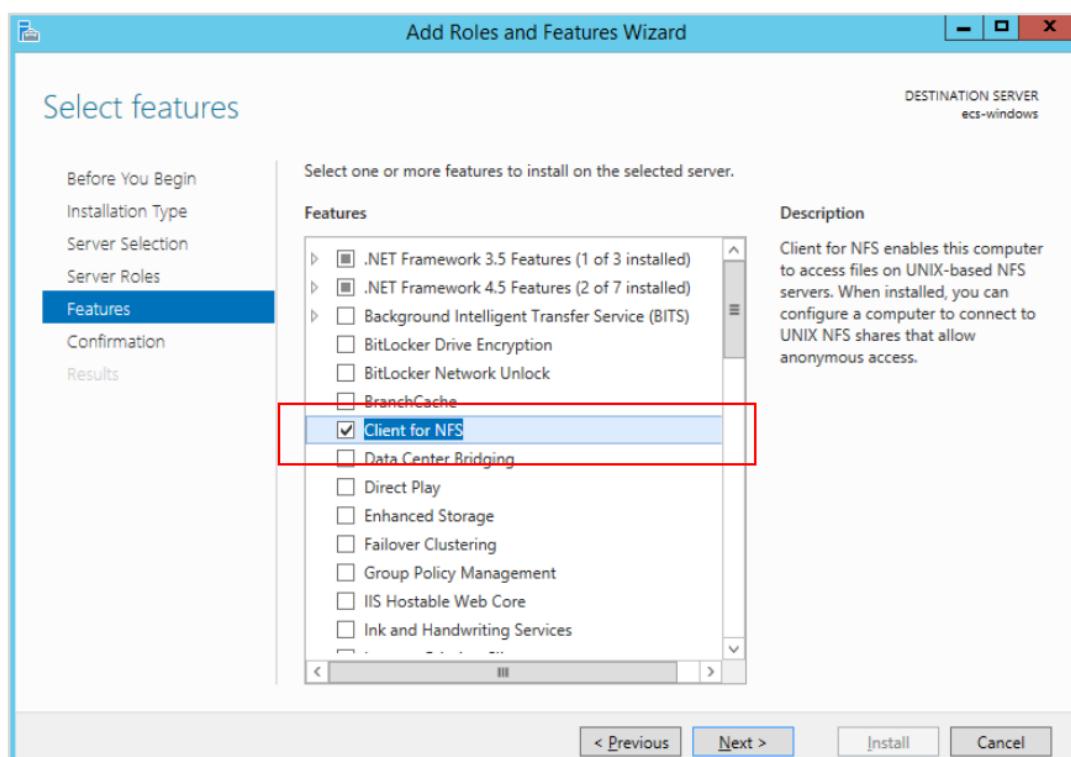


Figure 4-99 Selecting Client for NFS

Click Next to go to the Confirmation page.

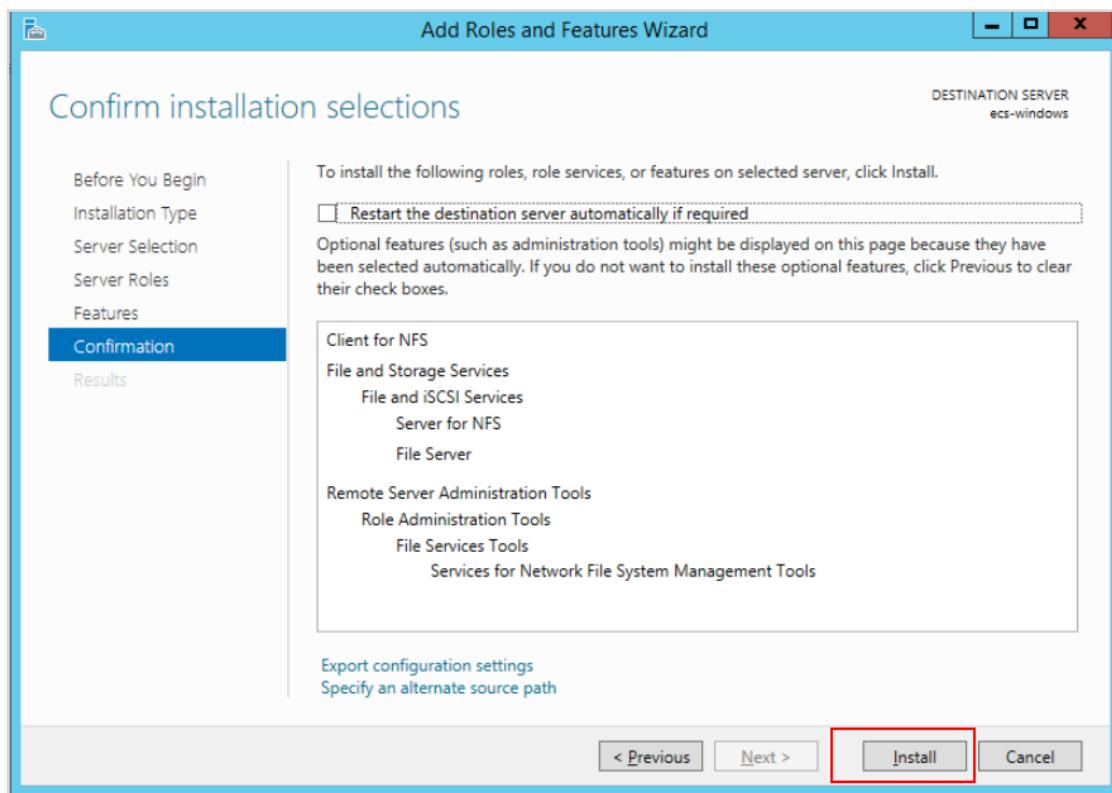


Figure 4-100 Confirmation

Click Install.

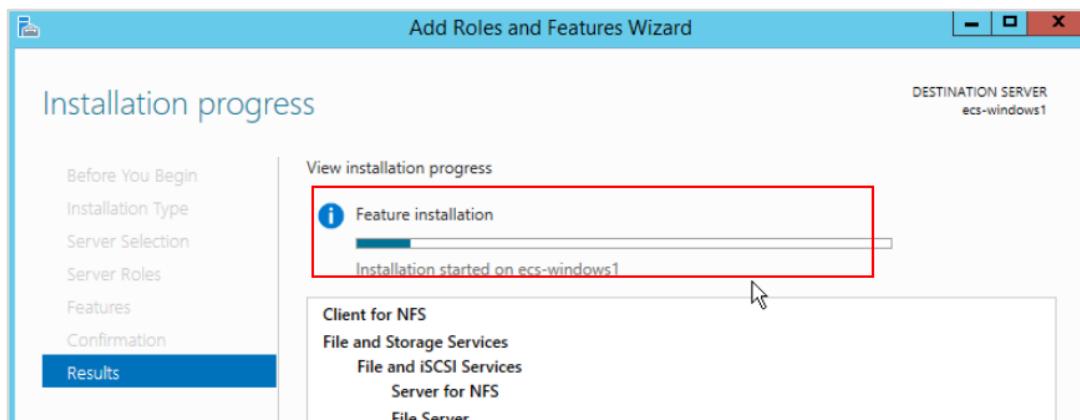


Figure 4-101 Installing

After the installation is complete, restart the client and log to the ECS again as prompted.

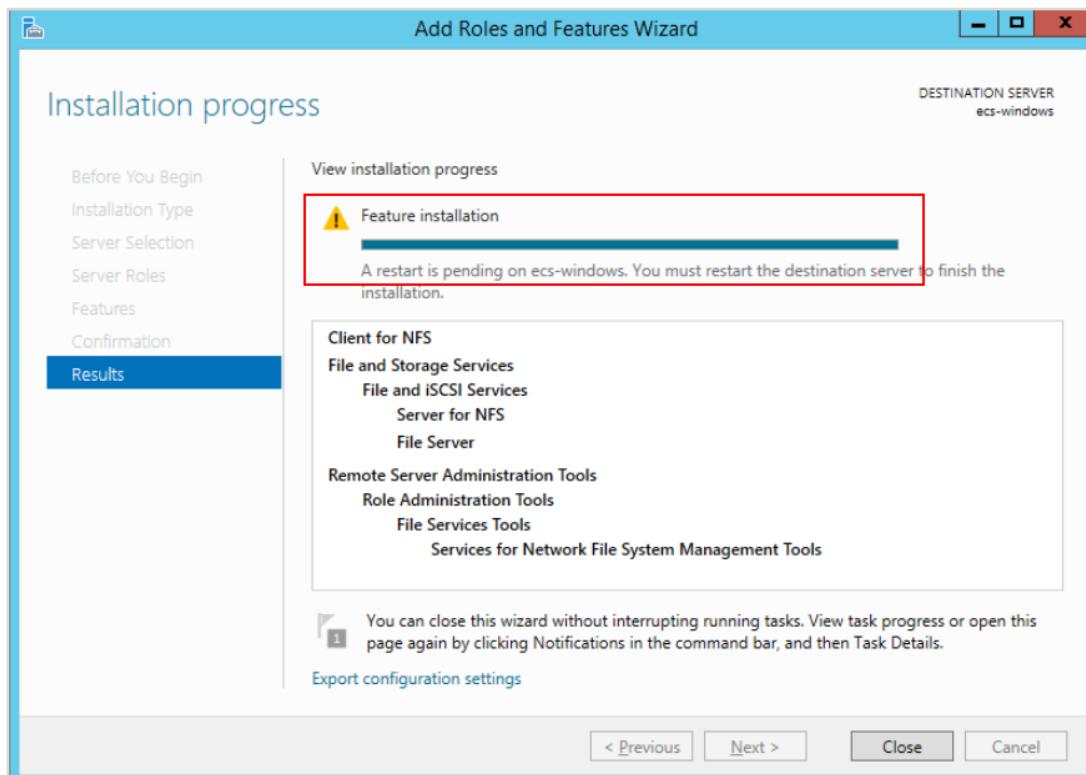


Figure 4-102 Installation completed

Mounting the File System

Open Control Panel and choose to view by category.



Figure 4-103 Control Panel

On the Control Panel, choose System and Security > Administrative Tools > Services for Network File System (NFS).

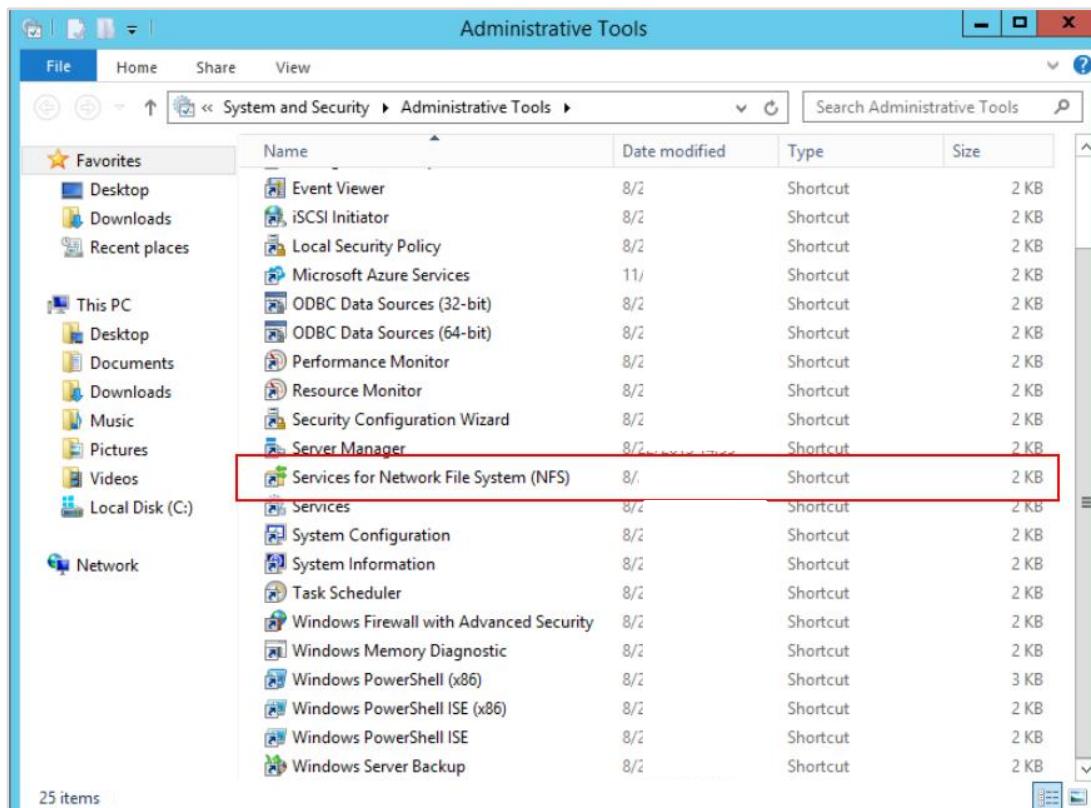


Figure 4-104 Selecting the NFS service

Right-click Client for NFS and choose Properties. In the displayed dialog box, change the transport protocol to TCP and select Use hard mounts as the default mount type.

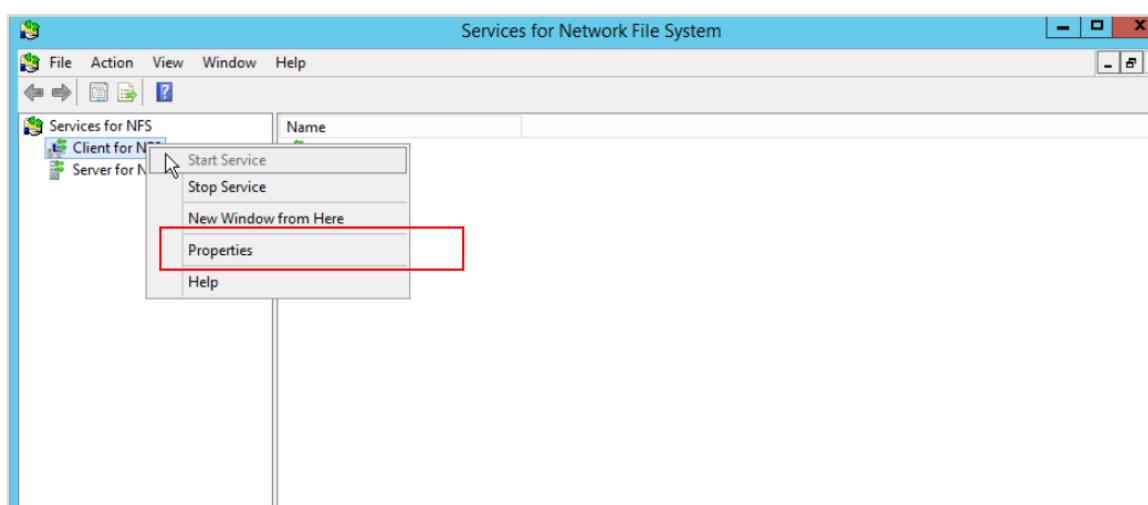


Figure 4-105 Opening Client for NFS Properties

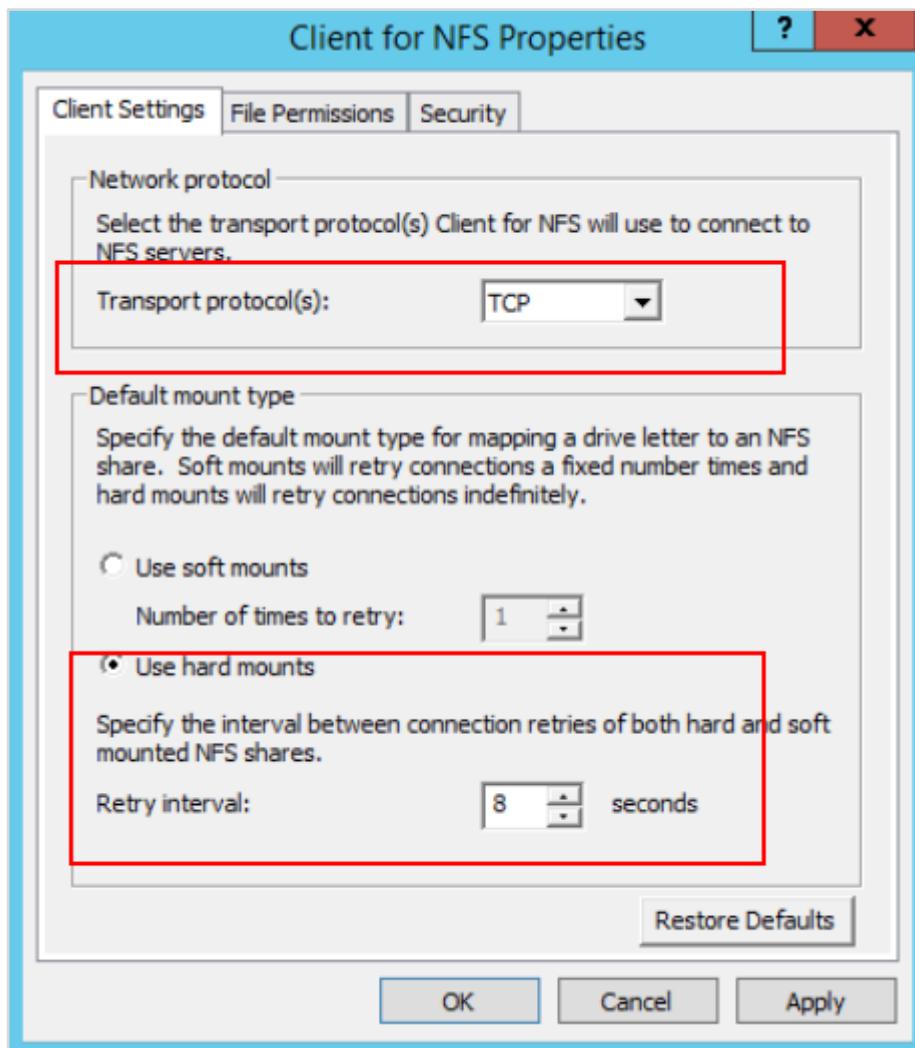


Figure 4-106 Setting properties

Run the following command in the Command Prompt of the Windows Server 2012 (X is the drive letter of the free disk):

For the SFS file system, run the following command:

```
mount -o nolock sfs-nas01.ap-southeast-2a.myhuaweicloud.com:/share-c343b993 X:
```

Note that `nolock sfs-nas01.ap-southeast-2a.myhuaweicloud.com:/share-c343b993` is the mount address obtained from the SFS console. (The mount address varies with the file system. Replace this mount address with your file system's mount address. Do not copy the address in this example.)

```
C:\Users\Administrator>mount -o nolock sfs-nas01.ap-southeast-2a.myhuaweicloud.com:/share-c343b993 X:  
X: is now successfully connected to sfs-nas01.ap-southeast-2a.myhuaweicloud.com:  
/share-c343b993  
The command completed successfully.  
C:\Users\Administrator>
```

Figure 4-107 SFS file system mounted

Verification

On the Windows ECS, open This PC to check that the mounted file system is available.

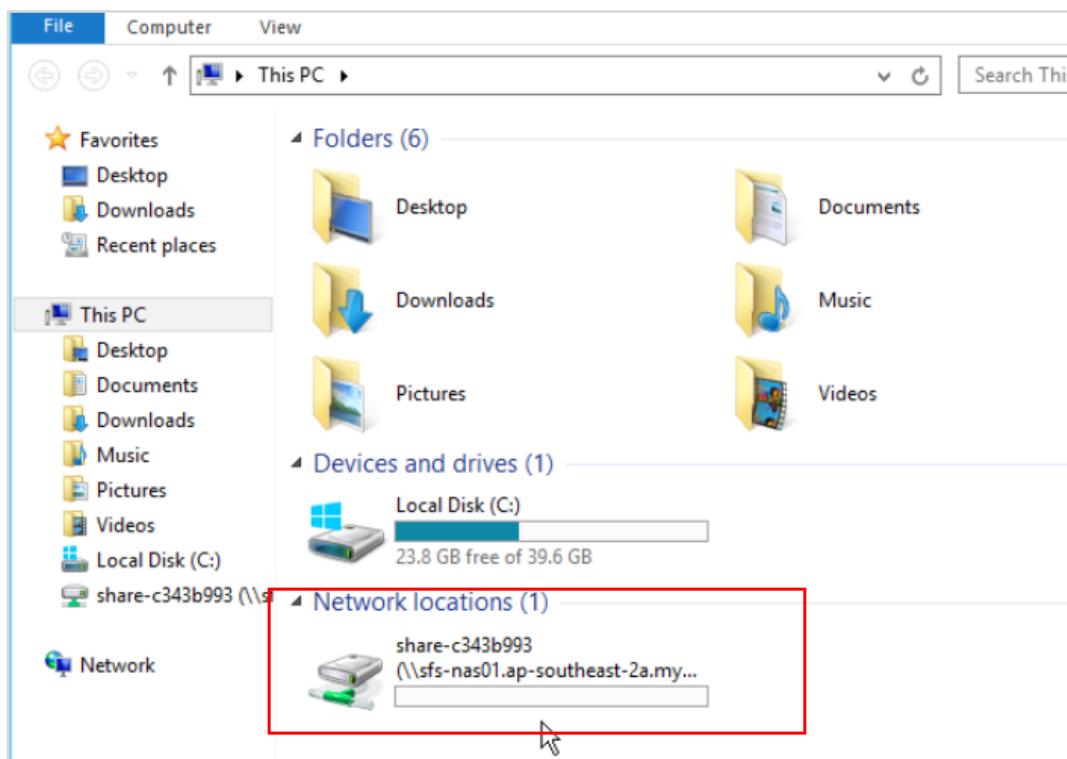


Figure 4-108 SFS file system displayed under Network Locations

Access share-c343b993 and check that file new exists. This file is created in the file system from ECS ecs-linux, indicating that the SFS file system can be shared among servers.

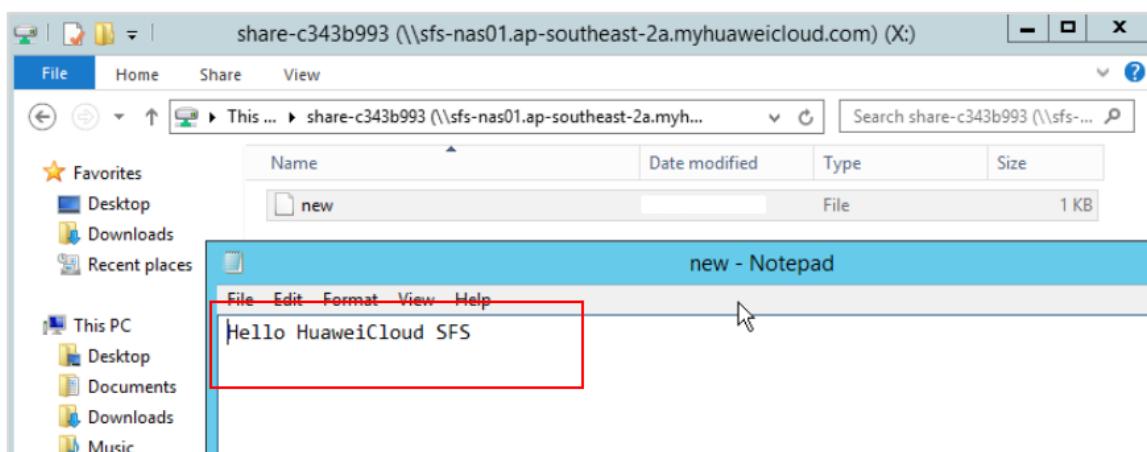


Figure 4-109 Verification succeeded

4.3.3 Deleting Resources

4.3.3.1 Unmounting a File System (Linux)

Log in to ECS ecs-linux and run the following command to unmount the file system:

```
umount /localfolder
```

```
[root@ecs-linux ~]# umount /localfolder
```

Figure 4-110 Unmounting the file system

Run the following command to check whether the file system has been unmounted:

```
mount -l
```

4.3.3.2 Unmounting a File System (Windows)

Log in to ECS ecs-windows. Open This PC, right-click the file system to be unmounted and choose Disconnect from the shortcut menu. The file system has been unmounted after it disappears from This PC.

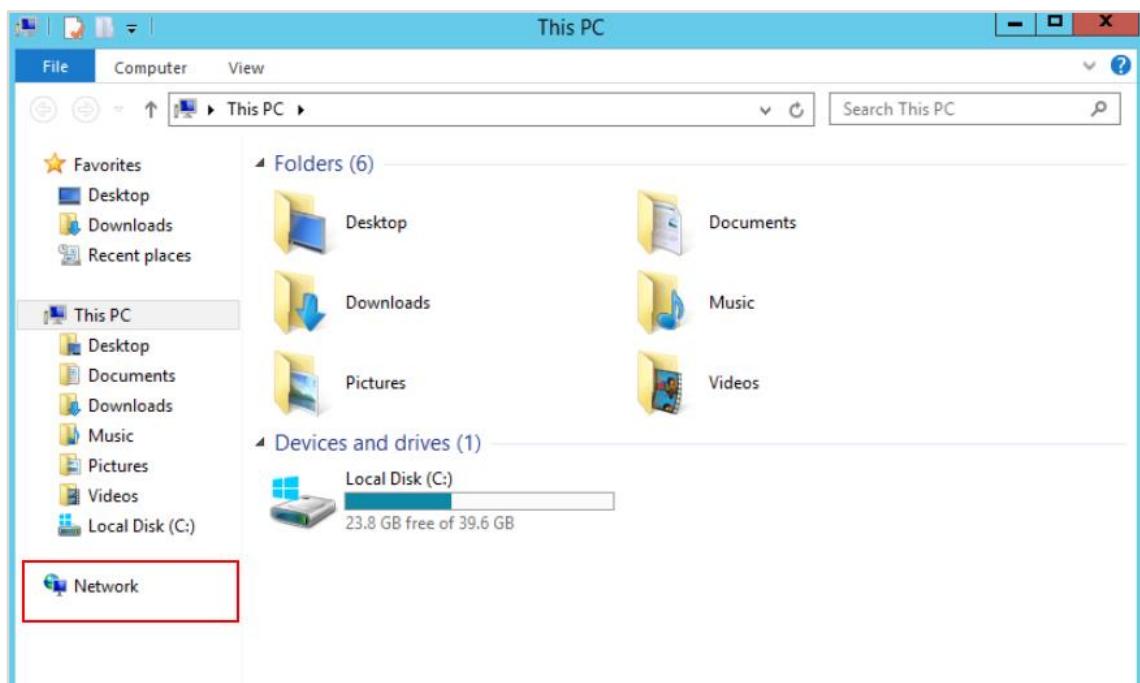


Figure 4-111 File system unmounted

4.3.3.3 Deleting a File System

On the SFS console, locate the row that contains the file system and click Delete in the Operation column.

| Name | AZ | Status | Type | Protocol Type | Available Capacity (G...) | Maximum Capacity (G...) | Mount Address | Operation |
|--------|-----|-----------|--------------------|---------------|---------------------------|-------------------------|--|---|
| sfs-mp | AZ1 | Available | SFS Capacity-Or... | NFS | 1.00 | 1.00 | sfs-nas01.ap-southeast-2a.myhuaweicloud.com/share-c343b993 | Resize Delete |

Figure 4-112 Delete File System

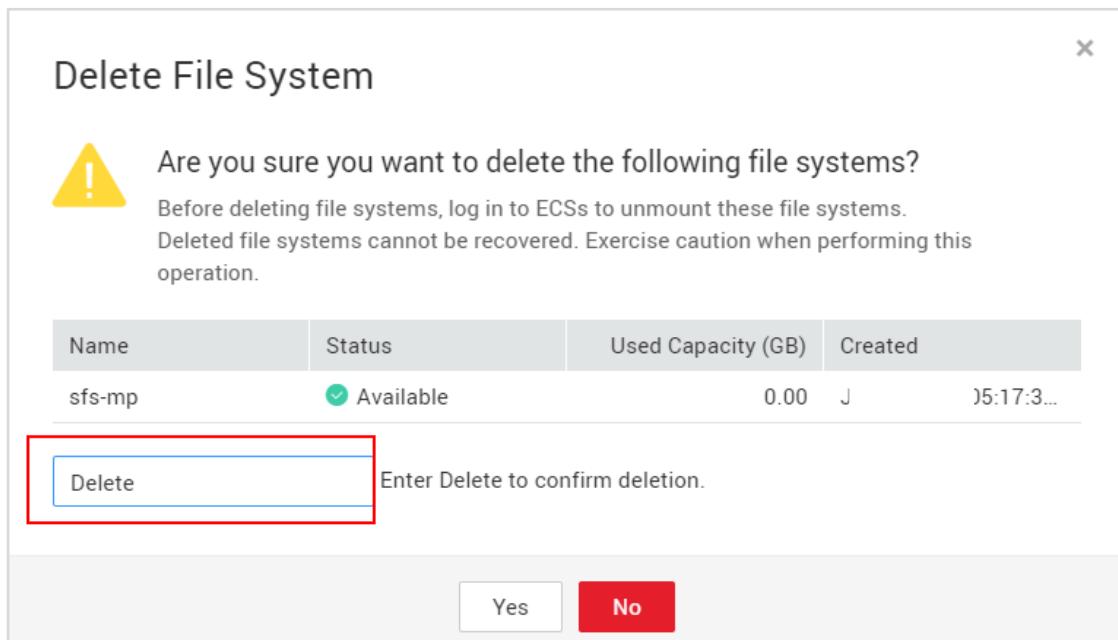


Figure 4-113 Delete File System

5 O&M Services

5.1 Introduction

5.1.1 About This Exercise

In this exercise, you will:

- View the CTS console.
- Use LTS to check ECS logs.
- Run commands to increase ECS CPU usage and check for a generated alarm.

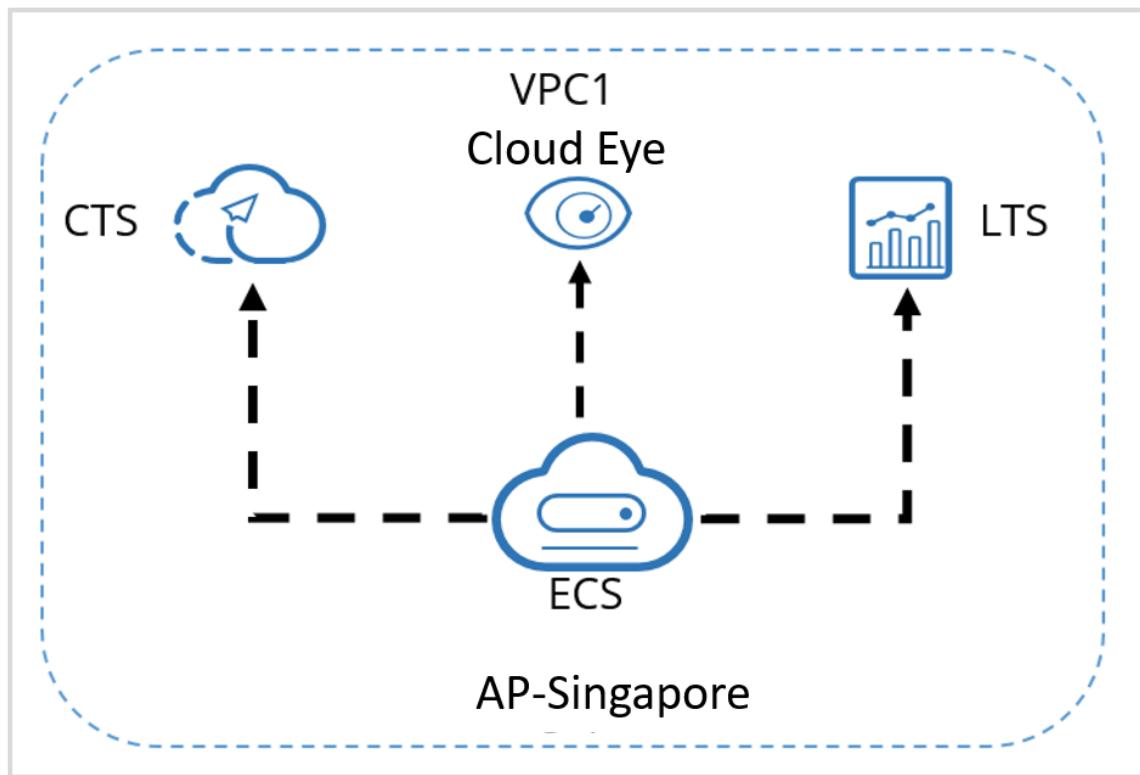


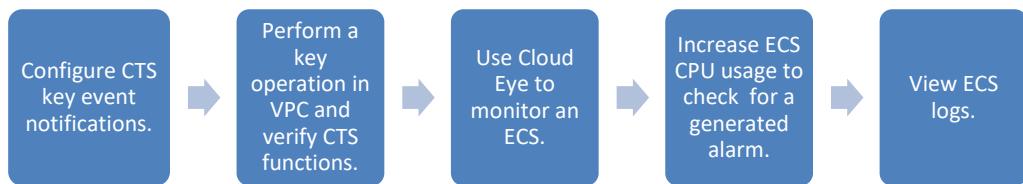
Figure 5-1 Topology

5.1.2 Objectives

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

- Use CTS.
- Configure and use Cloud Eye.
- View and search for logs in LTS.

5.2 Tasks



5.2.1 Configuring CTS Key Event Notifications

5.2.1.1 Enabling a Tracker

Log in to the management console.

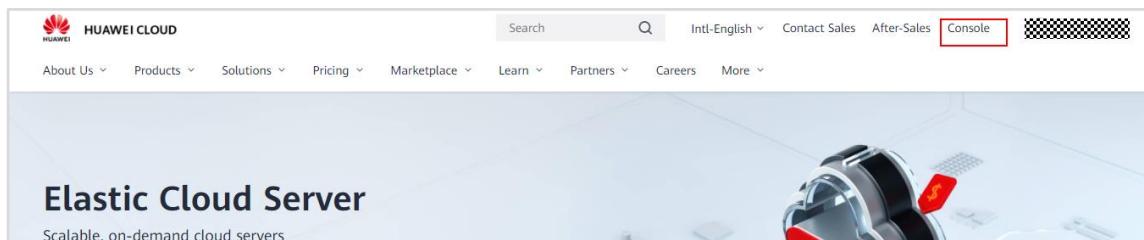


Figure 5-2 Accessing the console

Search for Cloud Trace Service to access the CTS console on **LA-SaoPaulo1 region.**

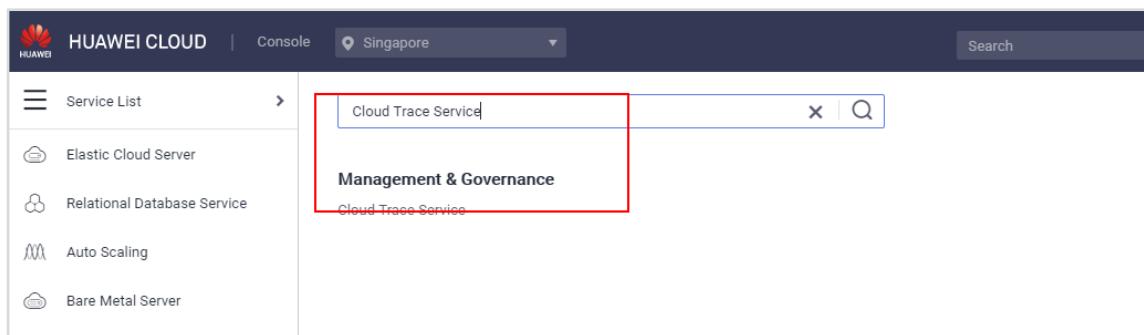


Figure 5-3 Accessing CTS

Enable and authorize CTS. The CTS tracker created identifies and associates itself with all cloud services you are using.

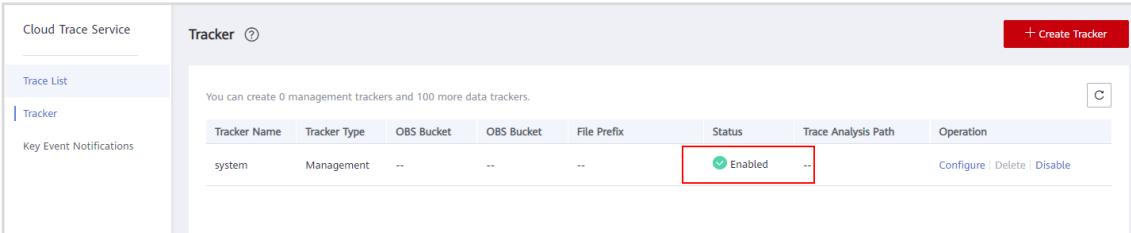
CTS is requesting permissions to access the following cloud resources:

- Object Storage Service (OBS)
CTS will be able to synchronize traces to OBS for long-term storage.
- Simple Message Notification (SMN)
Notifications of key events can be sent to subscribers in real time.
- Key Management Service (KMS)
Trace files stored in OBS can be encrypted.

Once CTS is authorized, an agency named `cts_admin_trust` will be created on [Identity and Access Management](#). View the [agency list](#) for details. CTS will also begin to track the operations and changes on all cloud resources in your account and keep the traces for 7 days. To store the traces for a longer time, you can transfer them to OBS by configuring the tracker.

[Enable and Authorize](#)

If the tracker status is Enabled, the tracker is running.



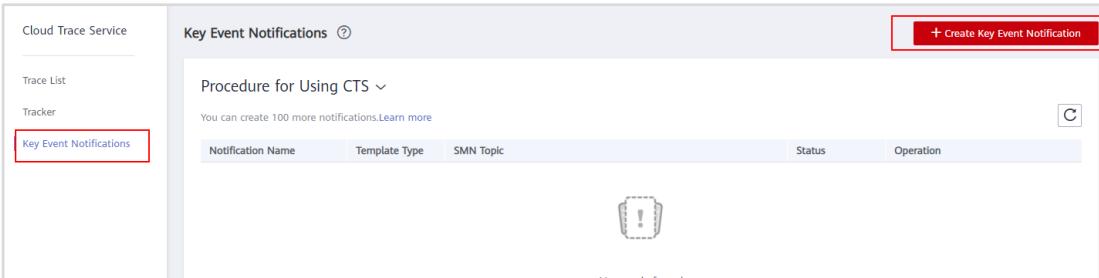
The screenshot shows the Cloud Trace Service interface with the 'Tracker' tab selected. A table lists one tracker entry:

| Tracker Name | Tracker Type | OBS Bucket | OBS Bucket | File Prefix | Status | Trace Analysis Path | Operation |
|--------------|--------------|------------|------------|-------------|--|---------------------|--|
| system | Management | -- | -- | -- | Enabled | -- | Configure Delete Disable |

Figure 5-4 Viewing the default tracker

5.2.1.2 Configuring Key Event Notifications

Configure key event notifications so you can be notified by SMS or email of specific operations. On the CTS console, choose Key Event Notifications in the navigation pane and click Create Key Event Notification in the upper right.

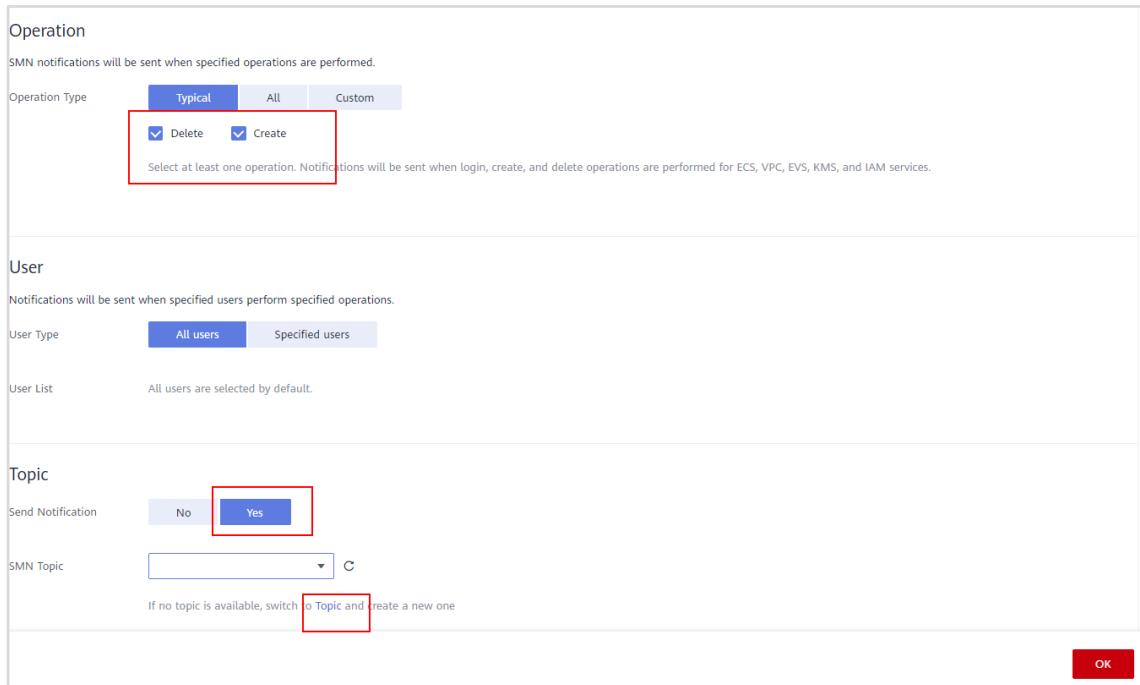


The screenshot shows the Cloud Trace Service interface with the 'Key Event Notifications' tab selected. A table is shown with one row, but it is empty. At the bottom, a message says 'No result found.'

Figure 5-5 Creating a key event notification

Configure notification parameters.

- **Notification Name:** user-defined
- **Operation Type:** Typical
- **User Type:** All users
- **Send Notification:** Yes



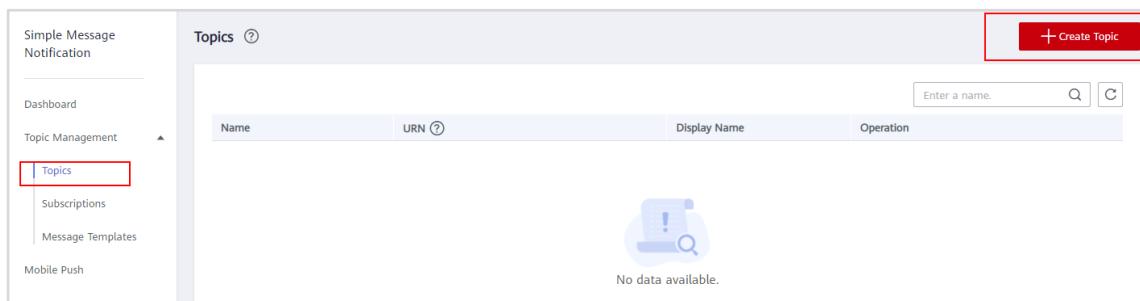
The screenshot shows the configuration interface for a notification. It includes three main sections: Operation, User, and Topic.

- Operation:** SMN notifications will be sent when specified operations are performed. The "Operation Type" is set to "Typical". Under "Operations", "Delete" and "Create" are selected, both highlighted with a red box. A note below says: "Select at least one operation. Notifications will be sent when login, create, and delete operations are performed for ECS, VPC, EVS, KMS, and IAM services."
- User:** Notifications will be sent when specified users perform specified operations. The "User Type" is set to "All users".
- Topic:** Send Notification is set to "Yes". The "SMN Topic" dropdown is empty and highlighted with a red box. A note below says: "If no topic is available, switch to Topic and create a new one."

An "OK" button is located at the bottom right of the form.

Figure 5-6 Configuring the notification

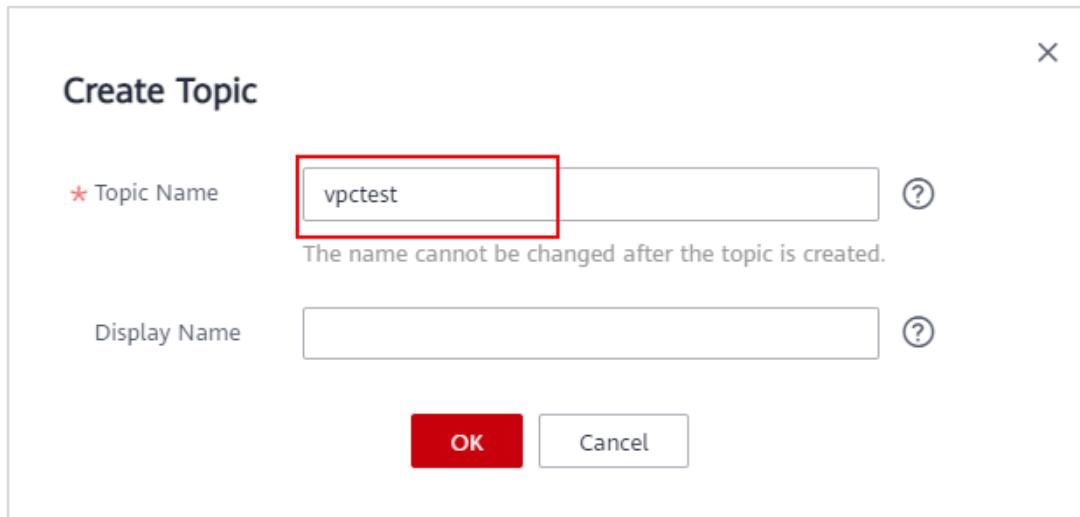
Simple Message Notification (SMN) pushes SMS, email, or app messages. A topic is used to publish or subscribe to messages. To create a topic, access the SMN console, choose Topic Management > Topics in the navigation pane, and click Create Topic in the upper right.



The screenshot shows the SMN console's Topics page. The left sidebar has a "Topic Management" section with "Topics" selected, highlighted with a red box. The main area displays a table with columns: Name, URN, Display Name, and Operation. A search bar at the top right allows entering a name, with a magnifying glass icon and a clear button. A "Create Topic" button is located in the top right corner of the main area. A note at the bottom says: "No data available."

Figure 5-7 Creating a topic

Enter a topic name and click OK.



Create Topic

* Topic Name (?)

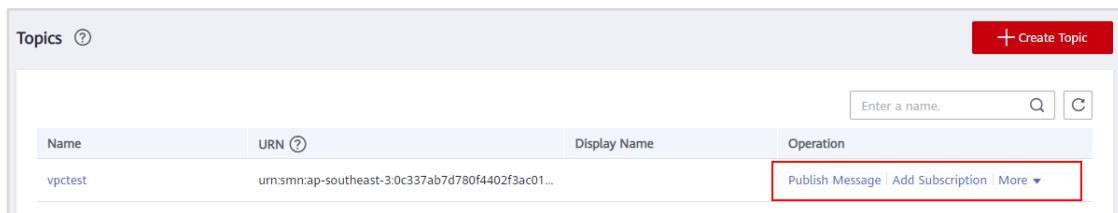
The name cannot be changed after the topic is created.

Display Name (?)

OK **Cancel**

Figure 5-8 Configuring the topic

Click Add Subscription to add a subscription for the created topic.

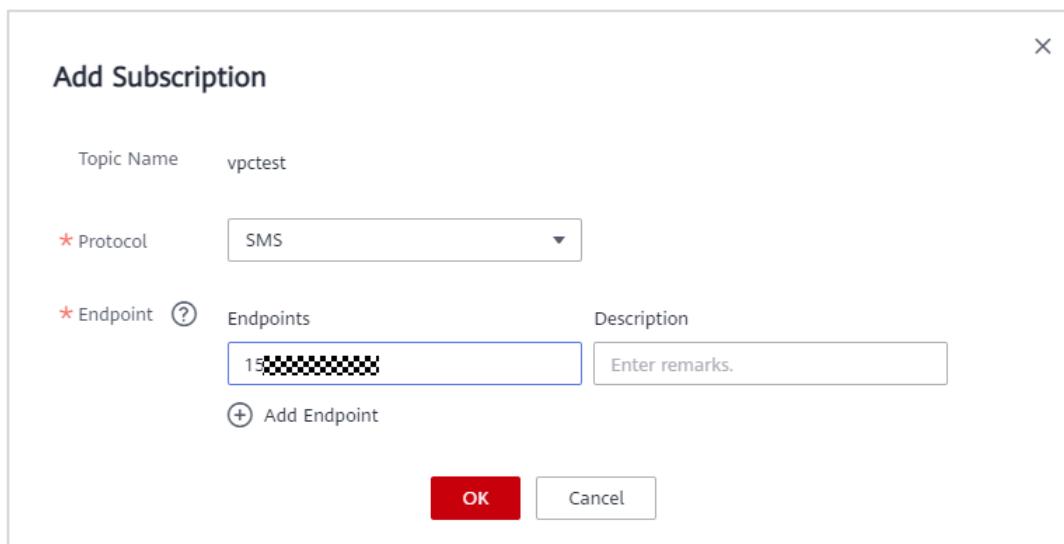


Topics (?) + Create Topic

| Name | URN (?) | Display Name | Operation |
|---------|---|--------------|---|
| vpctest | urn:smn:ap-southeast-3:0c337ab7d780f4402f3ac01... | | Publish Message Add Subscription More |

Figure 5-9 Adding a subscription

Select SMS for Protocol, enter your mobile number (for example: +5511998765432), and click OK.



Add Subscription

Topic Name vpctest

* Protocol

* Endpoint (?)

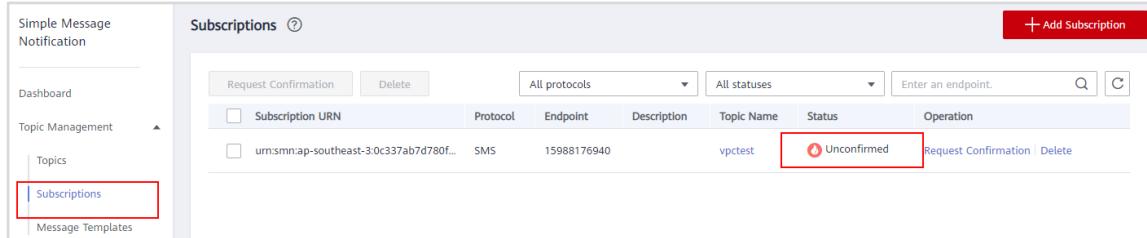
| Endpoints | Description |
|-----------|----------------|
| 15XXXXXX | Enter remarks. |

+ Add Endpoint

OK **Cancel**

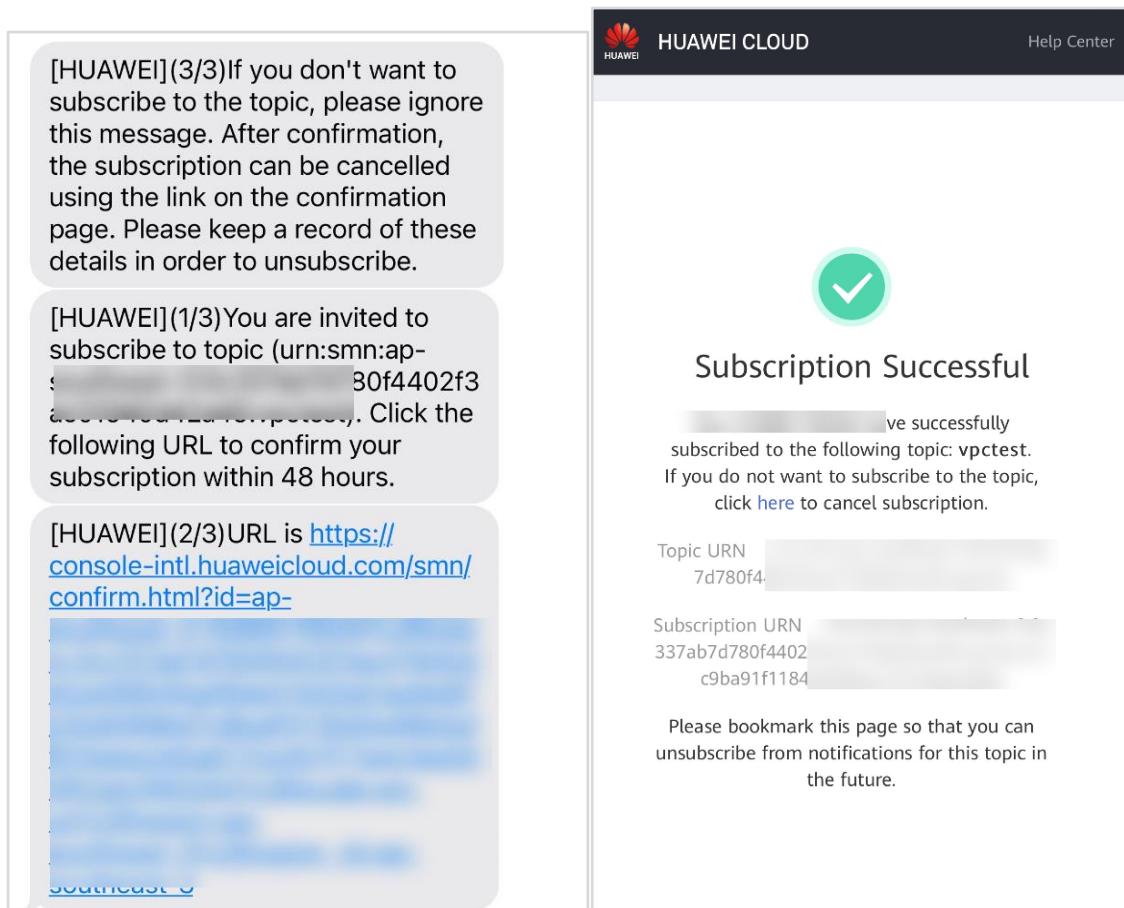
Figure 5-10 Configuring a subscription

Choose Subscriptions in the navigation pane and see that the subscription status is Unconfirmed. You will receive an SMS from HUAWEI CLOUD. Click the link in the message to confirm the subscription, and you will receive an SMS of successful subscription.



| Subscription URN | Protocol | Endpoint | Description | Topic Name | Status | Operation |
|---|----------|-------------|-------------|------------|-------------|---|
| urn:smn:ap-southeast-3:0c337ab7d780f4402f3c9ba91f1184 | SMS | 15988176940 | vpctest | vpctest | Unconfirmed | Request Confirmation Delete |

Figure 5-11 Viewing the subscription



[HUAWEI](3/3) If you don't want to subscribe to the topic, please ignore this message. After confirmation, the subscription can be cancelled using the link on the confirmation page. Please keep a record of these details in order to unsubscribe.

[HUAWEI](1/3) You are invited to subscribe to topic (urn:smn:ap-southeast-3:0c337ab7d780f4402f3c9ba91f1184). Click the following URL to confirm your subscription within 48 hours.

[HUAWEI](2/3) URL is <https://console-intl.huaweicloud.com/smn/confirm.html?id=ap-337ab7d780f4402f3c9ba91f1184>

HUAWEI CLOUD Help Center

Subscription Successful

You have successfully subscribed to the following topic: vpctest. If you do not want to subscribe to the topic, click [here](#) to cancel subscription.

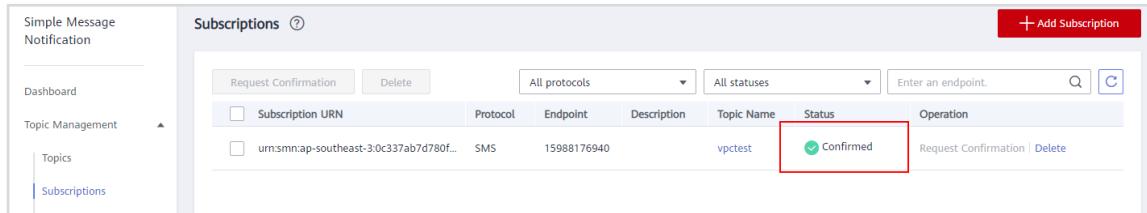
Topic URN 7d780f4402f3c9ba91f1184

Subscription URN 337ab7d780f4402f3c9ba91f1184

Please bookmark this page so that you can unsubscribe from notifications for this topic in the future.

Figure 5-12 Successful subscription

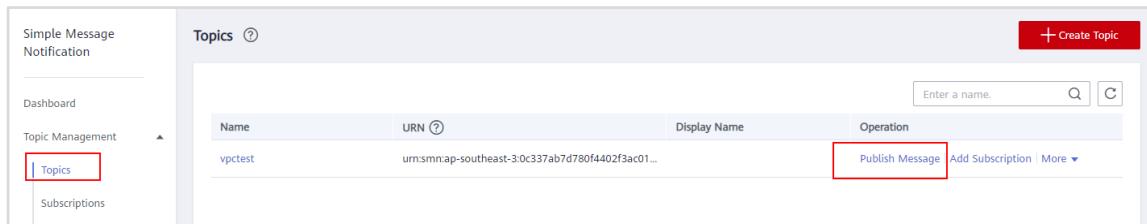
On the Subscriptions page, if the subscription status has changed to Confirmed, subscription was successful.



The screenshot shows the 'Subscriptions' page of the HUAWEI CLOUD Simple Message Notification interface. On the left sidebar, 'Topics' is selected under 'Topic Management'. The main area displays a table of subscriptions. One row is highlighted with a red box around the 'Status' column, which shows 'Confirmed' with a green checkmark. Other columns include 'Subscription URN', 'Protocol', 'Endpoint', 'Description', and 'Topic Name'. Buttons for 'Request Confirmation', 'Delete', and 'Operation' are also visible.

Figure 5-13 Successful subscription

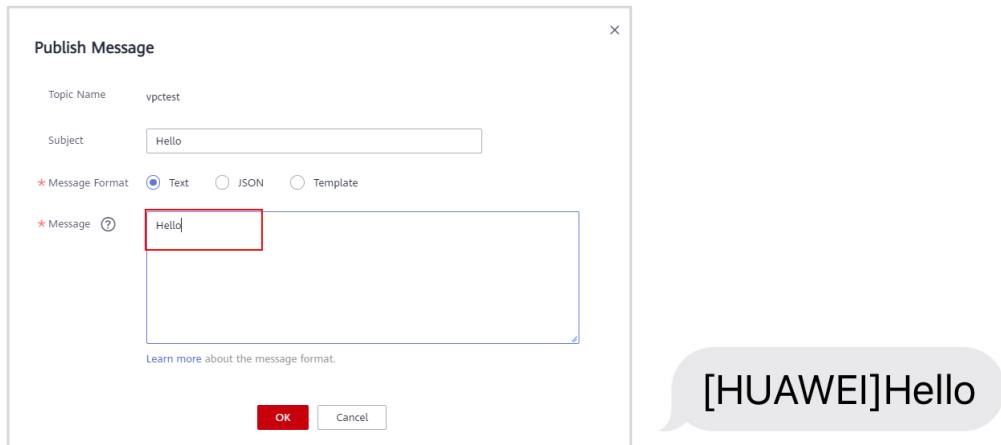
On the Topics page, click Publish Message to publish a message and check that you receive it.



The screenshot shows the 'Topics' page. The left sidebar has 'Topics' selected under 'Topic Management'. The main area shows a table with one topic entry: 'vpcitest' with URN 'urn:ssmn:ap-southeast-3:0c337ab7d780f4402f3ac01...'. A red box highlights the 'Publish Message' button in the 'Operation' column. Other buttons include 'Add Subscription' and 'More'.

Figure 5-14 Publishing a message

Enter Subject, select Text for Message Format, enter Hello in Message, and click OK. If you receive the Hello SMS message from HUAWEI CLOUD, the subscription is verified.

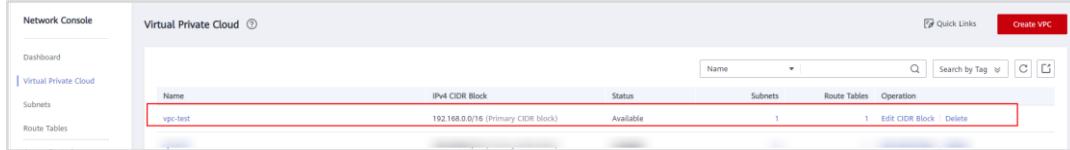


The screenshot shows the 'Publish Message' dialog box. It has fields for 'Topic Name' (vpcitest), 'Subject' (Hello), and 'Message'. Under 'Message Format', 'Text' is selected. The 'Message' field contains 'Hello'. A red box highlights the 'Message' input field. At the bottom are 'OK' and 'Cancel' buttons. To the right of the dialog, a speech bubble contains the text '[HUAWEI]Hello'.

Figure 5-15 Configuring the message

5.2.2 Performing a key operation in VPC and verifying CTS functions

Create a VPC in the **LA-SaoPaulo** region. For details about VPC creation, see [Creating VPCs](#).

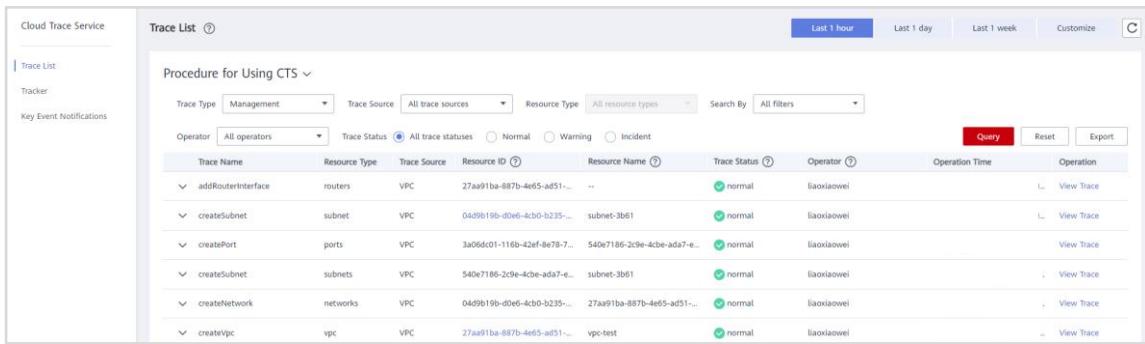


| Name | IPv4 CIDR Block | Status | Subnets | Route Tables | Operation |
|----------|-------------------------------------|-----------|---------|--------------|--|
| vpc-test | 192.168.0.0/16 (Primary CIDR block) | Available | 1 | 1 | Edit CIDR Block Delete |

Figure 5-16 Creating a VPC

When the VPC is created, check for an SMS about the VPC creation from HUAWEI CLOUD.

Access the CTS console and choose Trace List in the navigation pane. These are operation records generated in the last seven days. Information such as trace name, trace status, and operation time is displayed. You can also search for the traces you need.



| Trace Name | Resource Type | Trace Source | Resource ID | Resource Name | Trace Status | Operator | Operation Time | Operation |
|--------------------|---------------|--------------|------------------------------|------------------------------|---------------------|-------------|----------------|----------------------------|
| addRouterInterface | routers | VPC | 27aa91ba-887b-4e65-ad51... | -- | normal | liaoxiaowei | -- | View Trace |
| createSubnet | subnet | VPC | 04d9b190-d0e6-4cb0-b235... | subnet-3061 | normal | liaoxiaowei | -- | View Trace |
| createPort | ports | VPC | 3a066d01-116b-42ef-8e78-7... | 540e7186-2c9e-4cbe-ada7-e... | normal | liaoxiaowei | -- | View Trace |
| createSubnet | subnets | VPC | 540e7186-2c9e-4cbe-ada7-e... | subnet-3061 | normal | liaoxiaowei | -- | View Trace |
| createNetwork | networks | VPC | 04d9b190-d0e6-4cb0-b235... | 27aa91ba-887b-4e65-ad51... | normal | liaoxiaowei | -- | View Trace |
| createVpc | vpc | VPC | 27aa91ba-887b-4e65-ad51... | vpc-test | normal | liaoxiaowei | -- | View Trace |

Figure 5-17 Viewing traces

Congratulations! You have just learnt to configure key event notifications.

5.2.3 Use Cloud Eye to Monitor an ECS

5.2.3.1 Monitoring an ECS

On the management console on LA-SaoPaulo region, search for Cloud Eye and access it.

Cloud Eye is a multi-dimensional resource monitoring service.

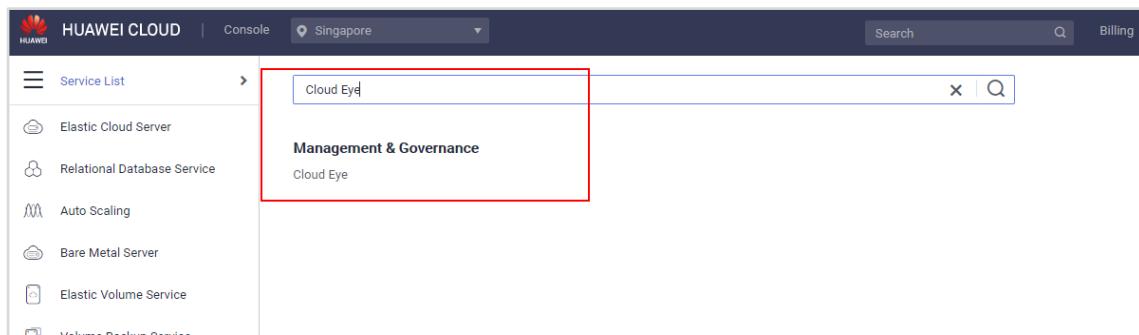
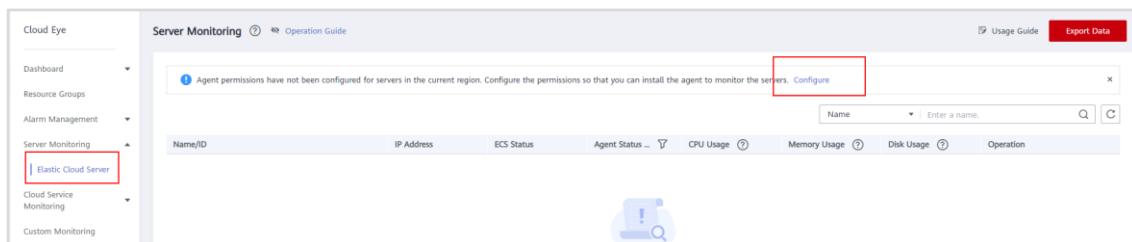


Figure 5-18 Accessing Cloud Eye

On the Cloud Eye console, in the navigation pane, on the left, choose Server Monitoring. Click Configure.

Server monitoring provides basic monitoring, OS monitoring, and process monitoring.



Go to the ECS console, locate ecs-linux, and in the Operation column, click Remote Login.

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|--|-----|---|---|---|----------------------------------|-----|---|
| ecs-linux e8543722-397c-447f-818a-982f3e... | AZ1 |  Running | 1 vCPUs 1GiB s6-small CentOS 7.6 64bit | 119.13.109.188 (EIP) 1... 192.168.1.109 (Private IP) | Pay-per-use Created on: | -- |  Remote Login More ▾ |

Figure 5-19 Remotely logging in to ecs-linux

Run the following command to install the Agent (a Cloud Eye plug-in) on ecs-linux:

```
cd /usr/local && curl -k -O https://obs.ap-southeast-3.myhuaweicloud.com/uniagent-ap-southeast-3/script/agent_install.sh && bash agent_install.sh
```

```
[root@ecs-linux ~]# cd /usr/local && curl -k -O https://obs.ap-southeast-3.myhuaweicloud.com/uniagent-ap-southeast-3/script/agent_install.sh && bash agent_install.sh
  % Total    % Received % Xferd  Average Speed   Time     Time     Time  Current
          0     0      0      0      0      0      0      0 --:--:-- 27684
  100  3837  100  3837    0      0 27580      0 --:--:-- --:--:-- 27684
  % Total    % Received % Xferd  Average Speed   Time     Time     Time  Current
          0     0      0      0      0      0      0      0 --:--:-- 27.8M
  100 9252k  100 9252k    0      0 27.7M      0 --:--:-- --:--:-- 27.8M
uniagent_linux_amd64/
uniagent_linux_amd64/bin/
uniagent_linux_amd64/bin/decrypt
uniagent_linux_amd64/bin/updater
uniagent_linux_amd64/bin/uniagent
uniagent_linux_amd64/script/
uniagent_linux_amd64/script/install.sh
uniagent_linux_amd64/script/uninstall.sh
uniagent_linux_amd64/conf/
uniagent_linux_amd64/conf/conf.json
uniagent_linux_amd64/conf/seelog.xml
Current user is root.
uniagent install to directory(/usr/local/uniagent) successfully
```

Figure 5-20 Installing and configuring the Agent

Figure 5-21

Confirm that the Agent was installed successfully.

If you can see the following information, the Agent is installed successfully.

```
/bin/curl
ces flag FOUND in __support_agent_list
Current user is root.
Current linux release version : CENTOS
Start to install telescope...
In chkconfig
Success to install telescope to dir: /usr/local/telescope.
Telescope process has been already running, please use restart command.
```

Figure 5-22 Agent installed successfully

Go to the ECS console. In the ECS list, locate ecs-linux, and in the Operation column, choose More > Restart.

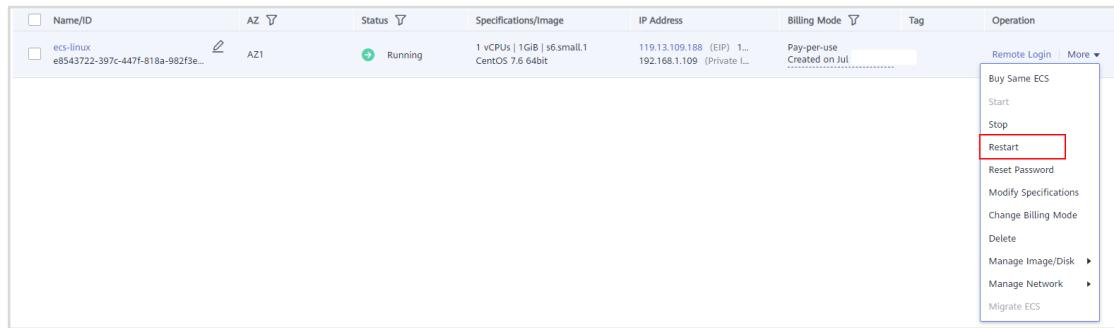


Figure 5-23 Restarting ecs-linux

Go to the Cloud Eye Server Monitoring page, locate ecs-linux, and click View Metric in the Operation column to view the running and performance parameters of ecs-linux.

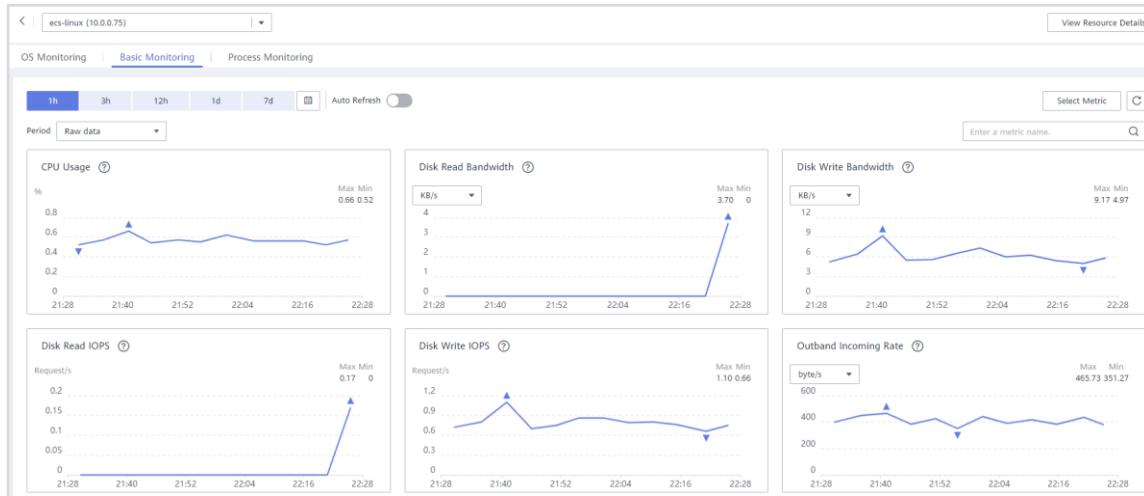


Figure 5-24 Viewing metrics

5.2.3.2 Creating an Alarm Rule to Monitor ECS CPU Usage

You can flexibly configure alarm rules and notifications on Cloud Eye to keep track of resource statuses and performance updates and prevent potential service losses.

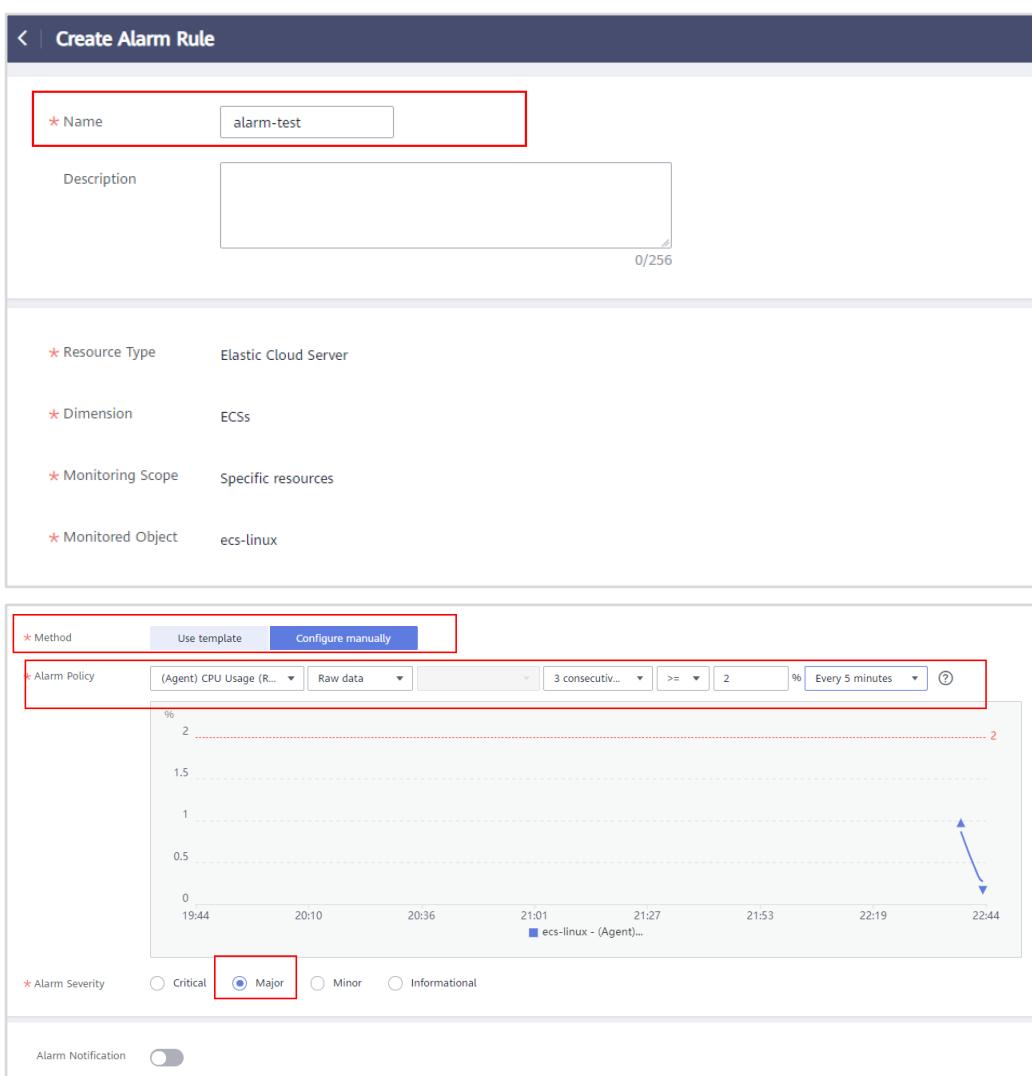
On the Cloud Eye Server Monitoring page, locate ecs-linux and click Create Alarm Rule in the Operation column.



Figure 5-25 Create Alarm Rule

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

- **Name:** Enter an alarm rule name.
- **Resource Type:** Elastic Cloud Server
- **Dimension:** ECSs
- **Monitoring Scope:** Specific resources
- **Monitored Object:** ecs-linux
- **Method:** Configure manually
- **Alarm Policy:** (Agent) CPU Usage (Recommended), Raw data, 3 consecutive periods, $\geq 2\%$, Every 5 minutes
- **Alarm Severity:** Major



The screenshot shows the 'Create Alarm Rule' interface in three main sections:

- Step 1: Basic Configuration**
 - Name:** alarm-test (highlighted with a red box)
 - Description:** (Empty text area with character count 0/256)
- Step 2: Resource Selection**
 - Resource Type:** Elastic Cloud Server
 - Dimension:** ECSs
 - Monitoring Scope:** Specific resources
 - Monitored Object:** ecs-linux
- Step 3: Policy Configuration**
 - Method:** Configure manually (selected, highlighted with a red box)
 - Alarm Policy:** (Agent) CPU Usage (Raw data, 3 consecutive periods, $\geq 2\%$, Every 5 minutes) (highlighted with a red box)
 - Graph:** A line graph showing CPU usage over time (19:44 to 22:44). The Y-axis ranges from 0 to 2%. Two horizontal dashed lines at 0% and 2% represent the baseline and threshold. An arrow points down from the 2% line to the graph area.
 - Alarm Severity:** Major (selected, highlighted with a red box)
 - Alarm Notification:** (Toggle switch)

Figure 5-26 Create Alarm Rule

Go to the Alarm Rules page and check the status of alarm rule alarm-test.

If Status changes to OK, alarm-test is successfully created.

| Name | Resource Type | Monitored Object | Alarm Severity | Alarm Policy | Status | Last Status Update | Operation |
|-----------------------------------|----------------------|-------------------------|----------------|--|--------|---------------------|--|
| alarm-test al1626533281662k... | Elastic Cloud Server | ECSS Specific resources | Major | Trigger an alarm if (Agent) CPU Usage Raw data >= 2% for 3 consecutive periods. Trigger an alarm every 5 minutes again if the alarm persists. | OK | 2021-07-17 22:15:12 | View Resource Disable More |

Figure 5-27 Viewing alarm-test

Go to the Server Monitoring page, locate ecs-linux, and in the Operation column, click View Metric.

| | | | | | | | | |
|---|---|---------|---------|------|--------|-------|-----------------------------|-----------------------------------|
| ecs-linux 8447f247-3416-44d9-8261-dccb434b1415 | 119.13.109.188 (EIP) 10.0.0.75 (Private) | Running | Running | 0.4% | 30.79% | 5.85% | View Metric | Create Alarm Rule |
|---|---|---------|---------|------|--------|-------|-----------------------------|-----------------------------------|

Figure 5-28 Viewing metrics

View the CPU usage of ecs-linux.

The current CPU usage does not meet the alarm triggering condition.

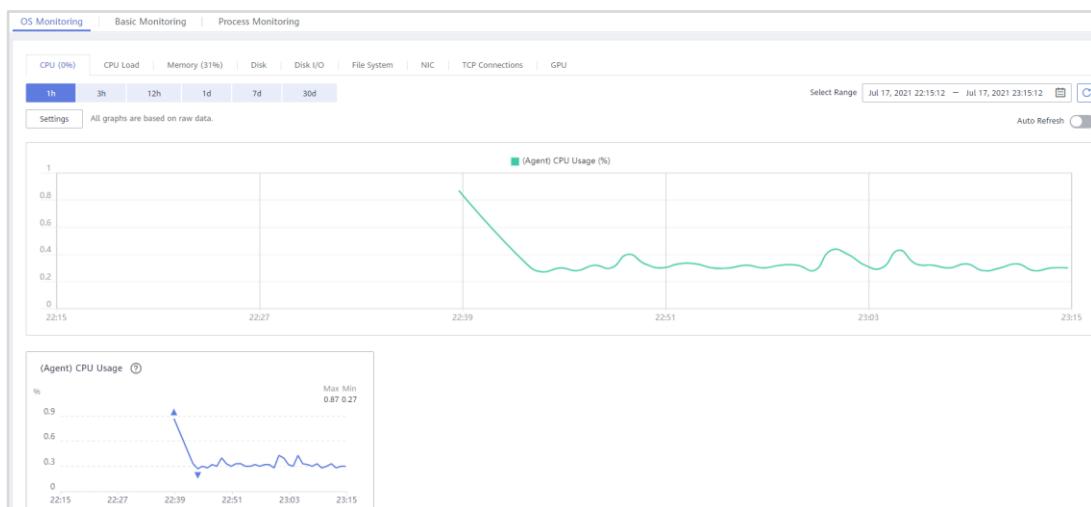


Figure 5-29 OS Monitoring

Go to the ECS console, log in to ecs-linux, and increase its CPU usage by running the following command. (5 to 10 minutes later, you will see that the CPU usage has been dramatically increased.)

```
for i in `seq 1 $(cat /proc/cpuinfo |grep "physical id" |wc -l)`; do dd if=/dev/zero of=/dev/null & done
```

```
[root@ecs-linux local]# for i in `seq 1 $(cat /proc/cpuinfo |grep "physical id" |wc -l)`; do dd if=/dev/zero of=/dev/null & done
[1]+ 1636
root@ecs-linux local]#
```

Figure 5-30 Logging in to ecs-linux

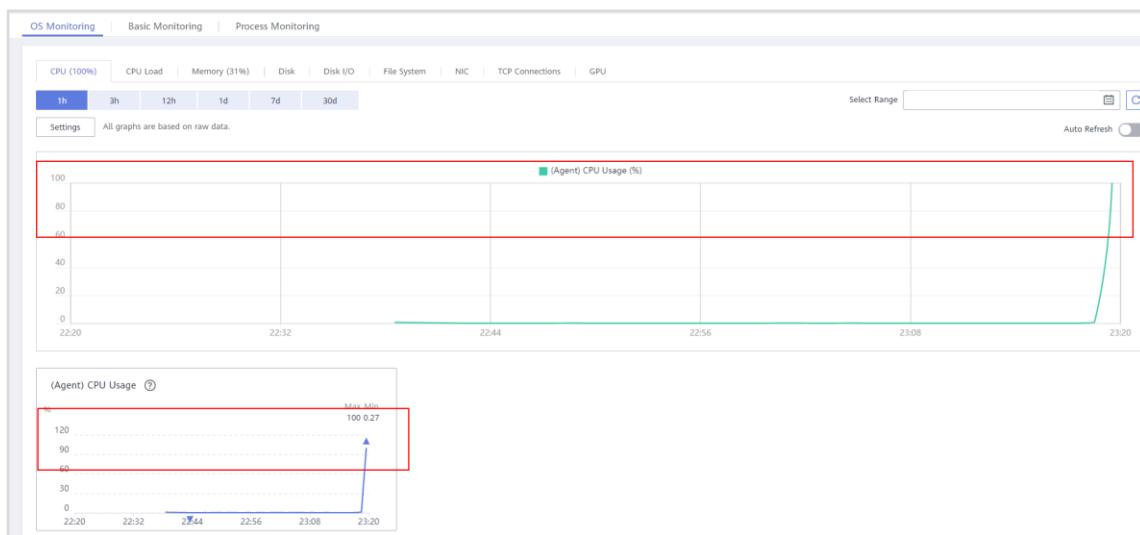


Figure 5-31 Fast and dramatic increase of the CPU usage

Go to the Cloud Eye console. In the navigation pane on the left, choose Alarm Management > Alarm History. Refresh the Alarm History page.

The status of alarm-test changes to Alarm.

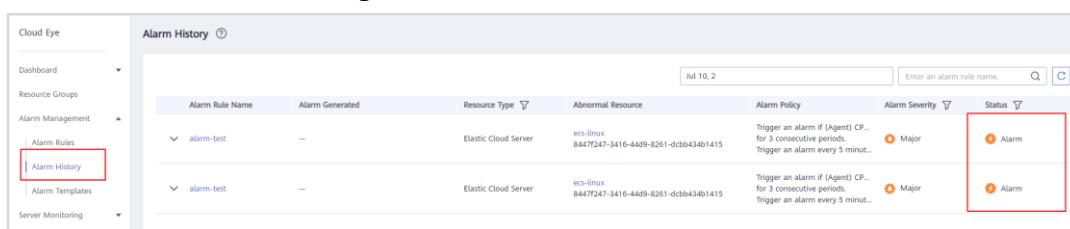


Figure 5-32 alarm-test status being Alarm

You have now completed the experiment of using Cloud Eye to monitor an ECS.

5.2.4 Viewing ECS Logs

5.2.4.1 Creating a Log Group and Log Stream

Pre-requisite: A Linux ECS must exists (t6.small.1, CentOS 7.6, 40GB, no EIP bounded). Log in to the management console on LA-SaoPaulo region, expand the service list, and click Log Tank Service.

The screenshot shows the HUAWEI CLOUD Management Console interface. The left sidebar lists various services: Compute, Storage, Networking, Databases, Application, Migration, EI Enterprise Intelligence, Management & Governance, Business Applications, and Media Services. Under 'Compute', 'Storage', and 'Networking', there are several sub-options. In the 'Management & Governance' section, 'Cloud Trace Service' is listed, and 'Log Tank Service' is highlighted with a red box. The top navigation bar includes 'Console', 'Singapore', 'Search', 'Billing Center', 'Resources', 'Service Tickets', 'Enterprise', and 'Support'.

Figure 5-33 Accessing LTS

Log groups and log streams are basic units for log management in LTS. Before using LTS, create a log group and log stream. On the LTS console, choose Log Management in the navigation pane, and click Create Log Group in the upper left.

The screenshot shows the LTS Management console. The left sidebar has options: LTS, Log Management (highlighted), Log Ingestion, Host Management, Log Transfer, and Log Configuration. The main area is titled 'Log Management'. It features a table with columns: Log Group Name/ID, Log Retention Duration, Created, Created By, and Operation. A search bar at the top right says 'Enter log group name/ID'. The message 'No records found.' is displayed below the table. The top navigation bar includes 'Console', 'Singapore', 'Search', 'Billing Center', 'Resources', 'Service Tickets', 'Enterprise', 'Support', 'English', and a language switcher.

Figure 5-34 Creating a log group

Give your group a name and choose how many days you want to retain its logs and click OK.

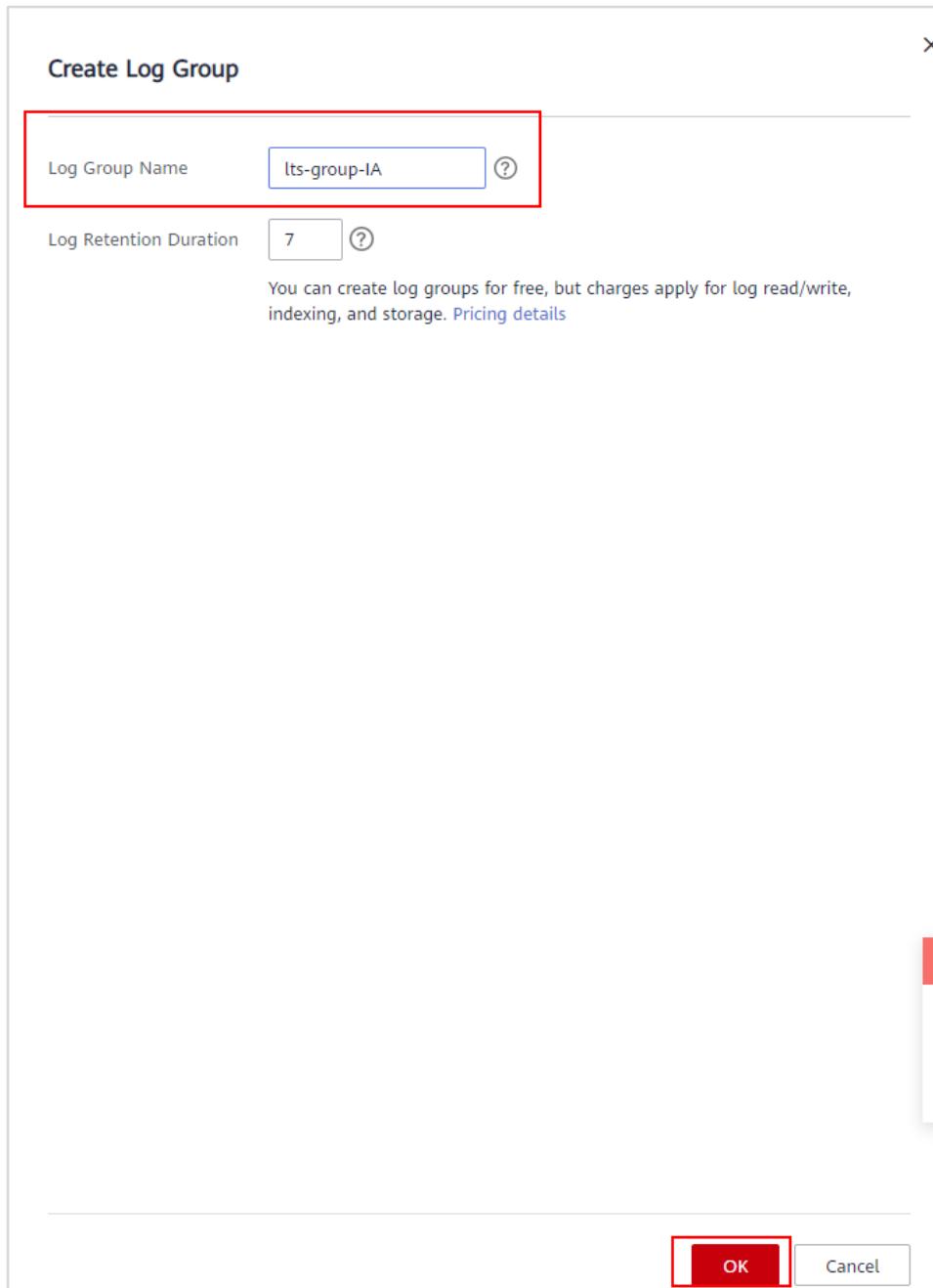


Figure 5-35 Configuring a log group

On the Log Management page, click the name of your log group.

| Log Stream Name/ID | Log Retention Duration | Created | Created By | Operation |
|--|------------------------|---------------------|------------|-----------------|
| lts-group-IA 10dc3ca9-49b0-493a-a10e-0c86507e1308 | 7 | 2023-09-01 10:00:00 | User | Modify Delete |

Figure 5-36 Accessing a log group

On the page displayed, Click Create Log Stream.

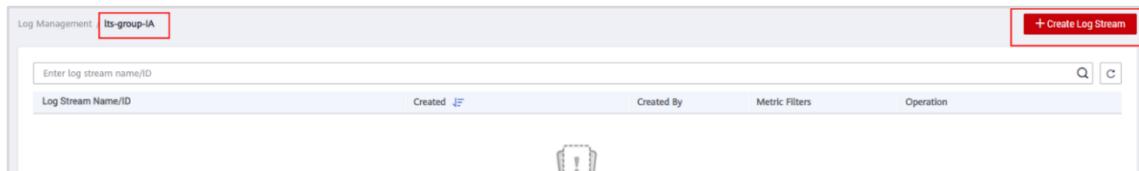
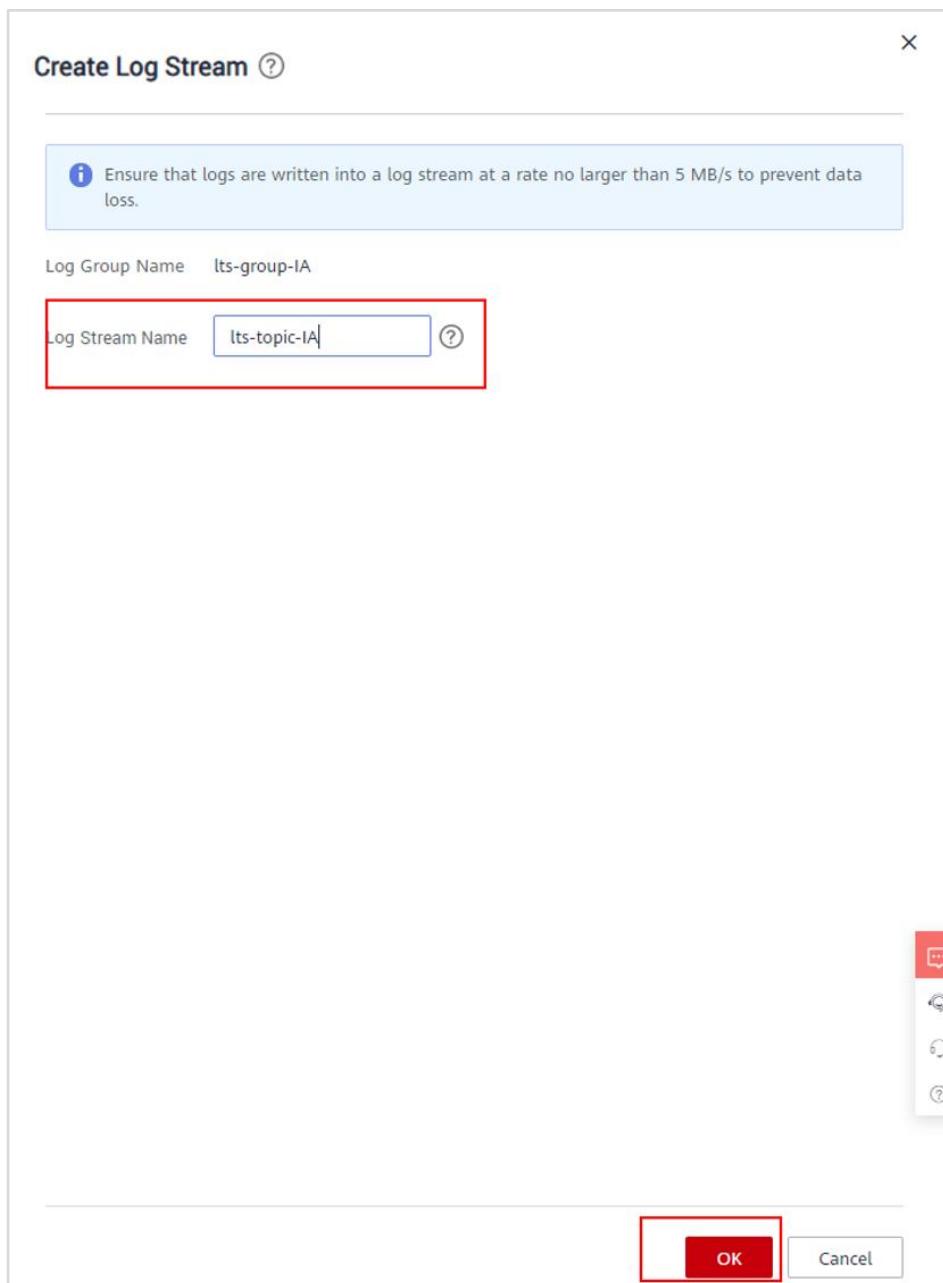


Figure 5-37 Creating a log stream

Enter a log stream name and click OK.



The screenshot shows a 'Create Log Stream' dialog box. It includes a note about log rate limits, a 'Log Group Name' field set to 'lts-group-IA', and a 'Log Stream Name' field containing 'lts-topic-IA'. A red box highlights the 'OK' button at the bottom right of the dialog. The right side of the dialog features a vertical toolbar with icons for message, refresh, save, and help.

Figure 5-38 Configuring a log stream

5.2.4.2 Installing ICAgent

ICAgent is a log collection tool of LTS. Install it in the ECS from which you want to collect logs. On the LTS console, choose **Host (or Agent) Management** in the navigation pane, and click **Install ICAgent** in the upper right.

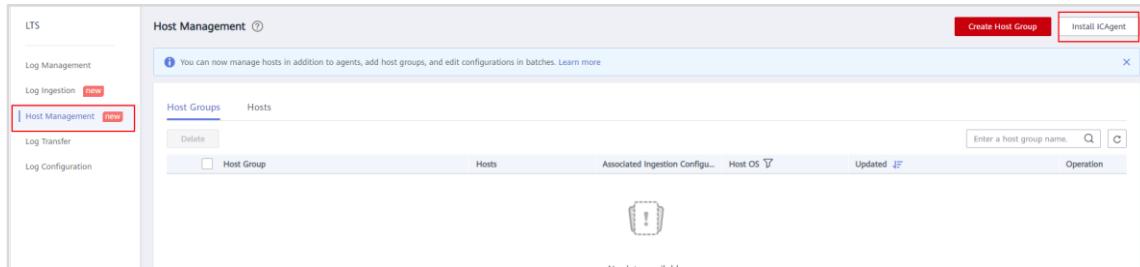
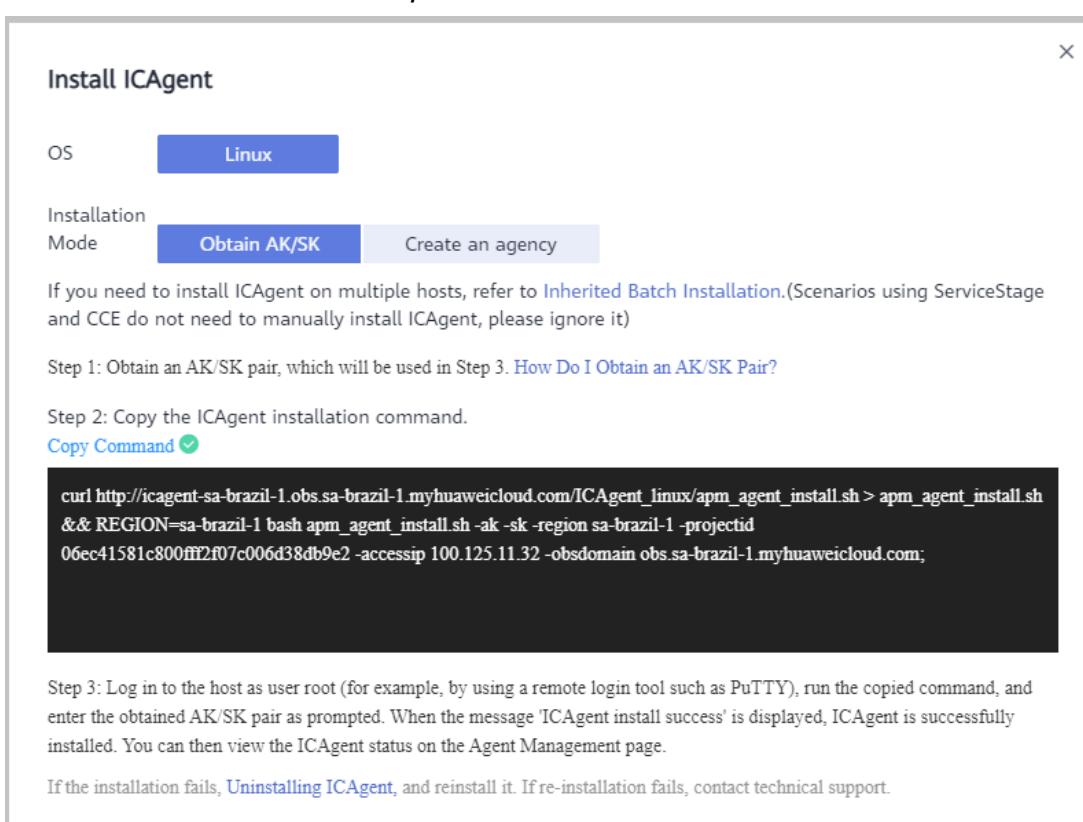


Figure 5-39 Accessing the Host Management page

Configure ICAgent installation parameters.

- **OS: Linux**
- **Installation Mode: Obtain AK/SK**



If you need to install ICAgent on multiple hosts, refer to [Inherited Batch Installation](#). (Scenarios using ServiceStage and CCE do not need to manually install ICAgent, please ignore it)

Step 1: Obtain an AK/SK pair, which will be used in Step 3. [How Do I Obtain an AK/SK Pair?](#)

Step 2: Copy the ICAgent installation command.
[Copy Command](#) ✓

```
curl http://icagent-sa-brazil-1.obs.sa-brazil-1.myhuaweicloud.com/ICAgent_linux/apm_agent_install.sh > apm_agent_install.sh
&& REGION=sa-brazil-1 bash apm_agent_install.sh -ak -sk -region sa-brazil-1 -projectid
06ec41581c800ff12f07c006d38db9e2 -accessip 100.125.11.32 -obsdomain obs.sa-brazil-1.myhuaweicloud.com;
```

Step 3: Log in to the host as user root (for example, by using a remote login tool such as PuTTY), run the copied command, and enter the obtained AK/SK pair as prompted. When the message 'ICAgent install success' is displayed, ICAgent is successfully installed. You can then view the ICAgent status on the Agent Management page.

If the installation fails, [Uninstalling ICAgent](#), and reinstall it. If re-installation fails, contact technical support.

Figure 5-40 Configuring ICAgent Installation

Copy the command in Step 2 (see Figure 5-40 above), replace the “-ak” to “-ak your_AK_key” and “-sk” to “-sk your_SK_key” and run it in the ECS. If the following information is displayed, the installation is successful.

```
[root@ecs-linux ~]# curl http://icagent-sa-brazil-1.obs.sa-brazil-1.myhuaweicloud.com/ICAgent_linux/apm_agent_install.sh > apm_agent_install.sh && REGION=sa-brazil-1 bash apm_agent_install.sh -ak 91YARNX1Z5ULUFSRMTYI -sk 9yRqrealADJSMU8M1RAYQLmGnu6TJW1WuQzK3x -region sa-brazil-1 -projectid 06ec41581c0000ff2f07c006d38db9e2 -accessip 100.125.11.32 -obsdomain obs.sa-brazil-1.myhuaweicloud.com
  Total  Received  Xferd  Average Speed   Time   Time  Current
          Dload  Upload   Total Spent  Left  Speed
100 7051  100 7051     0      0  133k  0:00:00 --:--:-- --:--:-- 135k
start to install ICAgent.
begin to download install package from icagent-sa-brazil-1.obs.sa-brazil-1.myhuaweicloud.com.
#####
download success.
start install package.
start install ICAgent...
no crontab for root
starting ICAgent...
ICAgent install success.
[root@ecs-linux ~]# _
```

Figure 5-41 Installing ICAgent

Refresh the Hosts tab under the Host Management page. If the ICAgent status for the ECS is Running, ICAgent has been installed.

| Host Name | Host OS | Host IP Address | Associated Host Groups | ICAgent Status | ICAgent Version | Updated |
|-----------|---------|-----------------|------------------------|----------------|-----------------|---------|
| ecs-linux | Linux | 100.0.75 | 0 | Running | 5.12.78 | |

Figure 5-42 Viewing the ICAgent status

5.2.4.3 Configuring Log Ingestion

On the LTS console, choose Log Ingestion in the navigation pane, click Ingest Log in the upper right corner, and click Host.

| Ingest Configuration Name | Ingestion Type | Collection Configuration | Log Group | Log Stream | Operation |
|---------------------------|----------------|--------------------------|-----------|------------|-----------|
| No data available. | | | | | |

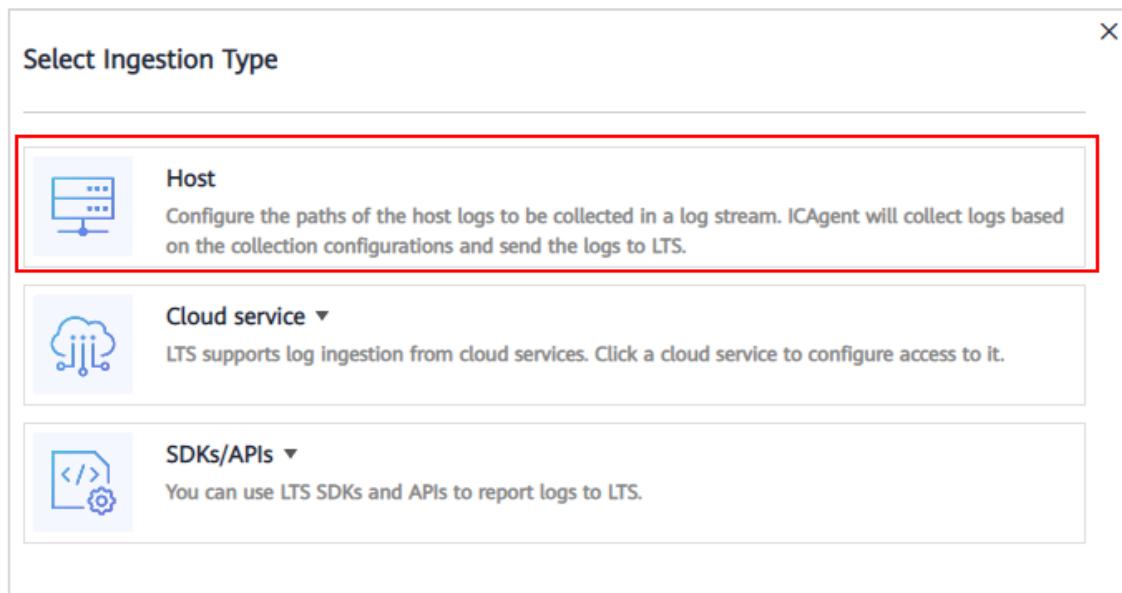


Figure 5-43 Selecting Host

On the Select Log Stream stage, select the log group and log stream you created. Click Next: Select Host Group.

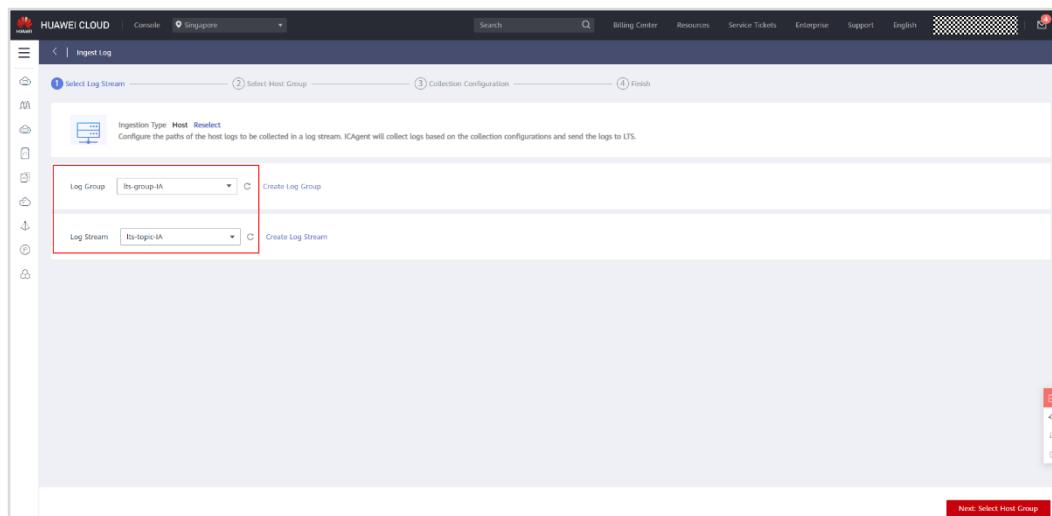
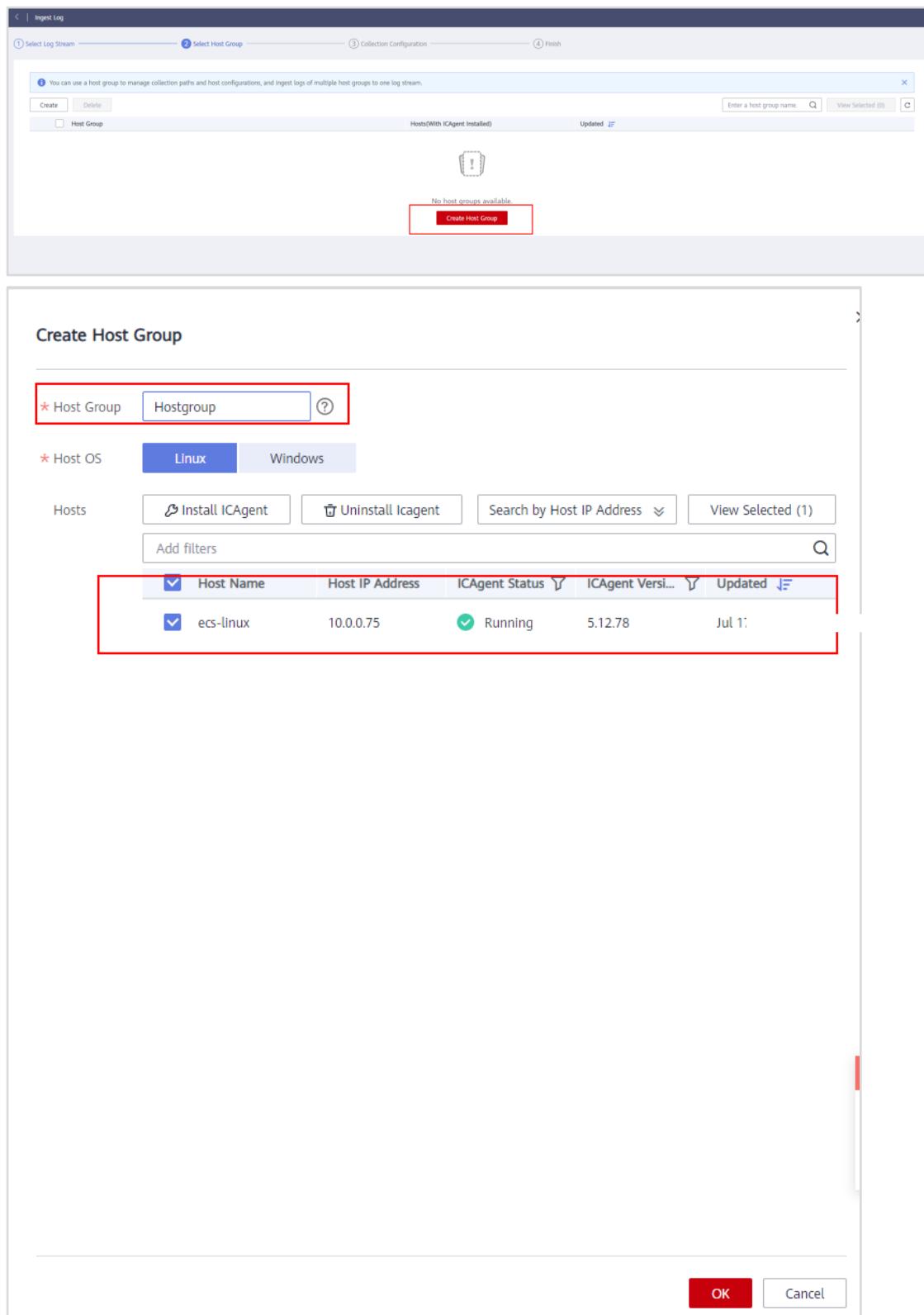


Figure 5-44 Selecting a log stream

Create a host group. Give the group a name. Select it in the list and go to the next step.



The screenshot shows the 'Create Host Group' interface. At the top, there's a navigation bar with steps: 1. Select Log Stream, 2. Select Host Group (which is currently active), 3. Collection Configuration, 4. Finish. A note says: 'You can use a host group to manage collection paths and host configurations, and ingest logs of multiple host groups to one log stream.' Below this are 'Create' and 'Delete' buttons, and a search bar 'Enter a host group name'. A table titled 'Hosts (With ICAgent Installed)' shows one entry: 'Host Group' (with a checkbox icon) and 'Host IP Address' (10.0.0.75). A red box highlights the 'Host Group' column header. A 'Create Host Group' button is at the bottom. In the main area, the 'Create Host Group' dialog has a title 'Create Host Group'. It includes fields for 'Host Group' (highlighted with a red border) and 'Host OS' (set to 'Linux'). Below are buttons for 'Install ICAgent' and 'Uninstall ICAgent', a search bar 'Search by Host IP Address', and a 'View Selected (1)' button. A table lists hosts with columns: Host Name, Host IP Address, ICAgent Status, ICAgent Version, and Updated. A row for 'ecs-linux' is selected and highlighted with a red border. The table headers are: Host Name, Host IP Address, ICAgent Status, ICAgent Version, Updated. The selected row shows: ecs-linux, 10.0.0.75, Running, 5.12.78, Jul 11. At the bottom right are 'OK' and 'Cancel' buttons.

Figure 5-45 Creating a host group

Configure the collection configuration name and collection paths. Collection paths are ECS log paths and the source of the logs ICAgent will collect.

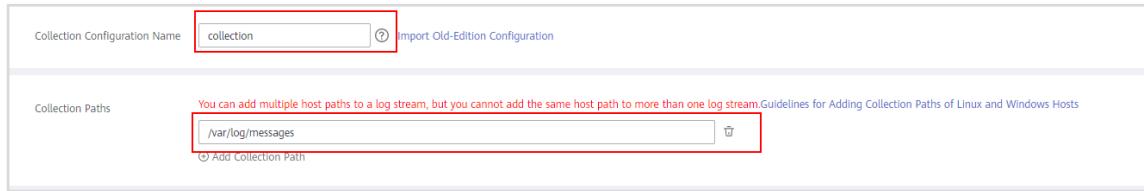


Figure 5-46 Configuring the collection

Configure the log format and log time and click OK.

- **Log Format:** Single-line
- **Log Time:** System time



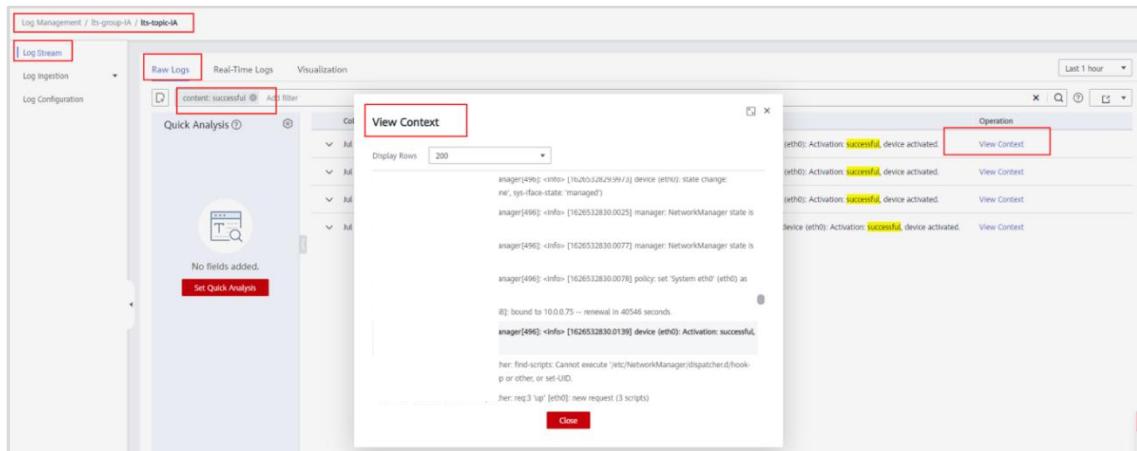
Figure 5-47 Configuring the collection

Wait a minute to view the ingested logs on the Real-Time Logs tab under a log stream.



Figure 5-48 Viewing real-time logs

Click the Raw Logs tab. Search successful log events and check their context.



The screenshot shows the Log Management interface for a specific log group. The 'Raw Logs' tab is active. A search filter 'content:successful' is applied. A 'View Context' dialog is open, showing log entries from the last hour. One entry is highlighted: 'eth0: Activation: successful, device activated.' with a 'View Context' button.

Figure 5-49 Searching for raw logs

Congratulations! You have just learnt to view ECS logs.

5.3 Deleting Resources

Delete resources, such as ECSs, ECS monitoring settings, alarm rules, cloud service logs, and VPCs.

Check that all resources in the account have been deleted.

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 |

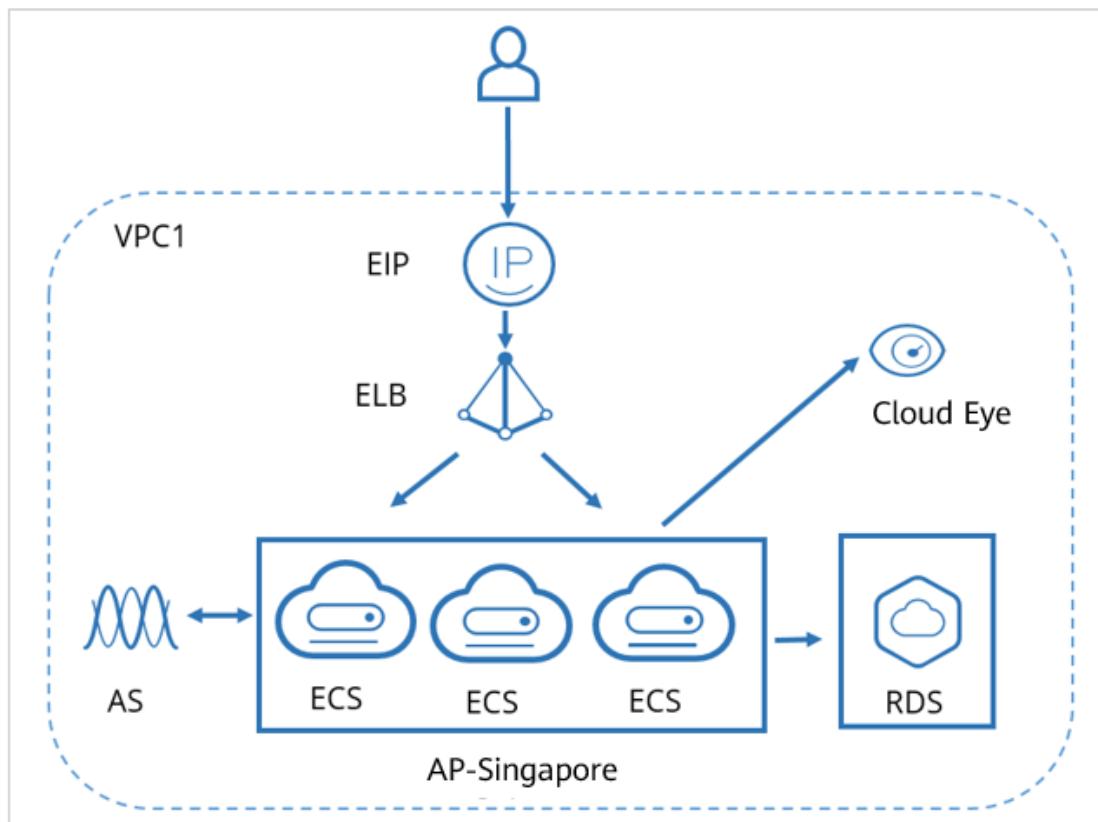


Figure 6-1 Solution topology

6.3 Preparations

6.3.1 Logging In to HUAWEI CLOUD

Visit the [HUAWEI CLOUD official website](#) and click Log In in the upper right corner.

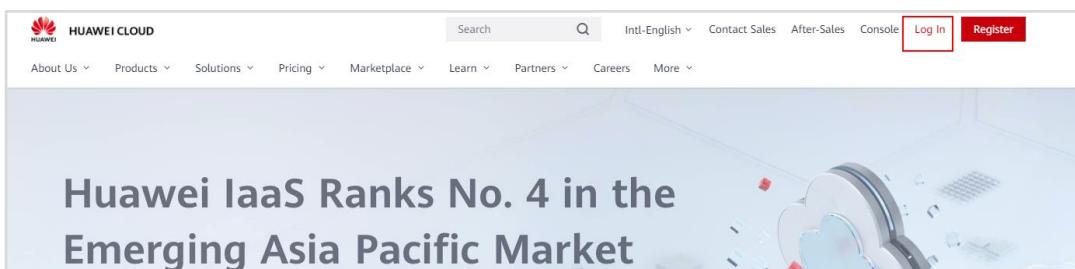


Figure 6-2 Visiting the HUAWEI CLOUD official website

On the login page, click HUAWEI CLOUD Account, enter your account and password, and then click Log In.

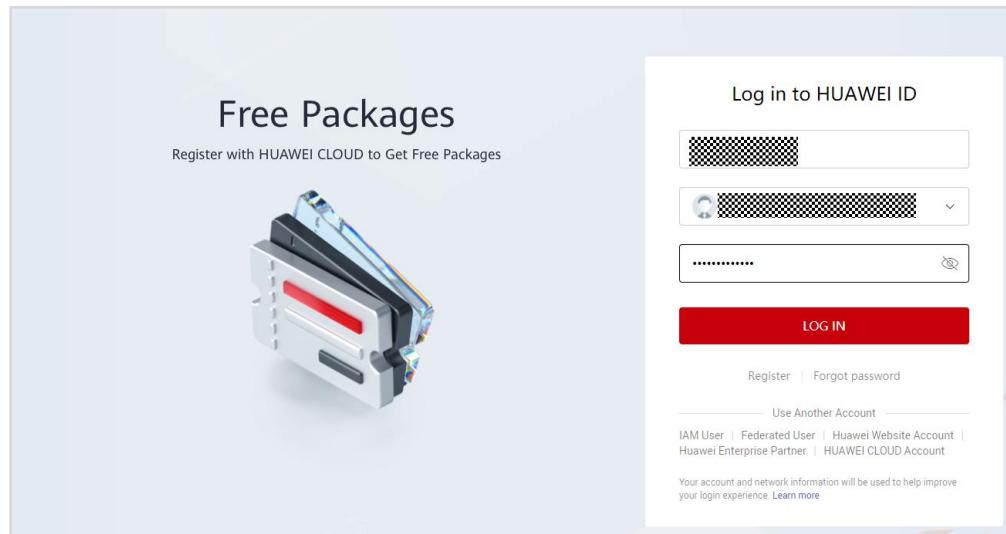


Figure 6-3 Logging in to the HUAWEI CLOUD official website

6.3.2 Creating a VPC

Switch to the management console, and select the AP-Singapore region. In the left navigation pane, choose Service List > Networking > Virtual Private Cloud.

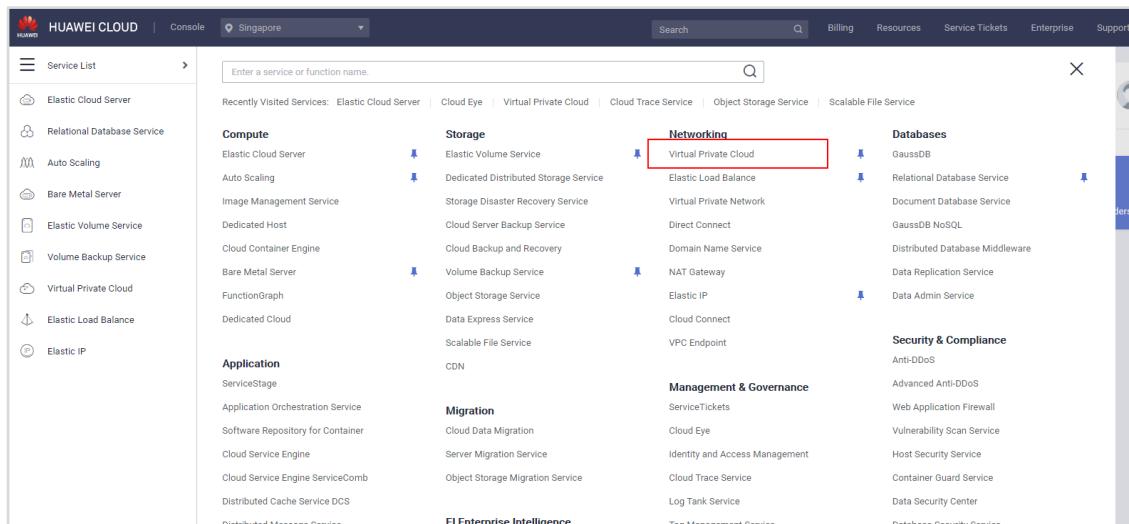


Figure 6-4 Switching to the VPC console

Click Create VPC.

| Name | IPv4 CIDR Block | Status | Subnets | Route Tables | Operation |
|-------------|----------------------------------|-----------|---------|--------------|--------------------------|
| vpc-default | 10.0.0.0/24 (Primary CIDR block) | Available | 1 | 1 | Edit CIDR Block Delete |

Figure 6-5 Creating a VPC

Configure the parameters as follows, and click Create Now.

- Region: AP-Singapore**
- Name: vpc-mp** (Change it as needed.)
- Retain the default settings for other parameters.

Figure 6-6 Configuring the VPC

View the created VPC in the VPC list.

| Name | IPv4 CIDR Block | Status | Subnets | Route Tables | Operation |
|-------------|-------------------------------------|-----------|---------|--------------|--------------------------|
| vpc-mp | 192.168.0.0/16 (Primary CIDR block) | Available | 1 | 1 | Edit CIDR Block Delete |
| vpc-default | 10.0.0.0/24 (Primary CIDR block) | Available | 1 | 1 | Edit CIDR Block Delete |

Figure 6-7 Viewing the VPC

6.3.3 Creating and Configuring a Security Group

On the Network Console, choose Access Control > Security Groups and create a security group.

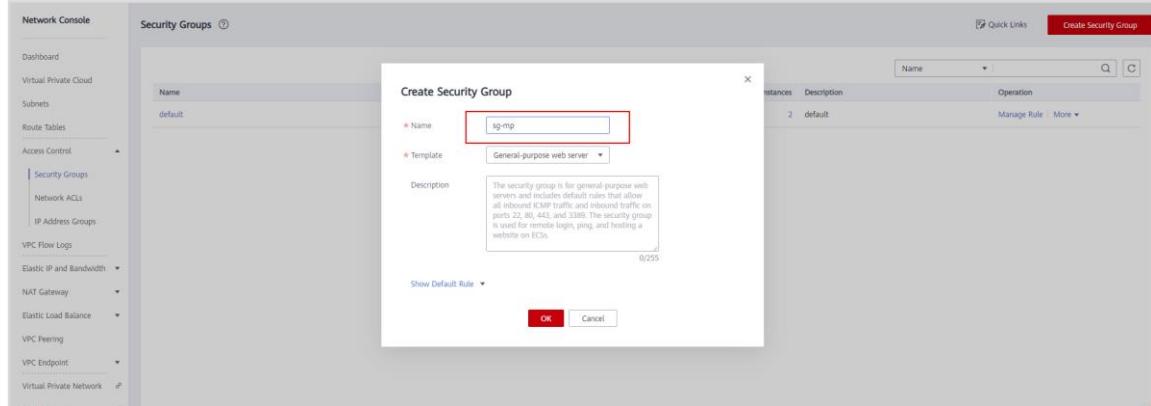


Figure 6-8 Creating a security group

Click the security group name.



Figure 6-9 Viewing the security group

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**

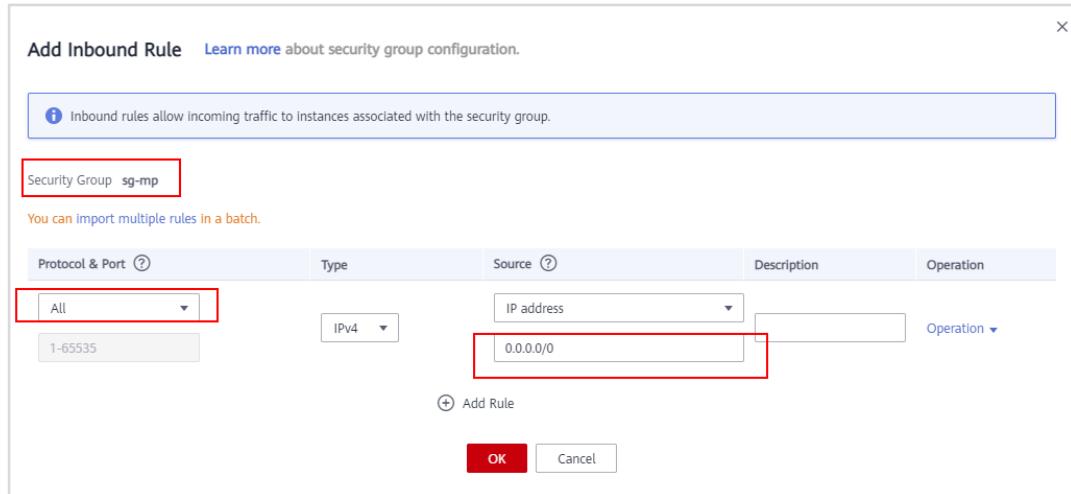


Figure 6-10 Adding an inbound rule

6.3.4 Buying an ECS

In the service list, choose Compute > Elastic Cloud Server.

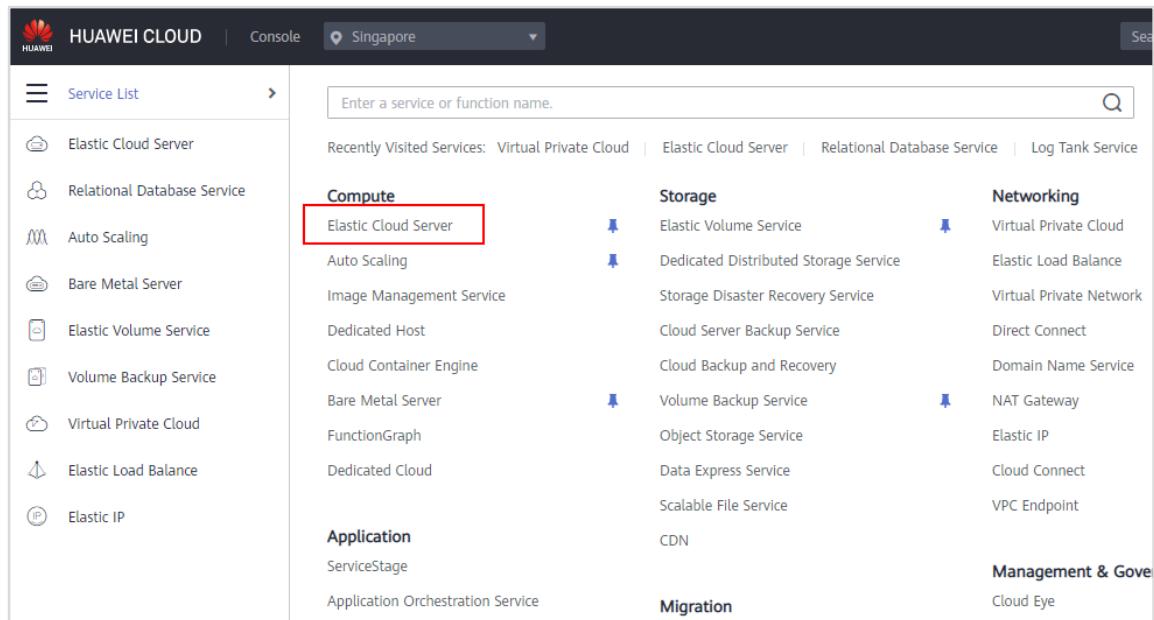


Figure 6-11 Acessing the ECS console

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**

| Flavor Name | vCPUs Memory | CPU | Assured / Maximum Bandwidth | Packets Per Second (PPS) |
|-------------------|----------------------|----------------------------------|-----------------------------|--------------------------|
| s3.2xlarge.4 | 8 vCPUs 32GB | Intel SkyLake 6161 2.2GHz | 0.8 / 3 Gbit/s | 200,000 |
| s3.4xlarge.2 | 16 vCPUs 32GB | Intel SkyLake 6161 2.2GHz | 1.5 / 4 Gbit/s | 300,000 |
| s3.4xlarge.4 | 16 vCPUs 64GB | Intel SkyLake 6161 2.2GHz | 1.5 / 4 Gbit/s | 300,000 |
| s6.small.1 | 1 vCPUs 1GB | Intel Cascade Lake 2.6GHz | 0.1 / 0.8 Gbit/s | 100,000 |
| s6.medium.2 | 1 vCPUs 2GB | Intel Cascade Lake 2.6GHz | 0.1 / 0.8 Gbit/s | 100,000 |
| s6.medium.4 | 1 vCPUs 4GB | Intel Cascade Lake 2.6GHz | 0.1 / 0.8 Gbit/s | 100,000 |
| s6.large.2 | 2 vCPUs 4GB | Intel Cascade Lake 2.6GHz | 0.2 / 1.5 Gbit/s | 150,000 |
| s6.large.4 | 2 vCPUs 8GB | Intel Cascade Lake 2.6GHz | 0.2 / 1.5 Gbit/s | 150,000 |

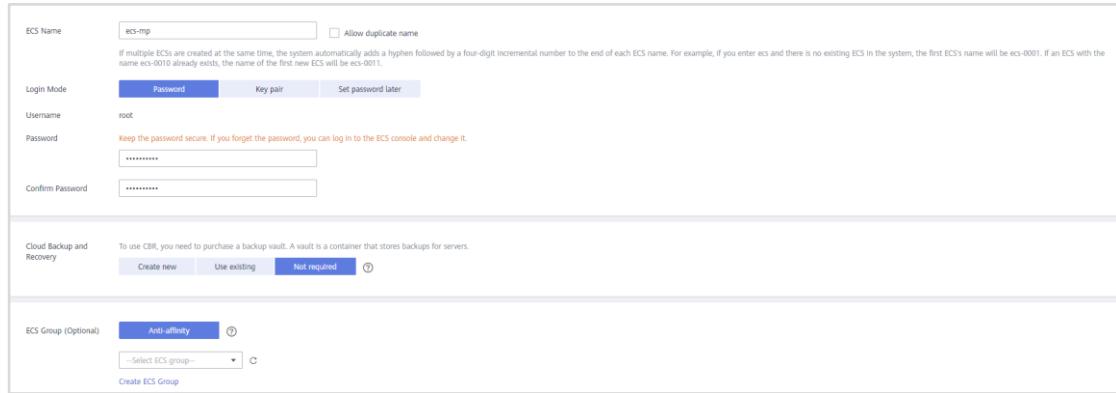
Figure 6-12 Configuring basic settings

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

Figure 6-13 Configuring network
Advanced settings:

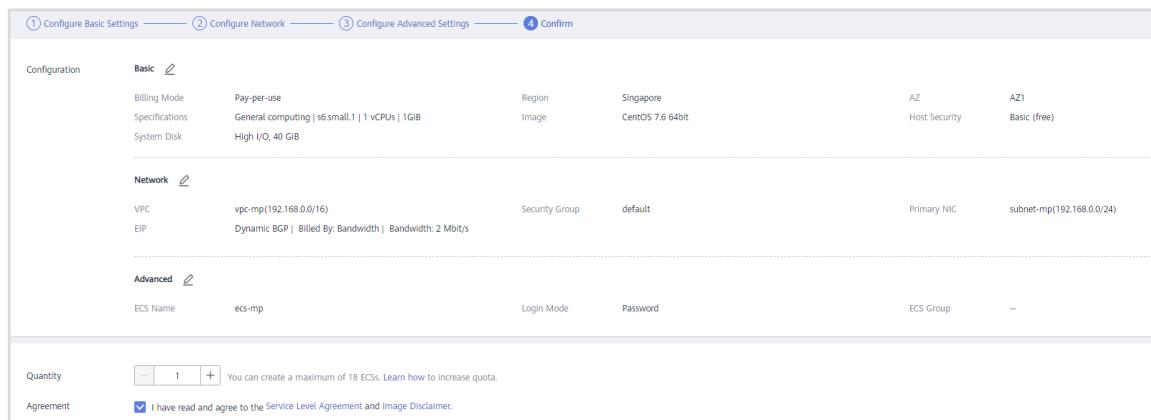
- ECS Name:** ecs-mp (Change it as needed.)
- Login Mode:** Password, for example, Huawei@123!
- Cloud Backup and Recovery:** Not required



The screenshot shows the 'Configure Advanced Settings' step of the ECS creation wizard. It includes fields for ECS Name (ecs-mp), Login Mode (Password selected), Username (root), Password, Confirm Password, Cloud Backup and Recovery (Not required), and ECS Group (Optional) with Anti-affinity selected.

Figure 6-14 Configuring advanced settings

Confirm the configuration, select I have read and agree to the Service Level Agreement and Image Disclaimer, and click Buy Now.



The screenshot shows the 'Confirm' step of the ECS creation wizard, displaying the configuration details from the previous steps. It includes sections for Configuration (Basic, Network, Advanced), a quantity selector (1), and an agreement checkbox. The configuration details include Billing Mode (Pay-per-use), Specifications (General computing | s6.small1 | 1 vCPUs | 1GiB), System Disk (High I/O, 40 GiB), Region (Singapore), Image (CentOS 7.6 64bit), AZ (AZ1), Host Security (Basic (free)), VPC (vpc-mp(192.168.0.0/16)), EIP (Dynamic BGP | Billed By: Bandwidth | Bandwidth: 2 Mbit/s), Primary NIC (subnet-mp(192.168.0.0/24)), ECS Name (ecs-mp), Login Mode (Password), and Password.

Figure 6-15 Confirmation

View the purchased ECS in the ECS list.

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|--|-----|---------|--|---|----------------------------------|-----|-----------------------|
| ecs-mp 25d052d1-e06e-452d-ac3e-821993685e80 | AZ1 | Running | 1 vCPUs 1GiB s6.small1 CentOS 7.6 64bit | 192.168.83.70 (EIP) 192.168.0.102 (Private IP) | Pay-per-use Created on J..... | -- | Remote Login More ▾ |

Figure 6-16 Viewing the ECS in the list

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

Go back to the service list, and choose Database > Relational Database Service.

The screenshot shows the HUAWEI CLOUD Service List interface. On the left, there's a sidebar with various service icons. In the main area, services are categorized into groups: Compute, Storage, Networking, Databases, Application, Migration, EI Enterprise Intelligence, Management & Governance, Business Applications, and Security & Compliance. The 'Relational Database Service' under the 'Databases' category is specifically highlighted with a red box.

Figure 6-17 Acessing the RDS console

Click Buy DB Instance.

The screenshot shows the Relational Database Service instance management page. The left sidebar lists options like Instance Management, Reserved Instance, Backup Management, Parameter Template Management, Task Center, Recycling Management, and Data Admin Service. The main area is titled 'Relational Database Service'. At the top right, there's a red box around the 'Buy DB Instance' button. Below it, there's a search bar and a table for managing database instances.

Figure 6-18 Buying a DB instance

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, Ultra-high I/O**
- Performance specifications: **General-enhanced II, 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: Pay-per-use

Region: AP-Singapore

DB Instance Name: rds-mp

DB Engine: MySQL

DB Engine Version: 8.0

DB Instance Type: Primary/Standby

Storage Type: Ultra-high I/O

Primary AZ: AZ1

Standby AZ: AZ2

Time Zone: UTC+08:00 Beijing, Chongqing, Hong K...

Figure 6-19 Configuring a DB instance

Instance Class: General-enhanced II

| vCPU Memory | Maximum Connections | TPS/QPS |
|-----------------|---------------------|----------------|
| 2 vCPUs 4 GB | 1,500 | 482 9,526 |
| 2 vCPUs 8 GB | 2,500 | 632 12,223 |
| 4 vCPUs 8 GB | 2,500 | 992 19,949 |
| 4 vCPUs 16 GB | 5,000 | 1,389 25,321 |
| 8 vCPUs 16 GB | 5,000 | 1,982 38,252 |
| 8 vCPUs 32 GB | 10,000 | 2,622 50,654 |

Storage Space (GB): 40

Disk Encryption: Recommended

VPC: vpc-mp

Database Port: Default port: 3306

Security Group: sq-mp

Figure 6-20 Configuring a DB instance

| Details | | Configuration | Billing Mode | Quantity | Price |
|-------------------------|--|---------------|--------------|----------|-------|
| Resource | | | | | |
| DB Instance | | | | | |
| Billing Mode | Pay-per-use | | | | |
| Region | Singapore | | | | |
| DB Instance Name | rds-mp | | | | |
| DB Engine | MySQL | | | | |
| DB Engine Version | 8.0 | | | | |
| DB Instance Type | Primary/Standby | | | | |
| Primary AZ | AZ1 | | | | |
| Standby AZ | AZ2 | | | | |
| Instance Specifications | General-enhanced II 2 vCPUs 4 GB, Maximum Connections: 1500, TPS/QPS: 482 9526 | | | | |
| Storage Type | Ultra-high I/O | | | | |
| Storage Space | 40 GB | | | | |
| Time Zone | UTC+08:00 | | | | |
| Disk Encryption | Disable | | | | |
| VPC | vpc-mp | | | | |
| Subnet | subnet-mp(192.168.0/24) | | | | |
| Floating IP Address | Automatically assigned | | | | |
| Security Group | sg-mp (Inbound: TCP(22, 443, 3389, 80; ICMP(-) Outbound: -)) | | | | |
| Database Port | Default port: 3306 | | | | |
| Parameter Template | Default-MYSQL 8.0 | | | | |
| Table Name | Case insensitive | | | | |

Figure 6-21 Confirmation

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 Instance ID | DB Engine Version | Status | Billing Mode | Floating IP Address | Operation |
|--|-------------|-----------------------------------|-------------------|-----------|-----------------------------------|---------------------|--|
| rds-mp e58cd1c7409345d58fc0bb23ea0fda66in01 | -- | Primary/Standby 2 vCPUs 4 GB | MySQL 8.0.21 | Available | Pay-per-use Created on Ju..... | 192.168.0.194 | View Metric More |

Figure 6-22 Viewing the DB instance

Click the DB instance name to view its floating IP address.

| DB Information | | Connection Management | | Storage Space | |
|------------------------------|--|------------------------------|--------------------------------------|-----------------------|------------------------------------|
| DB Instance Name | rds-mp | DB Instance ID | e58cd1c7409345d58fc0bb23ea0fda66in01 | DB Engine Version | MySQL 8.0.21 Upgrade Minor Version |
| Description | -- | DB Instance Type | Primary/Standby Switch | Synchronization Model | Semi-synchronous Change |
| Maintenance Window | 02:00 – 06:00 | Administrator | root | Event Scheduler | Reset Password |
| Instance Class | rds.mysql.c6.large.2.ha 2 vCPUs 4 GB | VPC | vpc-mp | Ultra-high I/O | Not encrypted |
| SSL | Certificate | Subnet | subnet-mp (192.168.0/24) | Used/Allocated | 2.45/40 GB |
| Failover Priority | Reliability | Security Group | sg-mp | Backup Space | Log Backup |
| AZ | AZ1 (Primary AZ), AZ2 (Standby AZ) | | | Free Space | 0/40 GB |
| Connection Information | | Billing Information | | Charging Space | |
| Floating IP Address | 192.168.0.194 | Database Port | 3306 | Used/Allocated | 0/40 GB |
| Database Port | 3306 | Recommended Max. Connections | 1,500 | Log Backup | Charging Space |
| Recommended Max. Connections | 1,500 | Billing Mode | Pay-per-use | Free Space | 0/40 GB |

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

Go back to the ECS console and click Remote Login in the Operation column of the purchased ECS.

| Name/ID | AZ | Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|--|-----|---------|--------------------------|--|---------------------------------|-----|---|
| ecs-mp 25d052d1-e06e-452d-ac3e-821993685e80 | AZ1 | Running | 1 vCPU 1 GB s6.small | 150.138.83.70 (EIP) 2 Mbit/s 192.168.0.102 (Private IP) | Pay-per-use Created on | -- | Remote Login More |

Figure 6-24 Remotely logging in to the ECS

In the VNC window, enter the username (root for Linux ECSs by default) and password for login.



Figure 6-25 Logging in to the Linux ECS

Run the following command to install LAMP and enable the services you will need:

```
yum install -y httpd php php-fpm php-server php-mysql mysql
```

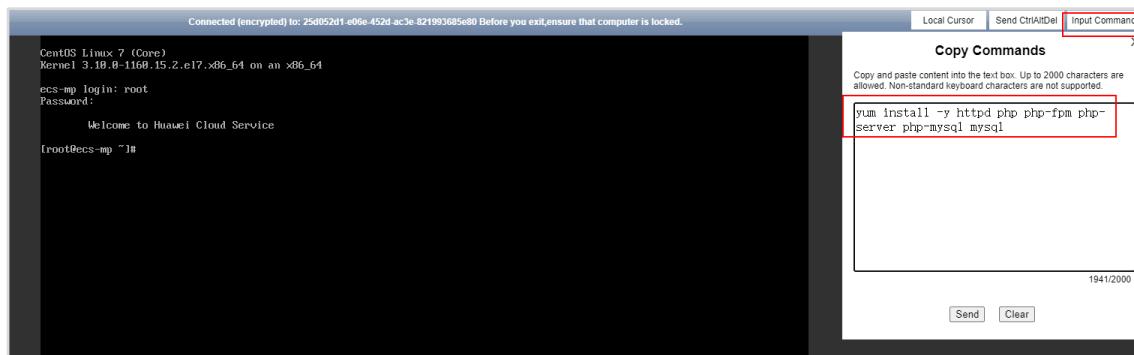


Figure 6-26 Installing LAMP

If Complete! is displayed, LAMP has been successfully installed.

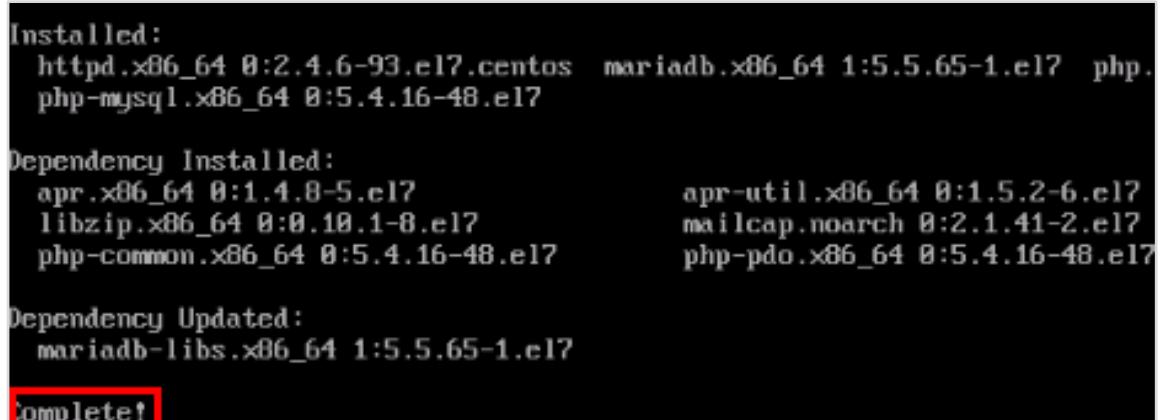


Figure 6-27 Installation succeeded

Configure httpd:

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

```
# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
# In particular, see
# <URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
# for a discussion of each configuration directive.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:\\" for Win32), the
# server will use that explicit path. If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
# with ServerRoot set to '/www' will be interpreted by the
# server as '/www/log/access_log', where as '/log/access_log' will be
# interpreted as '/log/access_log'.
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
#ServerRoot "/etc/httpd"
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
"/etc/httpd/conf/httpd.conf" 353L, 11753C
```

Figure 6-28 Opening the httpd configuration file

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
```

Figure 6-29 Configuring HTTP ports

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

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

Figure 6-30 Saving and exiting

Run the following command to download the WordPress installation package:

```
 wget -c https://wordpress.org/wordpress-4.9.10.tar.gz
```

If `wordpress-4.9.10.tar.gz` is displayed, the WordPress installation package has been downloaded.

```
[root@ecs-mp ~]# wget -c https://wordpress.org/wordpress-4.9.10.tar.gz
--2021-07-18 01:55:54--  https://wordpress.org/wordpress-4.9.10.tar.gz
Resolving wordpress.org (wordpress.org)... 198.143.164.252
Connecting to wordpress.org (wordpress.org):198.143.164.252:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8744264 (8.3M) [application/octet-stream]
Saving to: 'wordpress-4.9.10.tar.gz'

100%[=====] 8,744,264   3.94MB/s   in 2.1s

[██████████] 5:57 (3.94 MB/s) - 'wordpress-4.9.10.tar.gz' saved [8744264/8744264]

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

Figure 6-31 Downloading WordPress installation package

Run the following command to decompress the WordPress installation package to the `/var/www/html` directory:

```
tar -zxf wordpress-4.9.10.tar.gz -C /var/www/html
```

The command output similar to the following is displayed.

```
wordpress/wp-admin/js/code-editor.min.js
wordpress/wp-admin/js/set-post-thumbnail.js
wordpress/wp-admin/options-permalink.php
wordpress/wp-admin/widgets.php
wordpress/wp-admin/setup-config.php
wordpress/wp-admin/install.php
wordpress/wp-admin/admin-header.php
wordpress/wp-admin/post-new.php
wordpress/wp-admin/themes.php
wordpress/wp-admin/options-reading.php
wordpress/wp-trackback.php
wordpress/wp-comments-post.php
[root@ecs-mp ~]#
```

Figure 6-32 Decompressing the WordPress installation package

Run the following command to grant the read and write permissions to the directory where the file is located:

```
chmod -R 777 /var/www/html
```

```
[root@ecs-mp ~]# chmod -R 777 /var/www/html  
[root@ecs-mp ~]# _
```

Figure 6-33 Granting permissions to the directory

Run the following command to enable httpd:

```
systemctl start httpd.service
```

```
[root@ecs-mp ~]# systemctl start httpd.service  
[root@ecs-mp ~]# _
```

Figure 6-34 Enabling httpd

Run the following command to enable php-fpm:

```
systemctl start php-fpm.service
```

```
[root@ecs-mp ~]# systemctl start php-fpm.service  
[root@ecs-mp ~]# _
```

Figure 6-35 Enabling php-fpm

Run the following command to check the httpd status, which should be active (running) and highlighted:

```
systemctl status httpd
```

```
[root@ecs-mp ~]# 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 Sun 2021-07-18 00:50:10 CST; 30s ago  
    Docs: man:httpd(8)  
          man:apachectl(8)  
 Main PID: 1656 (httpd)  
 Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"  
 CGroup: /system.slice/httpd.service  
         ├─1656 /usr/sbin/httpd -DFOREGROUND  
         ├─1658 /usr/sbin/httpd -DFOREGROUND  
         ├─1659 /usr/sbin/httpd -DFOREGROUND  
         ├─1660 /usr/sbin/httpd -DFOREGROUND  
         ├─1661 /usr/sbin/httpd -DFOREGROUND  
         └─1662 /usr/sbin/httpd -DFOREGROUND  
  
           ecs-mp systemd[1]: Starting The Apache HTTP Server...  
           ecs-mp systemd[1]: Started The Apache HTTP Server.  
[root@ecs-mp ~]#
```

Figure 6-36 Checking the httpd status

Run the following command to check the php-fpm status, which should be active (running) and highlighted:

```
systemctl status php-fpm
```

```
[root@ecs-mp ~]# 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 Sun 2021-07-18 00:50:23 CST; 52s ago
    Main PID: 1669 (php-fpm)
      Status: "Processes active: 0, idle: 5, Requests: 0, slow: 0, Traffic: 0req/sec"
      CGroup: /system.slice/php-fpm.service
              ├─1669 php-fpm: master process (/etc/php-fpm.conf)
              ├─1671 php-fpm: pool www
              ├─1672 php-fpm: pool www
              ├─1673 php-fpm: pool www
              ├─1674 php-fpm: pool www
              └─1675 php-fpm: pool www

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

Figure 6-37 Checking the php-fpm status

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.

```
systemctl enable httpd
```

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

Figure 6-38 Setting httpd to start upon system startup

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.

```
systemctl enable php-fpm
```

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

Figure 6-39 Setting php-fpm to start upon system startup

In the browser, access the EIP bound to the ECS. If the following figure is displayed, LAMP has been installed.

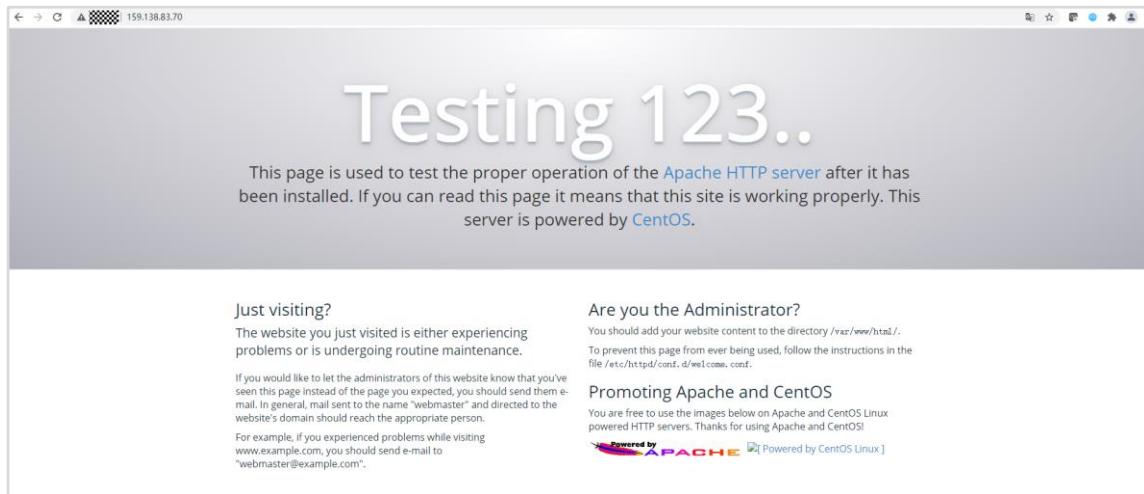


Figure 6-40 Checking environment installation

6.4.2 Creating a Database for WordPress

Go back to the RDS console and click Log In in the Operation column of the created RDS MySQL database instance.

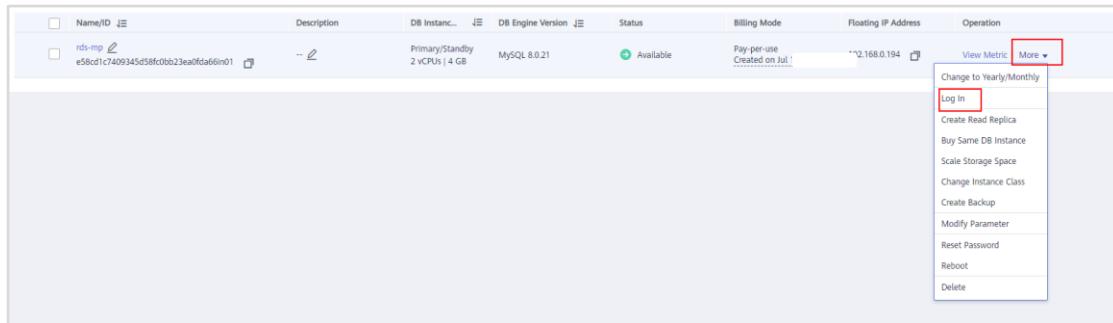


Figure 6-41 Logging in to the DB instance

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.

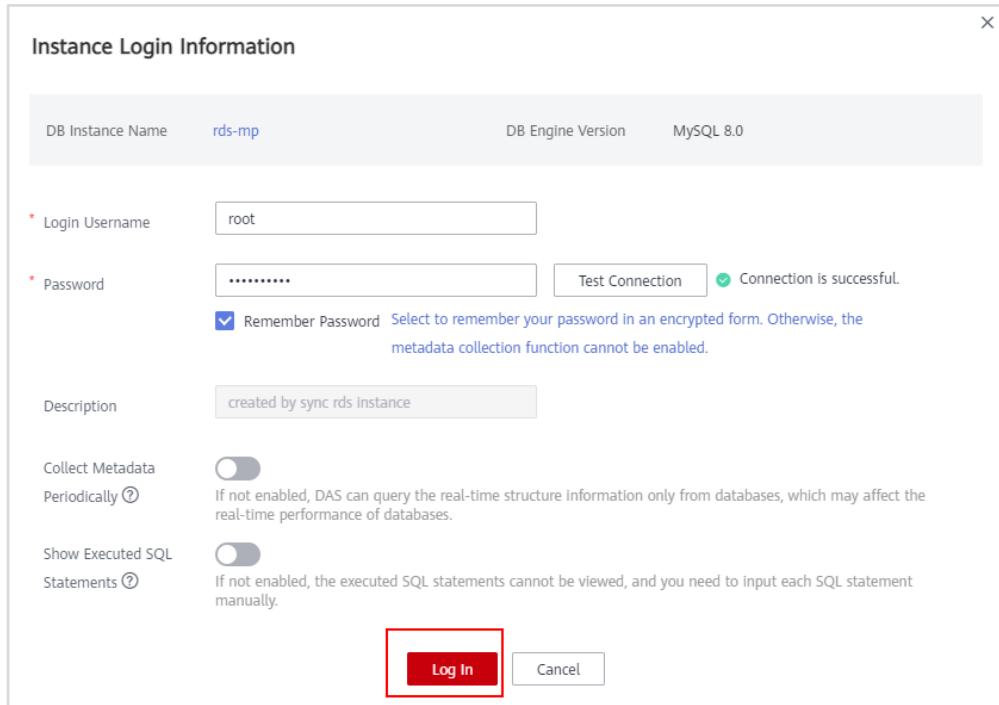


Figure 6-42 Instance Login information

On the top menu bar, choose SQL Operations > SQL Window, as shown in the following figure. Delete the default content in the command line under SQL Window.

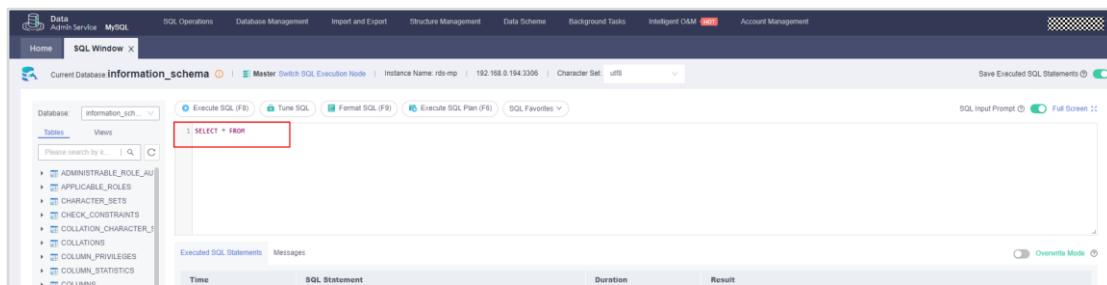


Figure 6-43 Selecting SQL Operations

Enter the following SQL statement and click Execute SQL. If the following information is displayed, the database for WordPress has been created.

```
create database wordpress
```

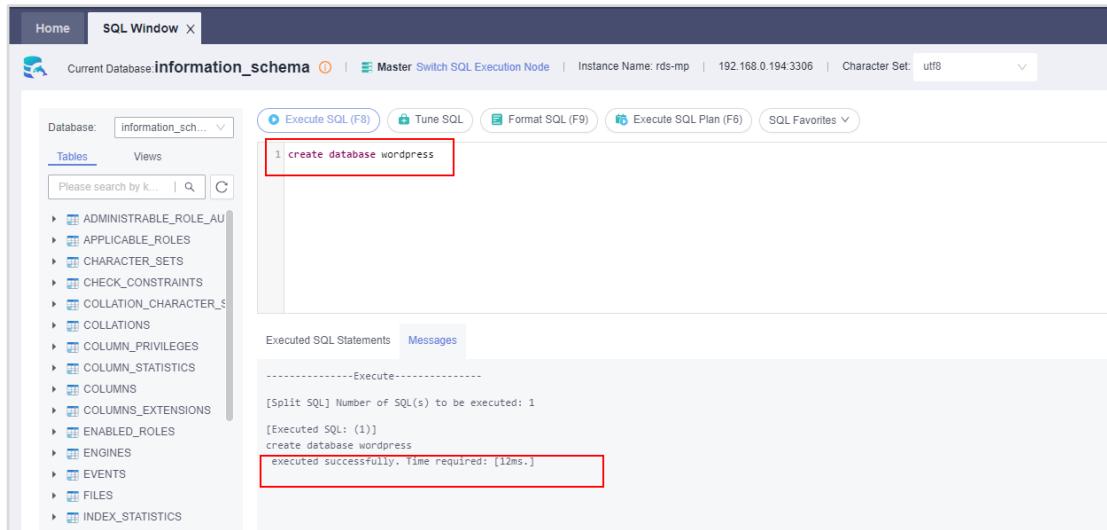


Figure 6-44 Creating a database

6.4.3 Installing WordPress

In the address box of the browser, enter http://ECS_EIP/wordpress to access the WordPress installation wizard.

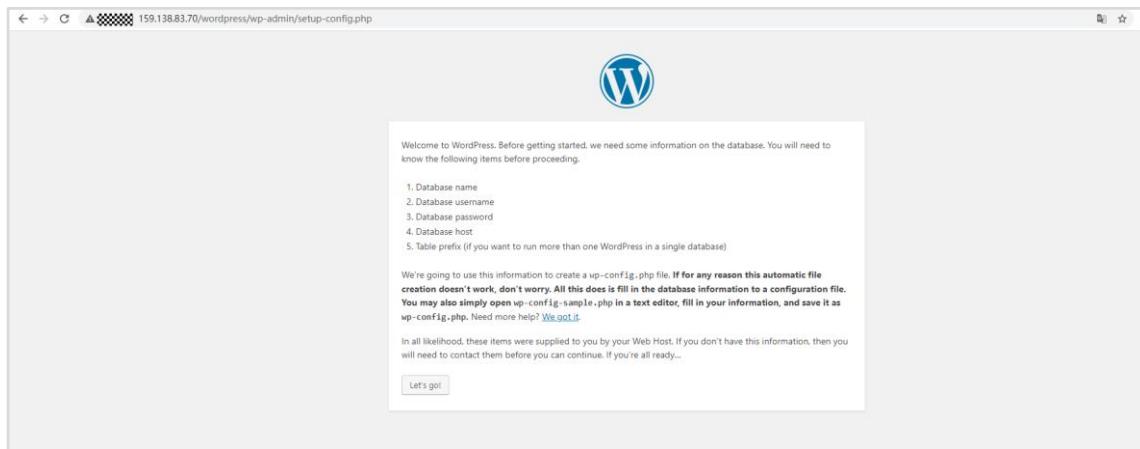
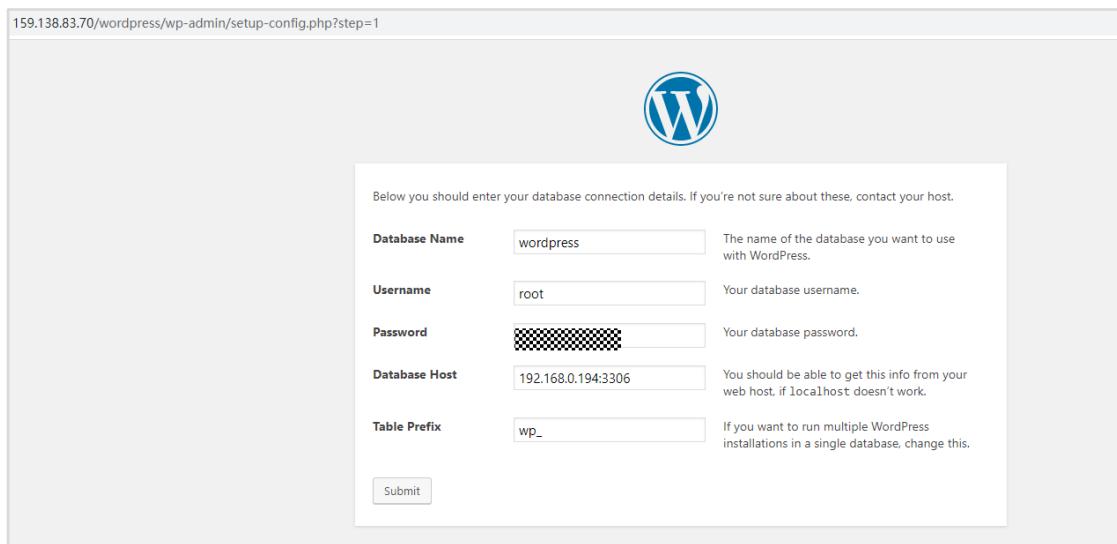


Figure 6-45 Opening the WordPress installation wizard

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.



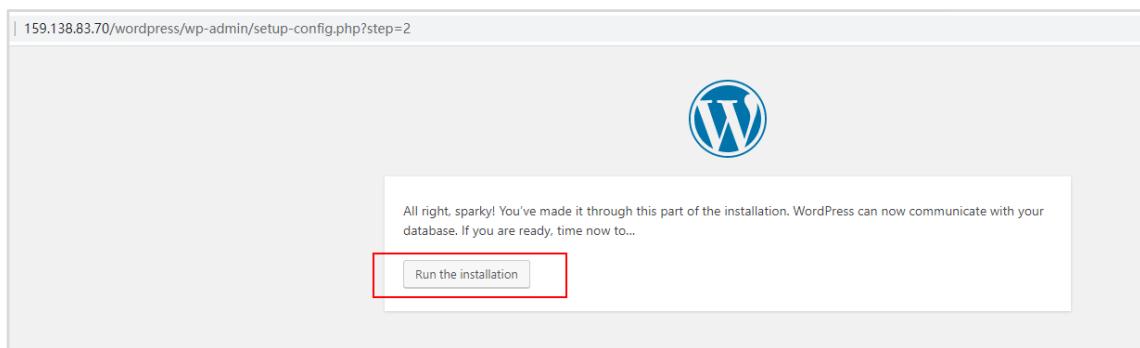
The screenshot shows a web browser window with the URL 159.138.83.70/wordpress/wp-admin/setup-config.php?step=1. At the top, there is a large blue 'W' logo. Below it, a message says: "Below you should enter your database connection details. If you're not sure about these, contact your host." There are four input fields with their respective descriptions:

- Database Name:** wordpress (The name of the database you want to use with WordPress.)
- Username:** root (Your database username.)
- Password:** [REDACTED] (Your database password.)
- Database Host:** 192.168.0.194:3306 (You should be able to get this info from your web host, if localhost doesn't work.)

A "Table Prefix" field contains "wp_". A "Submit" button is at the bottom.

Figure 6-46 Configuring the connection between WordPress and the database

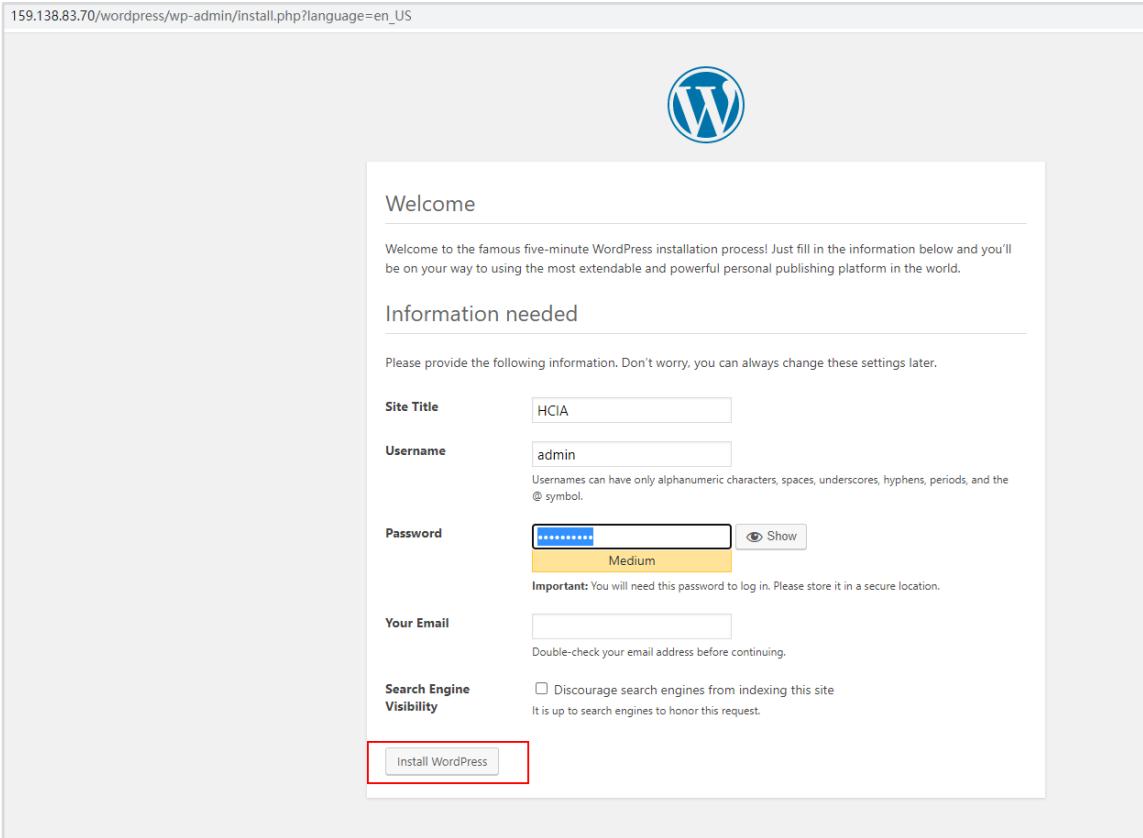
- Click Run the installation.



The screenshot shows a web browser window with the URL 159.138.83.70/wordpress/wp-admin/setup-config.php?step=2. At the top, there is a large blue 'W' logo. Below it, a message says: "All right, sparky! You've made it through this part of the installation. WordPress can now communicate with your database. If you are ready, time now to...". A "Run the installation" button is at the bottom, enclosed in a red rectangular box.

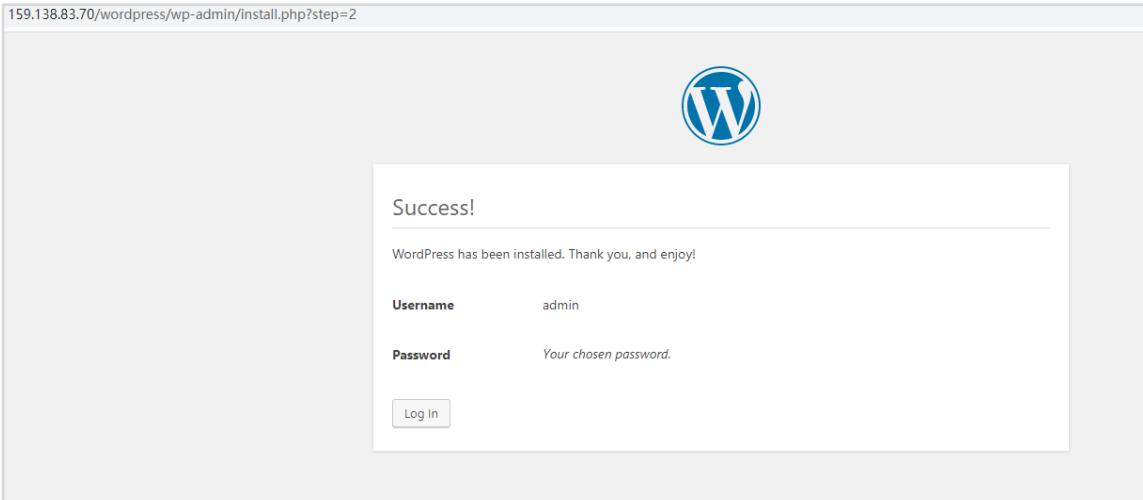
Figure 6-47 Run the installation

- Set Site Title, Username, Password, and Your Email, and click Install WordPress.



The screenshot shows the initial step of the WordPress installation process. At the top, it says "Welcome" and "Information needed". It asks for Site Title (HClA), Username (admin), and Password (a masked password). Below that is "Your Email" and "Search Engine Visibility" (unchecked). A red box highlights the "Install WordPress" button at the bottom.

Figure 6-48 Install WordPress



The screenshot shows the success screen after the installation. It says "Success!" and "WordPress has been installed. Thank you, and enjoy!". It displays the "Username" (admin) and "Password" (Your chosen password). A red box highlights the "Log In" button at the bottom.

Figure 6-49 Installation succeeded

Enter the user name and password on the displayed login page. Then, click Log In.

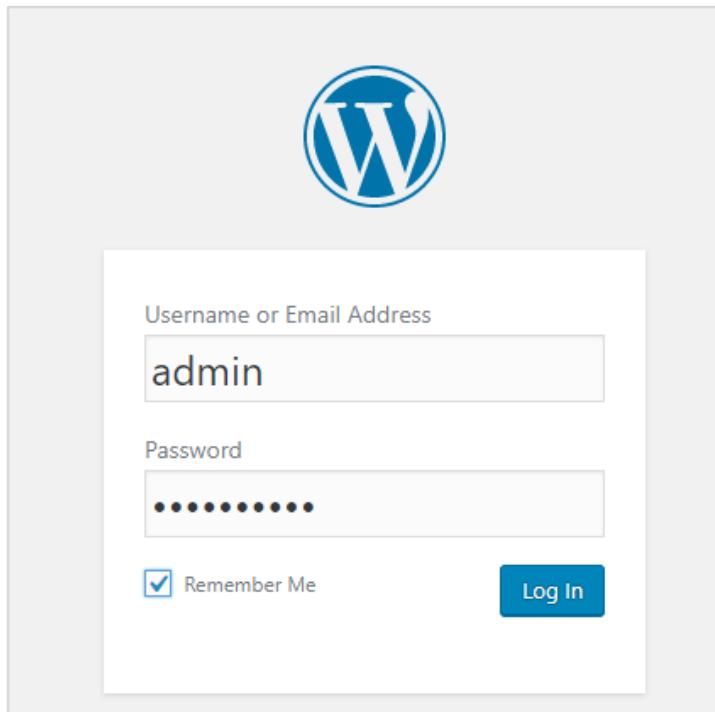


Figure 6-50 Logging in

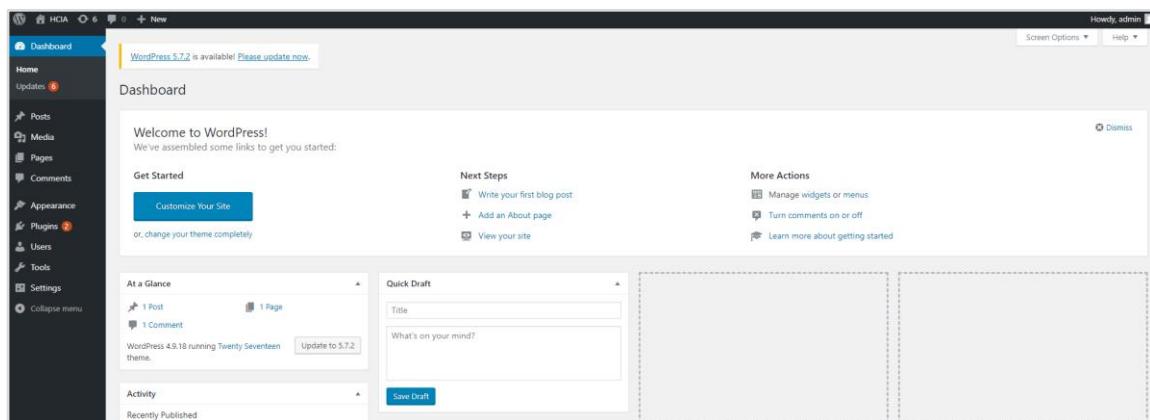


Figure 6-51 Login succeeded

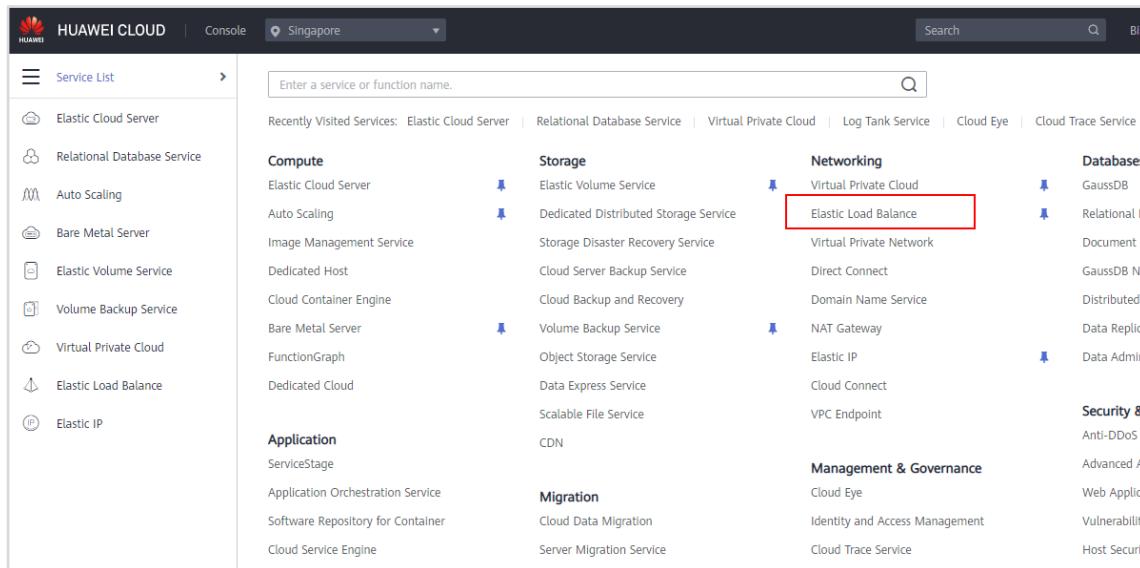
Now the initial configurations of the WordPress website server and its back-end database instance are complete. Next, we will configure ELB and AS for the WordPress website server.

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

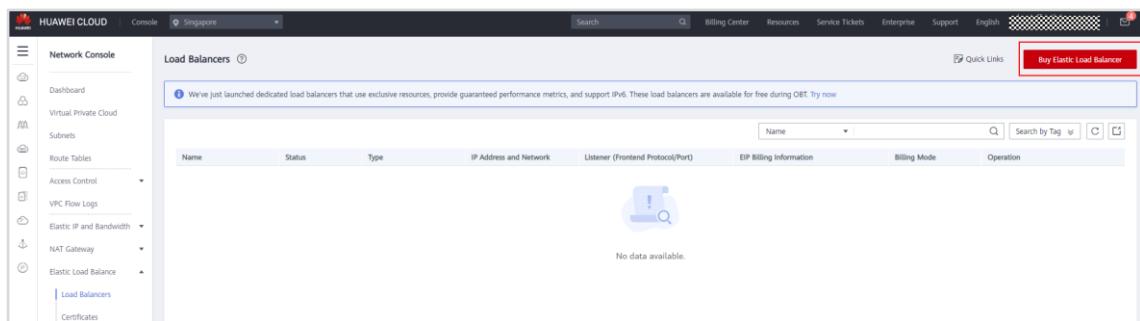
On the management console, hover on the upper left to display Service List and choose Networking > Elastic Load Balance.



The screenshot shows the HUAWEI CLOUD Service List interface. The left sidebar lists services like Compute, Storage, Networking, and Databases. The Networking section is expanded, and the Elastic Load Balance service is highlighted with a red box. Other services in the Networking category include Virtual Private Cloud, Virtual Private Network, Direct Connect, Domain Name Service, NAT Gateway, Elastic IP, Cloud Connect, VPC Endpoint, and Cloud Trace Service. The right side of the interface shows a search bar and various cloud services listed under Compute, Storage, Networking, and Databases categories.

Figure 6-52 Accessing Elastic Load Balance

Click Buy Elastic Load Balancer.

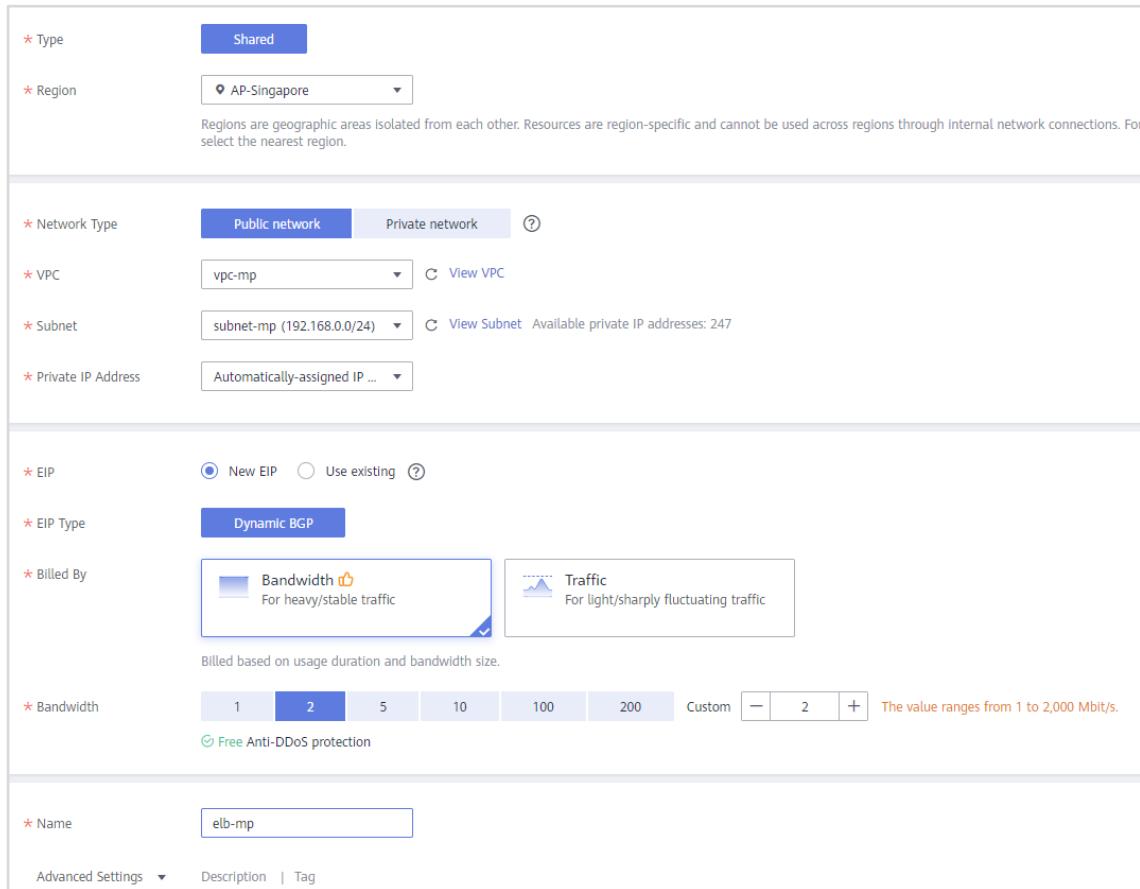


The screenshot shows the HUAWEI CLOUD Network Console with the Load Balancers page. The left sidebar includes options like Dashboard, Subnets, Route Tables, Access Control, VPC Flow Logs, Elastic IP and Bandwidth, NAT Gateway, and Load Balancers. The Load Balancers page displays a table with columns: Name, Status, Type, IP Address and Network, Listener (Frontend Protocol/Port), IP Billing Information, Billing Mode, and Operation. A message at the top states, "We've just launched dedicated load balancers that use exclusive resources, provide guaranteed performance metrics, and support IPv6. These load balancers are available for free during Q1. Try now." A red box highlights the "Buy Elastic Load Balancer" button in the top right corner of the page.

Figure 6-53 Buy Elastic Load Balancer

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:** New EIP, Dynamic BGP, 2 Mbit/s
- **Name:** elb-mp (Change it as needed.)



The screenshot shows a multi-step configuration interface for creating a new Elastic IP (EIP) on the HUAWEI CLOUD. The steps are as follows:

- Step 1: Basic Configuration**
 - Type:** Shared
 - Region:** AP-Singapore
- Step 2: Network Configuration**
 - Network Type:** Public network
 - VPC:** vpc-mp
 - Subnet:** subnet-mp (192.168.0.0/24)
 - Private IP Address:** Automatically-assigned IP ...
- Step 3: EIP Configuration**
 - EIP:** New EIP
 - EIP Type:** Dynamic BGP
 - Billed By:** Bandwidth (selected) - For heavy/stable traffic. An alternative option is Traffic (For light/sharply fluctuating traffic).
 - Bandwidth:** 2 Mbit/s (selected from a dropdown menu ranging from 1 to 2,000 Mbit/s). A note indicates: "Billed based on usage duration and bandwidth size." An option for "Free Anti-DDoS protection" is checked.
- Step 4: Name Configuration**
 - Name:** elb-mp

Figure 6-54 Configuring parameters

Confirm the configuration and submit your request.

| Resource | Configuration | Billing Mode | Quantity | Subtotal |
|-----------------------|----------------|----------------------------|----------|------------------|
| Elastic load balancer | Region | Singapore | 1 | Free |
| | Name | elb-mp | | |
| | Network Type | Public network | | |
| | VPC | vpc-mp | | |
| | Type | Shared | | |
| | Subnet | subnet-mp (192.168.0.0/24) | | |
| | Tag | -- | | |
| EIP | Description | -- | 1 | Free |
| | EIP Type | Dynamic BGP | | |
| Bandwidth | Bandwidth Size | 2 Mbit/s | 1 | \$0.048 USD/hour |
| | Billed By | Bandwidth | | |

Figure 6-55 Confirming the configuration

Go back to the load balancer list and ensure that the load balancer is in the Running state.

| Name | Status | Type | IP Address and Network | Listener (Frontend Protocol/Port) | EIP Billing Information | Billing Mode | Operation |
|--------|---------|--------|---|-----------------------------------|-------------------------|--------------|------------------------------------|
| elb-mp | Running | Shared | 192.168.0.33 (Private IP address) vpc-mp (VPC) | Add listener | -- | -- | Modify Bandwidth Delete More ▾ |

Figure 6-56 Viewing the load balancer

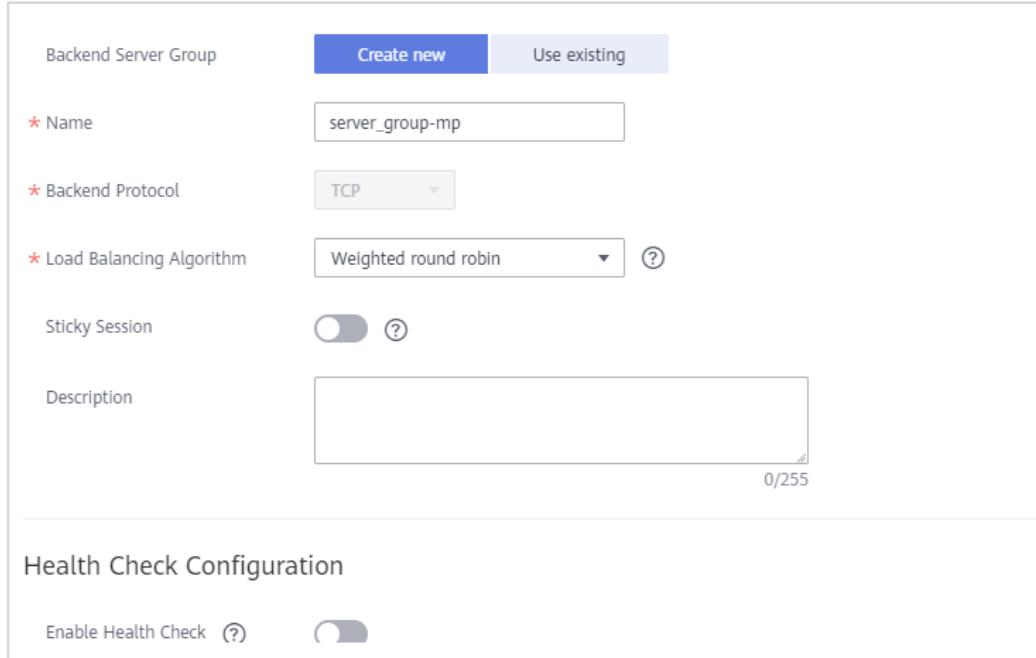
Click the name of the load balancer. Under Listeners, click Add Listener. Configure the name, protocol, and port for the listener.

The screenshot shows the 'Add Listener' dialog box for a load balancer named 'elb-mp'. The 'Listeners' tab is selected in the navigation bar. The dialog has three steps: 1) Configure Listener, 2) Configure Backend Server Group, and 3) Finish. Step 1 is active. The 'Name' field contains 'listener-mp'. The 'Frontend Protocol/Port' dropdown shows 'TCP' with port '80' selected. A note below says 'Select TCP or UDP for load balancing at Layer 4. Select HTTP or HTTPS for load balancing at Layer 7. When HTTPS is selected, the backend protocol can only be HTTP.' The 'Advanced Settings' section is collapsed. At the bottom right are 'Cancel' and 'Next' buttons.

Figure 6-57 Adding a listener

Click Next, configure the backend server group, and click Finish.

- **Name:** listener-mp (Change it as needed.)
- **Health Check:** disabled
- Remain the default settings for other parameters.



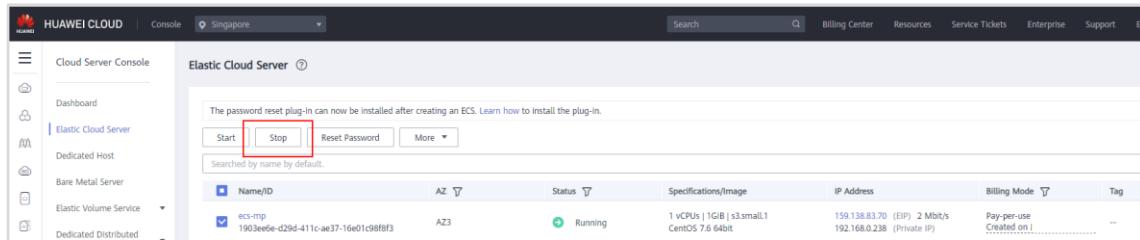
The screenshot shows the 'Backend Server Group' configuration page. At the top, there are two buttons: 'Create new' (highlighted in blue) and 'Use existing'. Below these are fields for 'Name' (set to 'server_group-mp'), 'Backend Protocol' (set to 'TCP'), and 'Load Balancing Algorithm' (set to 'Weighted round robin'). A 'Sticky Session' toggle switch is turned off. A 'Description' text area is present but empty. In the 'Health Check Configuration' section, the 'Enable Health Check' toggle switch is turned off. The bottom right corner of the text area shows '0/255'.

Figure 6-58 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

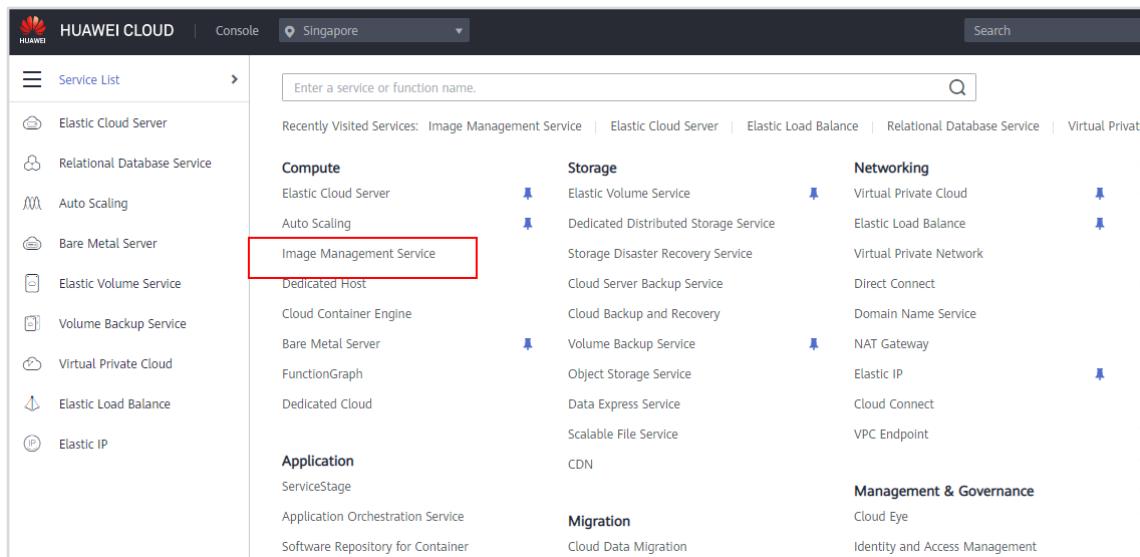
Go back to the ECS console, locate the ECS you created, and choose More > Stop in the Operation column.



The screenshot shows the HUAWEI CLOUD console interface for the Elastic Cloud Server service. In the center, there is a table listing an ECS instance. The first column contains checkboxes, the second column is 'Name/ID' with 'ecs-mp' checked, the third is 'AZ' with 'AZ3' selected, the fourth is 'Status' with 'Running' indicated by a green circle, the fifth is 'Specifications/Image' showing '1 vCPU | 1GB | s3.small.1 CentOS 7.6 64bit', and the sixth is 'IP Address' with '159.138.83.70 (EIP) 2 Mbit/s 192.168.0.238 (Private IP)'. At the top of the table, there are buttons for 'Start', 'Stop', 'Reset Password', and 'More'. The 'Stop' button is highlighted with a red box.

Figure 6-59 Stopping the ECS

Go back to the service list. Under Compute, click Image Management Service.

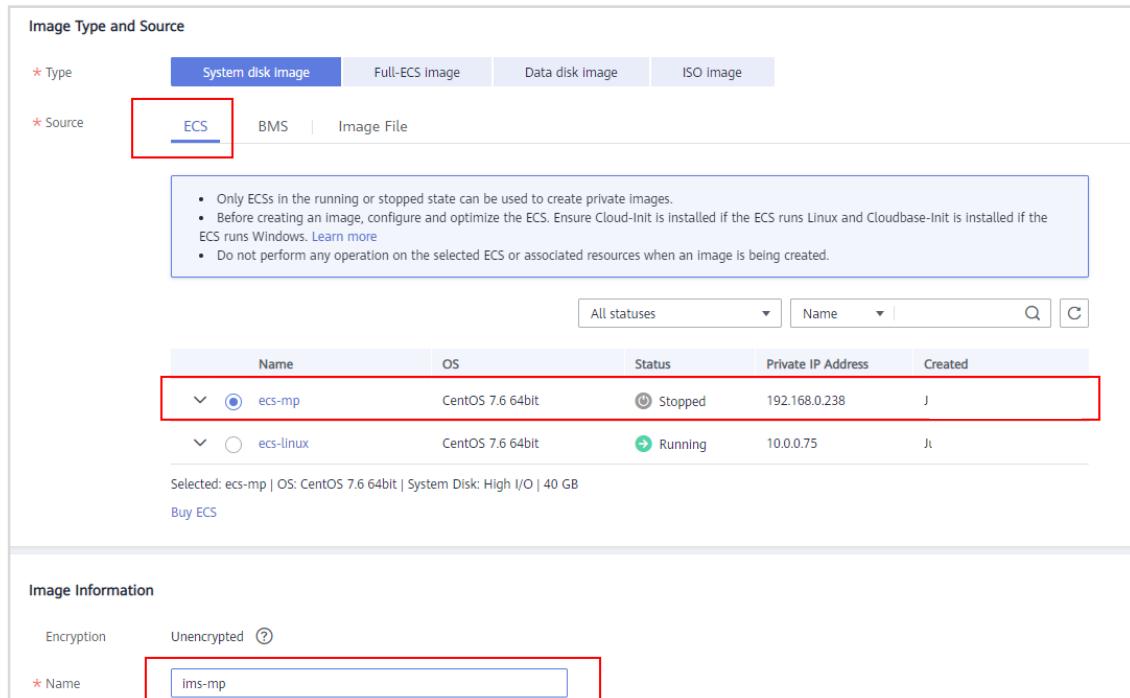


The screenshot shows the HUAWEI CLOUD Service List interface. On the left, there is a sidebar with various service icons. Under the 'Compute' section, the 'Image Management Service' is highlighted with a red box. The main area displays a grid of services categorized into Compute, Storage, Networking, Application, Migration, and Management & Governance. Some services have blue edit icons next to them.

Figure 6-60 Accessing Image Management Service

Click Create Image and configure the parameters as follows:

- **Type:** System disk image
- **Source:** the ECS you created
- **Name:** ims-mp (Change it as needed.)

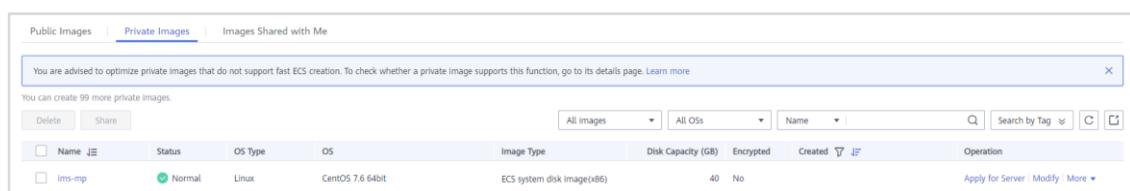


The screenshot shows the 'Image Type and Source' step of a 'Create Image' wizard. The 'Type' dropdown is set to 'System disk image'. The 'Source' dropdown is set to 'ECS', which is highlighted with a red box. Below the source dropdown is a note: 'Only ECSS in the running or stopped state can be used to create private images. Before creating an Image, configure and optimize the ECS. Ensure Cloud-Init is installed if the ECS runs Linux and Cloudbase-Init is installed if the ECS runs Windows. Learn more. Do not perform any operation on the selected ECS or associated resources when an image is being created.' The main table lists two ECS instances: 'ecs-mp' (selected, stopped, 192.168.0.238) and 'ecs-linux' (running, 10.0.0.75). The 'Name' field in the 'Image Information' section is highlighted with a red box and contains 'ims-mp'.

Figure 6-61 Configuring parameters

Click Next, confirm the configuration, and click Submit.

Wait until the image status becomes Normal. Then, switch back to the ECS console, and start the ECS.

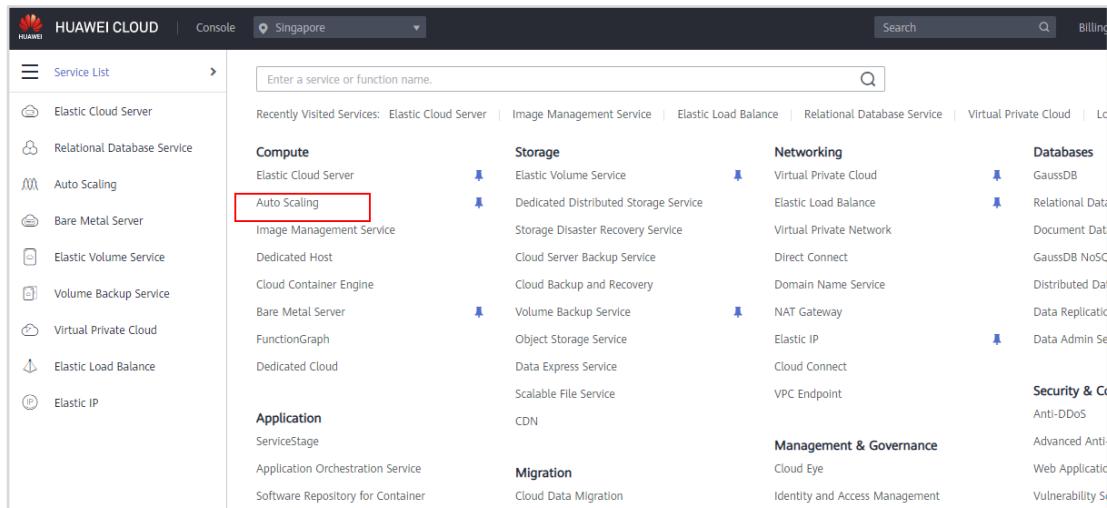


The screenshot shows the 'Private Images' page. It displays a table of images, with one row selected: 'ims-mp' (Status: Normal, OS Type: Linux, OS: CentOS 7.6 64bit, Image Type: ECS system disk image(x86), Disk Capacity (GB): 40, Encrypted: No). The 'Status' column for 'ims-mp' is highlighted with a green circle indicating 'Normal'.

Figure 6-62 Viewing the created image

6.5.3 Configuring AS

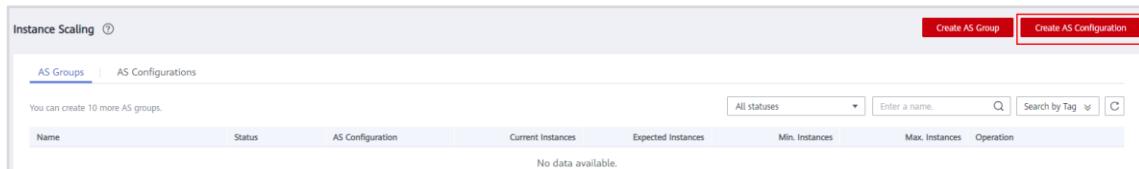
Go back to the service list. Under Compute, click Auto Scaling.



The screenshot shows the HUAWEI CLOUD Service List interface. On the left, there's a sidebar with various service icons and names. In the center, there are several categories of services: Compute, Storage, Networking, Databases, Application, Migration, Management & Governance, and Security & Compliance. The 'Compute' category is expanded, showing sub-services like Elastic Cloud Server, Auto Scaling, Bare Metal Server, etc. The 'Auto Scaling' service is highlighted with a red box. At the top, there's a search bar and a location dropdown set to 'Singapore'. The top right has 'Search' and 'Billing' buttons.

Figure 6-63 Accessing Auto Scaling

Click Create AS Configuration.



The screenshot shows the 'Instance Scaling' page. At the top, there are two red buttons: 'Create AS Group' and 'Create AS Configuration'. Below them is a navigation bar with tabs for 'AS Groups' and 'AS Configurations', with 'AS Groups' currently selected. A message says 'You can create 10 more AS groups.' There are several filter and search options at the top right. The main area is a table with columns: Name, Status, AS Configuration, Current Instances, Expected Instances, Min. Instances, Max. Instances, and Operation. A note at the bottom says 'No data available.'

Figure 6-64 Create AS Configuration

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.

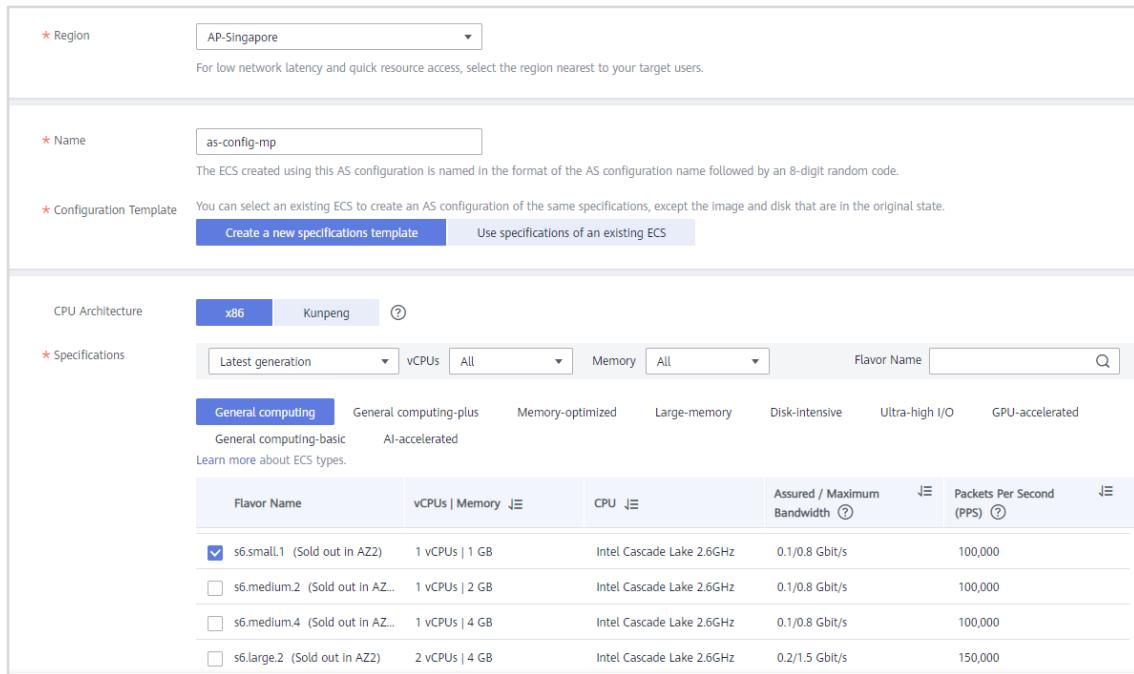


Figure 6-65 Configuring parameters

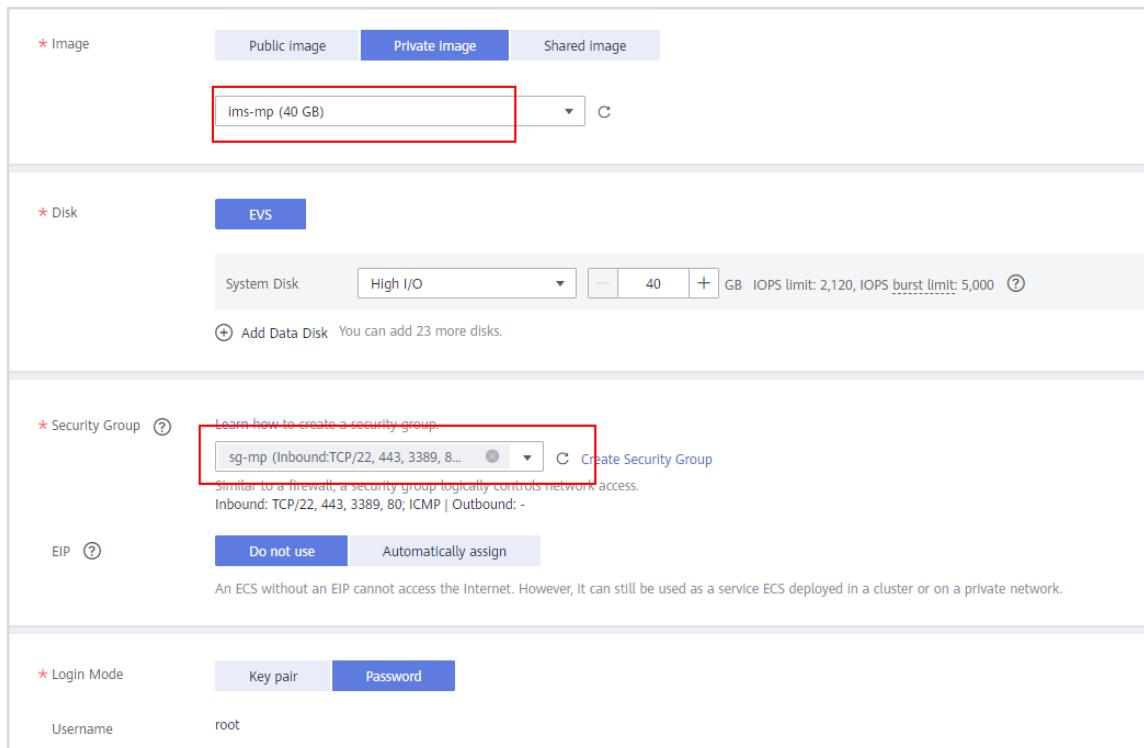


Figure 6-66 Configuring parameters

View the created AS configuration.

| AS Groups | | AS Configurations | | | | | | | |
|--------------|---------|-----------------------------|--------|------------------|------------|------------|---------------------------|--------------|---|
| Name | Status | Specifications | Image | System Disk | Data Disks | Login Mode | Created | Billing Mode | Operation |
| as-config-mp | Unbound | s6.small.1 1 vCPUs 1 GB | lms-mp | High I/O 40 GB | 0 | Password | Jul 18, 2021 02:29:28 ... | Pay-per-use | Copy Delete |

Figure 6-67 Viewing the AS configuration

Click Create AS Group.

| Instance Scaling | | | | | | | | Create AS Group | Create AS Configuration | |
|-----------------------------------|--------|-------------------|-------------------|--------------------|----------------|----------------|-----------|---------------------------------|---|---------------|
| AS Groups | | AS Configurations | | | | | | | | |
| You can create 10 more AS groups. | | | | | | | | All statuses | Enter a name | Search by Tag |
| Name | Status | AS Configuration | Current Instances | Expected Instances | Min. Instances | Max. Instances | Operation | | | |
| No data available. | | | | | | | | | | |

Figure 6-68 Create AS Group

Configure the parameters as shown in the following figure.

Region: AP-Singapore

AZ: AZ1, AZ2, AZ3

Multi-AZ Extension Policy: Load-balanced

Name: as-group-mp

Max. Instances: 3

Expected Instances: 2

Min. Instances: 1

Figure 6-69 Configuring parameters

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.

*** AS Configuration**: as-config-mp

*** VPC**: vpc-mp (192.168.0.0/16) [Create VPC](#)

*** Subnet**: subnet-mp (192.168.0.0/24) [Create Subnet](#)

Load Balancing: [Elastic load balancer](#) [Create ELB](#)

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

| | | | |
|---------------|---------------------|-------------------|---------------------|
| Load Balancer | elb-mp (d43a2bc...) | Backend ECS Group | server_group-mp ... |
| Backend Port | 80 | Weight | 1 |

[Add Load Balancer](#) You can add 5 more load balancers.

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

EIP: [Release](#) [Do not release](#)
If you select Release, EIPs bound to ECSSs are released when the ECSSs are removed from the AS group. Otherwise, EIPs will only be unbound from the ECSSs.

Data Disk: [Release](#) [Do not release](#)
If you select Release, data disks attached to ECSSs are deleted when the ECSSs are removed from the AS group. Otherwise, data disks will only be detached from the ECSSs.

*** Health Check Method**: ELB health check
When a protected instance is detected to be abnormal in a health check, AS removes the instance from the AS group and creates a new one. Ensure that the rule of the target security group allows packets from the port with IP address 100.125.0.0/16 to pass. Additionally, configure the protocol and port number for the load balancer. Otherwise, the health check will fail. [Learn more](#)

*** Health Check Interval**: 5 minutes

*** Health Check Grace Period (s)**: 600

Figure 6-70 Configuring parameters

Locate the AS group you created and click View AS Policy in the Operation column.

| AS Groups | AS Configurations | | | | | | |
|-------------|-------------------|------------------|-------------------|--------------------|----------------|----------------|---|
| Name | Status | AS Configuration | Current Instances | Expected Instances | Min. Instances | Max. Instances | Operation |
| as-group-mp | Enabled | as-config-mp | 0 | 2 | 1 | 3 | View AS Policy Disable More ▾ |

Figure 6-71 View AS Policy

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

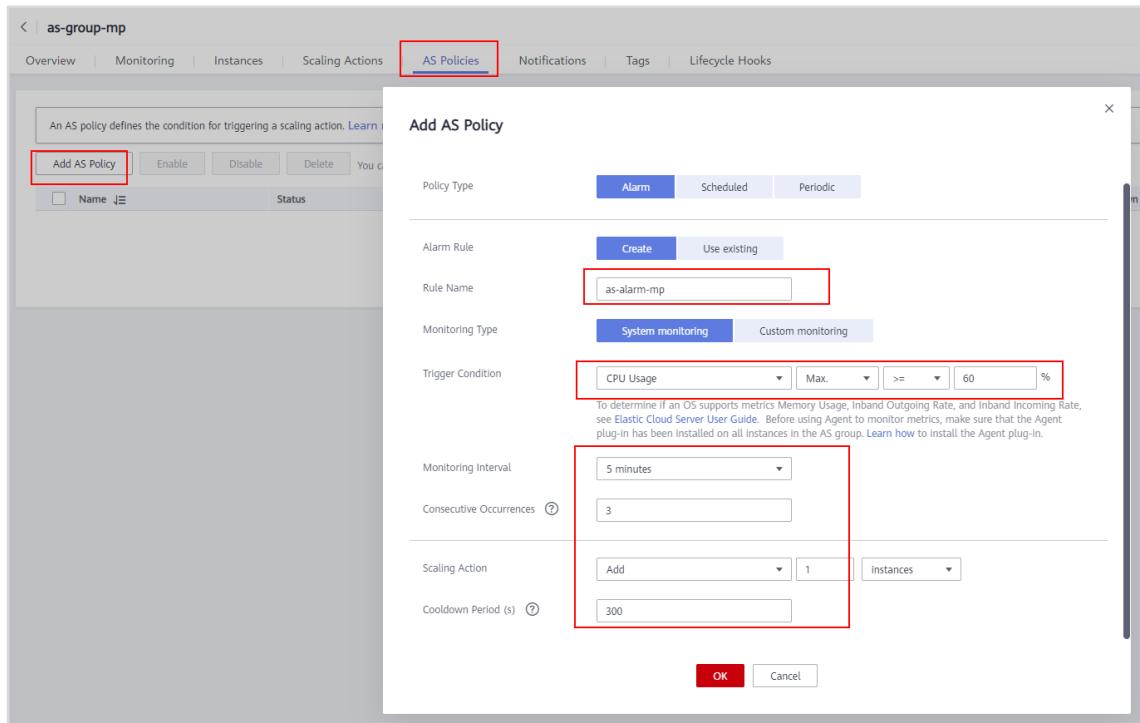


Figure 6-72 Add AS policy

Add AS Policy

| | |
|---|---|
| Policy Name | as-policy-mp2 |
| Policy Type | Alarm |
| Alarm Rule | Create |
| Rule Name | as-alarm-mp2 |
| Monitoring Type | System monitoring |
| Trigger Condition | CPU Usage Avg. <= 20 % To determine if an OS supports metrics Memory Usage, Inband Outgoing Rate, and Inband Incoming Rate, see Elastic Cloud Server User Guide . Before using Agent to monitor metrics, make sure that the Agent plug-in has been installed on all instances in the AS group. Learn how to install the Agent plug-in. |
| Monitoring Interval | 5 minutes |
| Consecutive Occurrences | 3 |
| Scaling Action | Reduce 1 instances |
| Cooldown Period (s) | 300 |
| <button>OK</button> <button>Cancel</button> | |

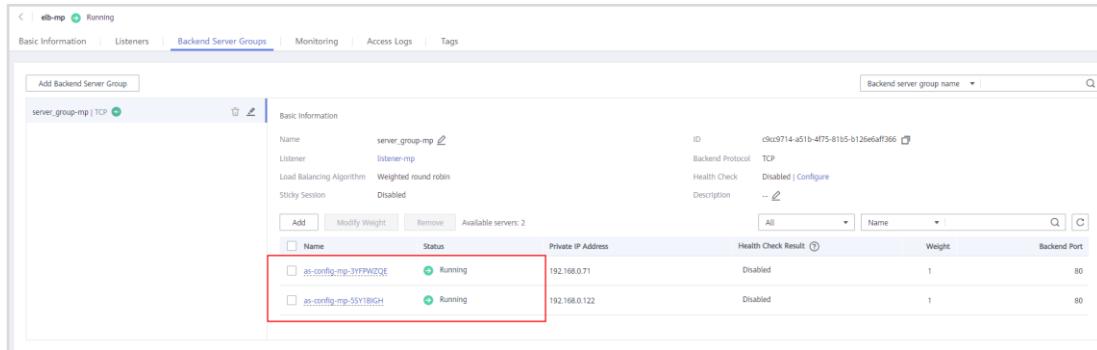
Figure 6-73 Adding an AS policy

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.

| Name | Lifecycle Status | Health Status | AS Configuration | Instance Add Mode | Instance Protection | Added | Operation |
|-----------------------|------------------|---------------|------------------|-------------------|---------------------|-------|--|
| as-config-mp-3YFPWZQE | Enabled | Normal | as-config-mp | Automatic | Off | | Remove Remove and Delete |
| as-config-mp-5SY1BIGH | Enabled | Normal | as-config-mp | Automatic | Off | | Remove Remove and Delete |

Figure 6-74 Viewing instance changes

Switch back to the ELB console and click the load balancer name, elb-mp. Locate the backend server group associated with the load balancer and view the two ECSs added by the AS service.



| Name | Status | Private IP Address | Health Check Result | Weight | Backend Port |
|-----------------------|---------|--------------------|---------------------|--------|--------------|
| as-config-mp-3YFPWZQE | Running | 192.168.0.71 | Disabled | 1 | 80 |
| as-config-mp-55Y1BGH | Running | 192.168.0.122 | Disabled | 1 | 80 |

Figure 6-75 Viewing the backend server group

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

In the address box of the browser on your PC, enter `http://Load balancer's EIP/wordpress/`, and press Enter.



Figure 6-76 Visiting the website

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.

Monitoring Resources

On the service list page, choose Management & Governance > Cloud Eye.

The screenshot shows the HUAWEI CLOUD Service List interface. On the left, there's a sidebar with icons for various services: Elastic Cloud Server, Relational Database Service, Auto Scaling, Bare Metal Server, Elastic Volume Service, Volume Backup Service, Virtual Private Cloud, and Elastic Load Balance. The main area is titled 'Management & Governance' and contains a single item: 'Cloud Eye'. A red box highlights the 'Cloud Eye' section.

Figure 6-77 Accessing Cloud Eye

On the Overview page, view overall resource information and alarm statistics.

The screenshot shows the HUAWEI CLOUD Cloud Eye Overview page. The left sidebar includes options like Dashboard, Resource Groups, Alarm Management (with 'Server Monitoring' selected), and Event Monitoring. The main area has sections for 'Resource Overview' (showing 1 out of 30 resources have alarms), 'Alarm Statistics' (a line chart showing the number of alarms over time), and a 'Breakdown' table for critical, major, minor, and informational alarms. A red box highlights the 'Resource Overview' section.

Figure 6-78 Resource Overview

In the left navigation pane, choose Alarm Management > Alarm History. View service alarms and handle any faults in a timely manner.

The screenshot shows the HUAWEI CLOUD Cloud Eye Alarm History page. The left sidebar has 'Alarm History' selected under 'Alarm Management'. The main table lists five alarm entries with columns for Alarm Rule Name, Alarm Generated, Resource Type, Abnormal Resource, Alarm Policy, Alarm Severity, and Status. A red box highlights the 'Alarm History' section in the sidebar.

| Alarm Rule Name | Alarm Generated | Resource Type | Abnormal Resource | Alarm Policy | Alarm Severity | Status |
|-----------------|-----------------|----------------------|--|---|----------------|--------|
| as-alarm-mp | -- | Auto Scaling | as-group-mp fc00ea48-f1c7-41f7-b424-f254fe8cad6 | Trigger an alarm if CPU Usage Max... for 3 consecutive periods of 5 minut... Trigger the alarm only once even th... | Major | OK |
| as-alarm-mp2 | -- | Auto Scaling | as-group-mp fc00ea48-f1c7-41f7-b424-f254fe8cad6 | Trigger an alarm if CPU Usage Avg... for 3 consecutive periods of 5 minut... Trigger the alarm only once even th... | Major | OK |
| alarm-test | -- | Elastic Cloud Server | ecs-1f447247-3416-44d9-8261-dccb434b1415 | Trigger an alarm if (Agent) CPU Usa... for 3 consecutive periods. Trigger an alarm every 5 minutes ag... | Major | Alarm |
| alarm-test | -- | Elastic Cloud Server | ecs-1f447247-3416-44d9-8261-dccb434b1415 | Trigger an alarm if (Agent) CPU Usa... for 3 consecutive periods. Trigger an alarm every 5 minutes ag... | Major | Alarm |
| | | | ecs-1f447247-3416-44d9-8261-dccb434b1415 | Trigger an alarm if (Agent) CPU Usa... | | |

Figure 6-79 Viewing alarm history

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 Usage | Memory Usage | Disk Usage | Operation |
|--|---|------------|--------------|-----------|--------------|------------|---|
| ecs-mp 1903ee6e-d29d-411c-a337-16e01c98fbf3 | 199.139.83.70 (IP) 192.168.0.238 (Private) | Running | Running | 1.02% | 34.87% | 6.42% | View Metric Create Alarm Rule |

Figure 6-80 Server Monitoring

Click the name of an ECS to view its monitoring details.

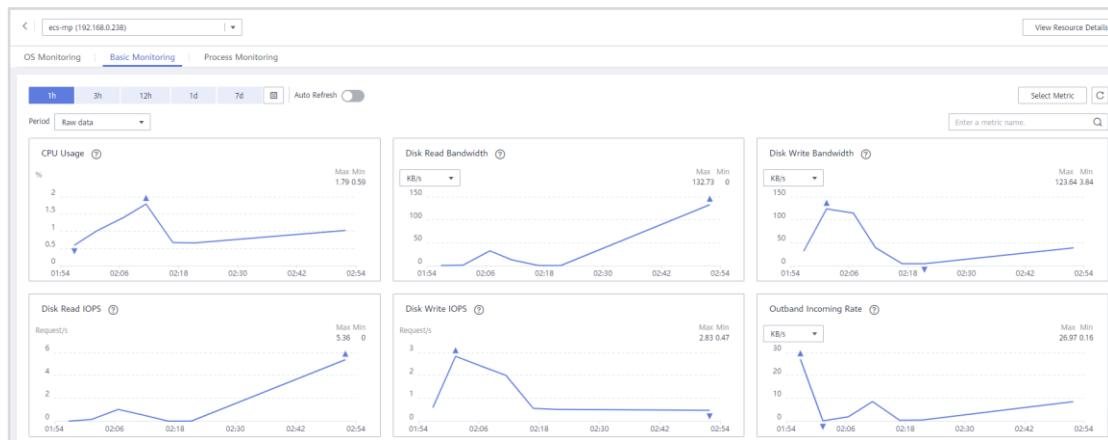


Figure 6-81 Basic Monitoring

6.7 Deleting Resources

6.7.1 Deleting ECSs

Select the ECSs you want to delete and click Delete.

The screenshot shows the 'Elastic Cloud Server' section of the Cloud Server Console. A dropdown menu for an ECS named 'ecs-mp' has been opened, and the 'Delete' option is highlighted with a red box. Below the dropdown, a table lists three running ECS instances:

| Status | Specifications/Image | IP Address | Billing Mode | Tag | Operation |
|---------|---|---|---|-----|---|
| Running | 1 vCPU 1GB s5.small,1 ims-mp | 192.168.0.71 (Private IP) | Pay-per-use Created on Jul 18, 2021 02:54:47 | -- | Remote Login More |
| Running | 1 vCPU 1GB s5.small,1 ims-mp | 192.168.0.122 (Private IP) | Pay-per-use Created on Jul 18, 2021 02:54:47 | -- | Remote Login More |
| Running | 1 vCPU 1GB s5.small,1 CentOS 7.6 (64bit) | 199.139.83.70 (IP), 2 MPEOs 192.168.0.238 (Private IP) | Pay-per-use Created on Jul 18, 2021 01:54:47 | -- | Remote Login More |

Figure 6-82 Deleting ECSs

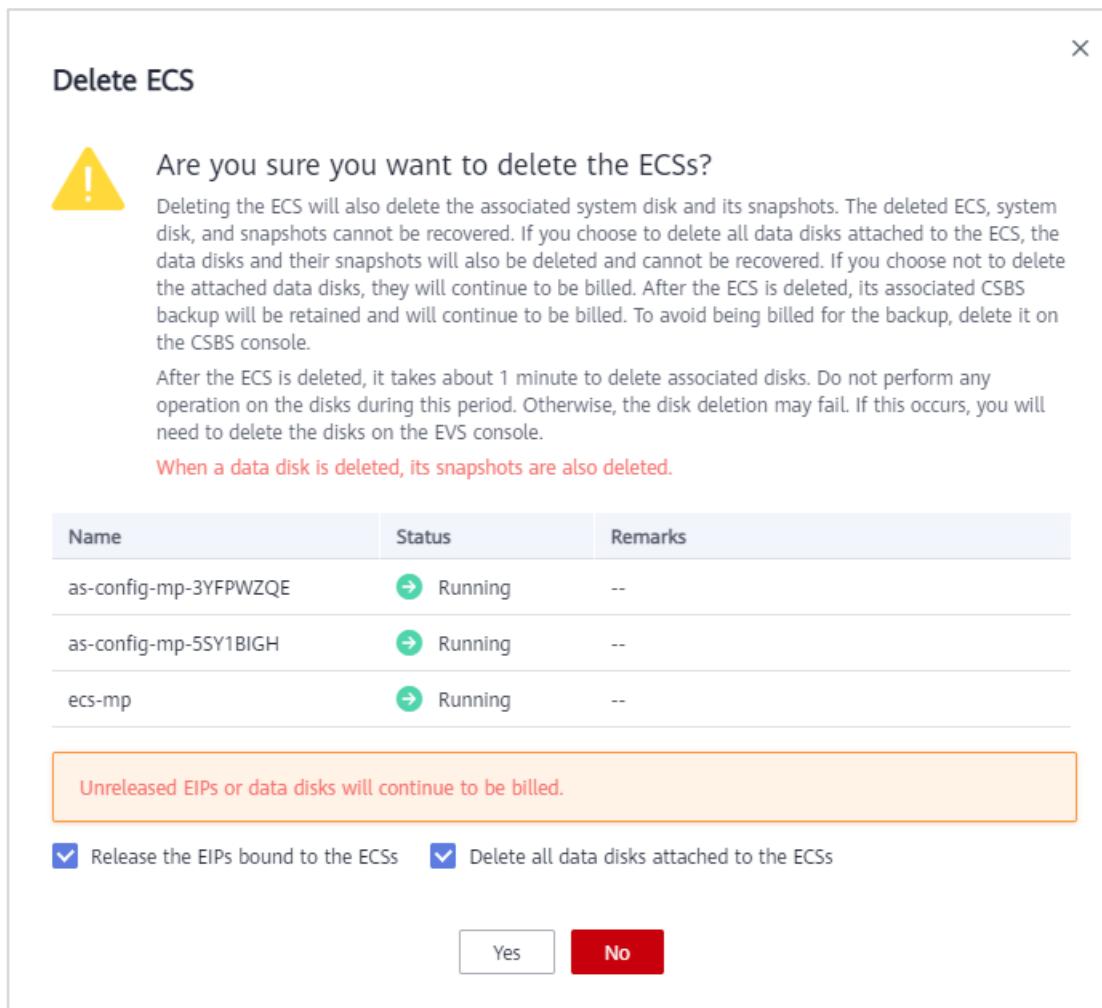


Figure 6-83 Confirming the deletion

6.7.2 Deleting the RDS DB Instance

On the service list page, choose Database > Relational Database Service.

Locate the RDS DB instance you want to delete and click Delete in the Operation column.

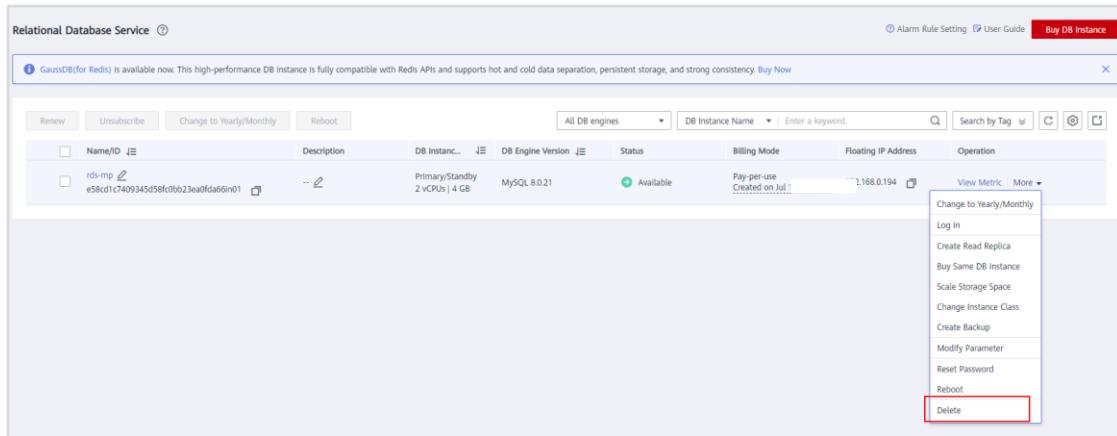


Figure 6-84 Deleting the RDS DB instance

6.7.3 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.

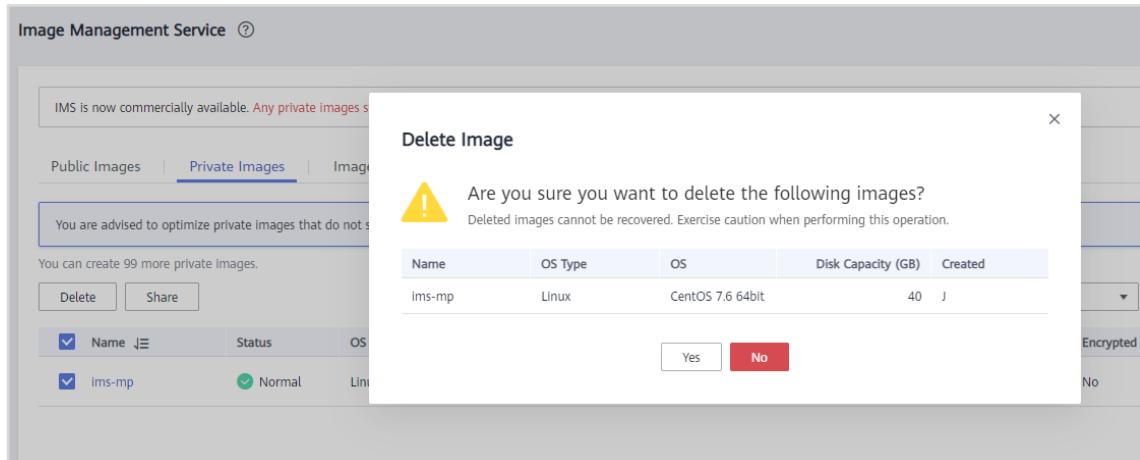


Figure 6-85 Deleting the private image

6.7.4 Deleting the Load Balancer

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.

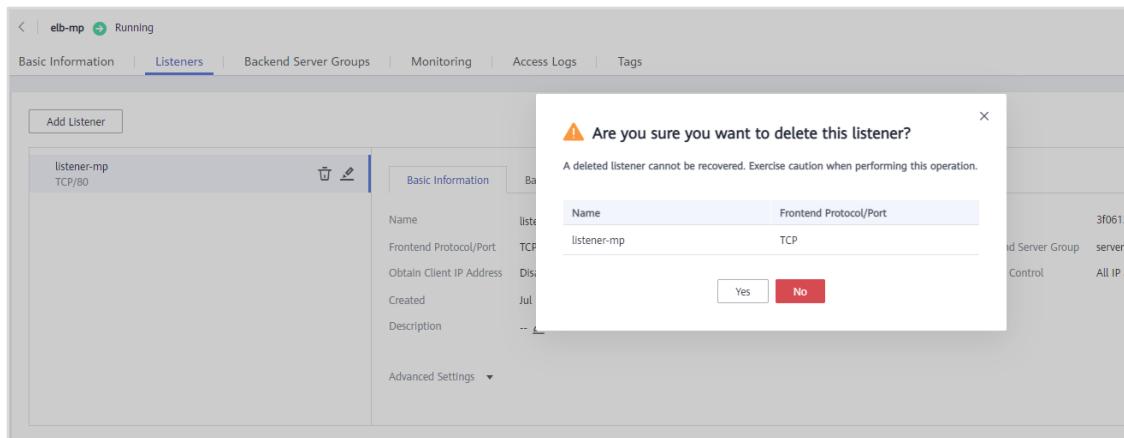


Figure 6-86 Deleting the listener

Locate the load balancer and click Delete. In the displayed dialog box, click Yes.



Figure 6-87 Deleting the load balancer

6.7.5 Deleting AS Resources

Locate the AS group you want to delete and click Delete. In the displayed dialog box, click Yes.

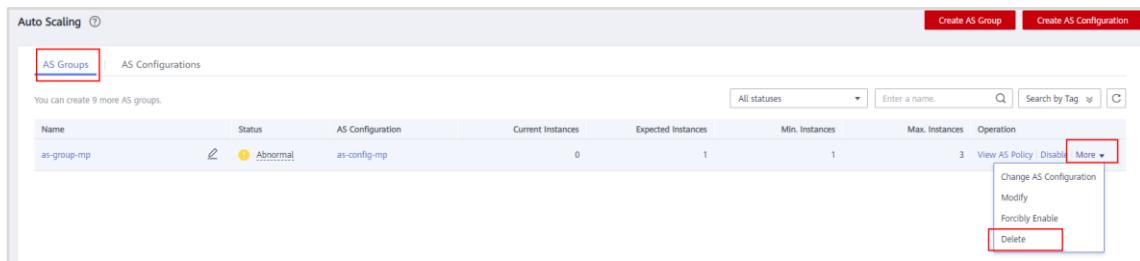


Figure 6-88 Deleting the AS group

Locate the AS configuration you want to delete and click Delete. In the displayed dialog box, click Yes.

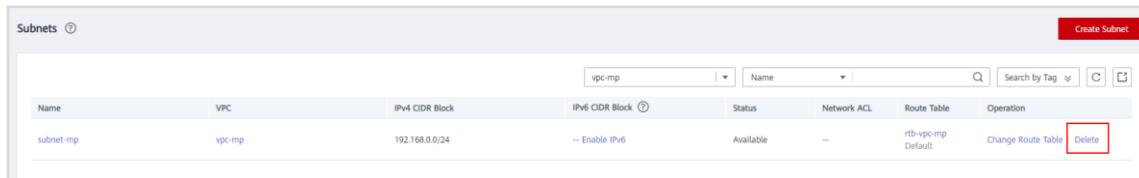


| Name | Status | Specifications | Image | System Disk | Data Disks | Login Mode | Created | Billing Mode | Operation |
|--------------|---------|-----------------------------|--------------|------------------|------------|------------|---------|--------------|---|
| as-config-mp | Unbound | s6.small.1 1 vCPUs 1 GB | -- (Deleted) | High I/O 40 GB | 0 | Password | | Pay-per-use | <button>Copy</button> <button>Delete</button> |

Figure 6-89 Deleting the AS configuration

6.7.6 Deleting VPC Resources

In the left navigation pane, choose Subnets and then delete the subnet.



| Name | VPC | IPv4 CIDR Block | IPv6 CIDR Block | Status | Network ACL | Route Table | Operation |
|-----------|--------|-----------------|-----------------|-----------|-------------|--------------------|---|
| subnet-mp | vpc-mp | 192.168.0.0/24 | -- Enable IPv6 | Available | -- | rtb-vpc-mp Default | <button>Change Route Table</button> <button>Delete</button> |

Figure 6-90 Deleting the subnet

In the left navigation pane, choose Access Control > Security Groups and then delete the security group. Then delete the VPC.



| Name | Security Group Rules | Associated Instances | Description | Operation |
|---------|----------------------|----------------------|--|--|
| default | 9 | 1 | default | <button>Manage Rule</button> <button>More</button> |
| sg-mp | 10 | 0 | The security group is for general-purpose web serve... | <button>Manage Rule</button> <button>More</button> |

Figure 6-91 Deleting the security group



| Name | IPv4 CIDR Block | Status | Subnets | Route Tables | Operation |
|-------------|-------------------------------------|-----------|---------|--------------|--|
| vpc-mp | 192.168.0.0/16 (Primary CIDR block) | Available | 0 | 1 | <button>Edit CIDR Block</button> <button>Delete</button> |
| vpc-default | 10.0.0.0/24 (Primary CIDR block) | Available | 1 | 1 | <button>Edit CIDR Block</button> <button>Delete</button> |

Figure 6-92 Deleting the VPC

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.

| Category | Count |
|--|-------|
| ECSs | 0 |
| DEHs | 0 |
| BMSs | 0 |
| EVS Disks | 0 |
| Dedicated Distributed Storage Services | 0 |
| Images | 0 |
| AS Groups | 0 |
| ECS Groups | 0 |

Figure 6-93 Checking ECS-related resources

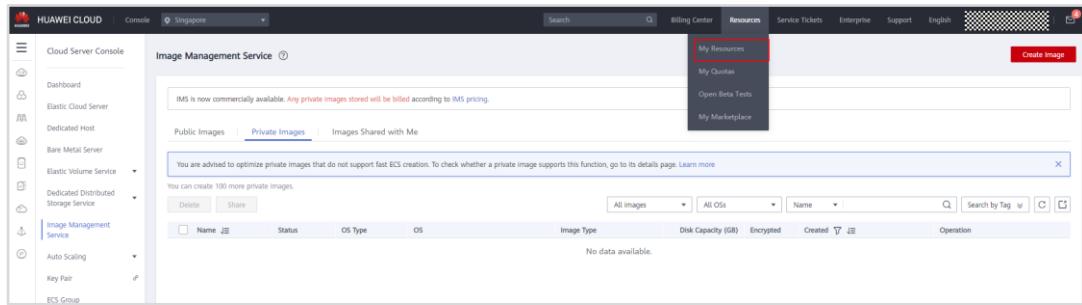
| Category | Count |
|----------------------|-------|
| VPCs | 0 |
| Subnets | 0 |
| Route Tables | 0 |
| Security Groups | 1 |
| Network ACLs | 0 |
| VPC Flow Logs | 0 |
| EIPs | 0 |
| Shared Bandwidths | 0 |
| Public NAT Gateways | 0 |
| Private NAT Gateways | 0 |
| Load Balancers | 0 |
| Peering Connections | 0 |
| VPC Endpoints | 0 |

Figure 6-94 Checking network resources

| Name | Status | OS Type | OS | Image Type | Disk Capacity (GB) | Encrypted | Created | Operation |
|--------------------|--------|---------|----|------------|--------------------|-----------|---------|-----------|
| No data available. | | | | | | | | |

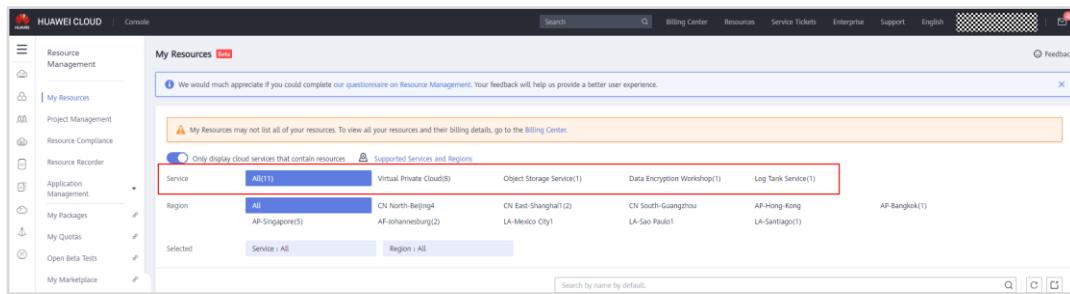
Figure 6-95 Viewing private images

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.



The screenshot shows the HUAWEI CLOUD Image Management Service (IMS) interface. The left sidebar includes options like Cloud Server Console, Dashboard, Dedicated Host, Bare Metal Server, Elastic Volume Service, Image Management Service (selected), Auto Scaling, Key Pair, and BCS Group. The main area displays the IMS service with tabs for Public Images, Private Images (selected), and Images Shared with Me. A message at the top states: "IMS is now commercially available. Any private images stored will be billed according to IMS pricing." Below this, a note says: "You are advised to optimize private images that do not support fast ECI creation. To check whether a private image supports this function, go to its details page. Learn more". A button "Create Image" is visible. A dropdown menu under the Resources tab shows "My Resources" (selected), "My Quotas", "Open Beta Tests", and "My Marketplace". At the bottom, there's a search bar and filter options for Name, OS Type, OS, Image Type, Disk Capacity (GB), Encrypted, and Created.

Figure 6-96 Resources



The screenshot shows the HUAWEI CLOUD Resource Management interface. The left sidebar includes options like Resource Management, Project Management, Resource Recorder, Application Management, My Packages, My Quotas, Open Beta Tests, and My Marketplace. The main area displays the "My Resources" section with a message: "We would much appreciate if you could complete our questionnaire on Resource Management. Your feedback will help us provide a better user experience." Below this, a note says: "My Resources may not list all of your resources. To view all your resources and their billing details, go to the Billing Center." A checkbox "Only display cloud services that contain resources" is checked. A link "Supported Services and Regions" is present. A table lists resources categorized by Service, Region, and Selected status. The table includes columns for Service (e.g., AIM(11), Virtual Private Cloud(8), Object Storage Service(1), Data Encryption Workshop(1), Log Tank Service(1)), Region (e.g., All, CN North-Beijing(4), CN East-Shanghai(2), CN South-Guangzhou, AP-Hong-Kong, AP-Singapore(3), AF-Johannesburg(2), LA-Mexico City(1), LA-Sao Paulo(1), LA-Santiago(1), AP-Bangkok(1)), and Selected status (e.g., Service : All, Region : All). A search bar at the bottom allows searching by name.

Figure 6-97 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