HCIA Cloud Service Certification Training

HCIA-Cloud Service

Lab Guide for HUAWEI CLOUD Service Engineers

Version: 3.0

Huawei Technologies Co., Ltd.

Trademarks and Permissions

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

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 and the estimated costs in the **AP-Singapore** region. The actual costs may vary, depending on your use of the cloud services.

Exercise	Cloud Service	Quantity	Specifications	Pricing	Duration (h)	Price (USD)	Total (USD)
Exercises on compute services	ECS	1	x86 | General computing | s6.large.2 | 2 vCPUs | 4 GB, High I/O | 40 GB | Windows Server 2012 R2 Standard 64-bit English (40 GB)	0.13/h	12	1.56	20.28
	ECS	1	x86 | General computing | s6.small.1 | 1 vCPU | 1 GB, High I/O | 40 GB, Dynamic BGP | Exclusive | Billed by bandwidth | 1 Mbit/s, Windows | Windows Server 2012 R2 Standard 64-bit English	0.04/h	12	0.48	
	IMS	1	Private image	Free	12	0	
	AS	1	N/A	Free	12	0	
	VPC	1	N/A	Free	12	0	
	HSS	1	N/A	Free	12	0	

Exercise	Cloud Service	Quantity	Specifications	Pricing	Duration (h)	Price (USD)	Total (USD)
	DEW	1	N/A	Free	12	0	
Exercises on networking services	ECS	2	x86 | General computing | s6.large.2 | 2 vCPUs | 4 GB, High I/O | 40 GB | Windows Server 2012 R2 Standard 64-bit English (40 GB)	0.13/h	12	3.12	
	ECS	1	x86 | General computing | s6.large.2 | 2 vCPUs | 4 GB, High IO | 40 GB | CentOS 64-bit	0.07/h	12	0.84	
	EIP	2	Dedicated | Dynamic BGP | Billed by bandwidth | 1 Mbit/s	0.03/h	12	0.72	
	ELB	1	Public network | Dynamic BGP, 1 Mbit/s	0.03/h	12	0.36	
	HSS	1	N/A	Free	12	0	
	DEW	1	N/A	Free	12	0	
Exercises on storage services	ECS	1	x86 | General computing | s6.large.2 | 2 vCPUs | 4 GB; High I/O | 40 GB | Windows Server 2012 R2 Standard 64-bit English (40 GB)	0.13/h	12	1.56	

Exercise	Cloud Service	Quantity	Specifications	Pricing	Duration (h)	Price (USD)	Total (USD)
	ECS	1	x86 | General computing | s6.large.2 | 2 vCPUs | 4 GB, High IO | 40 GB | CentOS 64-bit	0.07/h	12	0.84	
	EVS	2	40 GB, High I/O	0.01/h	12	0.24	
	SFS	1	500 GB	0.06/h	12	0.72	
	OBS	1	Pay per use	0.02/h	24	0.48	
	HSS	1	N/A	Free	12	0	
	DEW	1	N/A	Free	12	0	
Exercises on O&M services	IAM	1	N/A	Free	12	0	
	Cloud Eye	1	N/A		12		
	LTS	1	N/A		12		
	CTS	1	N/A		12		
Comprehen-sive exercise	VPC	1	N/A	Free	12	0	
	EIP	2	Dedicated | Dynamic BGP | Billed by bandwidth | 1 Mbit/s	0.03/h	12	0.72	
	RDS	1	RDS for MySQL | 8.0 | Active/standby | General-enhanced II 1 vCPU | 2 GB, Ultra-high I/O | 40 GB	0.36/h	12	4.32	

Exercise	Cloud Service	Quantity	Specifications	Pricing	Duration (h)	Price (USD)	Total (USD)
	ECS	3	x86 | General computing | s6.small.1 | 1 vCPU | 1 GB, High I/O | 40 GB, Dynamic BGP | Dedicated | Billed by bandwidth | 5 Mbit/s, CentOS | CentOS 7.6 64-bit	0.07/h	12	2.52	
	IMS	1	Private image	Free	12	0	
	AS	1	N/A	Free	12	0	
	ELB	1	Public network | Dynamic BGP, 5 Mbit/s	0.15/h	12	1.80	
	HSS	1	N/A	Free	12	0	
	DEW	1	N/A	Free	12	0	

Contents

1 Getting Started with HUAWEI CLOUD

1.1 Introduction

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.

Step 1 Visit HUAWEI CLOUD official website, and click **Register** in the upper right.

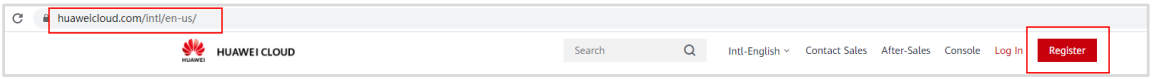


Figure 1-2 Visiting the HUAWEI CLOUD official website

Step 2 Enter the information required.

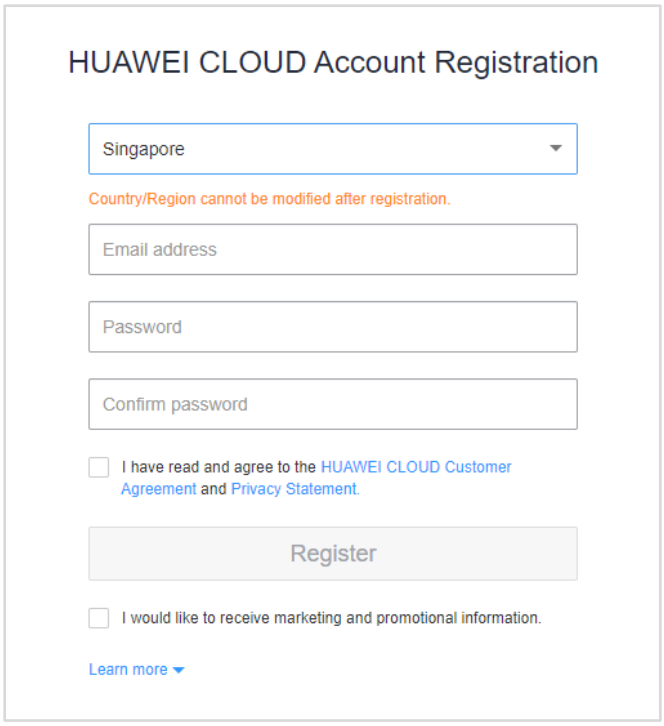


Figure 1-3 Registering a HUAWEI CLOUD account

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

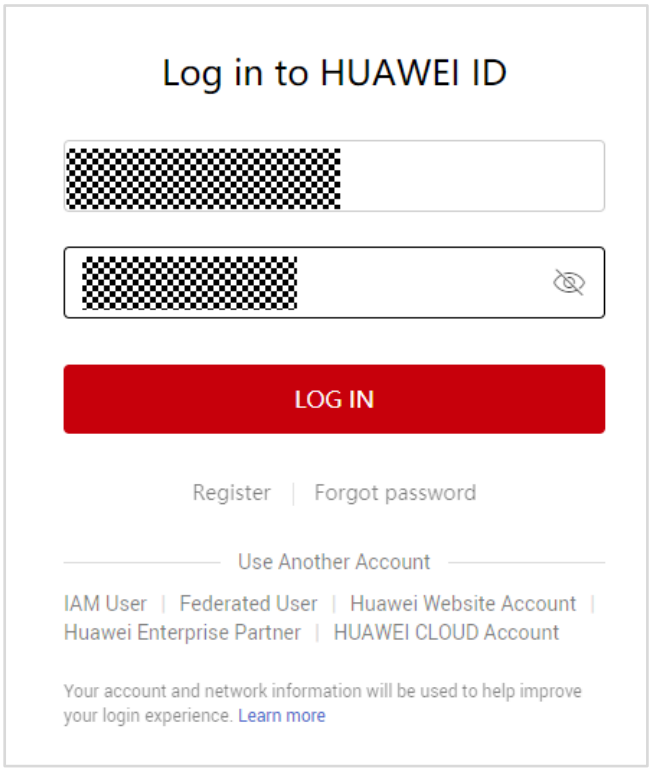


Figure 1-4 Logging in to HUAWEI COULD

Step 4 Click **Console** in the upper right.

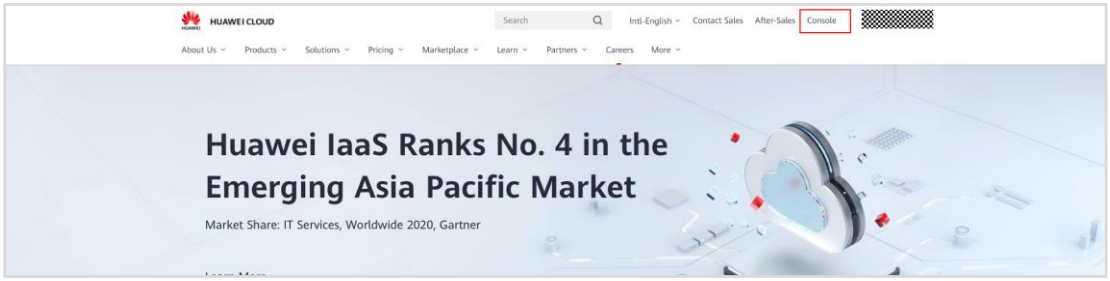


Figure 1-5 Accessing the console

Step 5 Hover over your username in the upper right and choose **Basic Information**.

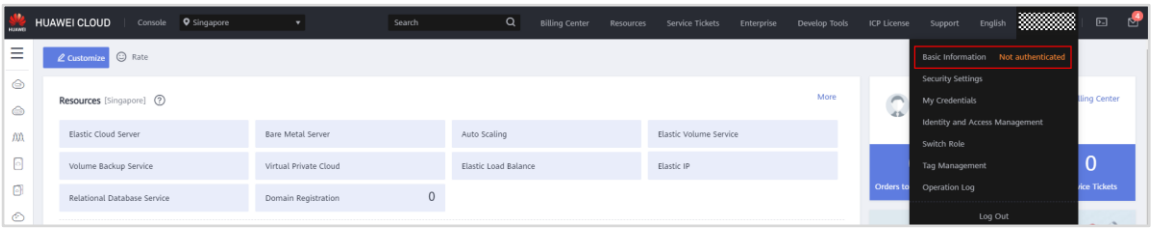


Figure 1-6 Going to My Account

Step 6 Click **Authenticate** next to Authentication Status.

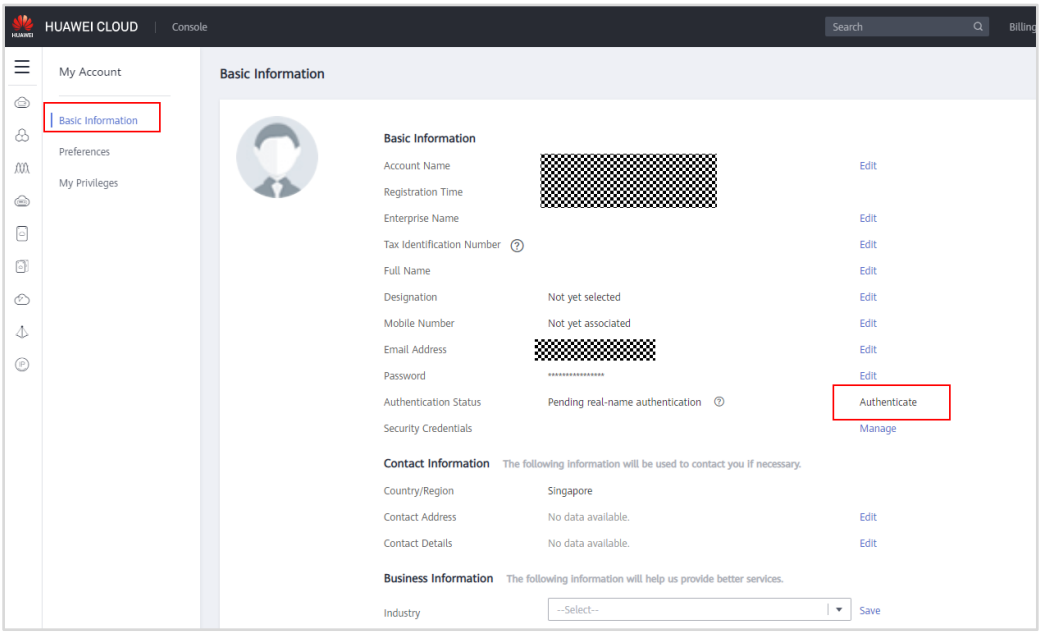


Figure 1-7 Clicking Authenticate

Step 7 Select a type that matches your account. Here, we'll select **Individual Authentication**.

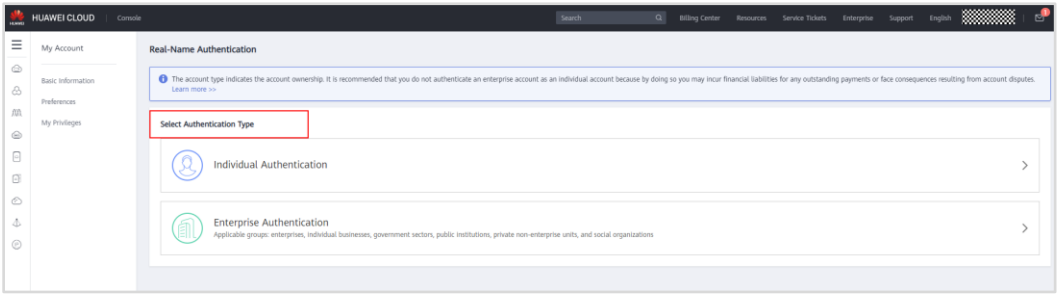


Figure 1-8 Selecting an authentication type

Step 8 Complete the information required.

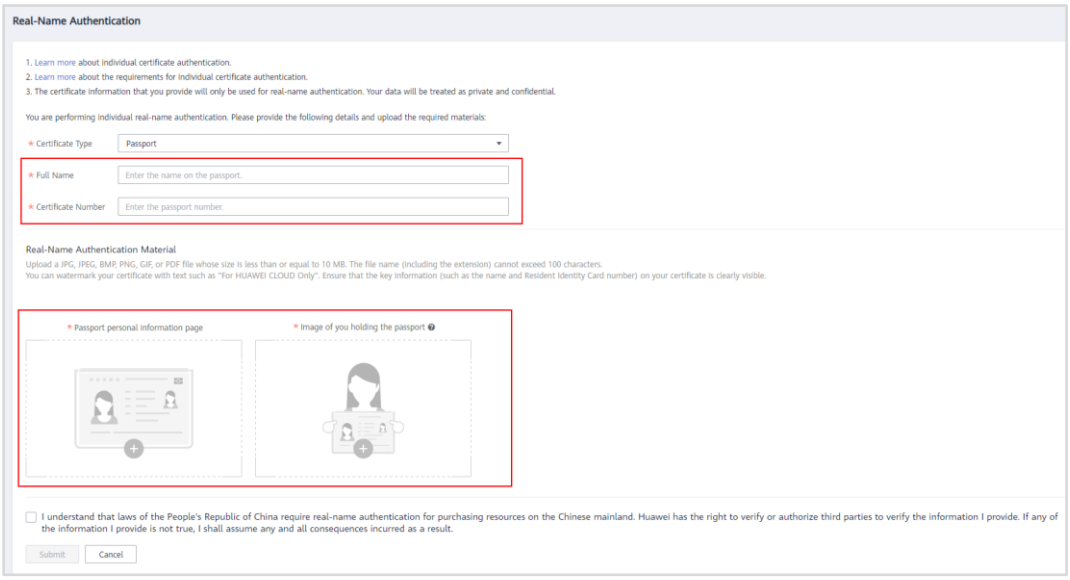


Figure 1-9 Individual authentication

Step 9 Once complete, refresh the **Real-Name Authentication** page. The authentication is successful, so let's proceed to the next exercise.

1.2.3 Creating an IAM User and Assigning Permissions

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

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

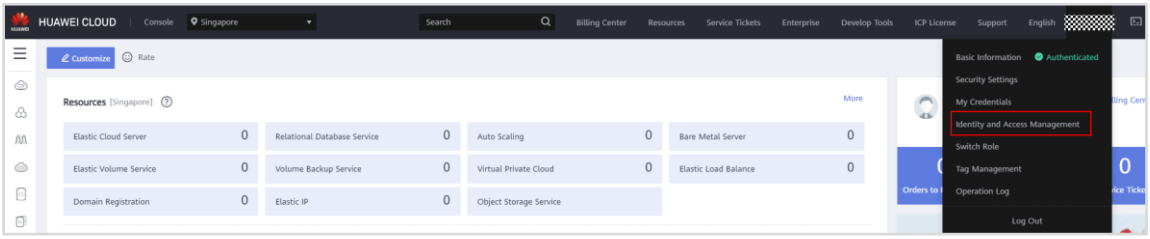


Figure 1-10 Choosing Identity and Access Management

Step 2 Choose **User Groups** in the navigation pane, and click **Create User Group**.

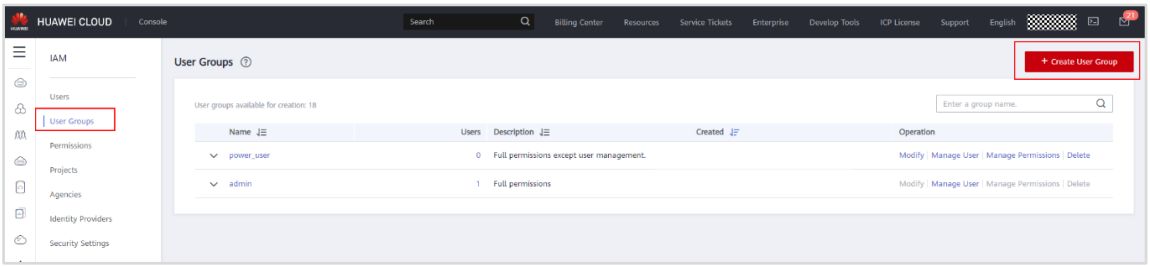


Figure 1-11 Creating a user group

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

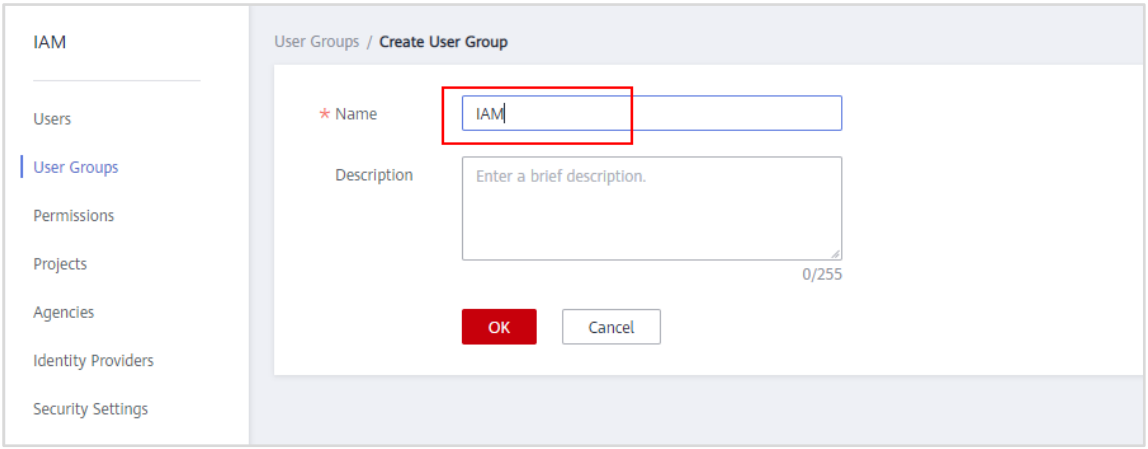


Figure 1-12 Configuring the user group information

Step 4 Click **Manage Permissions** for the user group you created.

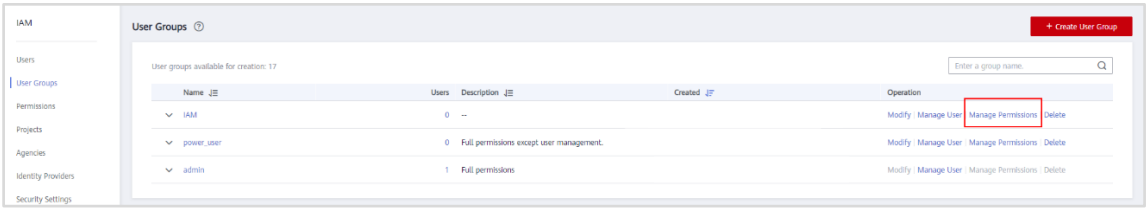


Figure 1-13 Clicking Manage Permissions

Step 5 Click **Assign Permissions**.

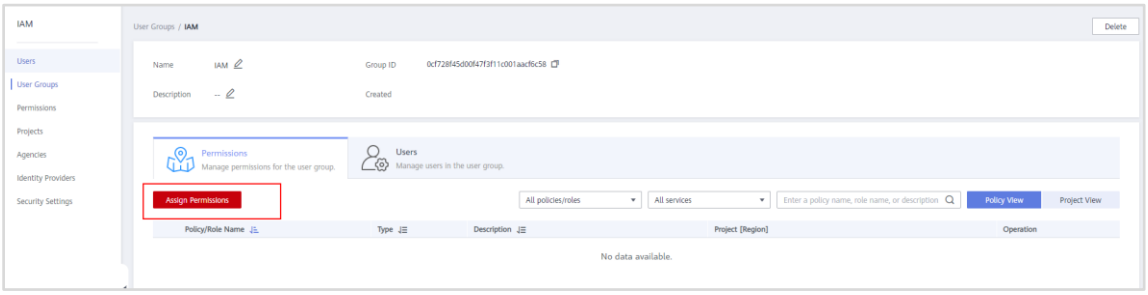


Figure 1-14 Permissions tab page

Step 6 Under **Scope**, click **Region-specific projects**, and select **AP-Singapore**. In the **Permissions** section, search for IAM, select **Tenant Guest** and **Tenant Administrator**, and click **OK**.

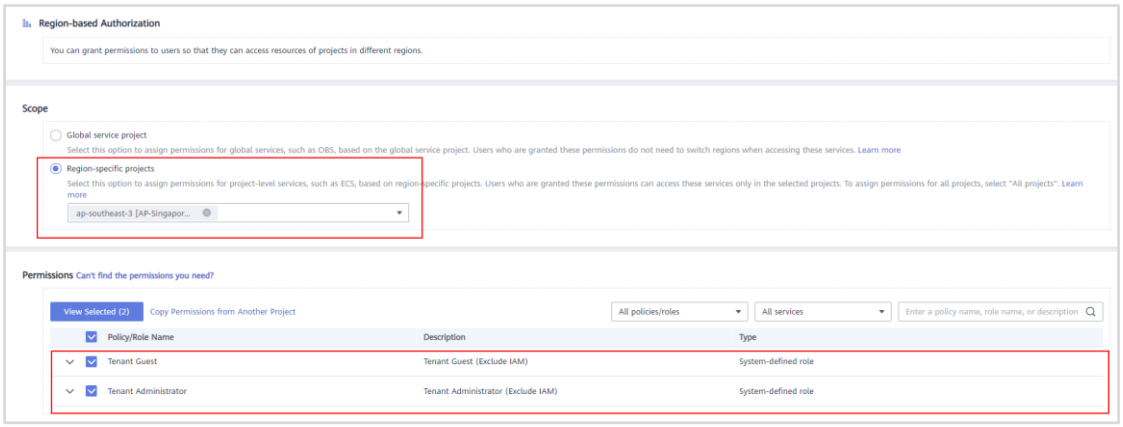


Figure 1-15 Assigning permissions

Step 7 Go to the **Users** page, and click **Create User** in the upper right.

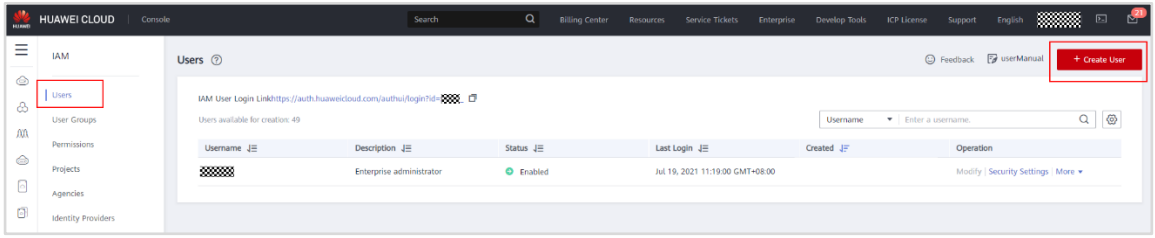


Figure 1-16 Creating a user

Step 8 Configure the user information and click **Next**.

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

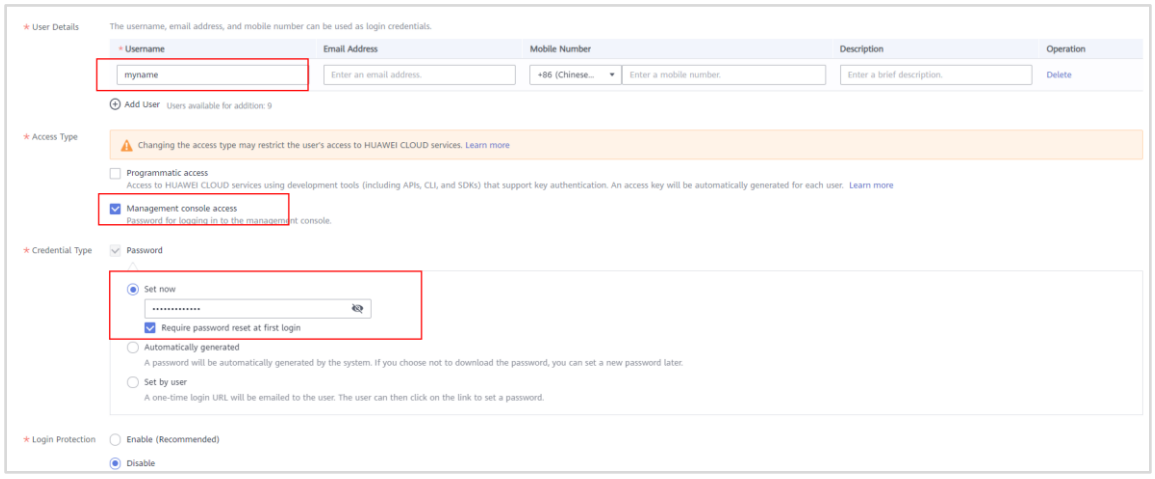


Figure 1-17 Configuring the basic user information

Step 9 Select the user group you created and click **Create**.

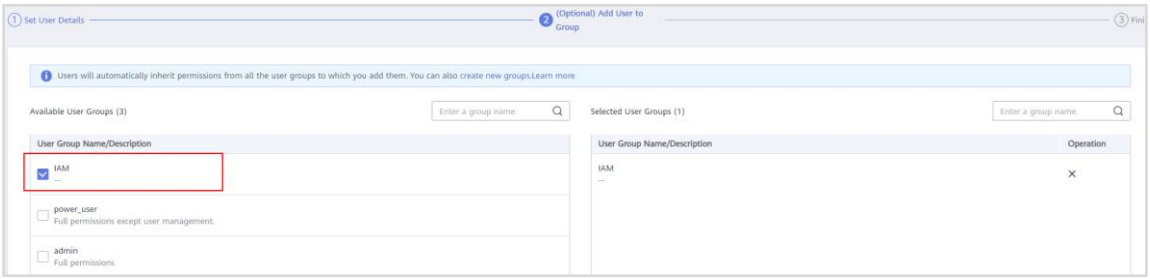


Figure 1-18 Adding the user to the created user group

Step 10 View the results. The user is created when you see this page.

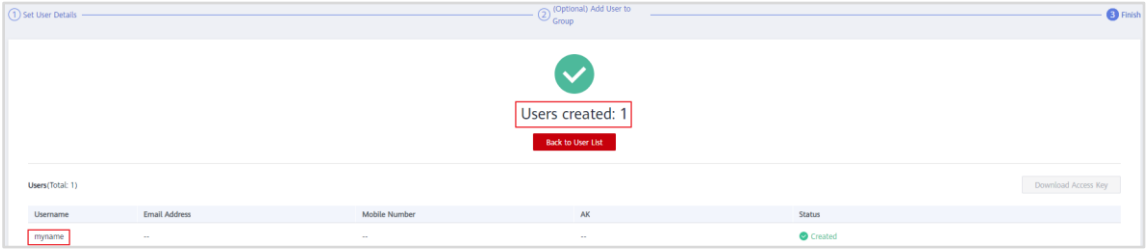


Figure 1-19 User created successfully

Step 11 Log out of the account and log in again as the IAM user.

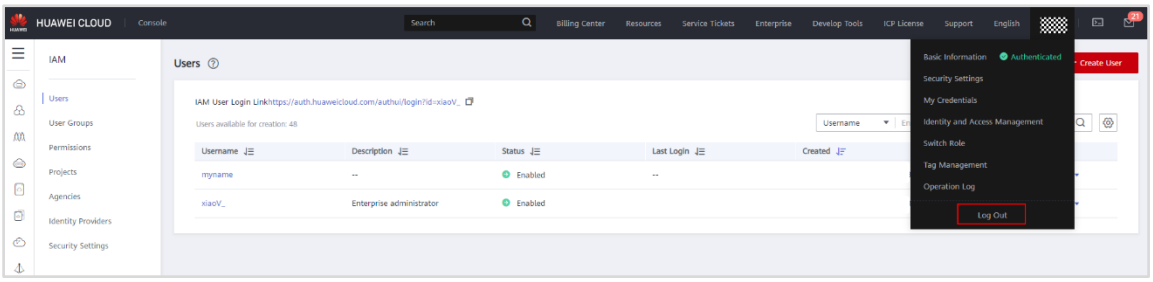


Figure 1-20 Logging out of the account

Step 12 Click **IAM User**.

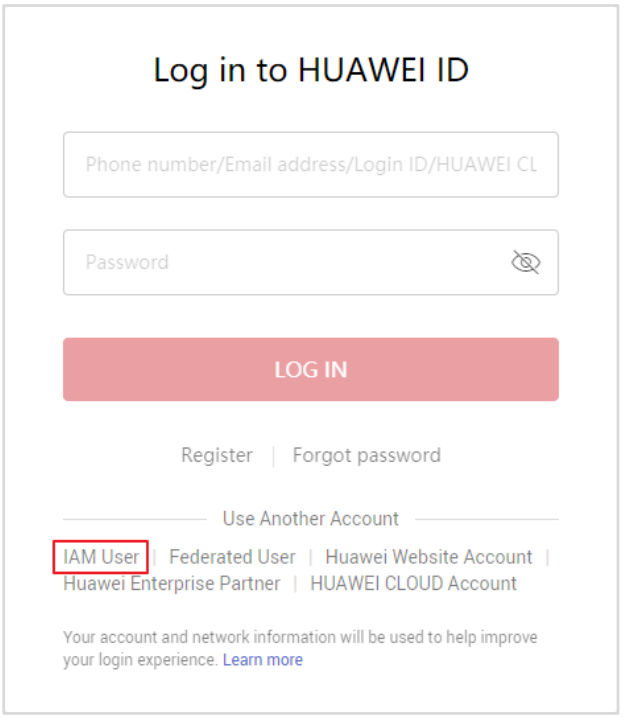


Figure 1-21 Clicking IAM User

Step 13 Log in as the IAM user you created.

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

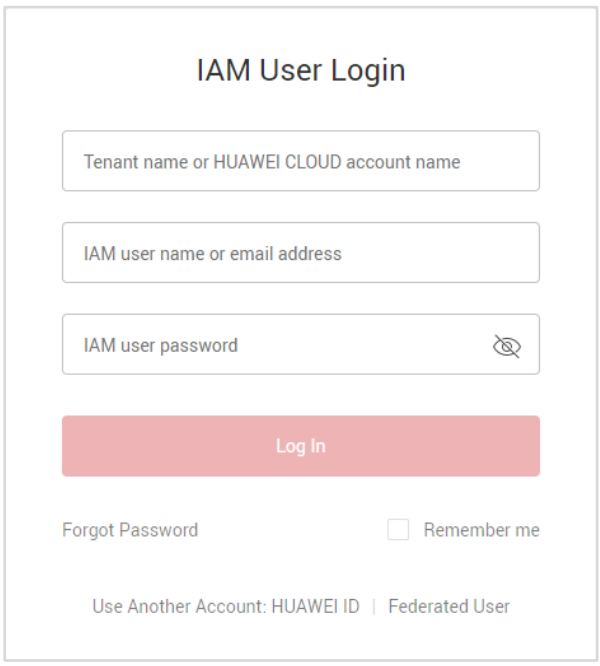


Figure 1-22 Logging in as an IAM user

Step 14 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.

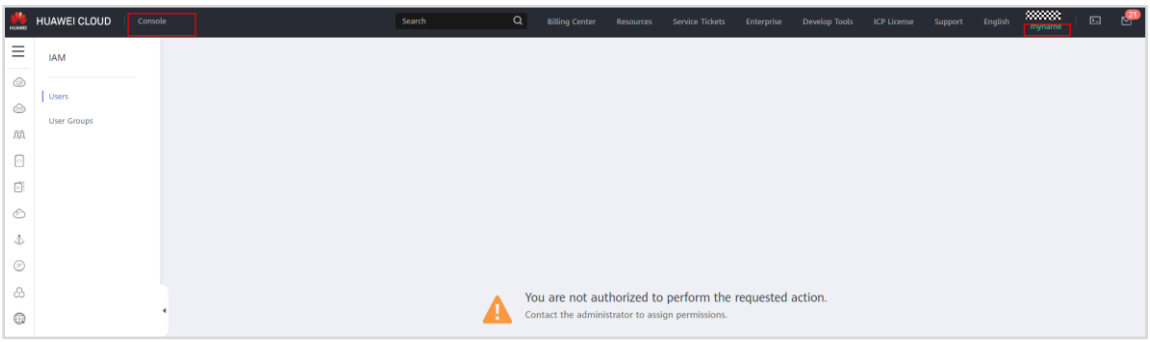


Figure 1-23 IAM user login successful

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.

Step 1 Log out of the IAM user account.

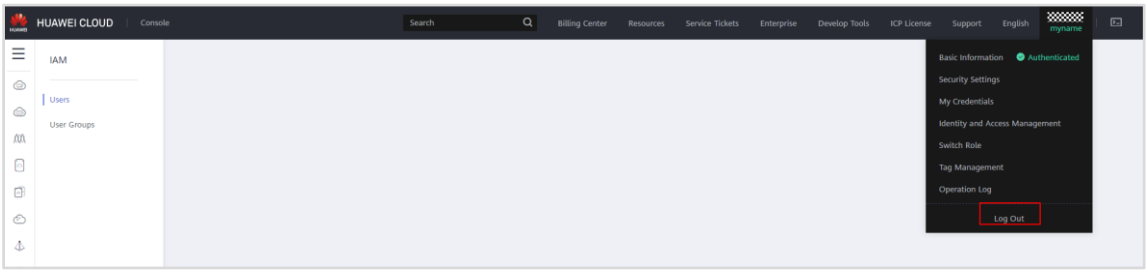


Figure 1-24 Logging out of the IAM user account

Step 2 Log in with your HUAWEI CLOUD account, and choose **Virtual Private Cloud** in the left pane.

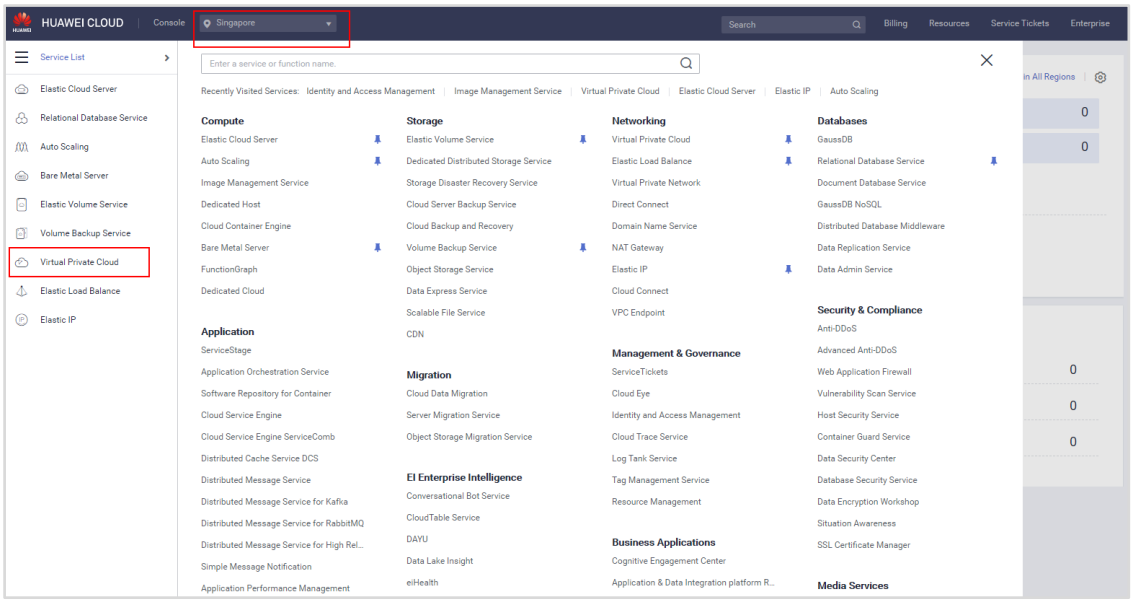


Figure 1-25 Choosing Virtual Private Cloud

Step 3 Click **Create VPC**.

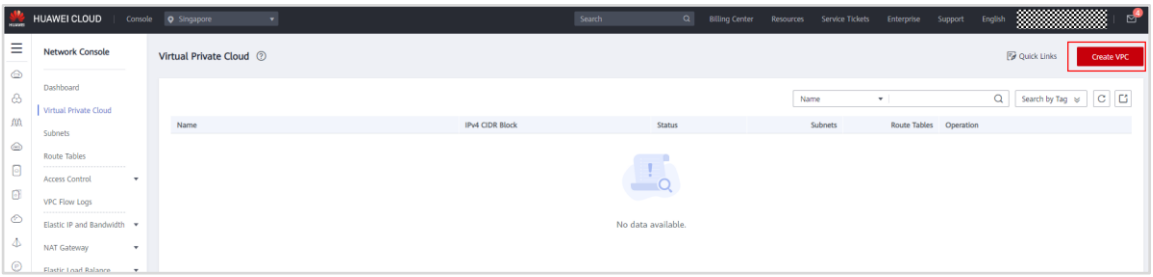


Figure 1-26 Creating a VPC

Step 4 Configure the VPC parameters and click **Create Now**.

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

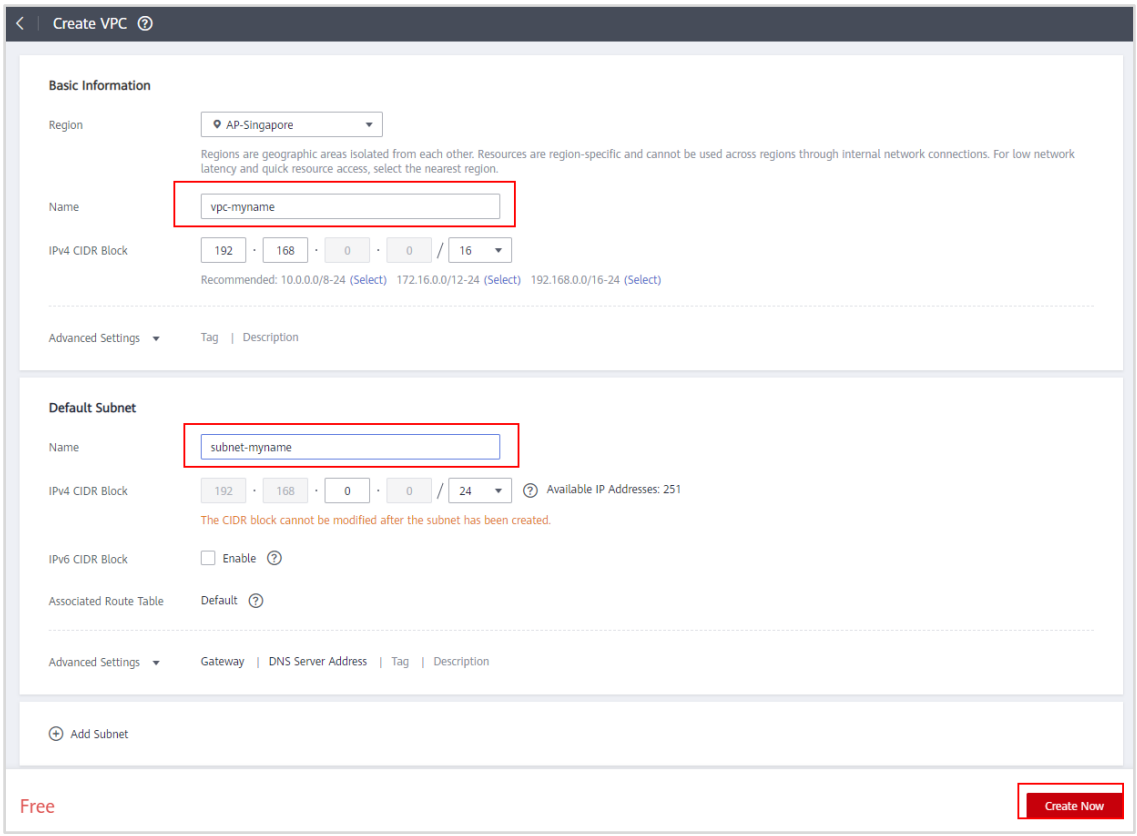


Figure 1-27 Configuring the VPC

Step 5 Delete the subnet of the VPC.

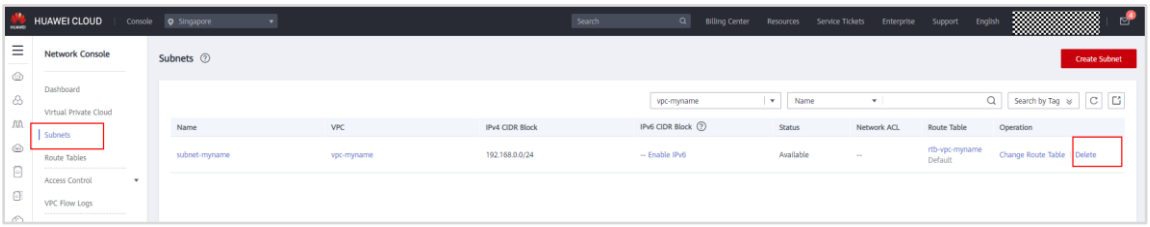


Figure 1-28 Deleting the subnet

Step 6 Delete the VPC.

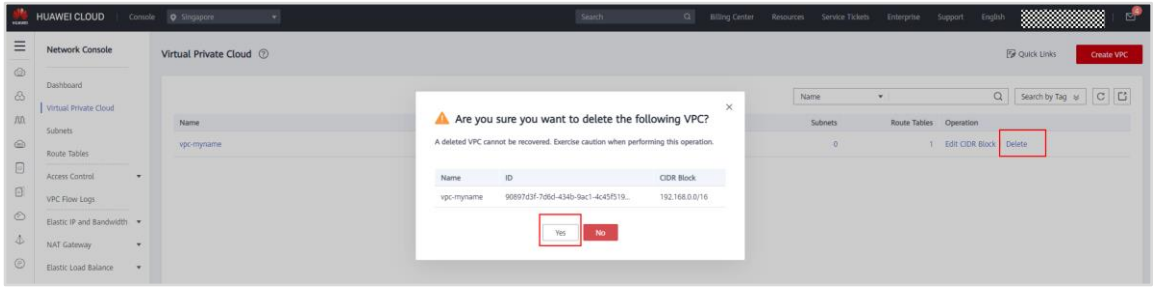


Figure 1-29 Deleting the VPC

1.3 Exercises

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

2 Compute Services

2.1 Introduction

2.1.1 About This Exercise

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

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.

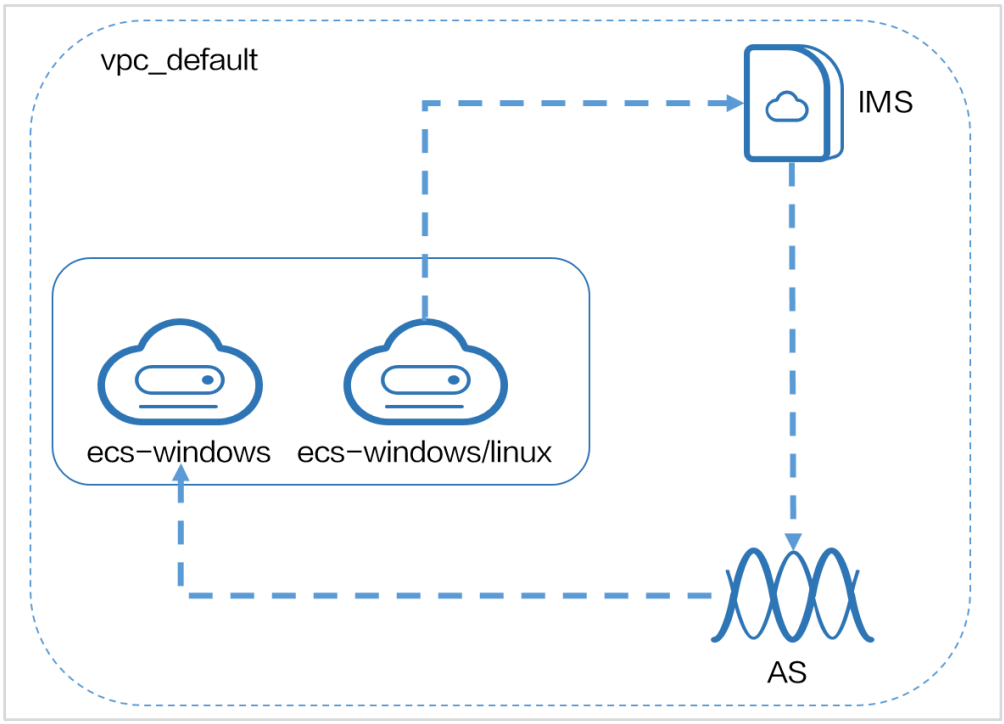


Figure 2-1 Topology

2.2.2 ECS Lifecycle Management

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

2.2.2.1 Creating Two Types of ECSs

Step 1 Go to HUAWEI CLOUD official website, and click **Log In** in the upper right corner.

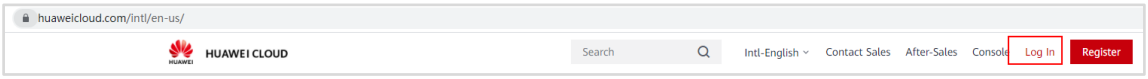


Figure 2-2 Logging in to HUAWEI COULD

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

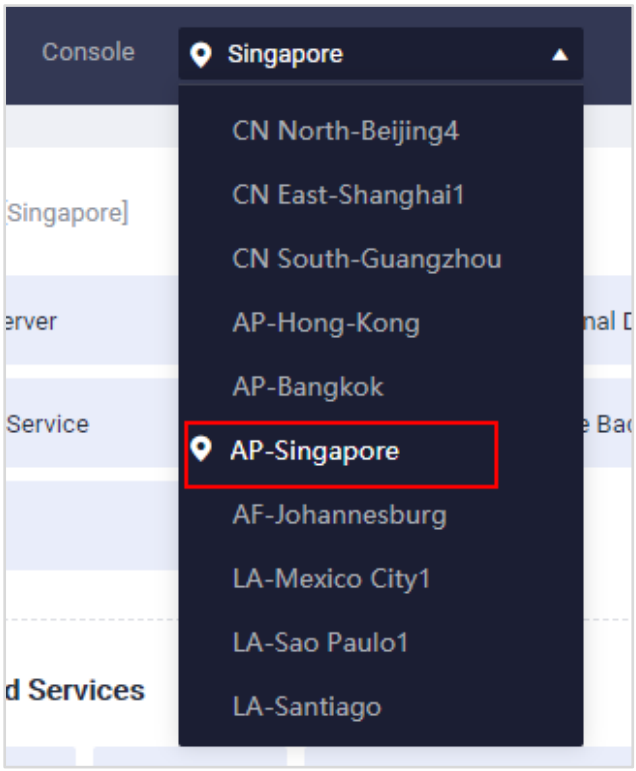


Figure 2-3 Choosing AP-Singapore

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

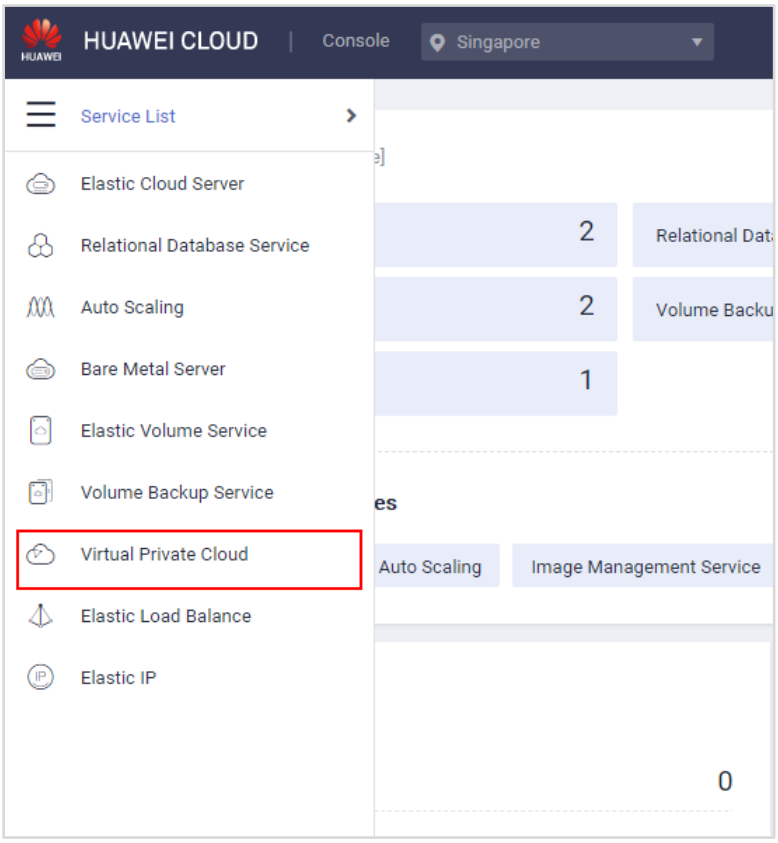


Figure 2-4 Choosing Virtual Private Cloud

Step 4 Click **Create VPC**.

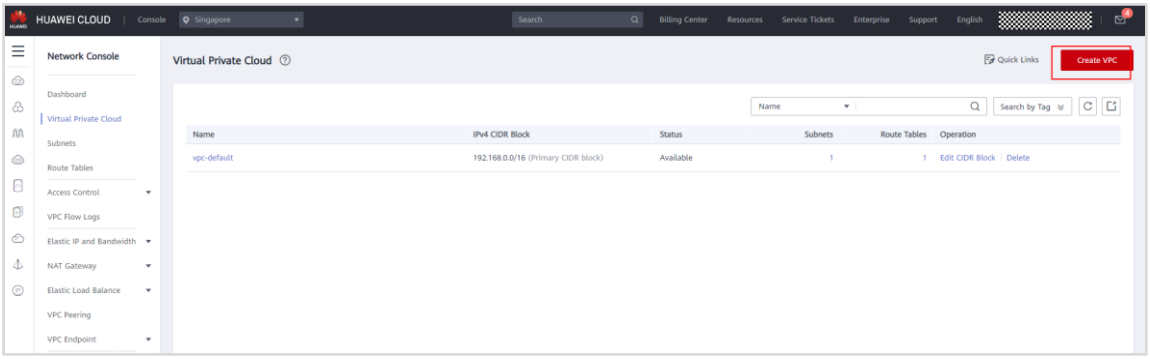


Figure 2-5 Create VPC

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

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

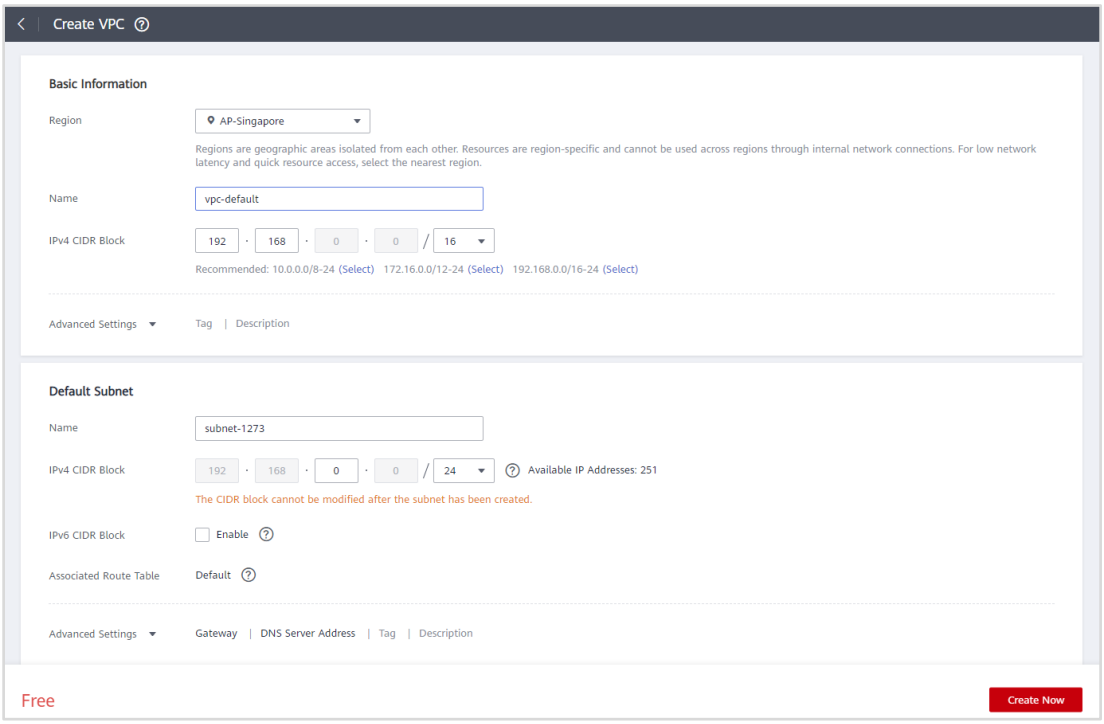


Figure 2-6 Configuring the VPC

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

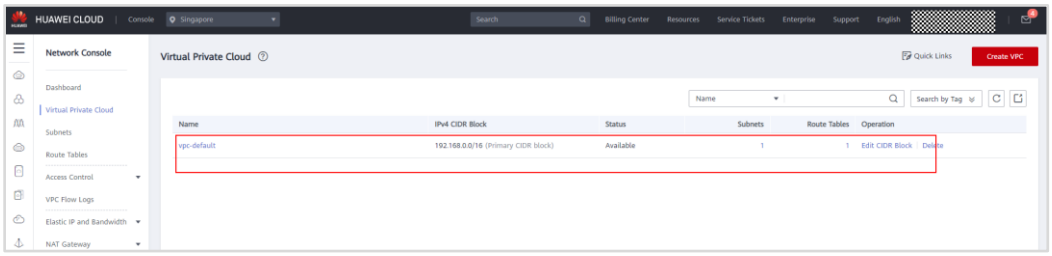


Figure 2-7 Viewing the VPC

Step 7 Click **Service List** on the left, and search for **Data Encryption Workshop** to configure a key pair for the ECS.

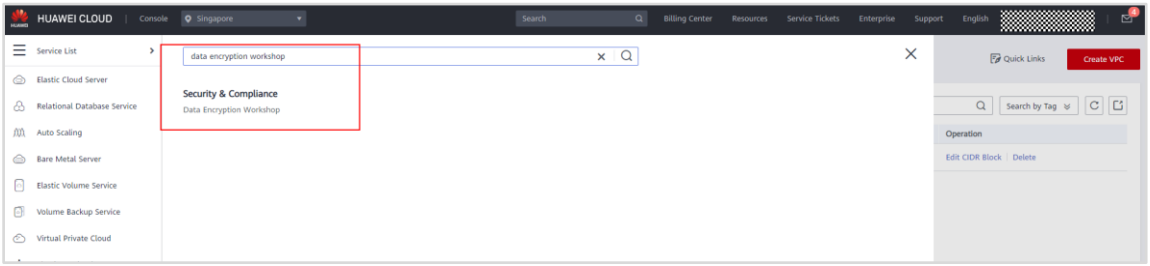


Figure 2-8 Data Encryption Workshop

Step 8 Choose **Key Pair Service** on the left.

Figure 2-9 Key Pair Service

Step 9 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.

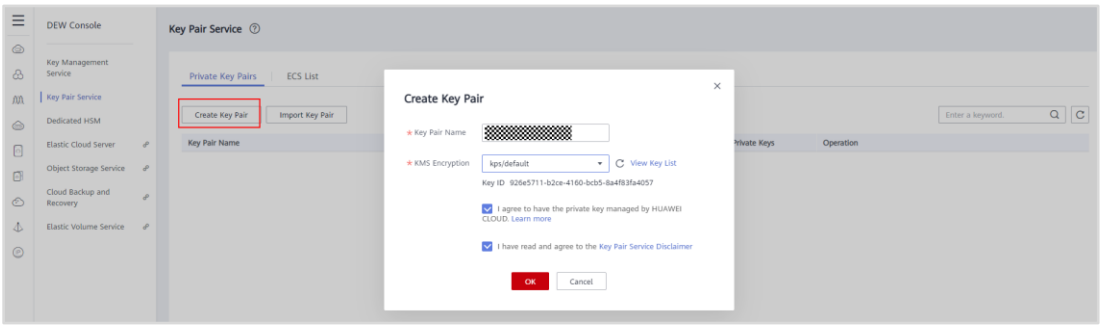


Figure 2-10 Create Key Pair

Figure 2-11 Downloading the key pair file

Step 10 Click **Service List** on the left and choose **Compute** > **Elastic Cloud Server**.

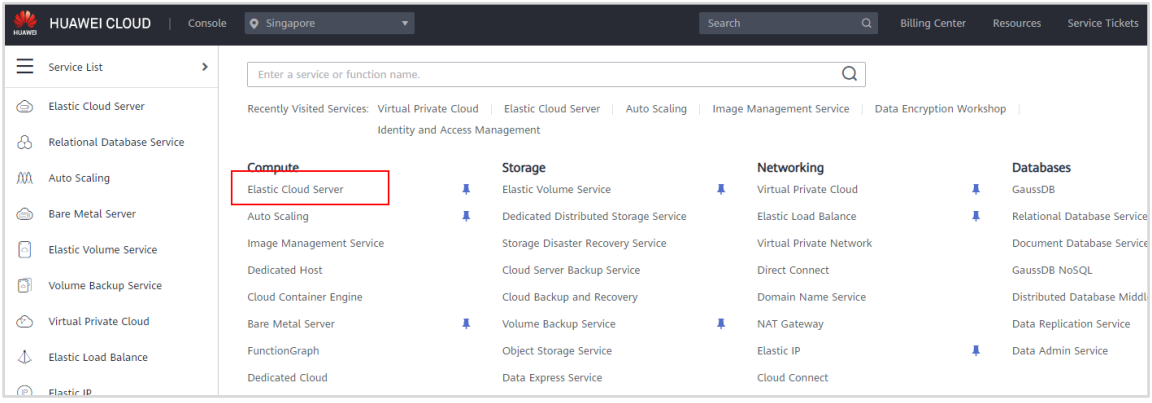


Figure 2-12 Choosing Elastic Cloud Server

Step 11 Click **Buy ECS**.

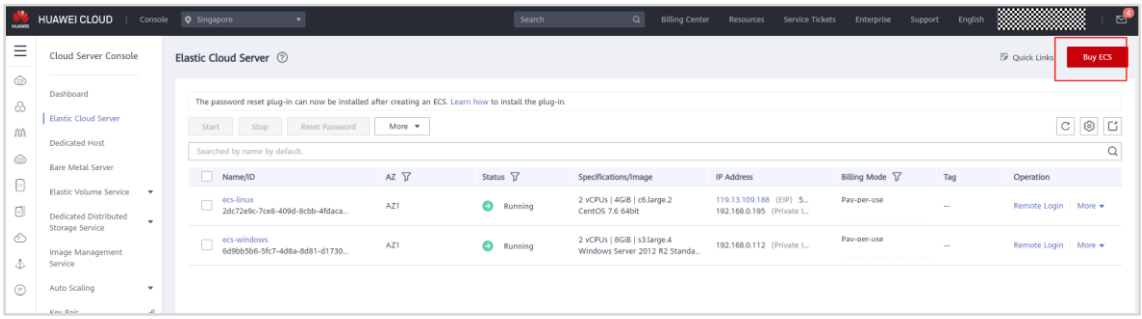


Figure 2-13 Buy ECS

Step 12 Configure basic settings as follows:

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

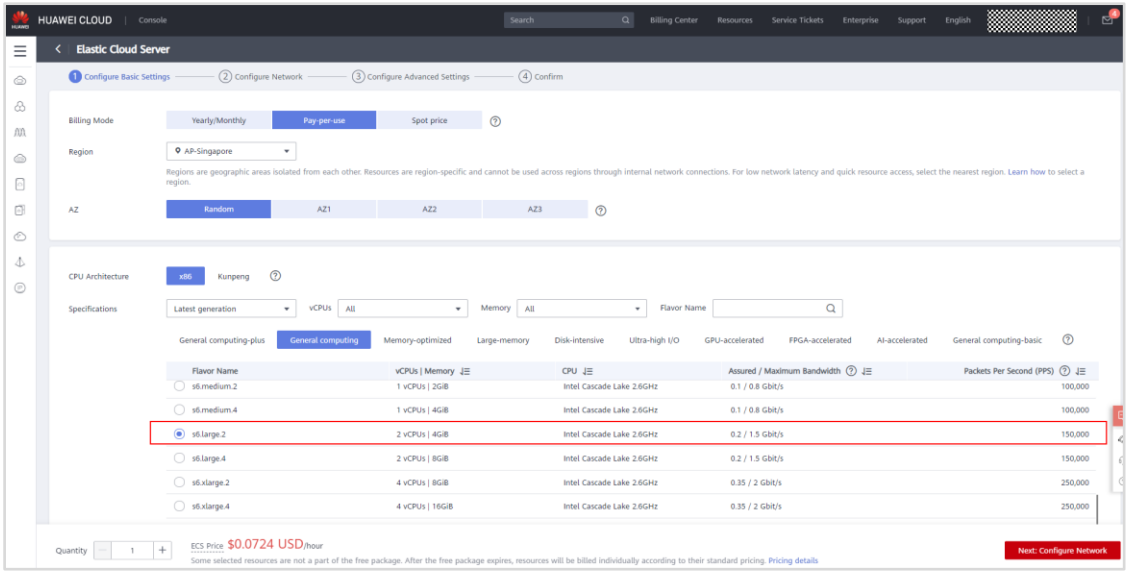


Figure 2-14 Configure Basic Settings

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

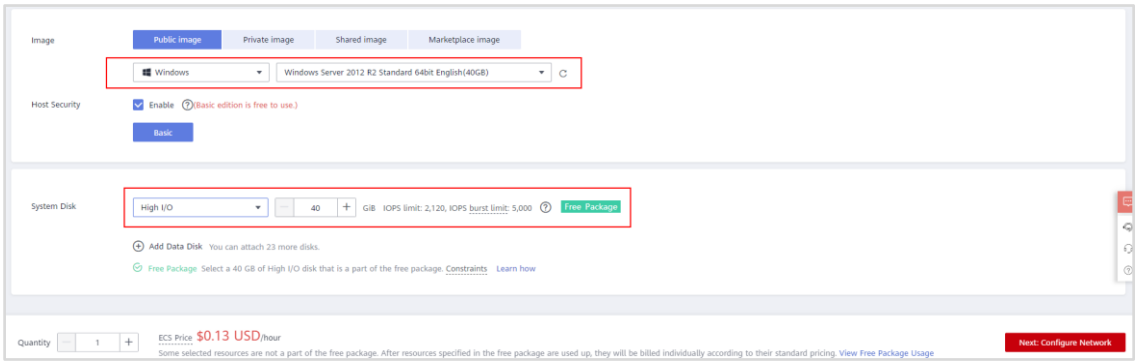


Figure 2-15 Configure Basic Settings

Step 13 Click **Next: Configure Network**. The **Configure Network** page is displayed. Configure the parameters as follows:

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

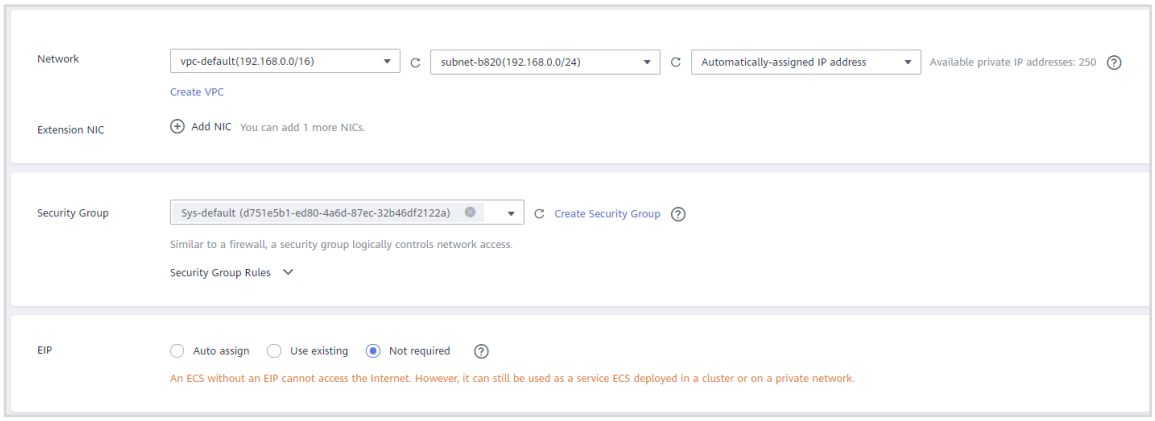


Figure 2-16 Configure Network

Step 14 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.

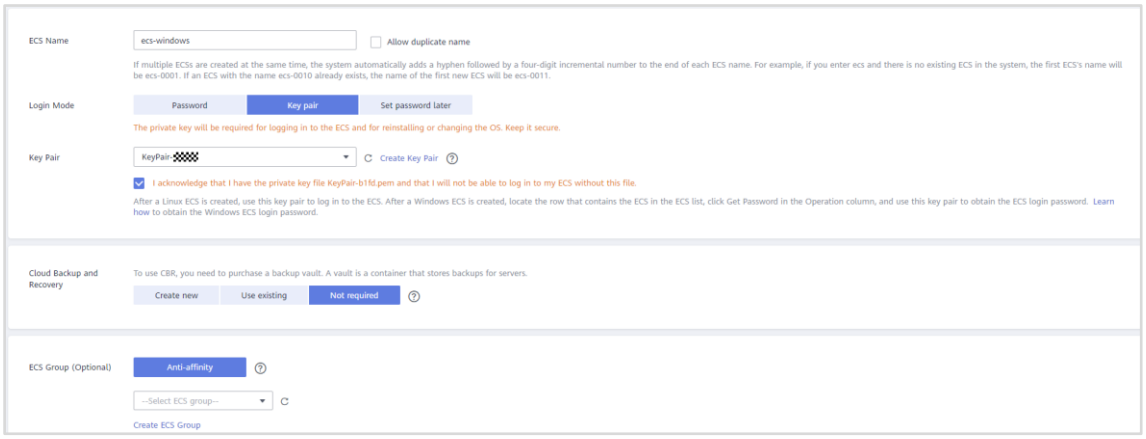


Figure 2-17 Configure Advanced Settings

Step 15 Click **Next: Confirm**. After confirming the ECS configurations, select **I have read and agree to the Service Level Agreement and Image Disclaimer**, and click **Submit**. After about 10 seconds, you can view the created ECS on the **Elastic Cloud Server** page. If the **Status** is **Running**, the ECS can work normally.

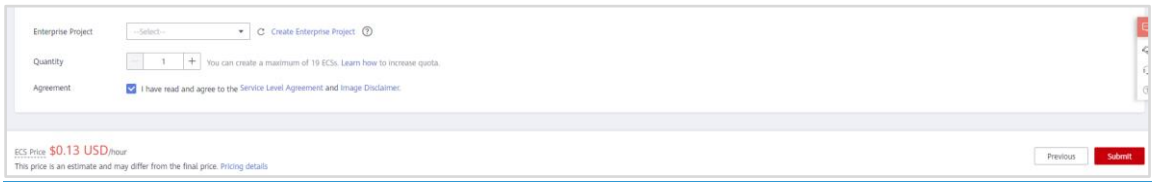


Figure 2-18 Purchasing ECS

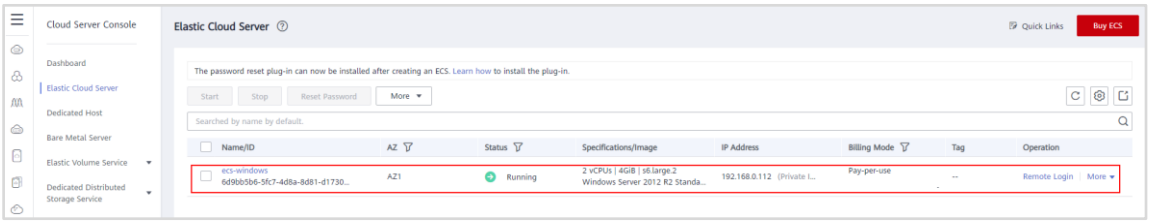


Figure 2-19 Viewing the created ECS

Step 16 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)

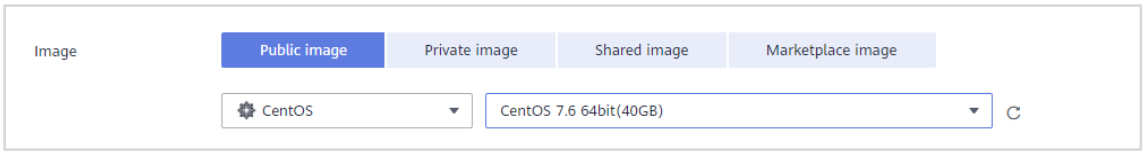


Figure 2-20 Purchasing a Linux ECS

2.2.2.2 Logging In to an ECS

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

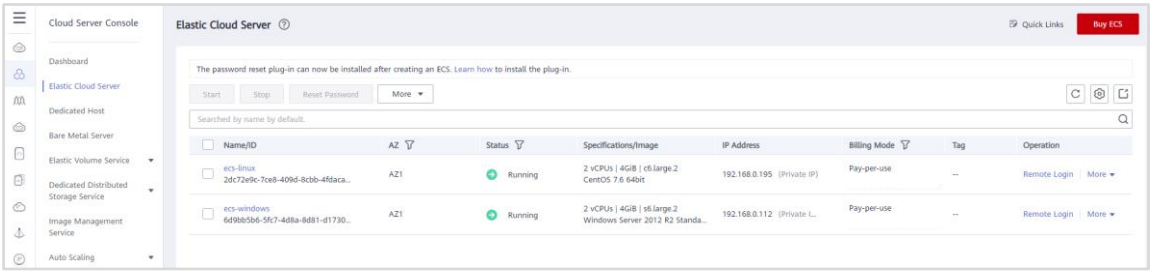


Figure 2-21 Remotely logging in to the ECS

Step 2 Locate the row containing **ecs-windows**, click **More**, and choose **Get Password**.

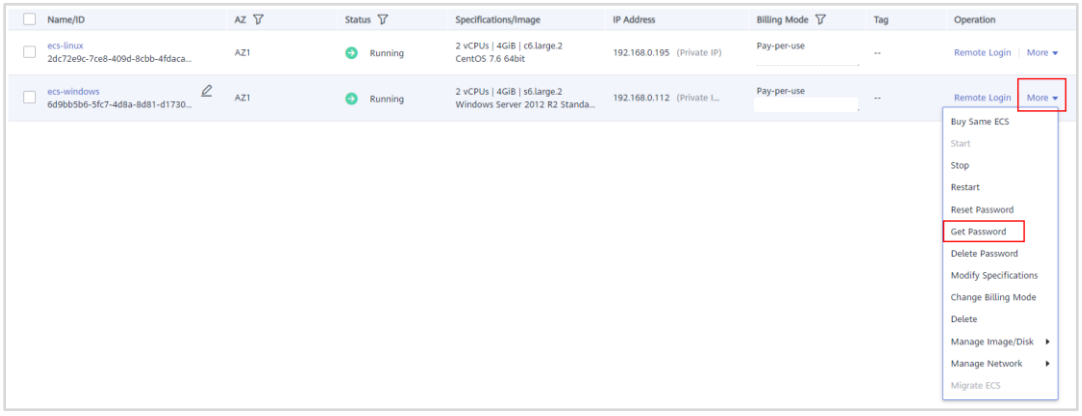


Figure 2-22 Get Password

Step 3 Click **Select File**, choose the downloaded key pair file, and click **Open**.

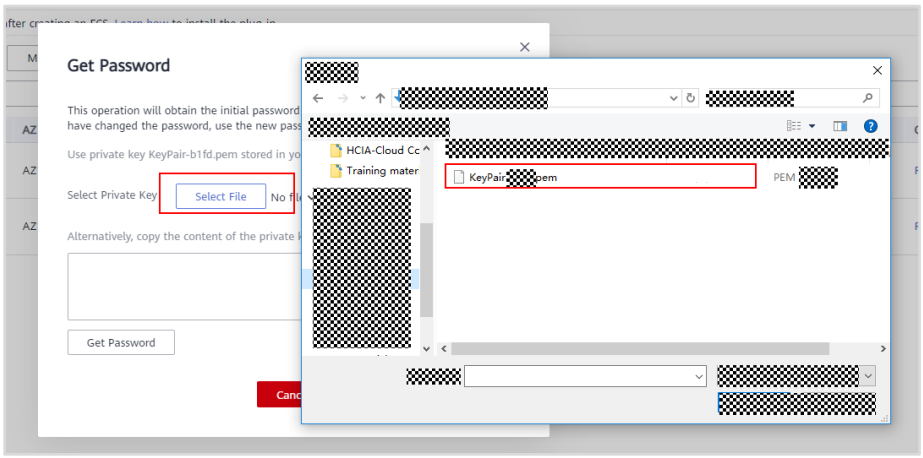


Figure 2-23 Choosing key pair file

Step 4 Click **Get Password**, copy the password, and close the window.

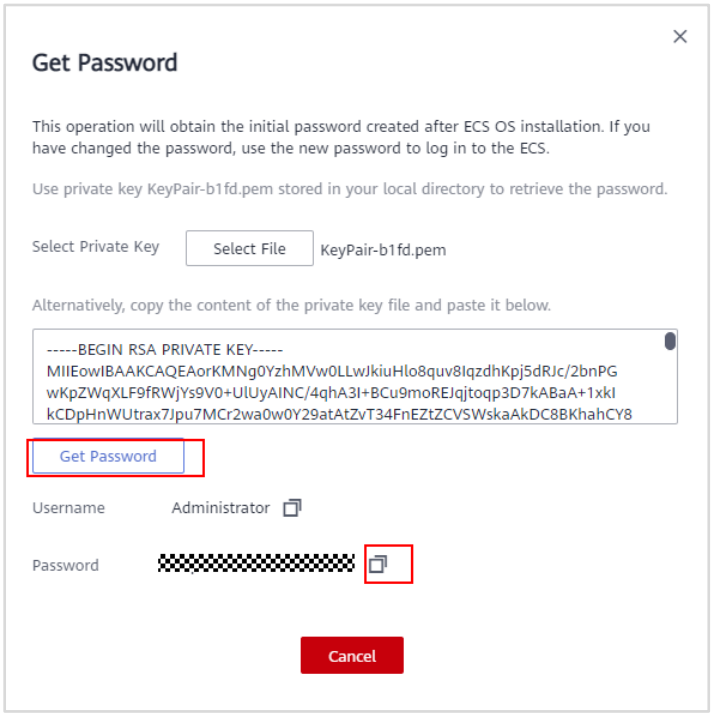


Figure 2-24 Get Password

Step 5 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.

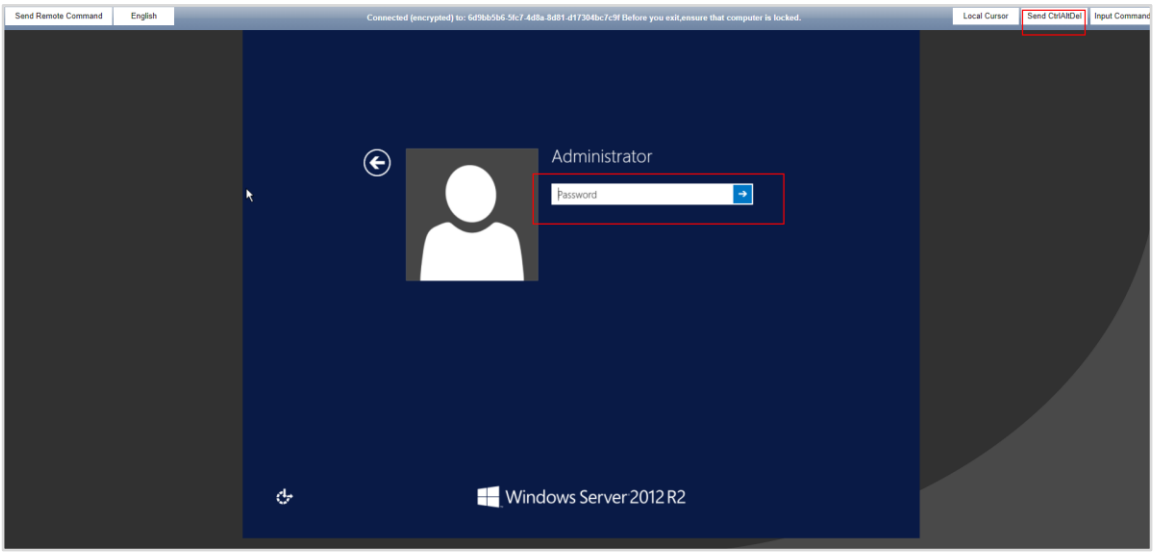


Figure 2-25 Logging In to Windows

Step 6 Click **Input Commands** in the upper right corner, paste the copied password, click **Send**, and then press **Enter**.

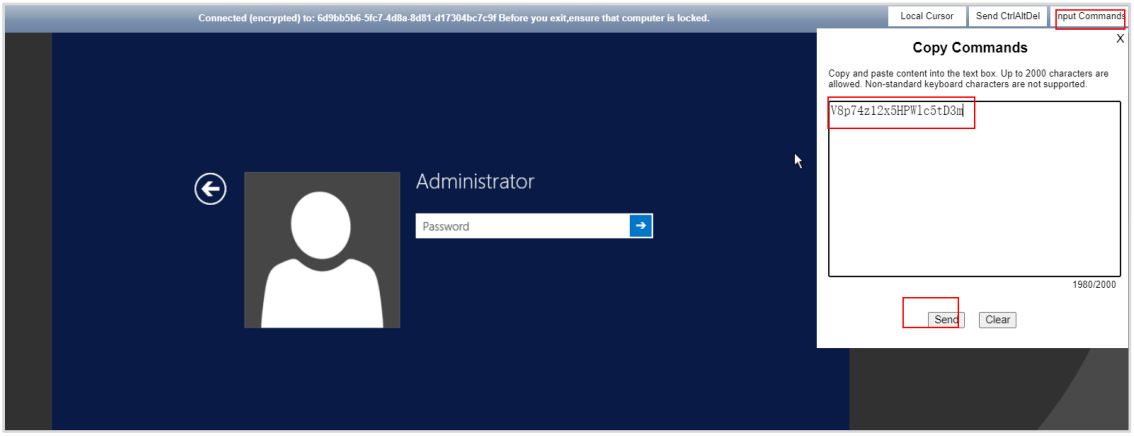


Figure 2-26 Entering the password

Step 7 If a page similar to the one in following figure is displayed, the ECS login was successful.

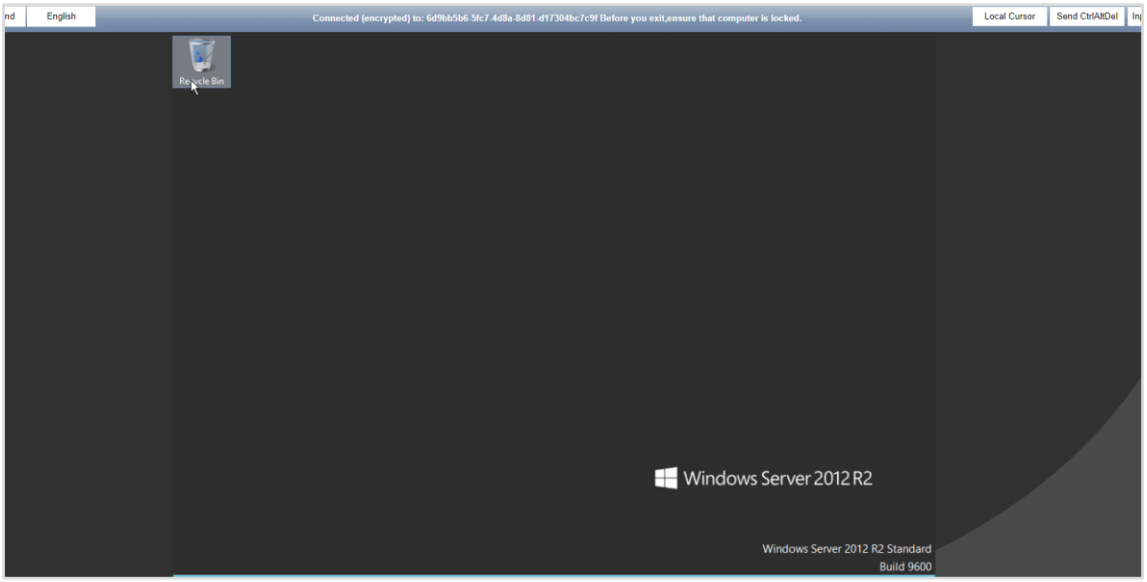


Figure 2-27 Successfully logging in to Windows

Step 8 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 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.

Figure 2-28 Successfully logging in to Linux

Step 9 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

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

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

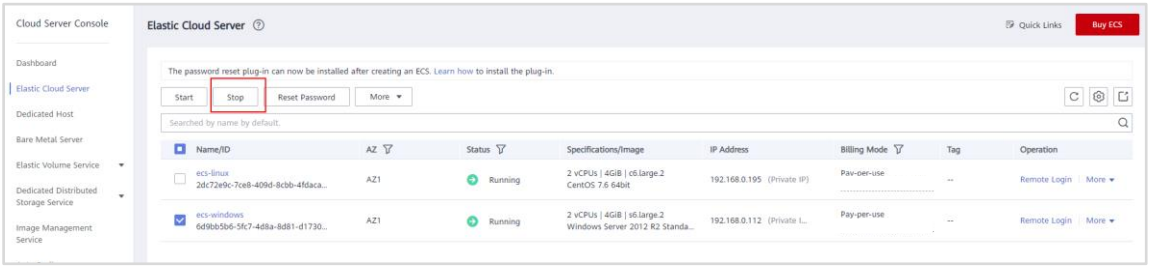


Figure 2-29 Stopping the ECS

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

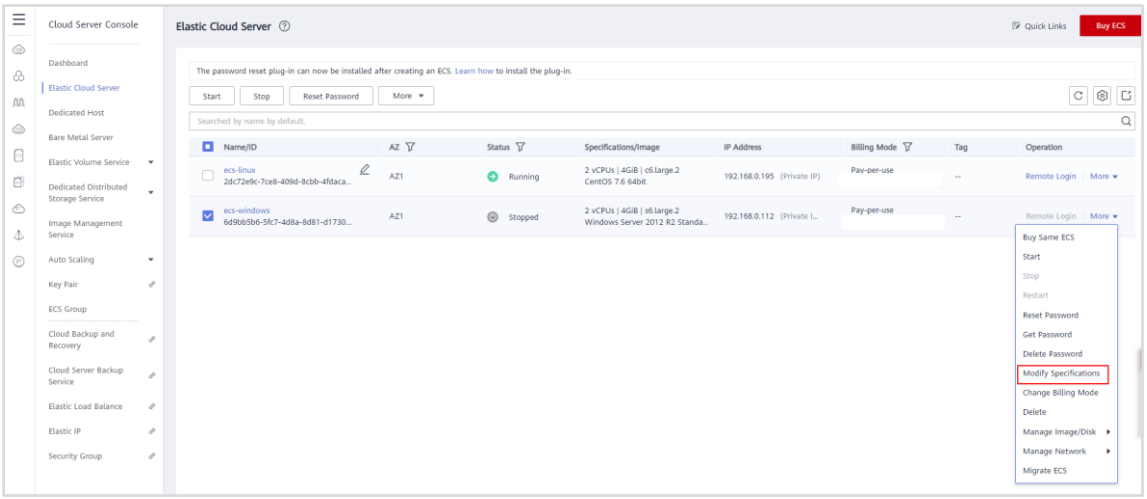


Figure 2-30 Modifying ECS Specifications

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

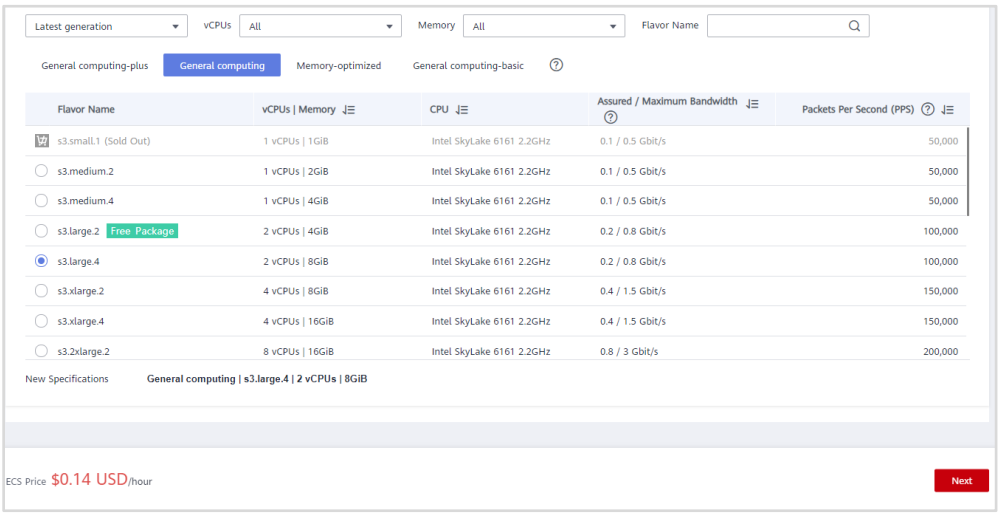


Figure 2-31 Choosing target specifications

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

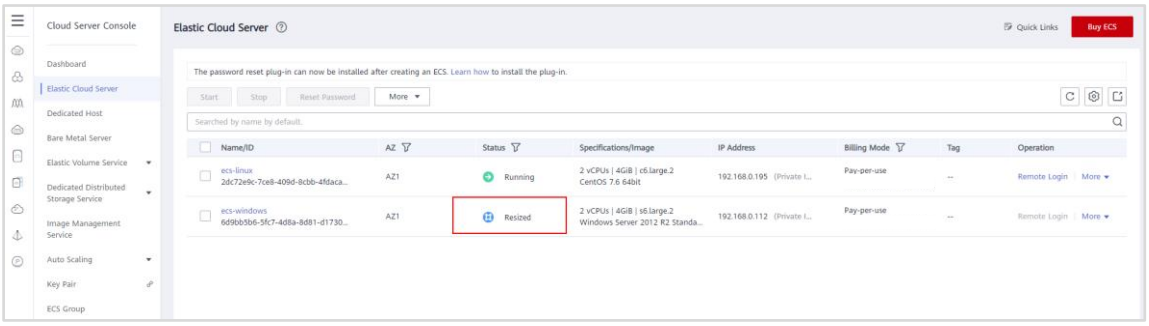


Figure 2-32 Specifications modifying

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

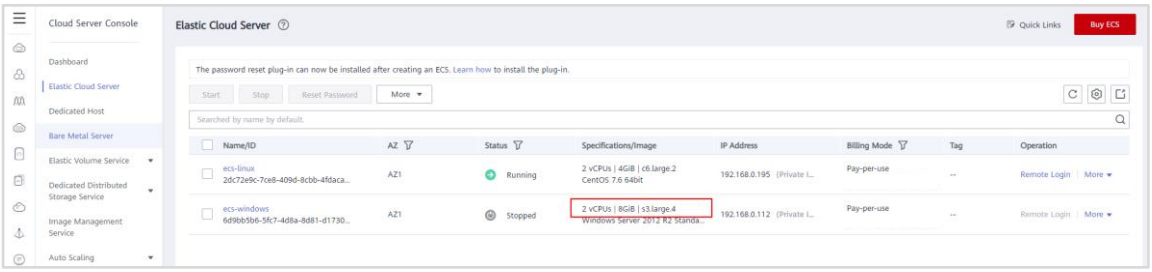


Figure 2-33 Specifications modified

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

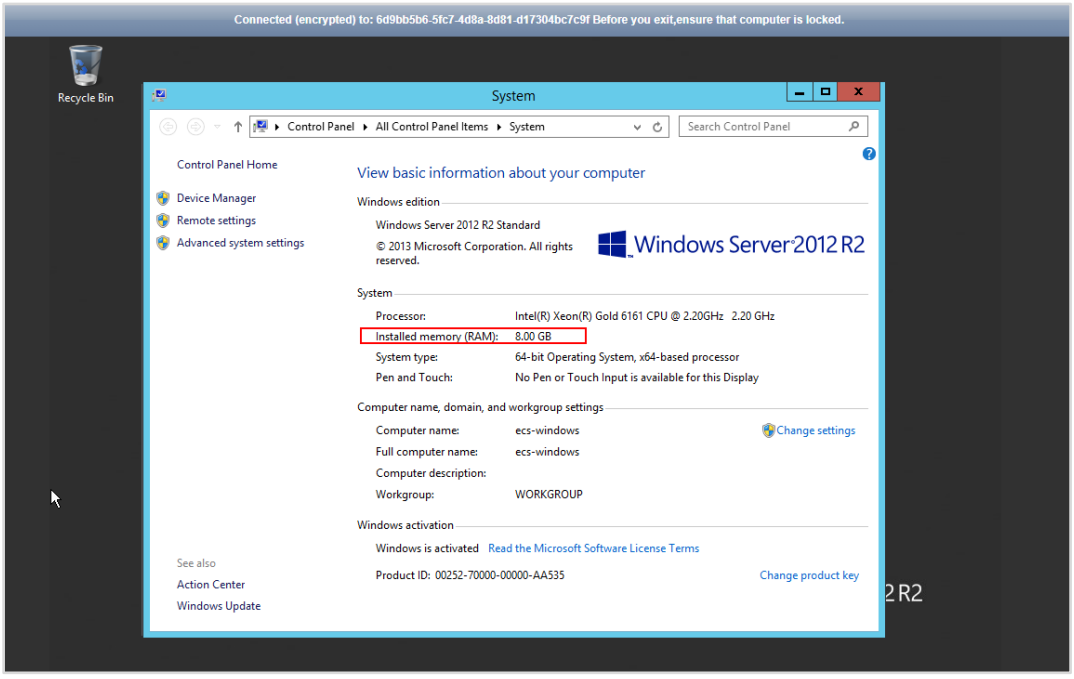


Figure 2-34 Confirming new specifications

2.2.3 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.

2.2.3.1 Configuring a Windows ECS

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

Step 1 Remotely log in to the ECS.

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

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

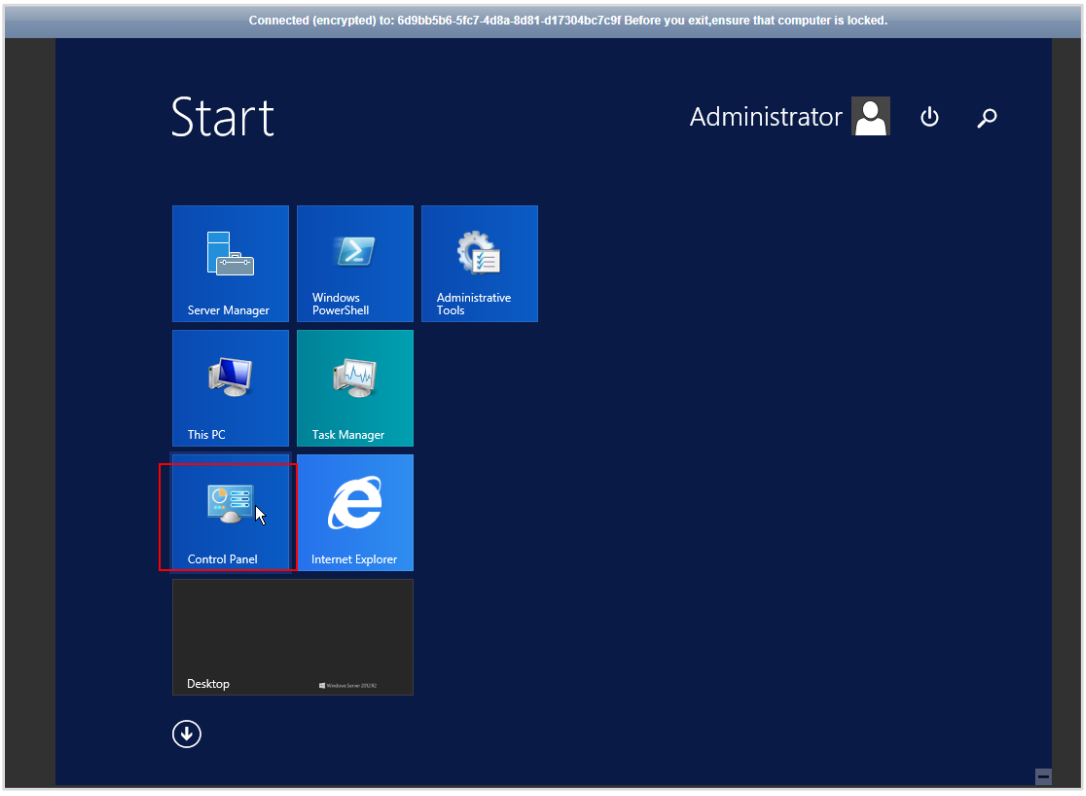


Figure 2-35 Control Panel

2. Click **Network and Sharing Center**.

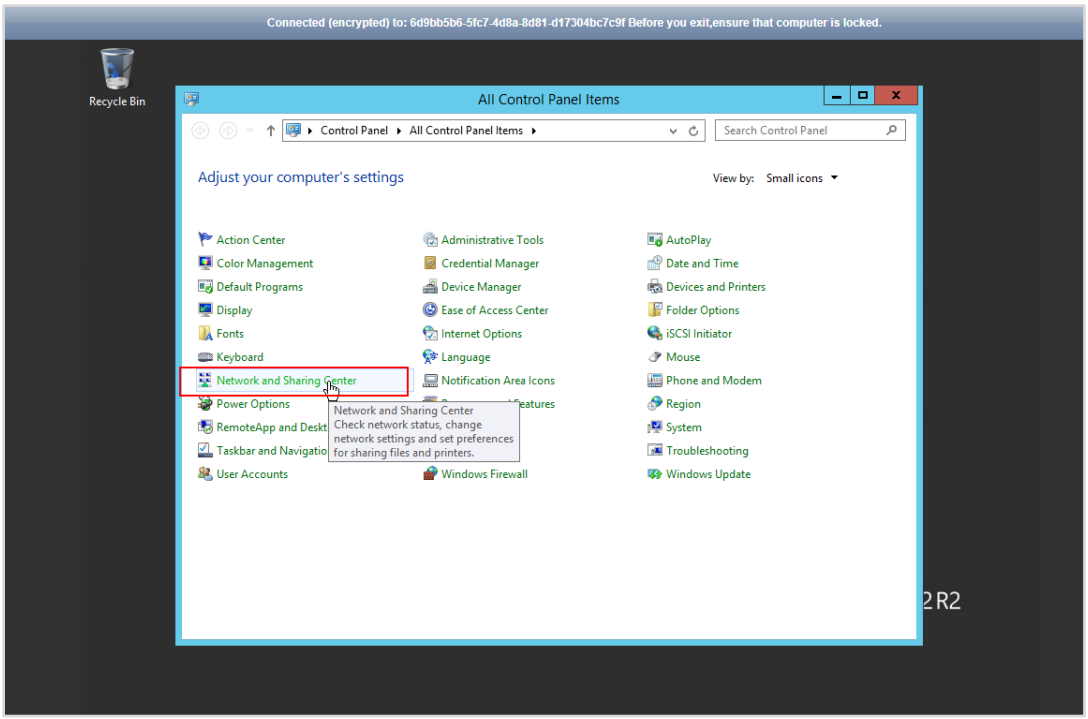


Figure 2-36 Network and Sharing Center

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

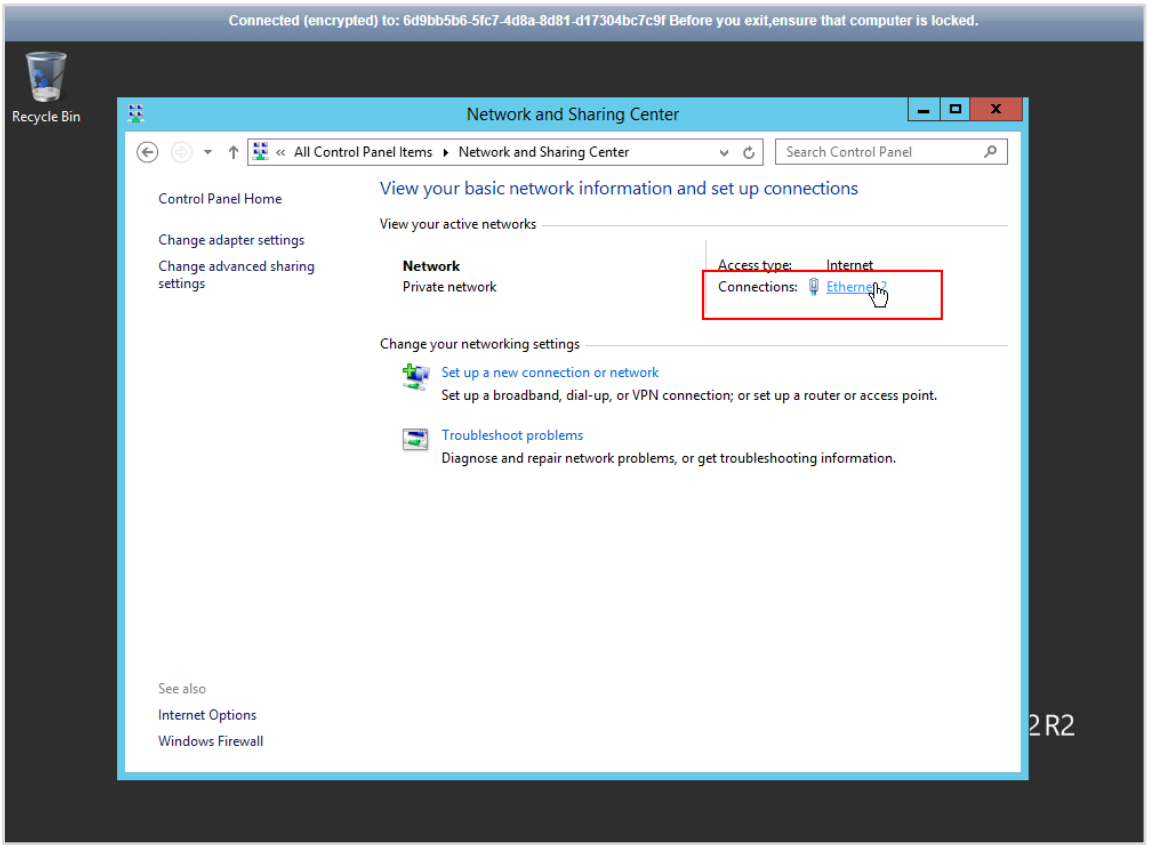


Figure 2-37 NIC

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

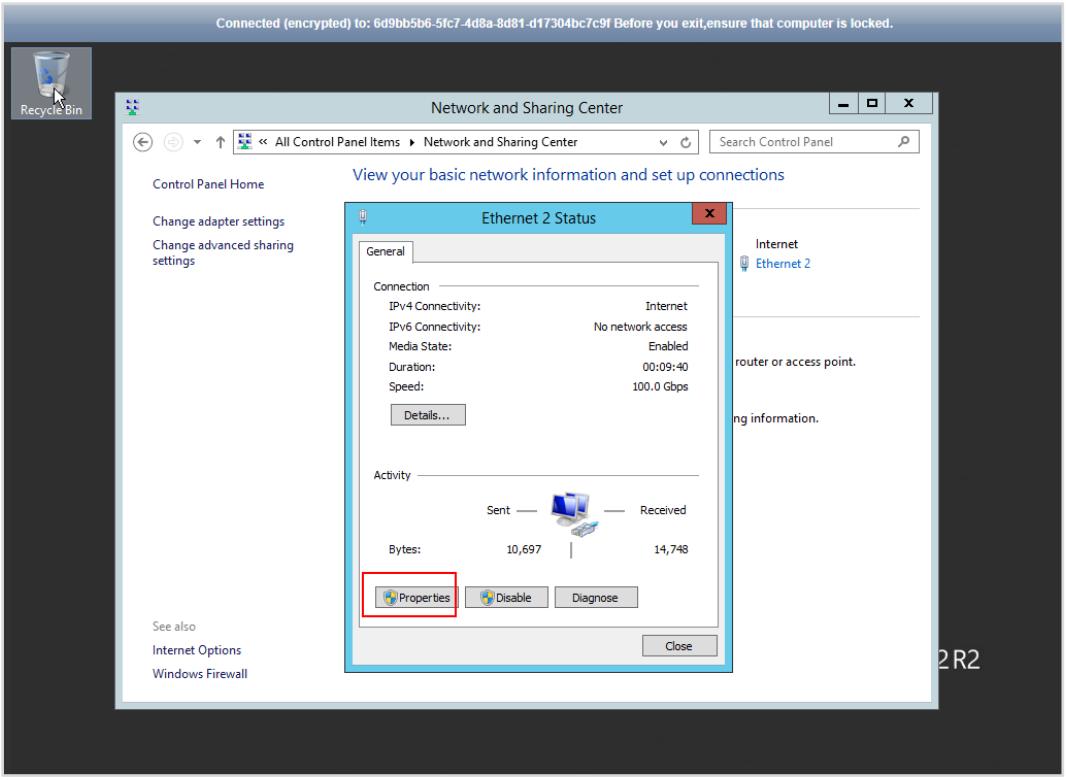


Figure 2-38 NIC properties

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**.

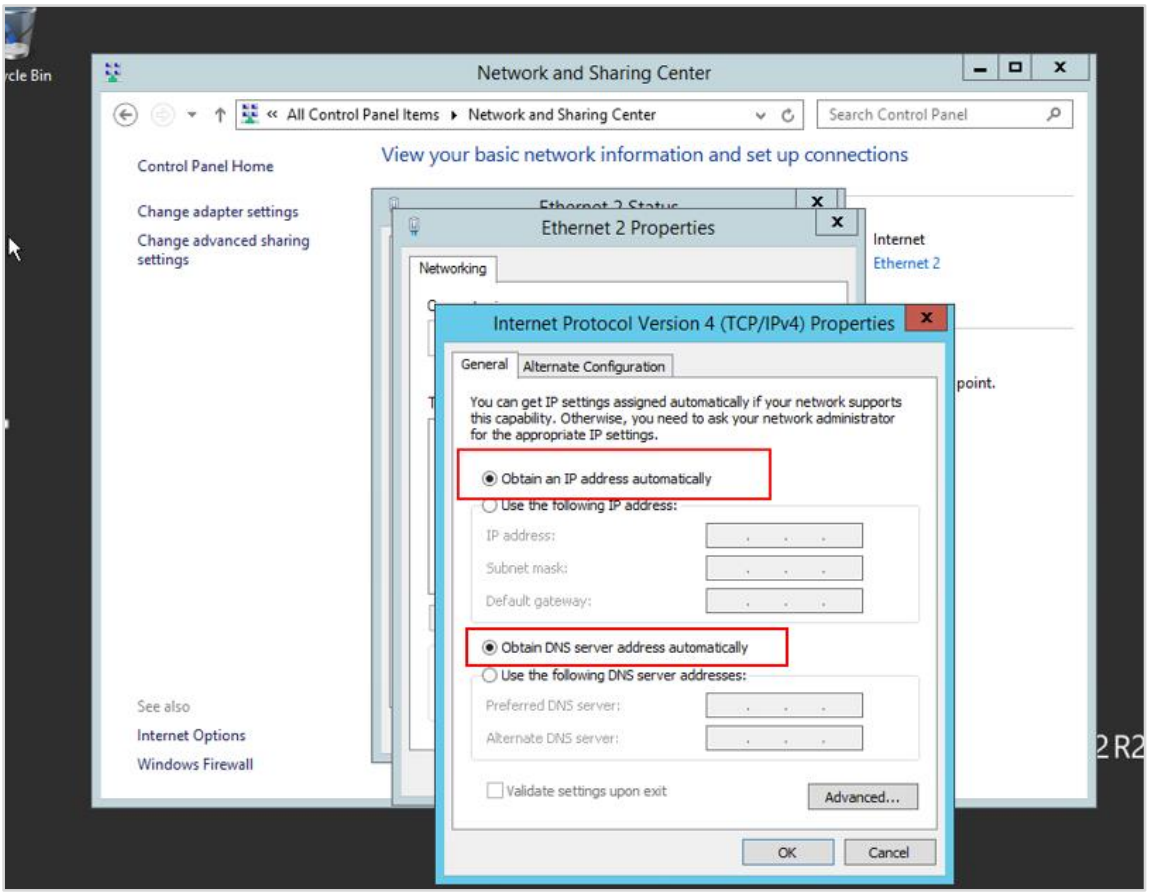


Figure 2-39 Configuring DHCP

Step 3 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.)

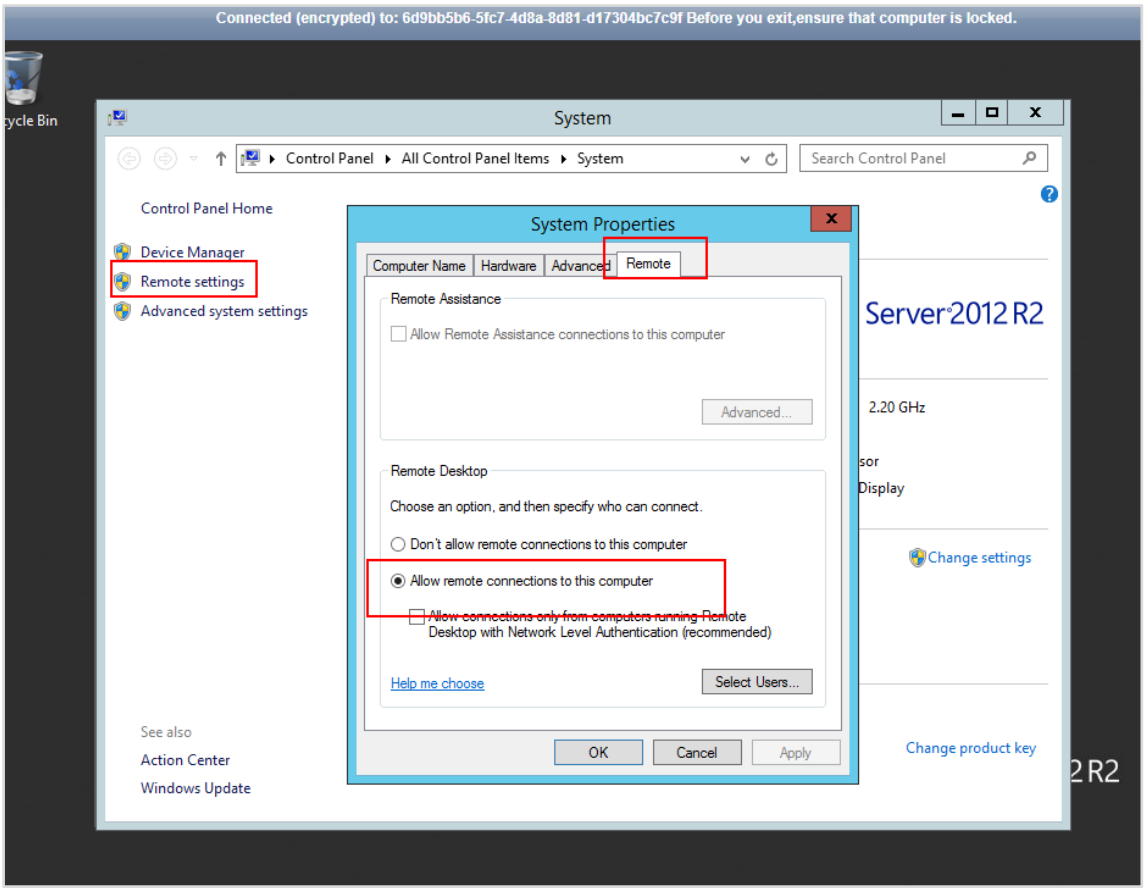


Figure 2-40 Configuring remote desktop

Step 4 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.

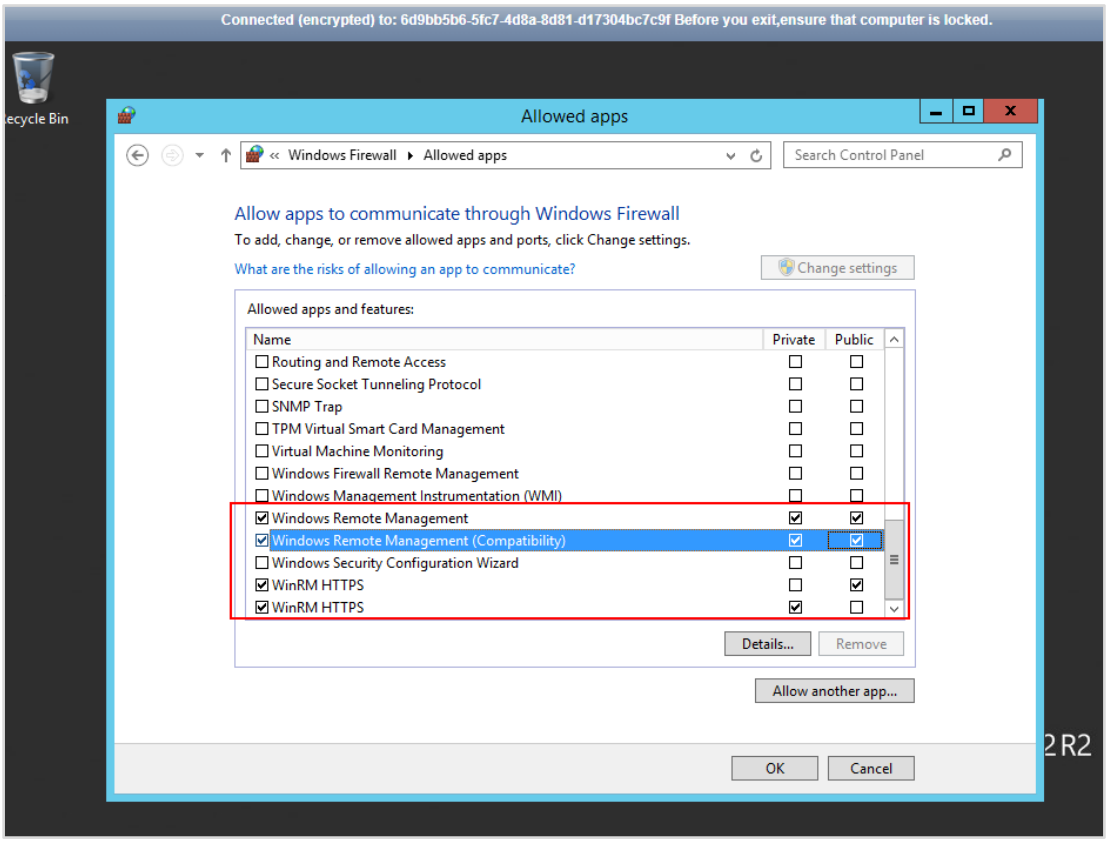


Figure 2-41 Configuring the firewall

Step 5 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.

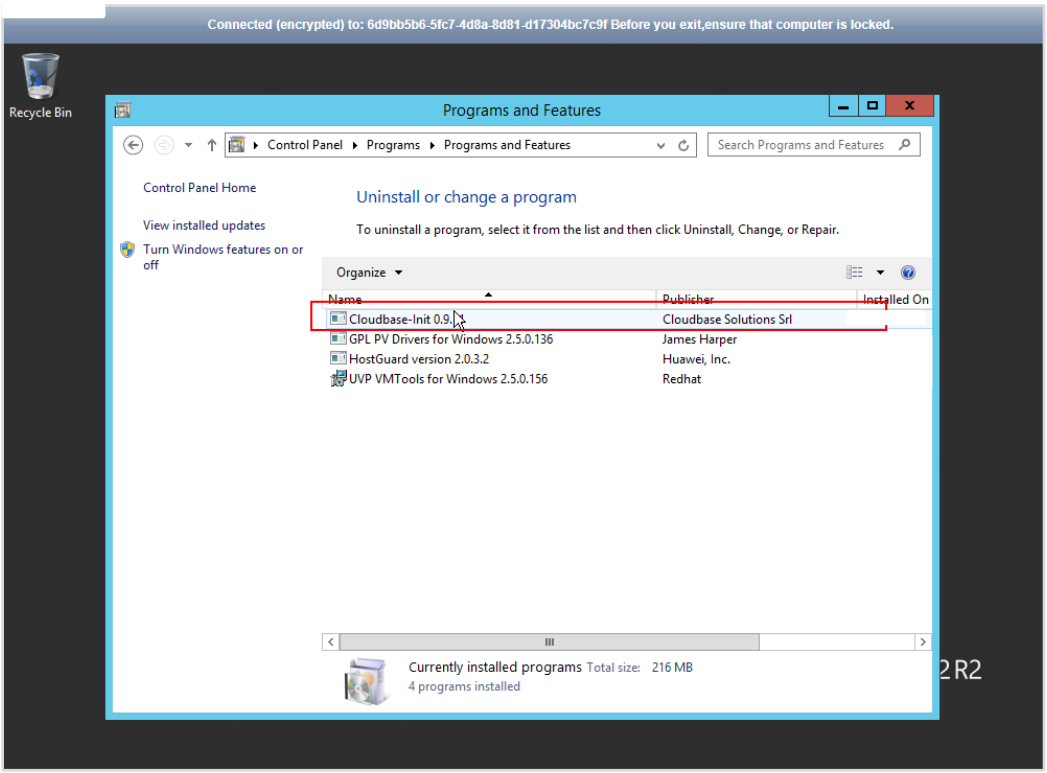


Figure 2-42 Checking whether Cloudbase-Init is installed

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.

2.2.3.2 Creating a Windows Private Image

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

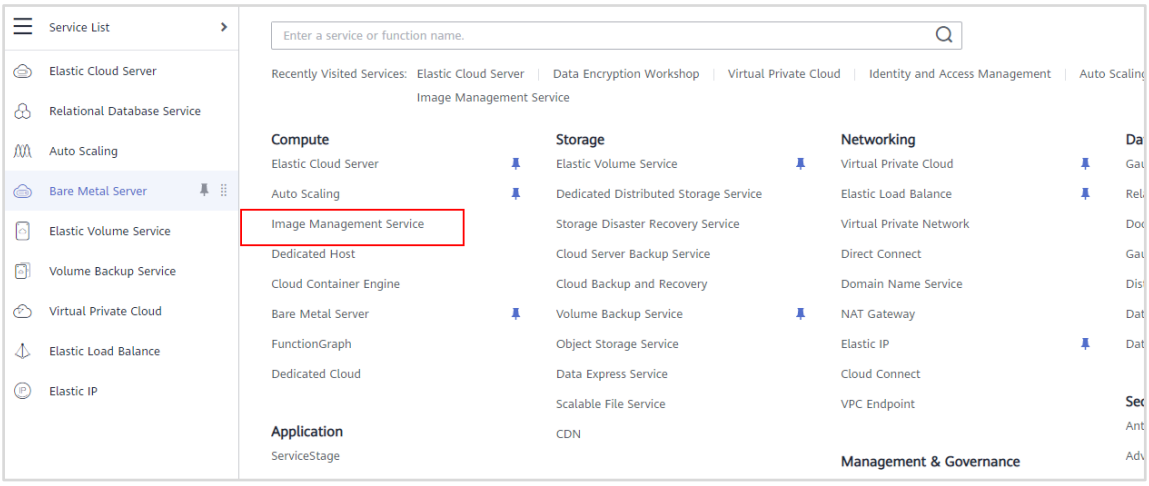


Figure 2-43 Accessing IMS

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

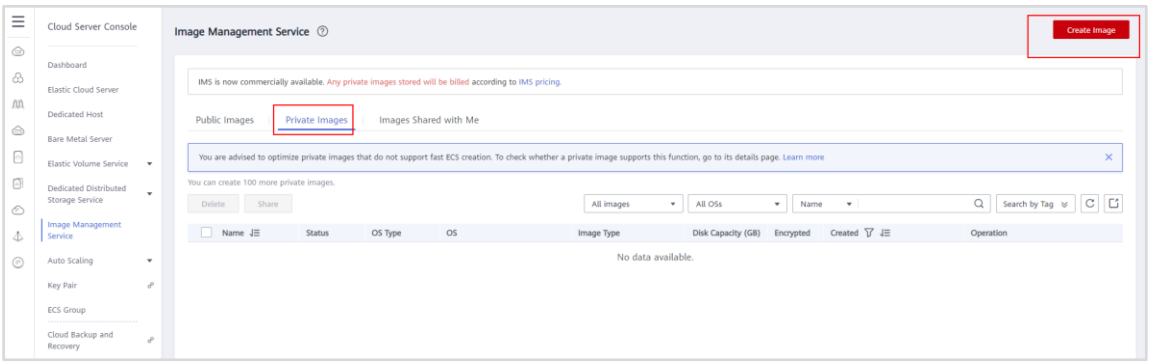


Figure 2-44 Creating a private image

Step 3 On the **Create Image** page, set the following parameters and click **Next**. (Retain the defaults for the rest of the parameters.)

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

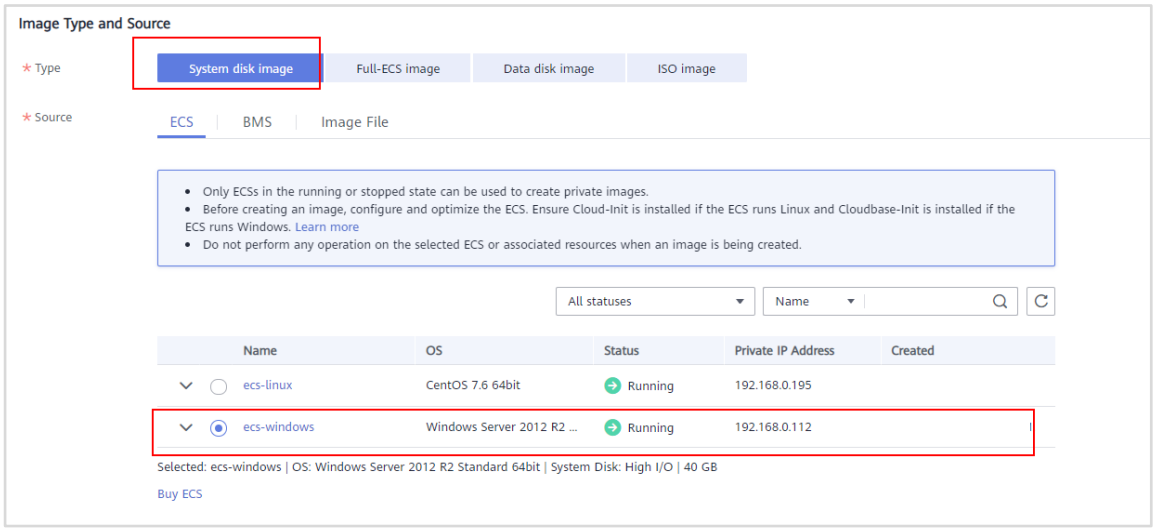


Figure 2-45 Setting private image parameters

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

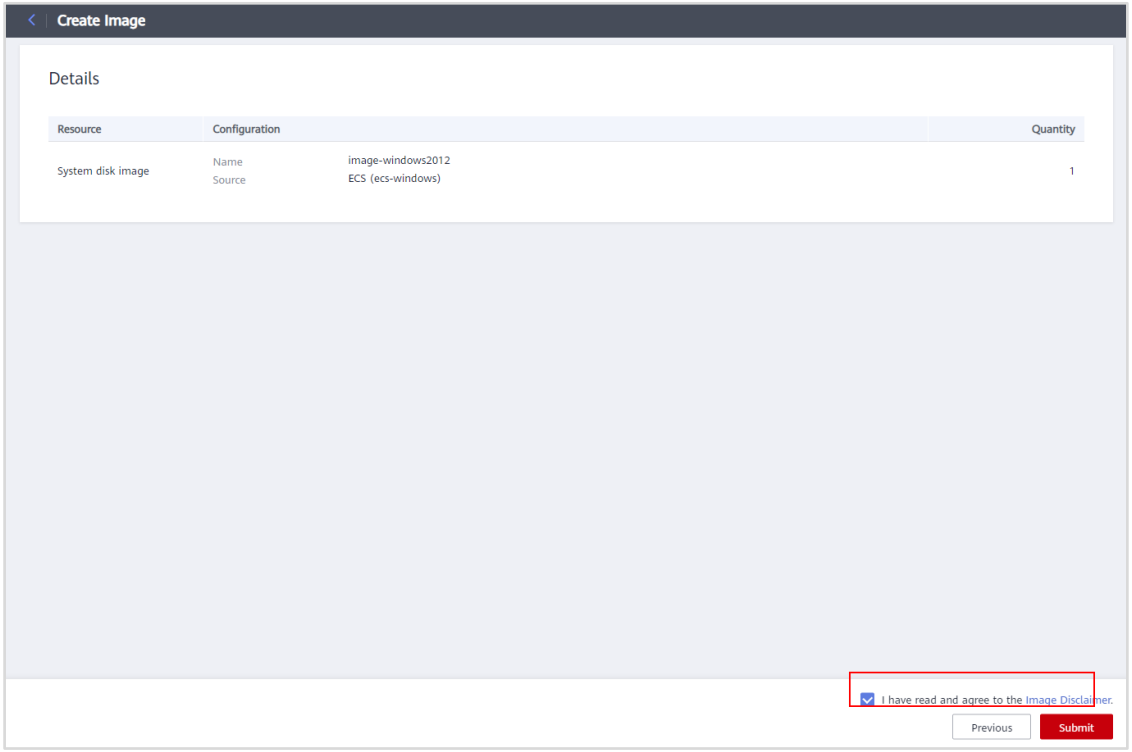


Figure 2-46 Confirming the primate image settings

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

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

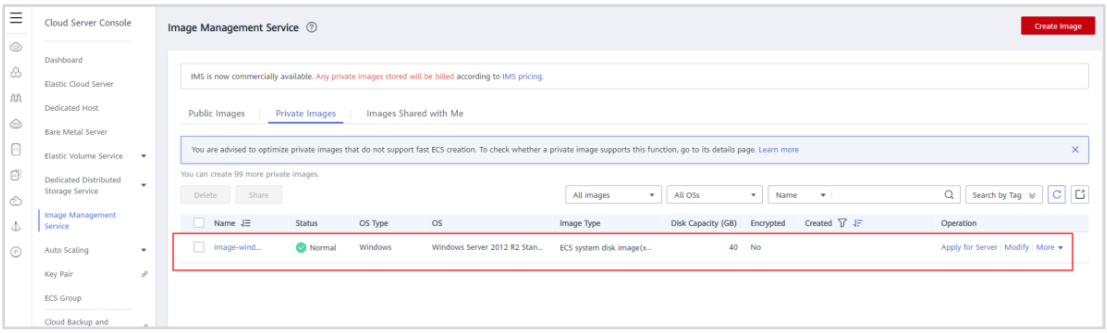


Figure 2-47 Viewing the private image status

2.2.3.3 Modifying Image Information

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

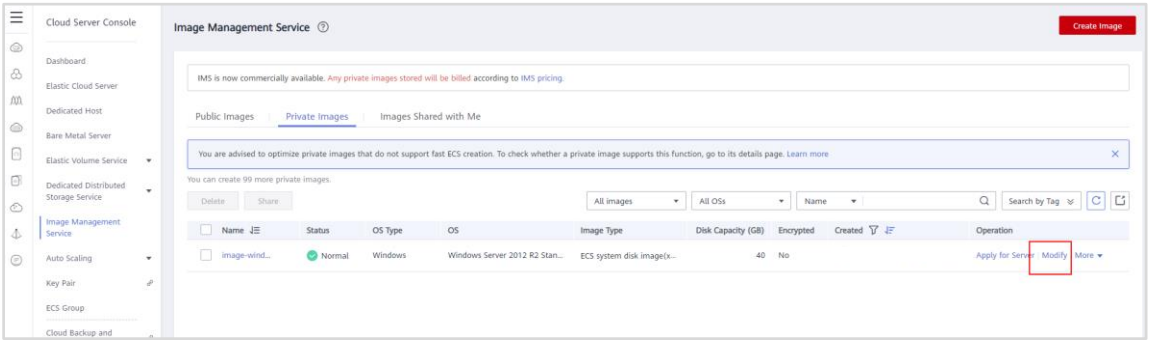


Figure 2-48 Modifying image information

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

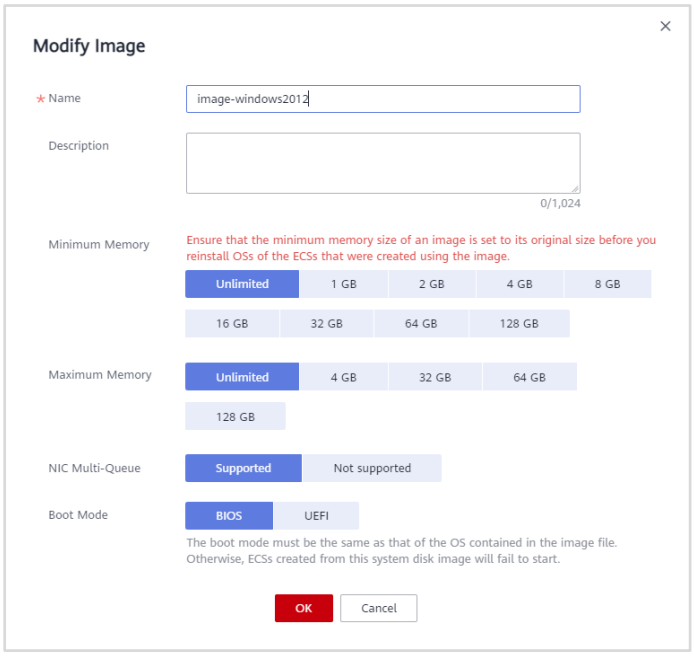


Figure 2-49 Parameters for image modification

2.2.3.4 Replicating an Image Within a Region

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

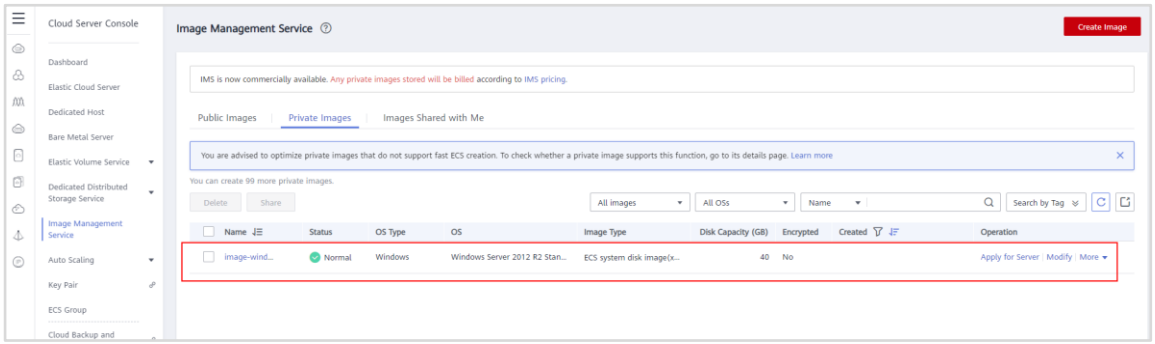


Figure 2-50 Viewing private images

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

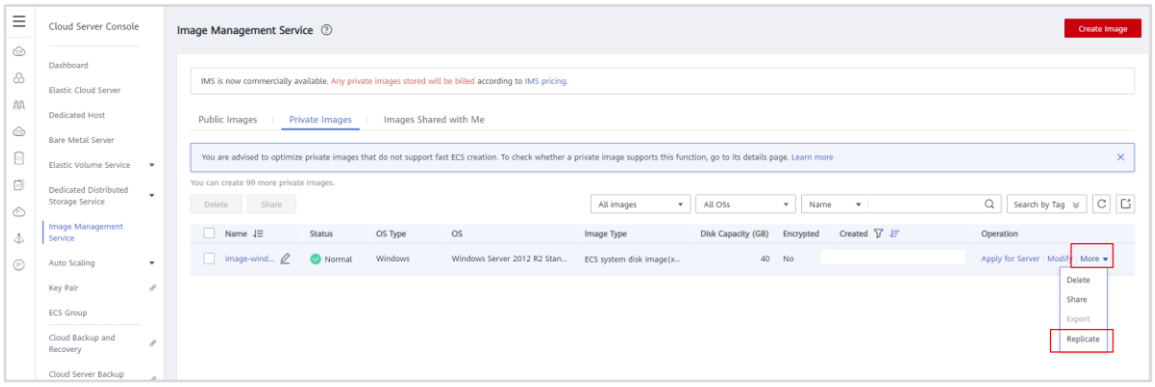


Figure 2-51 Replicating a private image

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

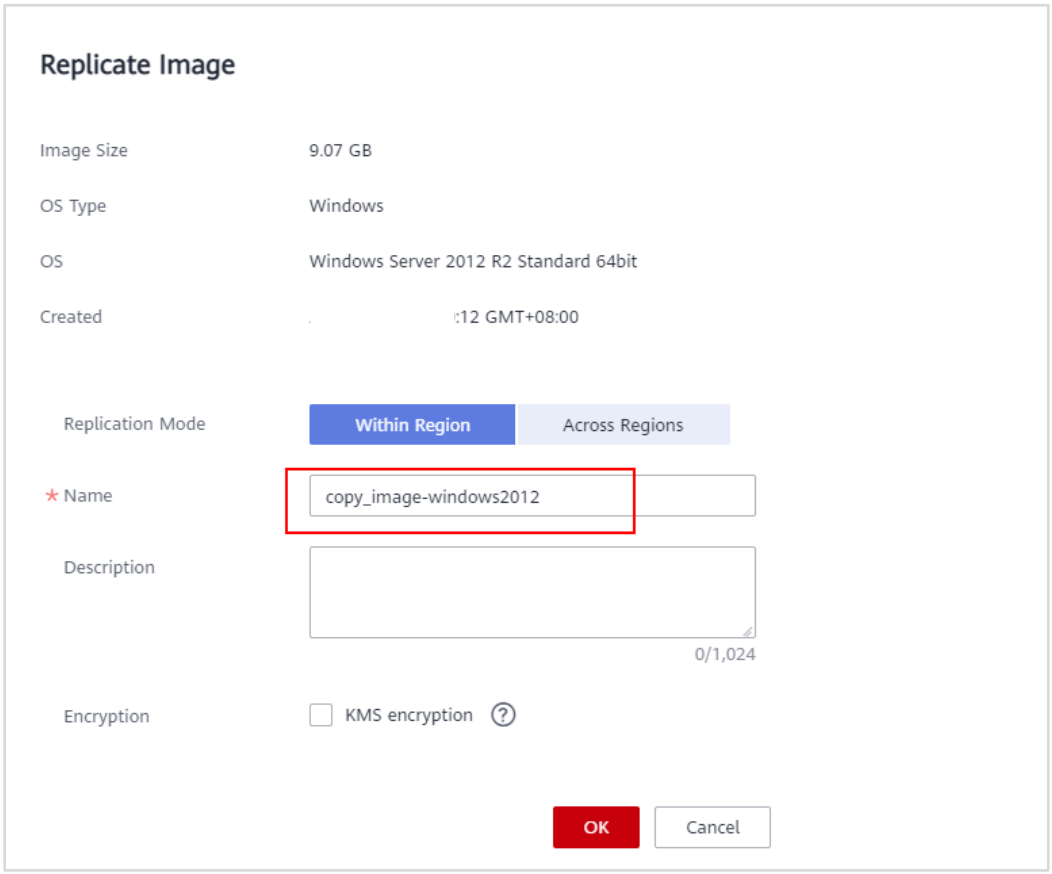


Figure 2-52 Parameters for in-region image replication

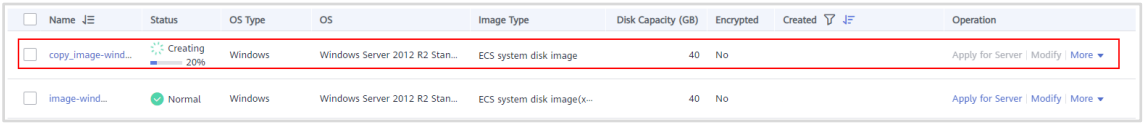


Figure 2-53 Replicated image

2.2.3.5 Sharing an Image

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

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

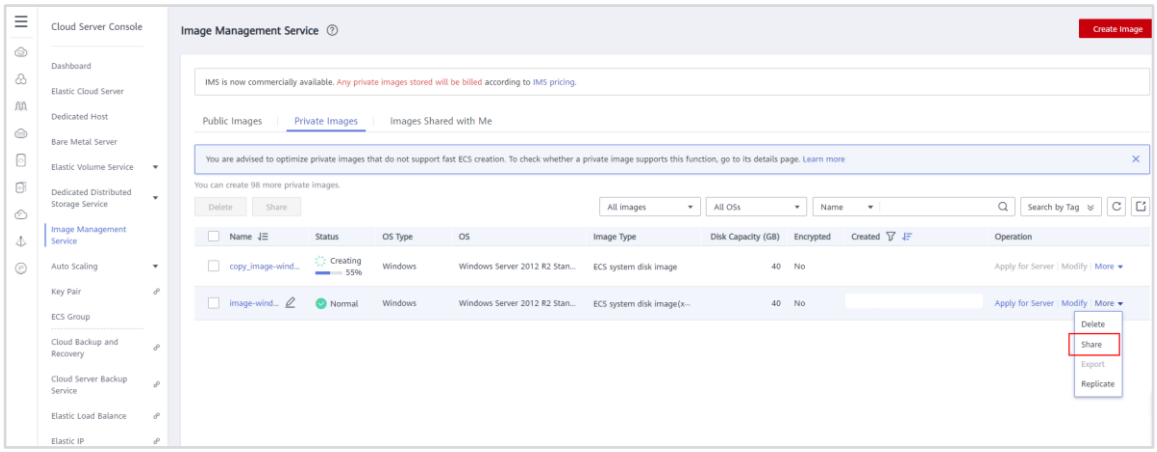


Figure 2-54 Sharing a private image

Step 2 In the **Share Image** dialog box, enter the account name 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).

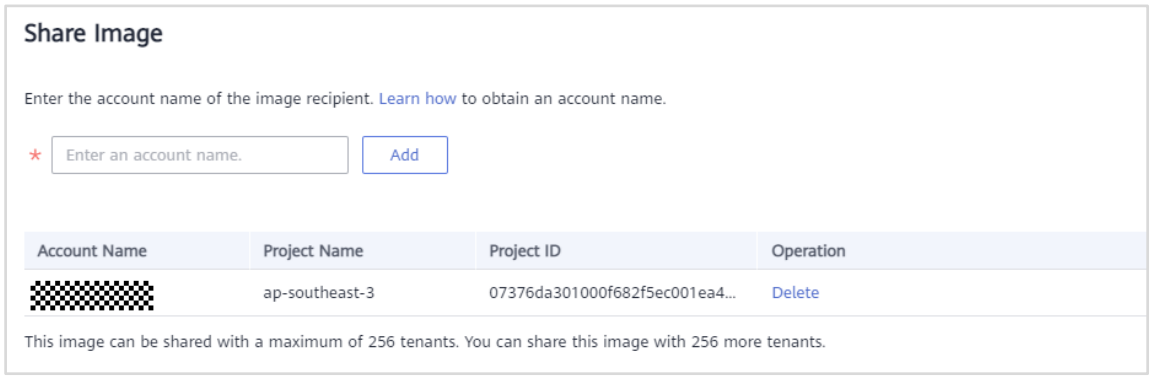


Figure 2-55 Sharing an image

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

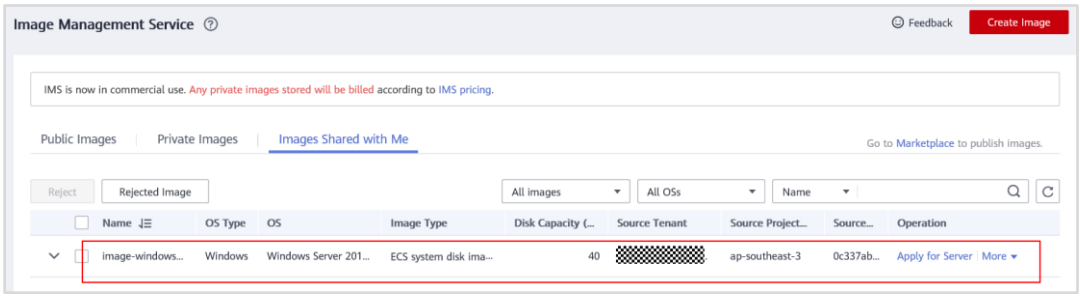


Figure 2-56 Accepting the shared image

2.2.3.6 Adding Tenants Who Can Use Shared Images

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

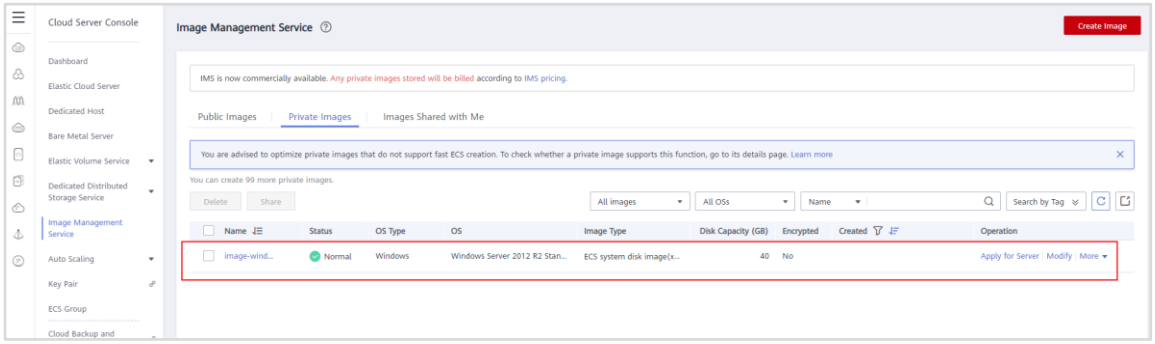


Figure 2-57 Viewing private images

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

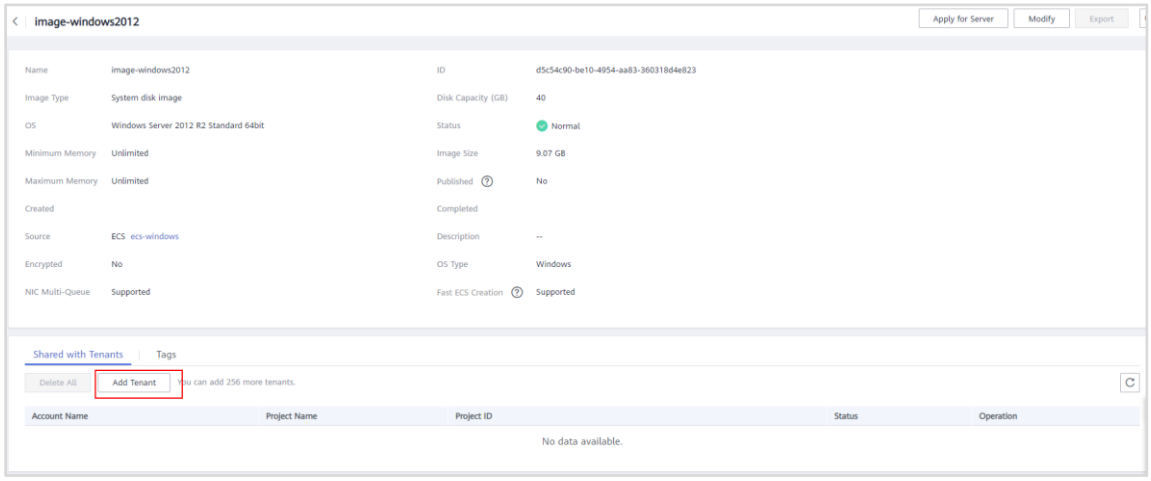


Figure 2-58 Adding tenants who can use the shared image

Step 3 In the **Add Tenant** dialog box, enter the account name (and project name if the tenant is a DeC or multi-project user) and click **Add**.

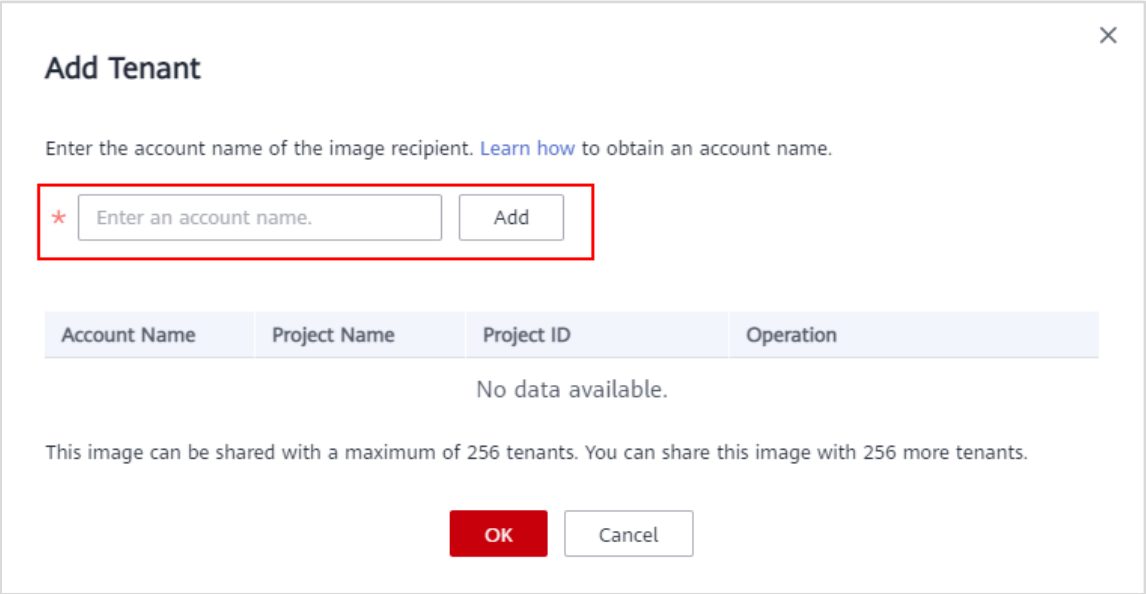


Figure 2-59 Adding tenants

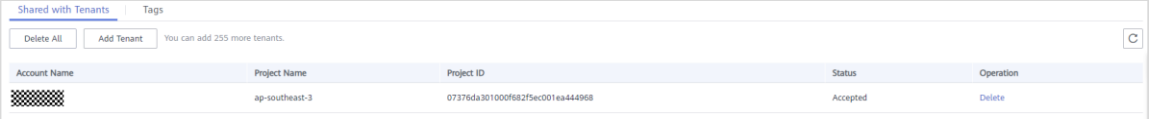


Figure 2-60 Added tenants

2.2.3.7 Applying for an ECS Using a Private Image

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

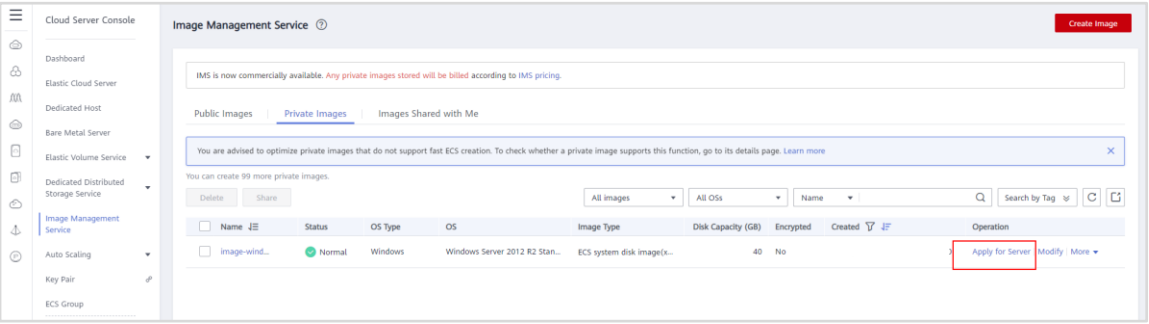


Figure 2-61 Applying for an ECS

Step 2 On the ECS purchase page, ensure that the private image is selected.

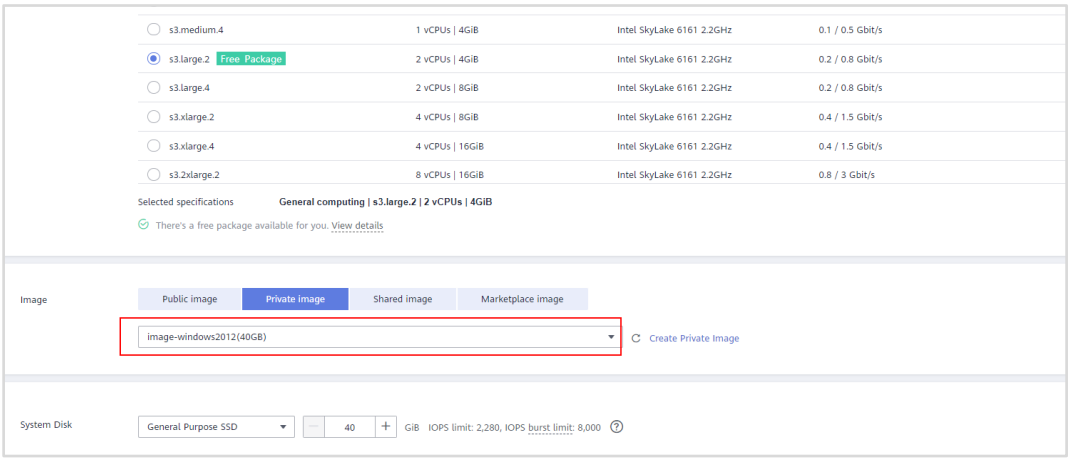


Figure 2-62 Creating an ECS using a private image

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

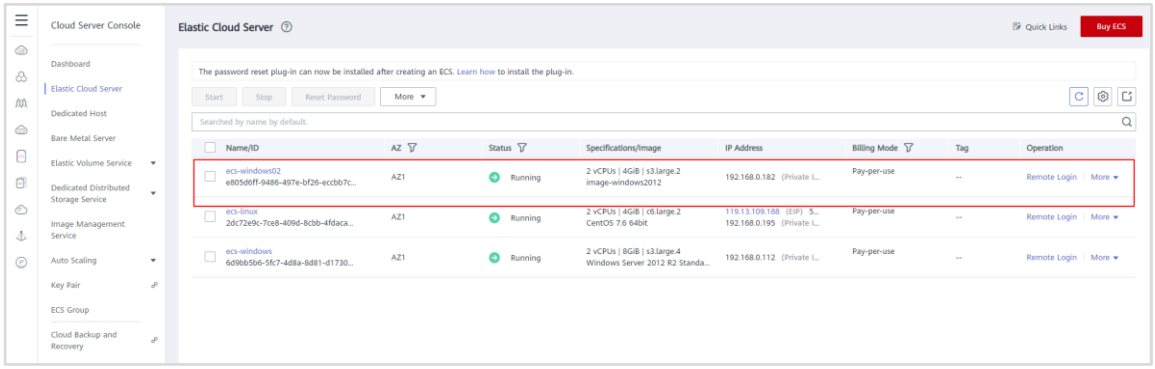


Figure 2-63 Viewing the ECS

2.2.4 Creating a Linux System Disk Image from an ECS

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

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

2.2.4.1 Configuring a Linux ECS

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

Step 1 Remotely log in to the ECS.

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

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

```
[root@ecs-linux ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Figure 2-64 Opening the NIC configuration file

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

Figure 2-65 Checking whether DHCP is configured

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

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

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

```
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

/CloudrResetPwdAgent:
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 2-66 Checking whether CloudResetPwdAgent is installed

Step 4 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:

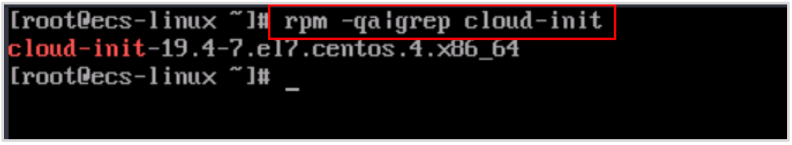


Figure 2-67 Checking whether Cloud-Init is installed

- 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
```

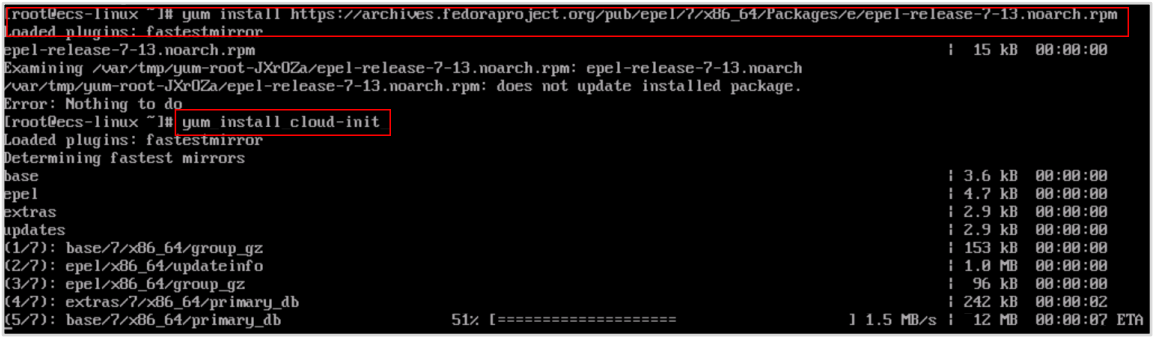


Figure 2-68 Installing Cloud-Init

Step 5 Delete files from the network rule directory.

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

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

```
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 2-69 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.

2.2.4.2 Creating a Linux Private Image

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

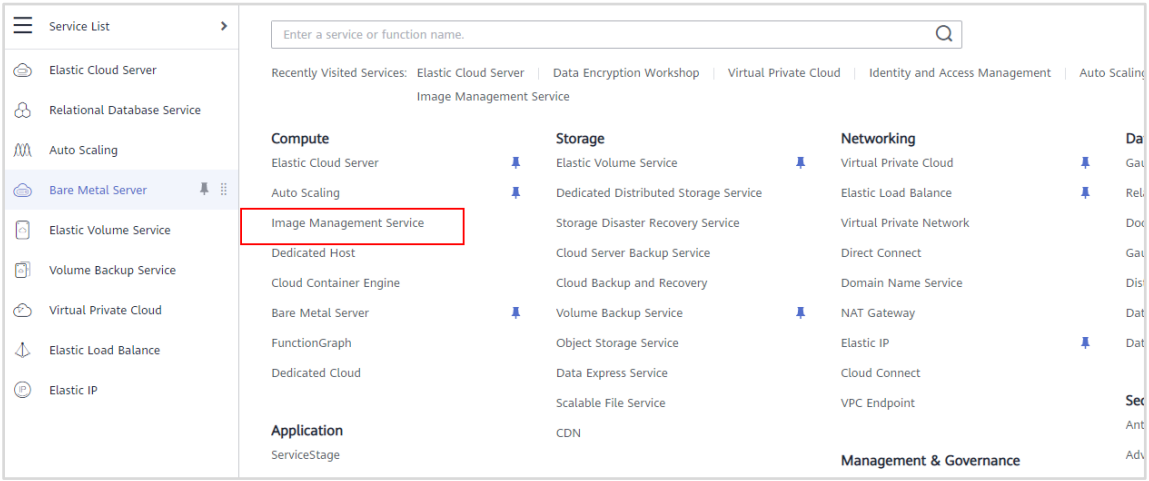


Figure 2-70 Accessing IMS

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

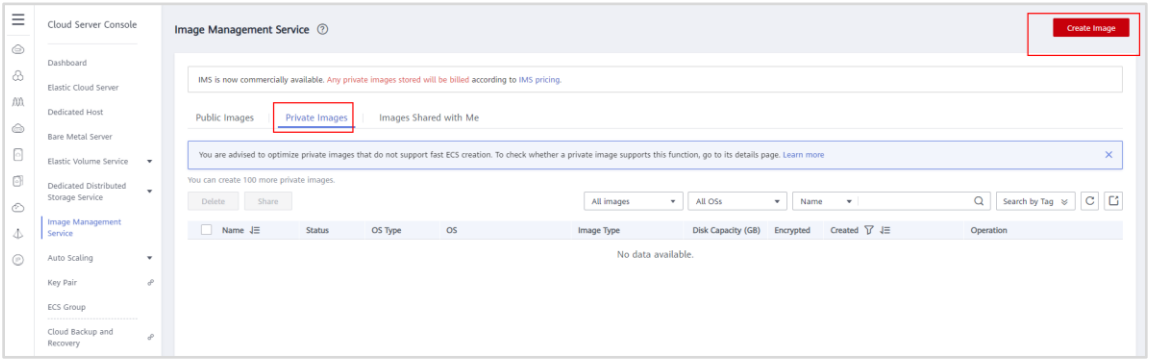


Figure 2-71 Creating a private image

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

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

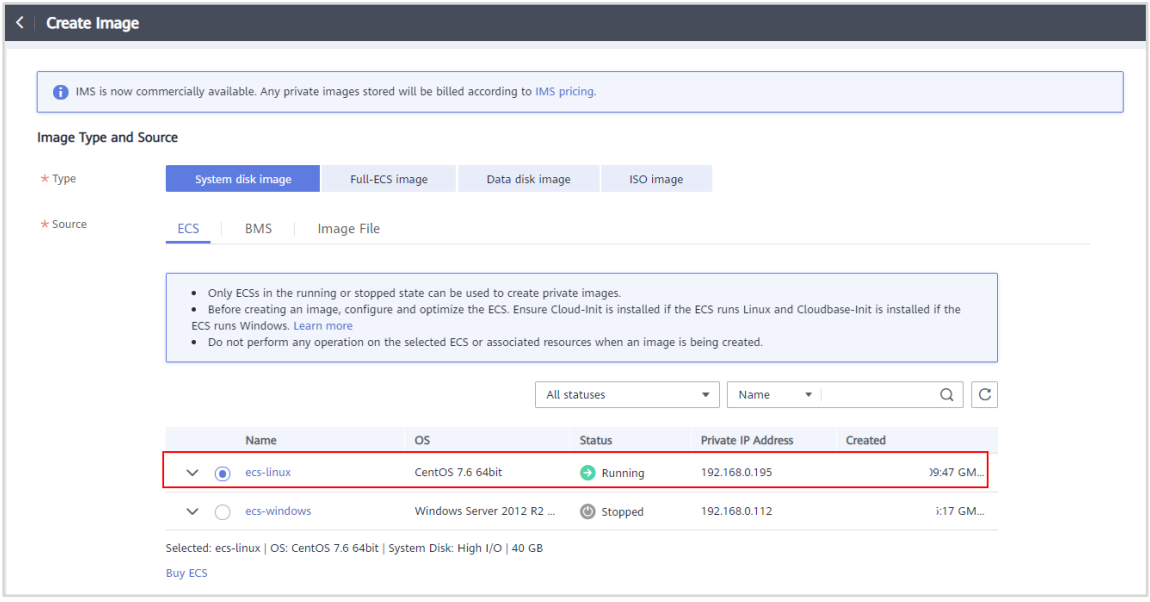


Figure 2-72 Setting private image parameters (1)

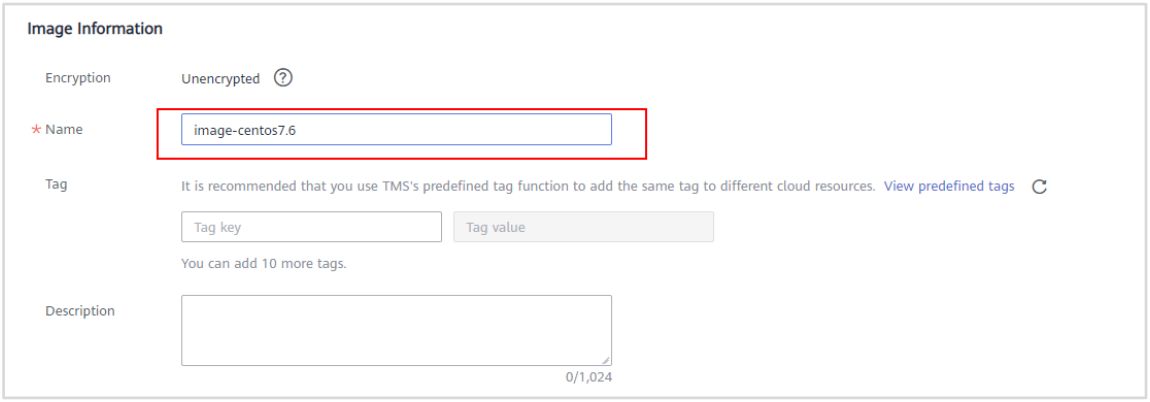


Figure 2-73 Setting private image parameters (2)

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

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

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

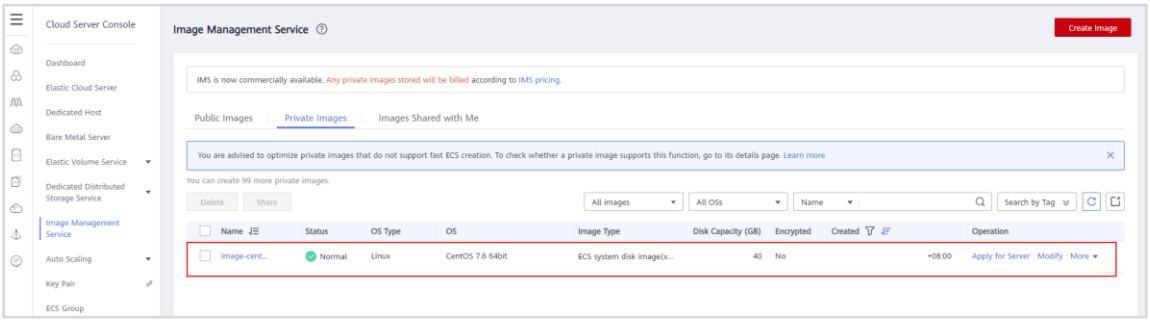


Figure 2-74 Viewing the private image status

2.2.5 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.

2.2.5.1 Creating an AS Configuration

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

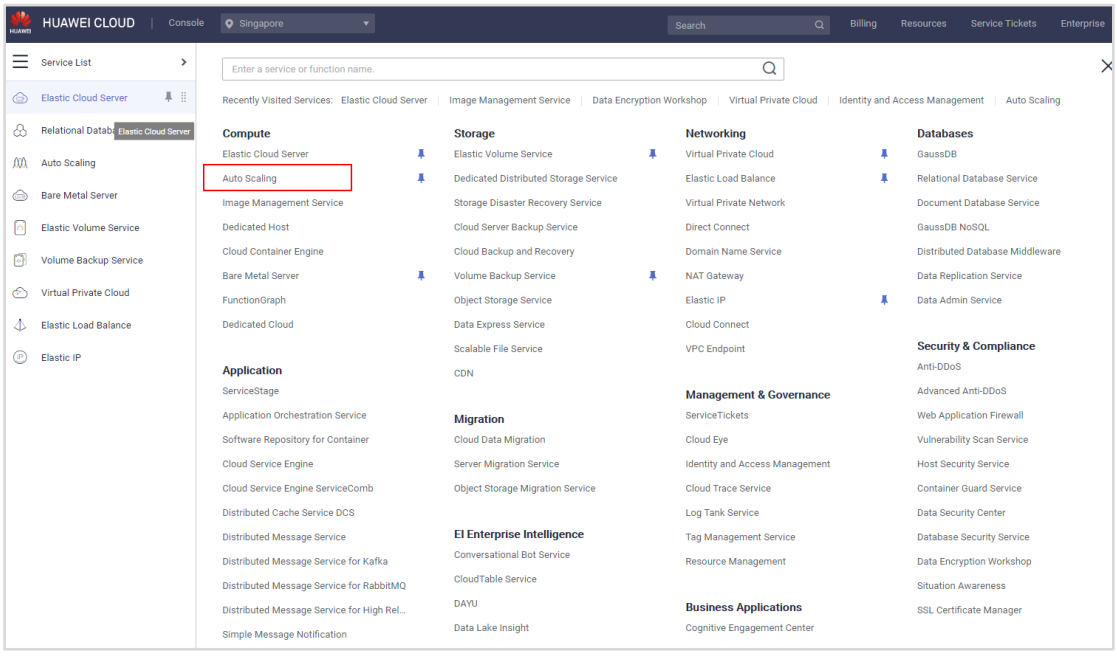


Figure 2-75 Accessing AS

Step 2 Click **Create AS Configuration**.

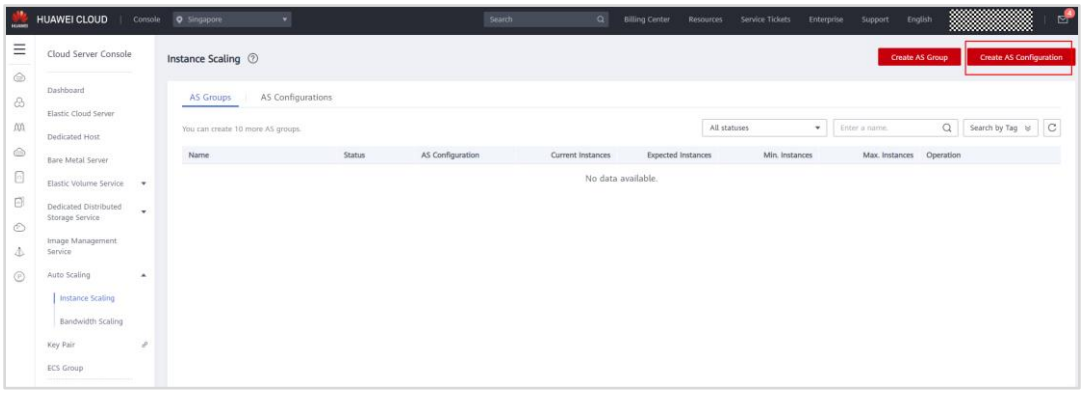


Figure 2-76 Creating an AS configuration

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

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

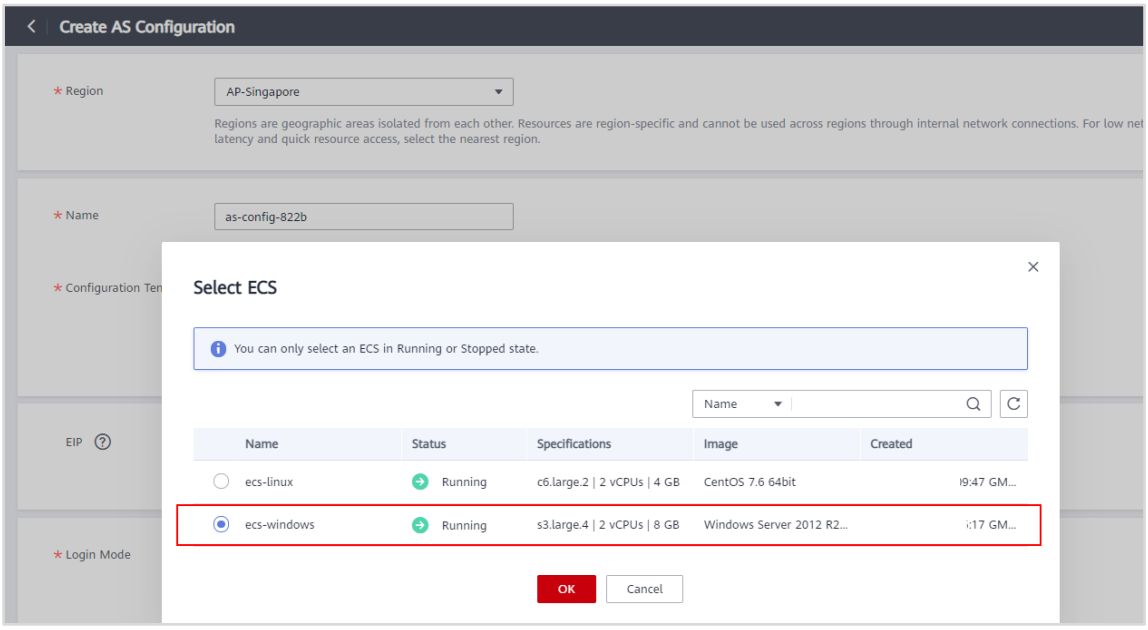


Figure 2-77 Selecting a configuration template

- **EIP**: **Automatically assign**
- **Type**: **Dynamic BGP**
- **Billed By**: **Bandwidth**
- **Bandwidth**: **5 Mbit/s**
- **Login Mode**: **Key pair**

- **Key Pair**: Select the created key pair.

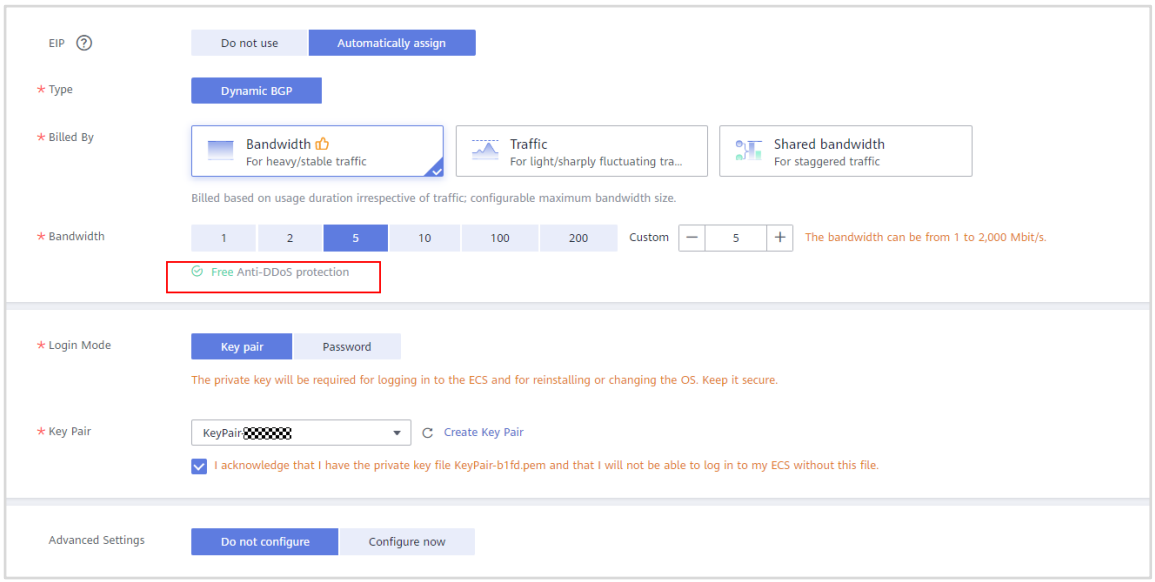


Figure 2-78 Configuring scaling parameters

Step 4 Click **Create Now**.

Request submitted successfully is displayed.

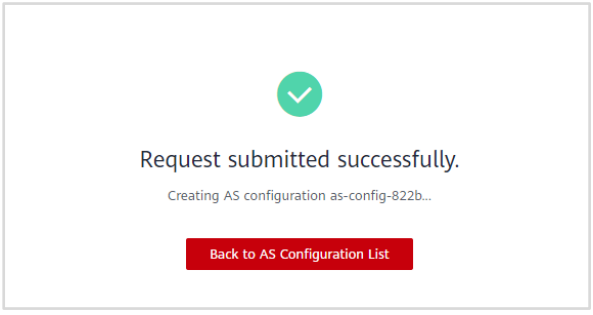


Figure 2-79 AS configuration created

Step 5 In the AS configuration list, view the created AS configuration **as-config-822b**.

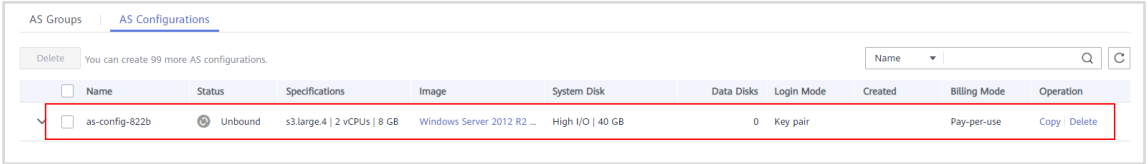


Figure 2-80 Viewing the AS configuration

2.2.5.2 Creating an AS Group

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

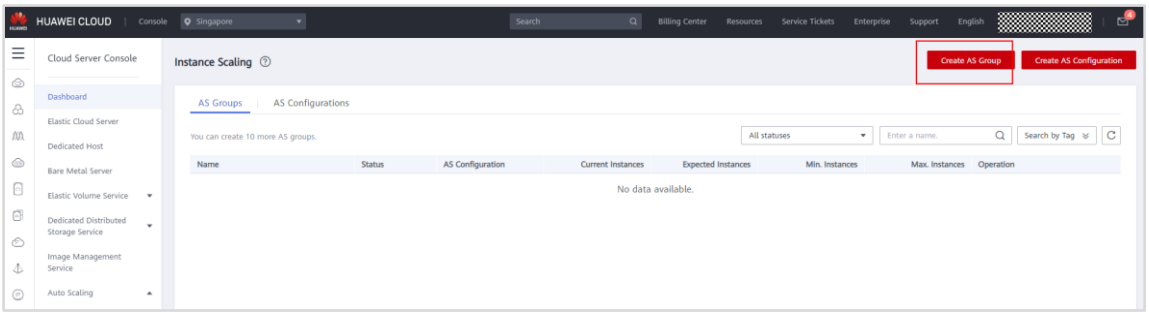


Figure 2-81 Creating an AS group

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

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

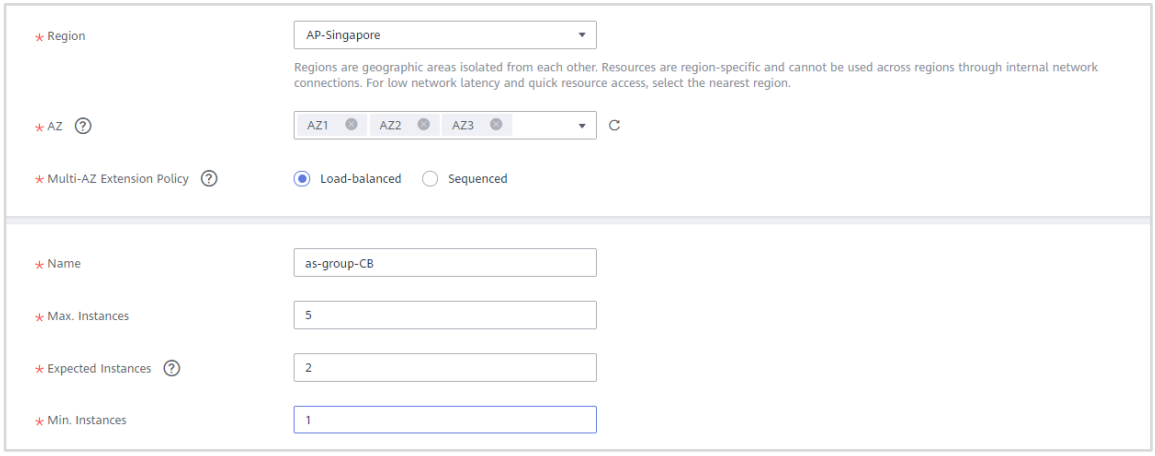


Figure 2-82 Configuring AS group parameters

- **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**

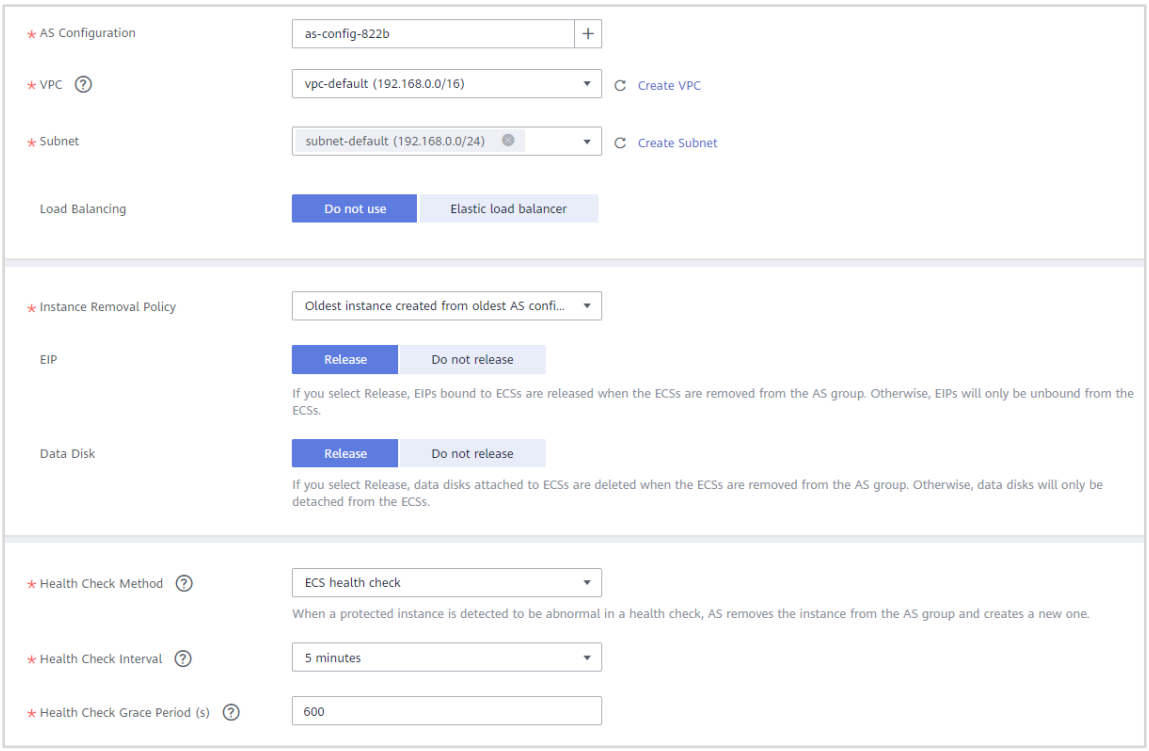


Figure 2-83 Configuring an AS group

Step 3 Click **Back to AS Group List**.

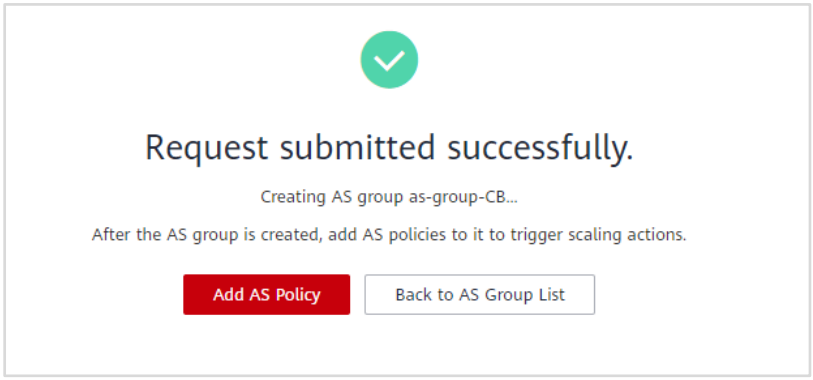


Figure 2-84 AS group created

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

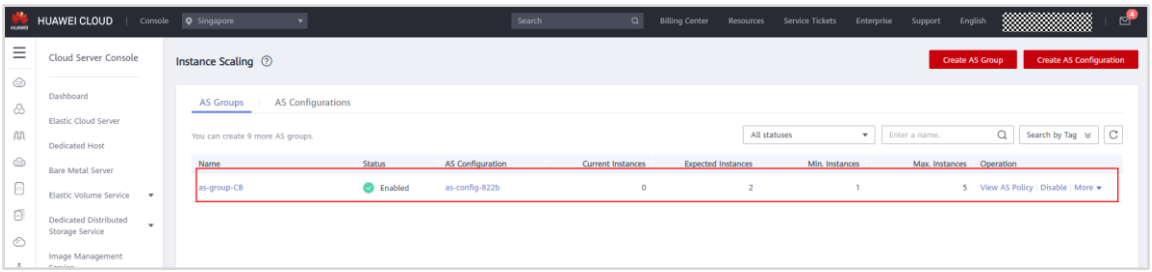


Figure 2-85 Viewing the AS group

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

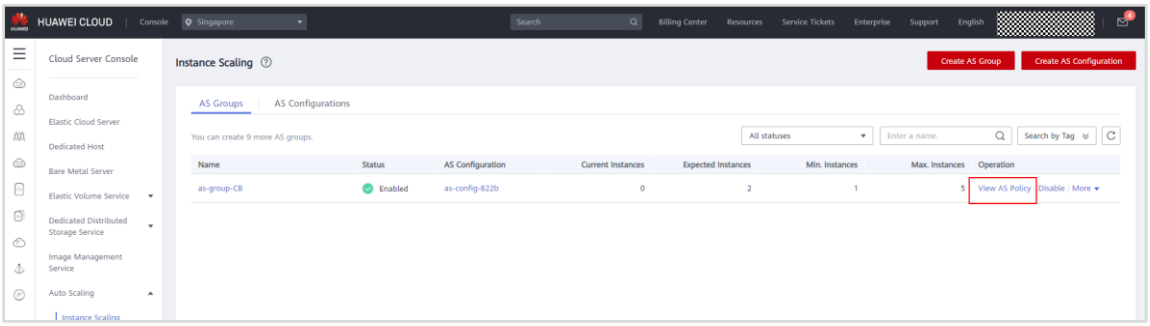


Figure 2-86 View AS Policy

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

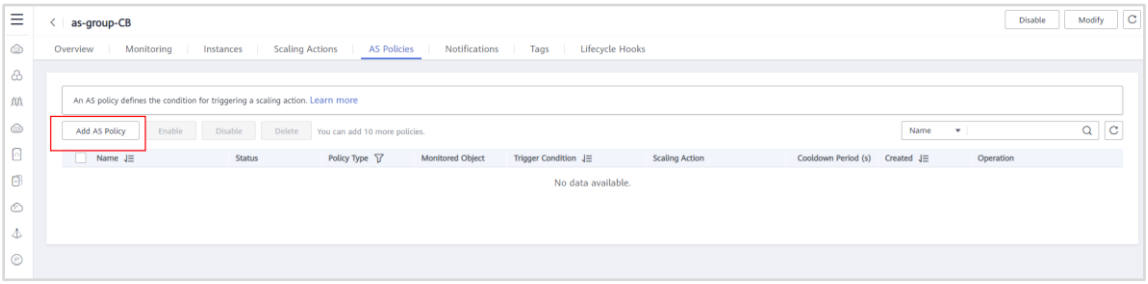


Figure 2-87 Adding an AS policy

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

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

- **Policy Name**: **as-policy-test1**
- **Policy Type**: **Periodic**
- **Interval**: **One day**
- **Triggered At**: **18:00**
- **Time Range**: Retain the default settings.
- **Scaling Action**: **Add 1 instance**

- **Cooldown Period (s)**: **900**

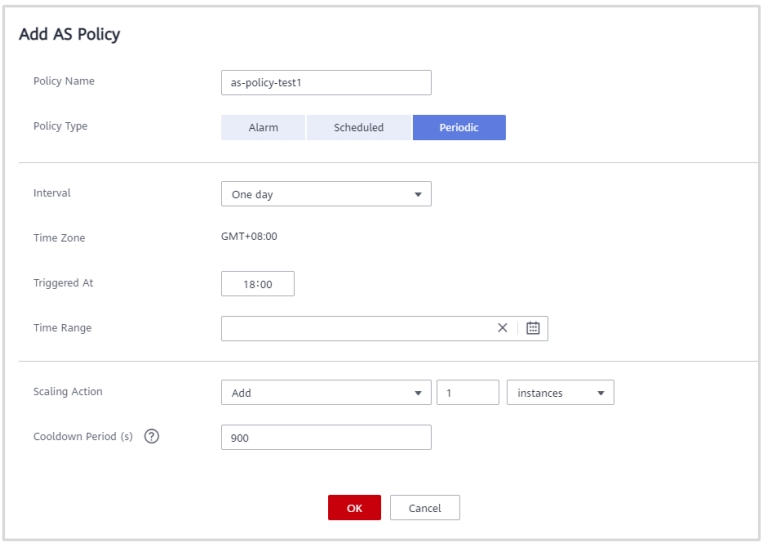


Figure 2-88 Configuring an AS policy

Step 8 Click **OK**.

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

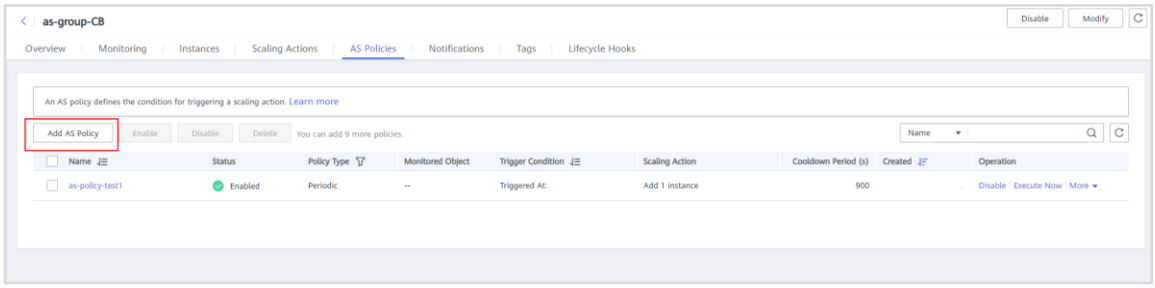


Figure 2-89 Adding another AS policy

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

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

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

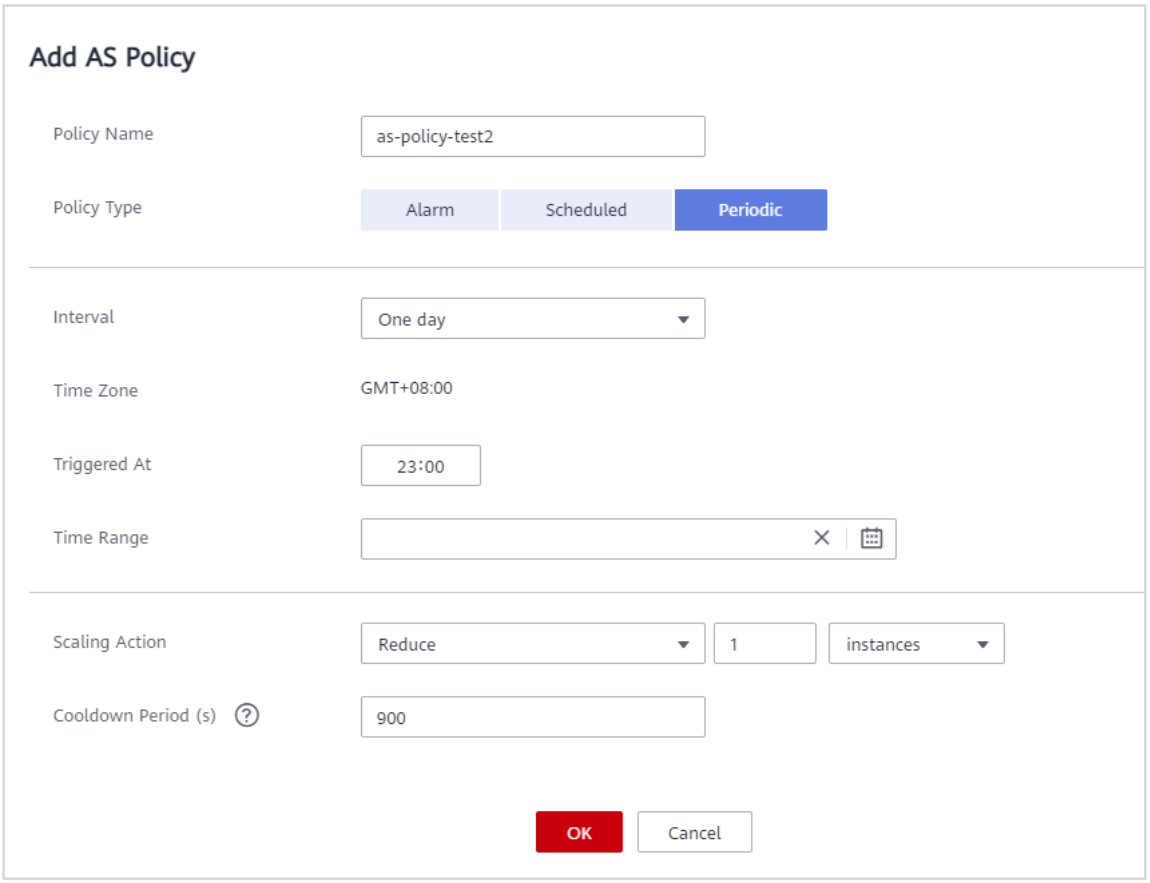


Figure 2-90 Configuring another AS policy

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

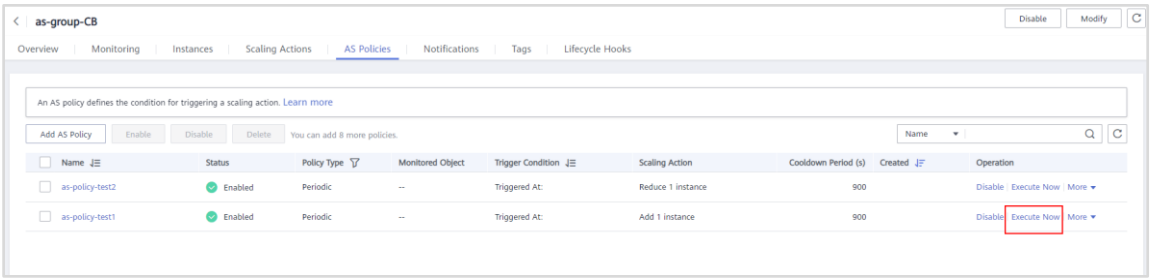


Figure 2-91 Executing an AS policy

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

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

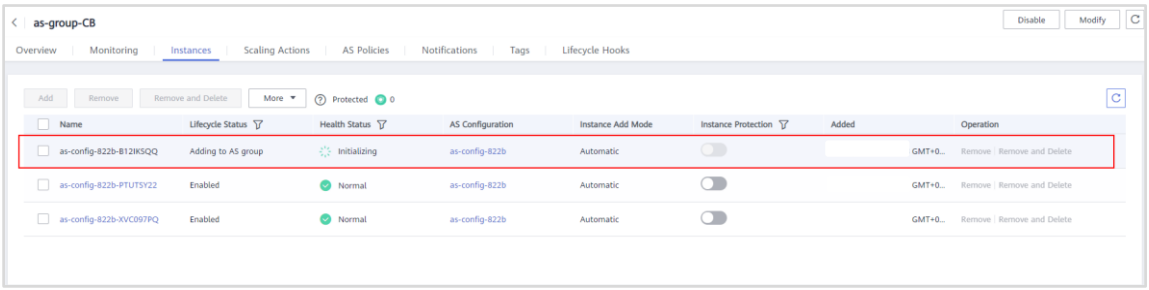


Figure 2-92 Viewing instance scaling

2.2.5.3 Creating a Bandwidth Scaling Policy

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

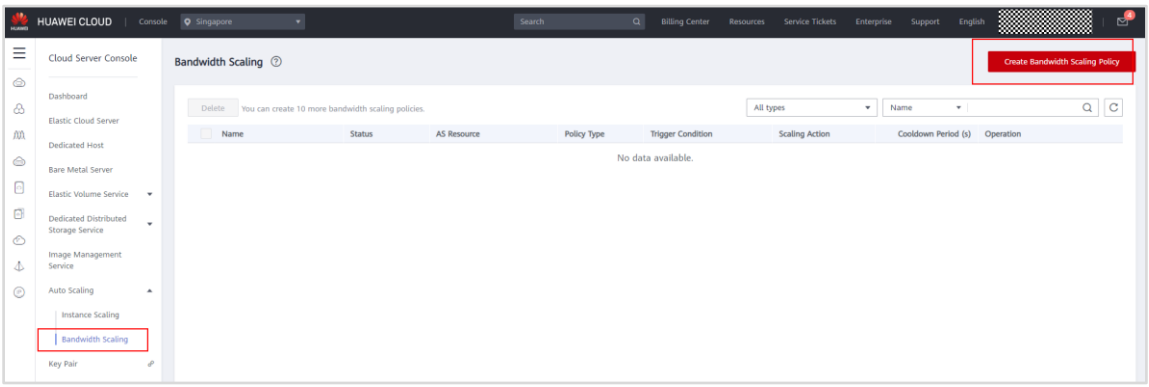


Figure 2-93 Creating a bandwidth scaling policy

Step 2 Set the following parameters:

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

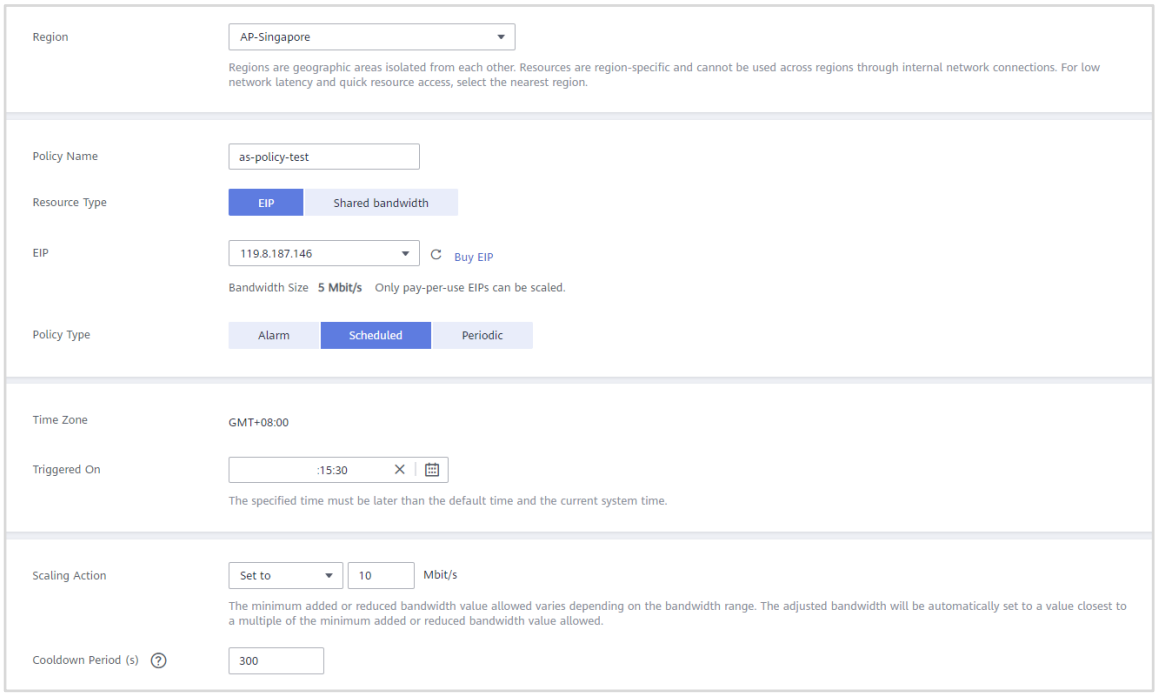


Figure 2-94 Configuring a bandwidth scaling policy

Step 3 Click **Create Now**.

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

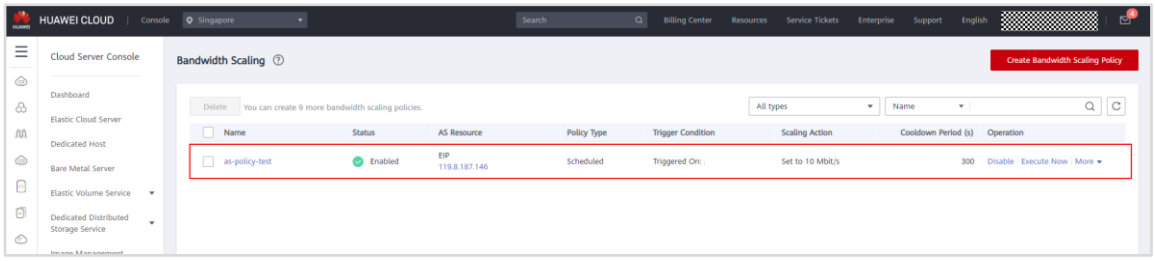


Figure 2-95 Viewing the bandwidth scaling policy

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

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

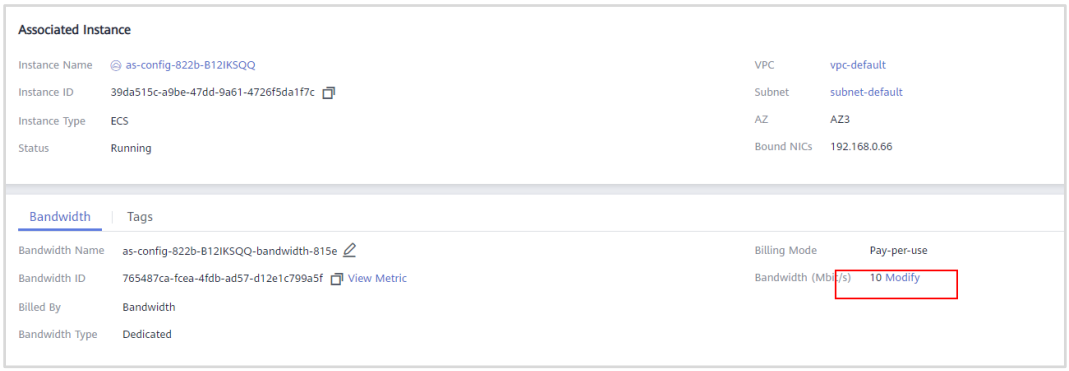


Figure 2-96 Viewing the bandwidth

2.2.6 Deleting Resources

Step 1 Delete the ECSs.

Step 2 Delete the private images.

Step 3 Delete the AS group and configuration.

Step 4 Delete the subnet and then the VPC.

Step 5 Confirm that all the resources created in the experiment have been deleted. If they have not, delete them.

2.3 Exercises

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

3 Networking Services

3.1 Introduction

3.1.1 About This Exercise

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

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

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

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

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

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

In this exercise, we will verify that:

- Two ECSs in a VPC can communicate with each other by default.
- Security groups can be used to control communication between 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.

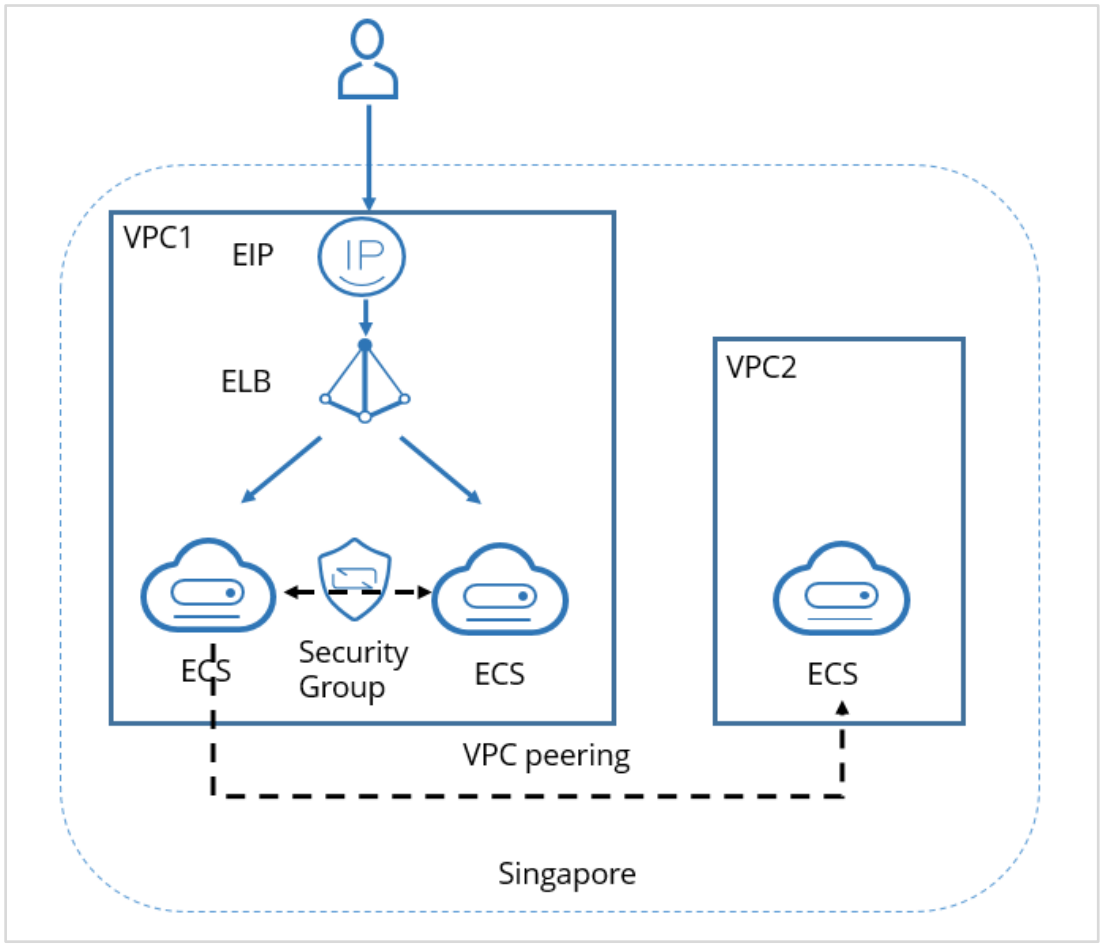
3.1.2 Objectives

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



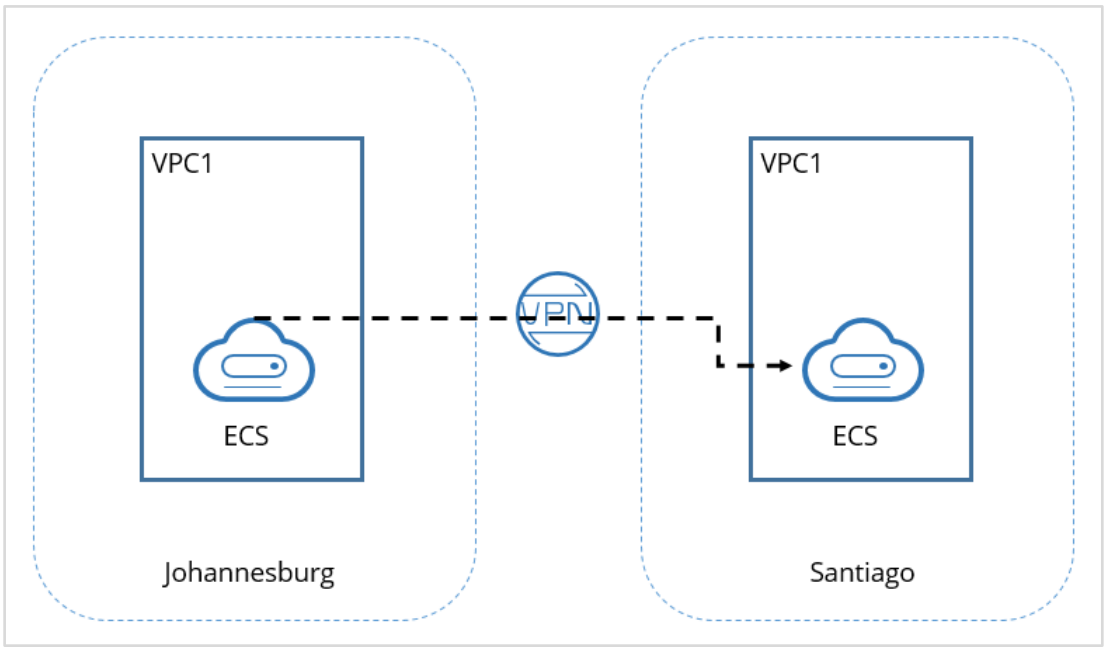


Figure 3-1 Network topology

3.2.2 Creating VPCs

Tasks:

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

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

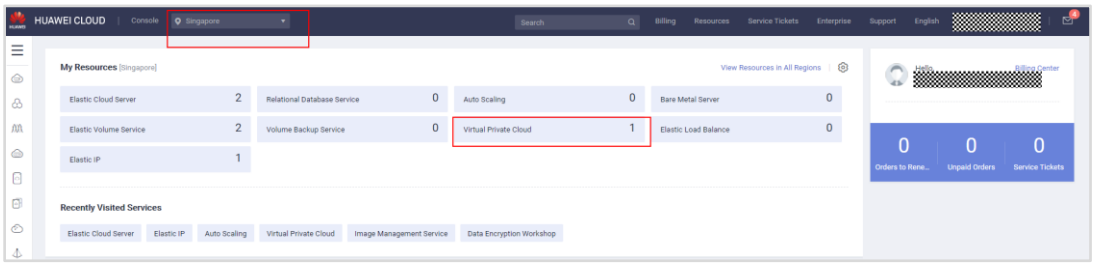


Figure 3-2 Switching to VPC console

Step 2 Click **Create VPC**.

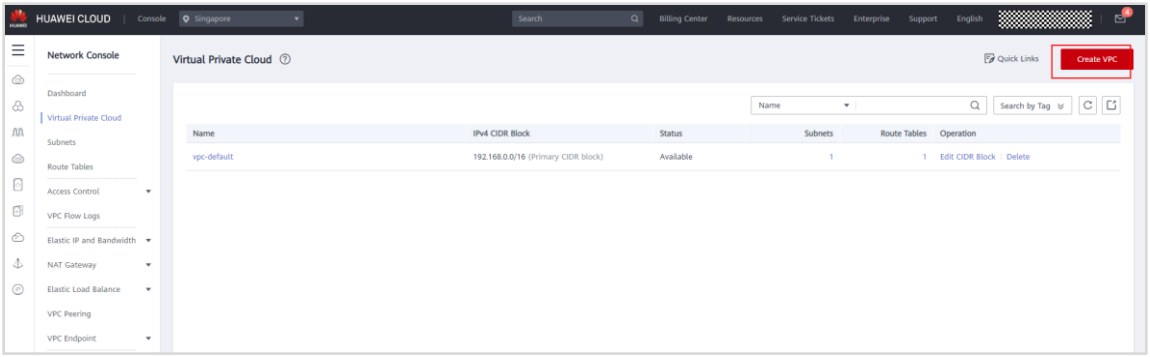


Figure 3-3 Create VPC

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

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

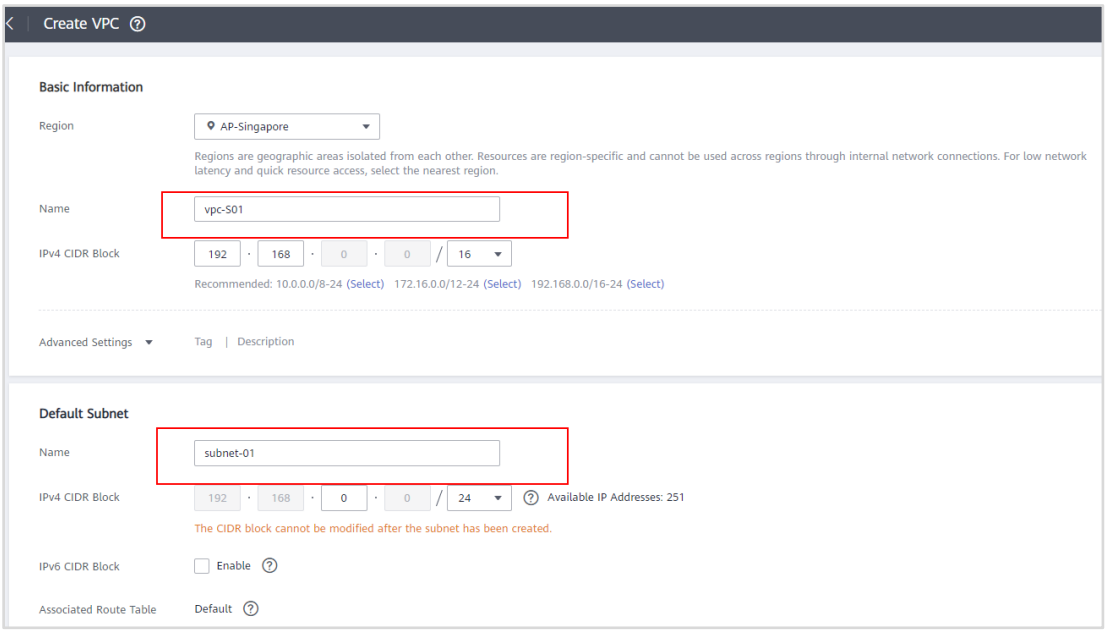


Figure 3-4 Configuring the VPC

Figure 3-5 Configuring the VPC

Step 4 View the created VPC in the VPC list.

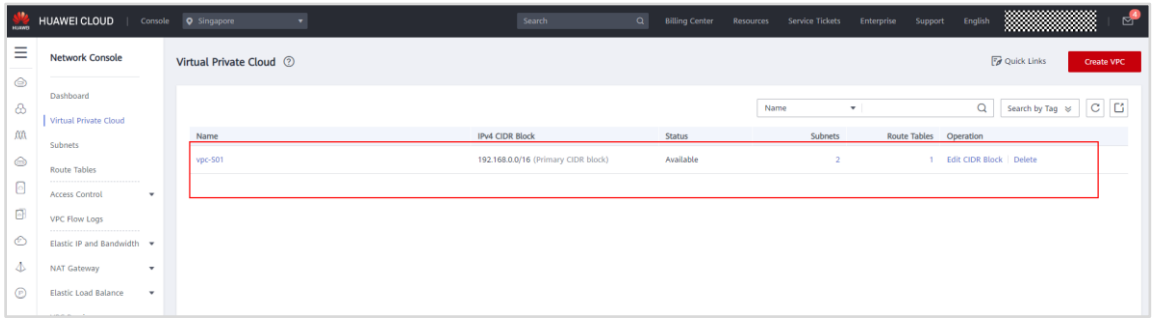


Figure 3-6 Viewing the VPC

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

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

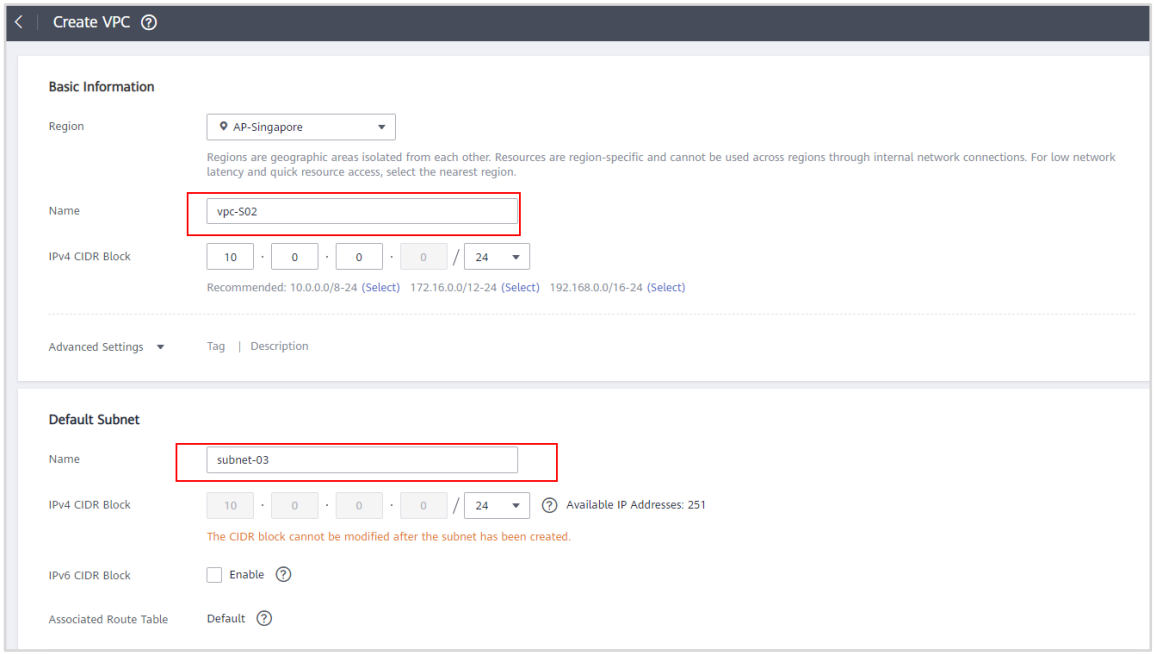


Figure 3-7 Configuring the VPC

Step 6 View the created VPC in the VPC list.

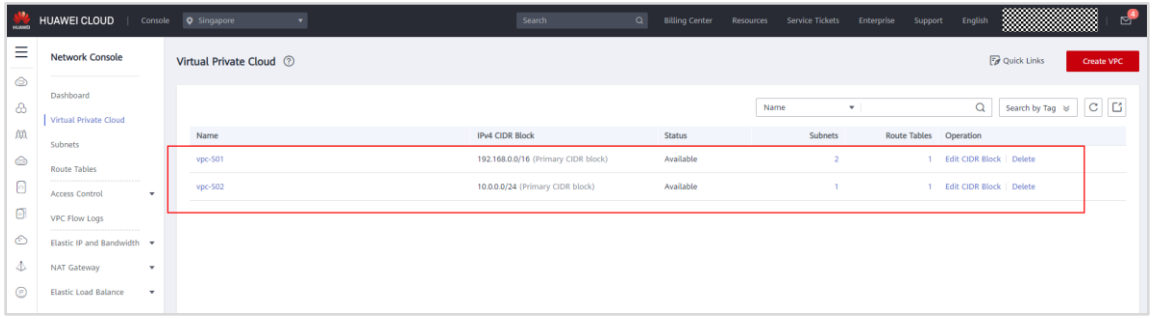


Figure 3-8 Viewing the VPC

Step 7 Create VPC-J01 with subnet-01 in AF-Johannesburg and VPC-Sa01 with subnet-01 in LA-Santiago.

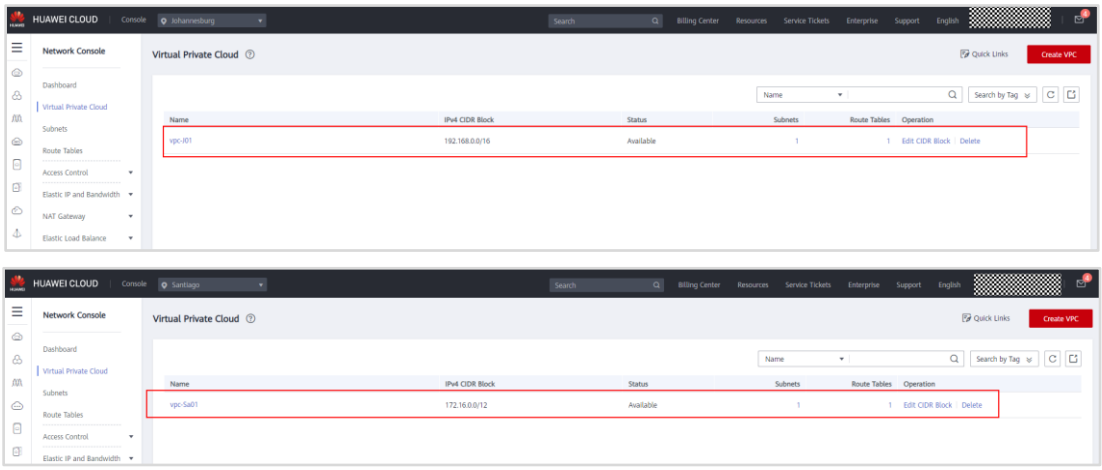


Figure 3-9 Viewing the VPC

3.2.3 Buying ECSs

Tasks:

- In the **AP-Singapore** region, create two ECSs in **VPC-S01**, one in **subnet-01** and one in **subnet-02**, and one ECS in **subnet-03** of **VPC-S02**.
- In the **AF-Johannesburg** region, create an ECS in **subnet-01** of **VPC-J01**.
- In the **LA-Santiago** region, create an ECS in **subnet-01** of **VPC-Sa01**.

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

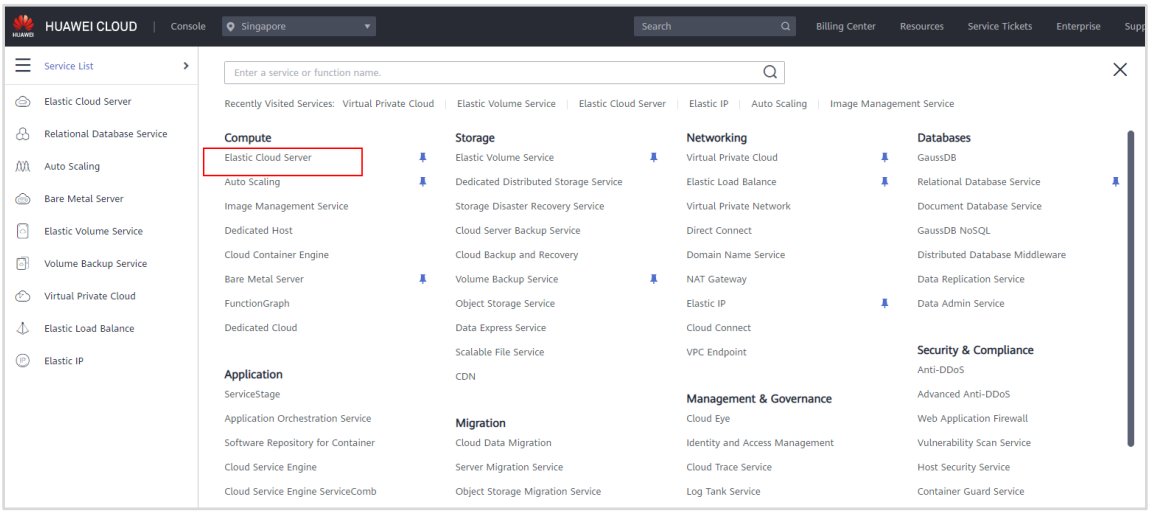


Figure 3-10 Switching to ECS console

Step 2 Click **Buy ECS**.

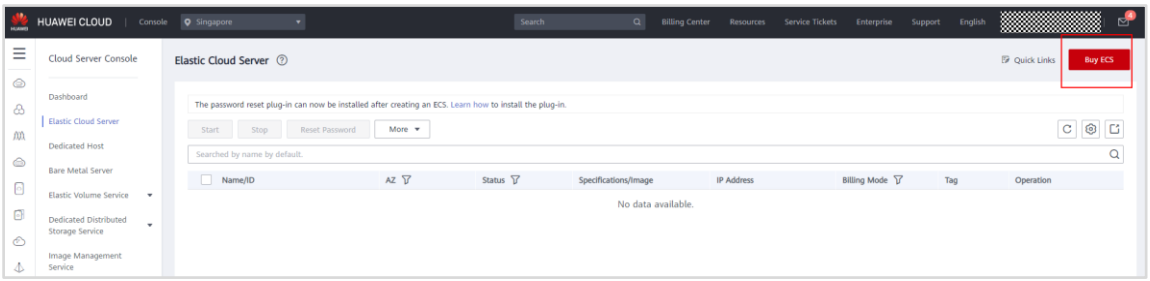


Figure 3-11 Buy ECS

Configure the parameters as follows.

Basic settings:

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

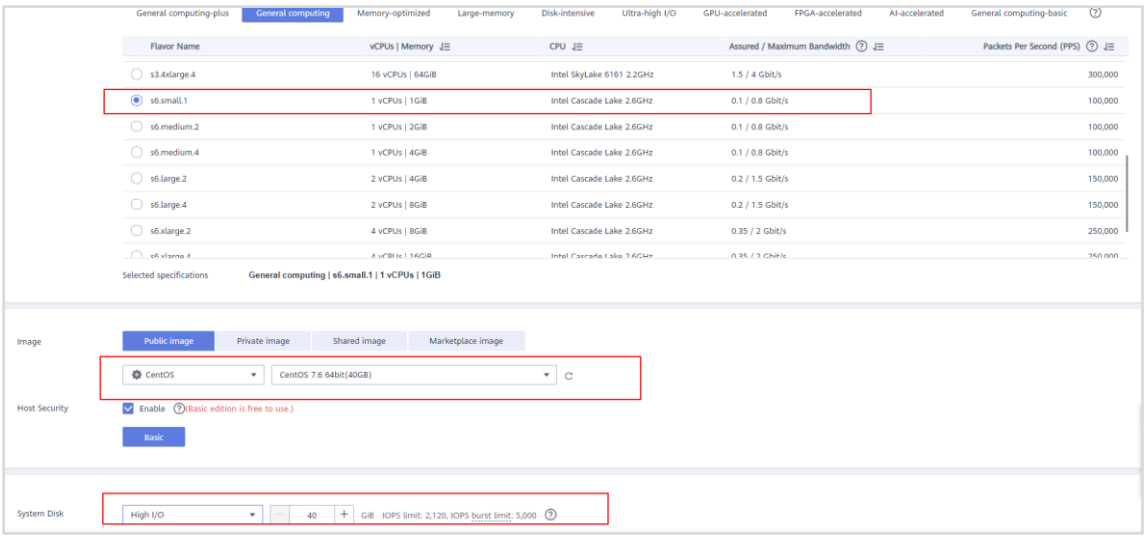


Figure 3-12 Configuring the ECS

Network configuration:

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

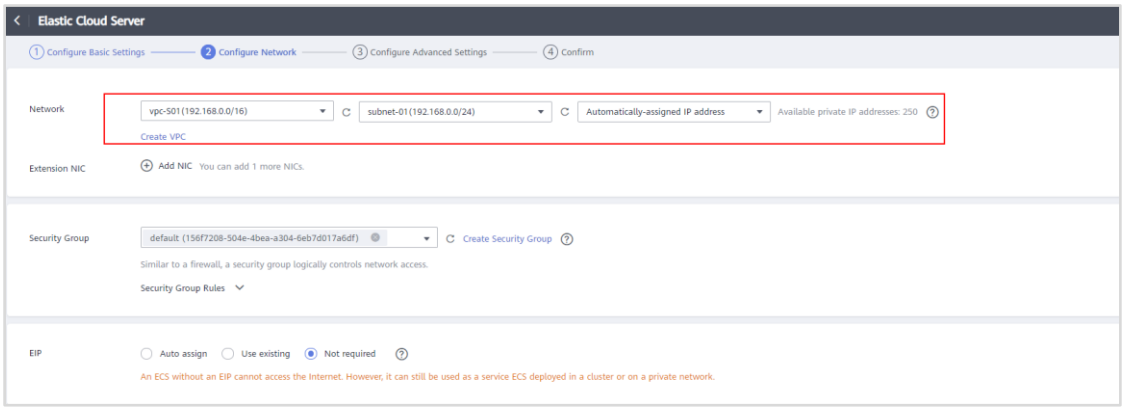


Figure 3-13 Configuring the ECS

Advanced settings:

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

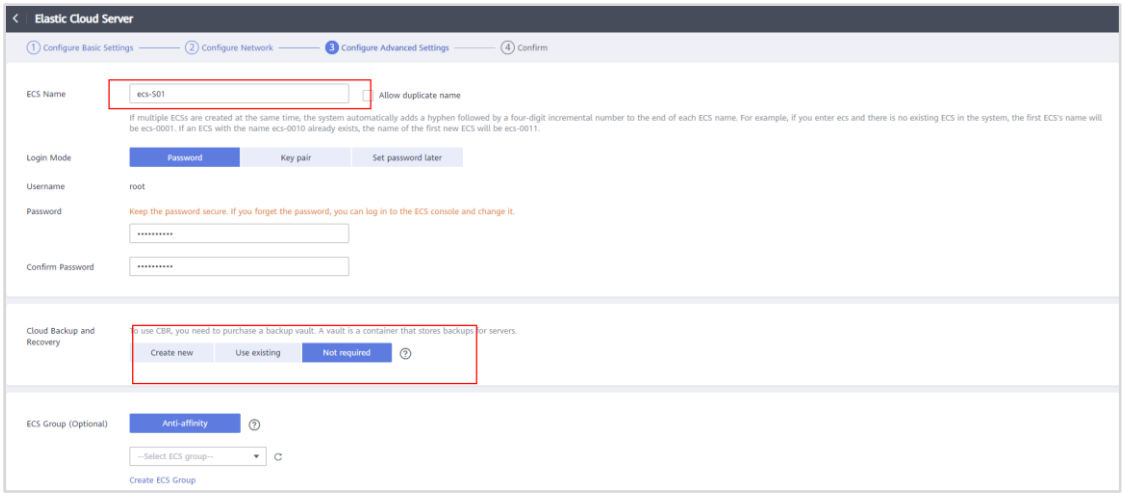


Figure 3-14 Configuring the ECS

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

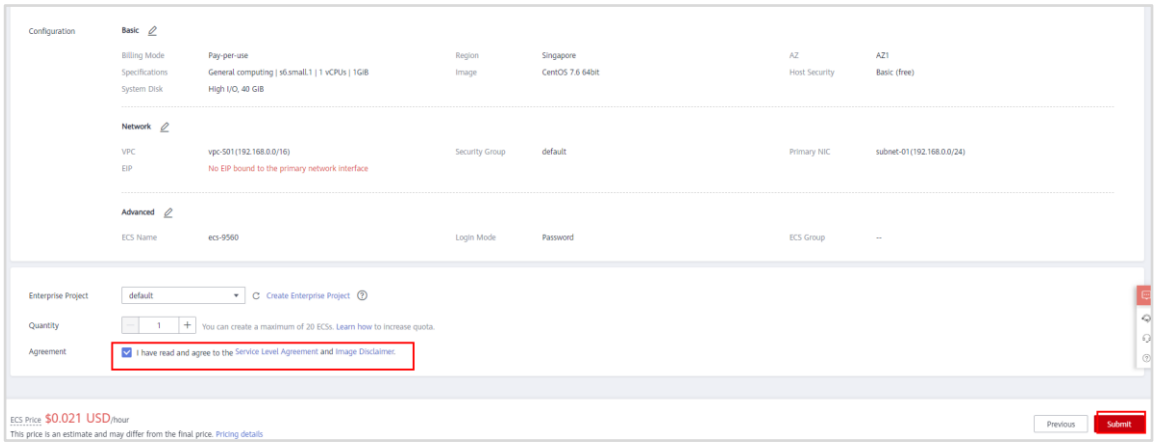


Figure 3-15 Confirming the configuration

Step 4 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 ECS with flavor c3.large.2, 2 vCPUs, and 4 GB of memory in the **LA-Santiago** and **AF-Johannesburg** regions.

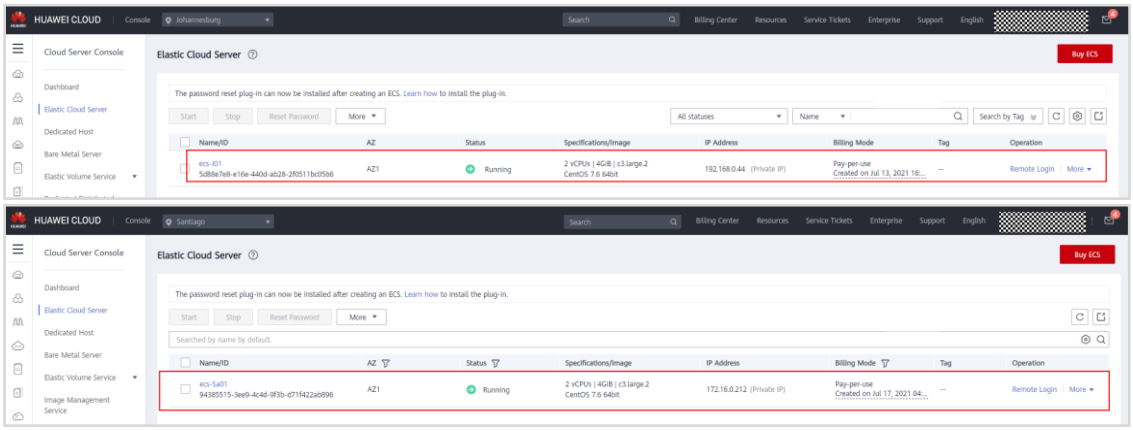


Figure 3-16 Viewing the ECSs

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

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

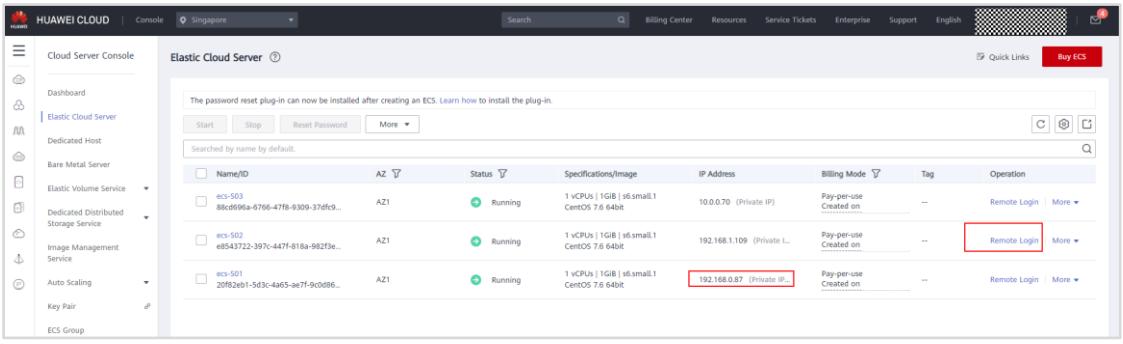


Figure 3-17 Remotely logging in to the ECS

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

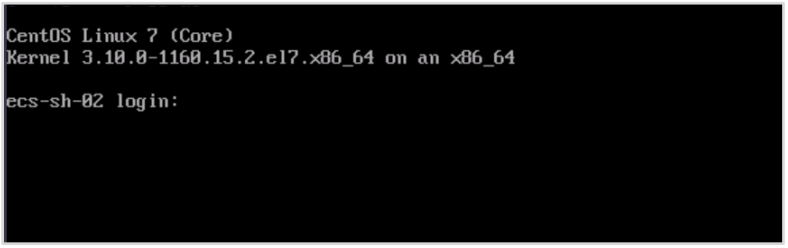


Figure 3-18 Logging in to the Linux ECS

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

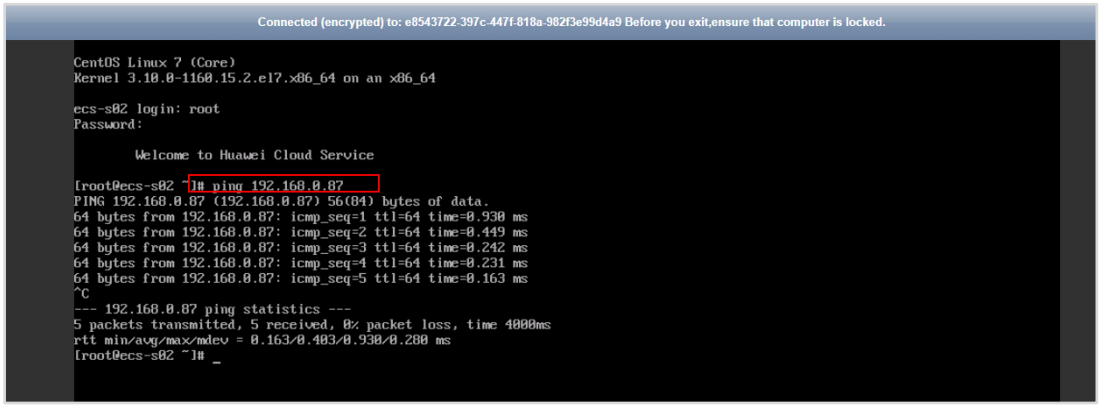


Figure 3-19 Successful ping

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

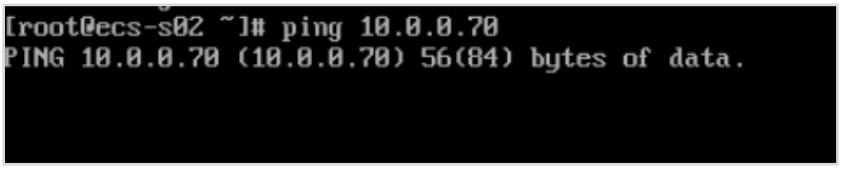


Figure 3-20 Ping failure

3.2.4.2 Traffic Control by Security Groups

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

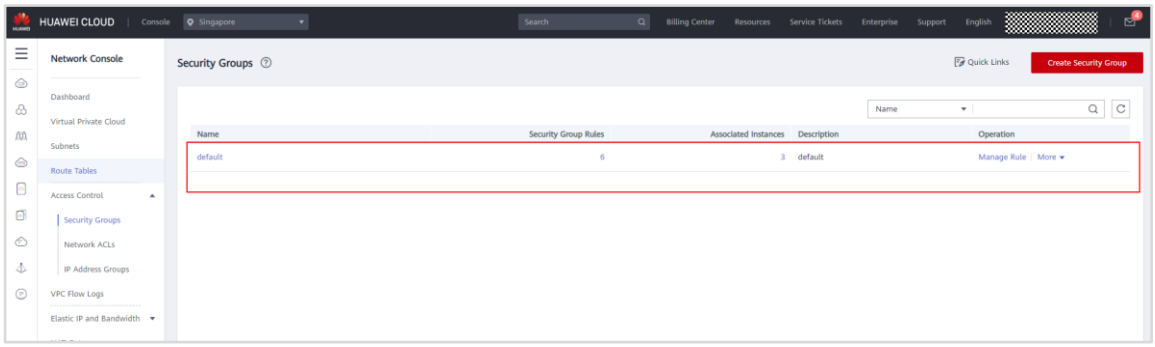


Figure 3-21 Viewing the security group

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

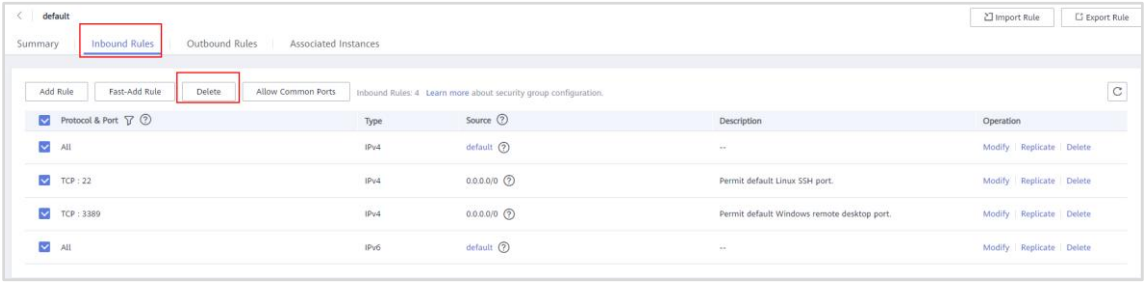


Figure 3-22 Deleting inbound rules

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

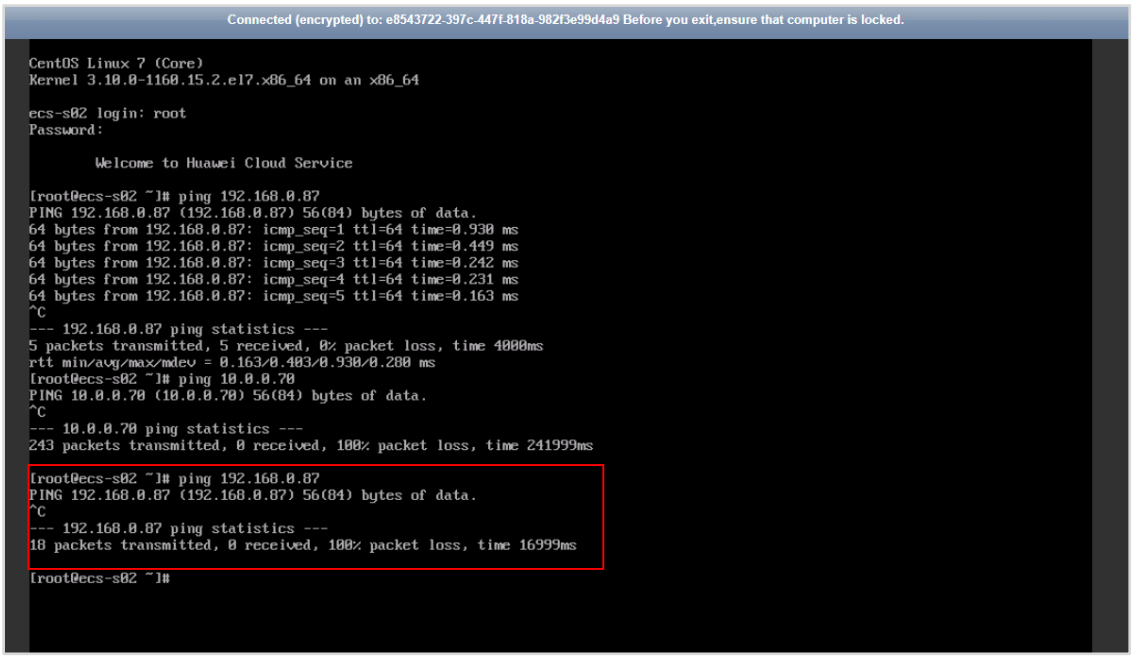


Figure 3-23 Ping failure

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

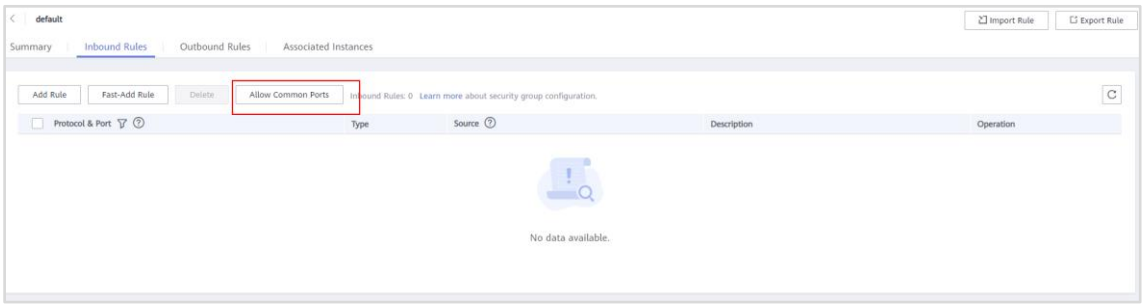


Figure 3-24 Allow Common Ports

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

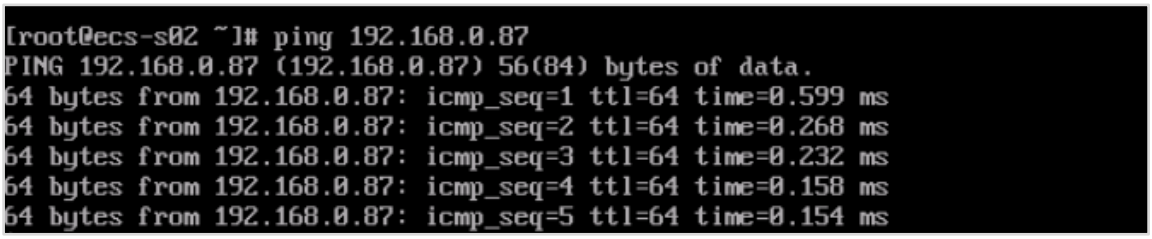


Figure 3-25 Successful ping

3.2.4.3 Access to the Internet with an EIP

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

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.

Step 2 Click **Service List**, search for Data Encryption Workshop, and click **Data Encryption Workshop** to go to the DEW console.

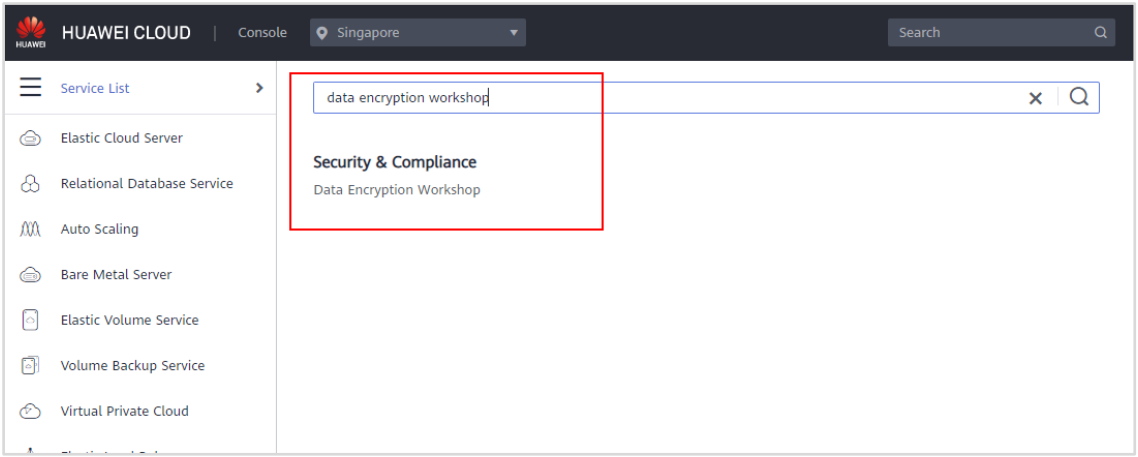


Figure 3-27 Switching to DEW console

Step 3 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.

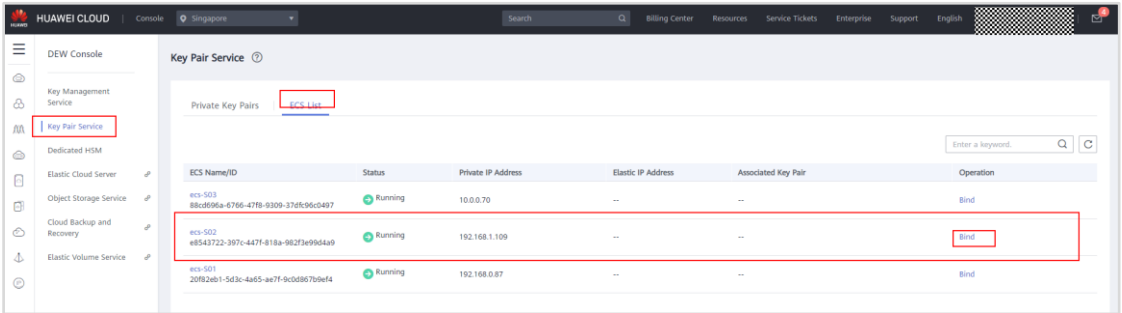


Figure 3-28 Viewing the ECS list

Step 4 Select the target key pair, enter the password of user **root** for logging in to the **ecs-S02**, and click **OK**.

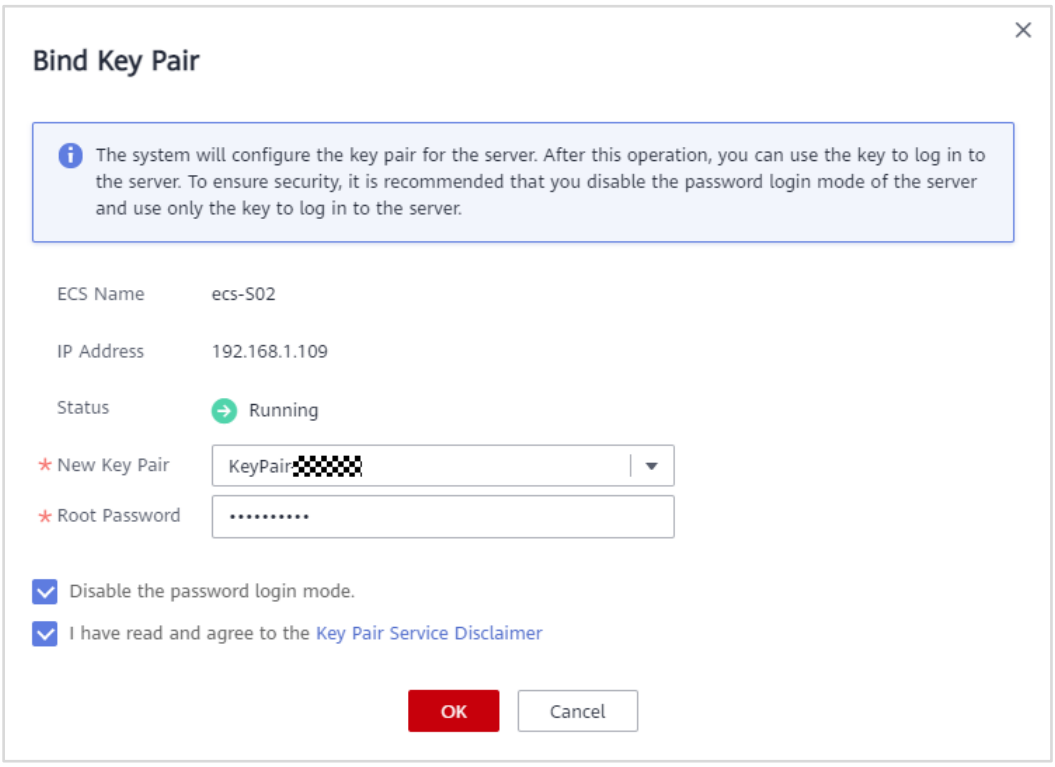


Figure 3-29 Binding a key pair

Step 5 View the binding result on the **ECS List** tab page.

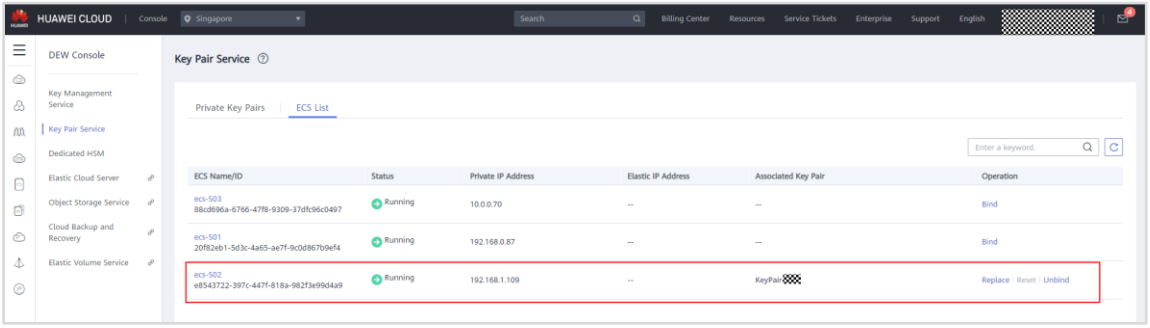


Figure 3-30 Successful binding

Step 6 Switch to the network console, choose **EIPs**, and click **Buy EIP**.

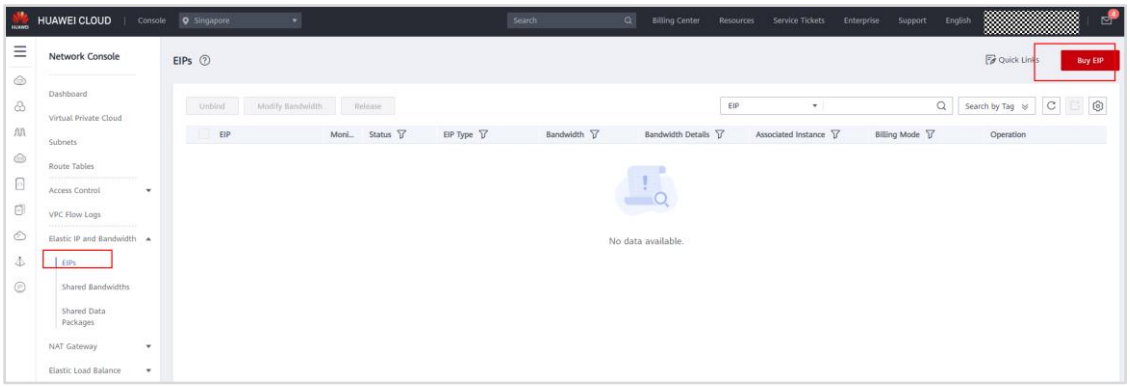


Figure 3-31 Buy EIP

Step 7 Configure the parameters as follows, click **Next**, confirm the parameters, and click **Submit**.

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

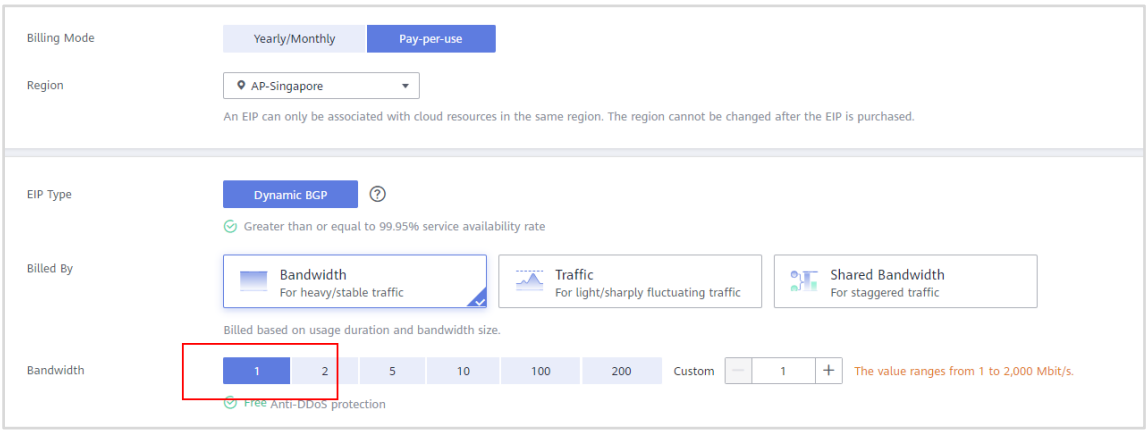


Figure 3-32 Configuring EIP

Step 8 On the **EIPs** page, locate the newly purchased EIP, click **Bind** in the **Operation** column, select **ecs-S02**, and click **OK**.

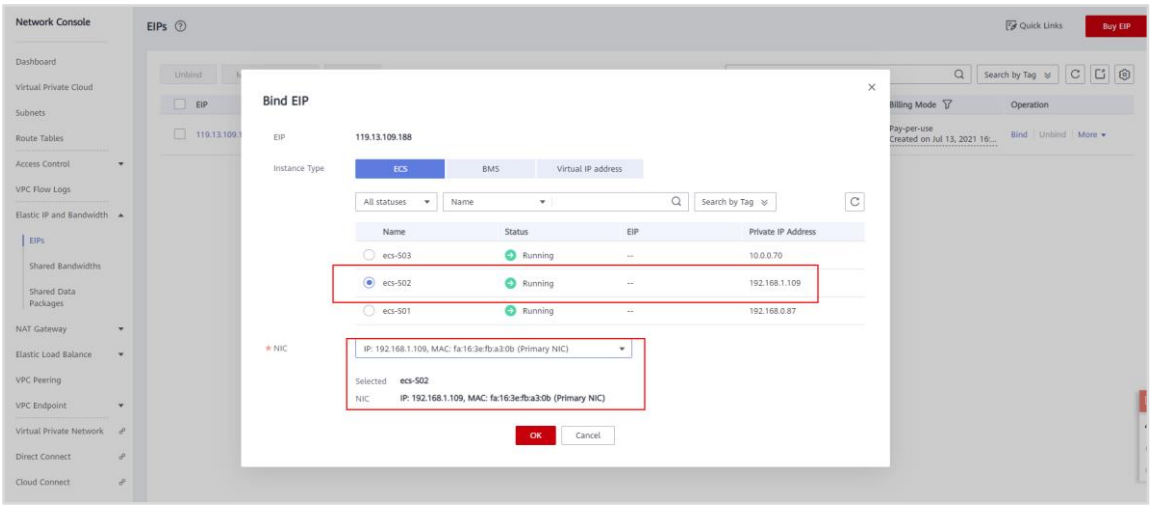


Figure 3-33 Binding an EIP

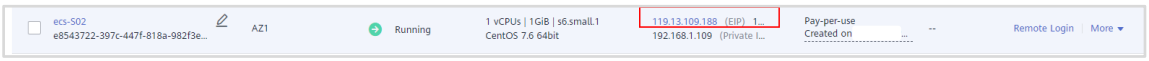


Figure 3-34 Viewing the EIP

Step 9 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.

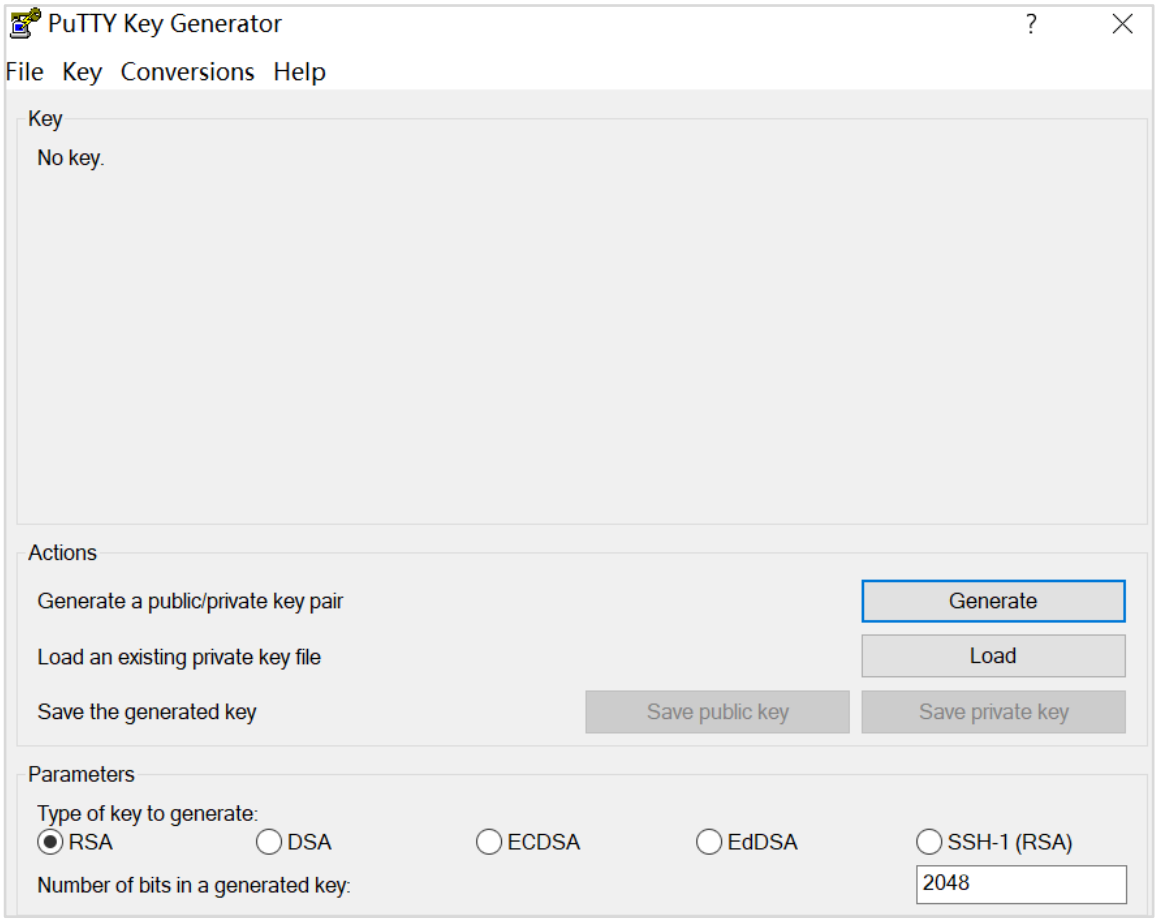


Figure 3-35 Opening the PuTTYgen program

Step 10 Go to **Conversions**, and then click **Import key** to load the key pair file.

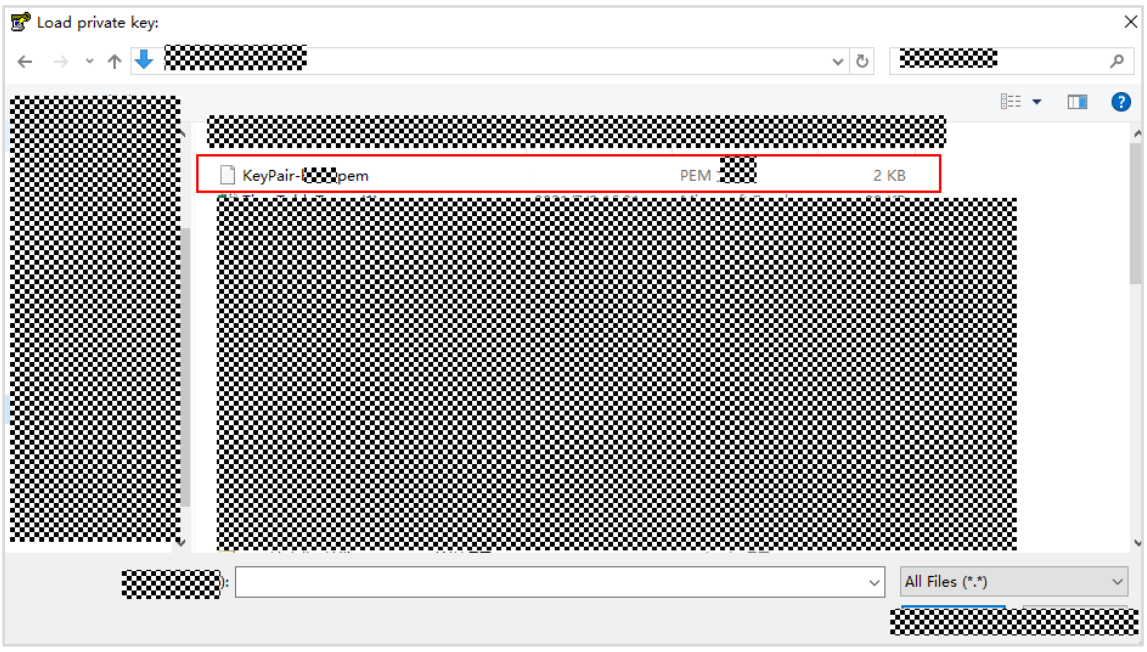


Figure 3-36 Importing the key pair file

Step 11 Click **Save private key** to save the key pair file in .ppk format to your local computer.

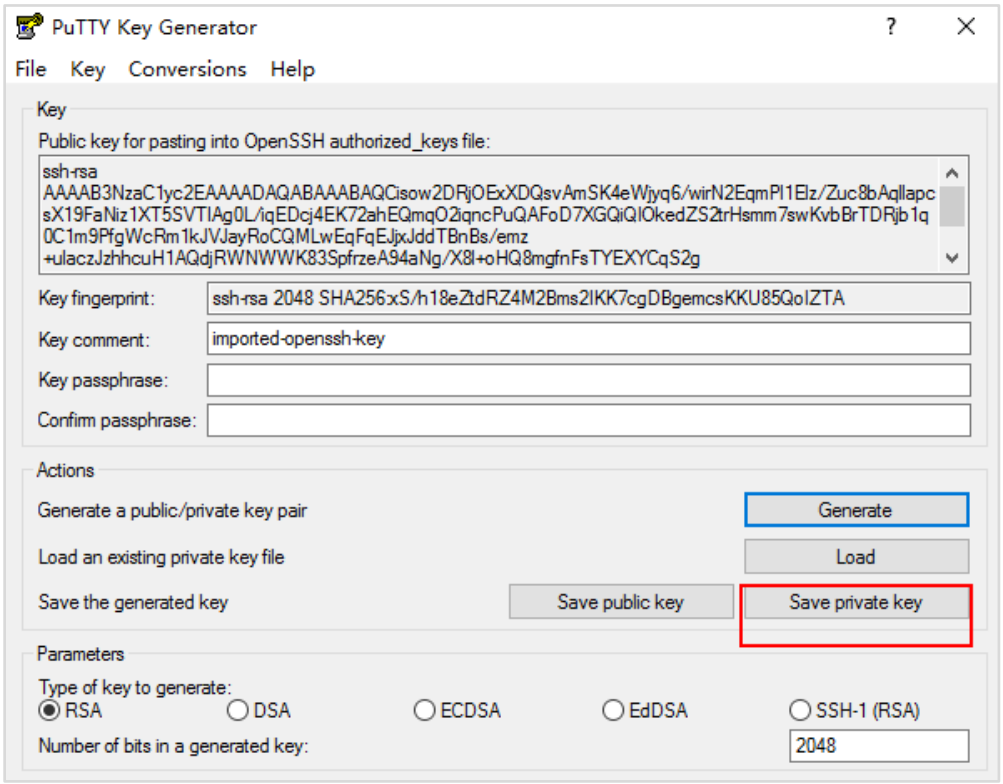


Figure 3-37 Saving the private key file

Step 12 Open PuTTY, click **Connection** > **Data** in the left navigation pane, and set the **Auto-login username** to **root**.

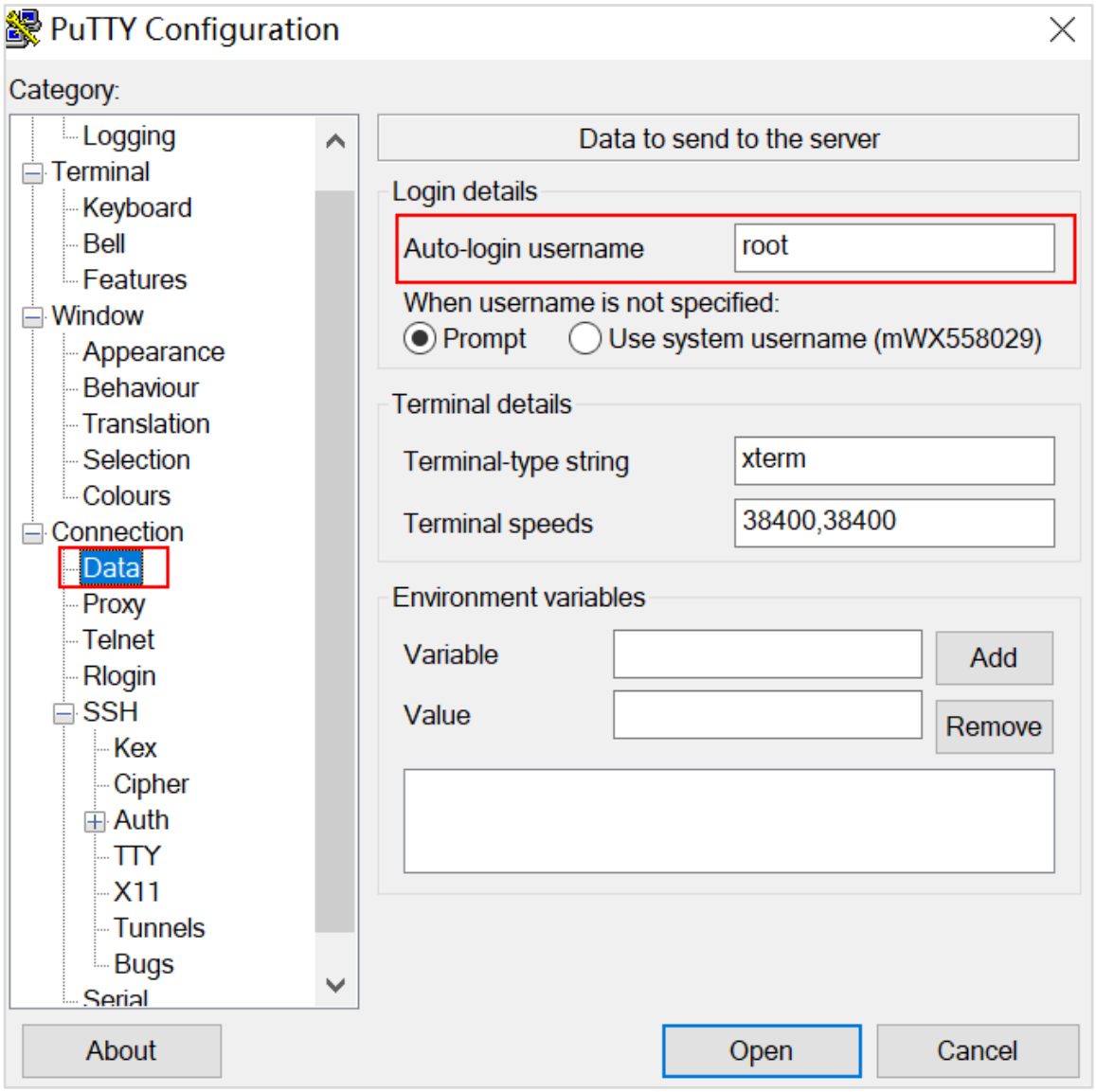


Figure 3-38 Setting the Auto-login username

Step 13 Click **Connection** > **SSH** > **Auth** in the left navigation pane, click the **Browse...** button and select your private key file (.ppk file).

Step 14 Click **Session** in the left navigation pane, enter the EIP of **ecs-S02** in **Host Name (or IP address)**, and click **Open**.

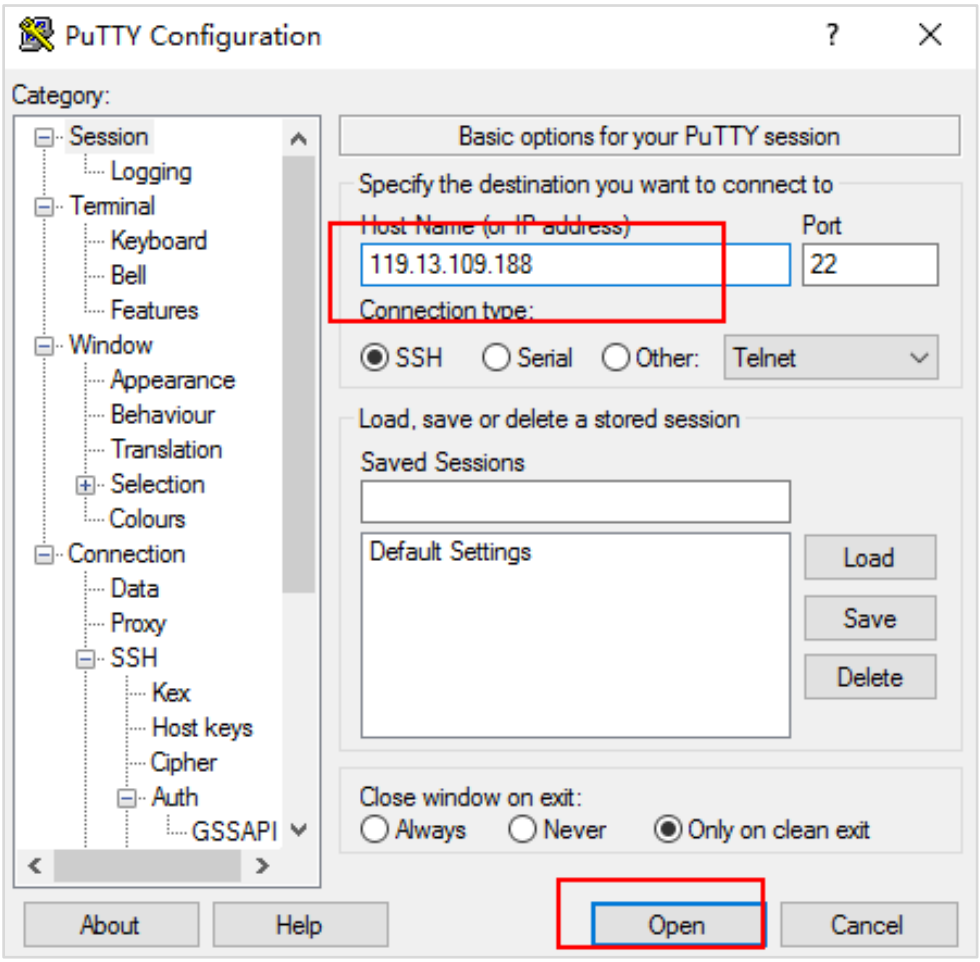


Figure 3-39 Configuring Host Name (or IP address)

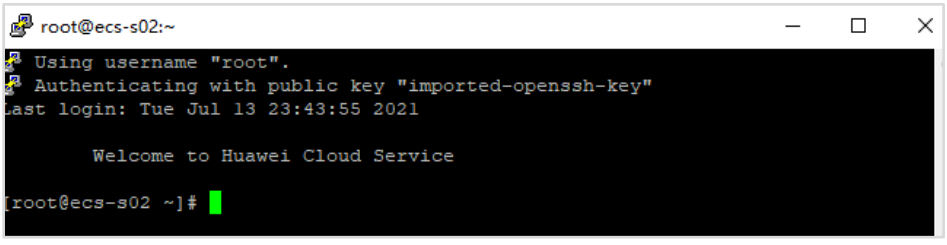


Figure 3-40 Logging in to ecs-S02 using a key pair

Step 15 Run the **ping baidu.com** command to check whether **ecs-S02** can access the Internet. The ping is successful, indicating that **ecs-S02** can access the Internet through an EIP.

```
[root@ecs-s02 ~]# ping baidu.com
PING baidu.com (39.156.69.79) 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-S01** and **ecs-S02**.
- Create a load balancer.
- Use the load balancer to route HTTP requests for the web page across two ECSs.

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

1. Start the HTTP service on each ECS.

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

2. 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-S01

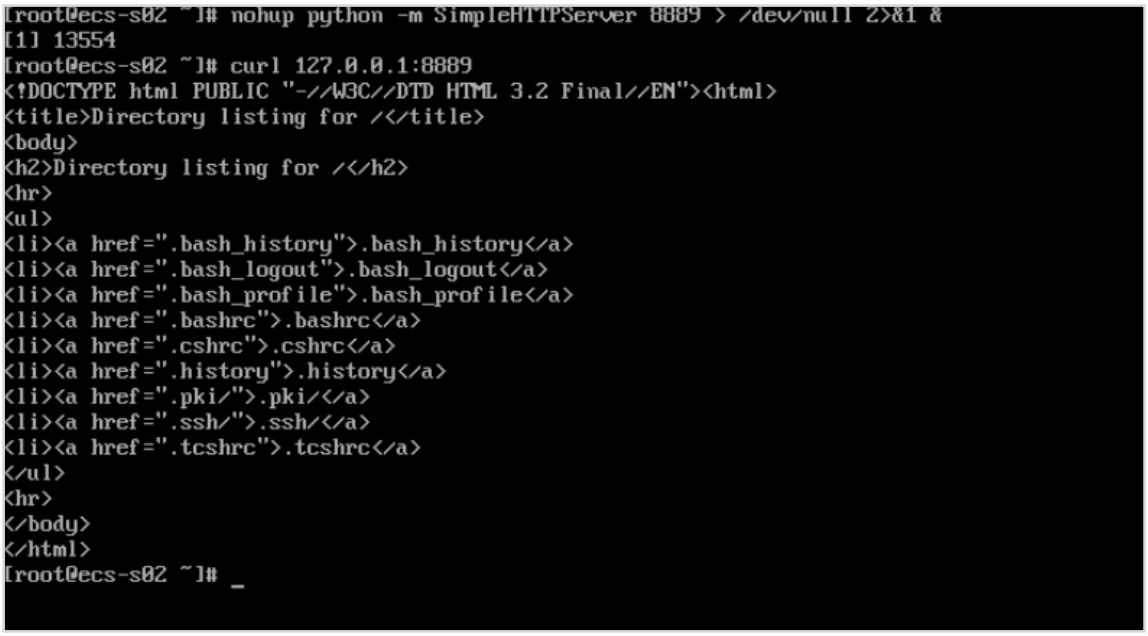


Figure 3-43 Port 8899 enabled on ecs-S02

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

```
touch SERVER1
touch SERVER2
```

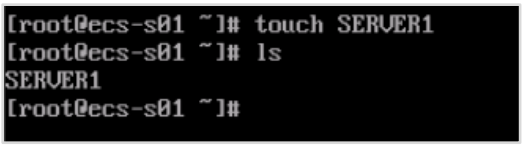


Figure 3-44 Creating file SERVER1

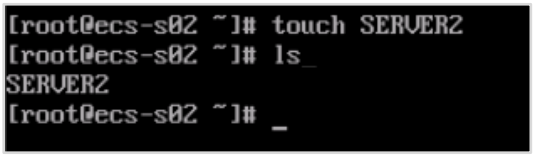


Figure 3-45 Creating file SERVER2

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

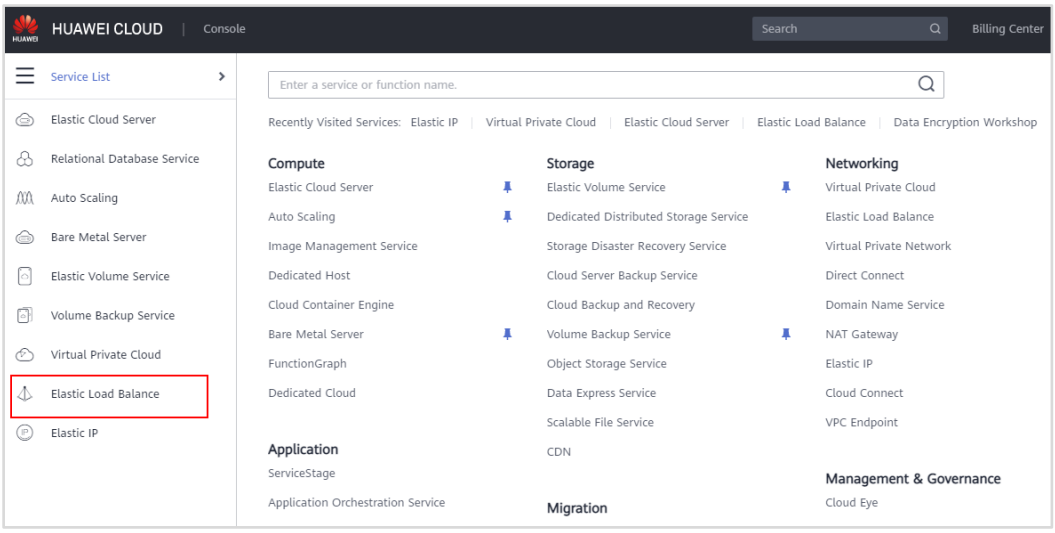


Figure 3-46 Accessing Elastic Load Balance

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

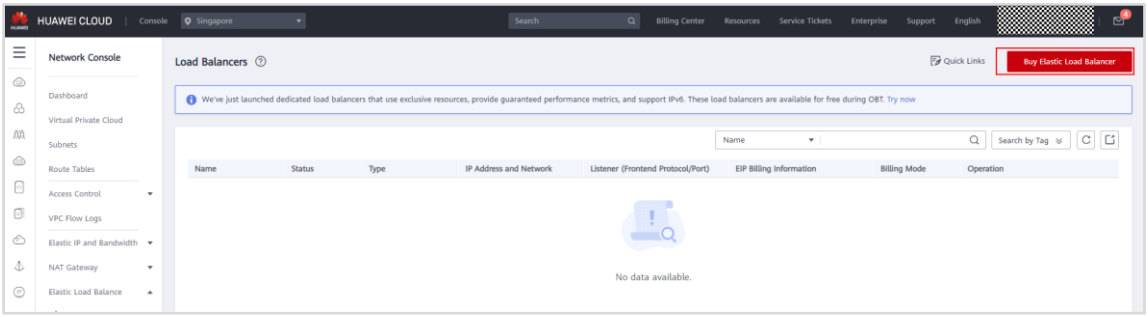


Figure 3-47 Buy Elastic Load Balancer

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

- **Type**: **Shared**
- **Region**: **AP-Singapore**
- **Network Type**: **Public 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.)

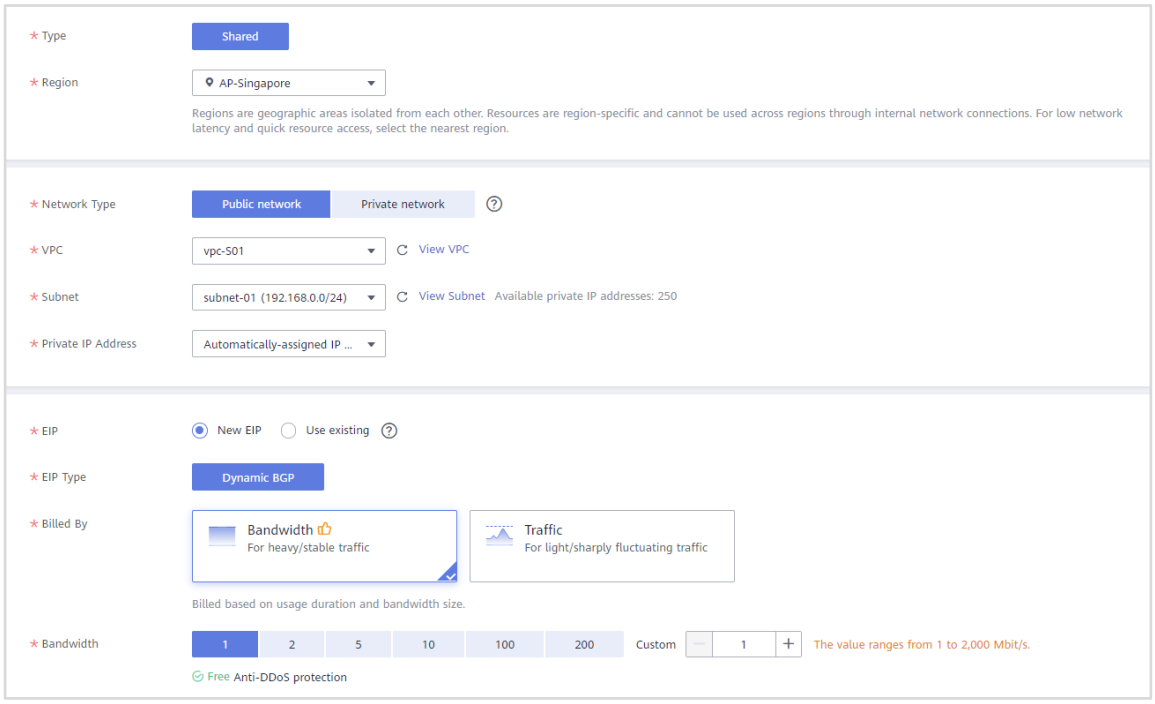


Figure 3-48 Configuring parameters

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

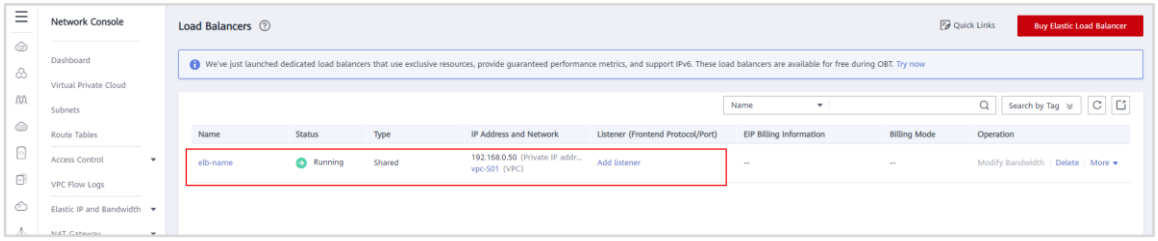


Figure 3-49 Viewing the load balancer

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

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

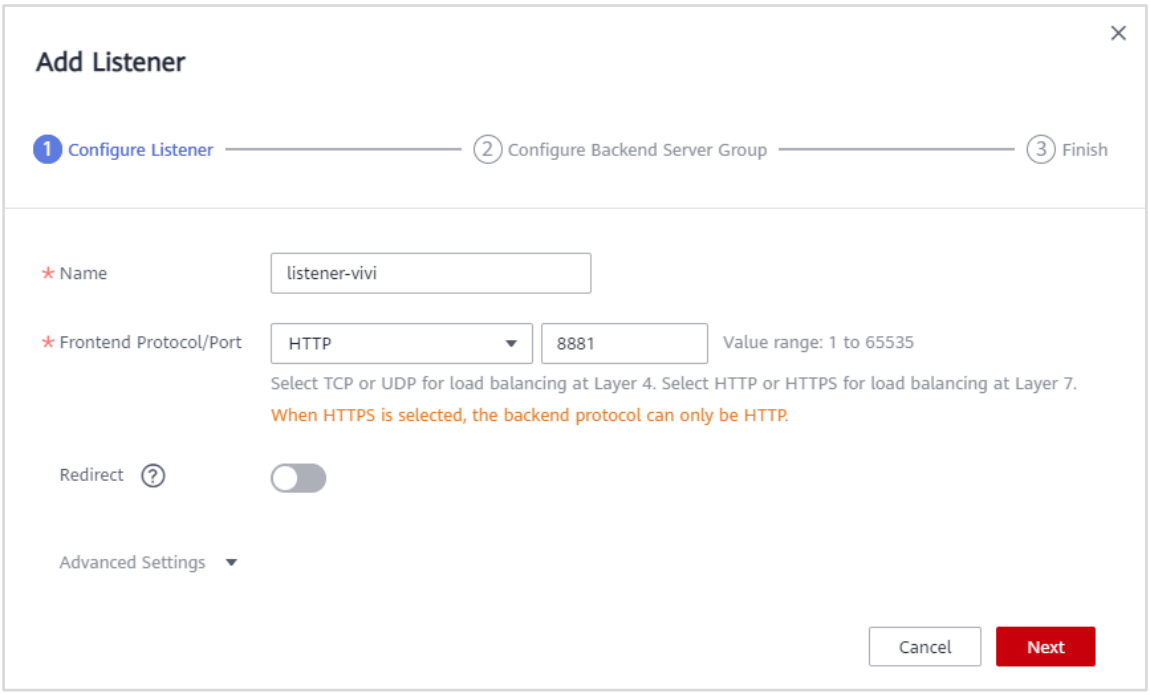


Figure 3-50 Configuring a listener

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

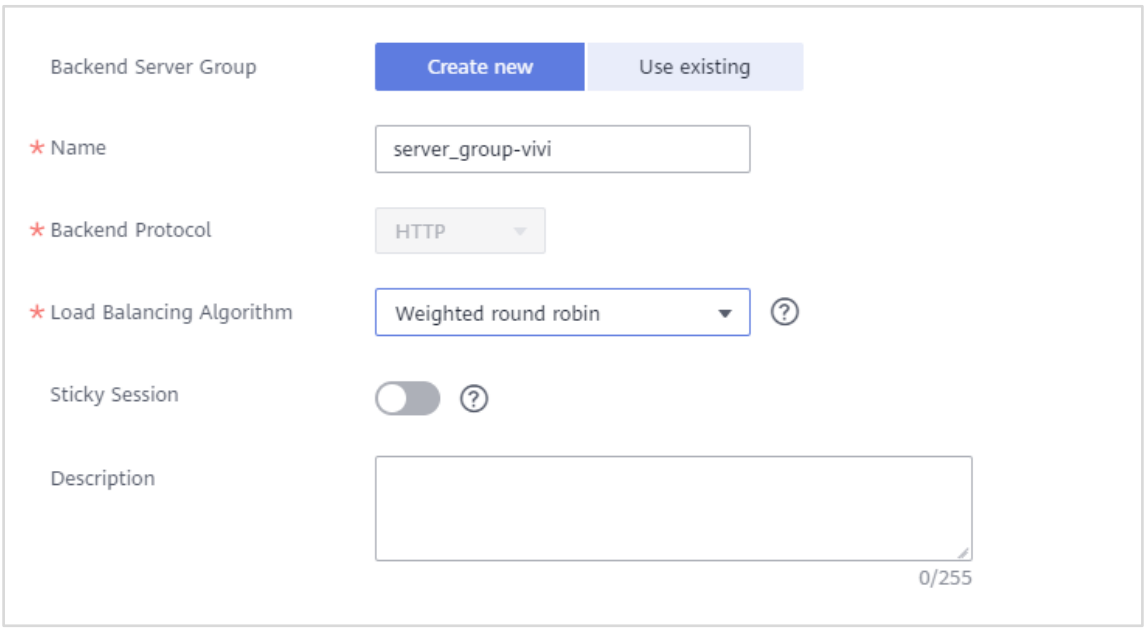


Figure 3-51 Configuring a backend server group

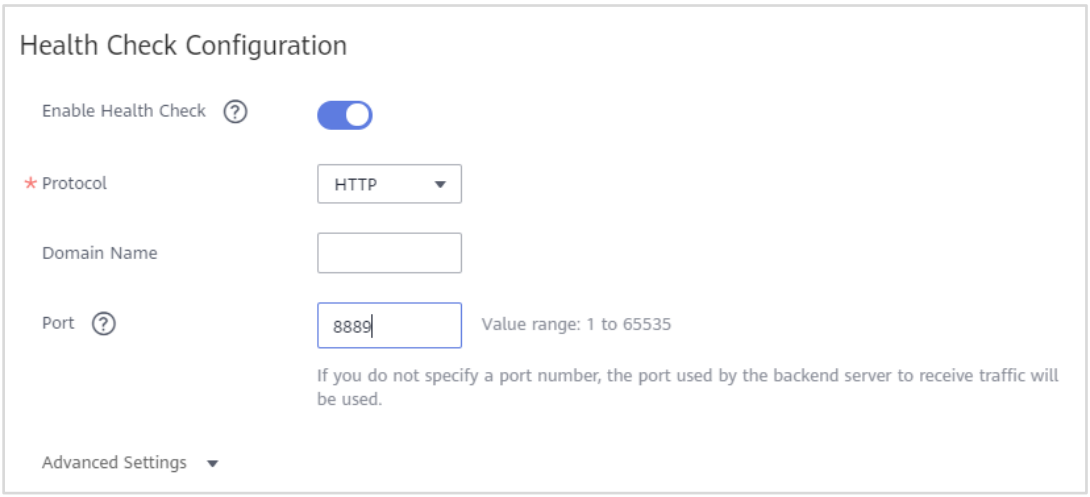


Figure 3-52 Configuring a health check

3. Click **Finish** and then click **OK**.

Step 7 Add **ecs-S01** and **ecs-S02** to the backend server group and set the backend port to 8889.

The two ECSs, **ecs-S01** and **ecs-S02,** are in different subnets (**subnet-01** and **subnet-02**). When you add them, each needs to be added separately. When you add **ecs-S01**, select **subnet-01**. When you add **ecs-S02**, select **subnet-02.**

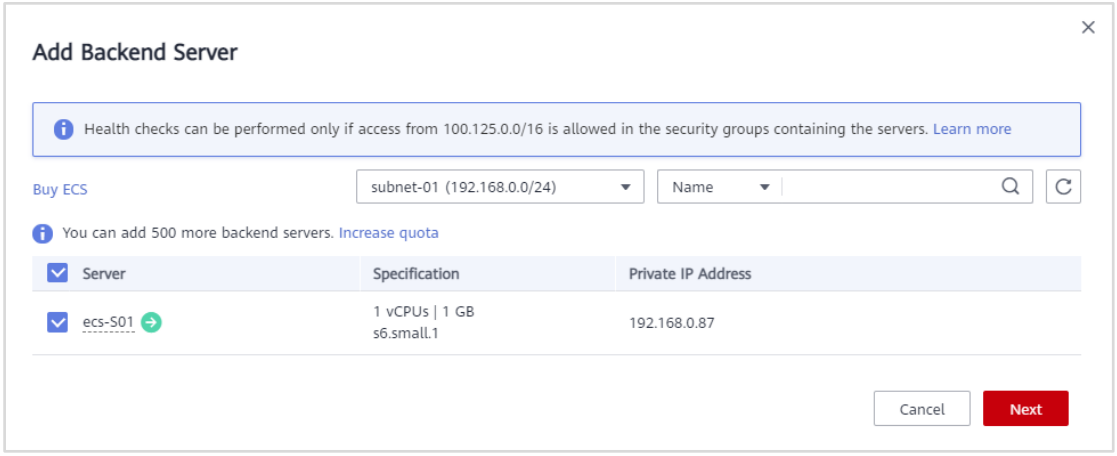


Figure 3-53 Adding ecs-S01 to the backend server group

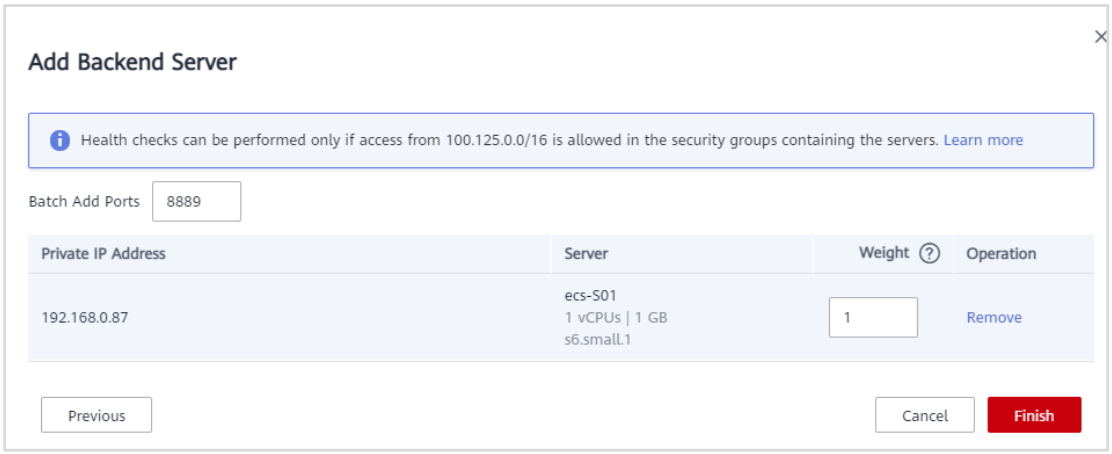


Figure 3-54 Adding ecs-S02 to the backend server group

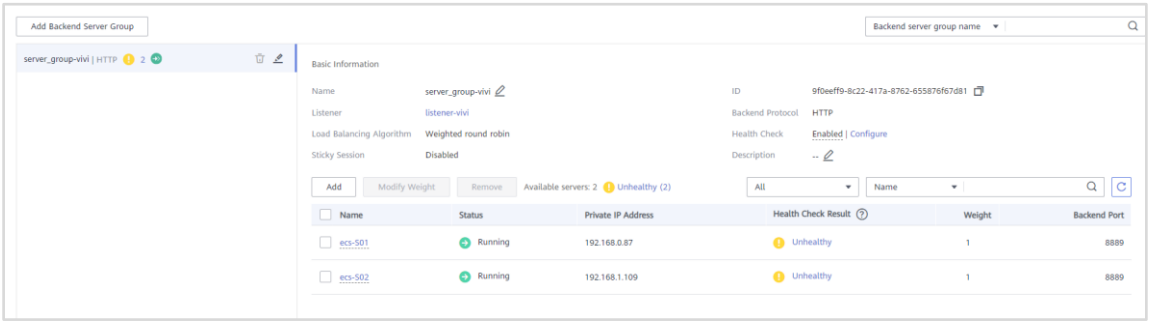


Figure 3-55 Viewing the backend servers

Step 8 Check the health check results for the two ECSs.

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 ECSs, and add security group rules.

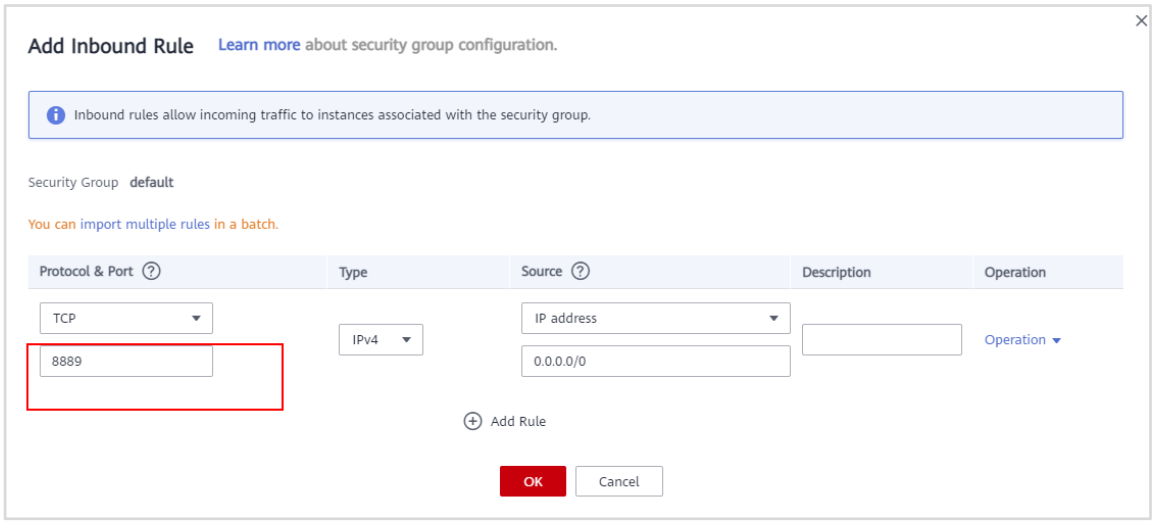


Figure 3-56 Configuring security group rules

Step 9 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**.

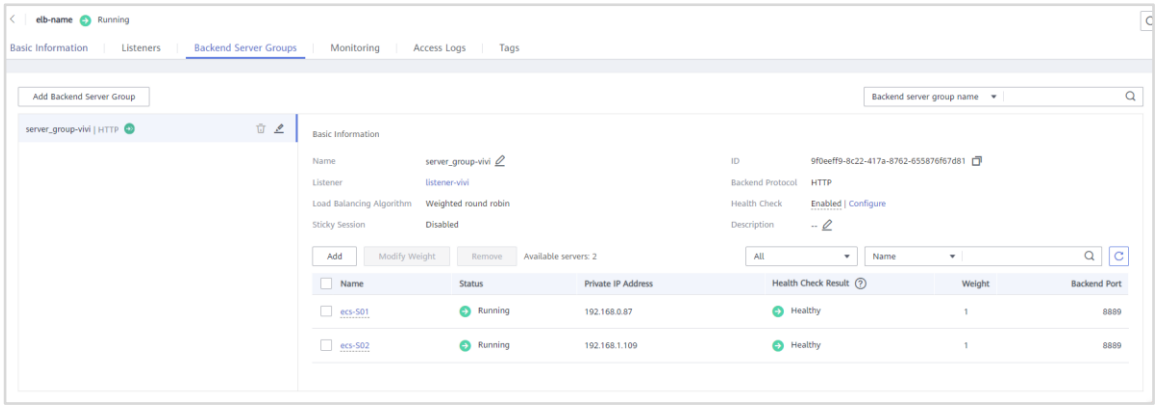


Figure 3-57 Viewing the backend server group

Step 10 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.

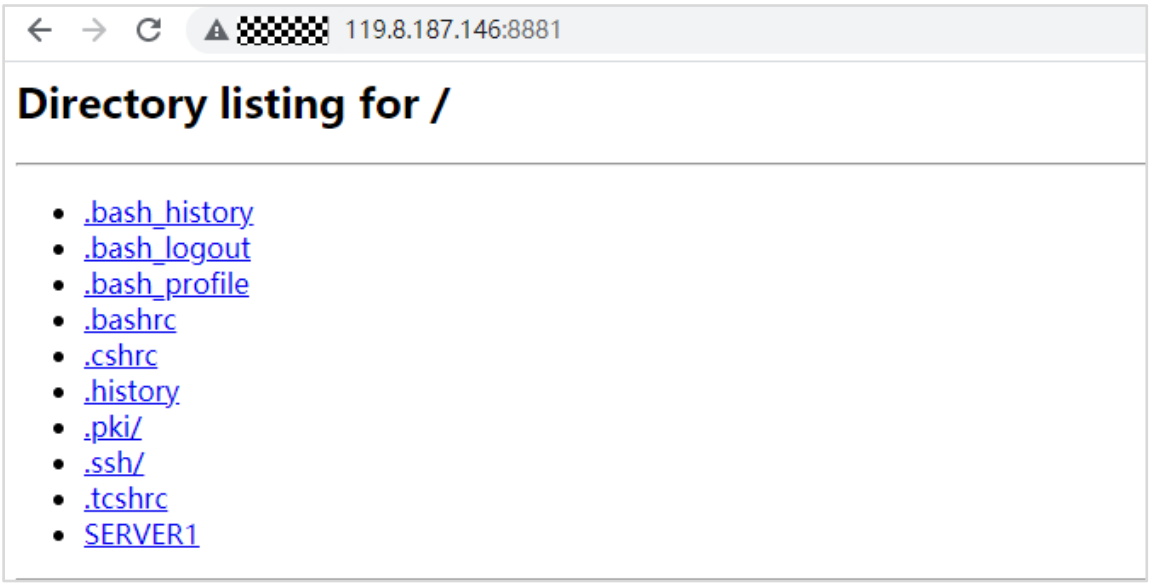


Figure 3-58 Accessing the web page

Step 11 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.

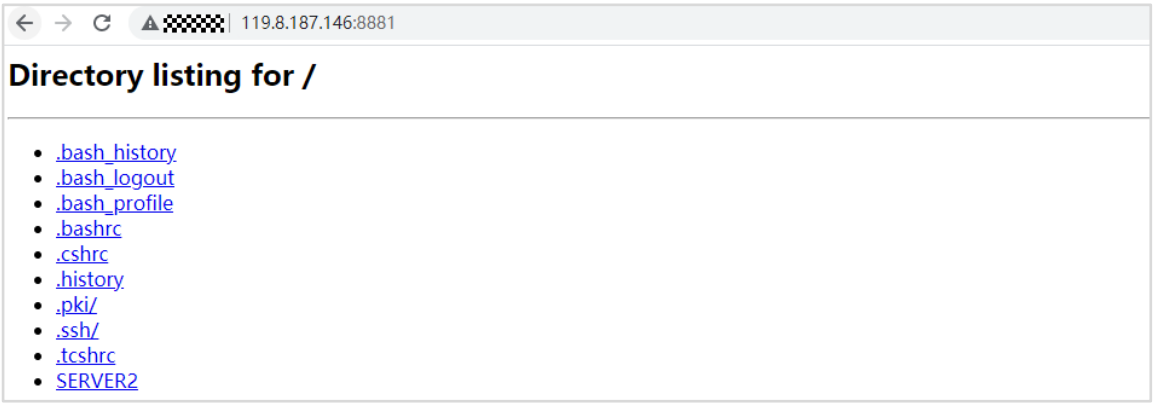


Figure 3-59 Verifying load balancing

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

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

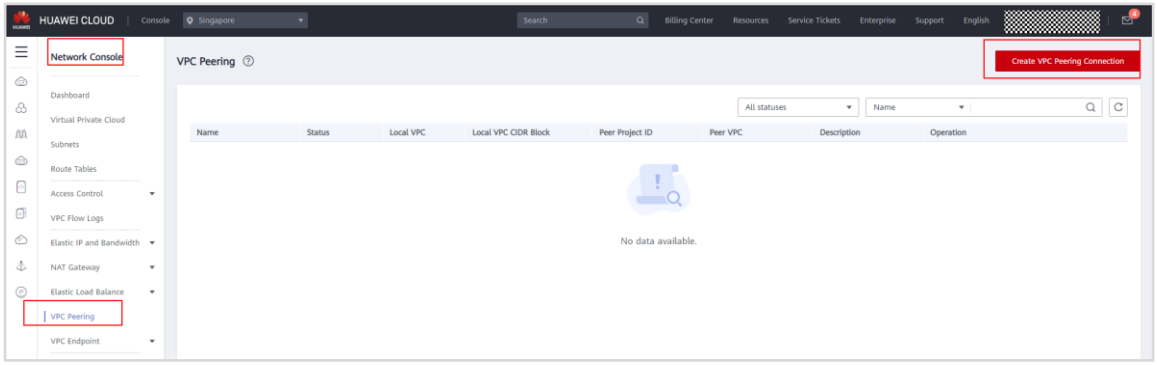


Figure 3-60 Create VPC Peering Connection

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

- **Name**: **peering-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.

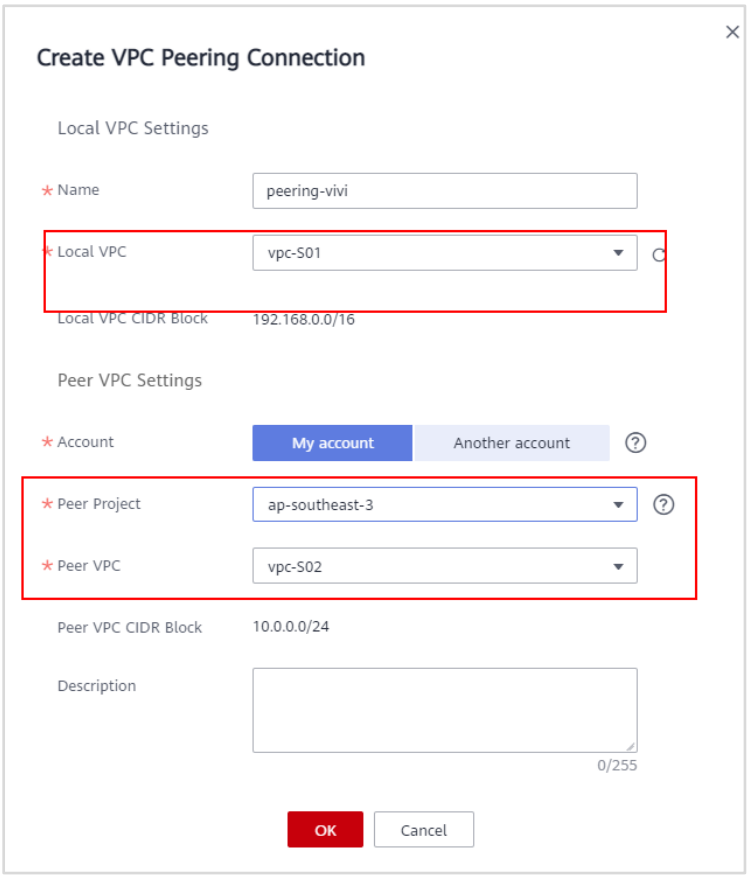


Figure 3-61 Configuring the VPC peering connection

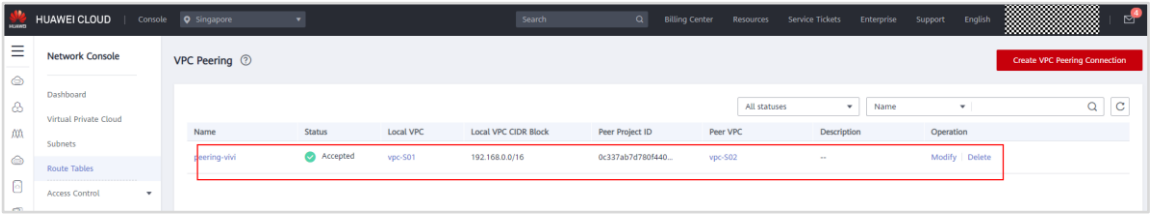


Figure 3-62 Viewing the VPC peering connection

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

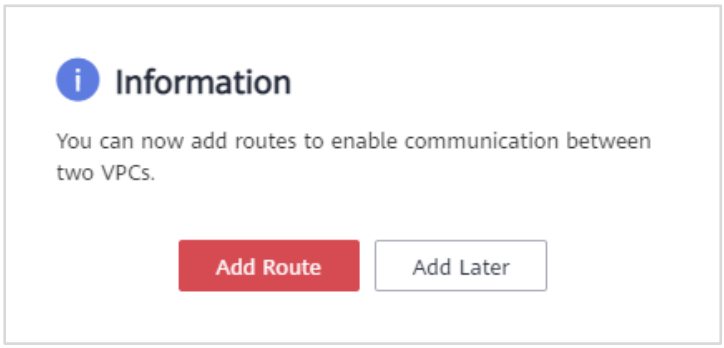


Figure 3-63 Add Route

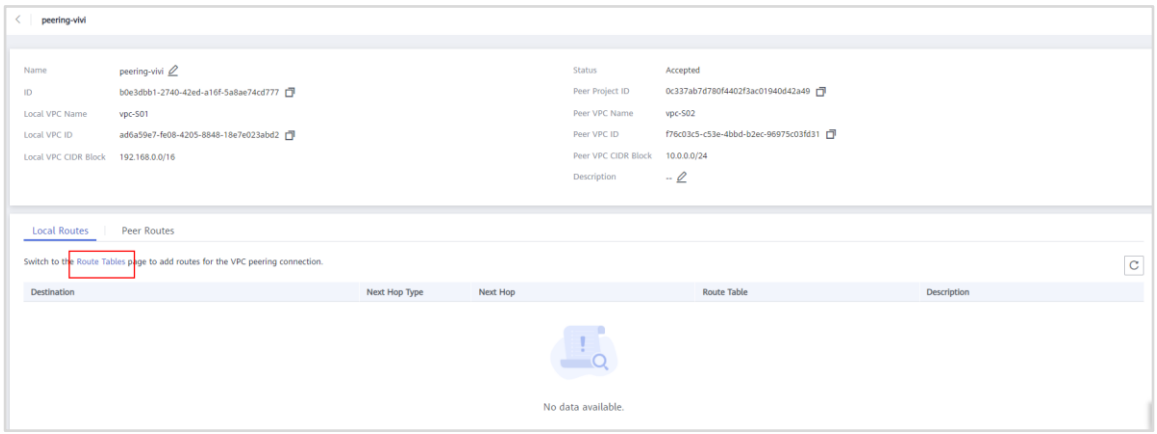


Figure 3-64 Route Tables

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

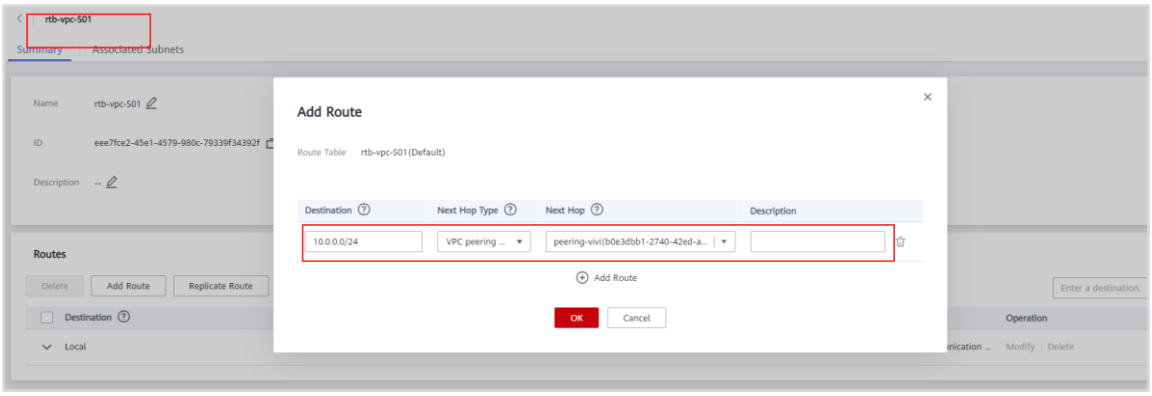


Figure 3-65 Add Route

Step 5 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**.

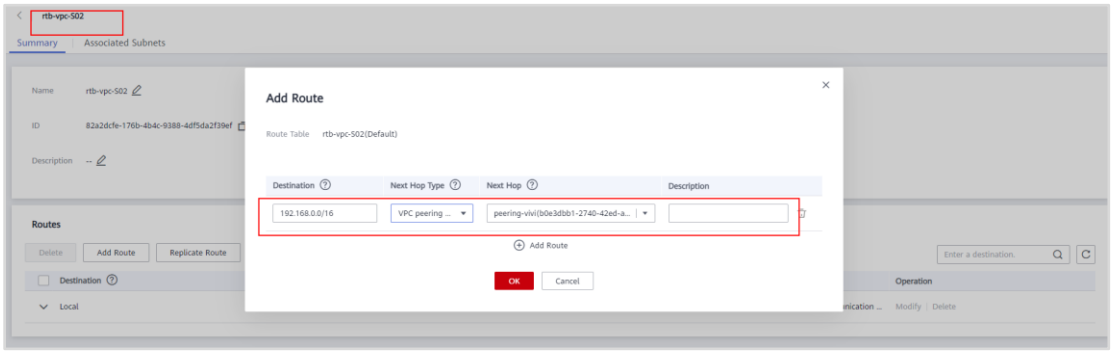


Figure 3-66 Add Route

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

```
[root@ecs-s01 ~]# ping 10.0.0.70
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:

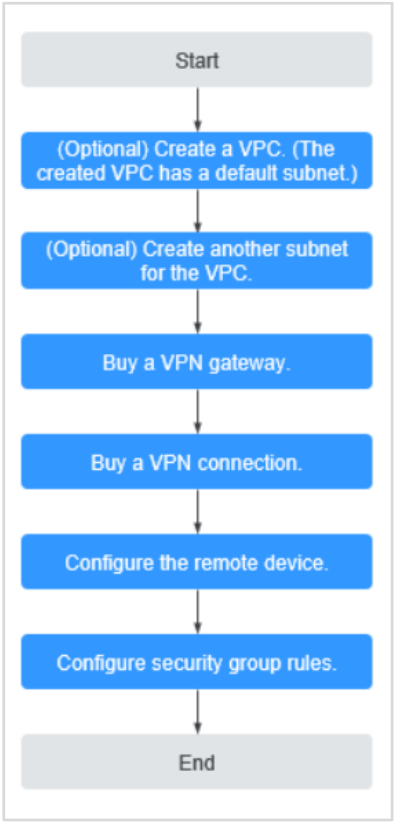


Figure 3-68 VPN configuration flowchart

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-J01**, in the **AF-Johannesburg** region, from **ecs-Sa01**, in the **LA-Santiago** region.
- View the VPN connection status.

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

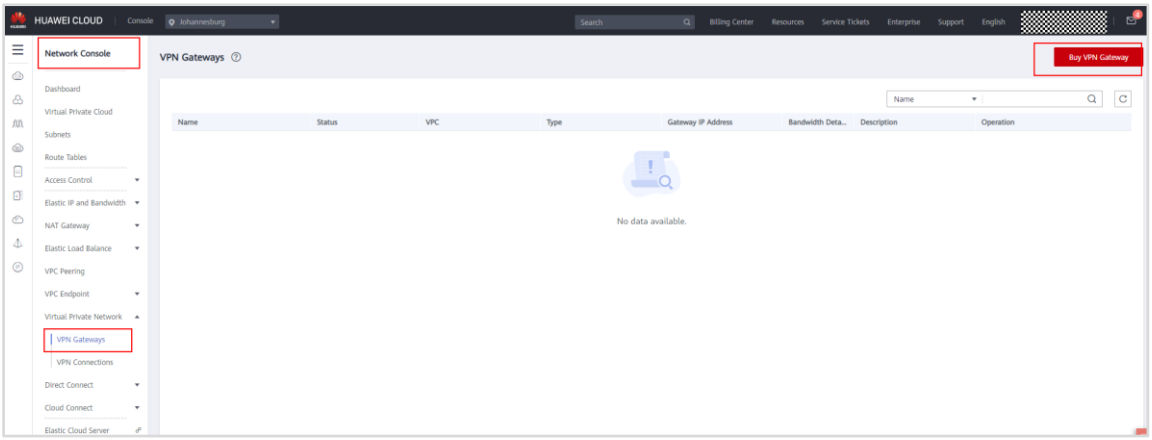


Figure 3-69 Buy VPN Gateway

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

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

VPN connection

- **Name**: **vpn-Johannesburg**
- **Local Subnet**: Select **subnet-01** of **vpc-J01**.
- **Remote Gateway**: Enter an IP address and then replace it with the IP address of the VPN gateway you will create in the **LA-Santiago** region.
- **Remote Subnet**: Enter subnet CIDR blocks of **vpc-Sa01**.
- **PSK**: Enter a value.
- **Advanced Settings**: **Default**

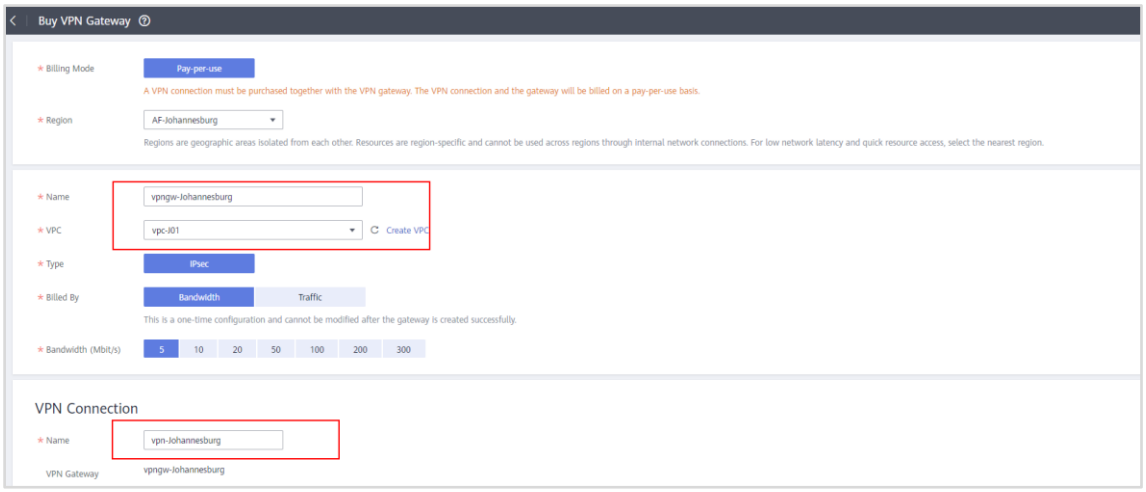


Figure 3-70 Configuring a VPN gateway

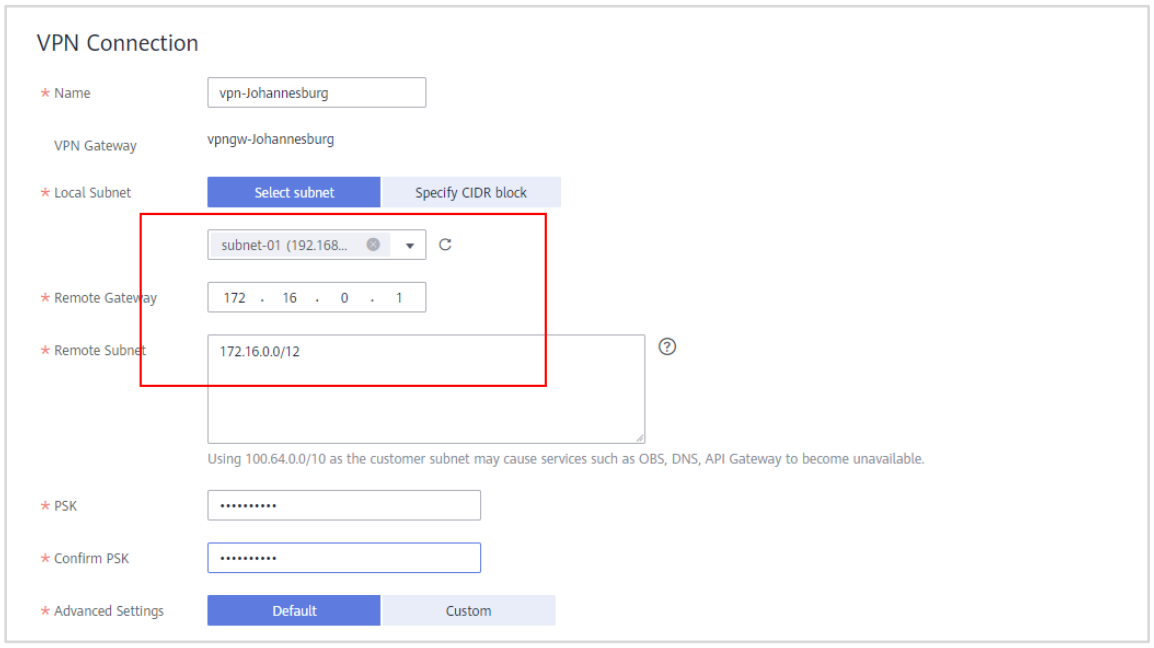


Figure 3-71 Configuring a VPN connection

Step 3 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-Sa01**
- **Type**: **IPsec**
- **Billed By**: **Bandwidth**

- **Bandwidth (Mbit/s)**: **5**

VPN connection

- **Name**: **vpn-Santiago**
- **Local Subnet**: Select **subnet-01** of **vpc-Sa01**.
- **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-J01**.
- **PSK**: Enter the PSK you configured in the **AF-Johannesburg** region.
- **Advanced Settings**: **Default**

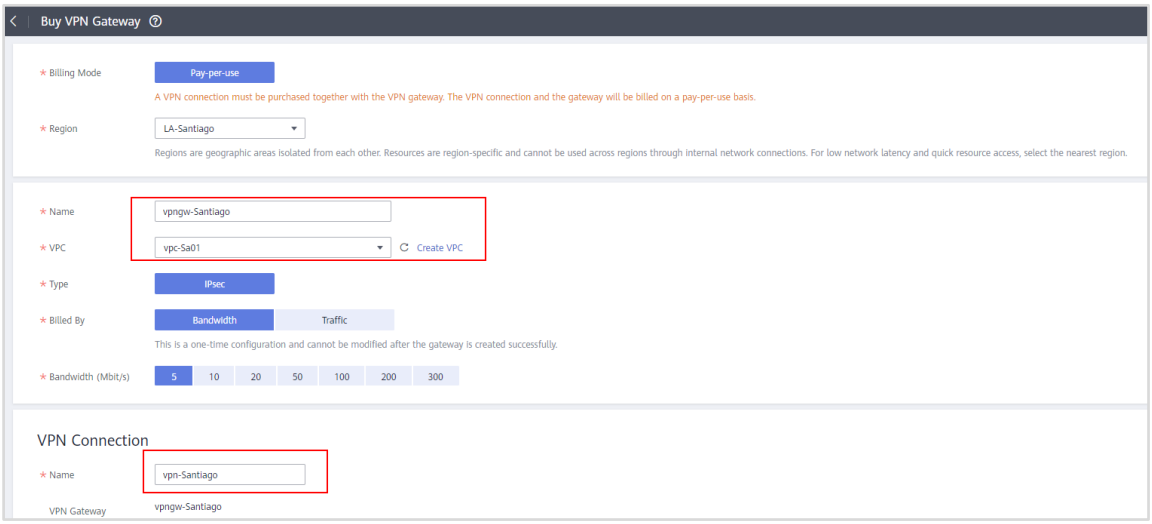


Figure 3-72 Configuring a VPN gateway

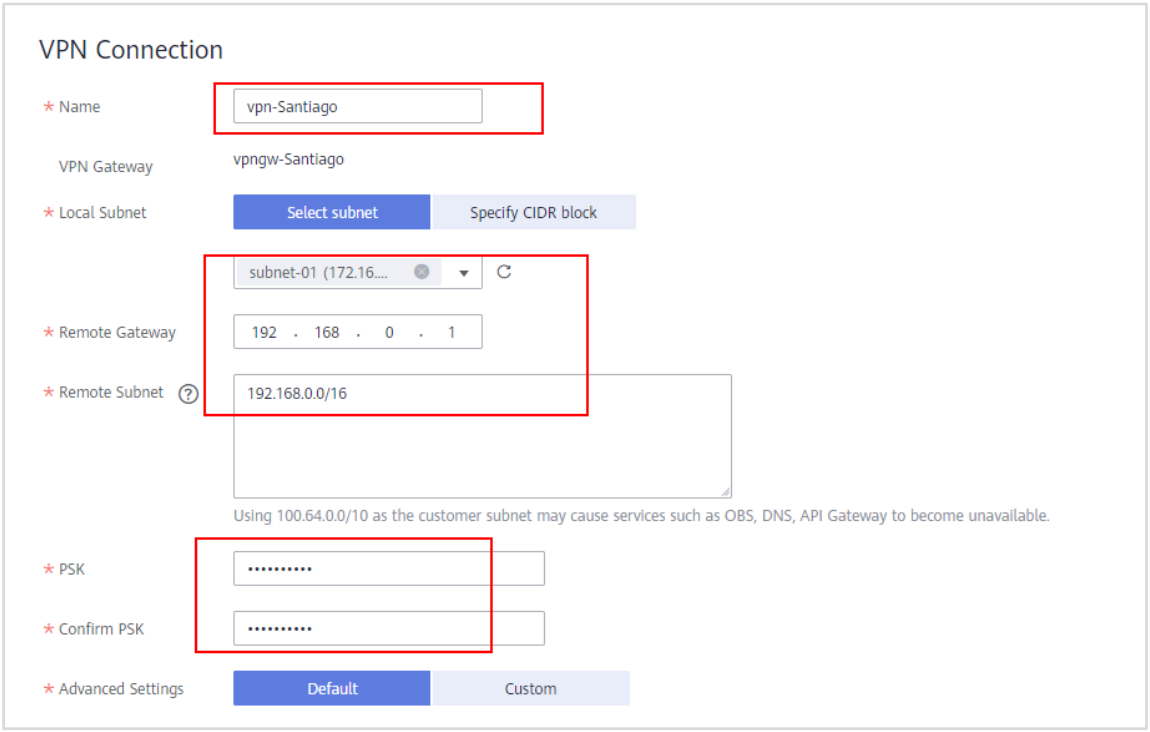


Figure 3-73 Configuring a VPN connection

Step 4 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**.

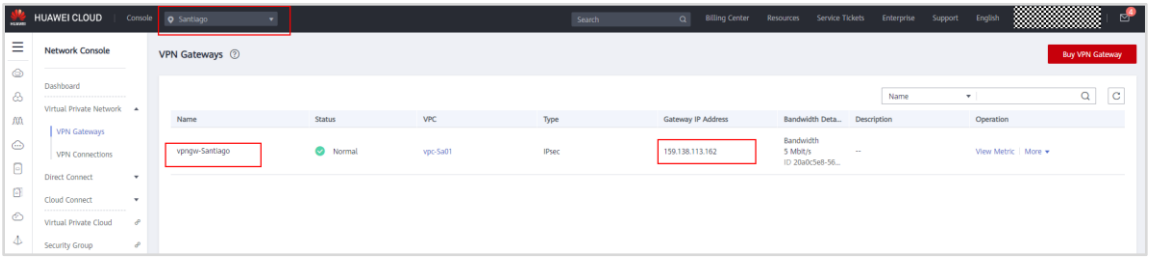


Figure 3-74 Viewing a VPN gateway

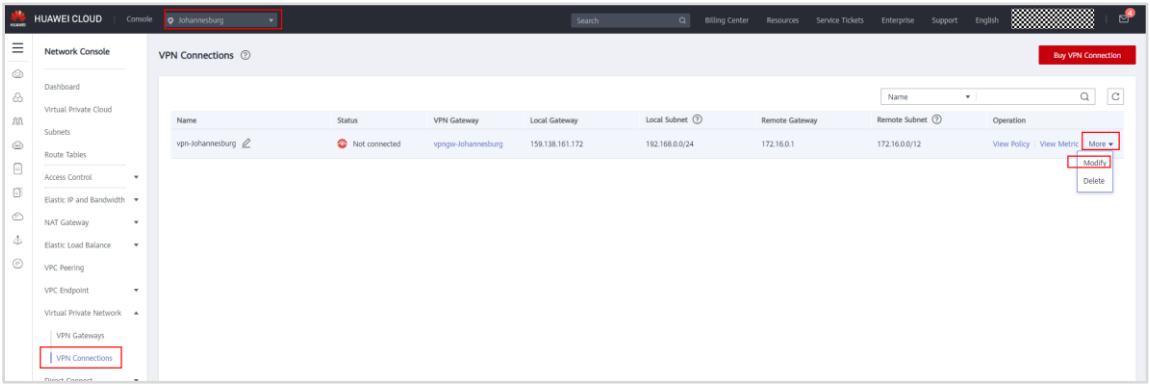


Figure 3-75 Modifying a VPN connection

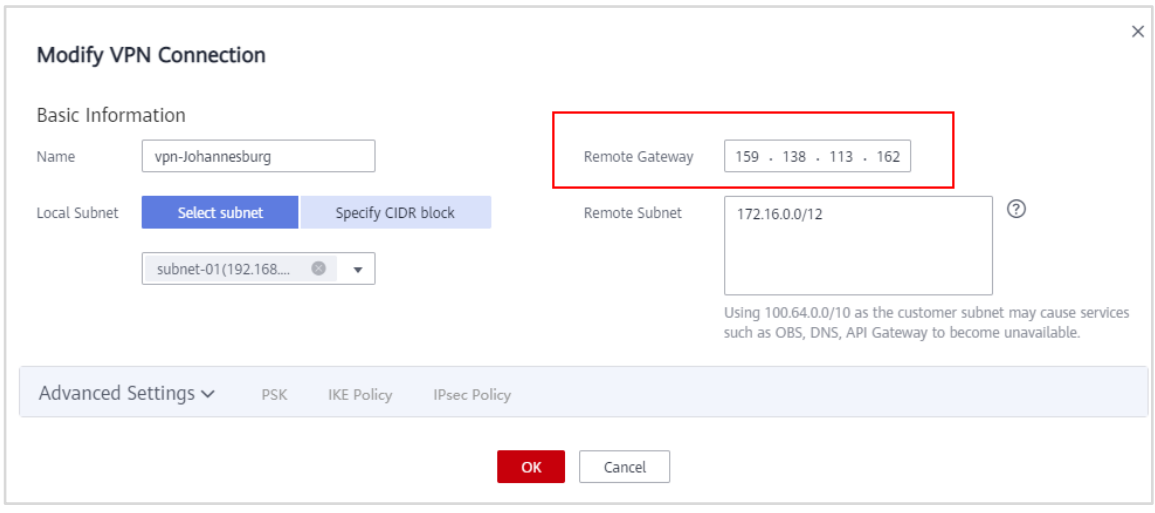


Figure 3-76 Changing the remote gateway IP address

Step 5 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**.

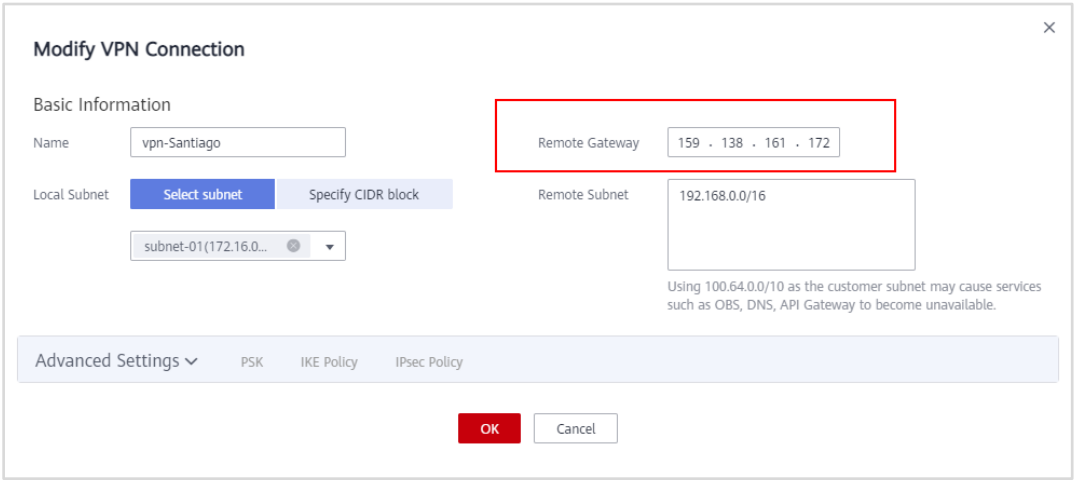


Figure 3-77 Changing the remote gateway IP address

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

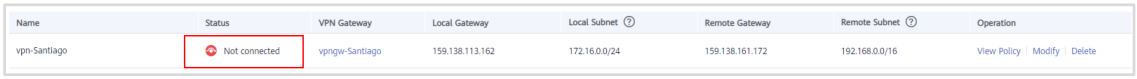


Figure 3-78 Viewing a VPN connection

Step 7 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.

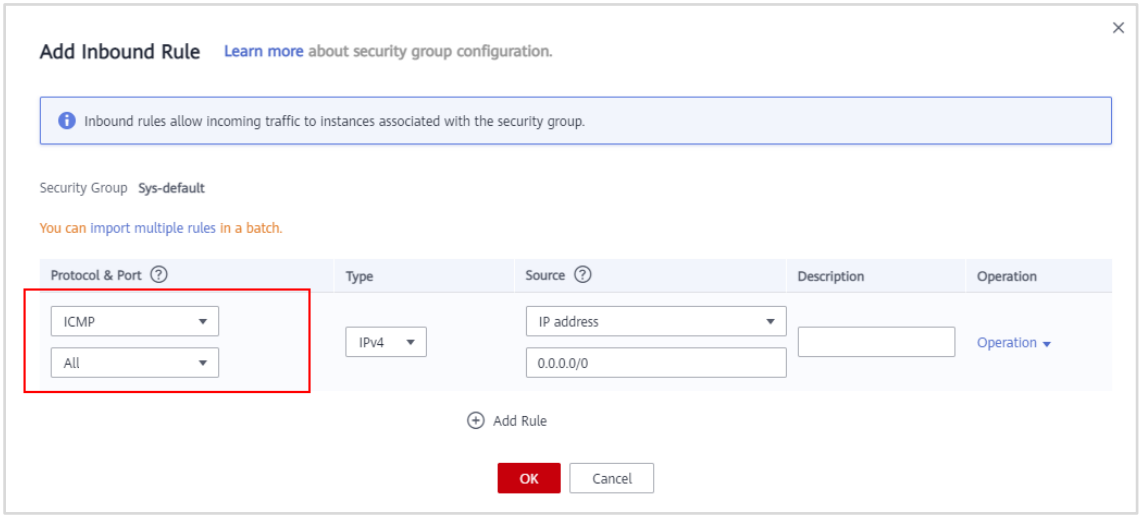


Figure 3-79 Add Inbound Rule

Step 8 In the LA-Santiago region, remotely log in to **ecs-Sa01** in **vpc-Sa01** and ping **ecs-J01** in **vpc-J01** in the **AF-Johannesburg** region. The result shows that ECSs in different regions can communicate with each other.

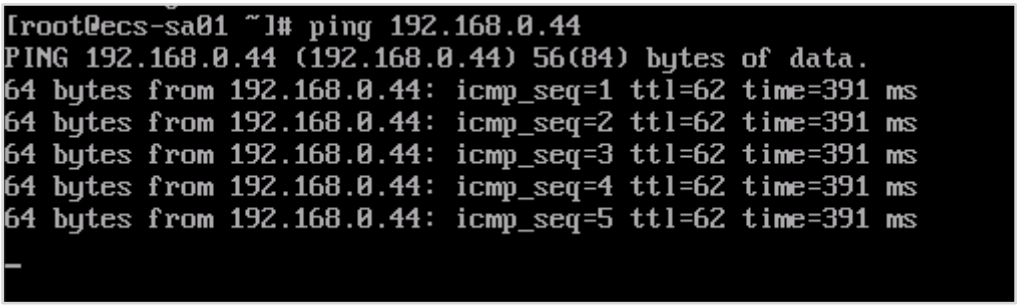


Figure 3-80 Verifying the network connection

Step 9 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**.

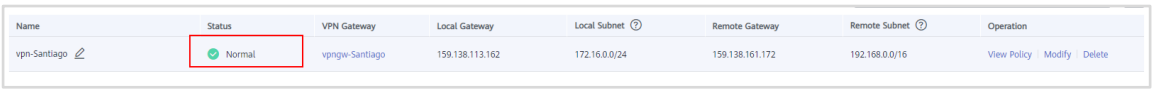


Figure 3-81 Viewing a VPN connection

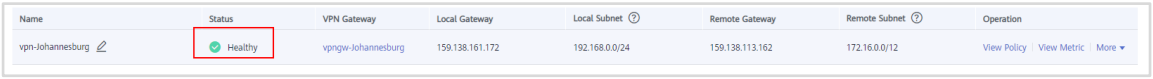


Figure 3-82 Viewing a VPN connection

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

3.2.5 Deleting Resources

Step 1 Delete the ECSs in all regions.

Step 2 Remove the ECSs, delete the listener, and then delete the load balancer in the corresponding region.

Step 3 Delete the VPC peering connection in the corresponding regions.

Step 4 Delete the VPN connection and gateways in the corresponding regions. If you delete the VPN connection, the gateways will be automatically deleted.

Step 5 Delete the VPCs and subnets in all regions.

3.3 Exercises

1. Create three ECSs in the same VPC, one as the client, and the other two as backend servers to receive requests from the load balancer.
2. Use the client to access the private IP address of the load balancer.

   If the web page can be accessed and the content changes after you refresh the web page, the configuration was successful. (For details, see the procedure for using a public network load balancer to route requests over the Internet.)
3. Delete the load balancer. If the load balancer cannot be deleted, locate the cause.
4. Verify a VPC peering connection.

   After you create a VPC peering connection by following the instructions from earlier, create a subnet in the local VPC with the same CIDR block as that of a subnet in the peer VPC. Check network connectivity and explain what you find.
5. Test a VPN connection.

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

4 Storage Services

4.1 EVS

4.1.1 Introduction

4.1.1.1 About This Exercise

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

4.1.1.2 Objectives

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

- Purchase EVS disks.
- Attach EVS disks.
- Initialize EVS disks 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.

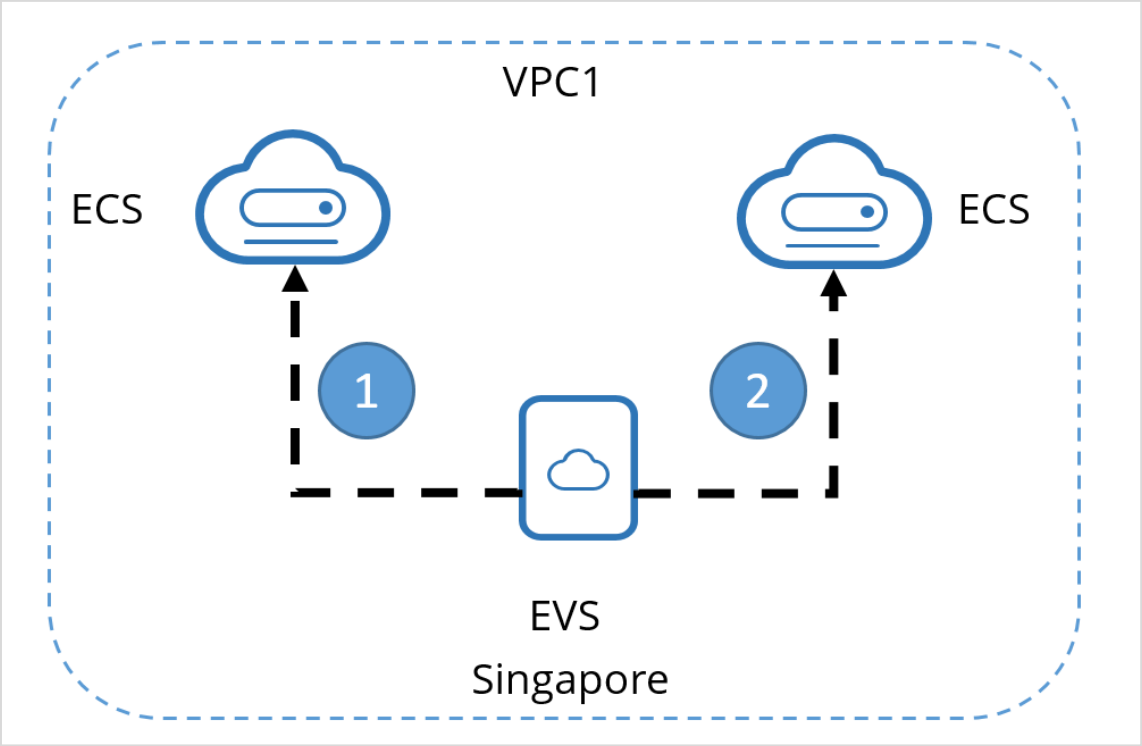


Figure 4-1 Topology

4.1.2.2 Attaching an EVS Disk to a Windows ECS

4.1.2.2.1 Purchasing an EVS Disk

Step 1 Buy a Windows ECS (Windows Server 2012 R2 Standard 64-bit English) by referring to the preceding sections.

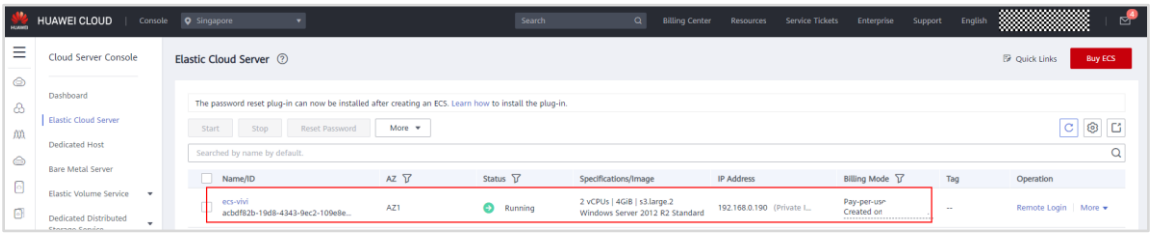


Figure 4-2 Viewing the ECS

Step 2 Log in to the management console. In the service list, choose **Elastic Volume Service** under **Storage** to go to the **Elastic Volume Service** page.

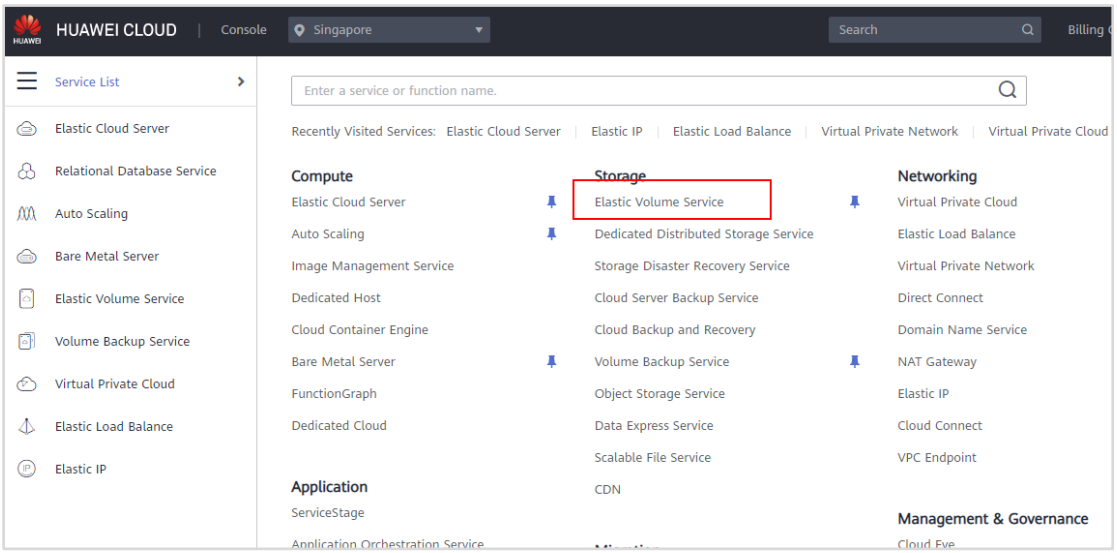


Figure 4-3 Opening EVS console

Step 3 Click **Buy Disk**.

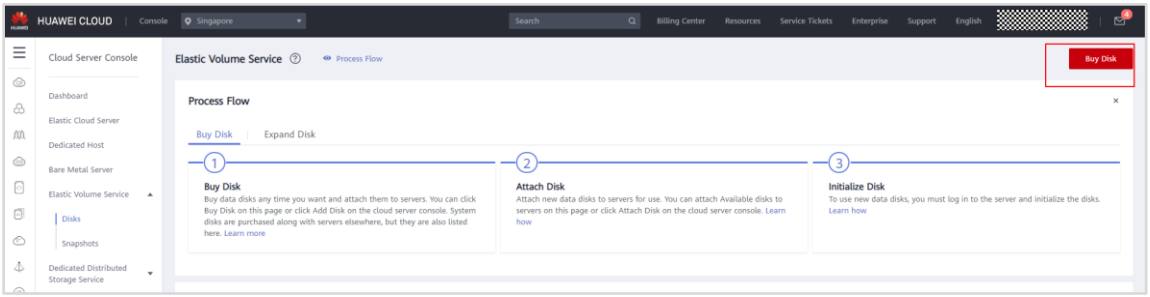


Figure 4-4 Buy Disk

Step 4 Set disk parameters as follows:

- **Billing Mode**: **Pay-per-use**
- **Region**: **AP-Singapore**
- **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** (custom)

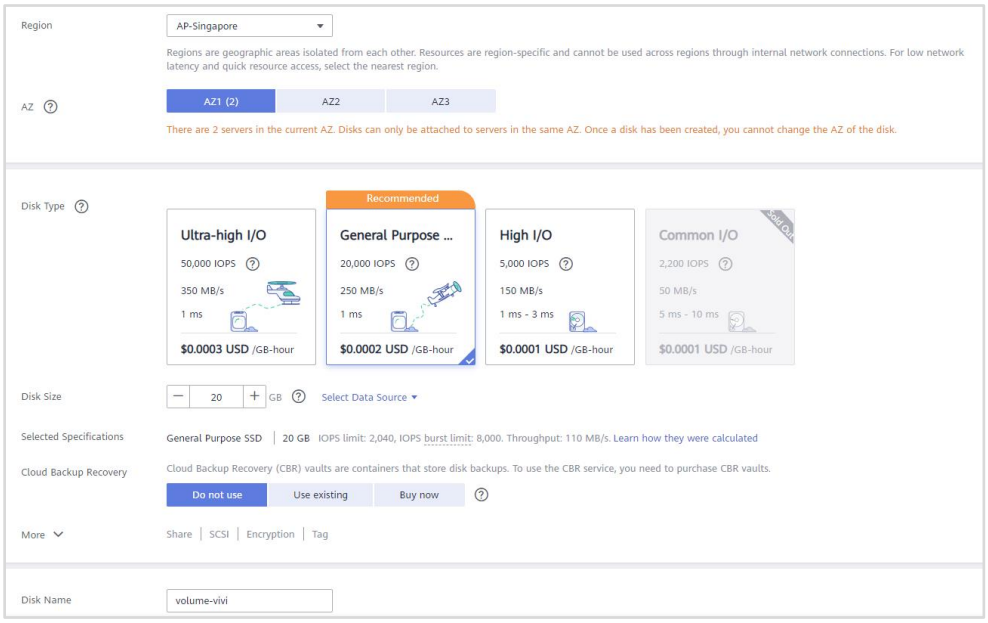


Figure 4-5 Setting disk parameters

Step 5 Click **Next**.

Step 6 On the **Details** page, confirm the disk configuration. If you need to modify the configuration, click **Previous**. If not, click **Submit**.

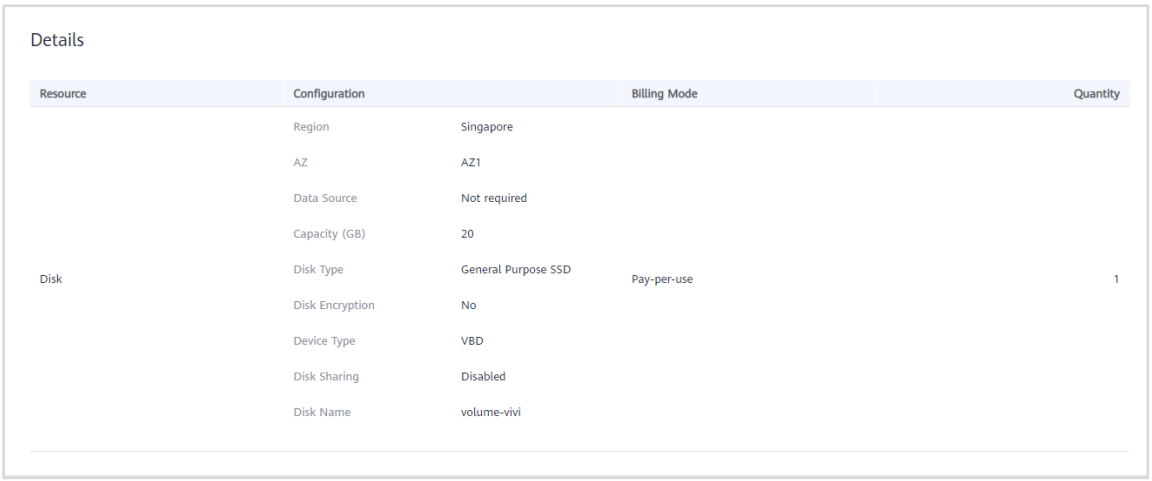


Figure 4-6 Confirming disk parameter settings

Step 7 Go back to the disk list page and view the disk status. When the disk status changes to **Available**, the disk has been purchased.

4.1.2.2.2 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.)

Step 1 In the EVS disk list, locate the EVS disk to be attached and click **Attach** in the **Operation** column.

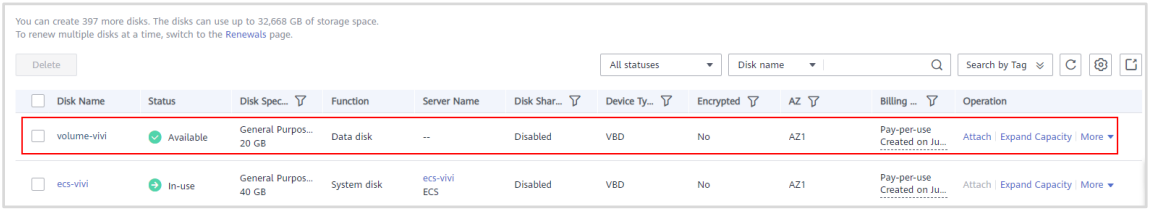


Figure 4-7 Viewing the EVS disk

Step 2 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.

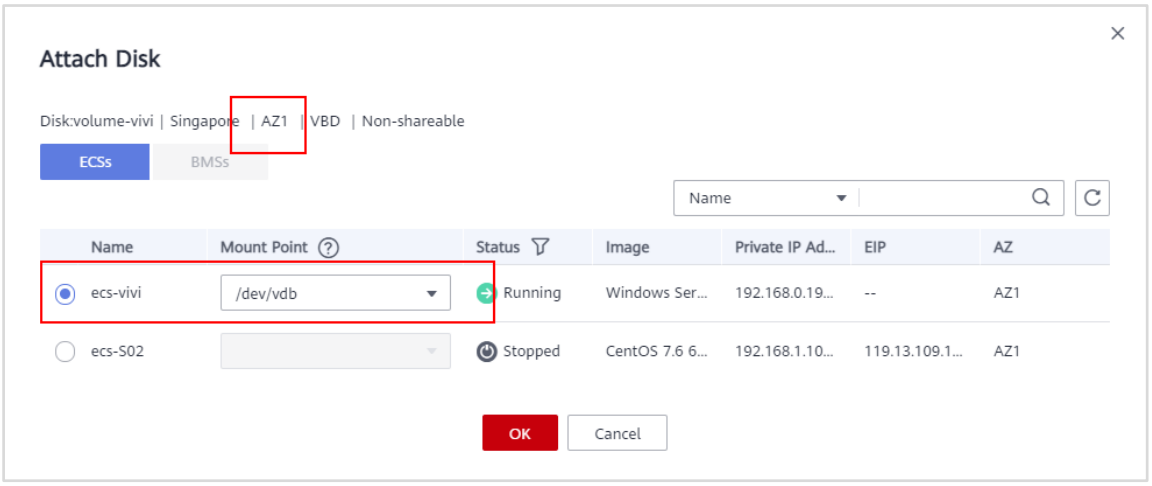


Figure 4-8 Attach Disk

Step 3 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.

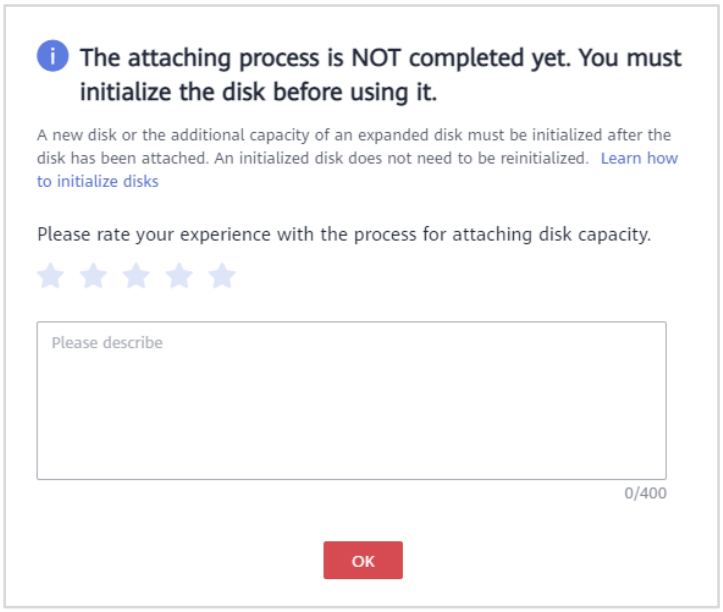


Figure 4-9 Disk attached

4.1.2.2.3 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.

Step 1 Locate the row that contains the target ECS and click **Remote Login** in the **Operation** column.

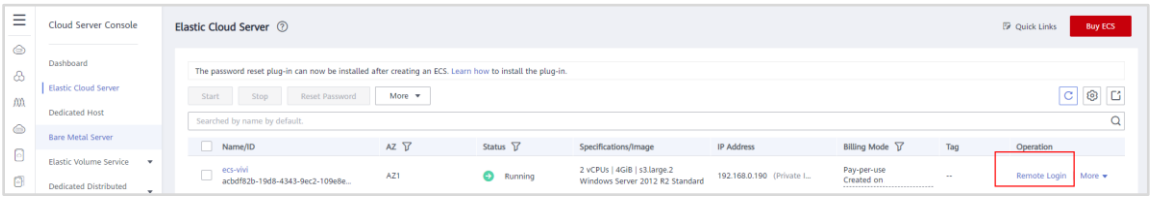


Figure 4-10 Logging in to the ECS

Step 2 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**.

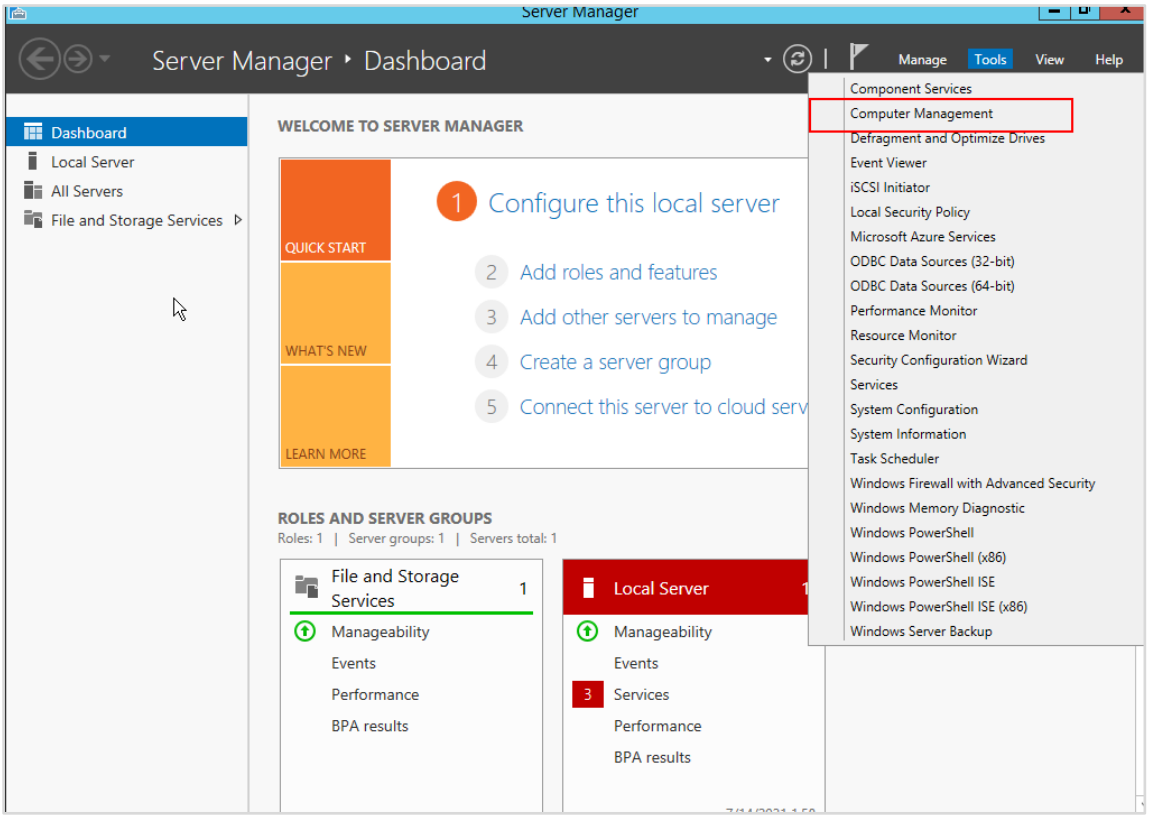


Figure 4-11 Opening Server Manager

Step 3 In the navigation tree on the left, choose **Storage** > **Disk Management**.

Step 4 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**.

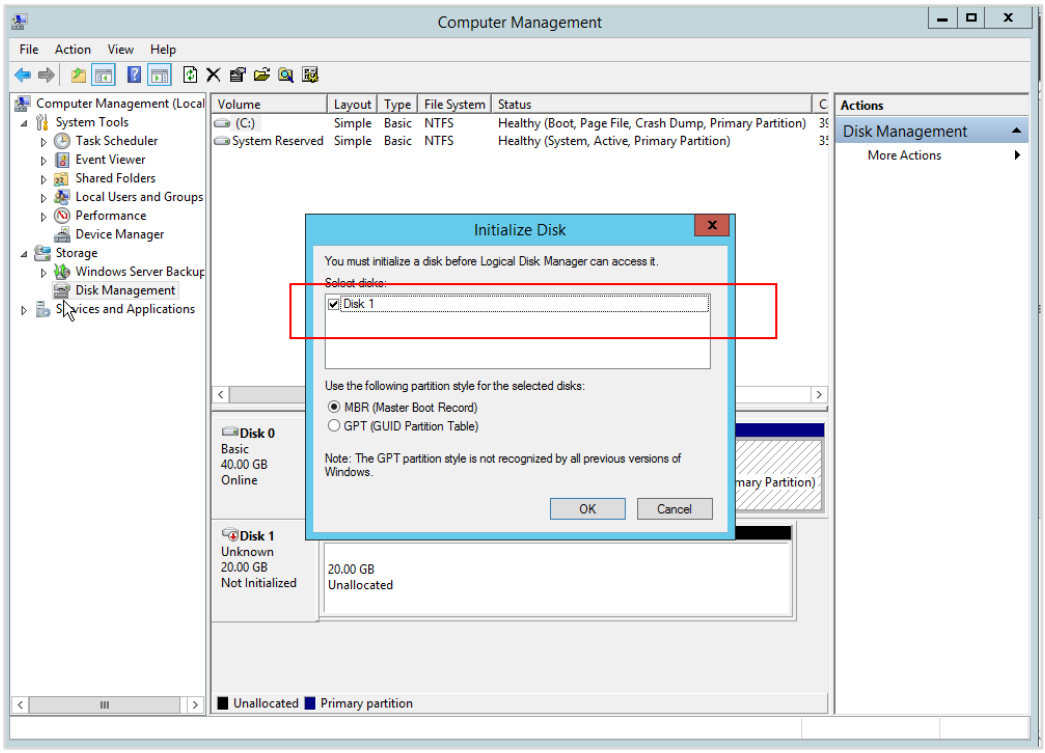


Figure 4-12 Initialize Disk

Step 5 Right-click the unallocated area and choose **New Simple Volume**.

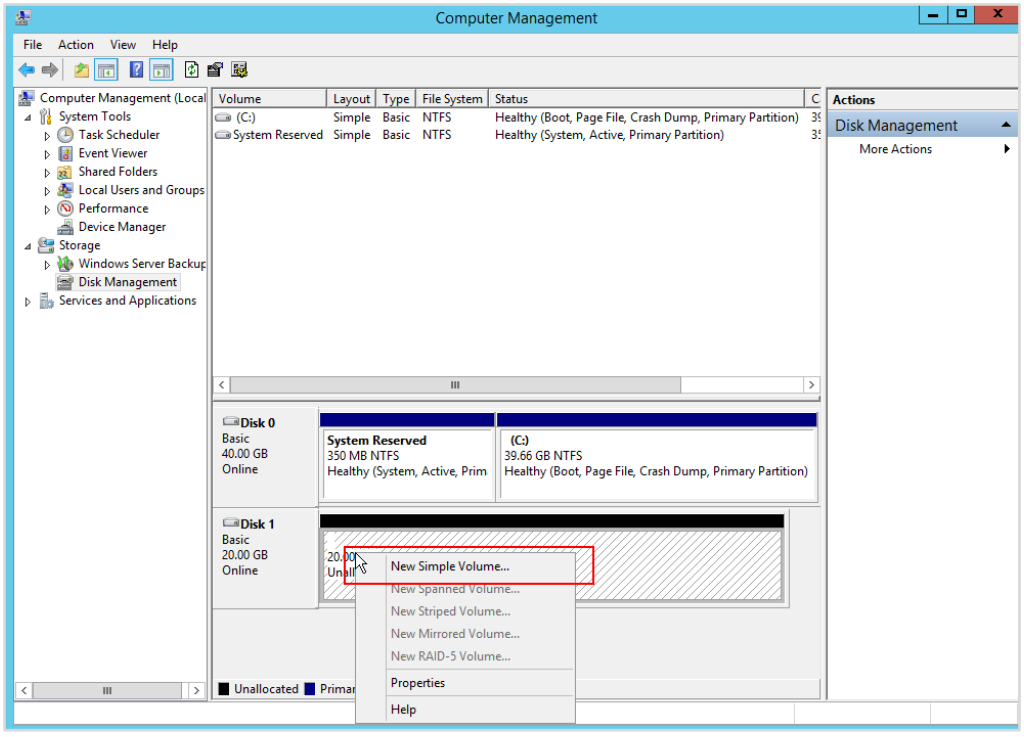


Figure 4-13 New Simple Volume

Step 6 In the displayed **New Simple Volume Wizard** window, click **Next**.

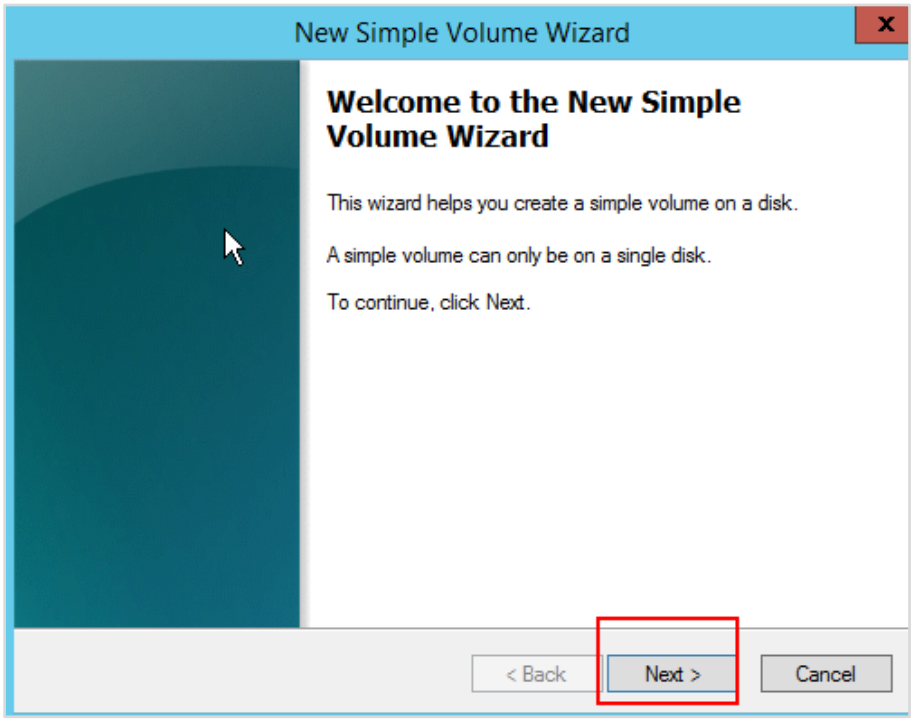


Figure 4-14 New Simple Volume

Step 7 Specify the volume size and click **Next**. The default value is the maximum size.

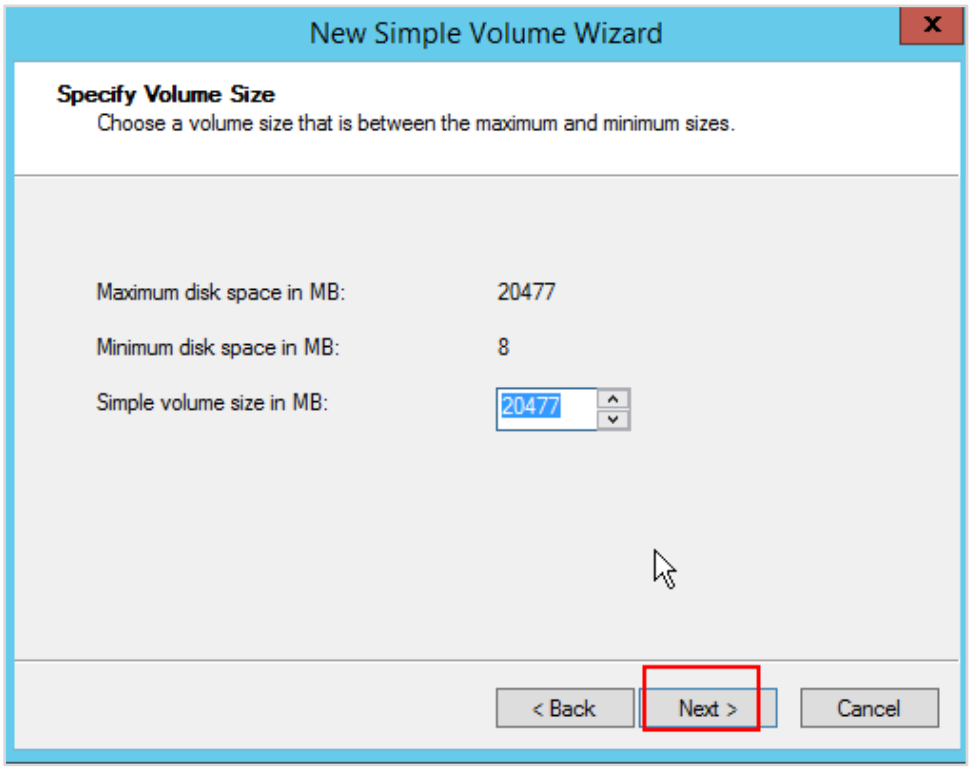


Figure 4-15 Specify Volume Size

Step 8 Assign a drive letter and click **Next**.

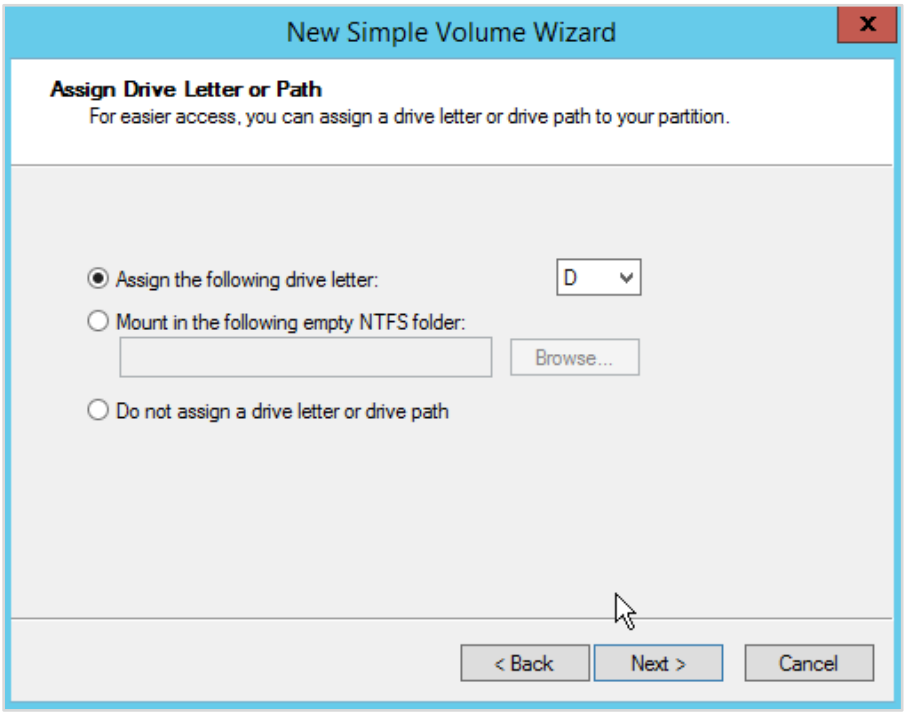


Figure 4-16 Assign Driver Letter or Path

Step 9 Select **Format this volume with the following settings**, set parameters based on the requirements, and select **Perform a quick format**. Then, click **Next**.

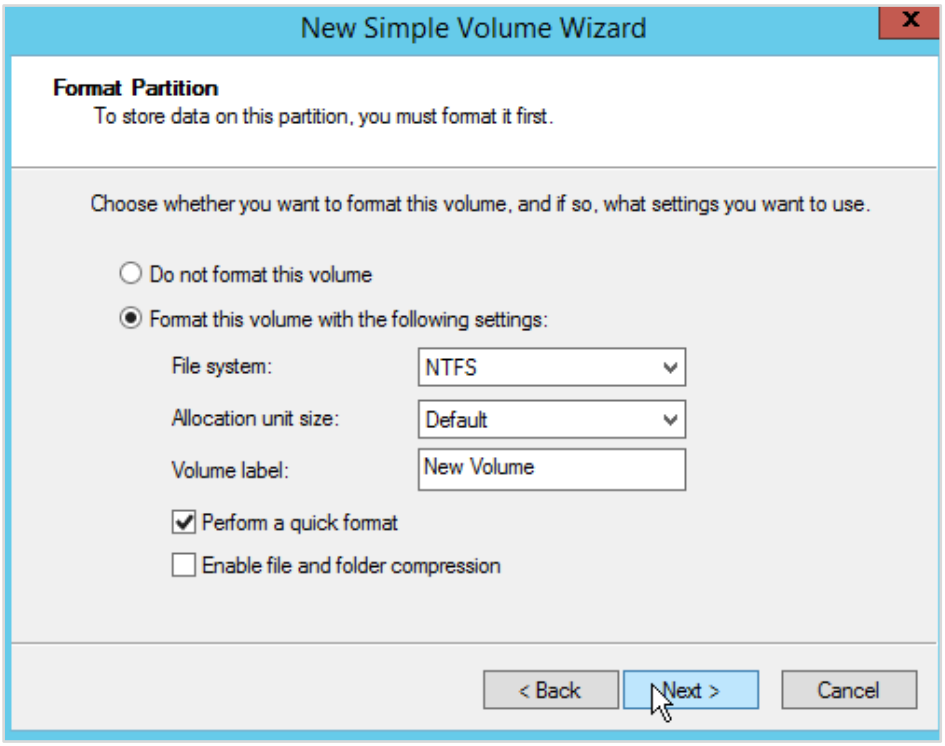


Figure 4-17 Formatting the partition

Step 10 Click **Finish**. Wait for the initialization to complete. When the volume status changes to **Healthy**, the initialization is complete.

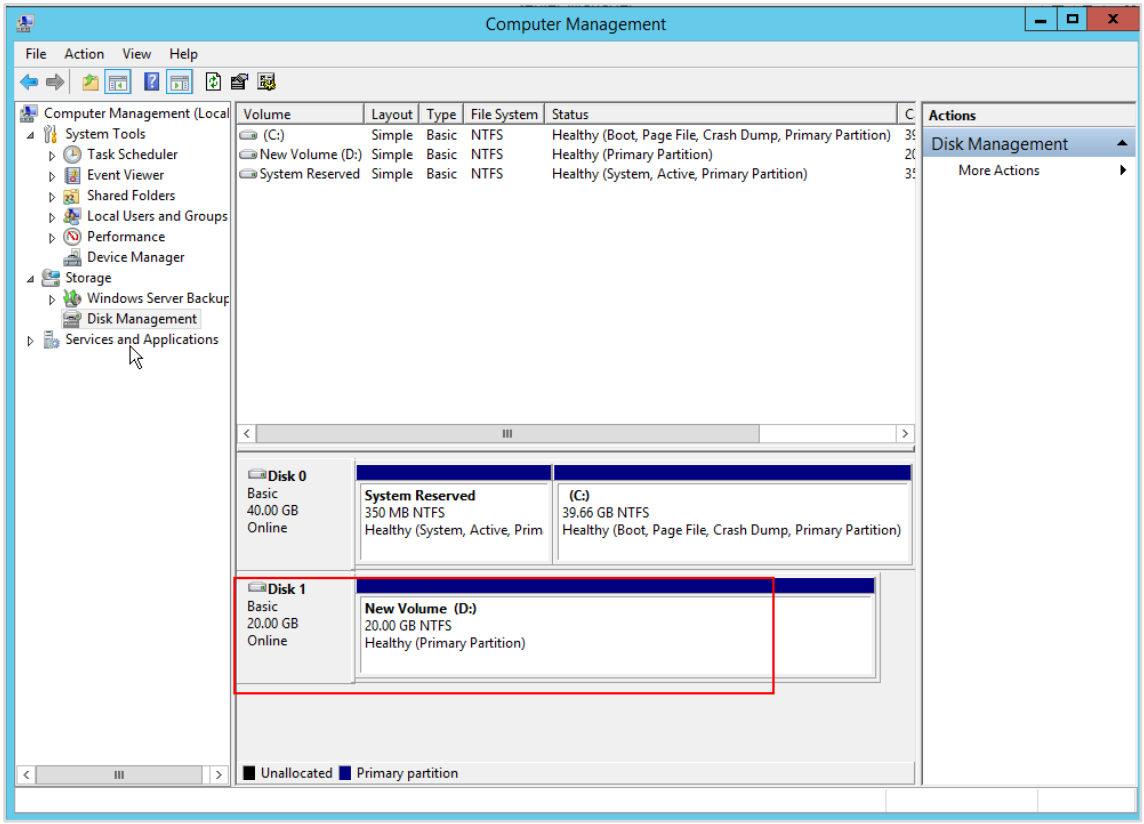


Figure 4-18 Viewing the initialized disk

Step 11 Open **This PC**. If a new volume appears, the disk has been attached.

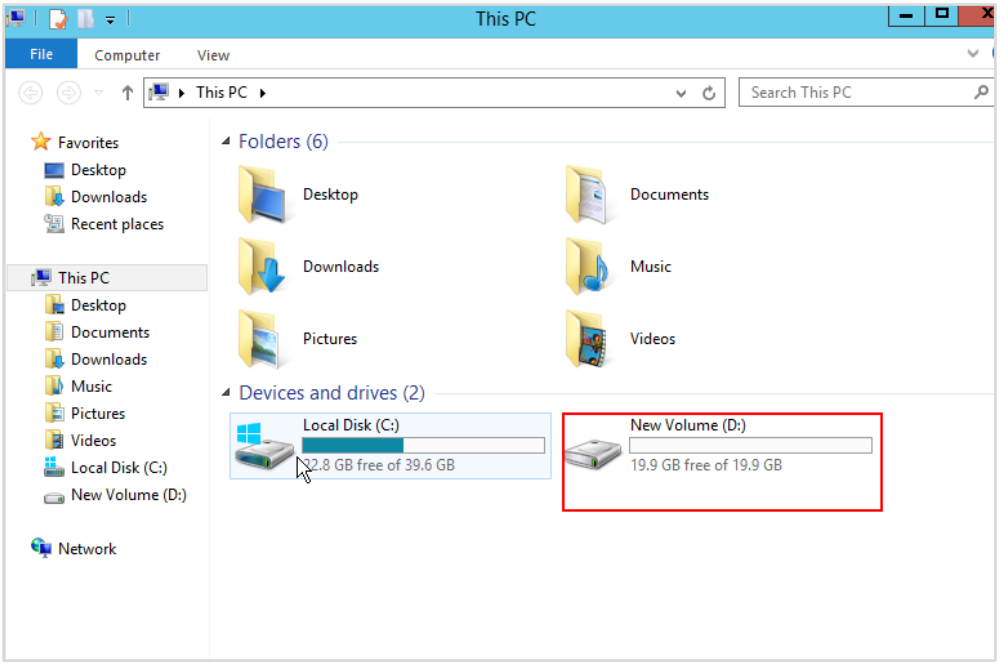


Figure 4-19 Viewing the new volume

4.1.2.2.4 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.

Step 1 Locate the row that contains the target ECS and click **Remote Login** in the **Operation** column.

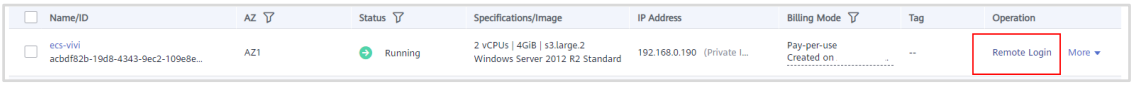


Figure 4-20 Remotely logging in to the ECS

Step 2 Create a test file **test.txt** on the attached EVS disk.

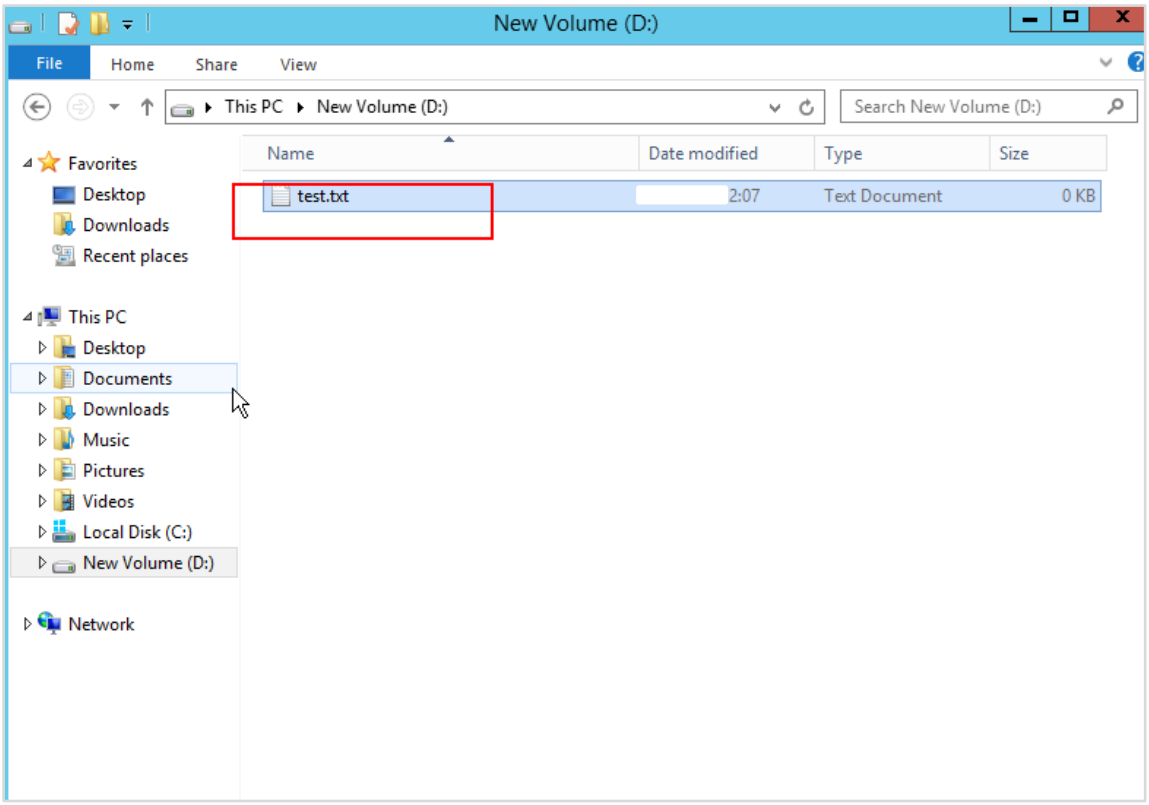


Figure 4-21 Creating the test file

Step 3 Open the **Disk Management** window and bring the EVS disk offline.

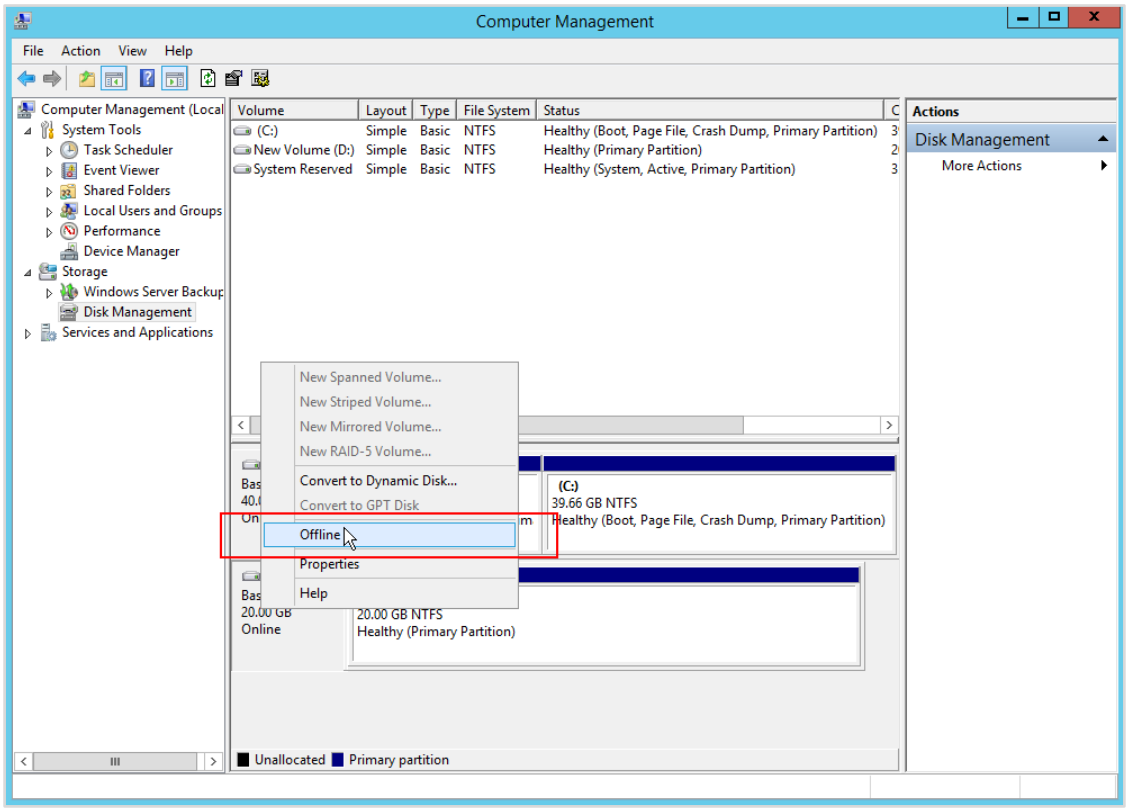


Figure 4-22 Bringing the new disk offline

Step 4 Open **This PC** and check that volume D disappears.

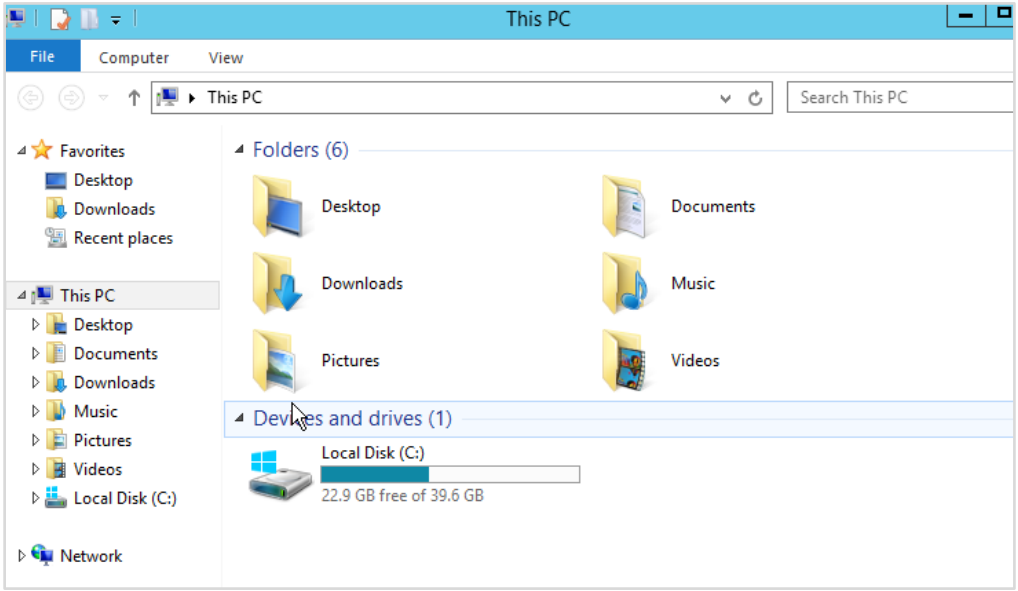


Figure 4-23 Checking whether the disk is offline

Step 5 Buy another Windows ECS (Windows Server 2012 R2 Standard 64-bit English) by referring to the preceding sections.

Figure 4-24 Purchasing an ECS

Step 6 Detach the EVS disk from ECS **ecs-vivi** and attach it to ECS **ecs-test**, the newly purchased ECS.

Figure 4-25 Detach Disk

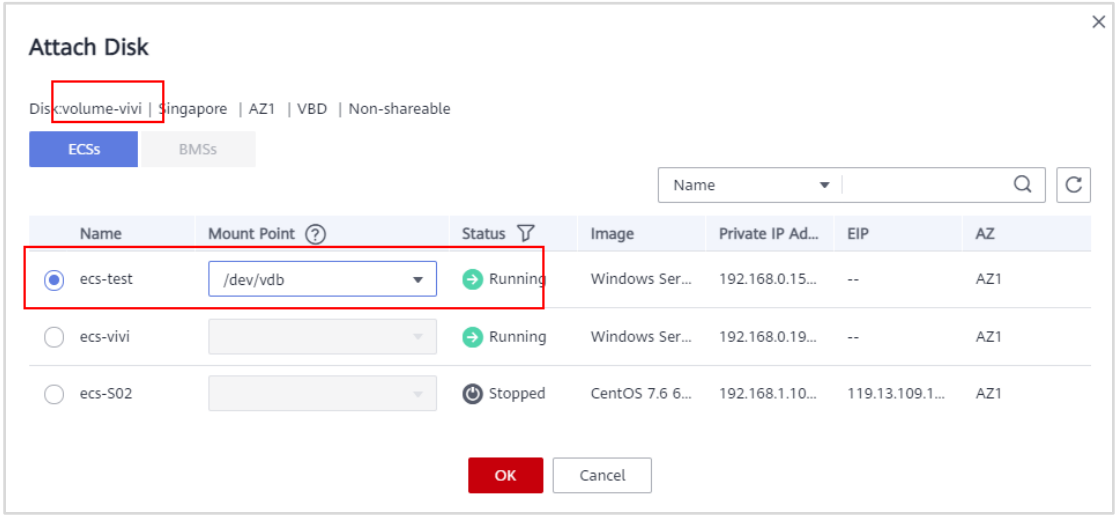


Figure 4-26 Attach Disk

Step 7 Log in to the ECS console, find ECS **ecs-test**, and click **Remote Login**.

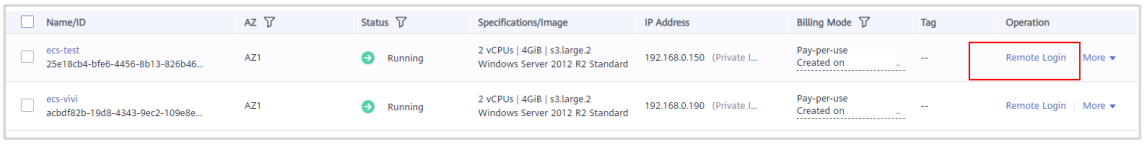


Figure 4-27 Remotely logging in to the ECS

Step 8 Open the **Disk Management** window and check that the EVS disk is online.

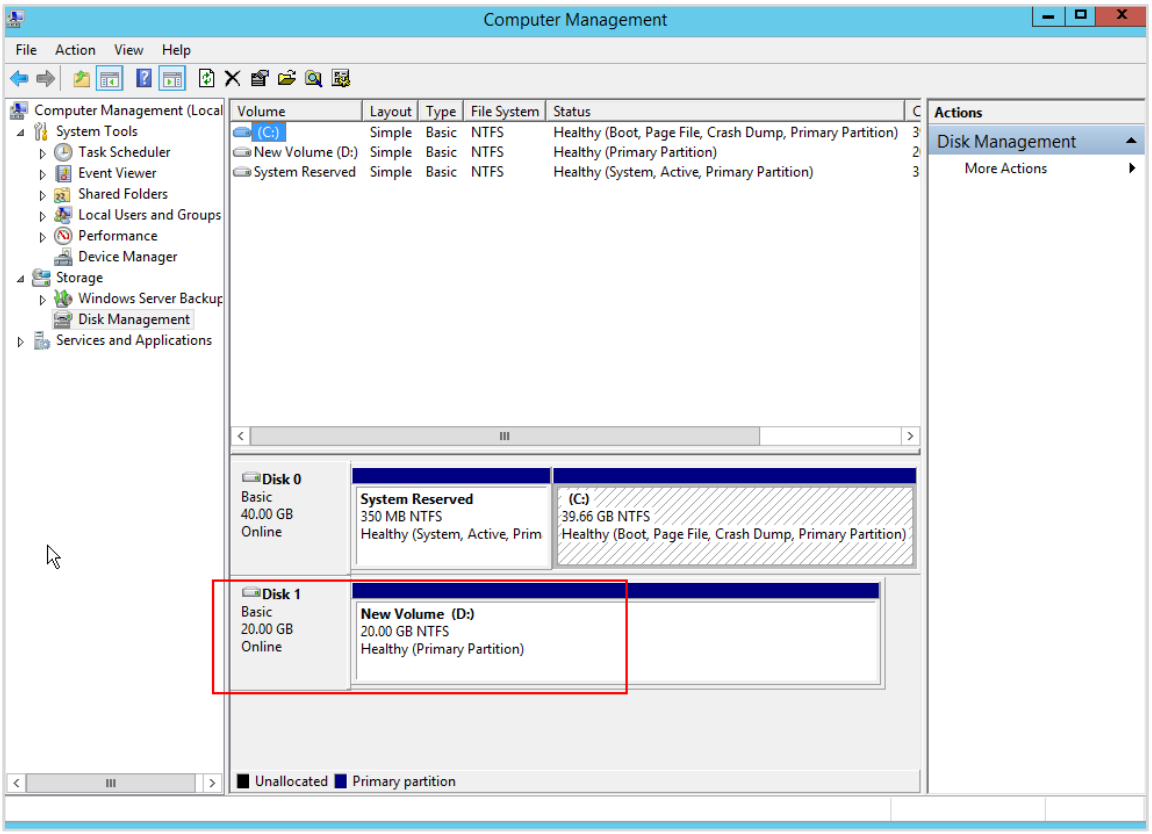


Figure 4-28 Viewing the disk status

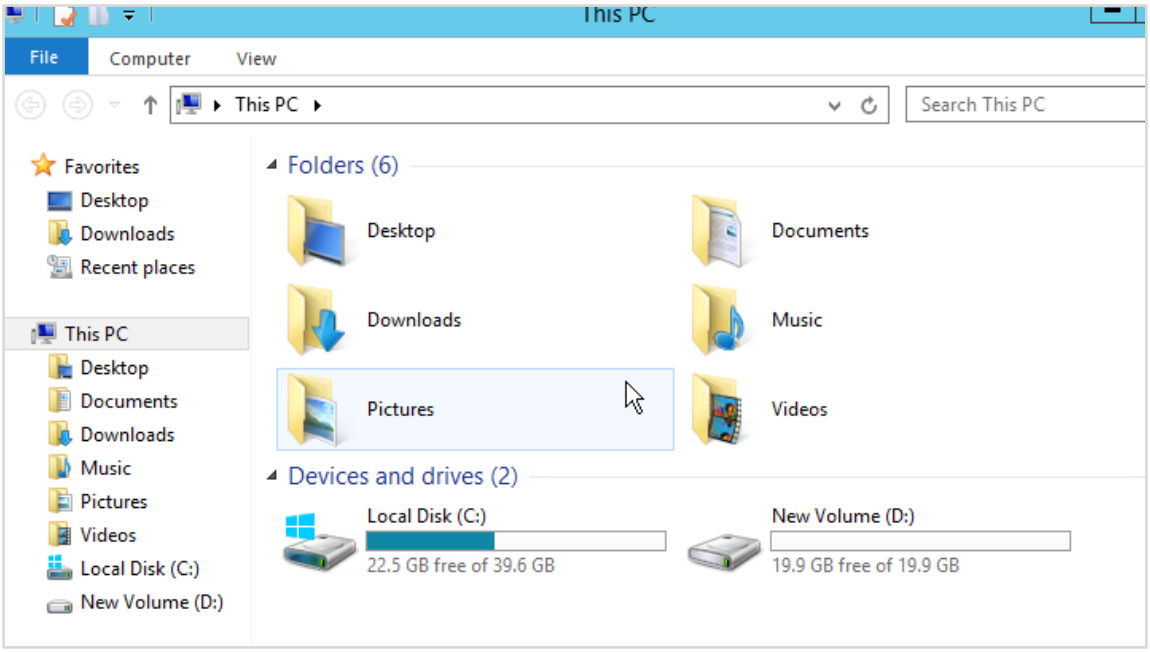


Figure 4-29 Checking whether a new volume appears

Step 9 Check whether test file **test.txt** exists.

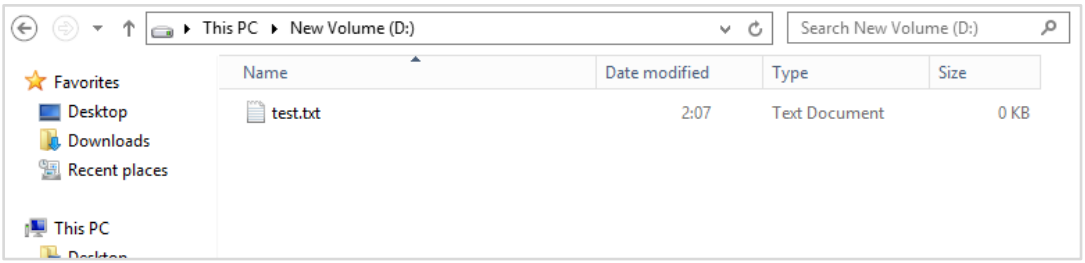


Figure 4-30 Viewing the test file

The file exists, verifying that this exercise succeeds.

4.1.2.3 Attaching an EVS Disk to a Linux ECS

Step 1 Buy a Linux ECS (CentOS 7.6 64 bit) by referring to the preceding sections.

Step 2 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.)

Step 3 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**.

Step 4 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

Step 5 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**.

Step 6 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**.

Step 7 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.

Step 8 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.

Step 9 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**.

Step 10 Run the following command to synchronize the changes in the partition table to the OS:

```
partprobe
```

Step 11 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**.

Step 12 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
```

Step 13 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
```

Step 14 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

Step 1 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

Step 2 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.

Step 3 Run the command to unmount the partition. In this example, run the following command:

```
umount /dev/vdb1
```

Step 4 Run the following command to reload all the content in the **/etc/fstab** file:

```
mount -a
```

Step 5 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

Step 1 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

Step 2 Locate the EVS disk purchased before and choose **More** > **Create Snapshot** in the **Operation** column.

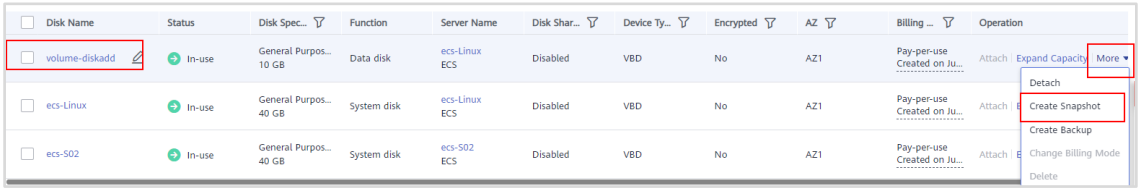


Figure 4-44 Create Snapshot

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

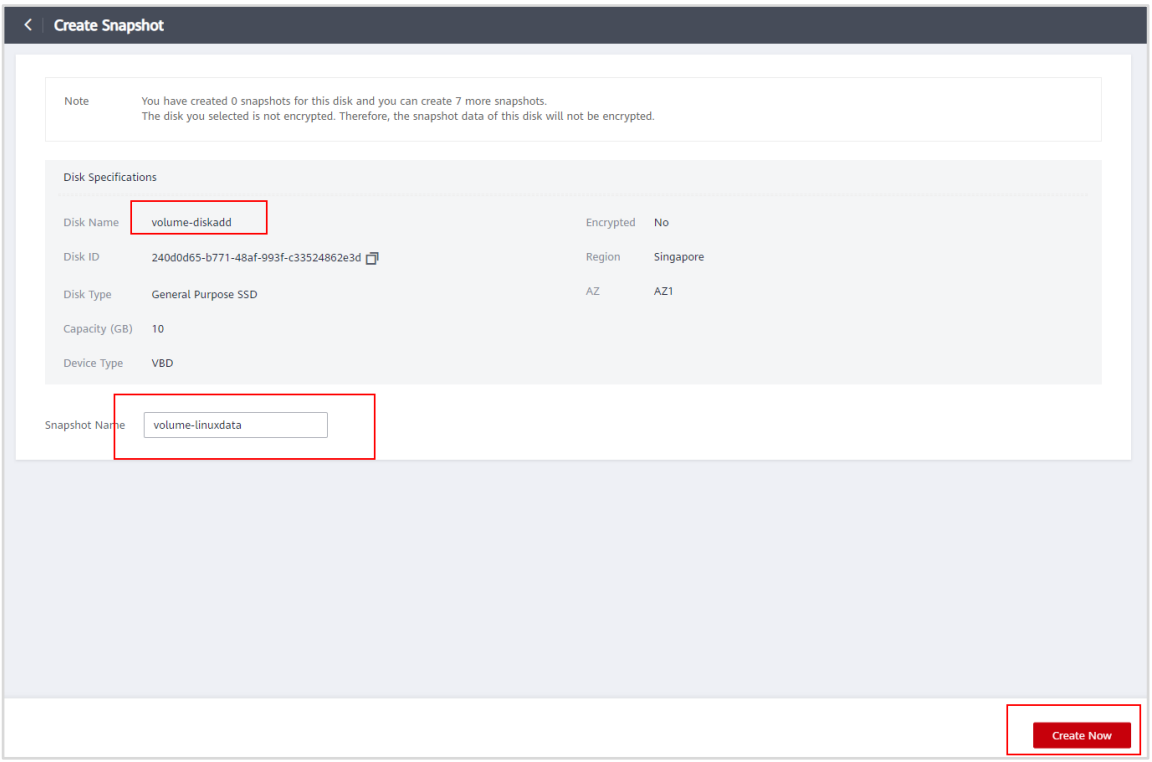


Figure 4-45 Setting snapshot parameters

Step 4 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.

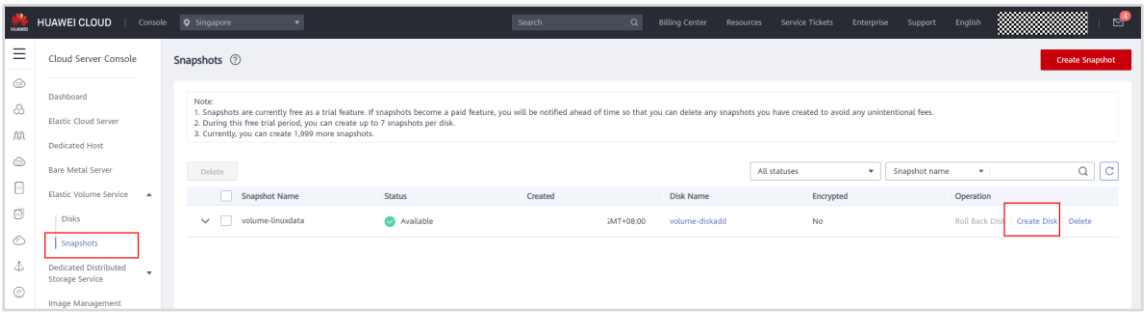


Figure 4-46 Create Disk

Step 5 Buy a disk according to the following figure.

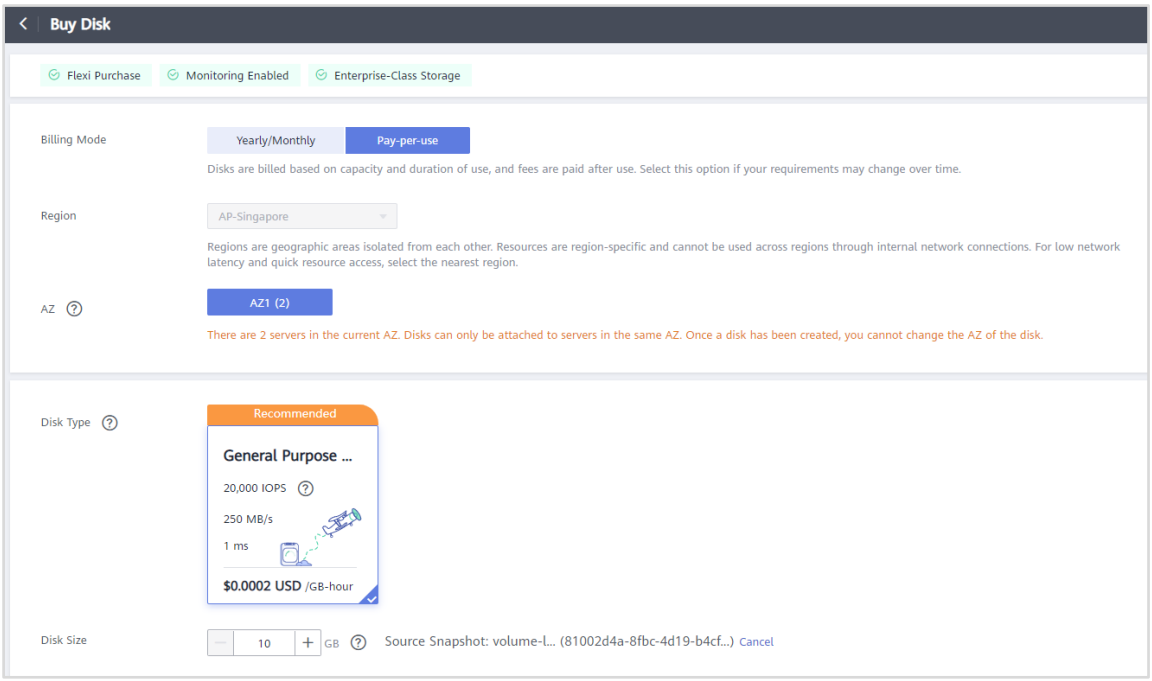


Figure 4-47 Setting disk parameters

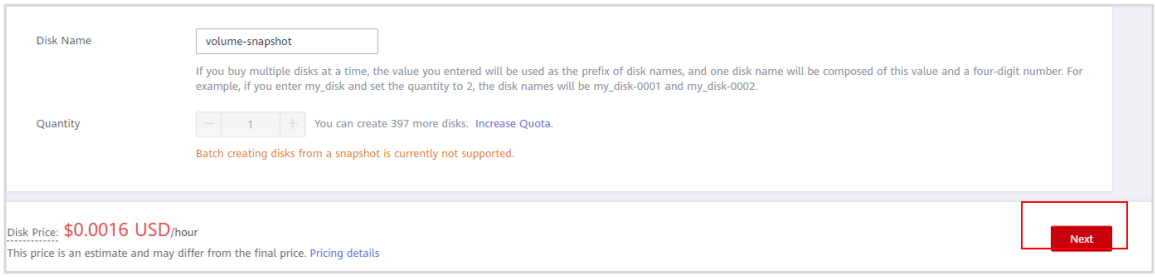


Figure 4-48 Setting disk parameters

Step 6 View the disk created from the snapshot.

Figure 4-49 Viewing the disk

Step 7 Attach the disk to ECS **ecs-linux**.

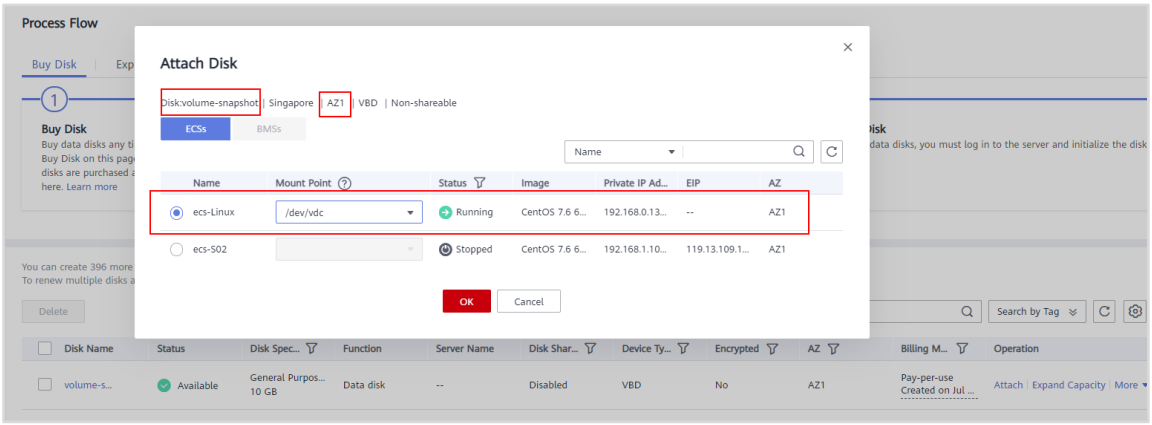


Figure 4-50 Attach Disk

Step 8 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

Step 9 Run the following command to create a mount point:

```
mkdir /mnt/mdc
```

Step 10 Run the following command to mount the new partition **/dev/vdc1** on **/mnt/mdc**:

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

Step 11 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+

4.2.2.2.1 Obtaining Access Keys (AK and SK)

Step 1 On the homepage of HUAWEI CLOUD console, hover your cursor over your username and choose **My Credentials**.

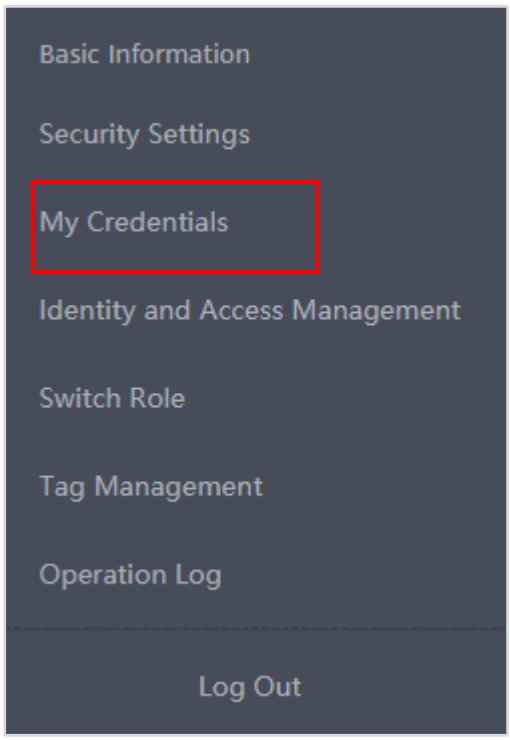


Figure 4-54 My Credentials

Step 2 In the navigation pane, choose **Access Keys**. Click **Create Access Key**.

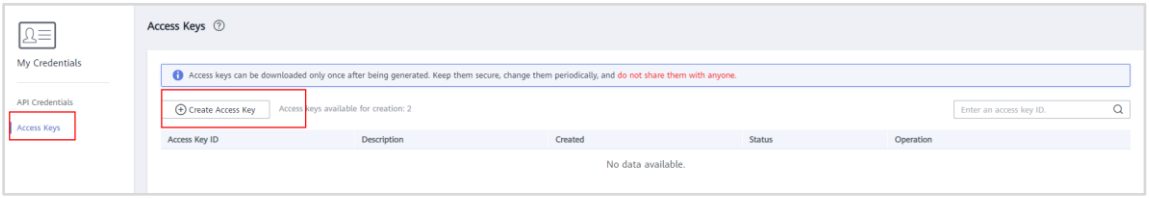


Figure 4-55 Create Access Key

Step 3 In the displayed dialog box, enter the email or SMS verification code.

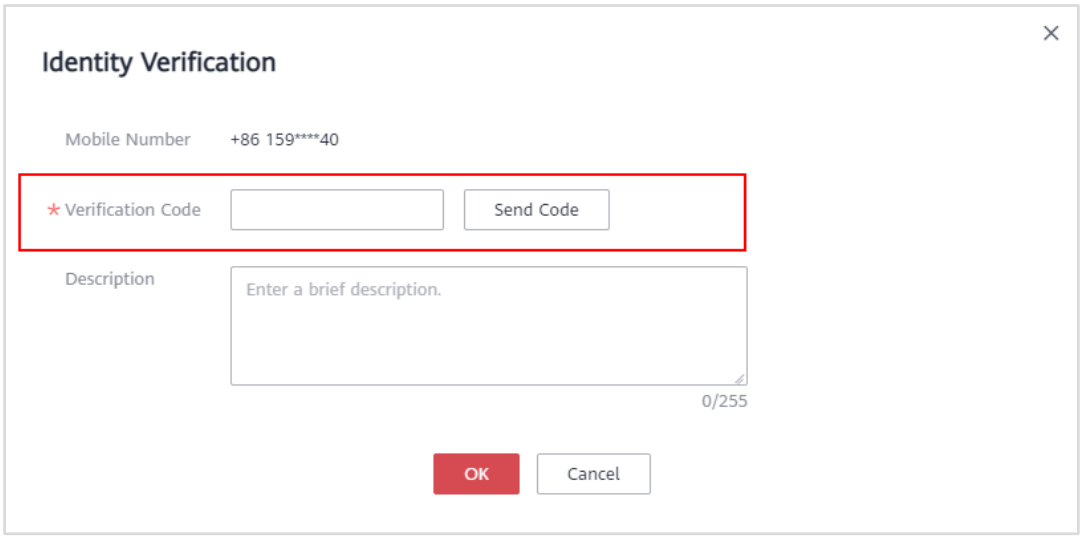


Figure 4-56 Identity Verification

Step 4 Click **OK** to download the key file.

Step 5 Save the key file when prompted.

Keep the access keys properly.

Step 6 Open the downloaded file **credentials.csv** to obtain the AK and SK pair.

4.2.2.2.2 Downloading and Initializing OBS Browser+

Step 1 On the console homepage, choose **Service List** > **Storage** > **Object Storage Service**.

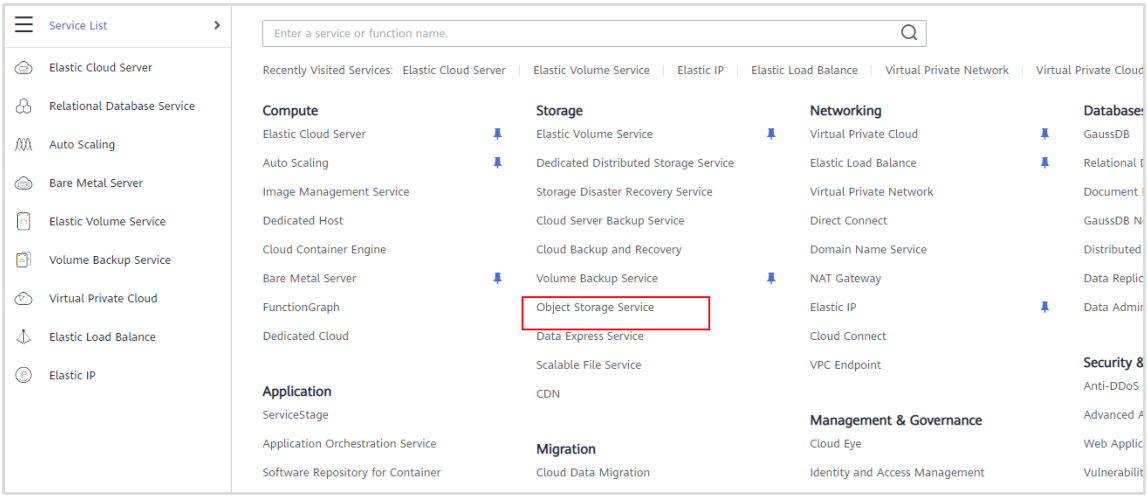


Figure 4-57 Accessing OBS Console

Step 2 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+

Step 3 Decompress the downloaded software package and install it.

Step 4 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.

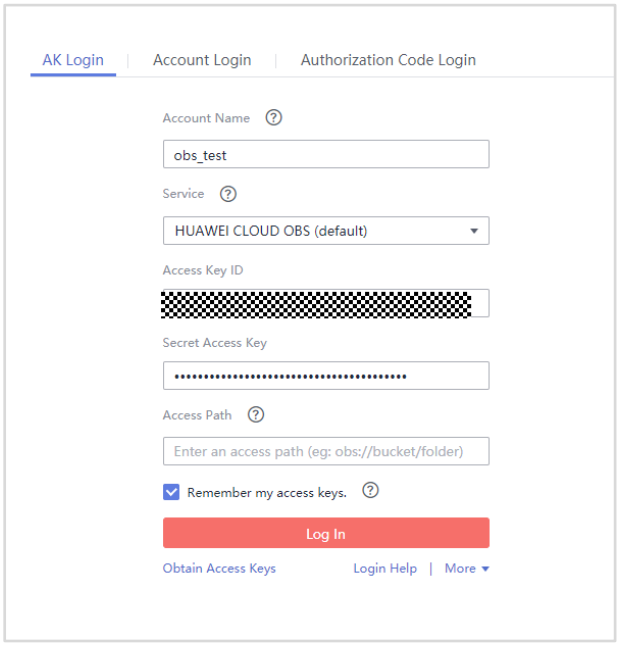


Figure 4-59 Logging in to OBS Browser+

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.

4.2.2.2.3 Creating a Bucket

Step 1 In the upper left corner of OBS Browser+ homepage, click **Create Bucket**.

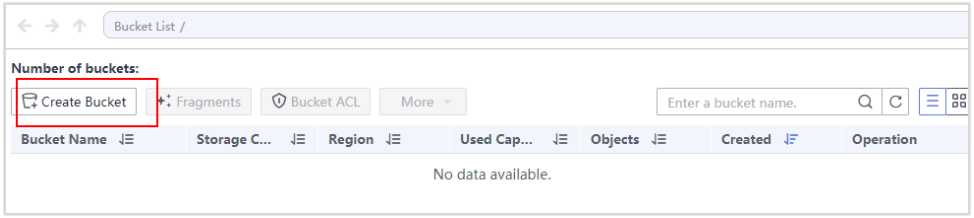


Figure 4-60 Creating a bucket

Step 2 In the **Create Bucket** dialog box, configure the following parameters:

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

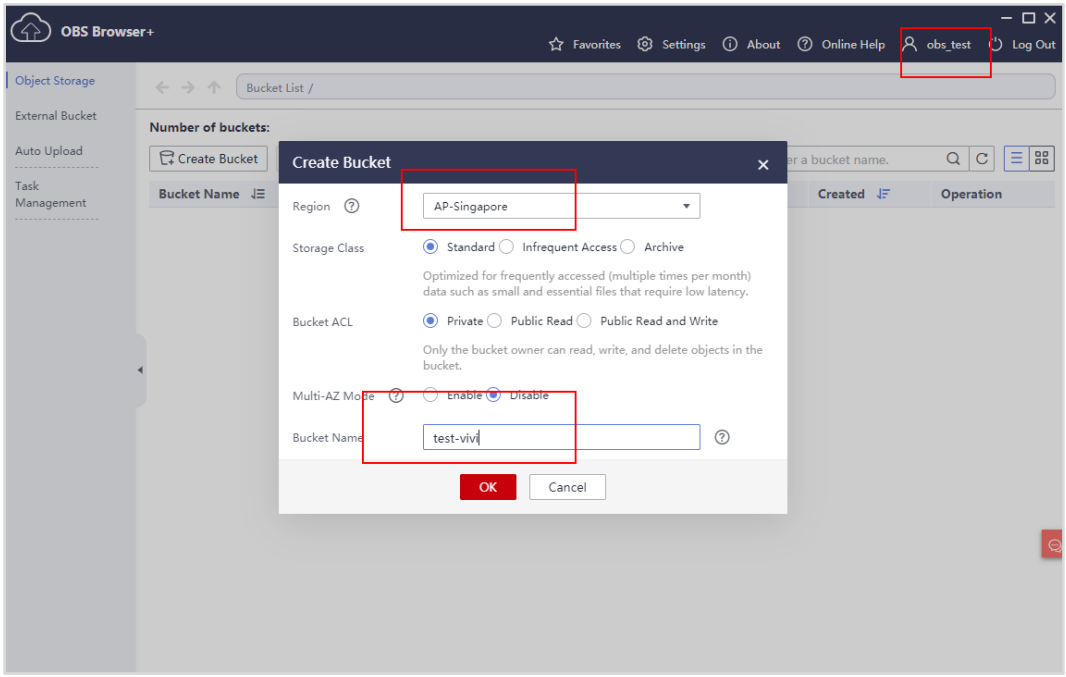


Figure 4-61 Configuring bucket information

Step 3 Click **OK**. A dialog box is displayed, indicating whether the bucket is created.

4.2.2.3 Uploading a File or Folder

Step 1 Click the name of the created bucket to go to the object list page.

Step 2 Click **Upload**.

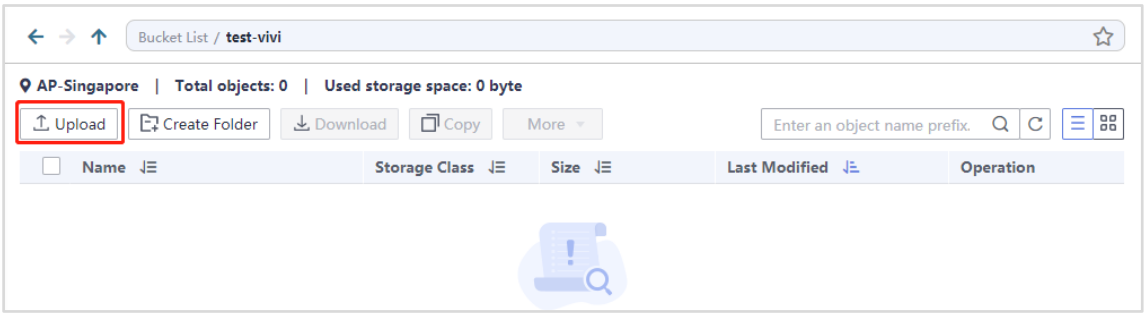


Figure 4-62 Uploading a file

Step 3 In the **Upload** dialog box, click **File**.

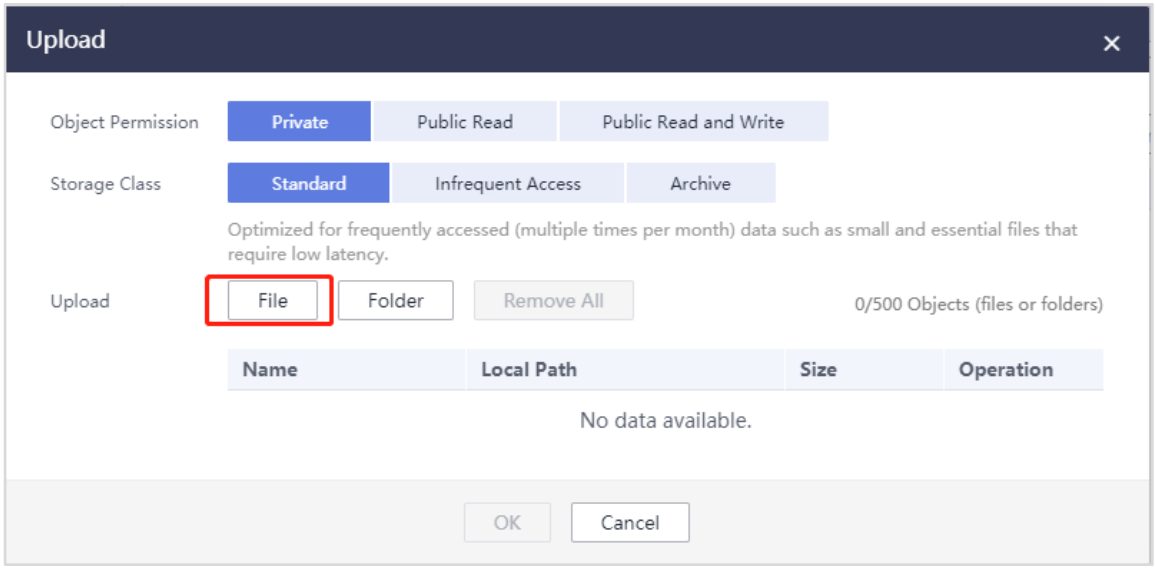


Figure 4-63 Adding a file

Step 4 Select the files to be uploaded and click **OK**.

Step 5 (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.

Step 6 View the uploaded file or folder in the list.

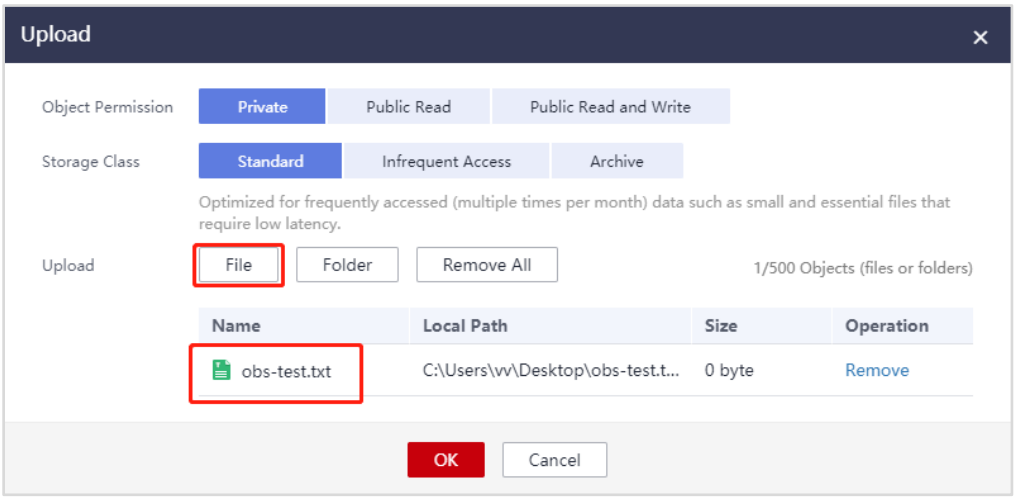


Figure 4-64 Viewing the uploaded file

4.2.2.4 Downloading a File or Folder

Step 1 In the object list, select the file or folder to be downloaded and click **Download**.

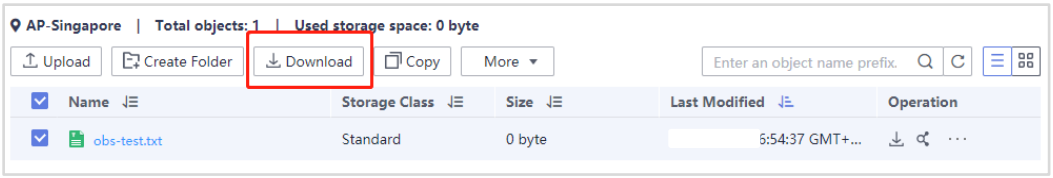


Figure 4-65 Downloading a file

Step 2 In the dialog box, select a path for saving the downloaded file on your local PC.

Step 3 (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

Step 1 In the object list, select the file or folder to be deleted, and choose **More** > **Delete** in the **Operation** column.

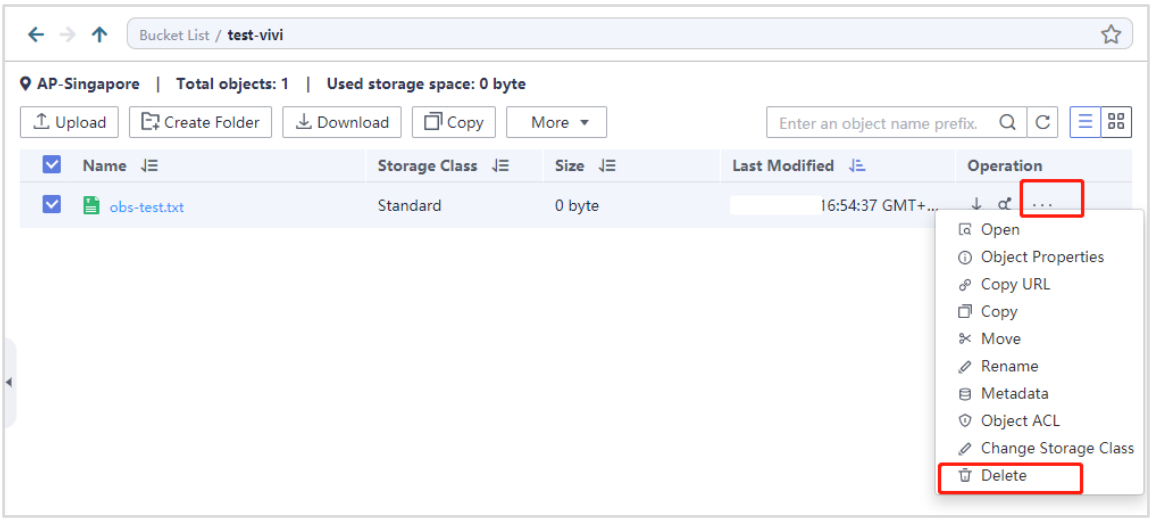


Figure 4-66 Deleting a file

Step 2 In the **Delete Object** dialog box, click **Yes**.

Step 3 (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

Step 1 Log in to OBS Console and find the created bucket from the bucket list.

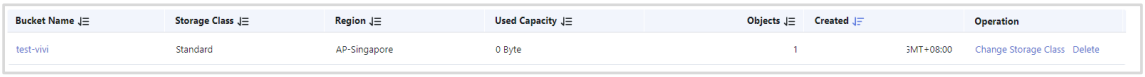


Figure 4-67 Logging in to OBS Console

Step 2 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.

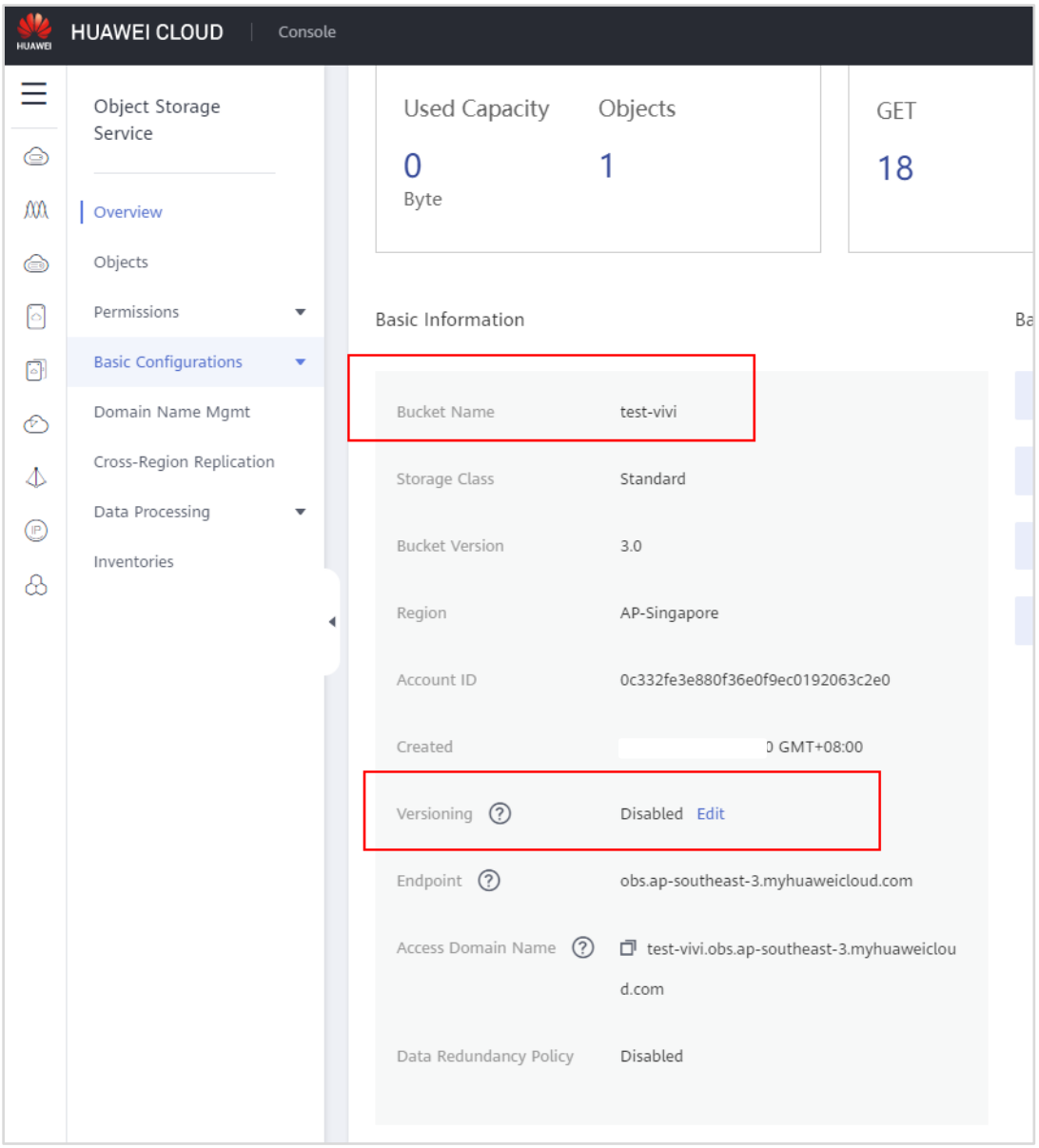


Figure 4-68 Viewing versioning status

Step 3 Click **Edit** next to **Versioning**. In the **Versioning** dialog box, select **Enable** and then **OK**.

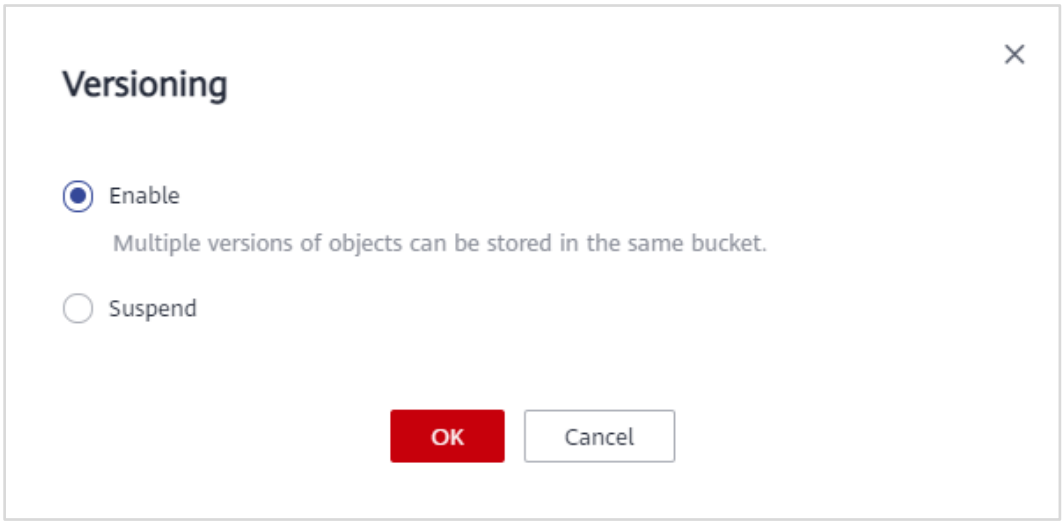


Figure 4-69 Enabling versioning

Step 4 In the navigation pane, choose **Objects**. On the displayed page, click **Upload Object** to upload two objects with the same name.

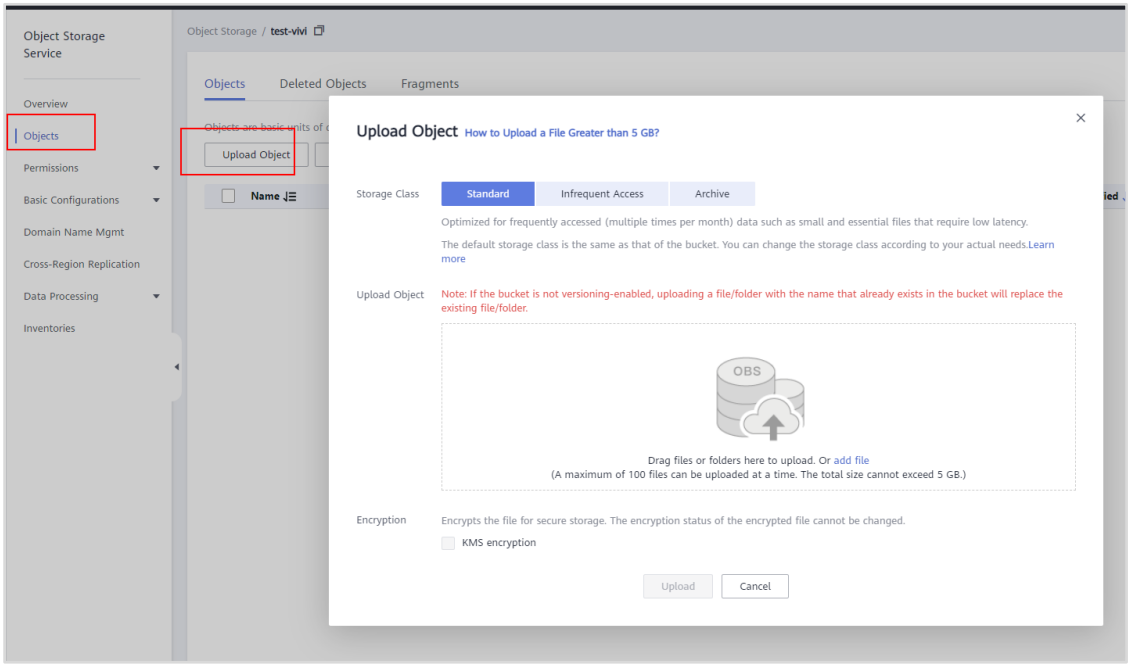


Figure 4-70 Uploading objects

Step 5 Click the name of the uploaded object to view its properties.

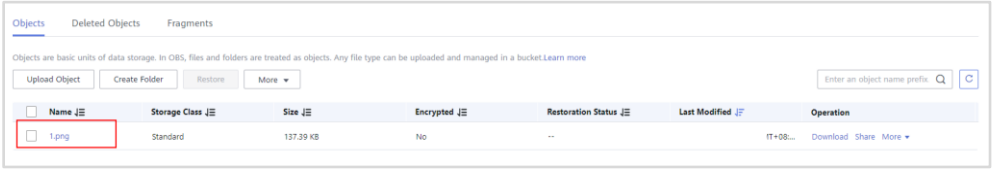


Figure 4-71 Viewing the uploaded objects

Step 6 On the **Versions** page, view the different object versions.

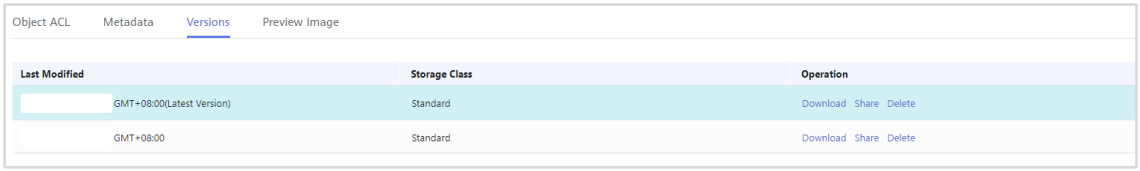


Figure 4-72 Viewing object versions

Step 7 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.

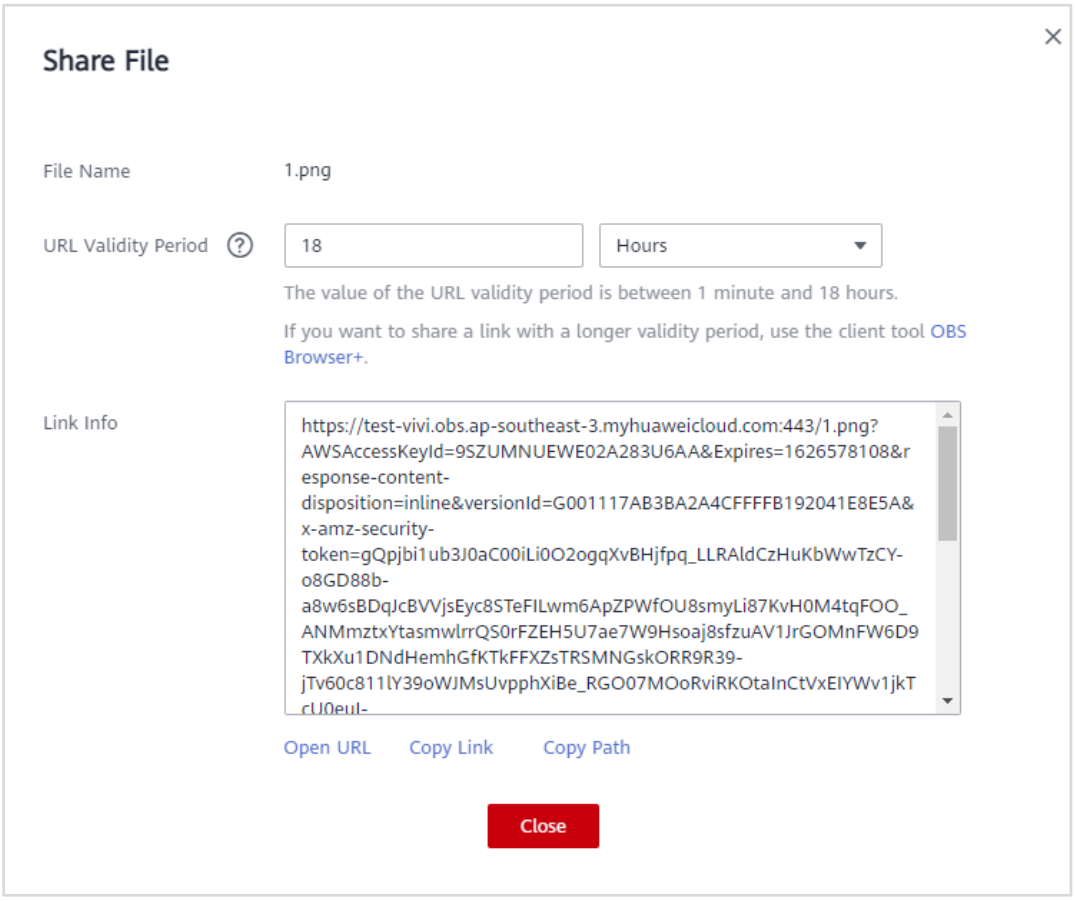


Figure 4-73 Sharing a file

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.

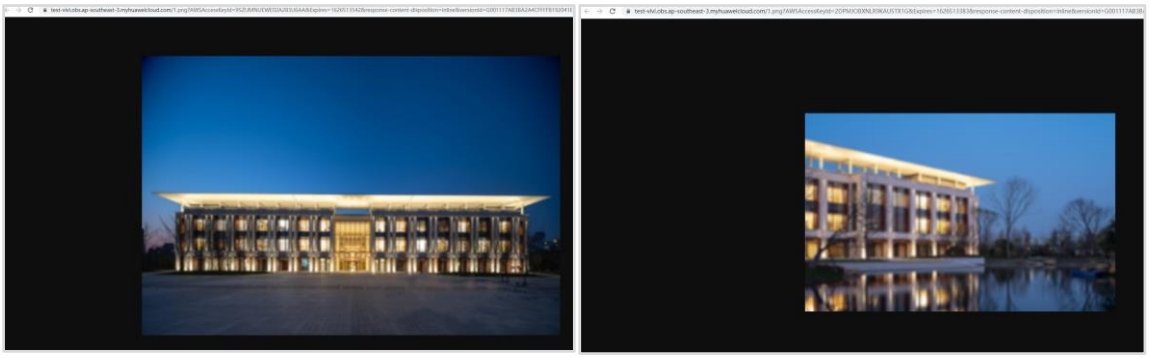


Figure 4-74 Viewing shared files

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.

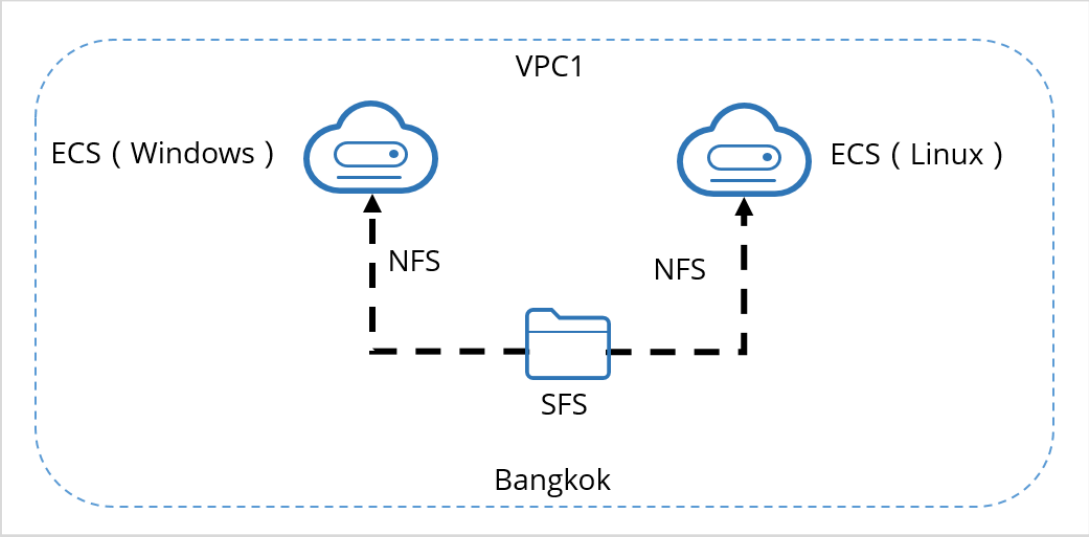


Figure 4-75 Topology

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

4.3.2.1.1 Prerequisites

- A VPC **vpc-mp** has been created.
- A Linux ECS **ecs-linux** running CentOS 7.6 has been purchased. 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 has been purchased. An EIP has been bound to the ECS, and the ECS locates in VPC **vpc-mp**.

4.3.2.1.2 Creating an SFS File System

Step 1 Log in to the HUAWEI CLOUD console and choose **Scalable File Service** in the service list.

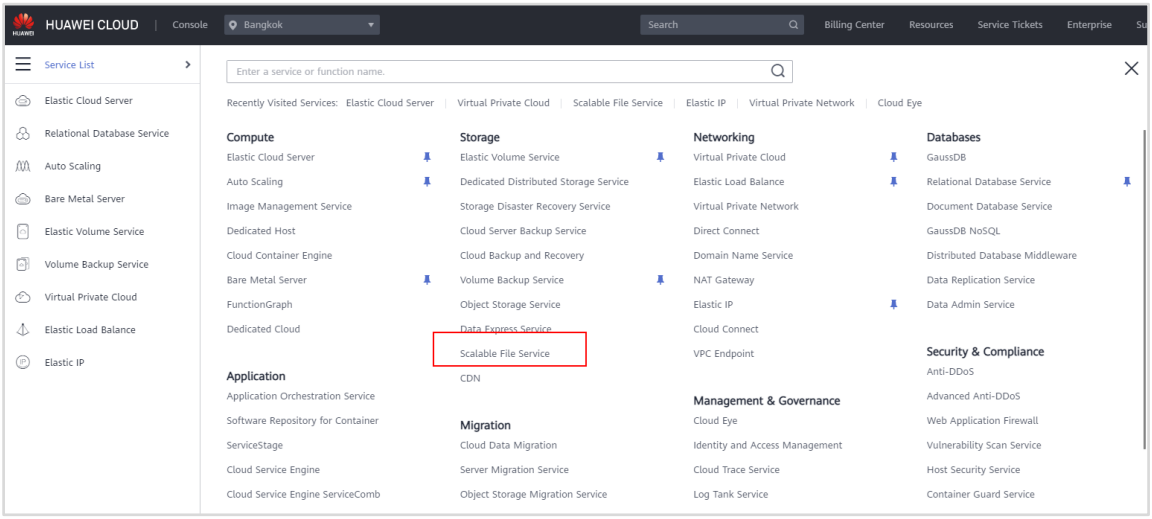


Figure 4-76 Opening the SFS console

Step 2 Click **Create File System**.

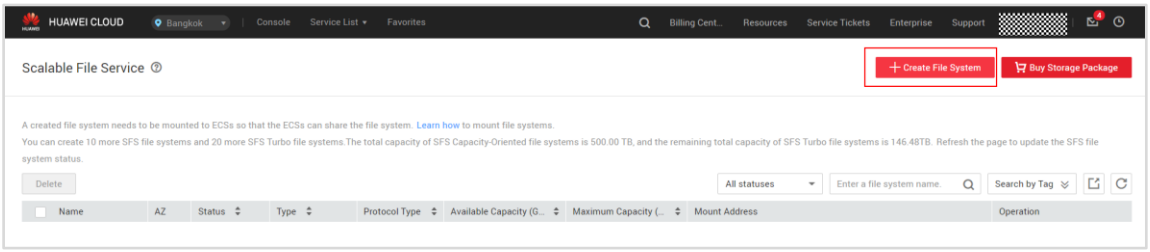


Figure 4-77 Create File System

Step 3 On the displayed page, set the name, file system type, and VPC for the file system you are creating.

- **File System Type**: **SFS**
- **Region**: **AP-Bangkok**
- **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.

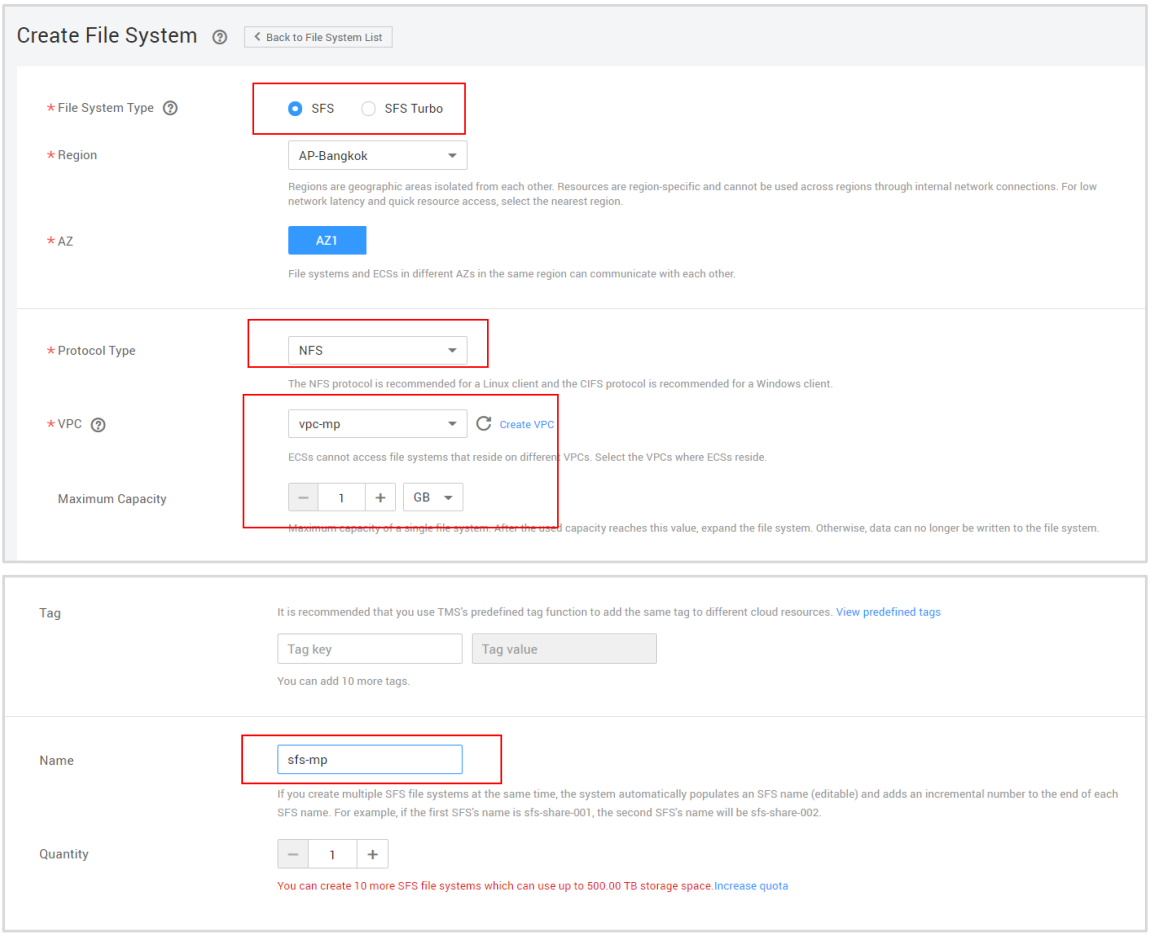


Figure 4-78 Setting file system parameters

Step 4 Click **Next**.

Step 5 On the **Details** page, confirm the configuration and click **Submit**.

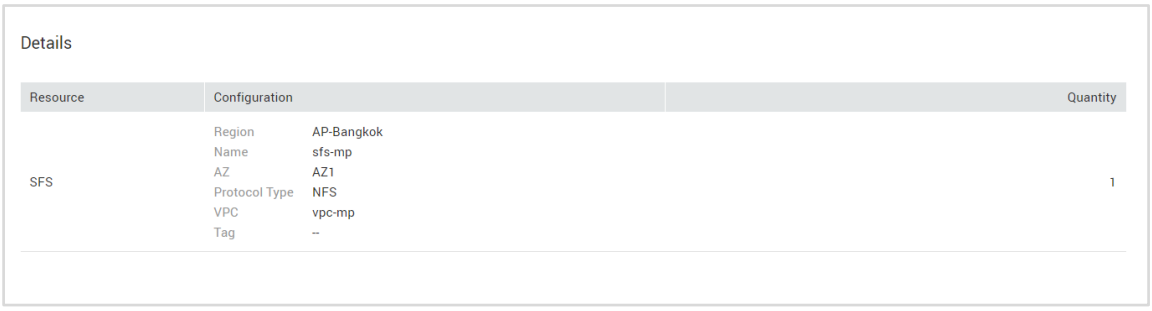


Figure 4-79 Confirming parameter settings

Step 6 A message is displayed indicating that the request has been submitted.

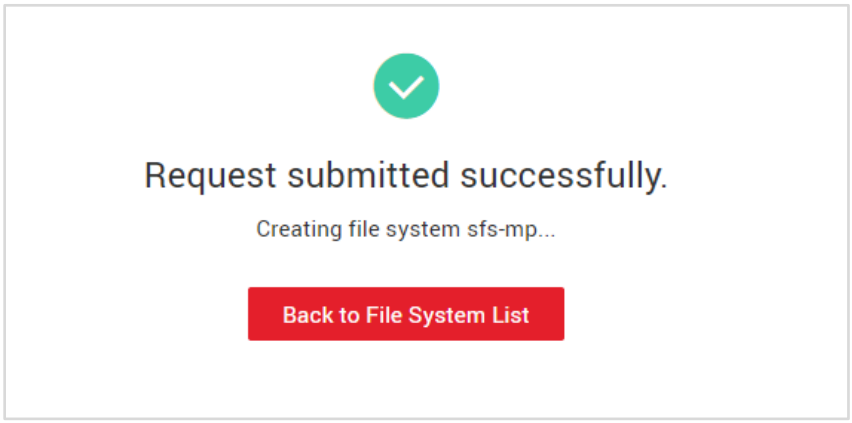


Figure 4-80 File system created

Step 7 Go back to the SFS console and view the result.

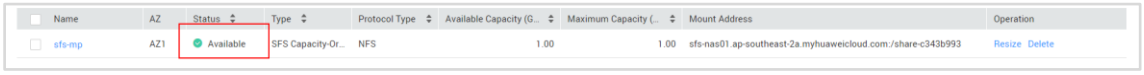


Figure 4-81 Viewing the file system

4.3.2.2 Mounting an SFS File System to a Linux ECS

4.3.2.2.1 Procedure

Step 1 Go to the ECS console. Locate the row that contains the purchased ECS and click **Remote Login**.

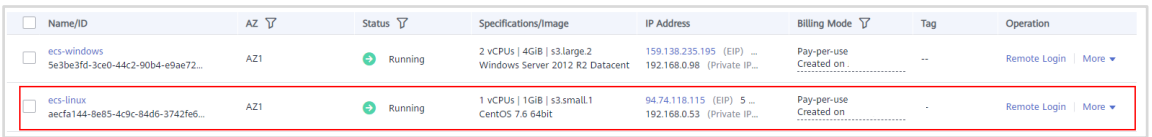


Figure 4-82 Remotely logging in to the ECS

Step 2 Log in the ECS as user **root**.

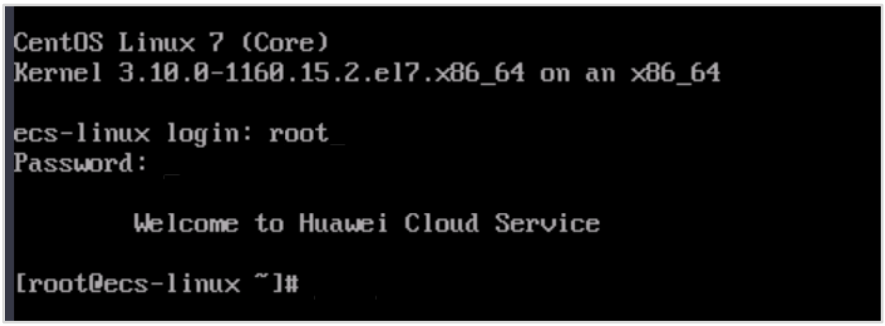


Figure 4-83 Logging in to Linux

Step 3 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
```

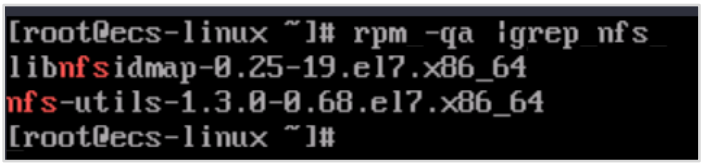


Figure 4-84 Checking whether NFS software package is installed

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

Step 4 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
```

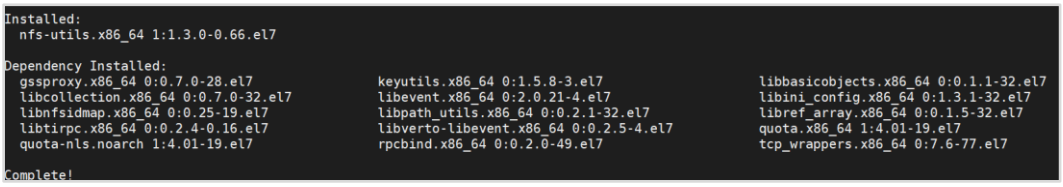


Figure 4-85 Installing the NFS software package

- In Debian or Ubuntu, run the following command:

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

- In OpenSUSE, run the following command:

```
zypper install nfs-client
```

Step 5 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.

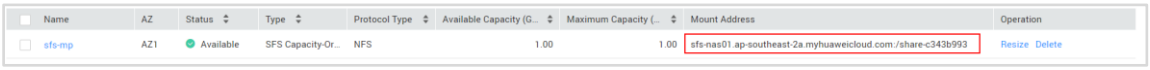


Figure 4-87 Viewing the mount address

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

Step 6 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

Step 7 Run the **mkdir** */local path* command to create a local directory for mounting the file system.

```
mkdir /localfolder
```

Step 8 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

Step 9 Run the following command to view the mounted file system:

```
mount -l
```

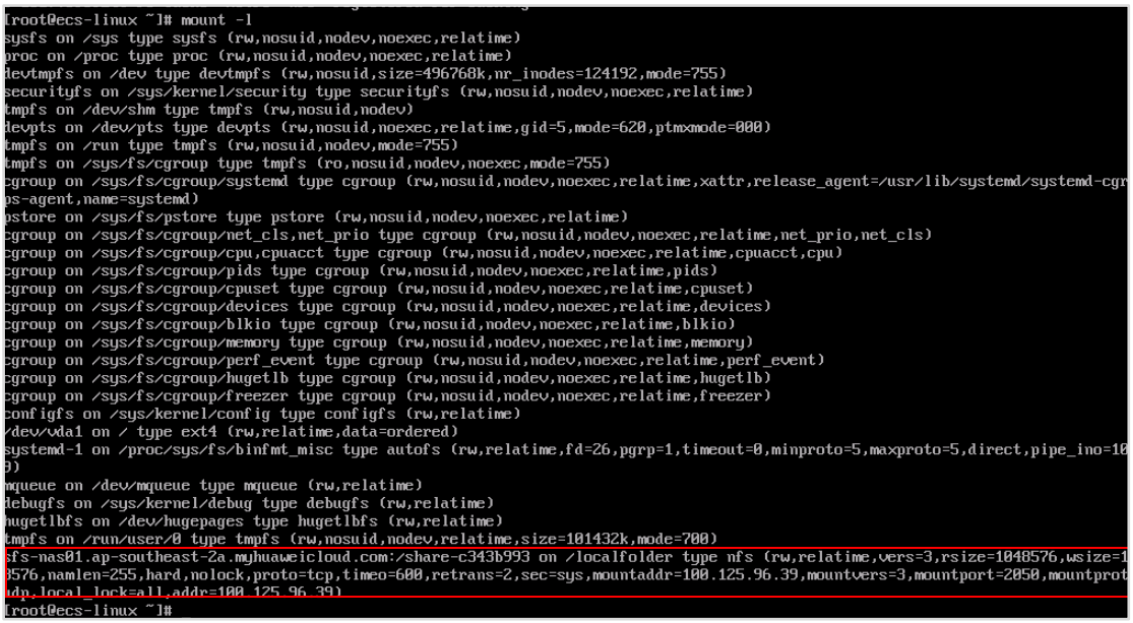


Figure 4-90 Viewing the mounted file system

Step 10 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 0 0
```

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

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

Step 11 Run the following command to view the changes of **fstab**:

```
cat /etc/fstab
```

Figure 4-91 Setting automatic mounting

Step 12 Restart the ECS.

```
reboot
```

Step 13 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,wsize=1
0576,namlen=255,hard,nolock,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=100.125.96.37,mountvers=3,mountport=2050,mountprot
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

Step 14 Create file **new**.

```
cd /localfolder
vim new
```

Step 15 Press **i** to enter editing mode. Enter **Hello HuaweiCloud SFS**, press **Esc**, and enter **:wq** to exit editing mode and save the change.

Figure 4-93 Creating the test file

Step 16 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

4.3.2.3.1 Logging In to a Windows ECS

Step 1 Log in to the ECS console. Locate the row that contains the purchased Windows ECS and click **Remote Login**.

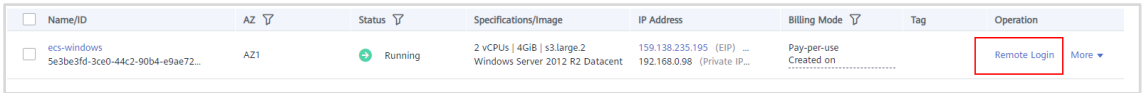


Figure 4-95 Viewing the Windows ECS

4.3.2.3.2 Installing the NFS Client

Step 1 Open **Server Manager** by clicking the icon in the lower left corner.

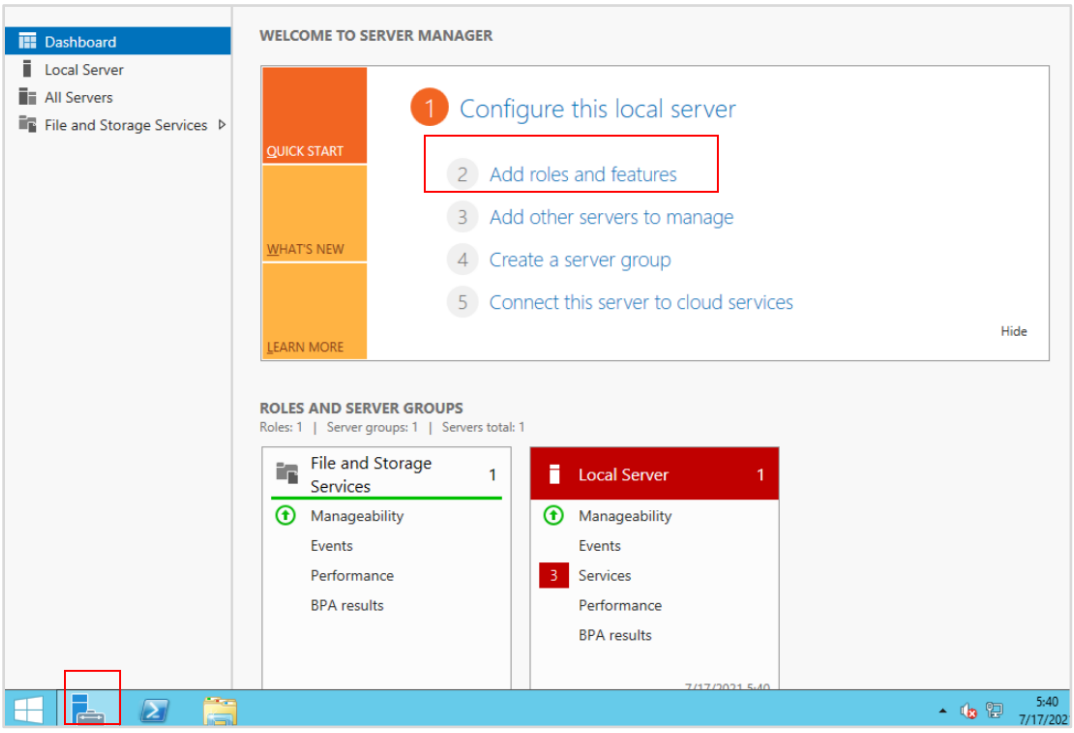


Figure 4-96 Opening Server Manager

Step 2 Click **Add Roles and Features** and click **Next** for three consecutive times to go to the **Server Roles** page.

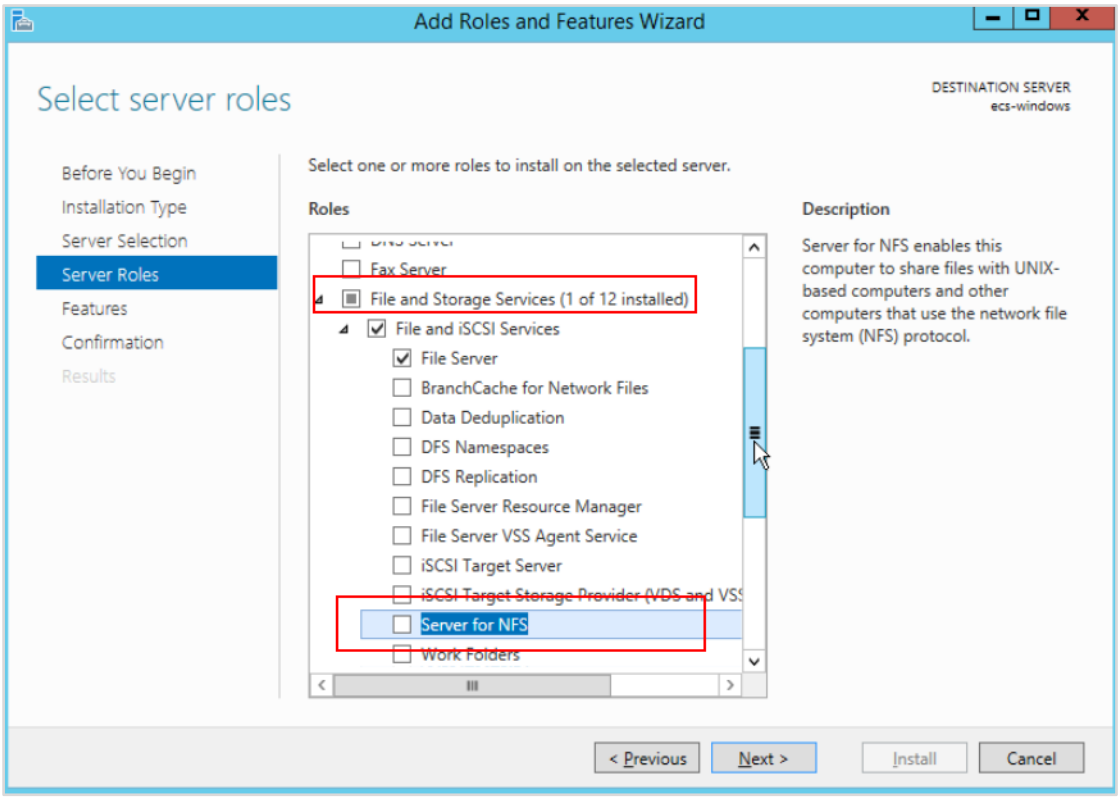


Figure 4-97 Selecting the server role

Step 3 Under File and Storage Services, click **Server for NFS**. In the displayed window, click **Add Features**.

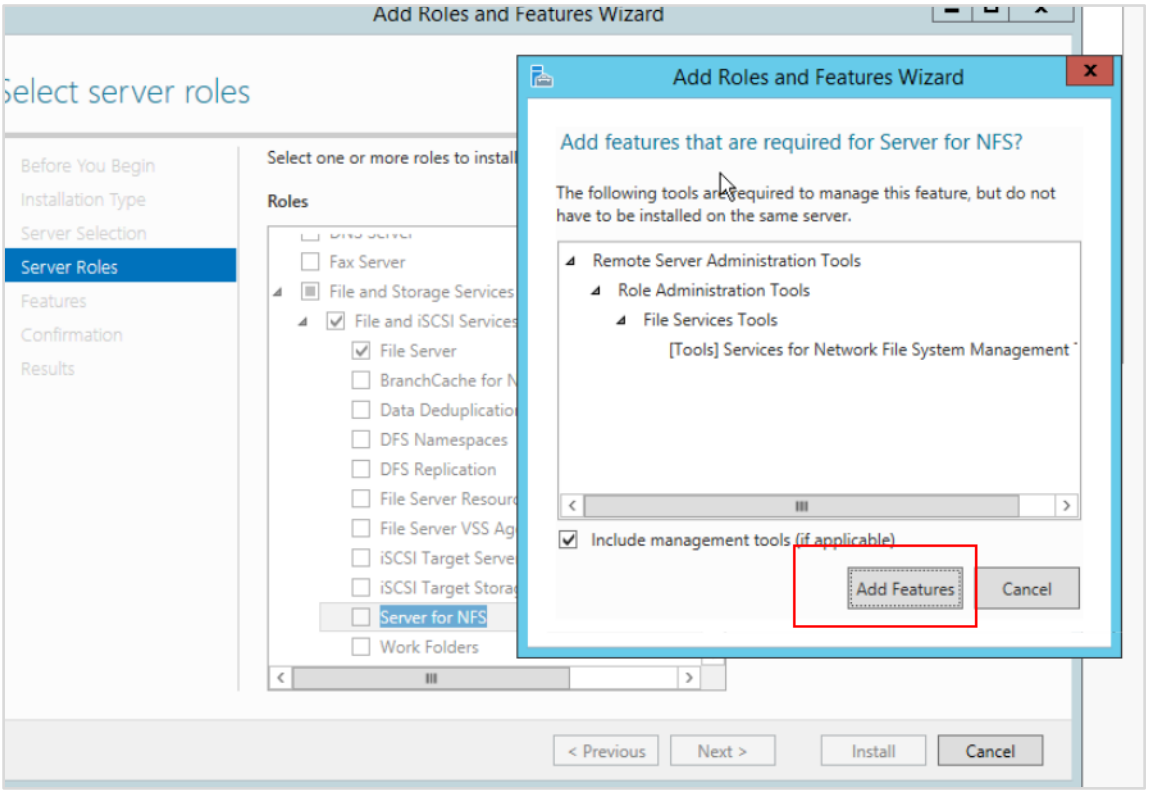


Figure 4-98 Clicking Server for NFS

Step 4 Click **Next**. On the **Features** page, click **Client for NFS**.

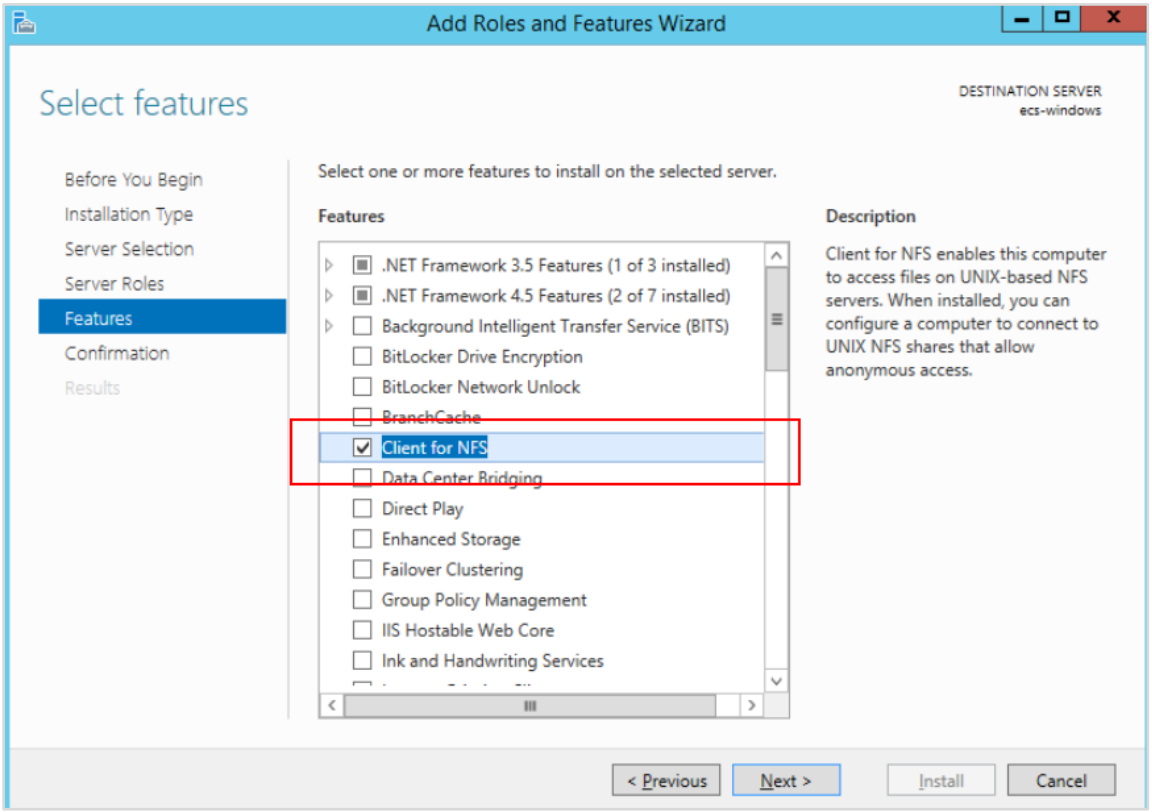


Figure 4-99 Selecting Client for NFS

Step 5 Click **Next** to go to the **Confirmation** page.

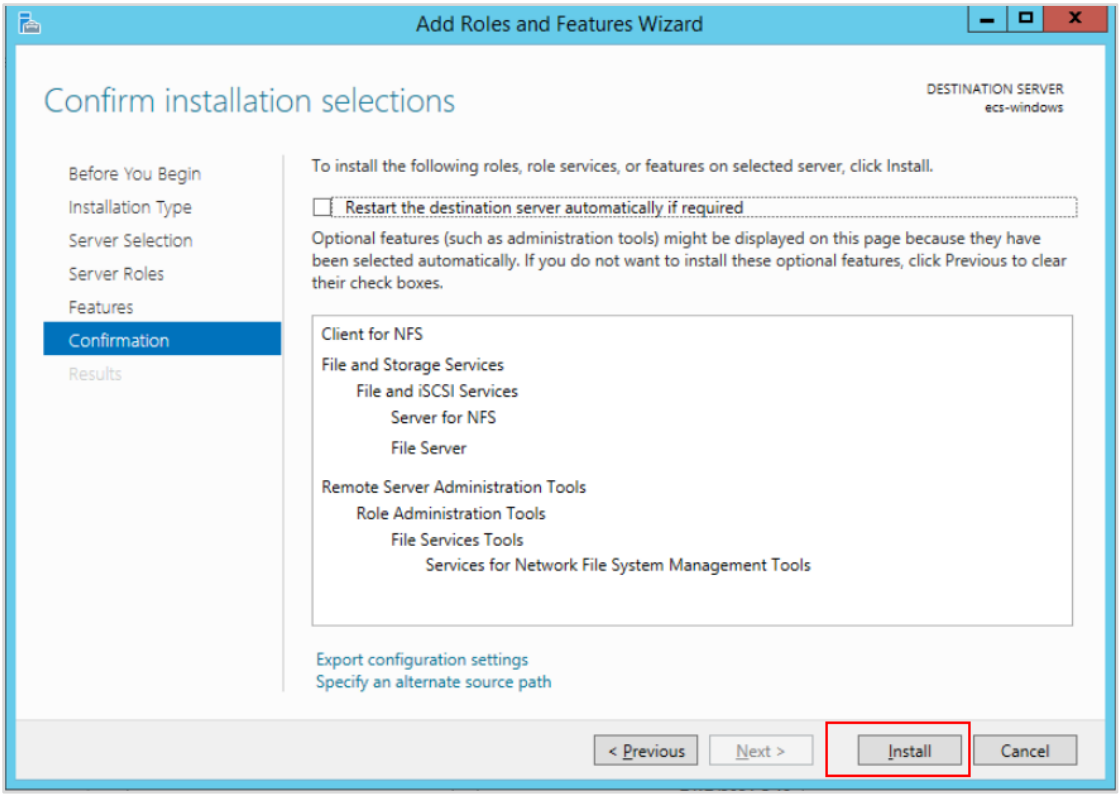


Figure 4-100 Confirmation

Step 6 Click **Install**.

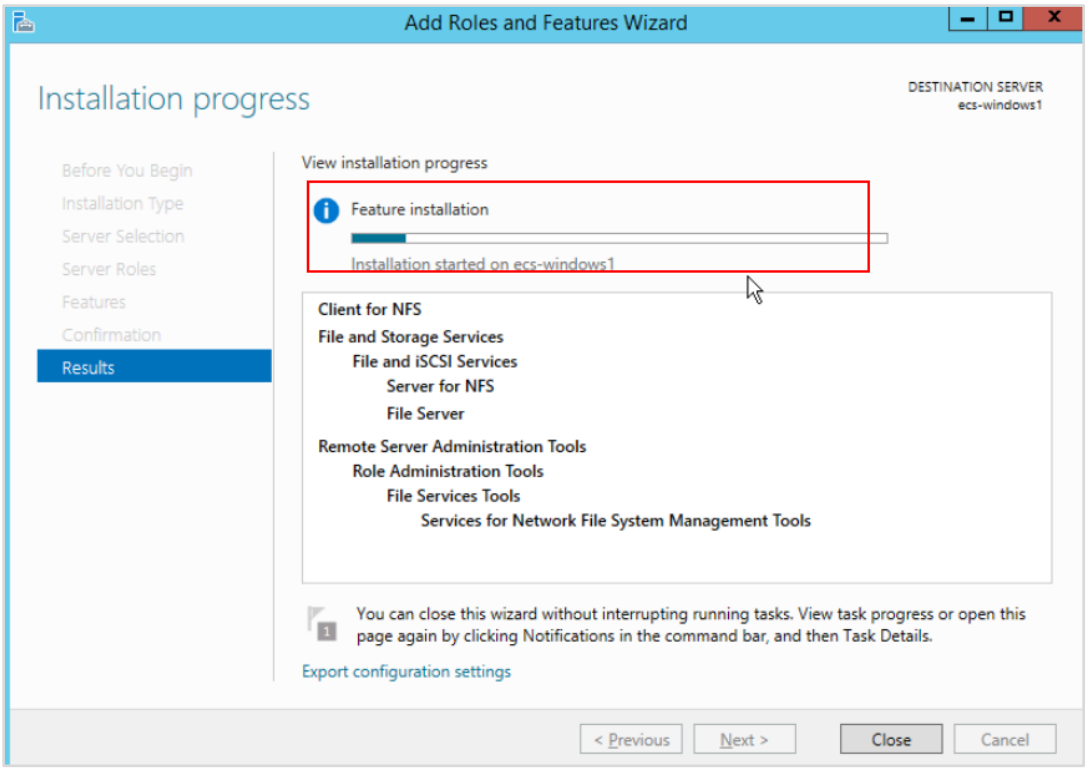


Figure 4-101 Installing

Step 7 After the installation is complete, restart the client and log to the ECS again as prompted.

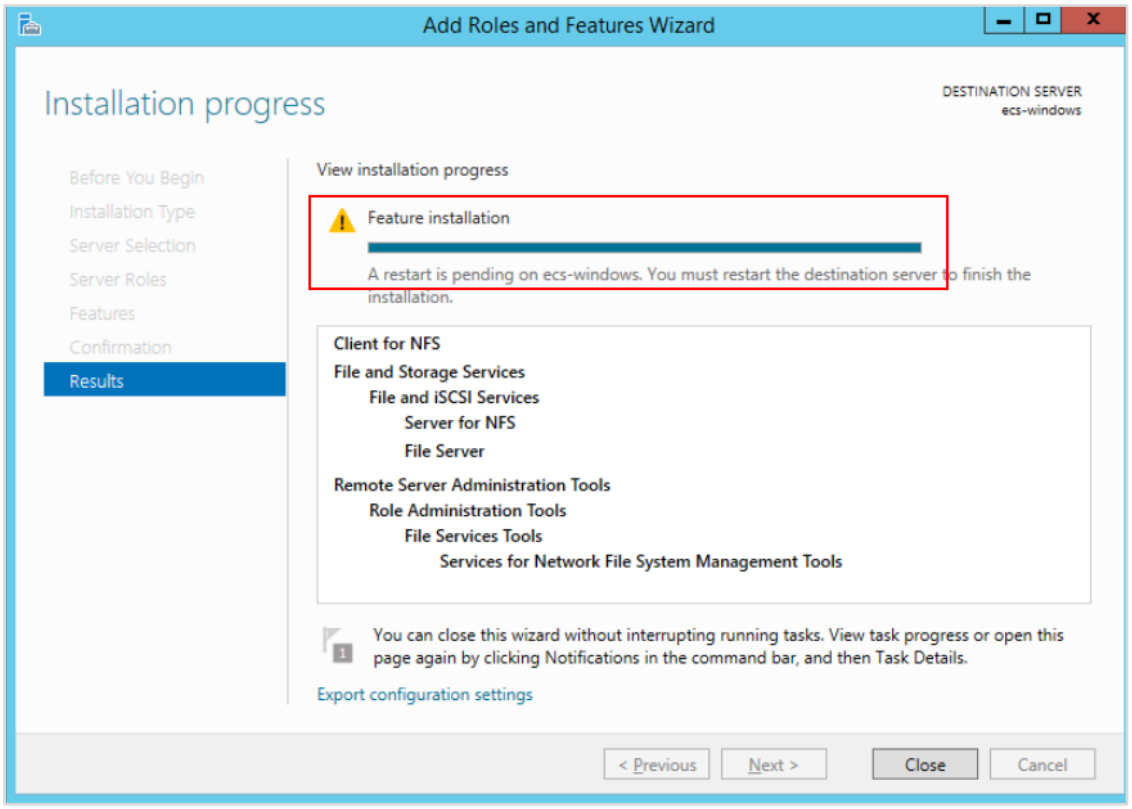


Figure 4-102 Installation completed

4.3.2.3.3 Mounting the File System

Step 1 Open **Control Panel** and choose to view by **category**.

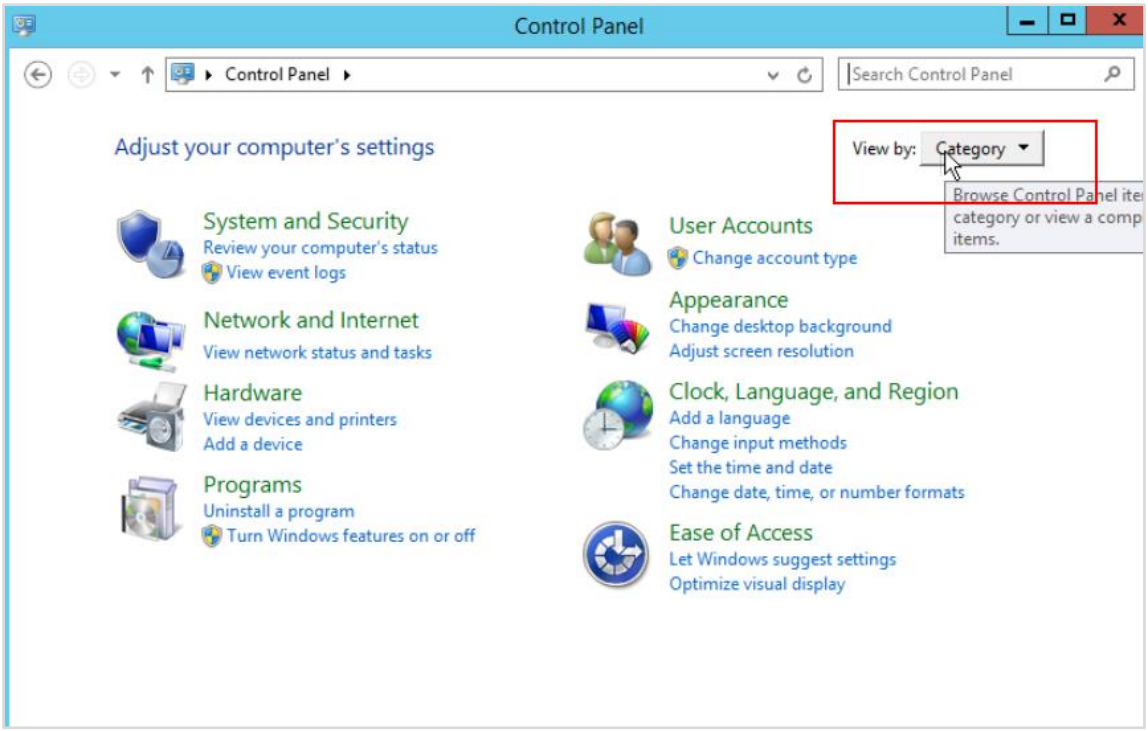


Figure 4-103 Control Panel

Step 2 On the Control Panel, choose **System and Security** > **Administrative Tools** > **Services for Network File System (NFS)**.

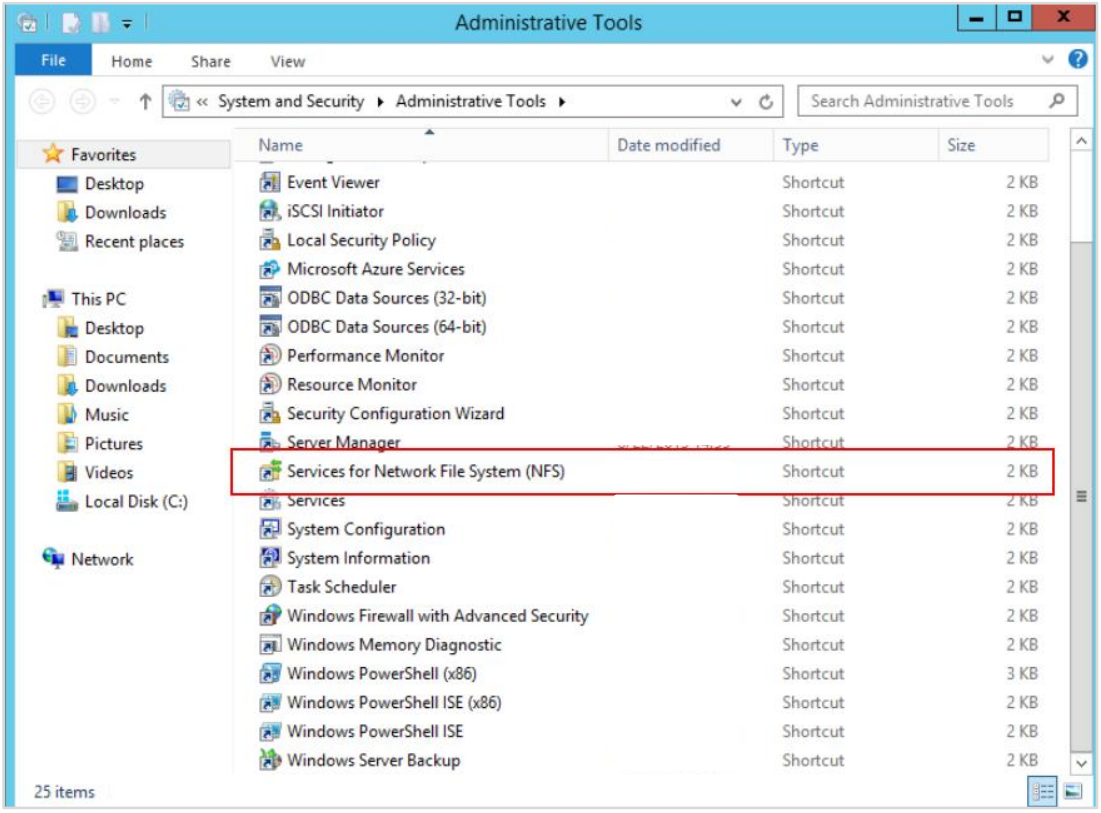


Figure 4-104 Selecting the NFS service

Step 3 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.

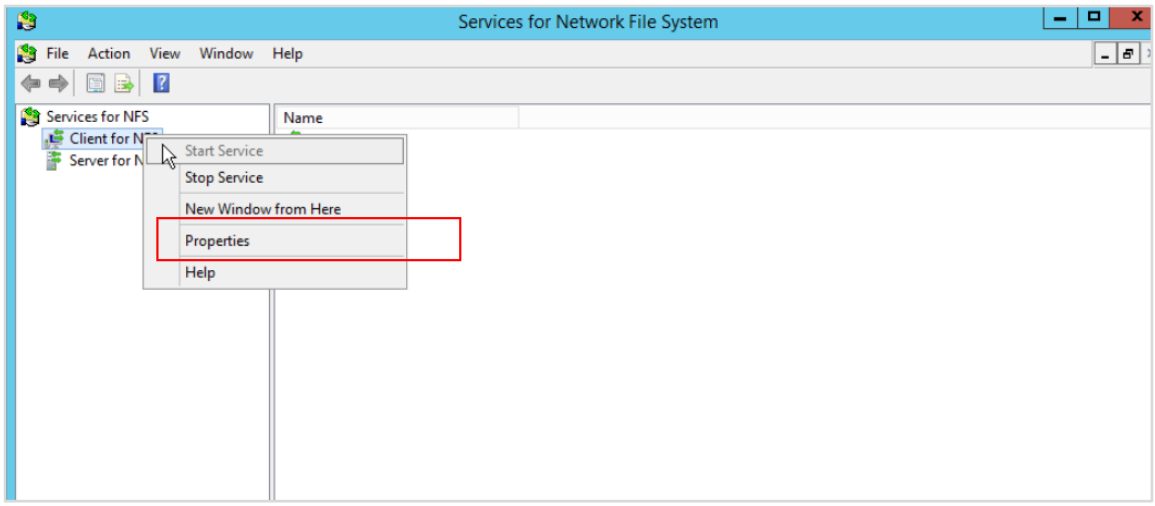


Figure 4-105 Opening Client for NFS Properties

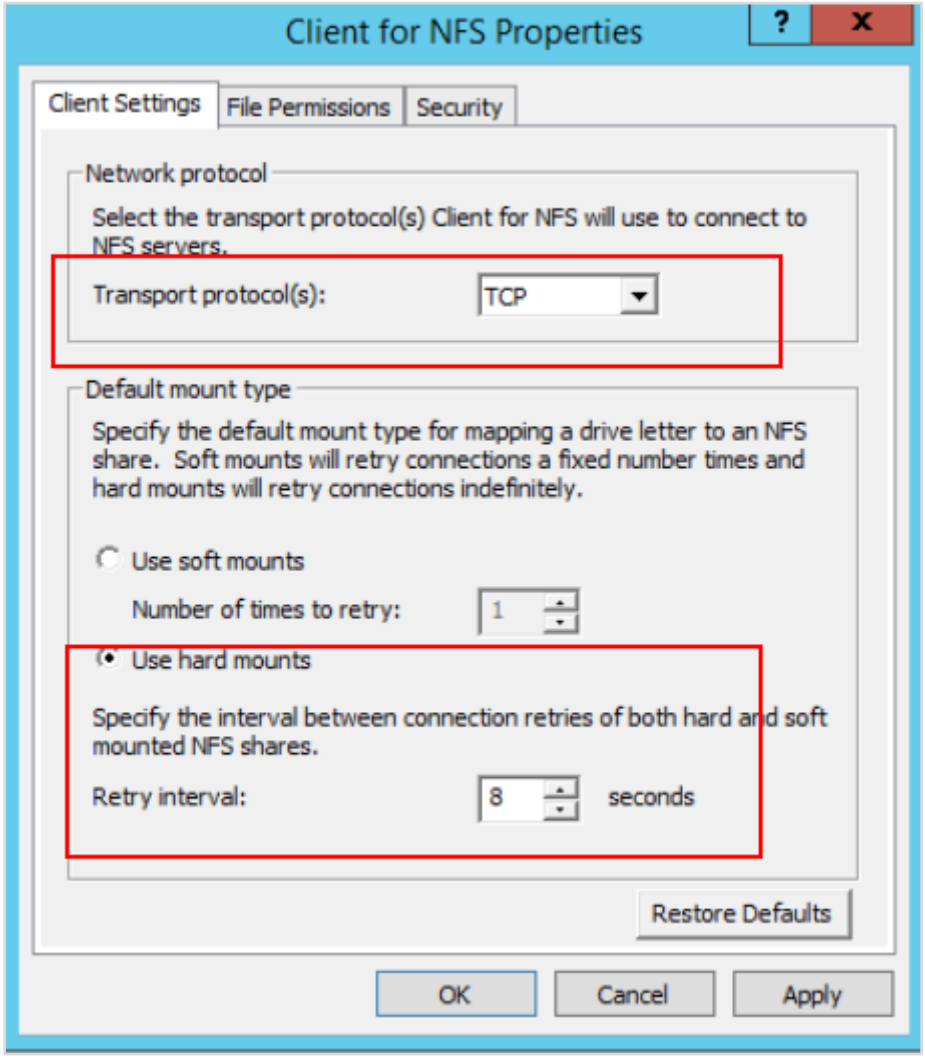


Figure 4-106 Setting properties

Step 4 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.c
om:/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

4.3.2.3.4 Verification

Step 1 On the Windows ECS, open **This PC** to check that the mounted file system is available.

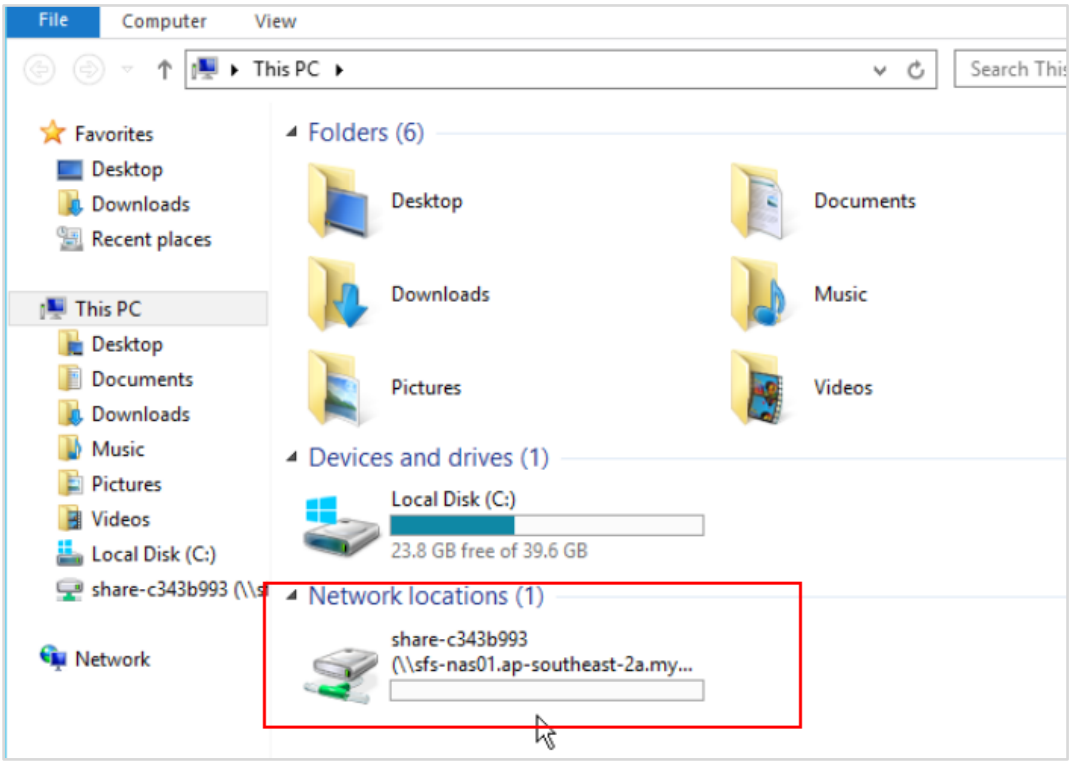


Figure 4-108 SFS file system displayed under Network Locations

Step 2 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.

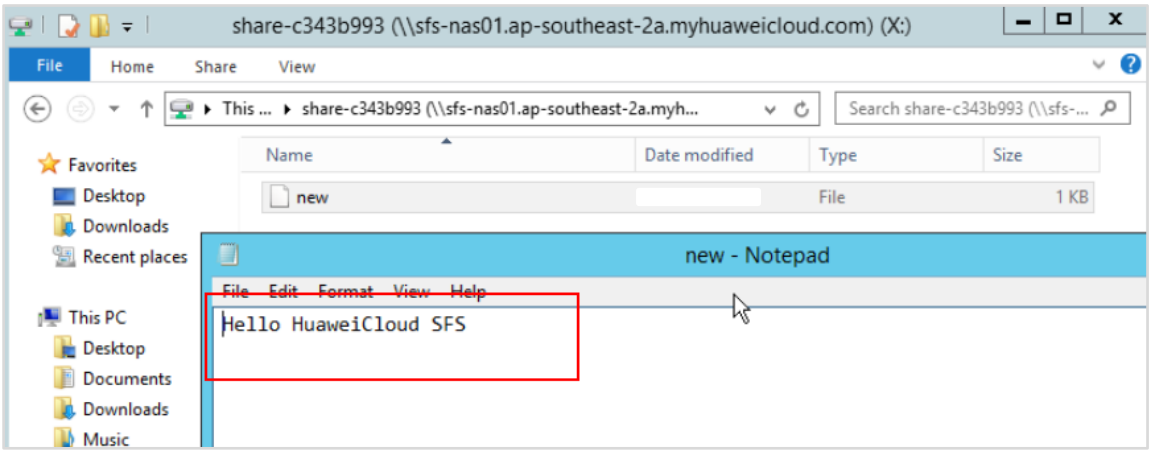


Figure 4-109 Verification succeeded

4.3.3 Deleting Resources

4.3.3.1 Unmounting a File System (Linux)

Step 1 Log in to ECS **ecs-linux** and run the following command to unmount the file system:

```
umount /localfolder
```

Figure 4-110 Unmounting the file system

Step 2 Run the following command to check whether the file system has been unmounted:

```
mount –l
```

4.3.3.2 Unmounting a File System (Windows)

Step 1 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**.

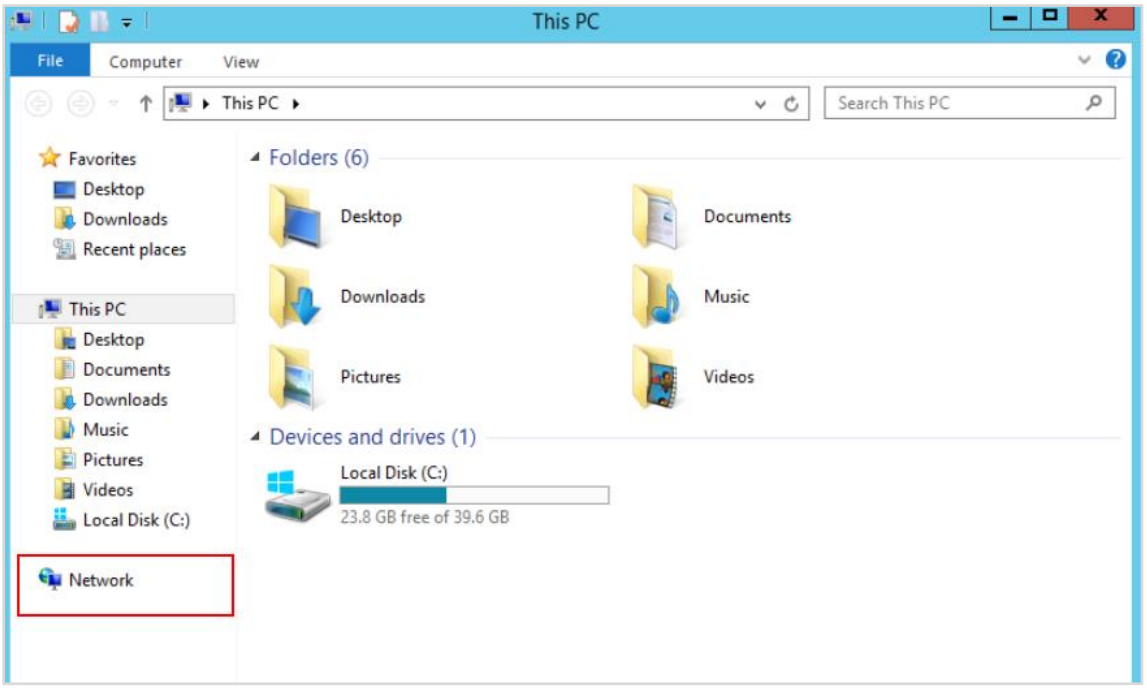


Figure 4-111 File system unmounted

4.3.3.3 Deleting a File System

Step 1 On the SFS console, locate the row that contains the file system and click **Delete** in the **Operation** column.

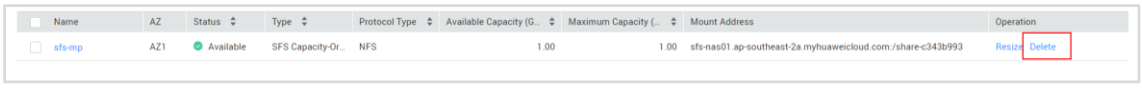


Figure 4-112 Delete File System

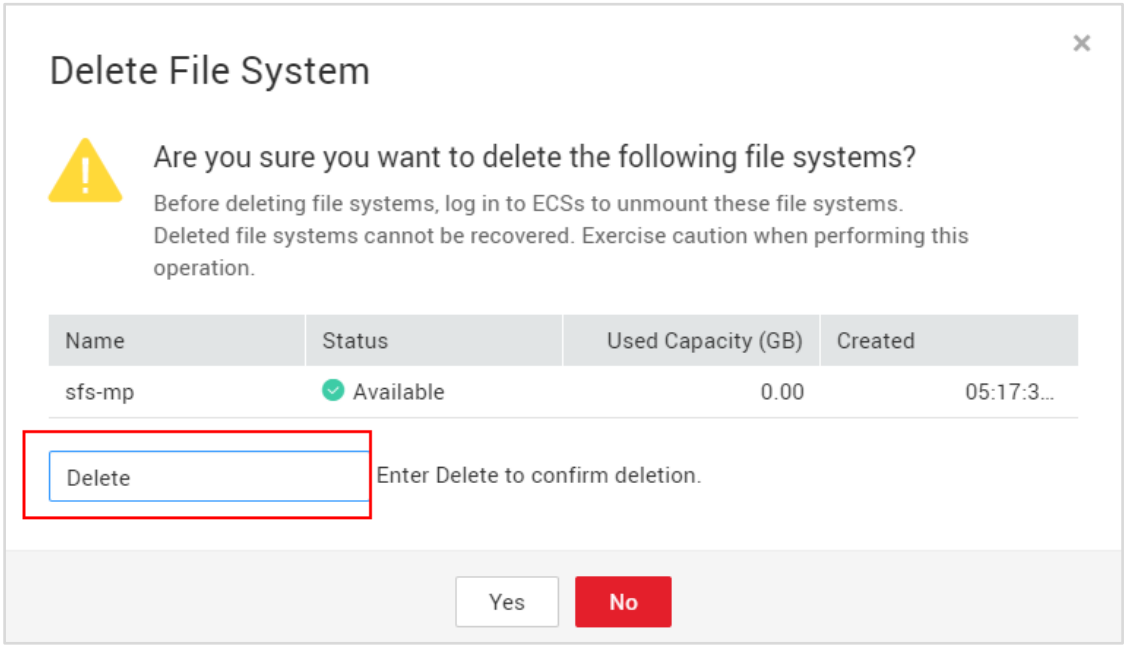


Figure 4-113 Delete File System

4.4 Exercises

1. Buy a Windows ECS and an EVS disk, attach the disk to the ECS, and create a test file on the disk. Try to roll back the disk data from a snapshot.
2. Attach the object storage on the Windows ECS using OBS Browser+ and configure synchronization policy to implement scheduled file synchronization.
3. Now that the file system has been mounted to the Linux ECS. Confirm that automatic mounting has been configured in **/etc/fstab**, and then create an ECS from the private image and verify whether the file system can be automatically mounted on the new ECS and whether files can be shared.

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.

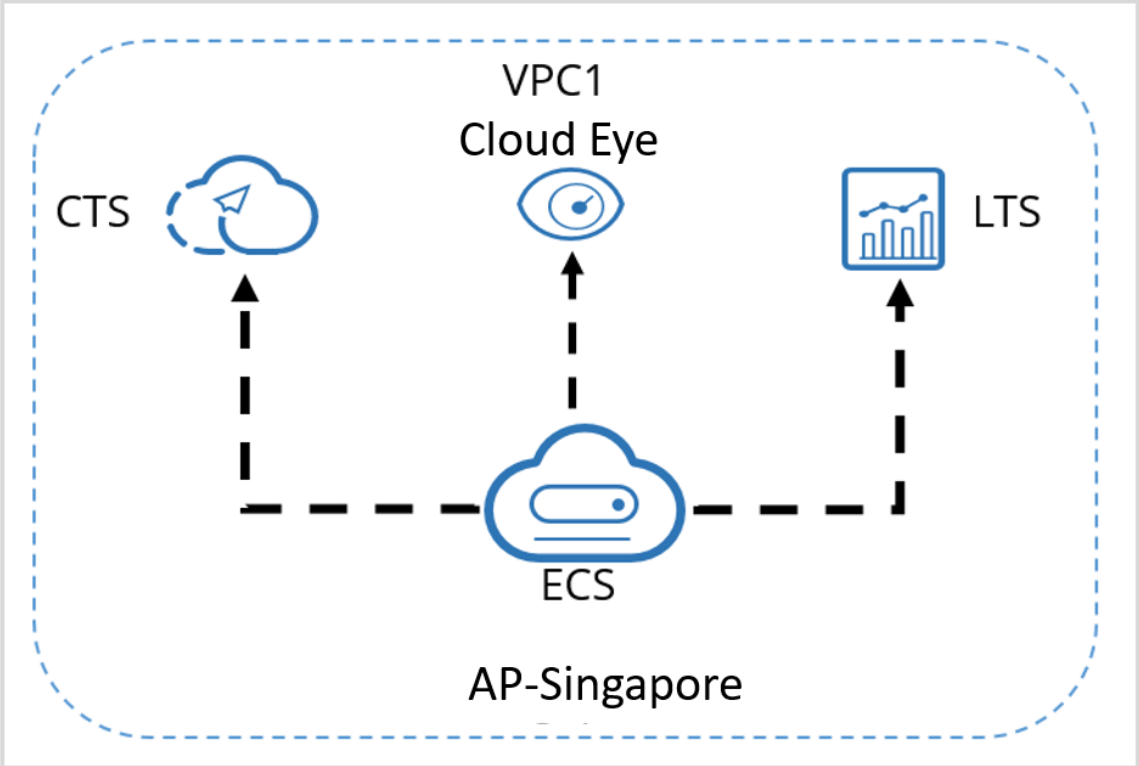


Figure 5-1 Topology

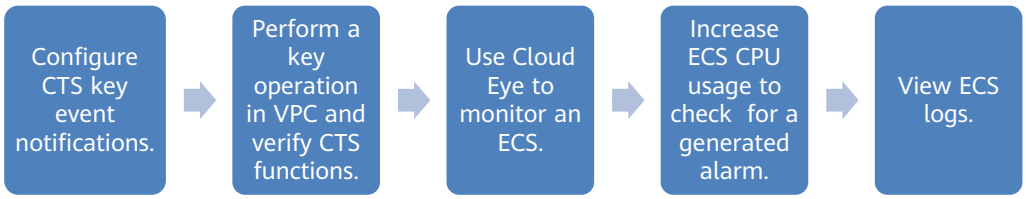
5.1.2 Objectives

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

Step 1 Log in to the management console.

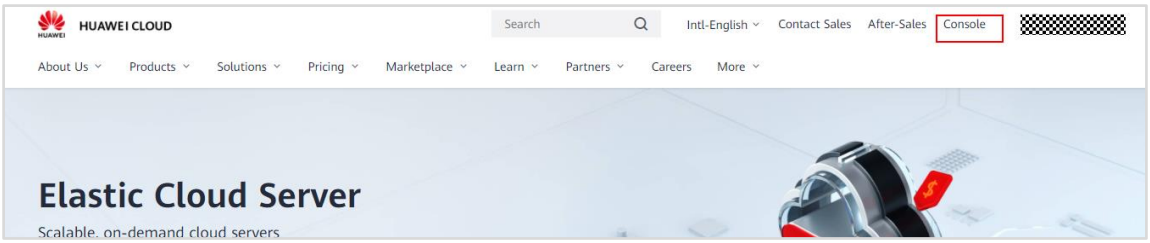


Figure 5-2 Accessing the console

Step 2 Search for **Cloud Trace Service** to access the CTS console.

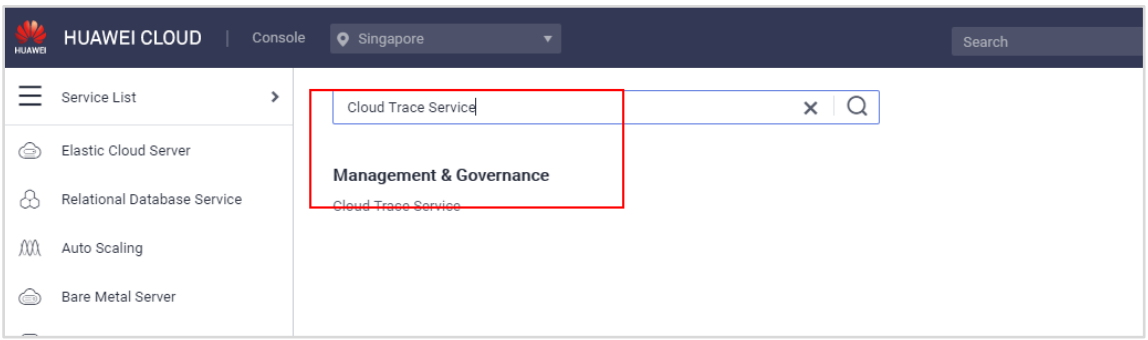
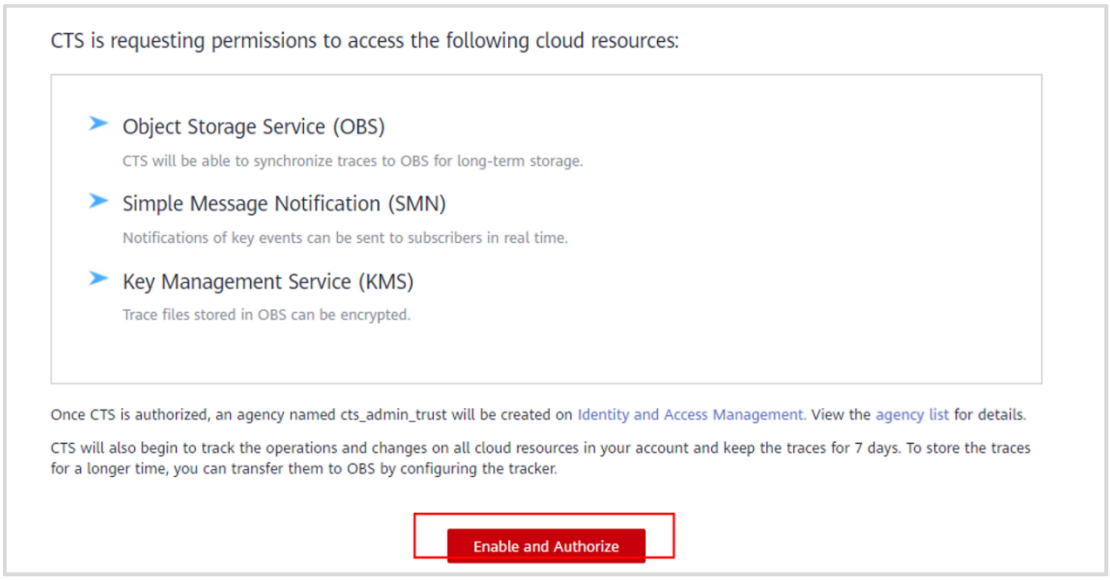


Figure 5-3 Accessing CTS

Step 3 Enable and authorize CTS. The CTS tracker created identifies and associates itself with all cloud services you are using.



Step 4 If the tracker status is **Enabled**, the tracker is running.

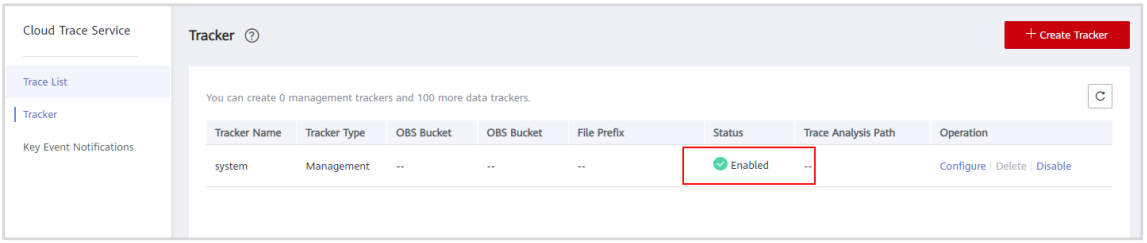


Figure 5-4 Viewing the default tracker

5.2.1.2 Configuring Key Event Notifications

Step 1 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.

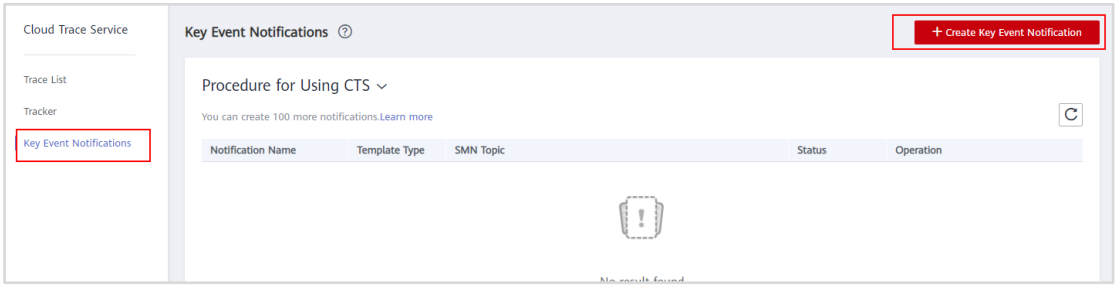


Figure 5-5 Creating a key event notification

Step 2 Configure notification parameters.

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

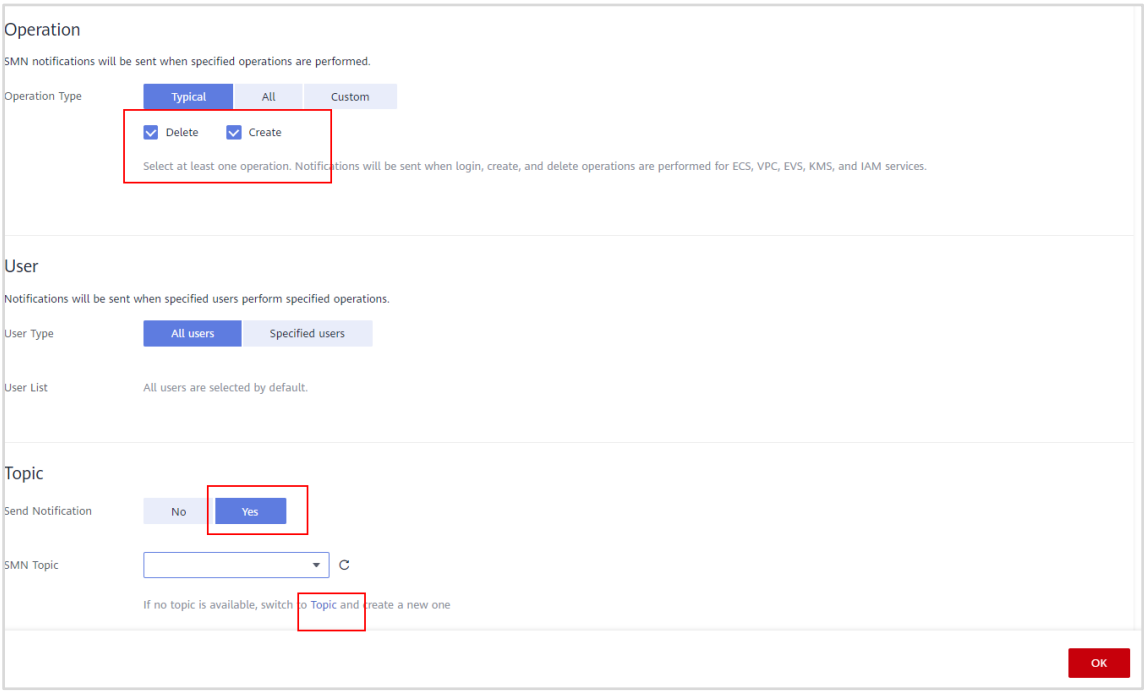


Figure 5-6 Configuring the notification

Step 3 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.

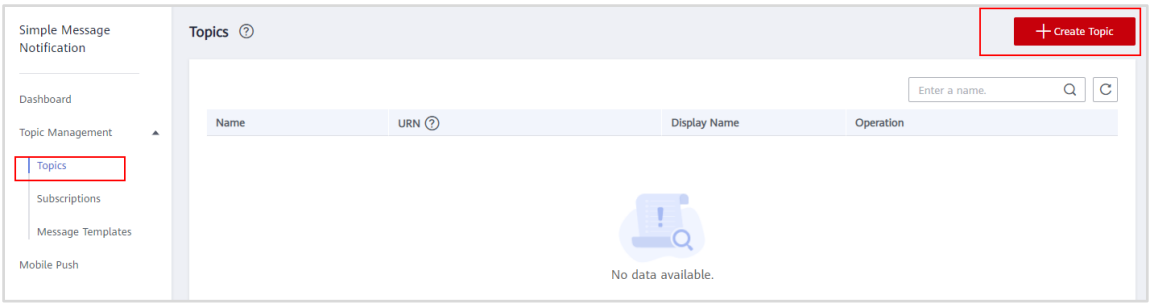


Figure 5-7 Creating a topic

Step 4 Enter a topic name and click **OK**.

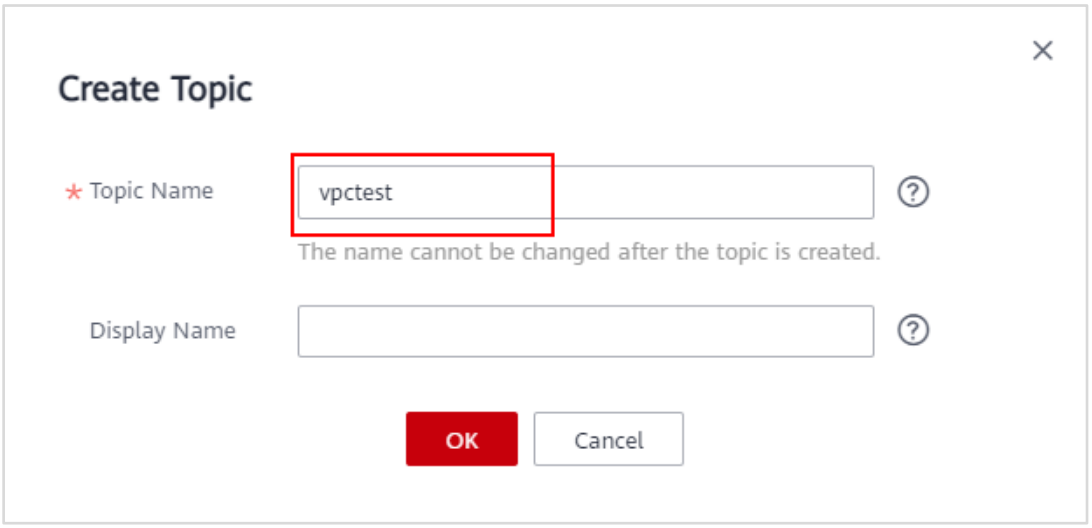


Figure 5-8 Configuring the topic

Step 5 Click **Add Subscription** to add a subscription for the created topic.

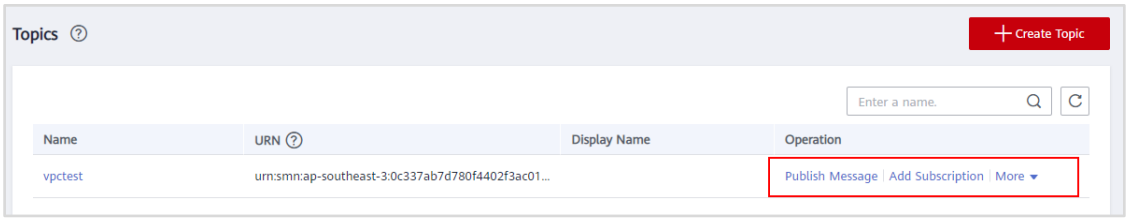


Figure 5-9 Adding a subscription

Step 6 Select **SMS** for **Protocol**, enter your mobile number, and click **OK**.

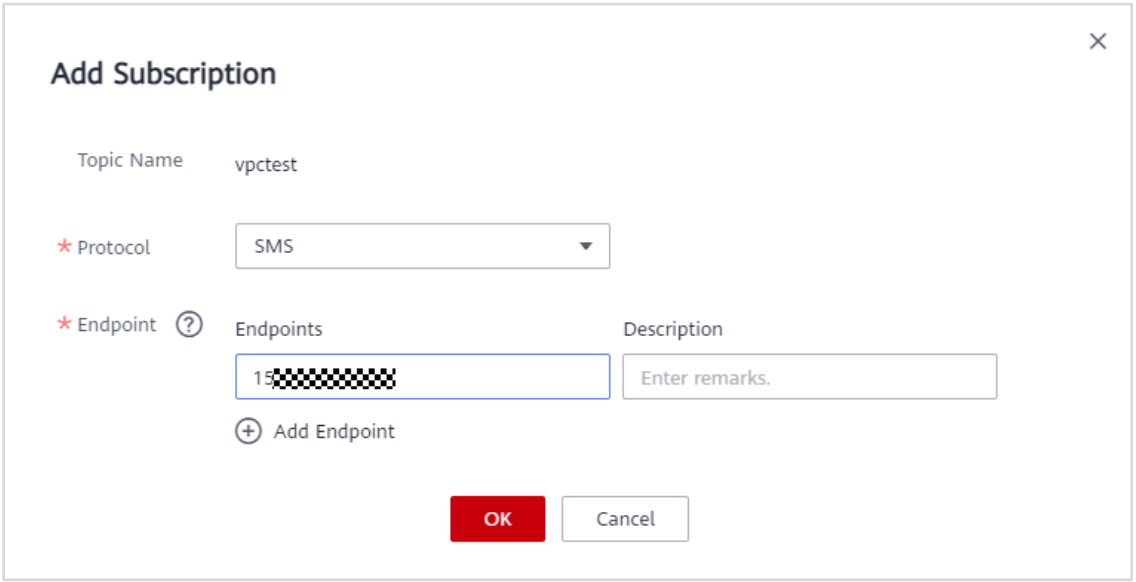


Figure 5-10 Configuring a subscription

Step 7 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.

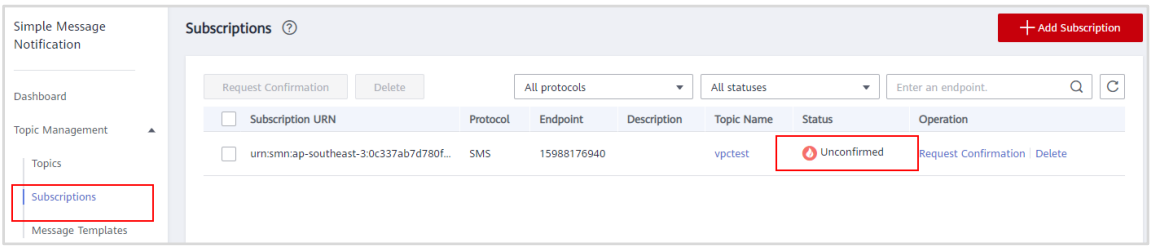


Figure 5-11 Viewing the subscription

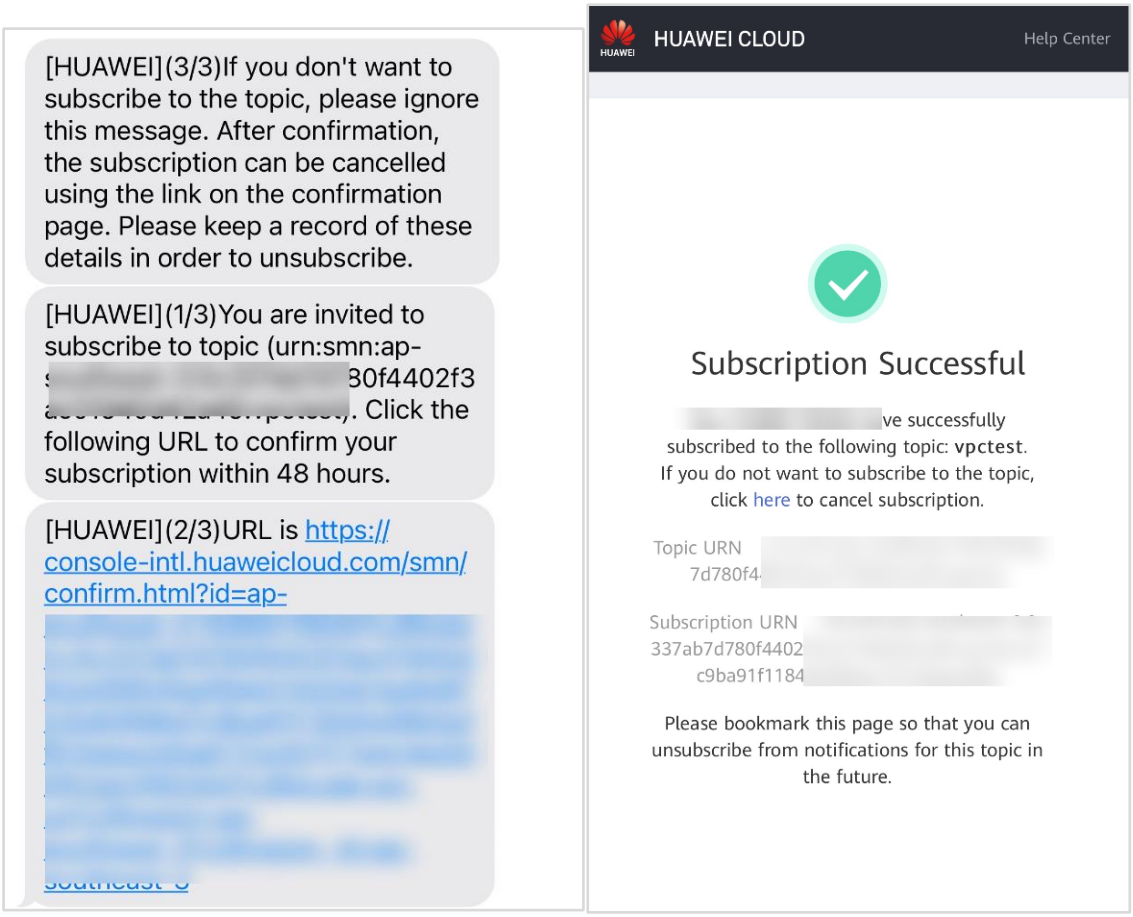


Figure 5-12 Successful subscription

Step 8 On the **Subscriptions** page, if the subscription status has changed to **Confirmed**, subscription was successful.

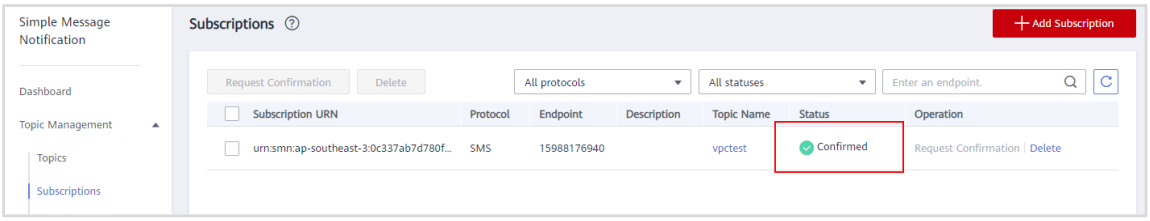


Figure 5-13 Successful subscription

Step 9 On the **Topics** page, click **Publish Message** to publish a message and check that you receive it.

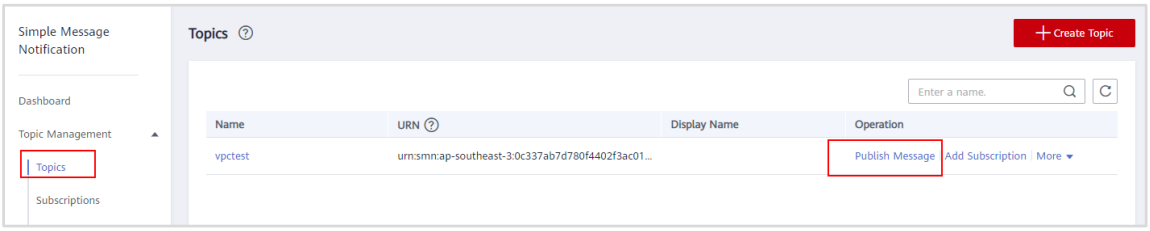


Figure 5-14 Publishing a message

Step 10 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.

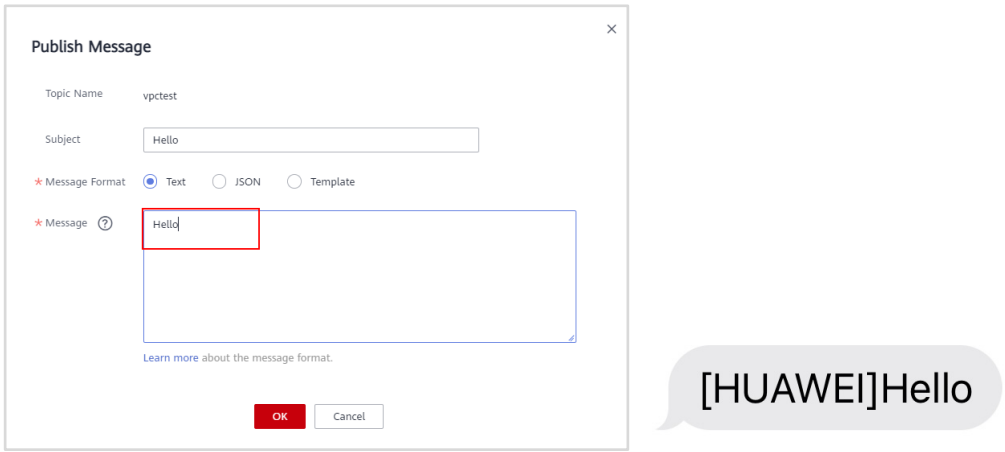


Figure 5-15 Configuring the message

5.2.2 Performing a key operation in VPC and verifying CTS functions

Step 1 Create a VPC in the **AP-Singapore** region. For details about VPC creation, see Creating VPCs.

Figure 5-16 Creating a VPC

Step 2 When the VPC is created, check for an SMS about the VPC creation from HUAWEI CLOUD.

Step 3 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.

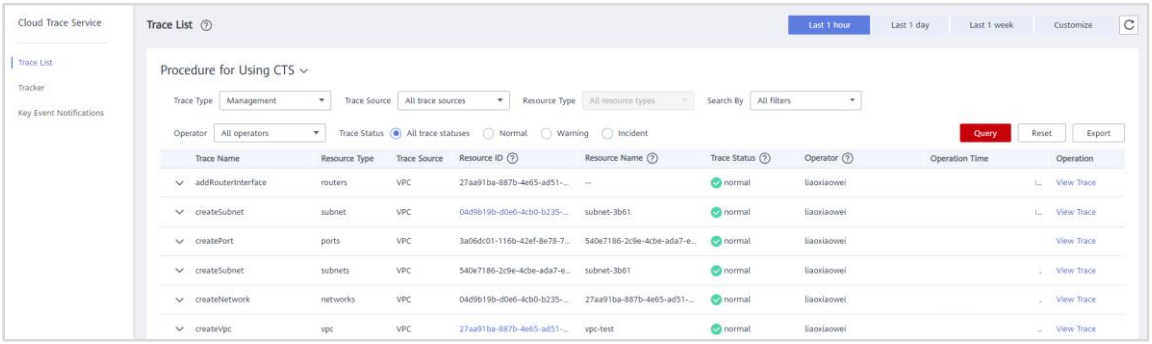


Figure 5-17 Viewing traces

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

Step 1 On the management console, search for **Cloud Eye** and access it.

Cloud Eye is a multi-dimensional resource monitoring service.

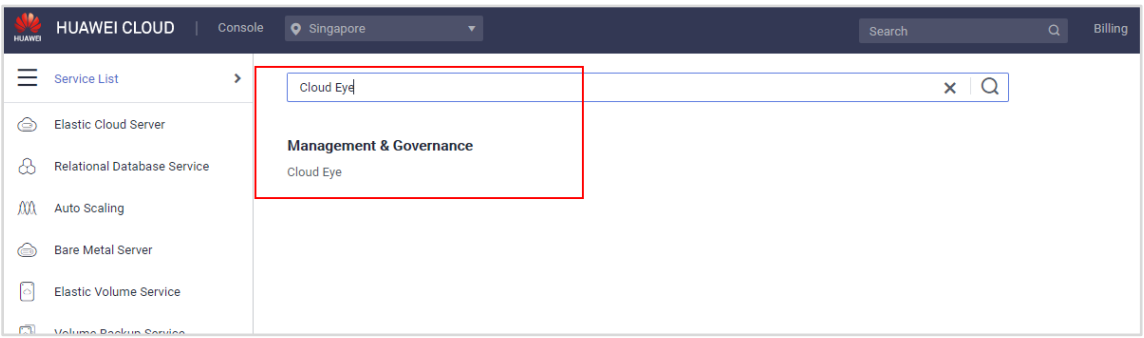
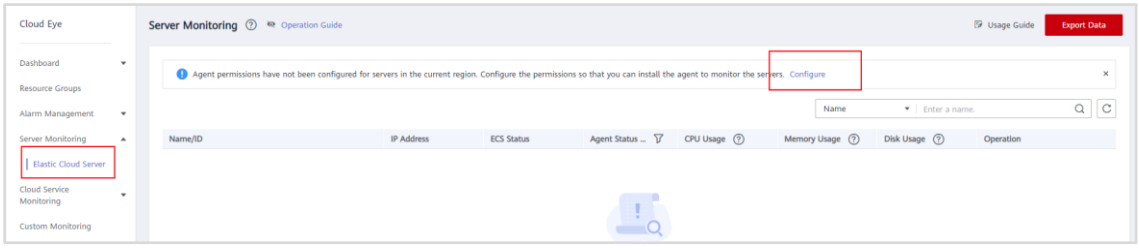


Figure 5-18 Accessing Cloud Eye

Step 2 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.



Step 3 Go to the ECS console, locate **ecs-linux**, and in the **Operation** column, click **Remote Login**.

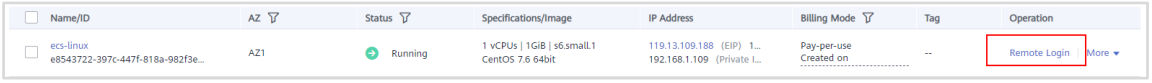


Figure 5-19 Remotely logging in to ecs-linux

Step 4 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
```

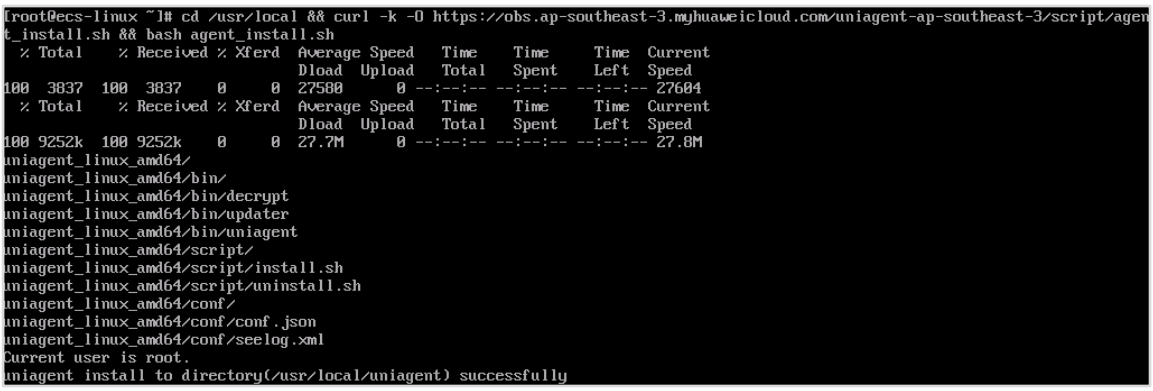


Figure 5-20 Installing and configuring the Agent

Step 5 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 5-21 Agent installed successfully

Step 6 Go to the ECS console. In the ECS list, locate **ecs-linux**, and in the **Operation** column, choose **More** > **Restart**.

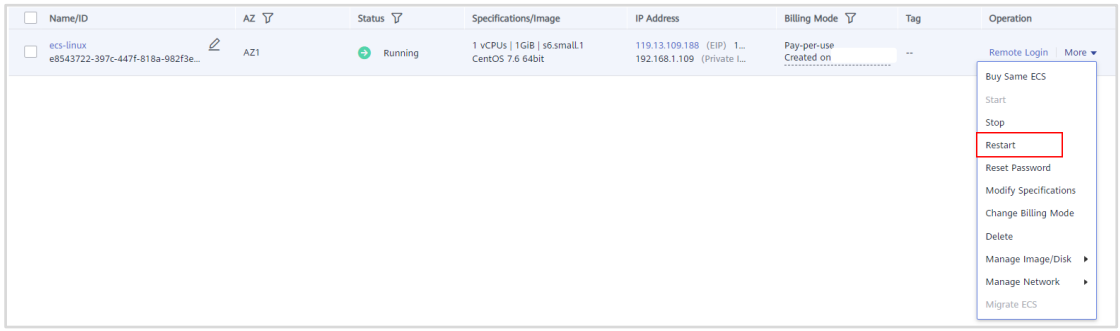


Figure 5-22 Restarting ecs-linux

Step 7 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**.

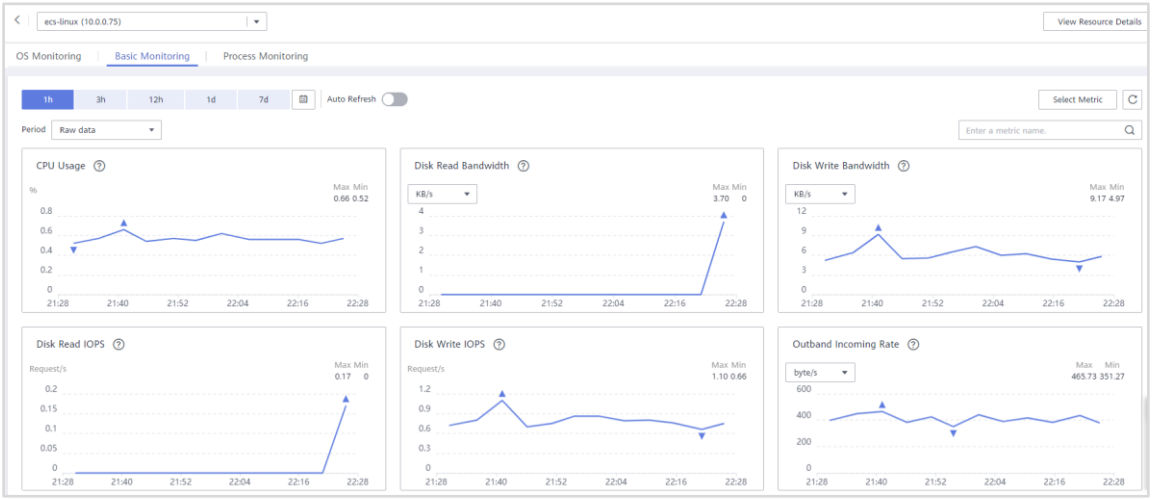


Figure 5-23 Viewing metrics

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.

Step 1 On the Cloud Eye **Server Monitoring** page, locate **ecs-linux** and click **Create Alarm Rule** in the **Operation** column.

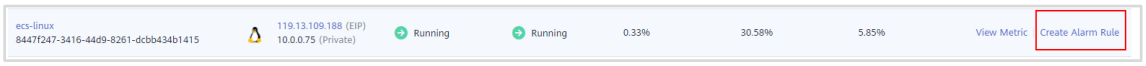
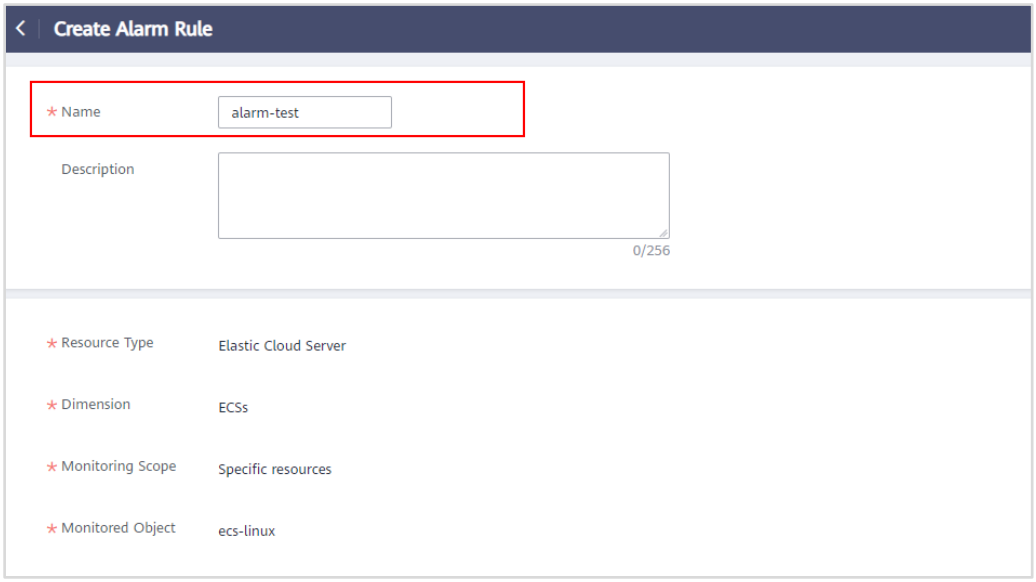


Figure 5-24 Create Alarm Rule

Step 2 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**, **>=2%**, **Every 5 minutes**
- **Alarm Severity**: **Major**



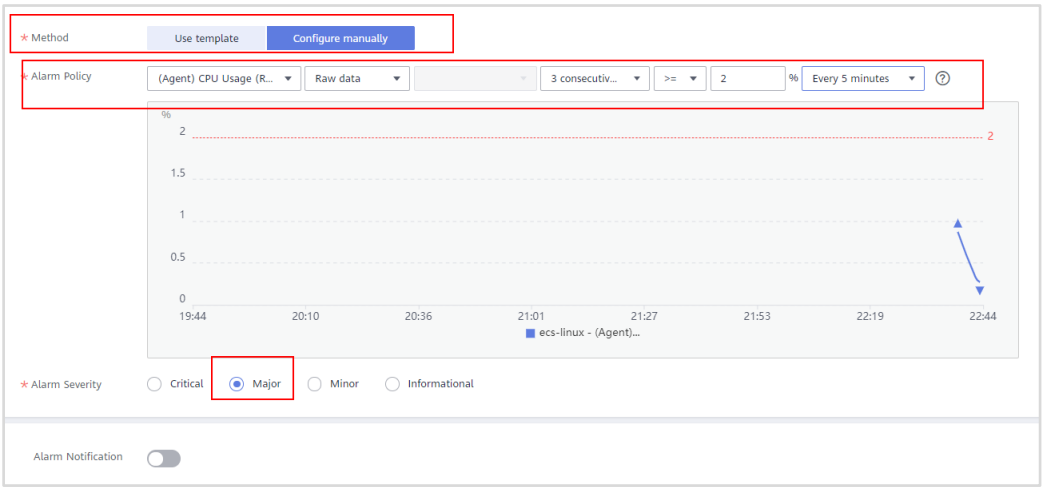


Figure 5-25 Create Alarm Rule

Step 3 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.

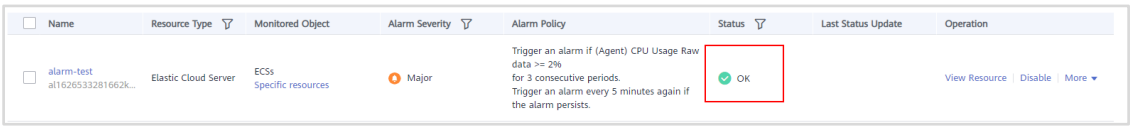


Figure 5-26 Viewing alarm-test

Step 4 Go to the **Server Monitoring** page, locate **ecs-linux**, and in the **Operation** column, click **View Metric**.

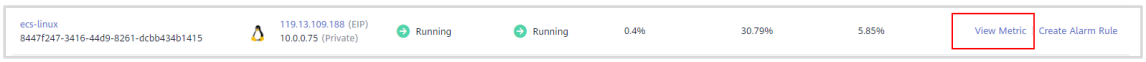


Figure 5-27 Viewing metrics

Step 5 View the CPU usage of **ecs-linux**.

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

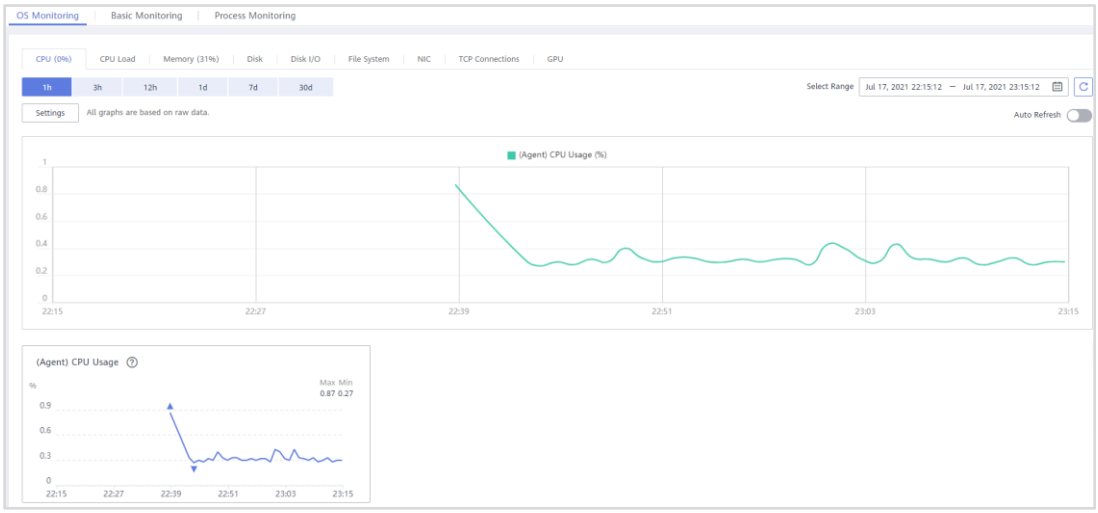


Figure 5-28 OS Monitoring

Step 6 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 dramaticaly increased.)

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

Figure 5-29 Logging in to ecs-linux

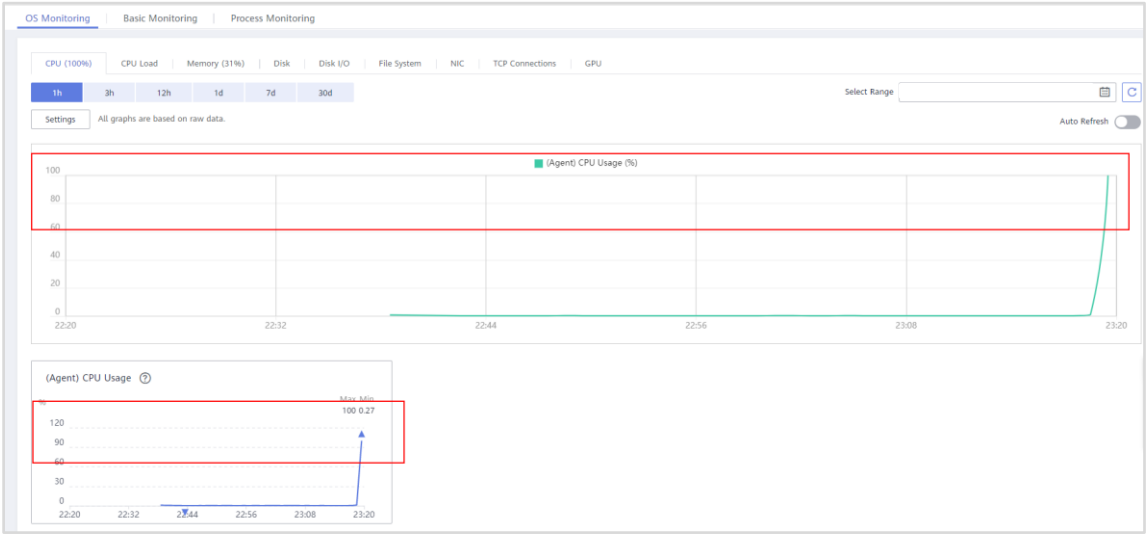


Figure 5-30 Fast and dramatic increase of the CPU usage

Step 7 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**.

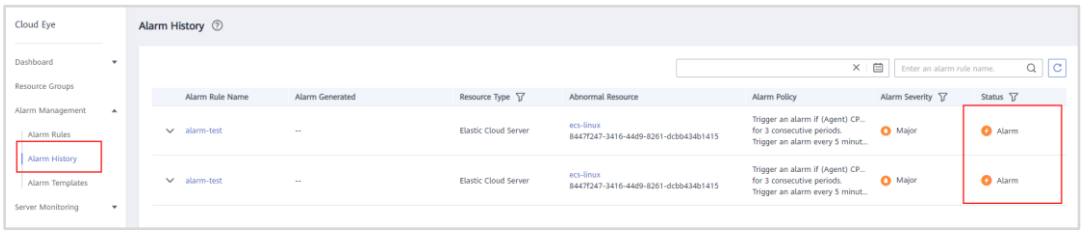


Figure 5-31 alarm-test status being Alarm

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

Step 1 Log in to the management console, expand the service list, and click **Log Tank Service**.

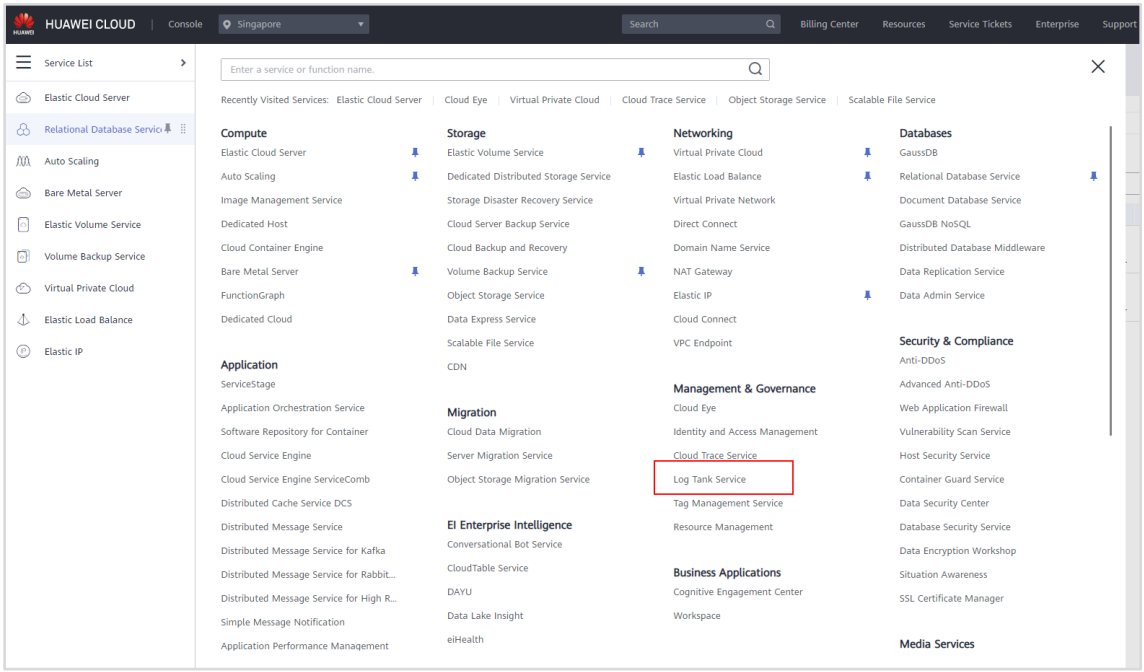


Figure 5-32 Accessing LTS

Step 2 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.

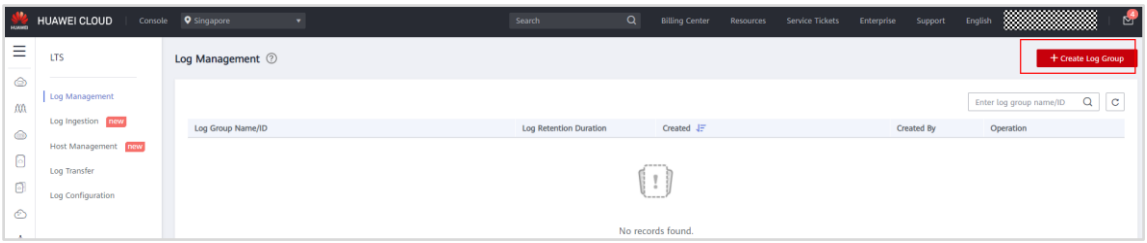


Figure 5-33 Creating a log group

Step 3 Give your group a name and choose how many days you want to retain its logs, and click **OK**.

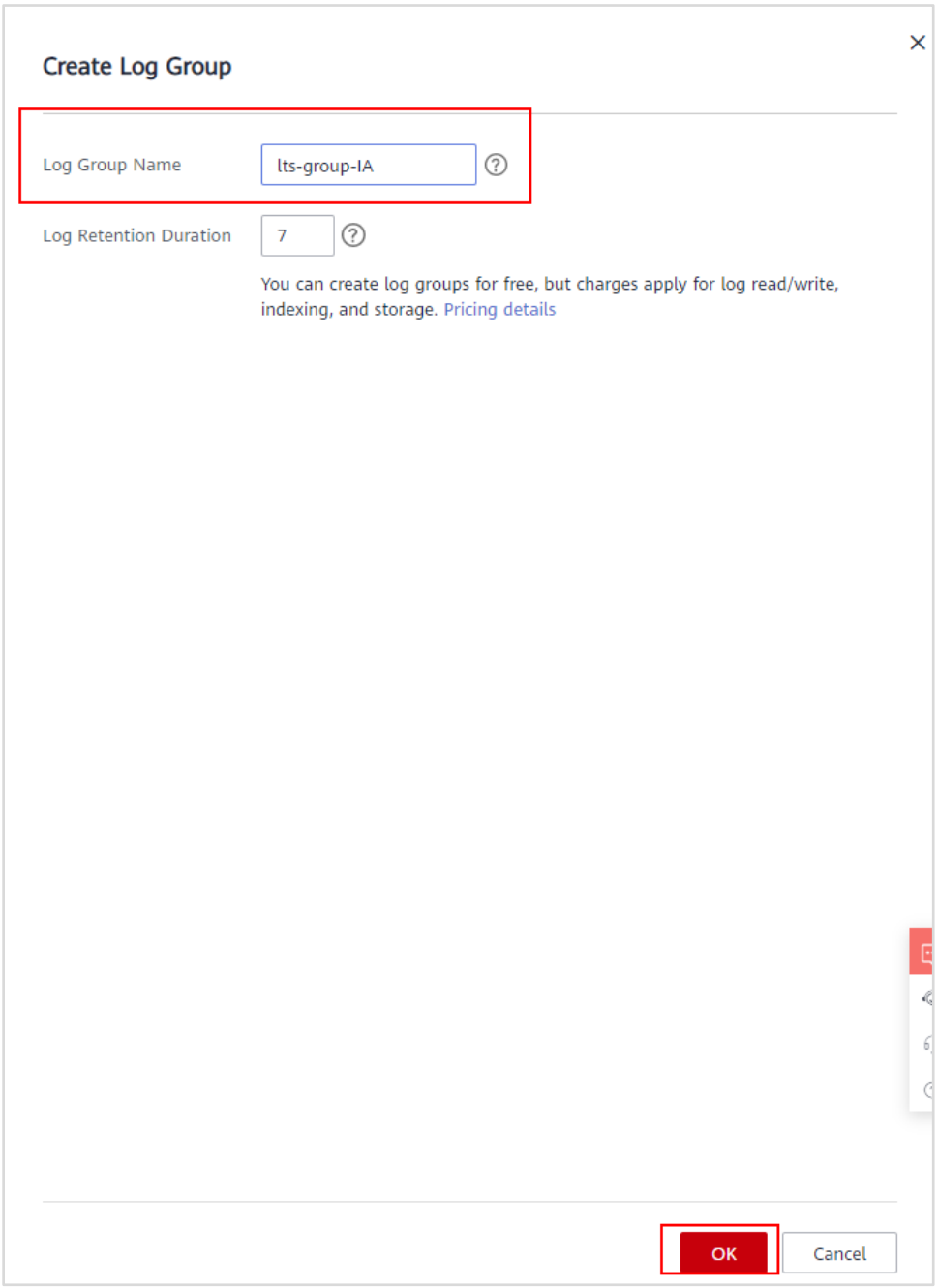


Figure 5-34 Configuring a log group

Step 4 On the **Log Management** page, click the name of your log group.

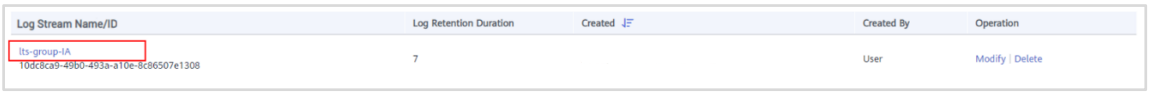


Figure 5-35 Accessing a log group

Step 5 On the page displayed, Click **Create Log Stream**.

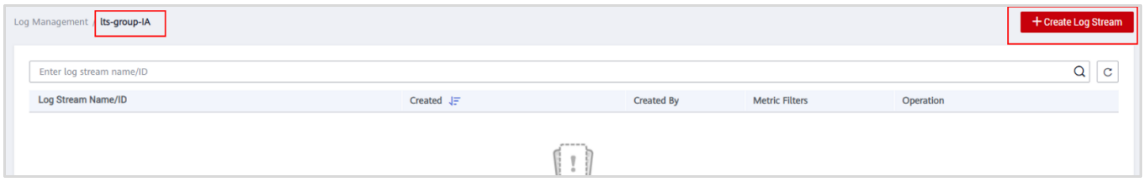


Figure 5-36 Creating a log stream

Step 6 Enter a log stream name and click **OK**.

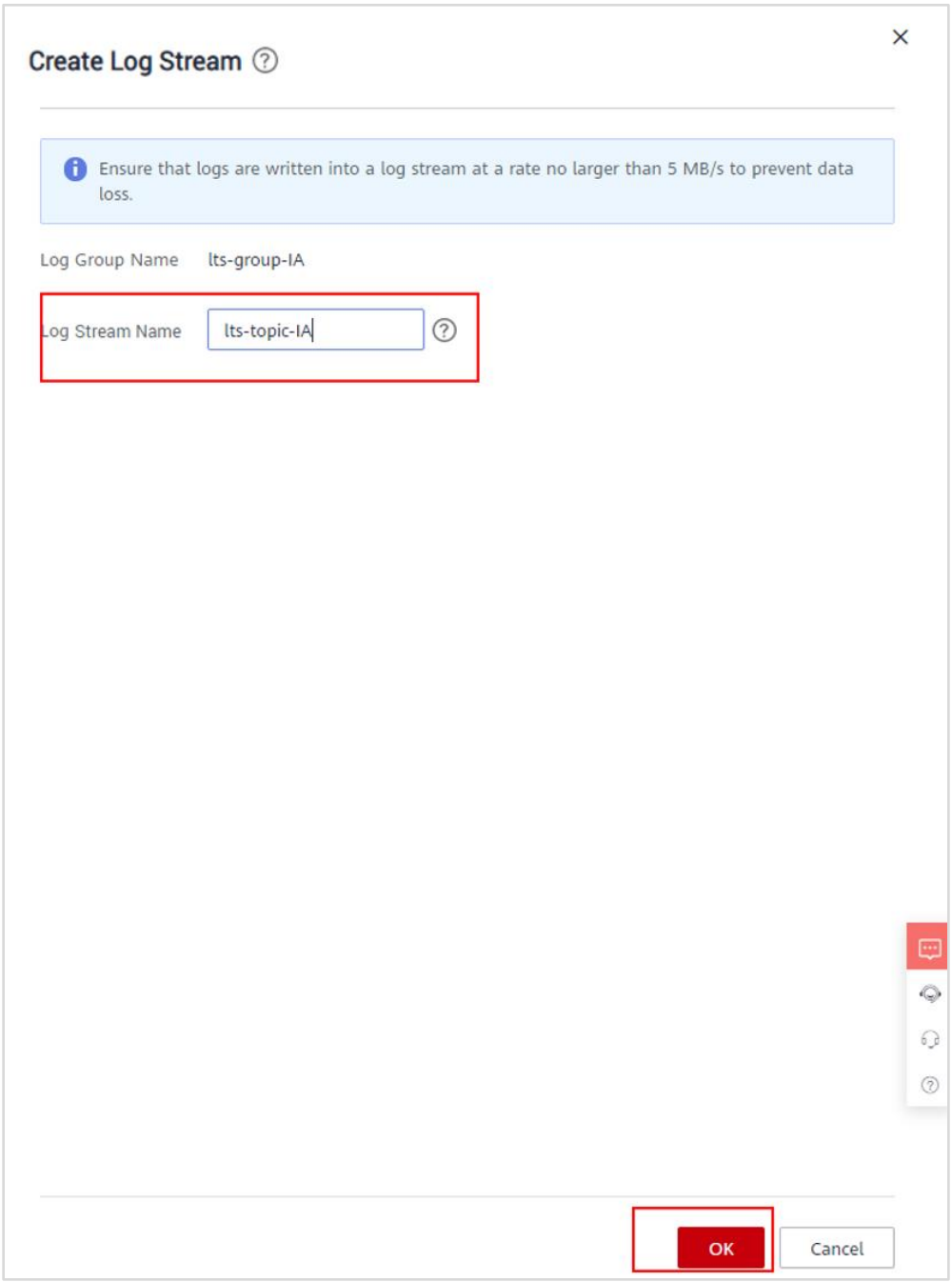


Figure 5-37 Configuring a log stream

5.2.4.2 Installing ICAgent

Step 1 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 Management** in the navigation pane, and click **Install ICAgent** in the upper right.

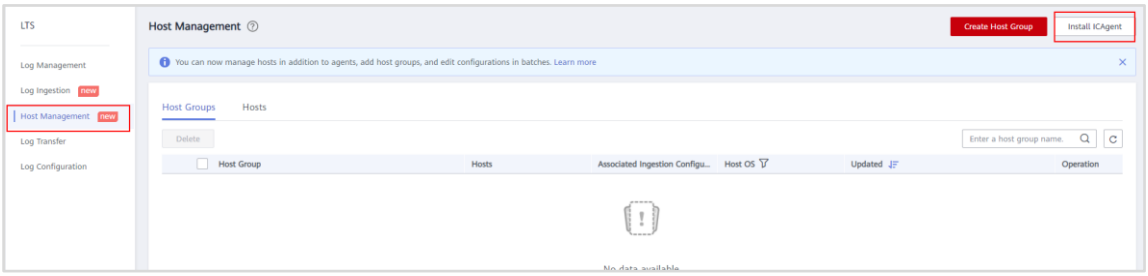


Figure 5-38 Accessing the Host Management page

Step 2 Configure ICAgent installation parameters.

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

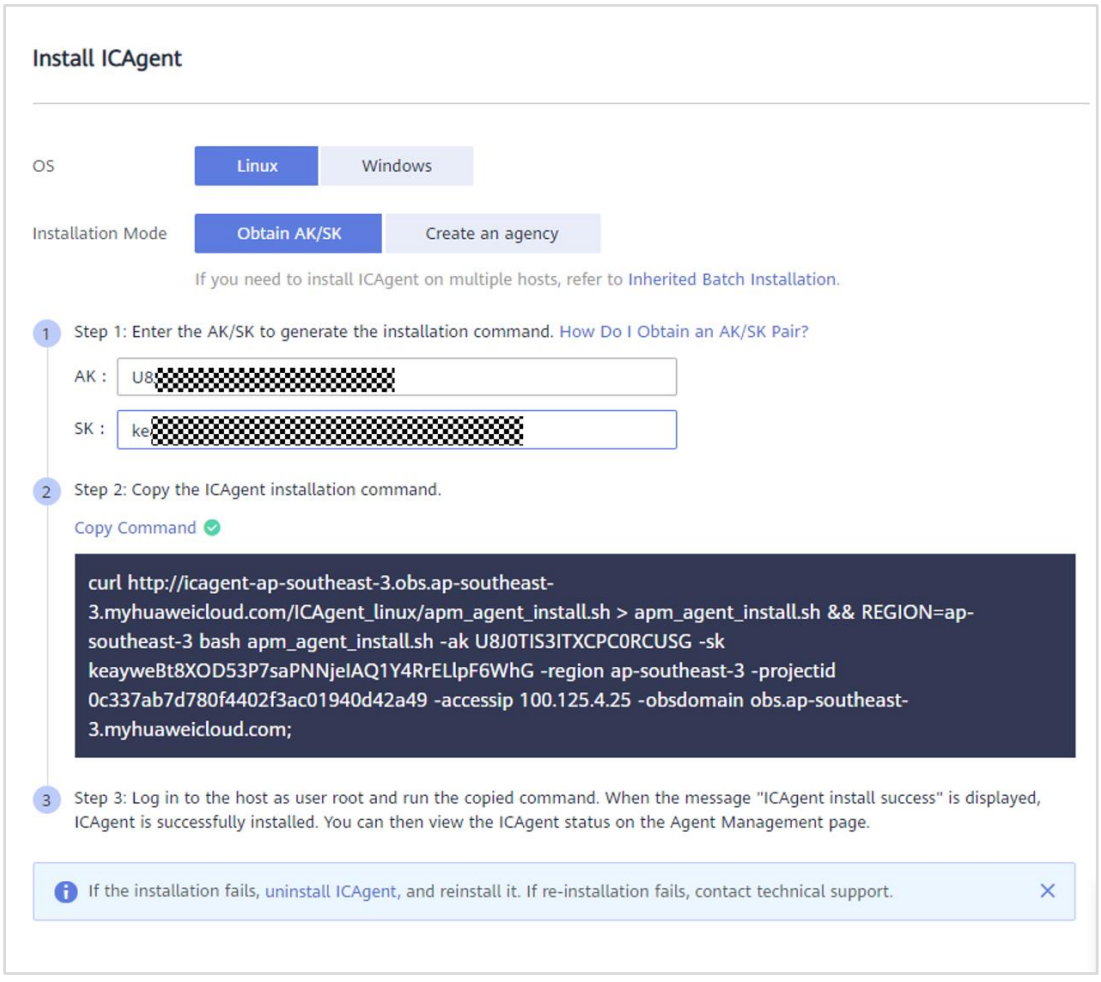


Figure 5-39 Configuring ICAgent Installation

Step 3 Copy the command in Step 2 and run it in the ECS. If the following information is displayed, the installation is successful.

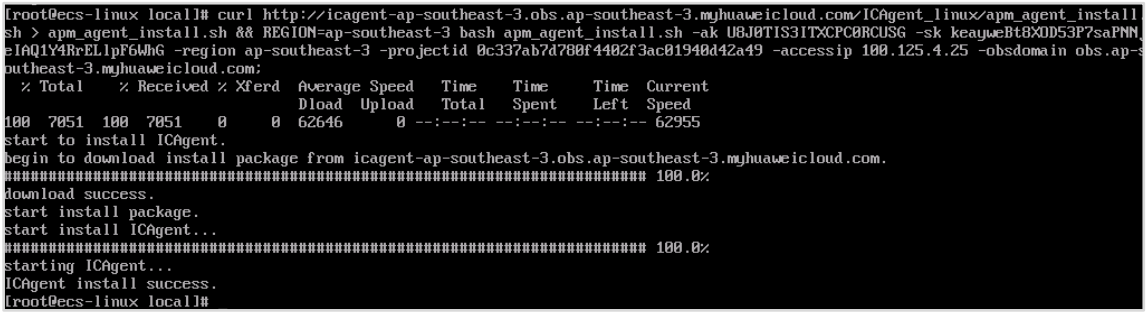


Figure 5-40 Installing ICAgent

Step 4 Refresh the **Hosts** tab under the **Host Management** page. If the ICAgent status for the ECS is **Running**, ICAgent has been installed.

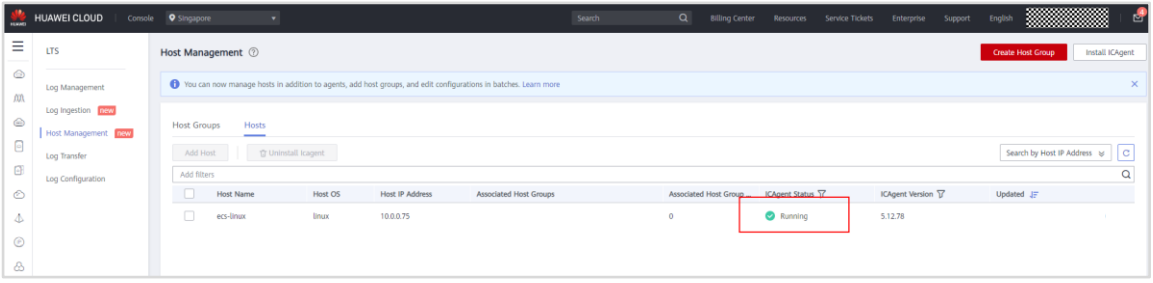
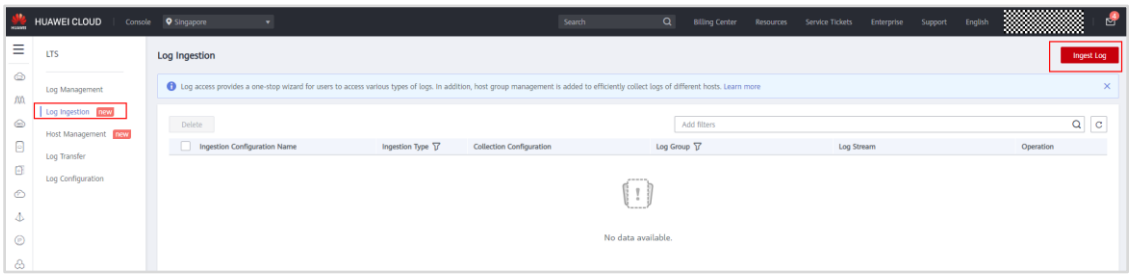


Figure 5-41 Viewing the ICAgent status

5.2.4.3 Configuring Log Ingestion

Step 1 On the LTS console, choose **Log Ingestion** in the navigation pane, click **Ingest Log** in the upper right corner, and click **Host**.



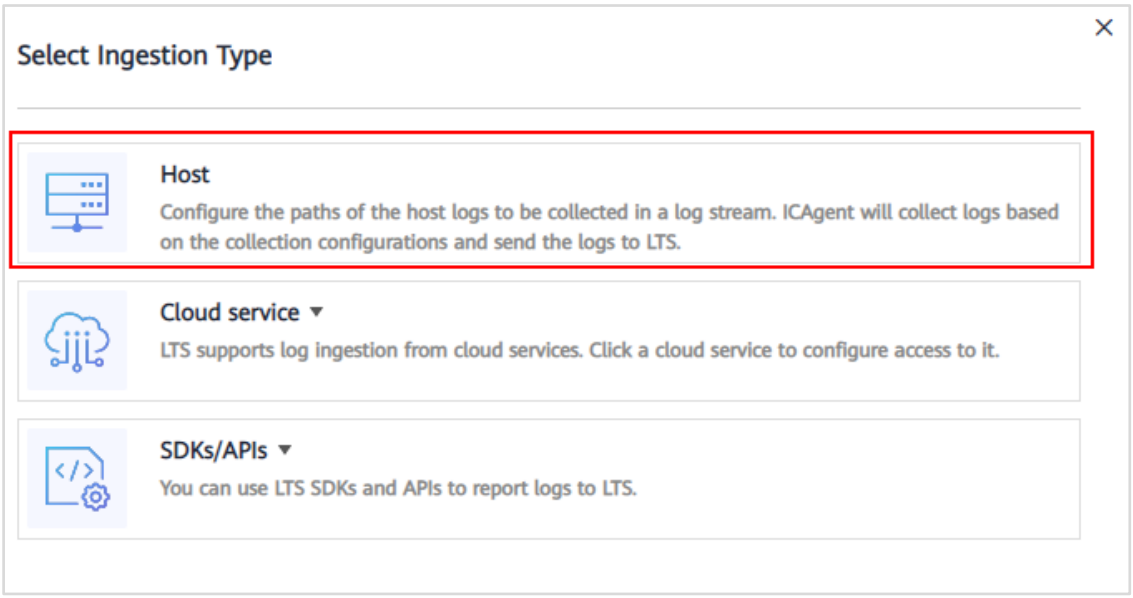


Figure 5-42 Selecting Host

Step 2 On the **Select Log Stream** stage, select the log group and log stream you created. Click **Next: Select Host Group**.

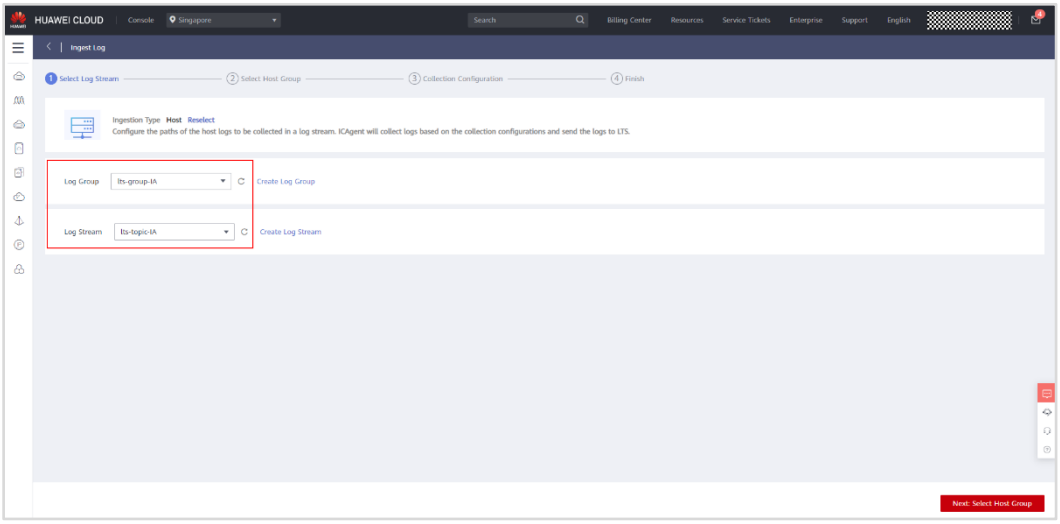


Figure 5-43 Selecting a log stream

Step 3 Create a host group. Give the group a name. Select it in the list and go to the next step.

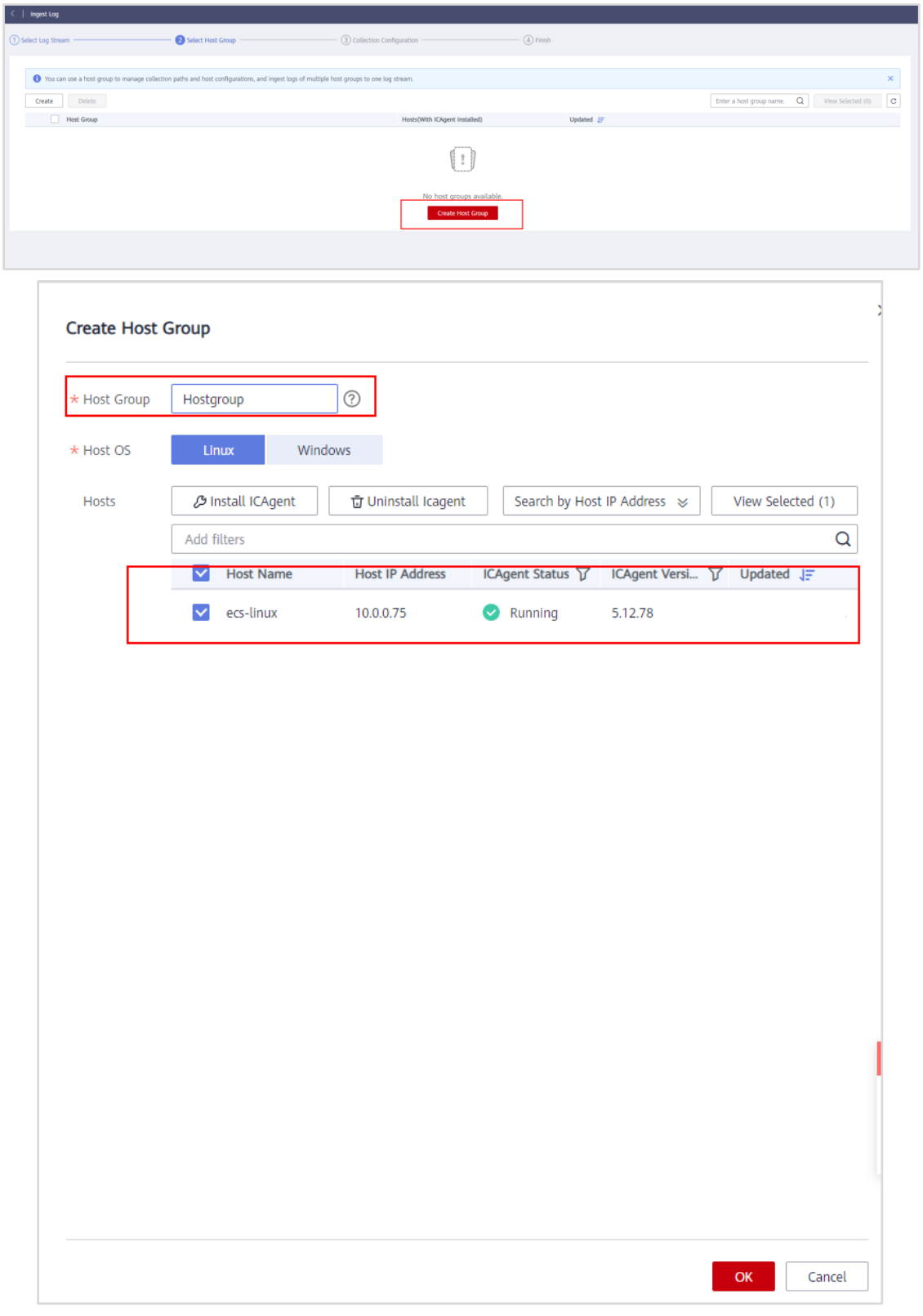


Figure 5-44 Creating a host group

Step 4 Configure the collection configuration name and collection paths. Collection paths are ECS log paths and the source of the logs ICAgent will collect.

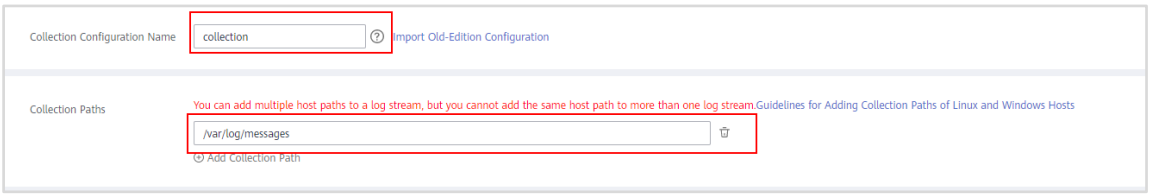


Figure 5-45 Configuring the collection

Step 5 Configure the log format and log time, and click **OK**.

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

Figure 5-46 Configuring the collection

Step 6 Wait a minute to view the ingested logs on the **Real-Time Logs** tab under a log stream.

Figure 5-47 Viewing real-time logs

Step 7 Click the **Raw Logs** tab. Search **successful** log events and check their context.

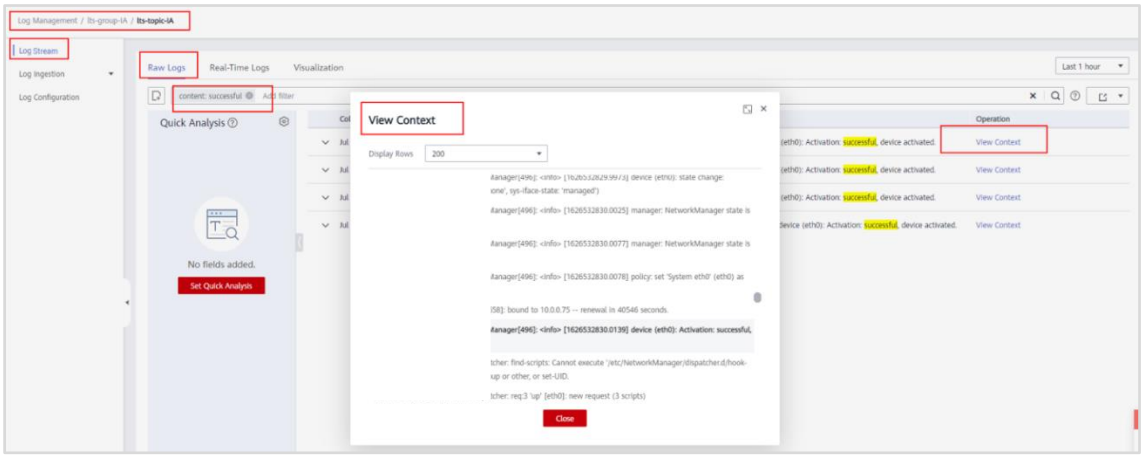


Figure 5-48 Searching for raw logs

Congratulations! You have just learnt to view ECS logs.

5.3 Deleting Resources

Step 1 Delete resources, such as ECSs, ECS monitoring settings, alarm rules, cloud service logs, and VPCs.

Step 2 Check that all resources in the account have been deleted.

5.4 Exercises

1. Create a Windows ECS.
2. Configure tracking of operations on the ECS in CTS.
3. Modify ECS specifications.
4. View related traces on the CTS console.

6 Comprehensive Exercise: Deploying an Enterprise Website on HUAWEI CLOUD

6.1 Background

An enterprise intends to deploy their website on HUAWEI CLOUD and they have the following requirements:

- Database nodes and service nodes are deployed on separate ECSs.
- ECSs are added or removed as incoming traffic changes over time.
- Incoming traffic is automatically distributed across the ECSs.
- Service statuses are monitored and visualized.

6.2 Solution

Table 6-1 Solution configuration table

Requirement	Solution	Involved Services
Database nodes and service nodes are deployed on separate ECS instances.	Website setup: Buy ECSs as service nodes and RDS instances as database nodes. Use VPC to provide network resources for ECSs.	ECS VPC RDS
ECSs are scaled in or out as service traffic changes over time.	Feature configuration: Use AS to scale in or out ECSs created from the image of a service node as required to ensure stable, efficient services.	AS, IMS
Service traffic is automatically distributed across the ECSs.	Feature configuration: Use ELB to automatically distribute incoming traffic across the ECSs for better fault tolerance.	ELB
Service statuses are monitored and visualized.	Feature configuration: Use Cloud Eye to monitor services.	Cloud Eye

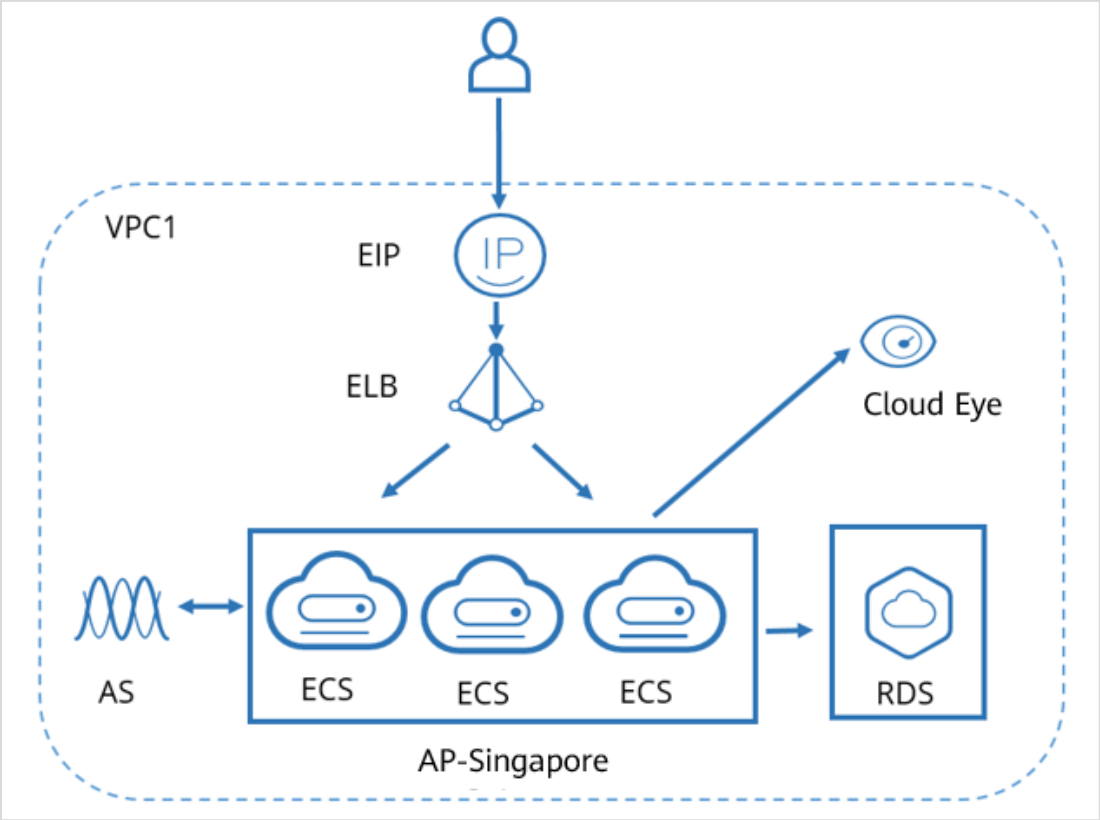


Figure 6-1 Solution topology

6.3 Preparations

6.3.1 Logging In to HUAWEI CLOUD

Step 1 Visit the HUAWEI CLOUD official website and click **Log In** in the upper right corner.

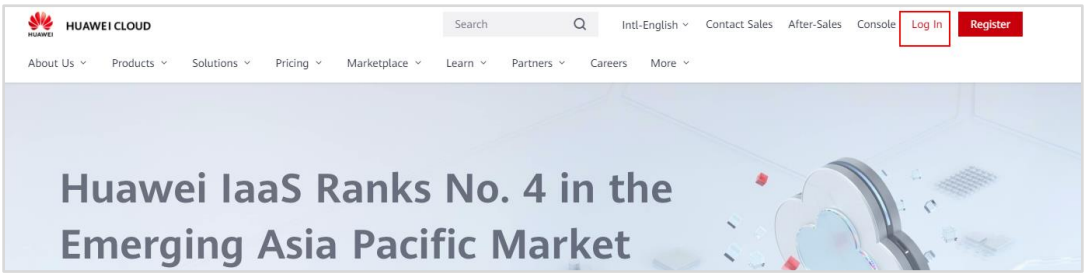


Figure 6-2 Visiting the HUAWEI CLOUD official website

Step 2 On the login page, click **HUAWEI CLOUD Account**, enter your account and password, and then click **Log In**.

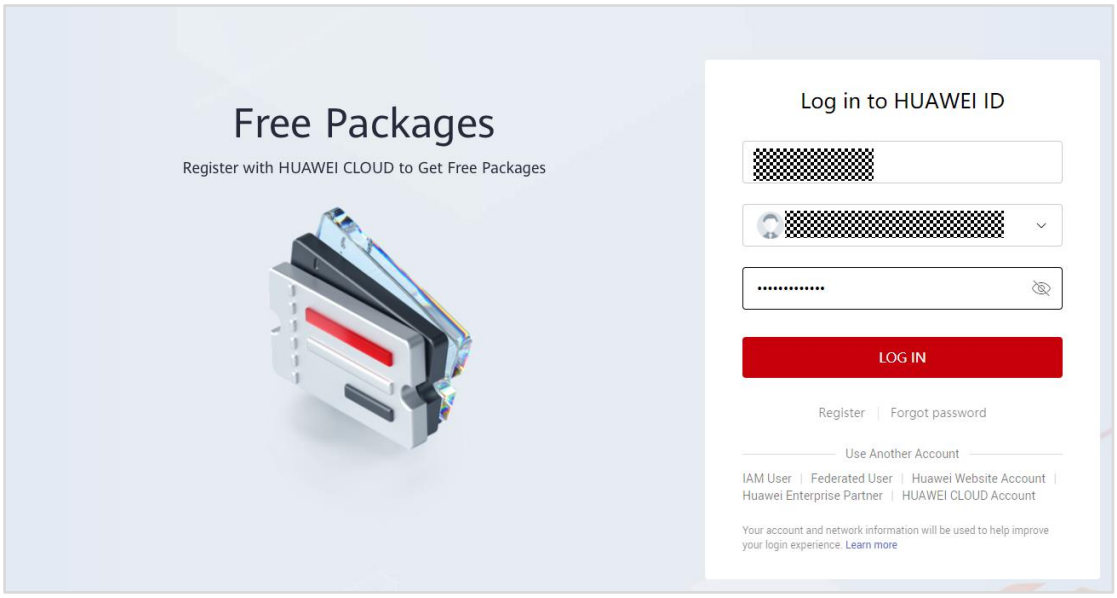


Figure 6-3 Logging in to the HUAWEI CLOUD official website

6.3.2 Creating a VPC

Step 1 Switch to the management console, and select the **AP-Singapore** region. In the left navigation pane, choose **Service List** > **Networking** > **Virtual Private Cloud**.

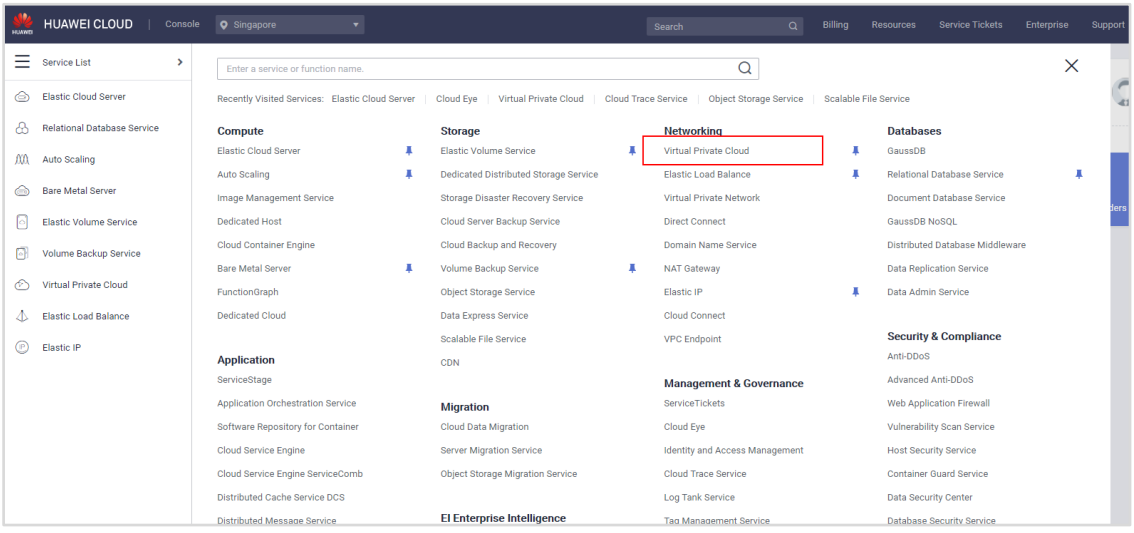


Figure 6-4 Switching to the VPC console

Step 2 Click **Create VPC**.

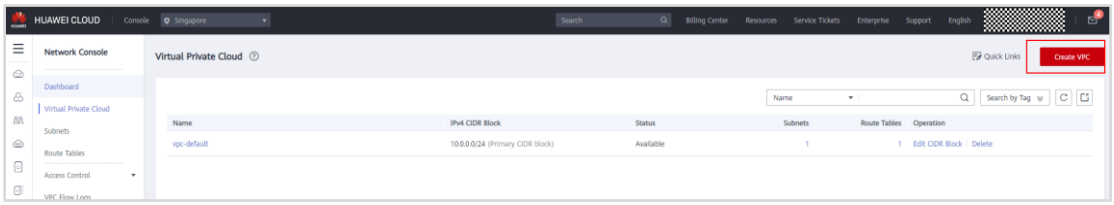


Figure 6-5 Creating a VPC

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

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

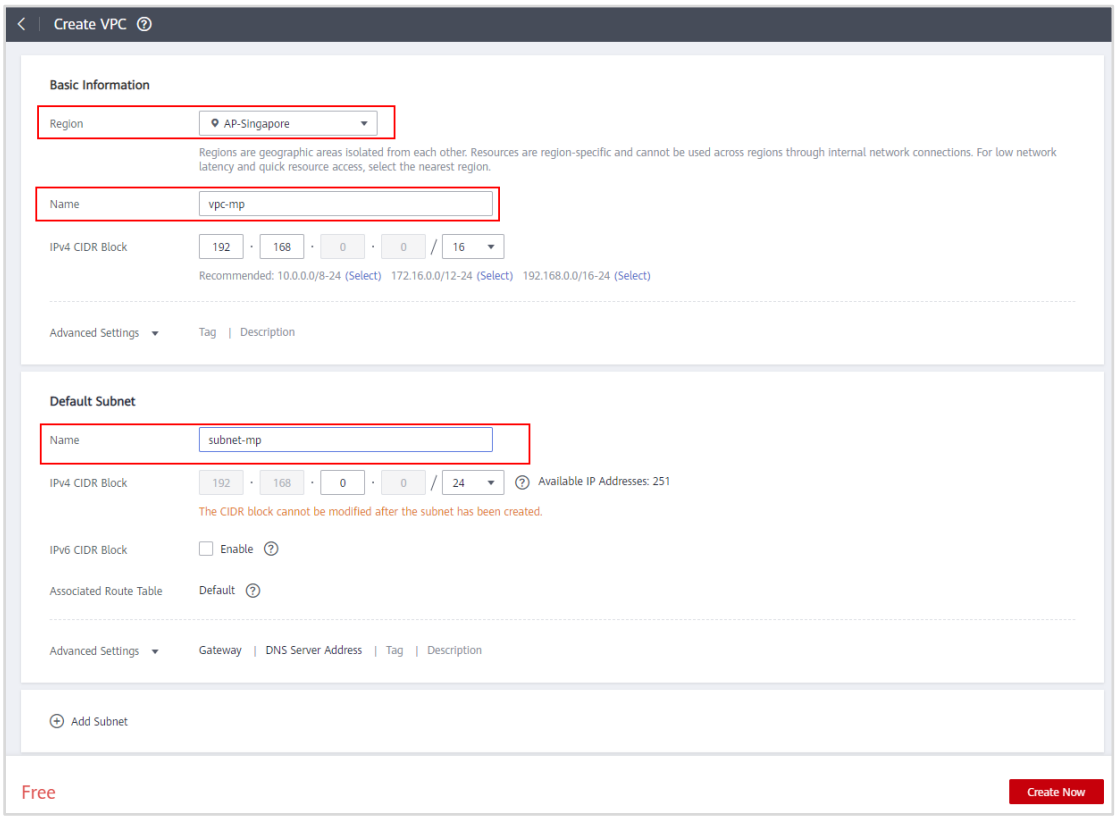


Figure 6-6 Configuring the VPC

Step 4 View the created VPC in the VPC list.

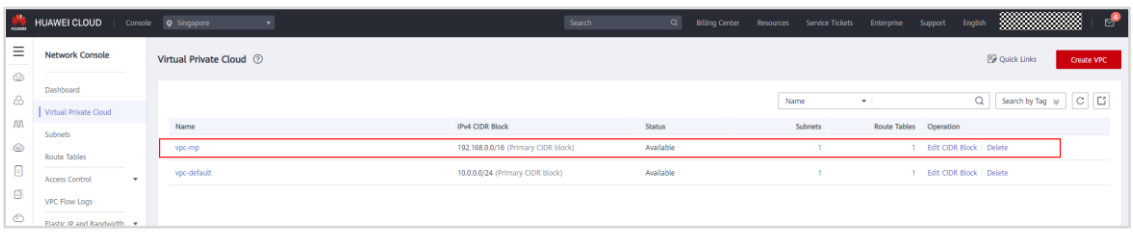


Figure 6-7 Viewing the VPC

6.3.3 Creating and Configuring a Security Group

Step 1 On the **Network Console**, choose **Access Control** > **Security Groups** and create a security group.

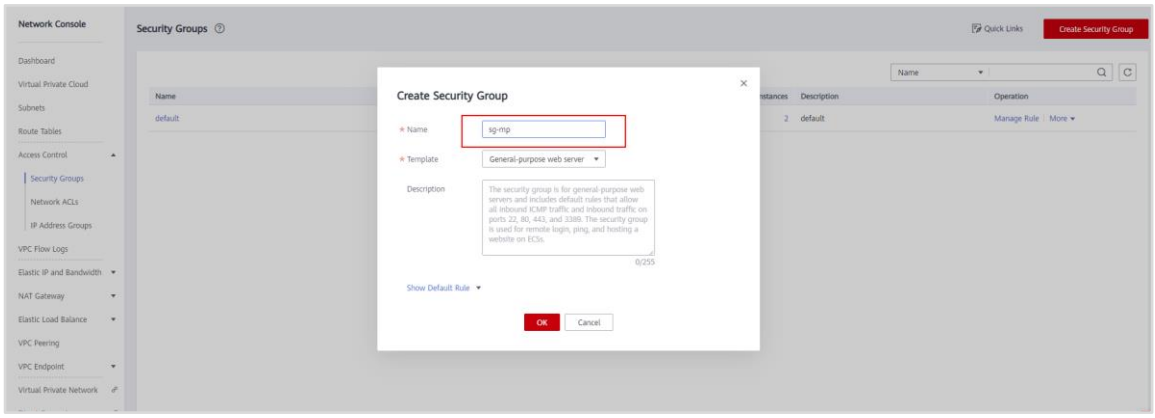


Figure 6-8 Creating a security group

Step 2 Click the security group name.

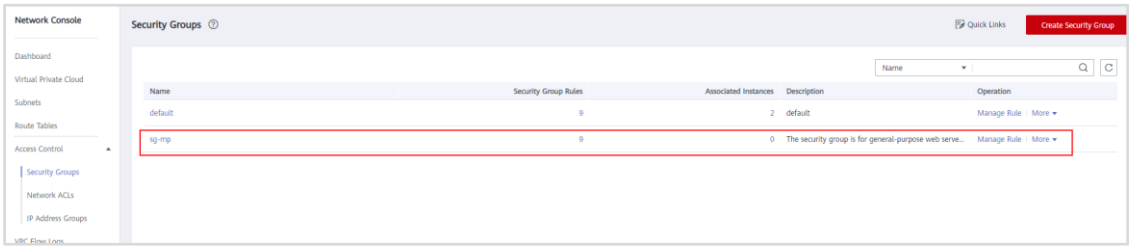


Figure 6-9 Viewing the security group

Step 3 Click **Inbound Rules** and then **Add Rule** to add an inbound rule with the following parameter settings:

- **Protocol & Port**: **All**
- **IP address** in **Source**: **0.0.0.0/0**

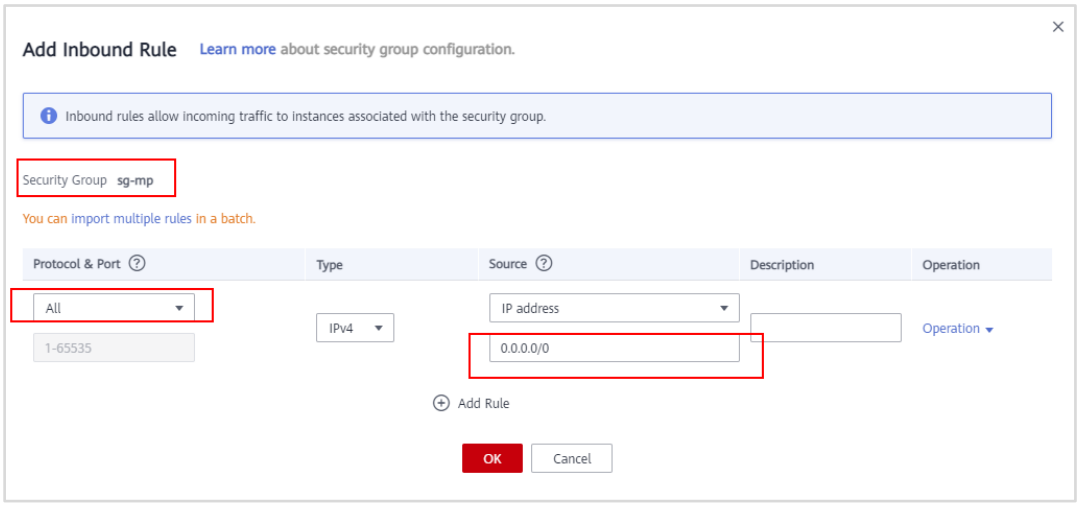


Figure 6-10 Adding an inbound rule

6.3.4 Buying an ECS

Step 1 In the service list, choose **Compute** > **Elastic Cloud Server**.

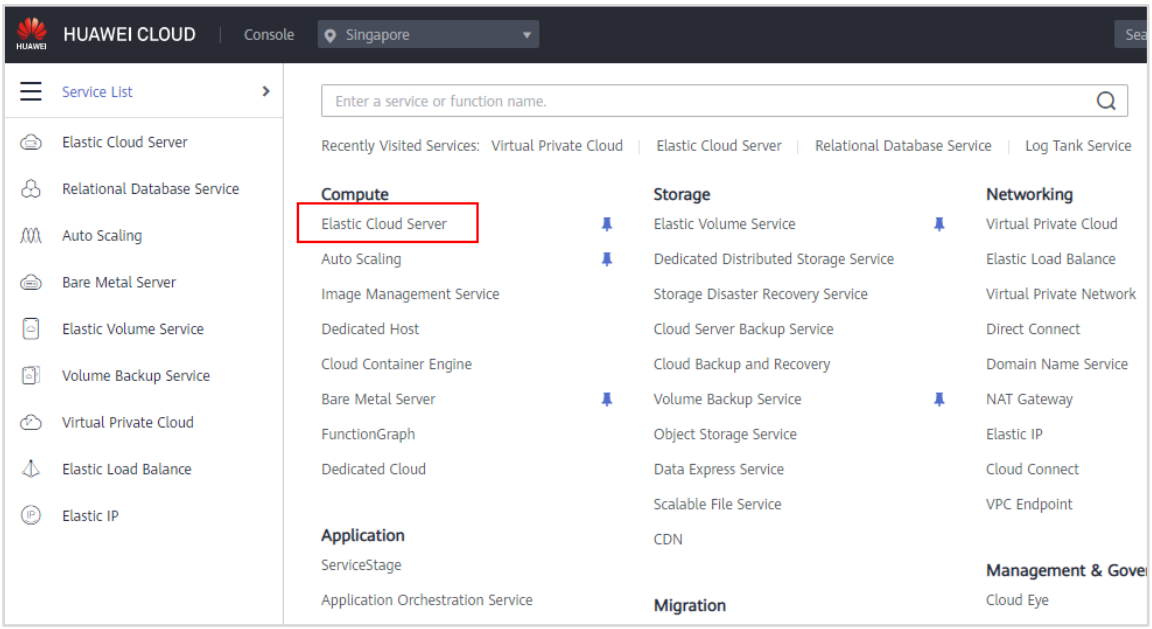


Figure 6-11 Acessing the ECS console

Step 2 Click **Buy ECS** and set the following parameters.

Basic settings:

- **Billing Mode**: **Pay-per-use**
- **Region**: **AP-Singapore**
- **AZ**: **Random**

- **CPU Architecture**: **x86**
- **Specifications**: **General computing**, **s6.small.1 1 vCPUs | 1 GB**
- **Image**: **Public image**, **CentOS 7.6 64bit (40 GB)**
- **System Disk**: **High I/O**, **40 GB**

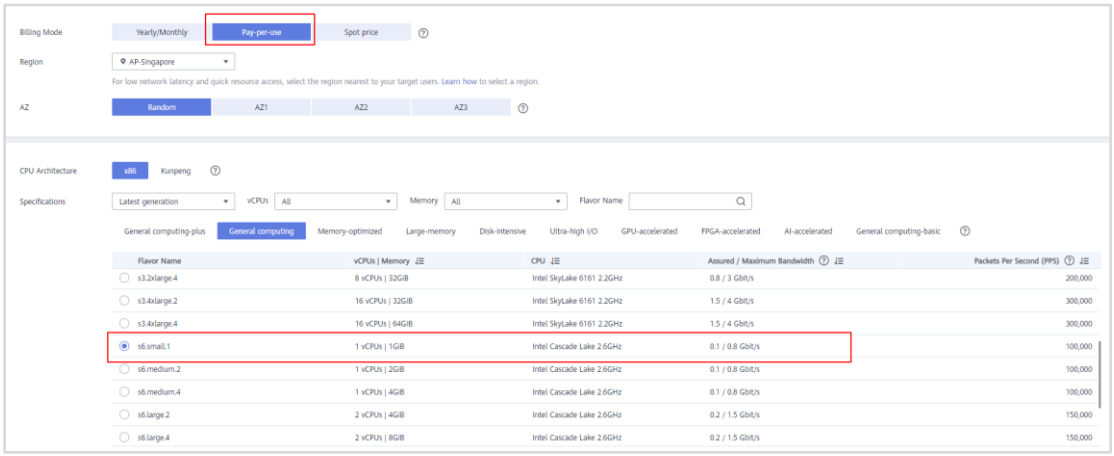


Figure 6-12 Configuring basic settings

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**

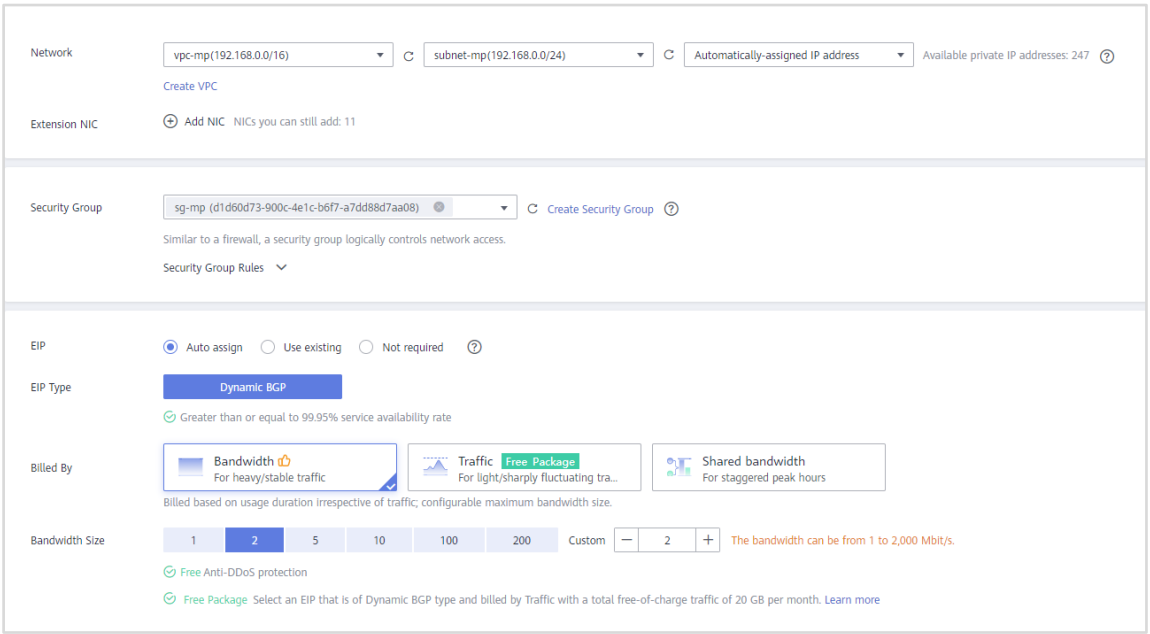


Figure 6-13 Configuring network

Advanced settings:

- **ECS Name**: **ecs-mp** (Change it as needed.)

- **Login Mode**: **Password**, for example, **Huawei@123!**
- **Cloud Backup and Recovery**: **Not required**

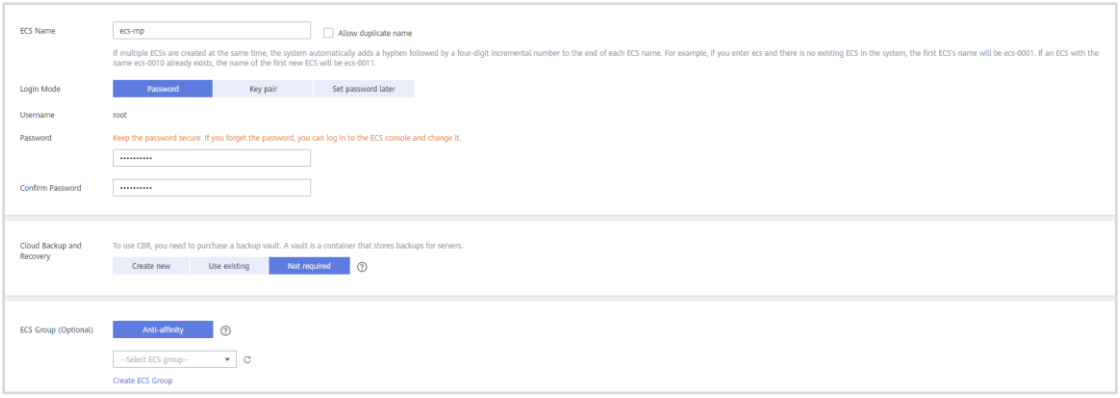


Figure 6-14 Configuring advanced settings

Step 3 Confirm the configuration, select **I have read and agree to the Service Level Agreement and Image Disclaimer**, and click **Buy Now**.

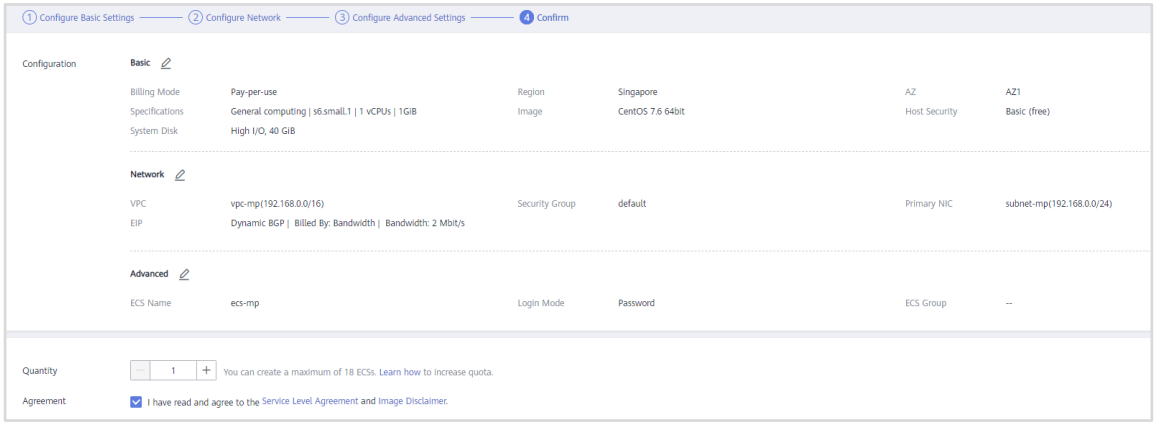


Figure 6-15 Confirmation

Step 4 View the purchased ECS in the ECS list.

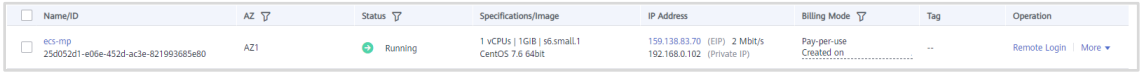


Figure 6-16 Viewing the ECS in the list

Step 5 An EIP has been bound to the ECS. To enhance ECS login security, you are advised to set the ECS login mode to key pair. For details, see Access to the Internet with an EIP.

6.3.5 Buying an RDS DB Instance

Step 1 Go back to the service list, and choose **Database** > **Relational Database Service**.

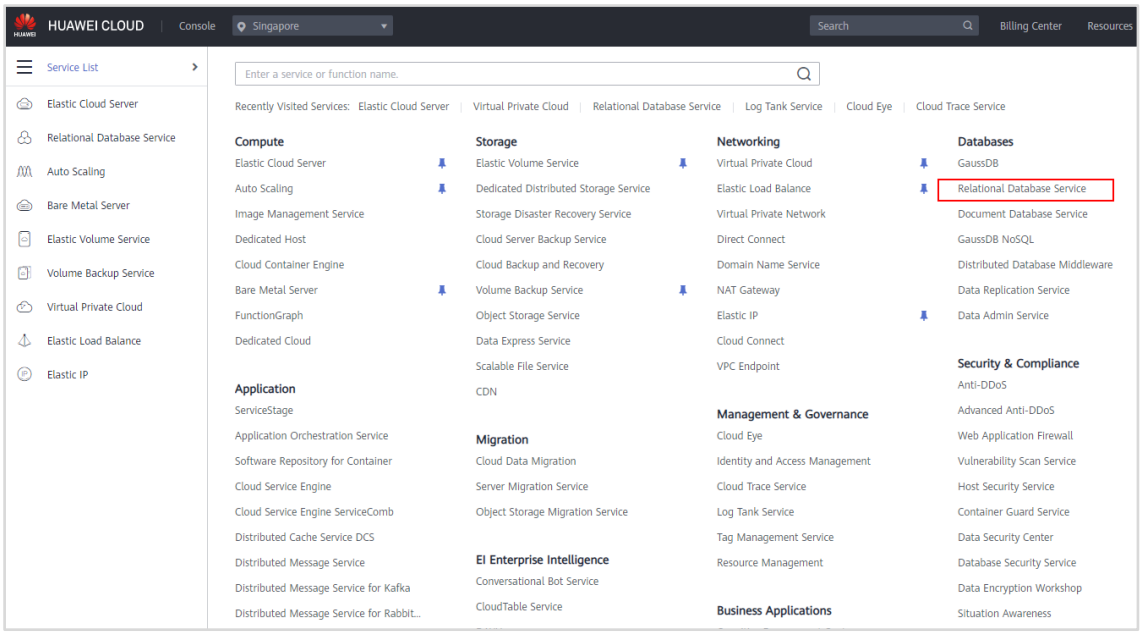


Figure 6-17 Acessing the RDS console

Step 2 Click **Buy DB Instance**.

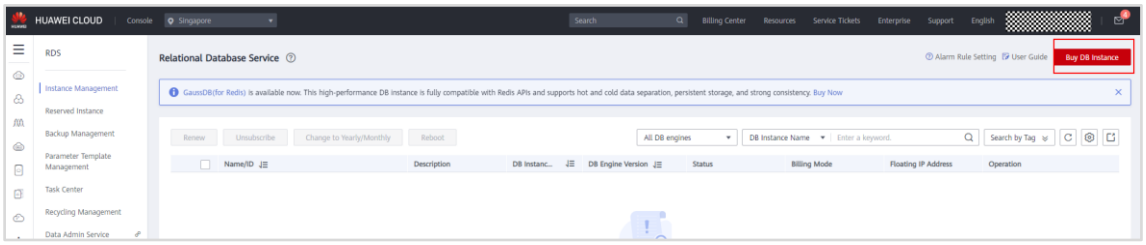


Figure 6-18 Buying a DB instance

Step 3 Set the parameters as follows and click **Next**.

- **Billing Mode**: **Pay-per-use**
- **Region**: **AP-Singapore**
- Instance parameters: **rds-***name* (customizable), **MySQL**, **8.0**, **Primary/Standby**, **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.

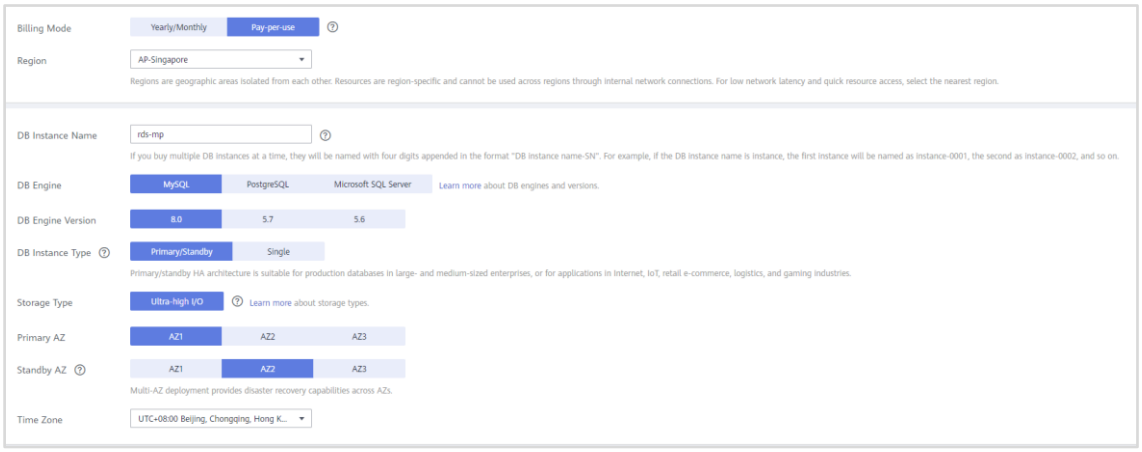


Figure 6-19 Configuring a DB instance

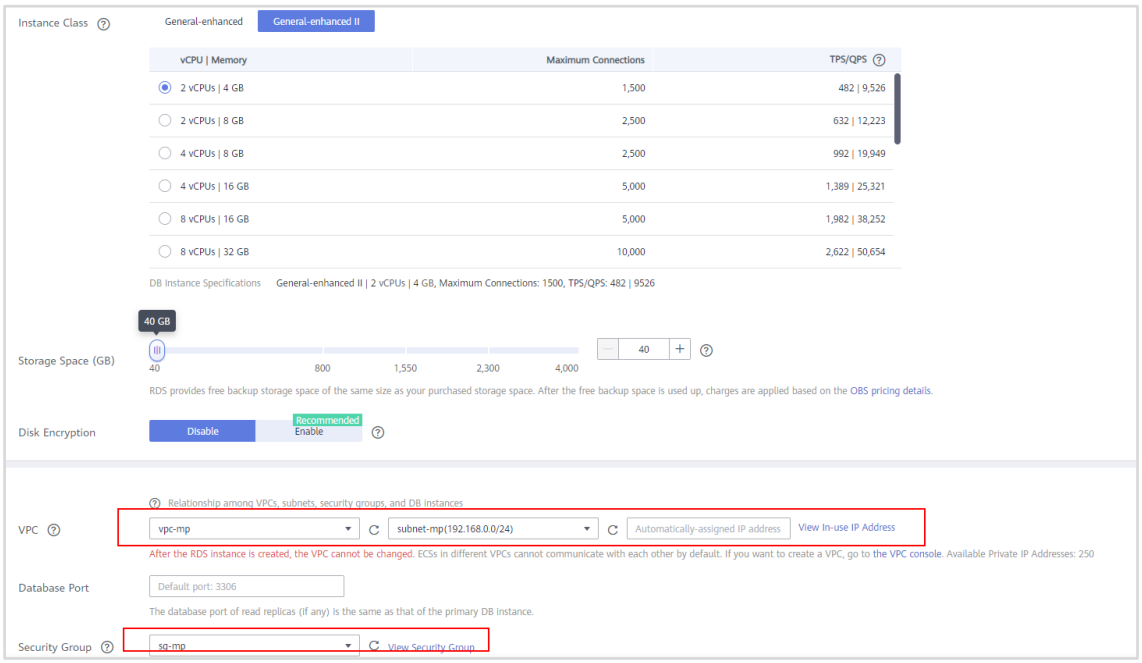


Figure 6-20 Configuring a DB instance

Figure 6-21 Confirmation

Step 4 Confirm the configuration, and click **Submit**. Go to the RDS DB instance list, and wait for the creation to complete, which takes 6 to 10 minutes.

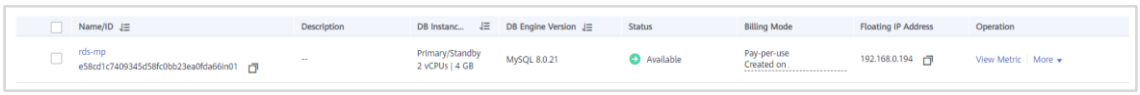


Figure 6-22 Viewing the DB instance

Step 5 Click the DB instance name to view its floating IP address.

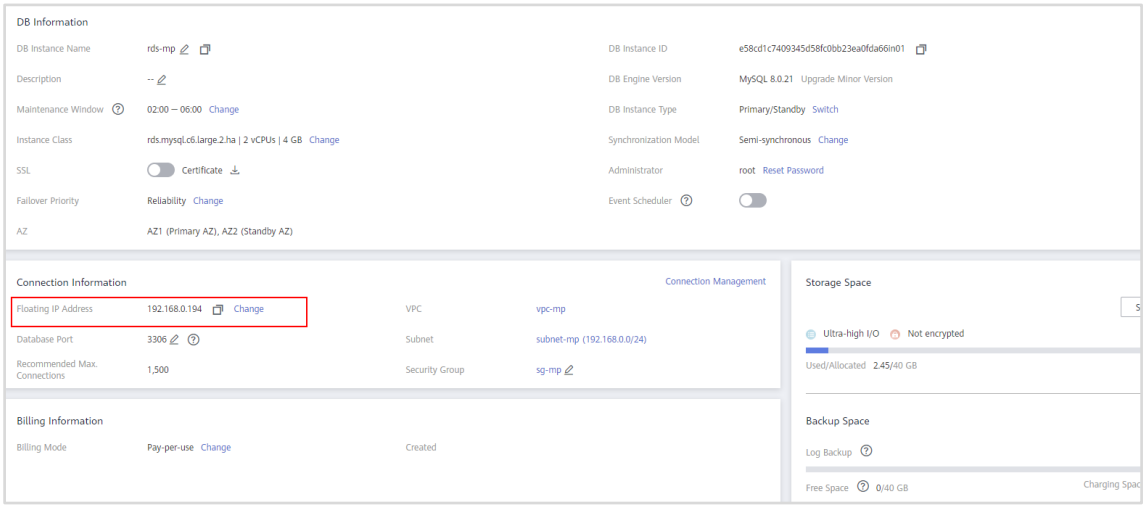


Figure 6-23 Viewing the floating IP address of the DB instance

6.4 Setting Up the Linux, Apache, MySQL, PHP (LAMP) Environment

6.4.1 Installing LAMP

Step 1 Go back to the ECS console and click **Remote Login** in the **Operation** column of the purchased ECS.

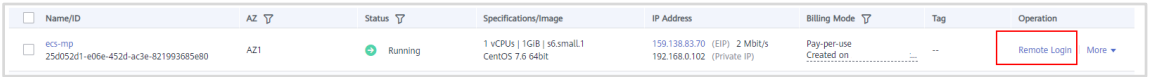


Figure 6-24 Remotely logging in to the ECS

Step 2 In the **VNC** window, enter the username (**root** for Linux ECSs by default) and password for login.

Figure 6-25 Logging in to the Linux ECS

Step 3 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
```

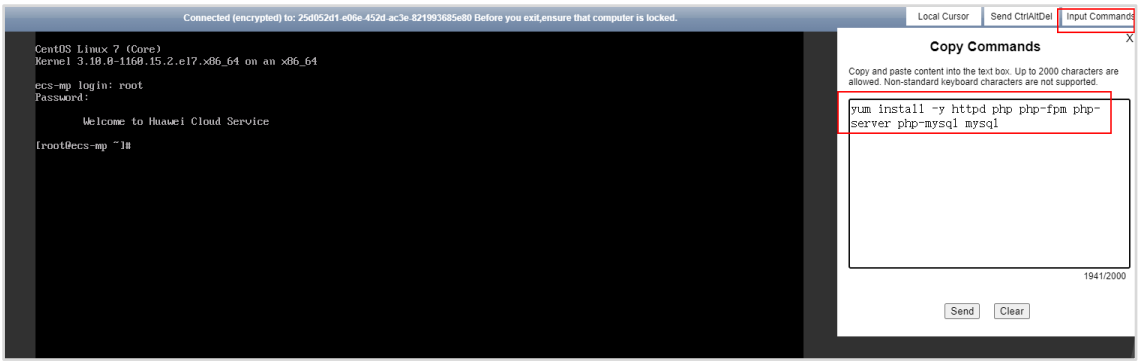


Figure 6-26 Installing LAMP

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

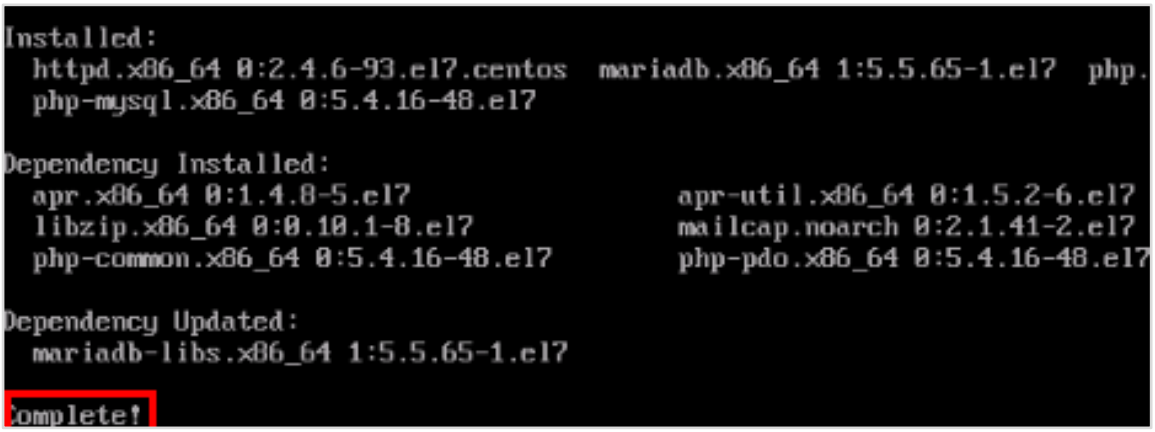


Figure 6-27 Installation succeeded

Step 4 Configure httpd:

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

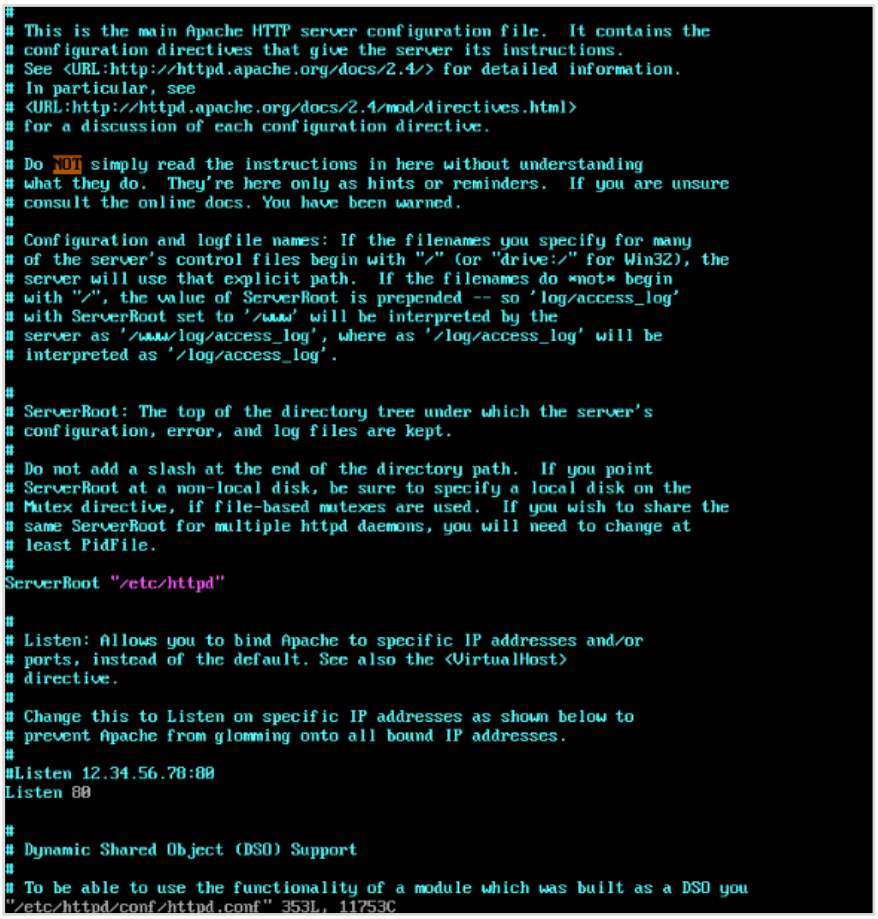


Figure 6-28 Opening the httpd configuration file

Step 5 In the configuration file, press **Shift+G** to go to the last line of the configuration file, press **I** to enter the editing mode, move the cursor to the end of the configuration file, and press **Enter**. Then copy and paste the following content:

```
ServerName localhost:80
```

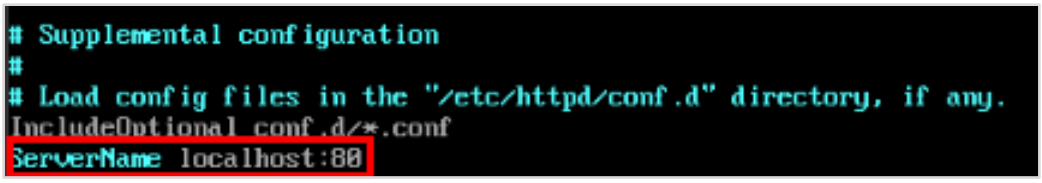


Figure 6-29 Configuring HTTP ports

Step 6 Press **Esc** to exit the editing mode, enter **:wq**, and press **Enter** to save and exit the configuration file.

Figure 6-30 Saving and exiting

Step 7 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.

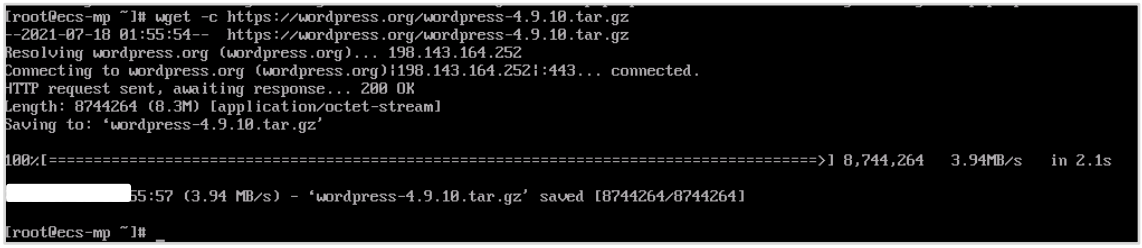


Figure 6-31 Downloading WordPress installation package

Step 8 Run the following command to decompress the WordPress installation package to the **/var/www/html** directory:

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

The command output similar to the following is displayed.

Figure 6-32 Decompressing the WordPress installation package

Step 9 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

Step 10 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

Step 11 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

Step 12 Run the following command to check the httpd status, which should be **active (running)** and highlighted:

```
systemctl status httpd
```

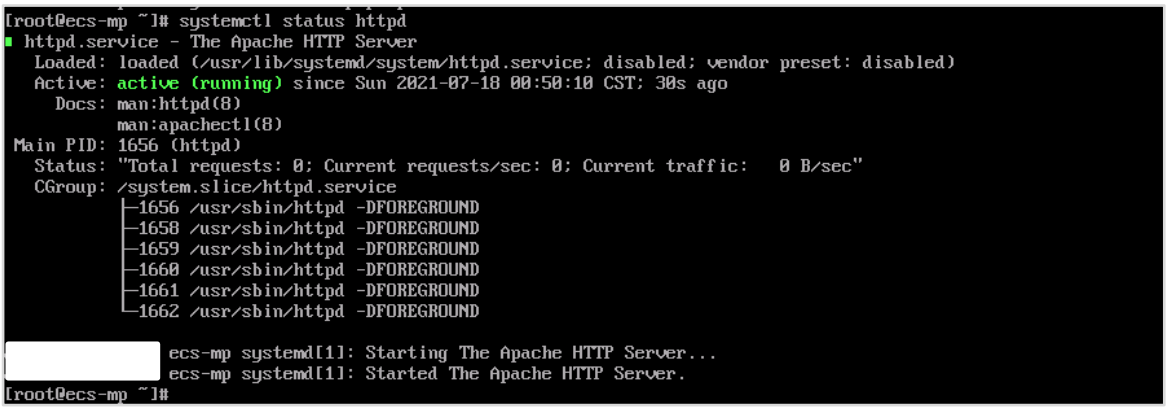


Figure 6-36 Checking the httpd status

Step 13 Run the following command to check the php-fpm status, which should be **active (running)** and highlighted:

```
systemctl status php-fpm
```

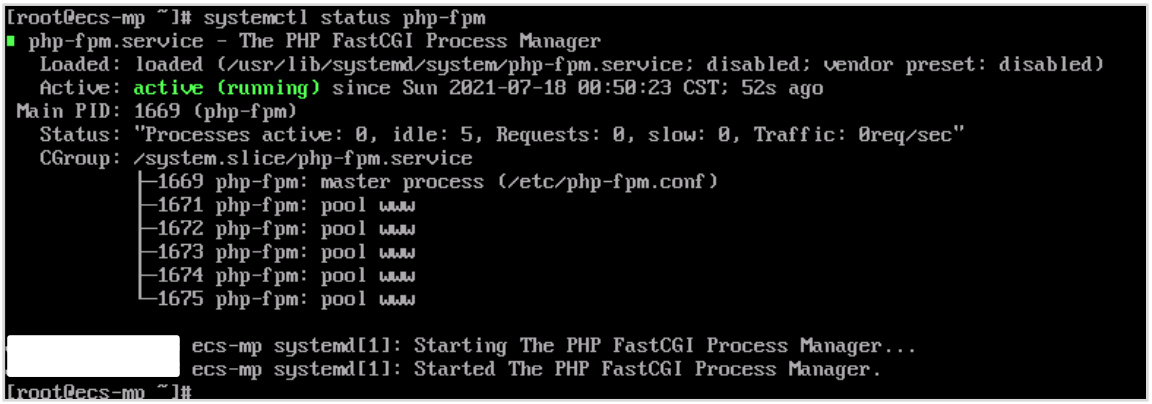


Figure 6-37 Checking the php-fpm status

Step 14 Run the following command to make httpd automatically start at boot. If information similar to what shown in the figure is displayed, httpd has been configured to automatically start at boot.

```
systemctl enable httpd
```

Figure 6-38 Setting httpd to start upon system startup

Step 15 Run the following command to configure php-fpm automatically start upon system boot. If information similar to what shown in the figure is displayed, php-fpm has been configured to automatically start upon system boot.

```
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

Step 16 In the browser, access the EIP bound to the ECS. If the following figure is displayed, LAMP has been installed.

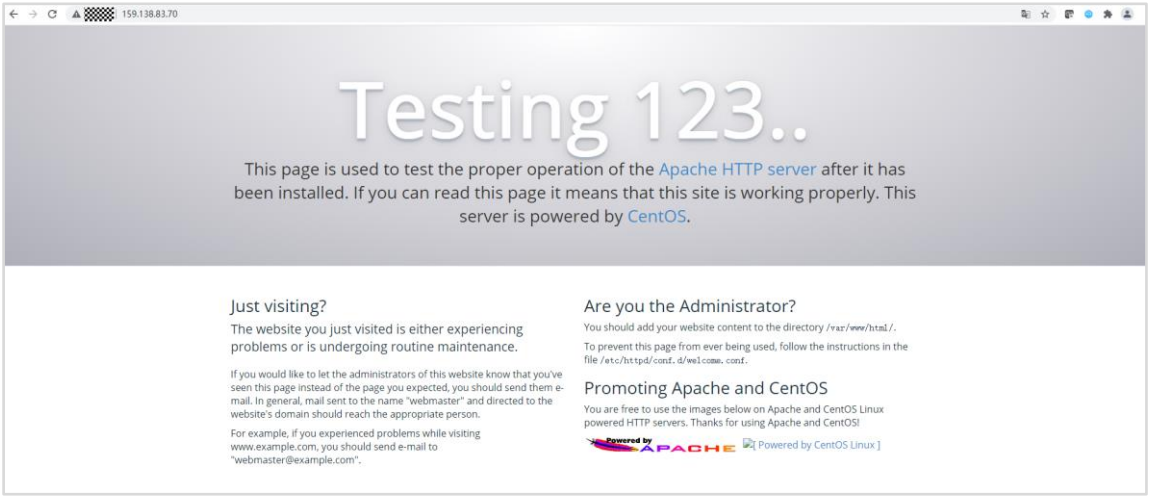


Figure 6-40 Checking environment installation

6.4.2 Creating a Database for WordPress

Step 1 Go back to the RDS console and click **Log In** in the **Operation** column of the created RDS MySQL database instance.

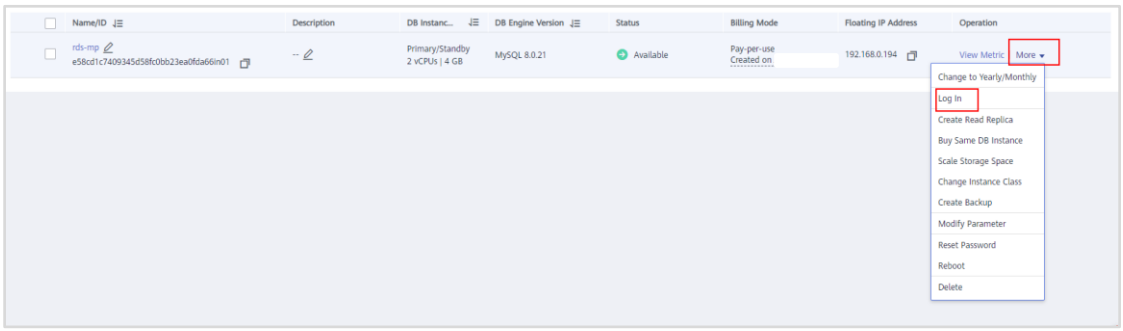


Figure 6-41 Logging in to the DB instance

Step 2 Enter the username (**root** by default) and password (you set when purchasing the RDS instance). Select **Remember Password**, enable **Collect Metadata Periodically** and **Show Executed SQL Statements**. If the connection test is successful, click **Log In**.

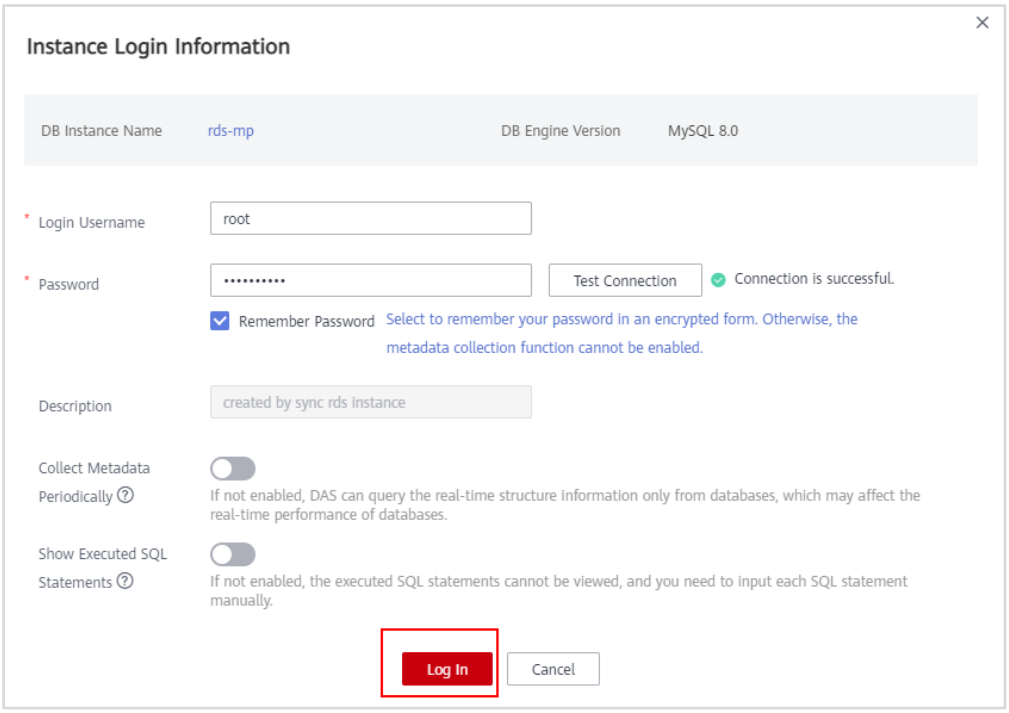


Figure 6-42 Instance Login information

Step 3 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**.

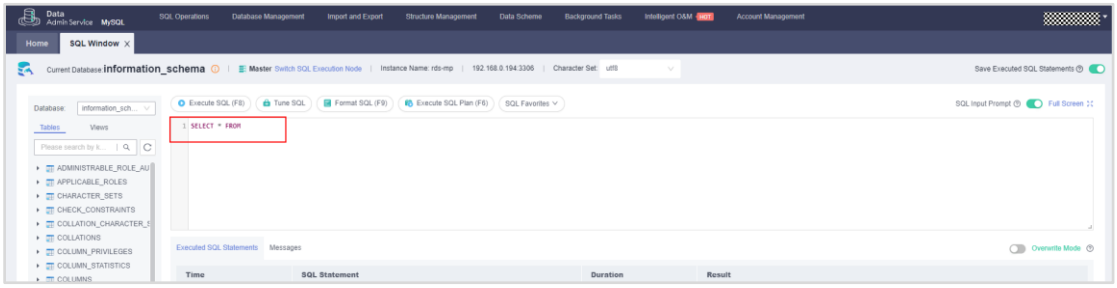


Figure 6-43 Selecting SQL Operations

Step 4 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
```

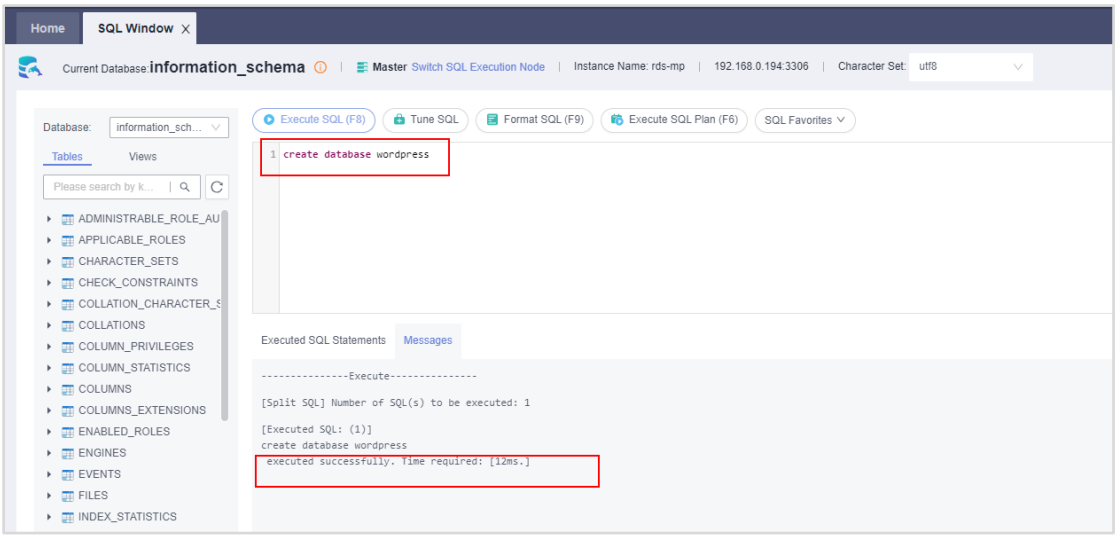


Figure 6-44 Creating a database

6.4.3 Installing WordPress

Step 1 In the address box of the browser, enter **http://***ECS EIP*/**wordpress** to access the WordPress installation wizard.

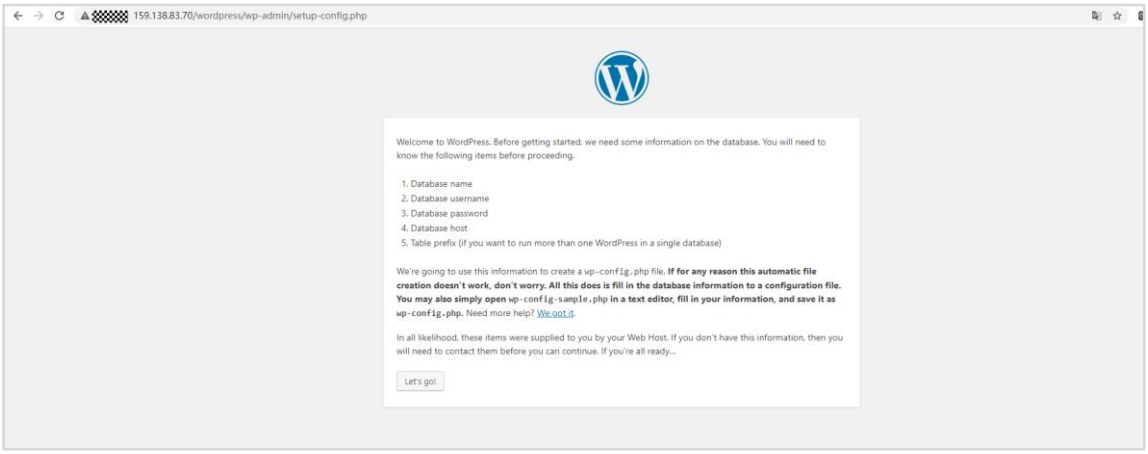


Figure 6-45 Opening the WordPress installation wizard

Step 2 Click **Let's go!**. in the displayed page, enter the database access information, and click **Submit**.

- **Database Name**: **wordpress**
- **Username**: **root**
- **Password**: Enter the password you set.
- **Database Host**: Enter the database floating IP address and port number obtained in step 4 of section Buying an RDS DB Instance.
- **Table Prefix**: Retain the default settings.

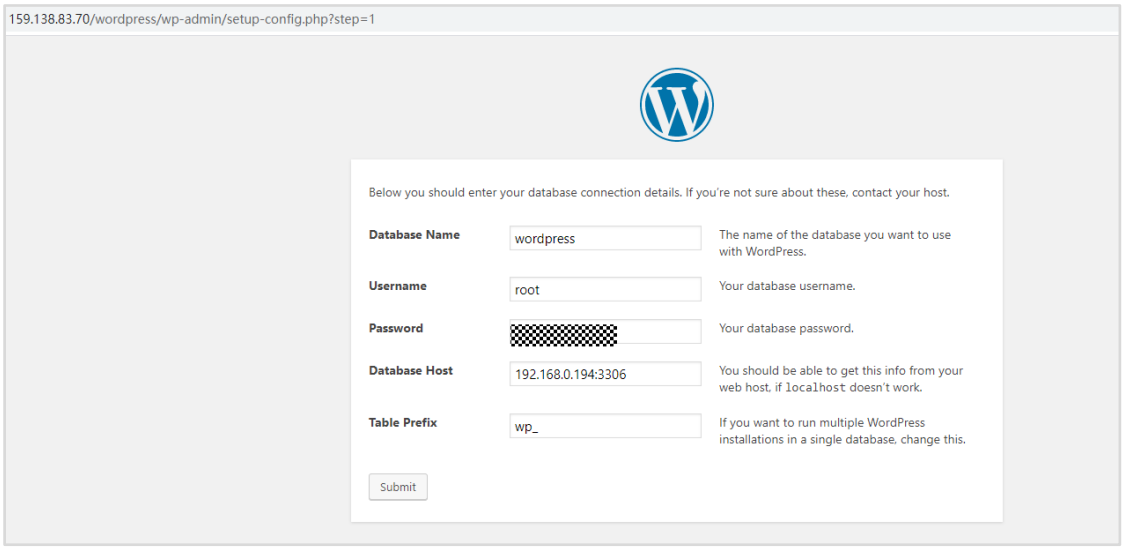


Figure 6-46 Configuring the connection between WordPress and the database

- Click **Run the installation**.

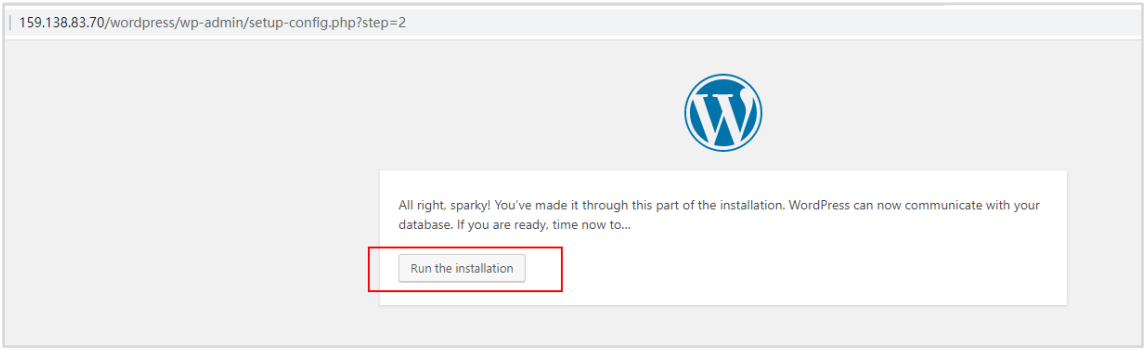


Figure 6-47 Run the installation

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

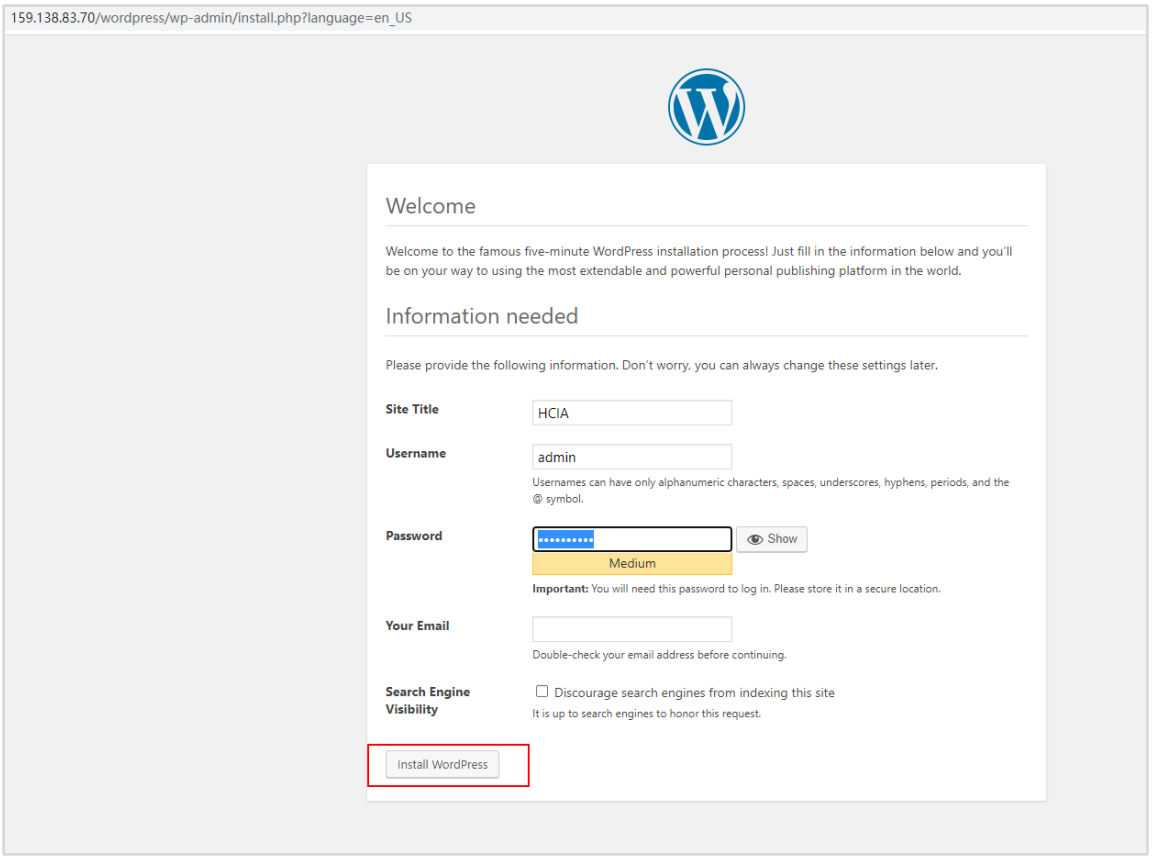


Figure 6-48 Install WordPress

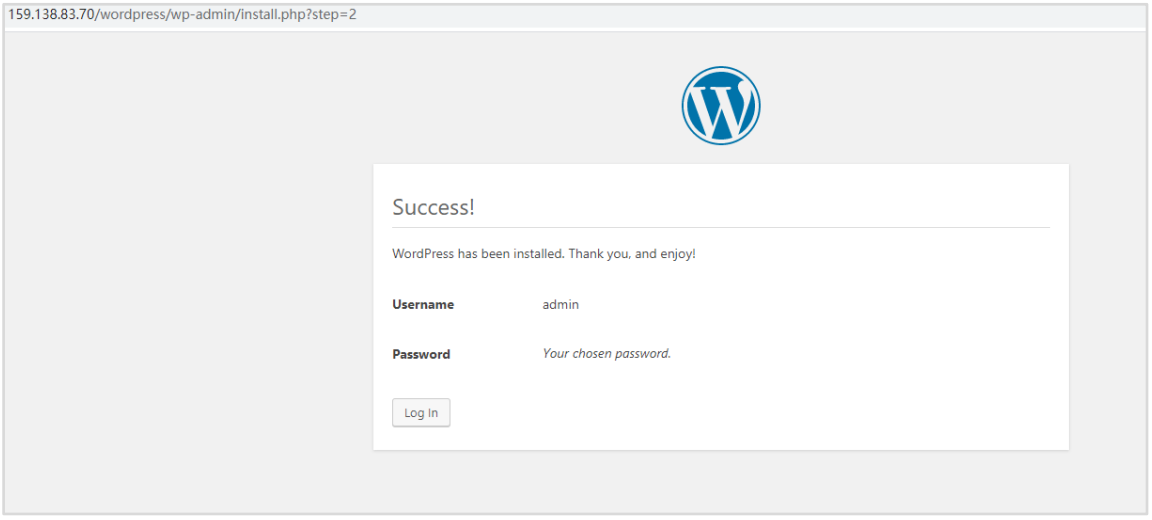


Figure 6-49 Installation succeeded

Step 3 Enter the user name and password on the displayed login page. Then, click **Log In**.

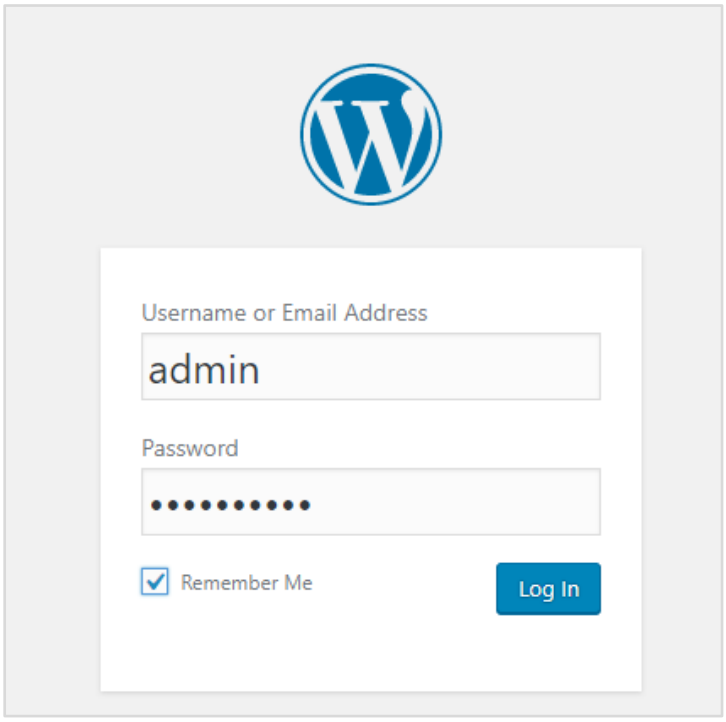


Figure 6-50 Logging in

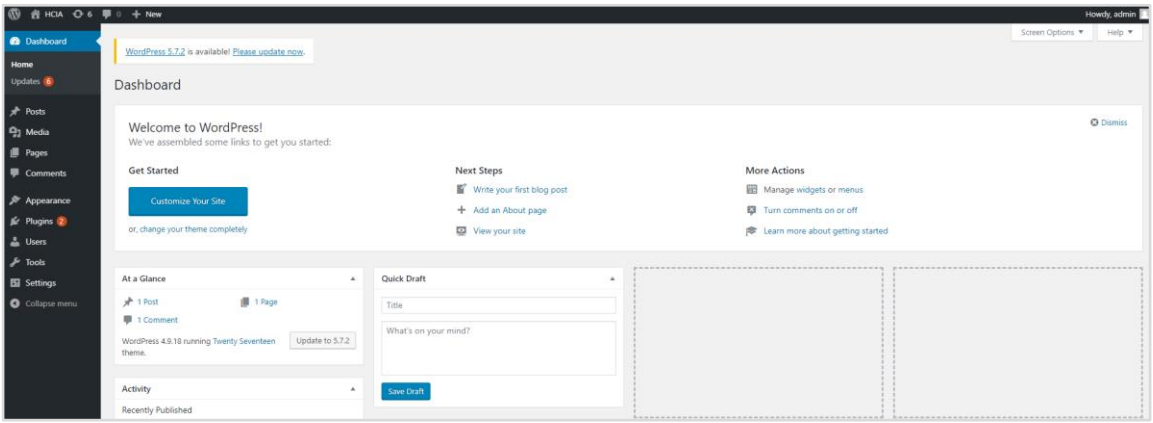


Figure 6-51 Login succeeded

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

Step 1 On the management console, hover on the upper left to display **Service List** and choose **Networking** > **Elastic Load Balance**.

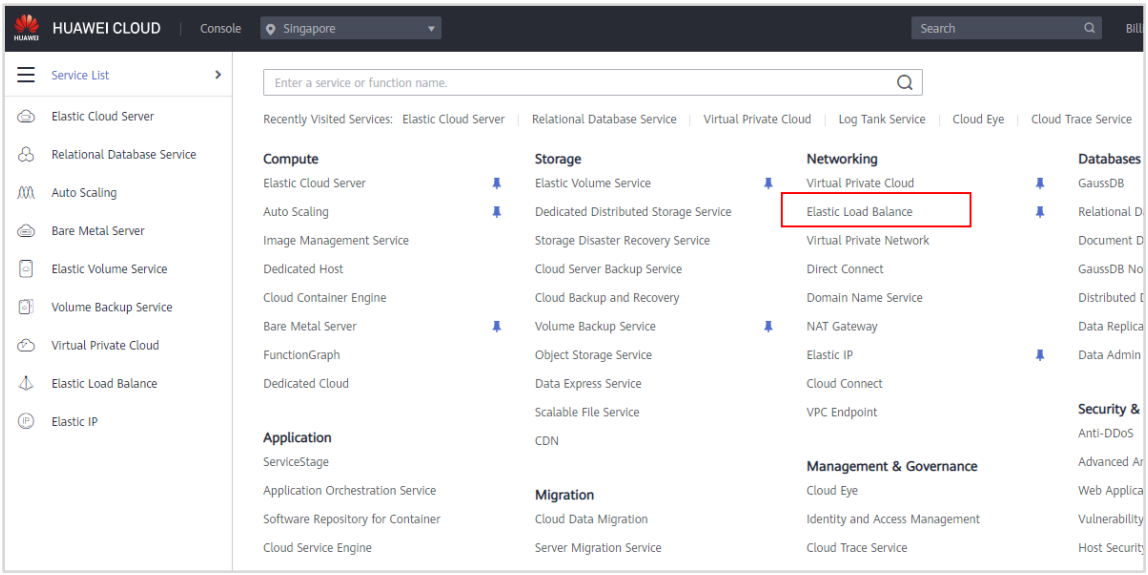


Figure 6-52 Accessing Elastic Load Balance

Step 2 Click **Buy Elastic Load Balancer**.

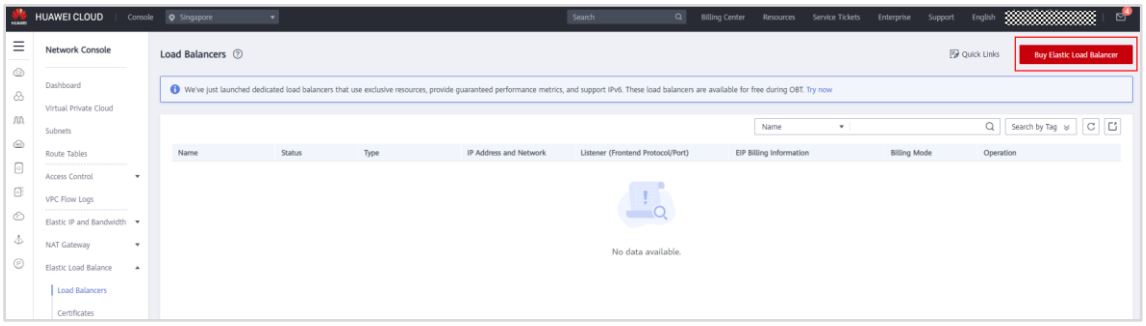


Figure 6-53 Buy Elastic Load Balancer

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

- **Type**: **Shared**
- **Region**: **AP-Singapore**
- **Network type**: **Public network**
- **VPC**: the VPC and subnet you created
- **EIP**: **New EIP**, **Dynamic BGP**, **2 Mbit/s**
- **Name**: **elb-mp** (Change it as needed.)

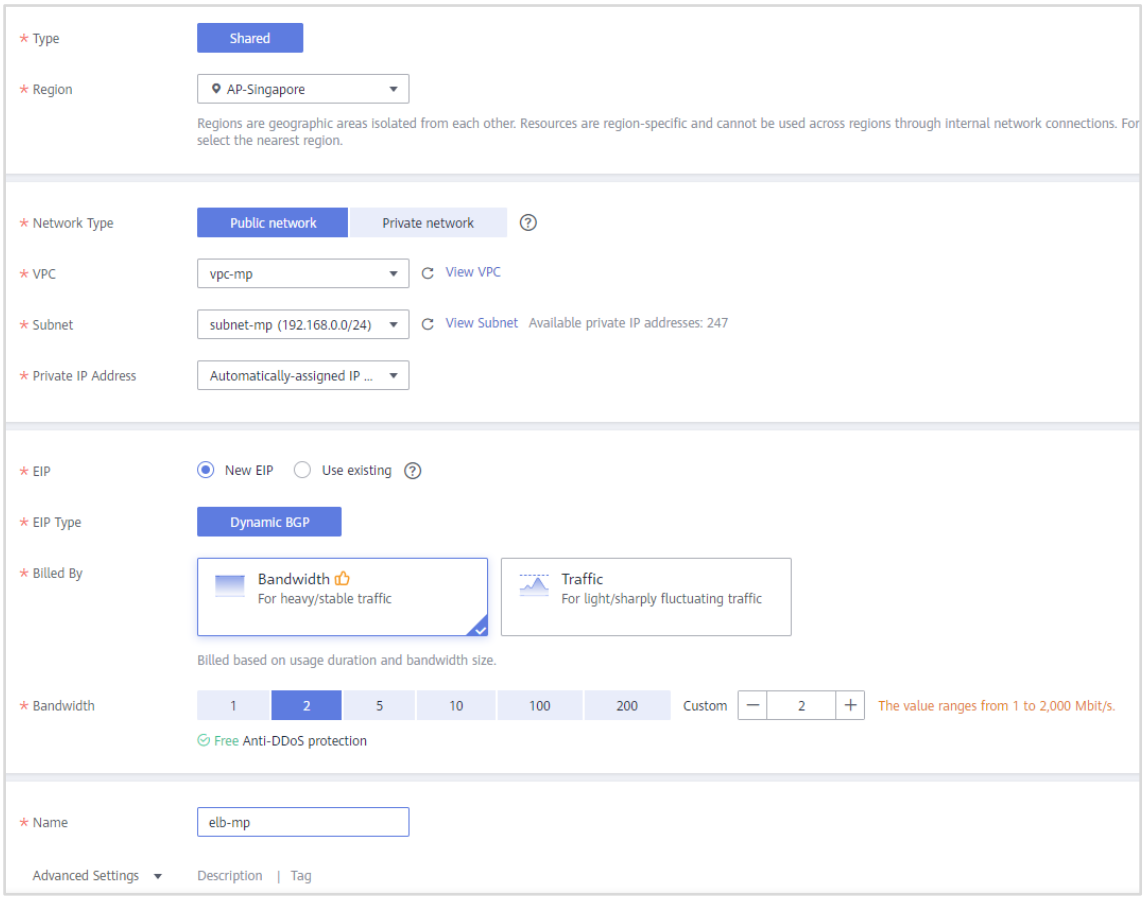
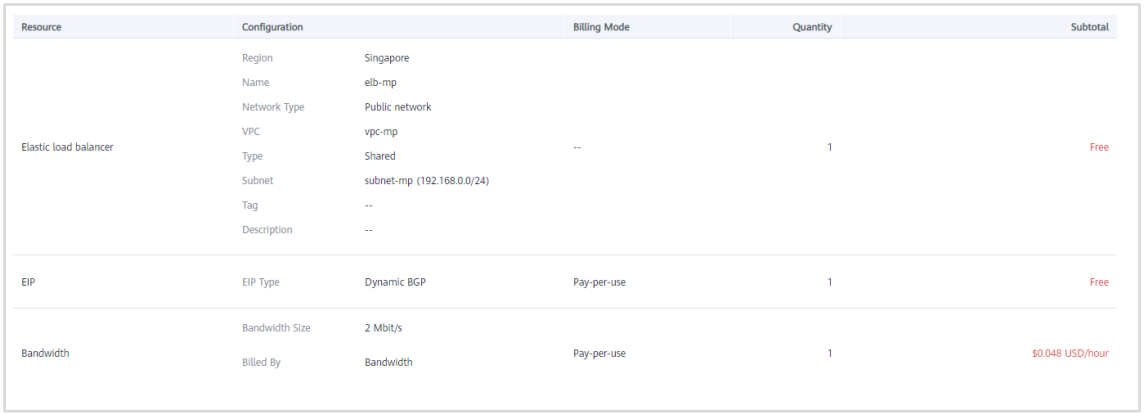


Figure 6-54 Configuring parameters

Step 4 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	--			
	Description	--			
EIP	EIP Type	Dynamic BGP	Pay-per-use	1	Free
Bandwidth	Bandwidth Size	2 Mbit/s	Pay-per-use	1	$0.048 USD/hour
	Billed By	Bandwidth			

Figure 6-55 Confirming the configuration

Step 5 Go back to the load balancer list and ensure that the load balancer is in the **Running** state.

Figure 6-56 Viewing the load balancer

Step 6 Click the name of the load balancer. Under **Listeners**, click **Add Listener**. Configure the name, protocol, and port for the listener.

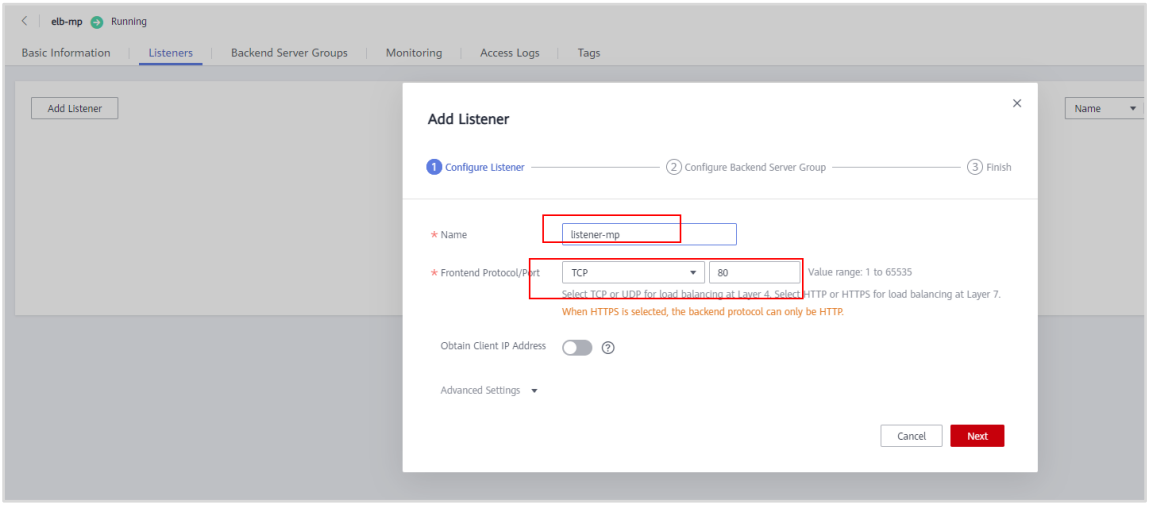


Figure 6-57 Adding a listener

Step 7 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.

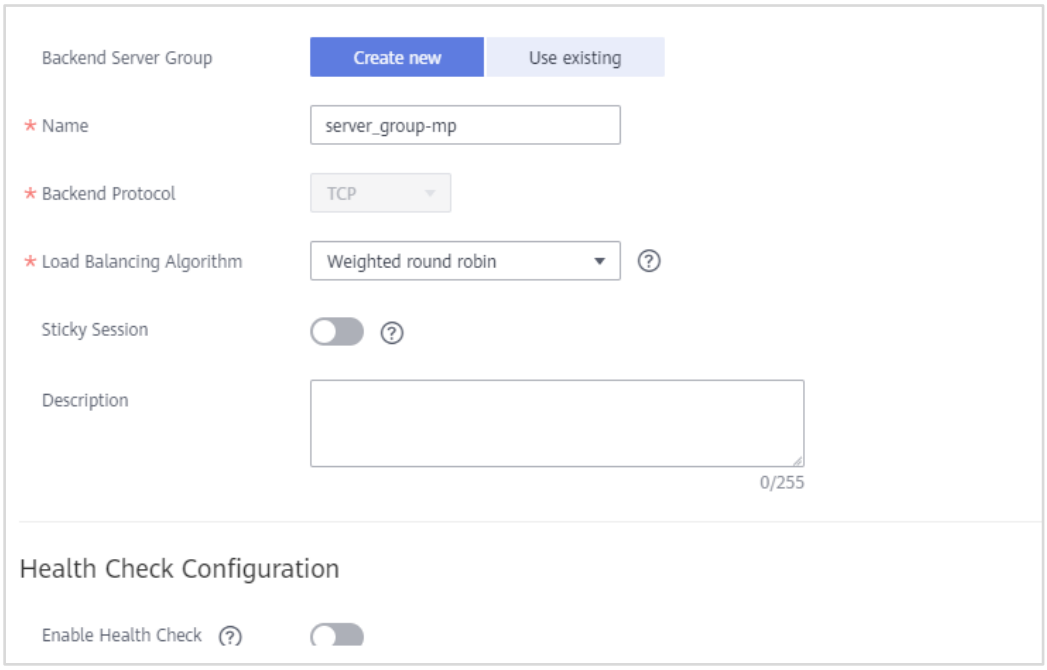


Figure 6-58 Configuring a backend server group

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

Step 1 Go back to the ECS console, locate the ECS you created, and choose **More** > **Stop** in the **Operation** column.

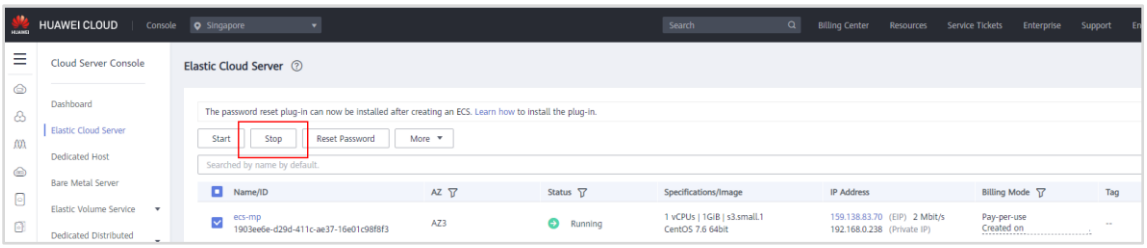


Figure 6-59 Stopping the ECS

Step 2 Go back to the service list. Under **Compute**, click **Image Management Service**.

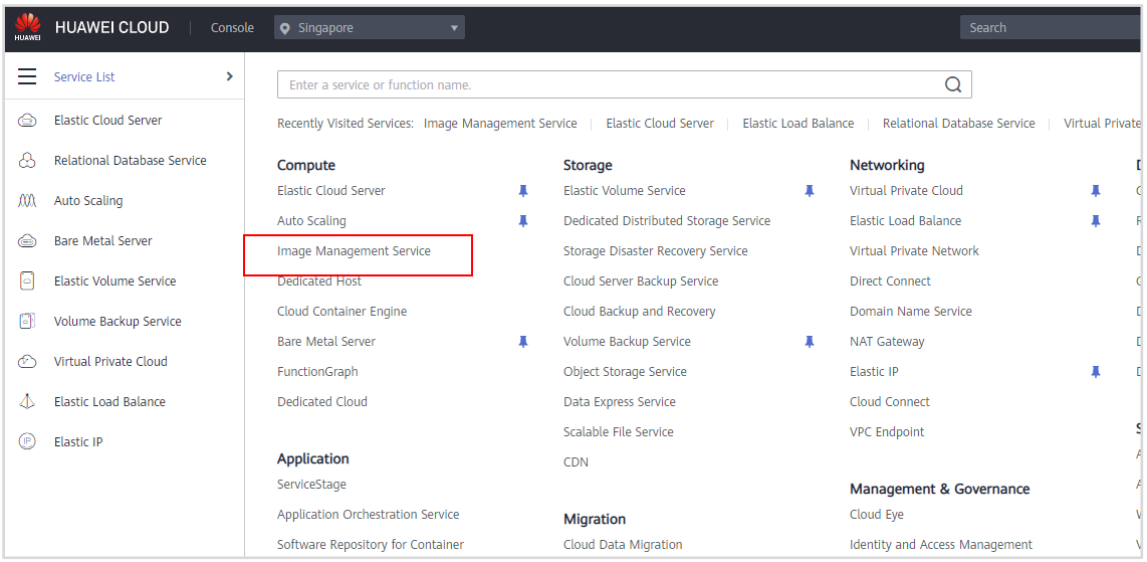


Figure 6-60 Accessing Image Management Service

Step 3 Click **Create Image** and configure the parameters as follows:

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

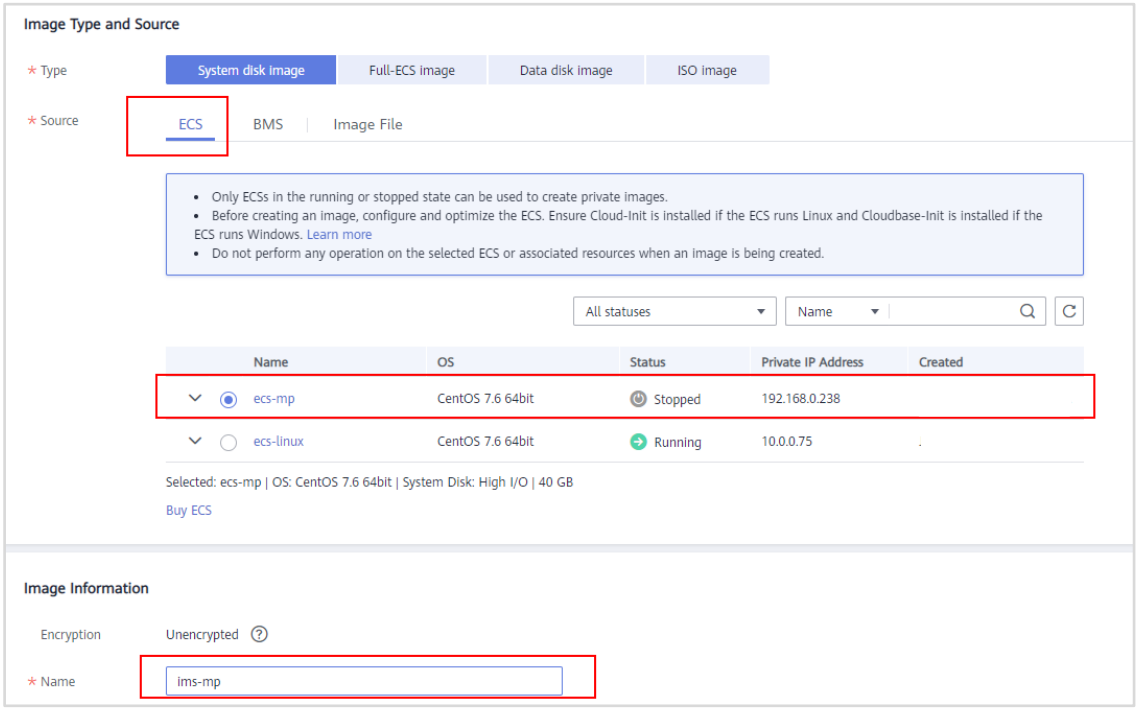


Figure 6-61 Configuring parameters

Step 4 Click **Next**, confirm the configuration, and click **Submit**.

Step 5 Wait until the image status becomes **Normal**. Then, switch back to the ECS console, and start the ECS.

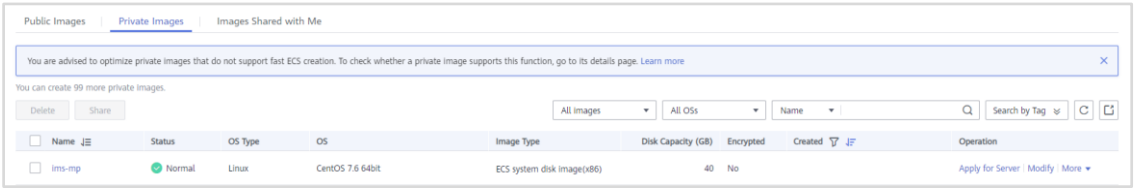


Figure 6-62 Viewing the created image

6.5.3 Configuring AS

Step 1 Go back to the service list. Under **Compute**, click **Auto Scaling**.

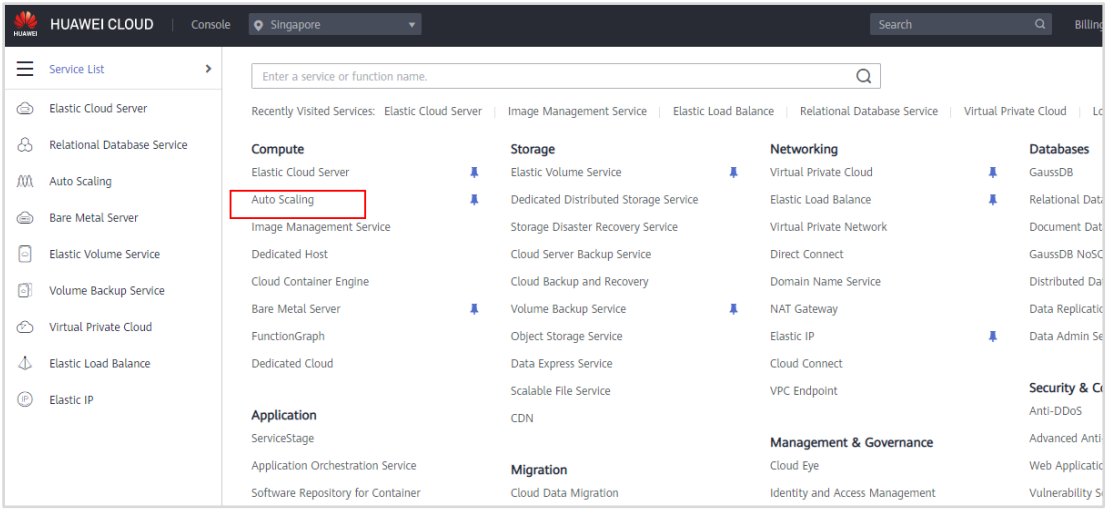


Figure 6-63 Accessing Auto Scaling

Step 2 Click **Create AS Configuration**.

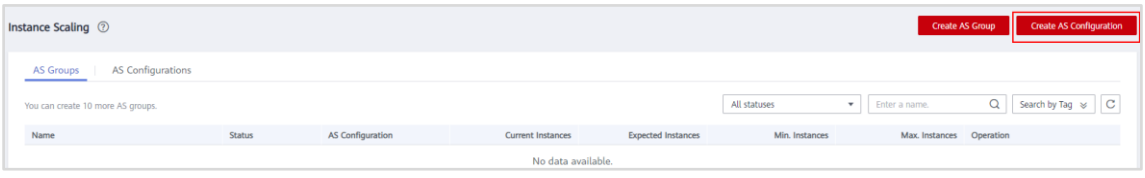


Figure 6-64 Create AS Configuration

Step 3 Configure the parameters as shown in the following figures and then click **Create Now**.

Select the system disk image and security group you just created and set **EIP** to **Do not use**.

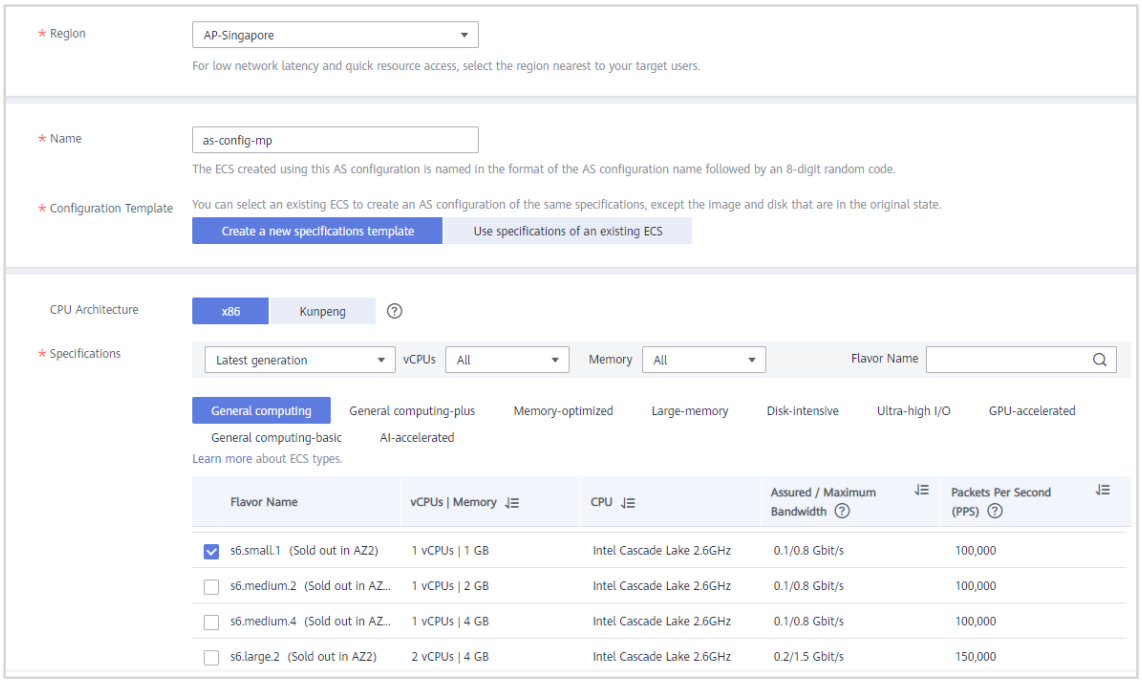


Figure 6-65 Configuring parameters

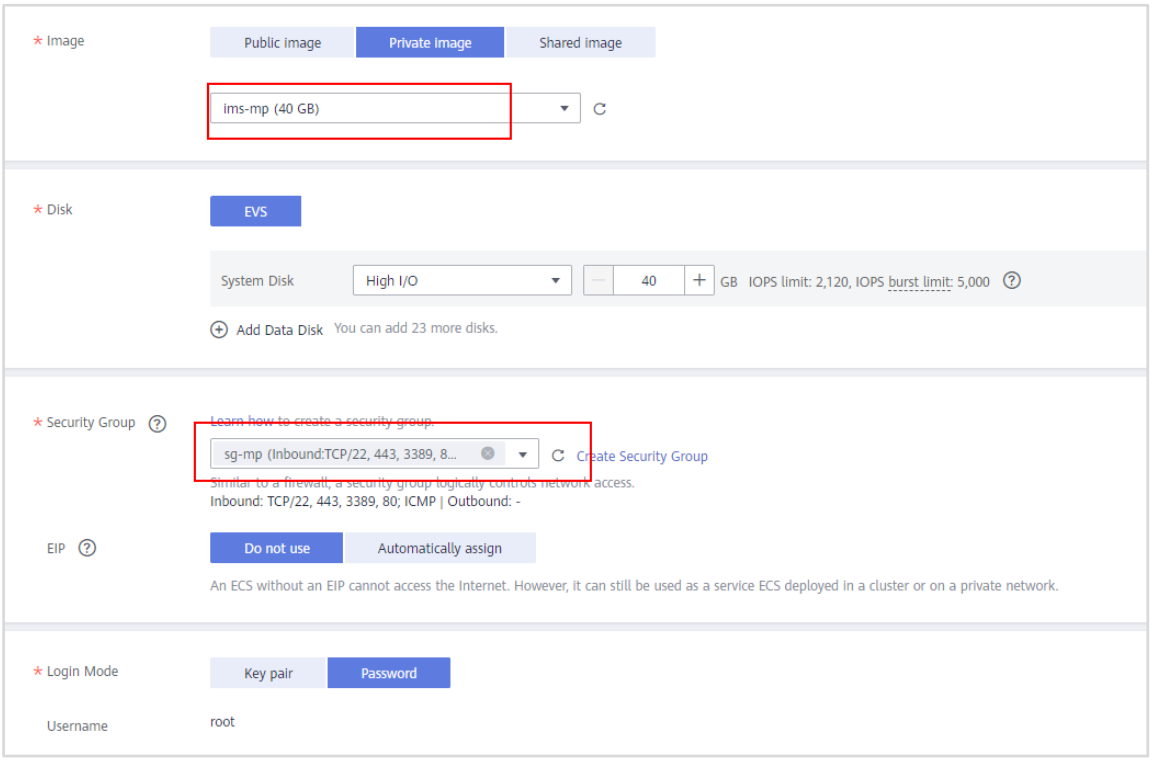


Figure 6-66 Configuring parameters

Step 4 View the created AS configuration.

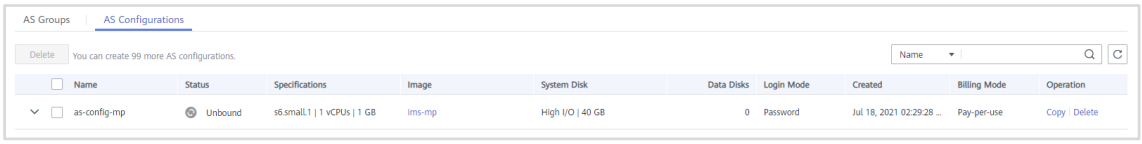


Figure 6-67 Viewing the AS configuration

Step 5 Click **Create AS Group**.

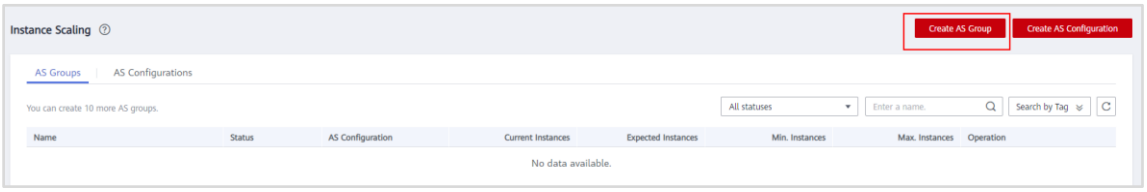


Figure 6-68 Create AS Group

Step 6 Configure the parameters as shown in the following figure.

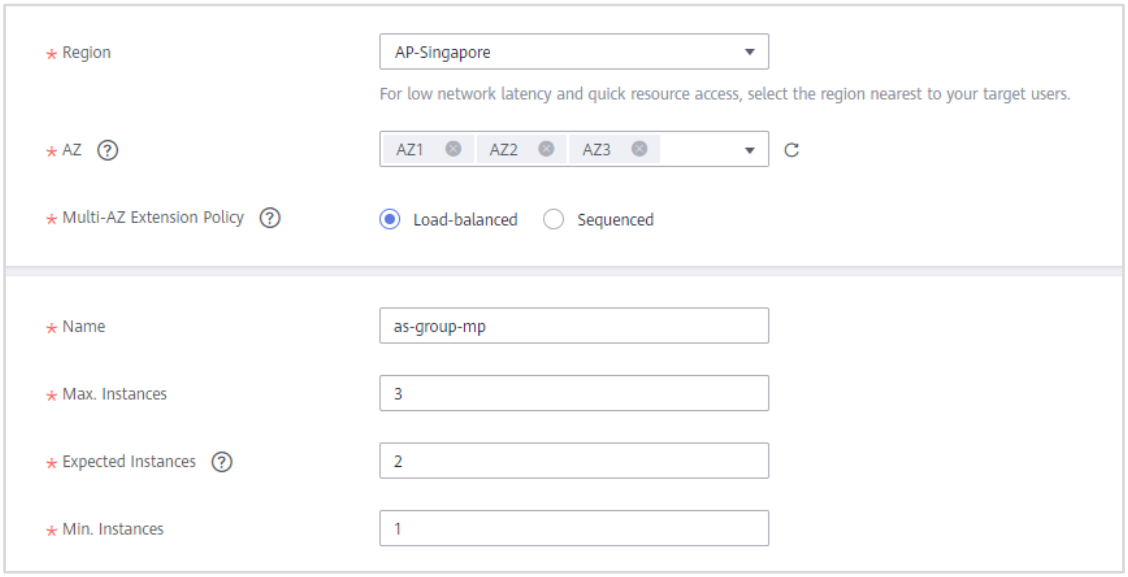


Figure 6-69 Configuring parameters

Step 7 Select the AS configuration and load balancer you just created. AS will dynamically adjust the number of ECSs in the backend server group using the image configured or used in the AS configuration.

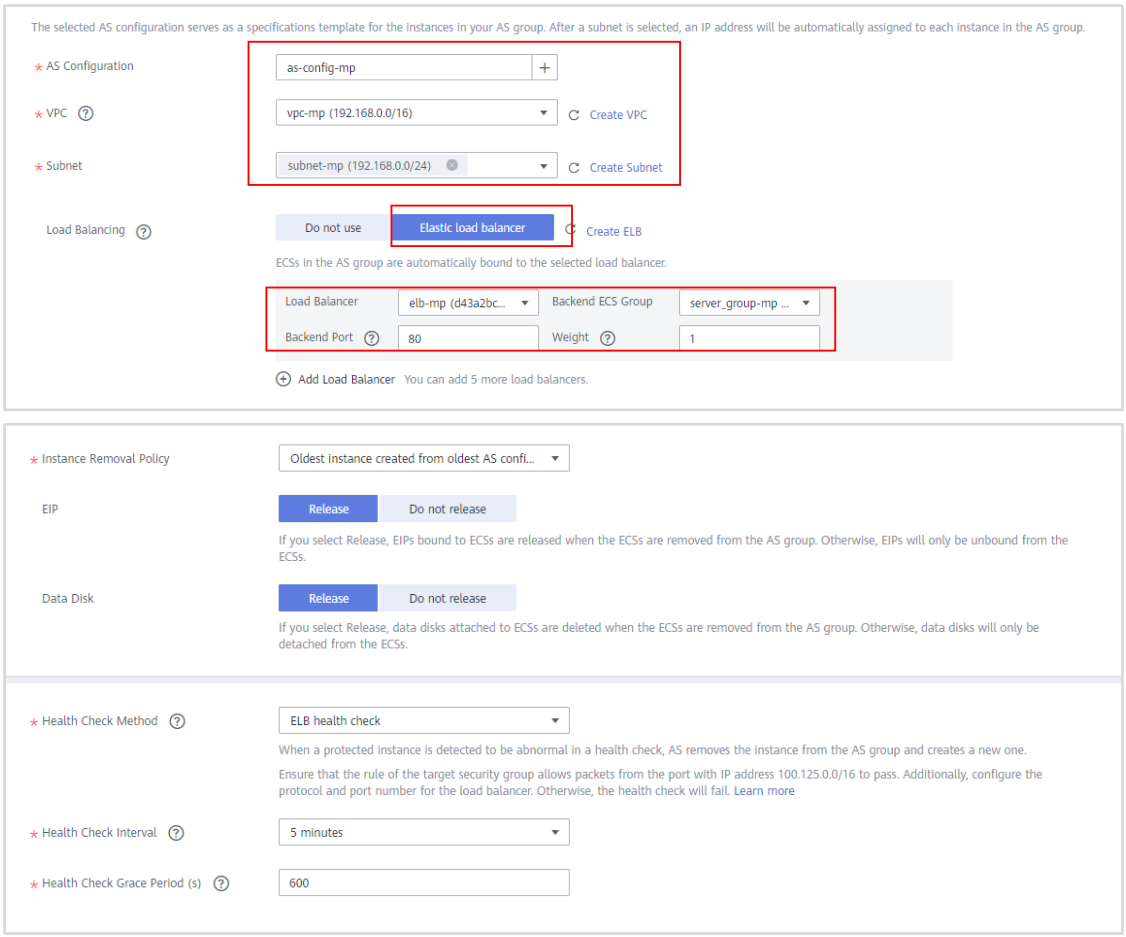


Figure 6-70 Configuring parameters

Step 8 Locate the AS group you created and click **View AS Policy** in the **Operation** column.

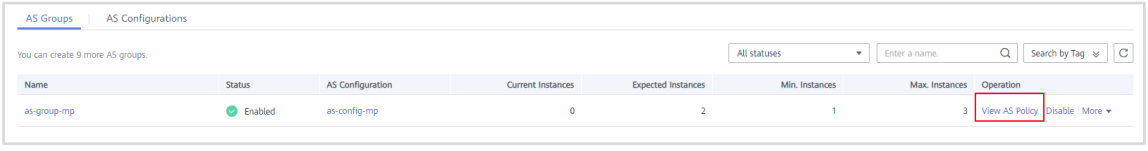


Figure 6-71 View AS Policy

Step 9 Under AS Policies, click **Add AS Policy**.

- **Trigger Condition**: **CPU Usage**, **Max.**, **>=**, **60**. **Scaling Action**: **Add**, **1**, **instances**
- **Trigger Condition**: **CPU Usage**, **Avg.**, **<=**, **20**. **Scaling Action**: **Reduce**, **1**, **instances**

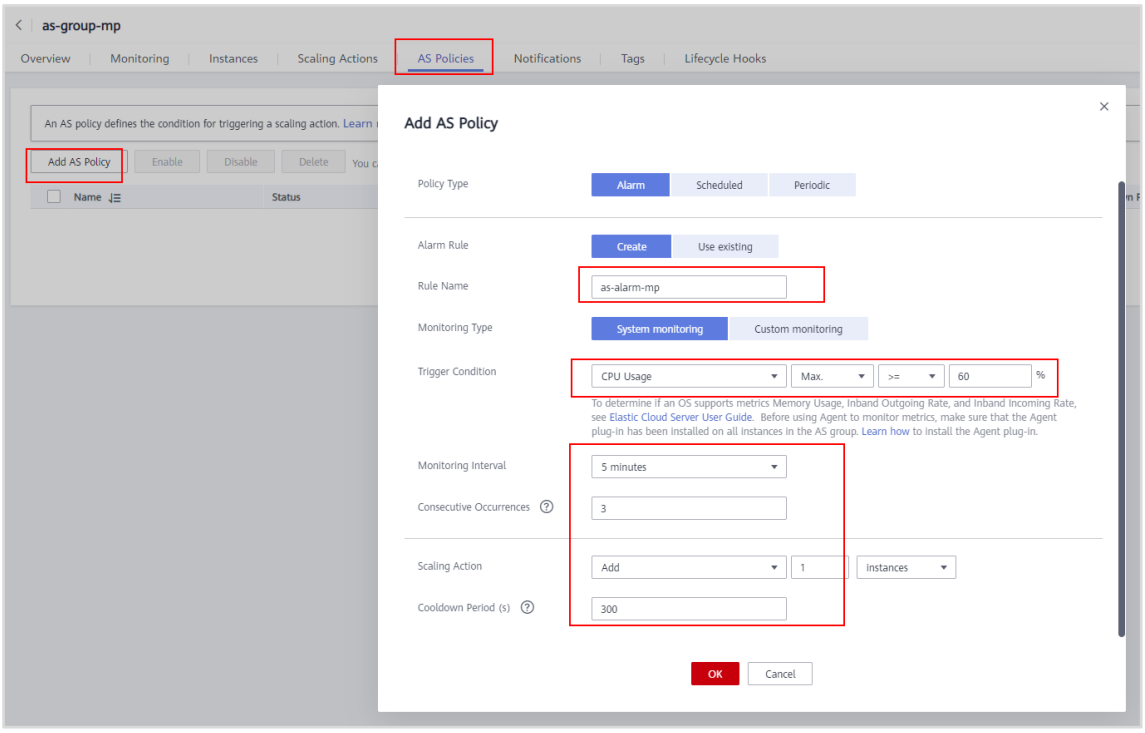


Figure 6-72 Add AS policy

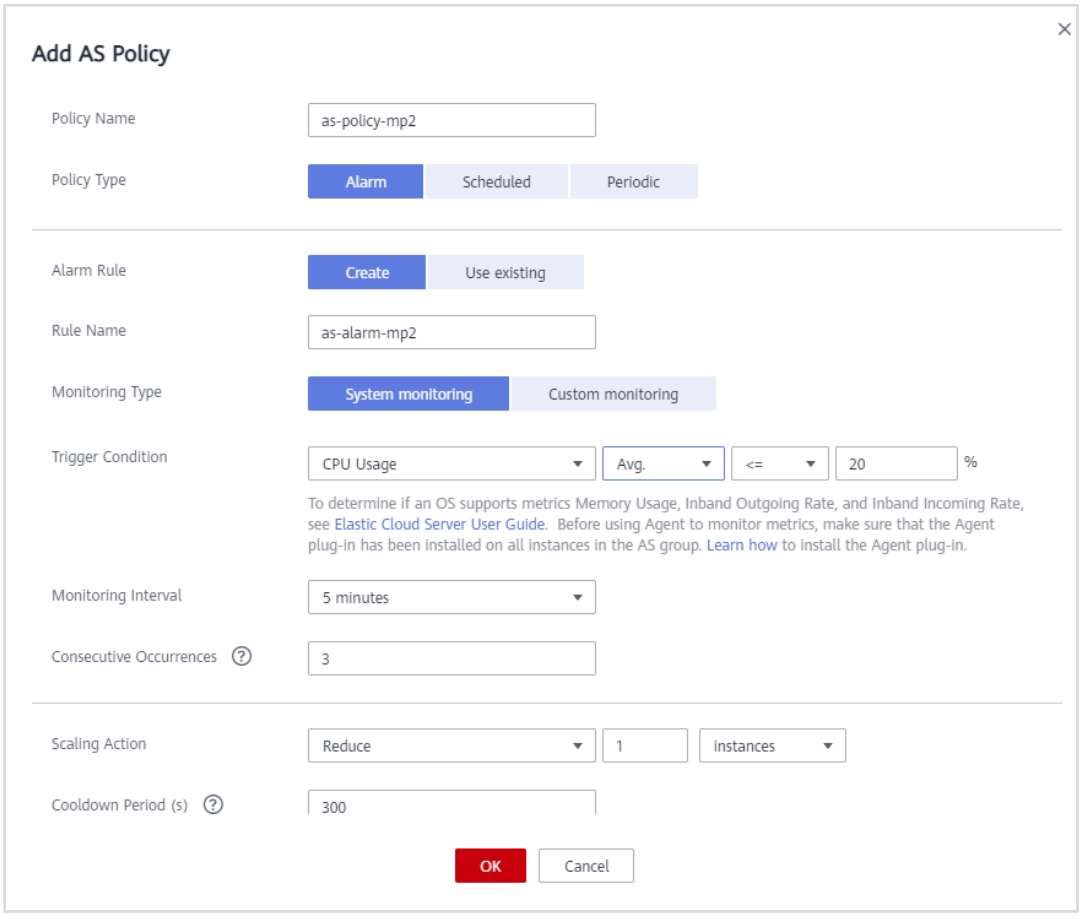


Figure 6-73 Adding an AS policy

Step 10 Wait for about 2 minutes and check whether the AS policy has taken effect. As we can see in the following figure, two ECSs have been added to the AS group. The AS policy has taken effect.

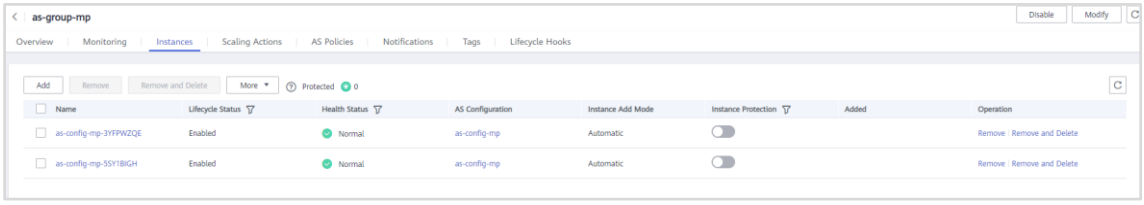


Figure 6-74 Viewing instance changes

Step 11 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.

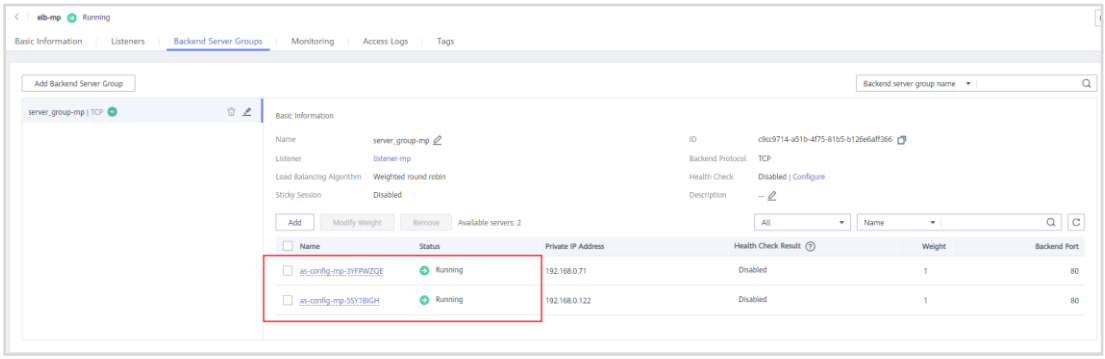


Figure 6-75 Viewing the backend server group

Step 12 Verify that web servers where the website is deployed can be accessed using the EIP bound to the load balancer. We have finished configuring AS and verified that AS can dynamically adjust the number of ECSs in the backend server group associated with the load balancer based on the configured AS policy.

6.6 Visiting the Website

Step 1 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

Step 2 Check whether the website can be accessed. If the website can be accessed, web servers where the website is deployed can provide Internet-accessible services using the load balancer's EIP.

6.7 Monitoring Resources

Step 1 On the service list page, choose **Management & Governance** > **Cloud Eye**.

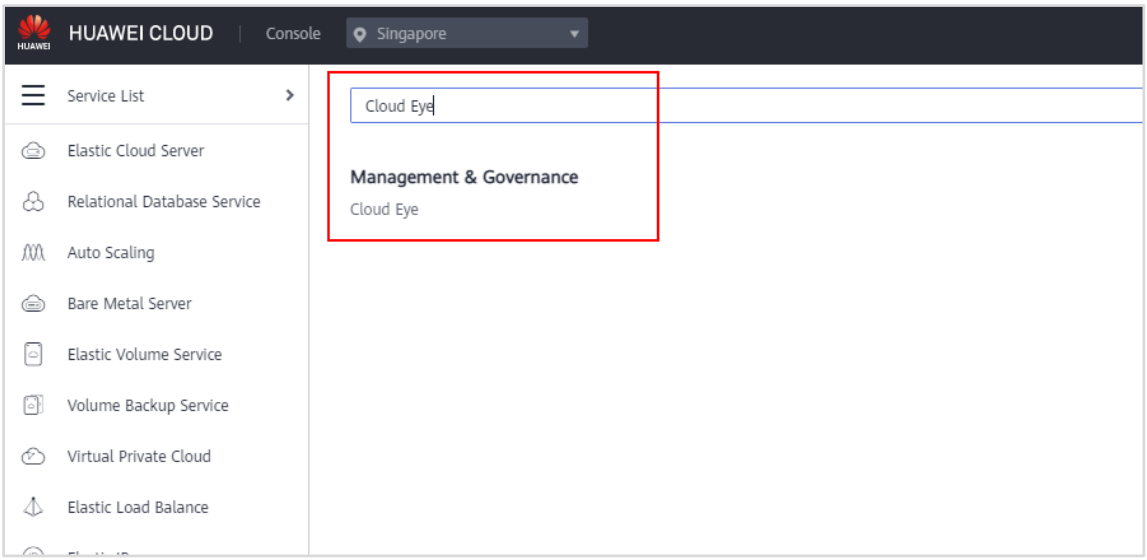


Figure 6-77 Accessing Cloud Eye

Step 2 On the **Overview** page, view overall resource information and alarm statistics.

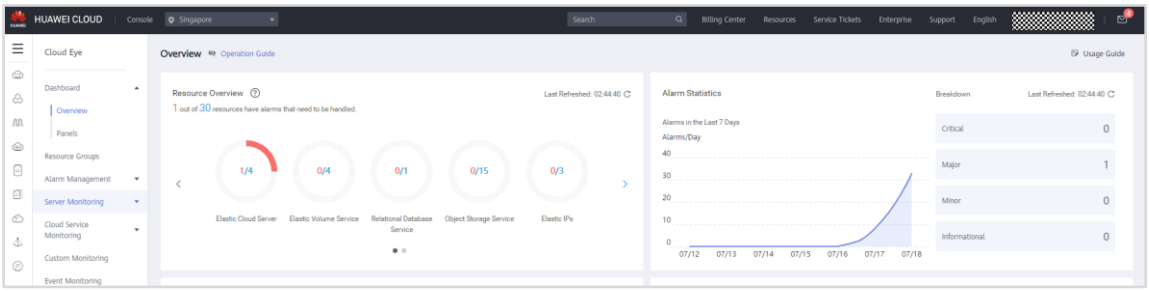


Figure 6-78 Resource Overview

Step 3 In the left navigation pane, choose **Alarm Management** > **Alarm History**. View service alarms and handle any faults in a timely manner.

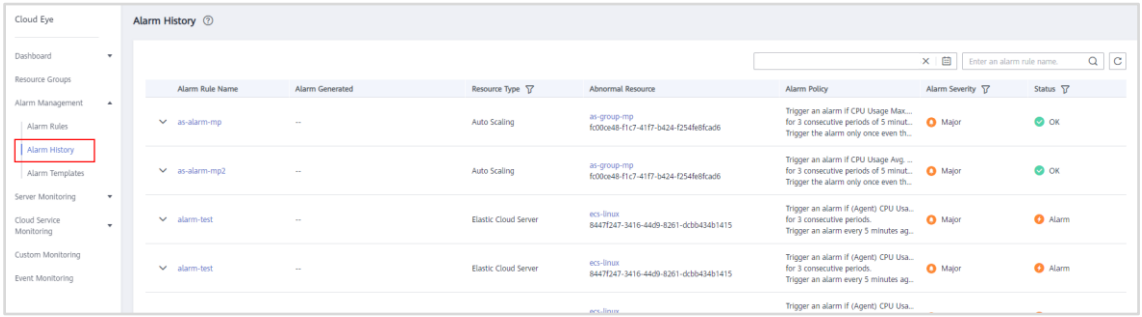


Figure 6-79 Viewing alarm history

Step 4 In the left navigation pane, choose **Server Monitoring** > **Elastic Cloud Server** and then view ECS monitoring information.

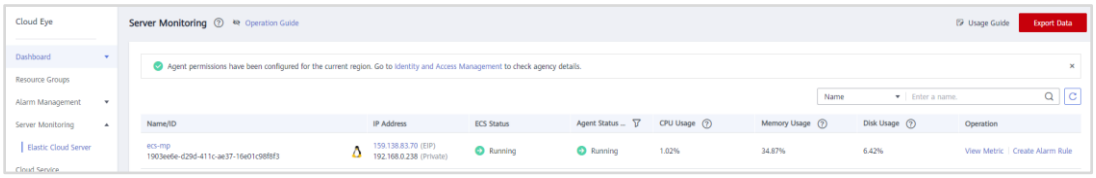


Figure 6-80 Server Monitoring

Step 5 Click the name of an ECS to view its monitoring details.

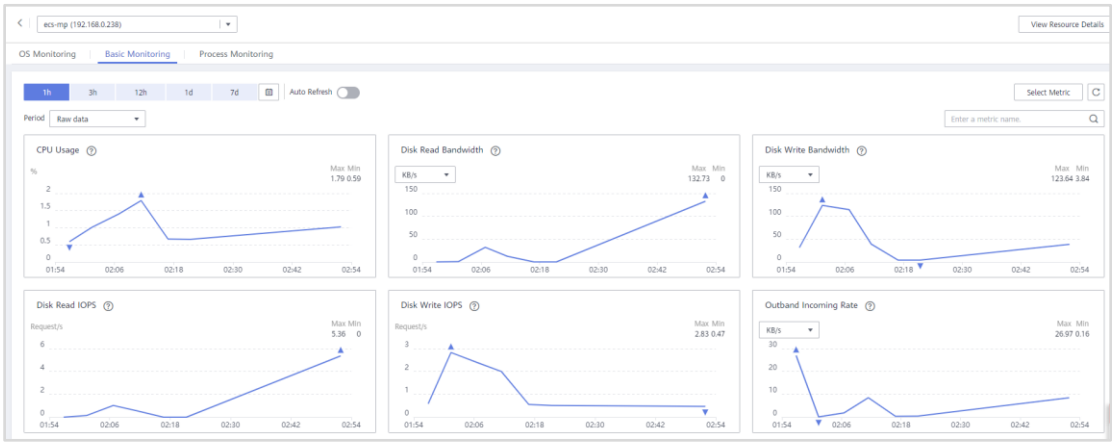


Figure 6-81 Basic Monitoring

6.8 Deleting Resources

6.8.1 Deleting ECSs

Select the ECSs you want to delete and click **Delete**.

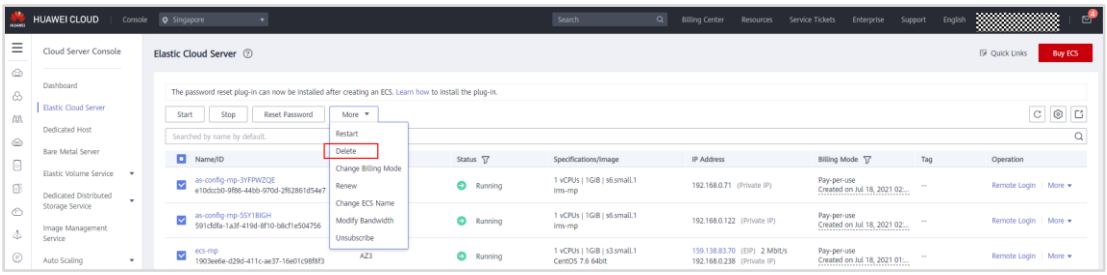


Figure 6-82 Deleting ECSs

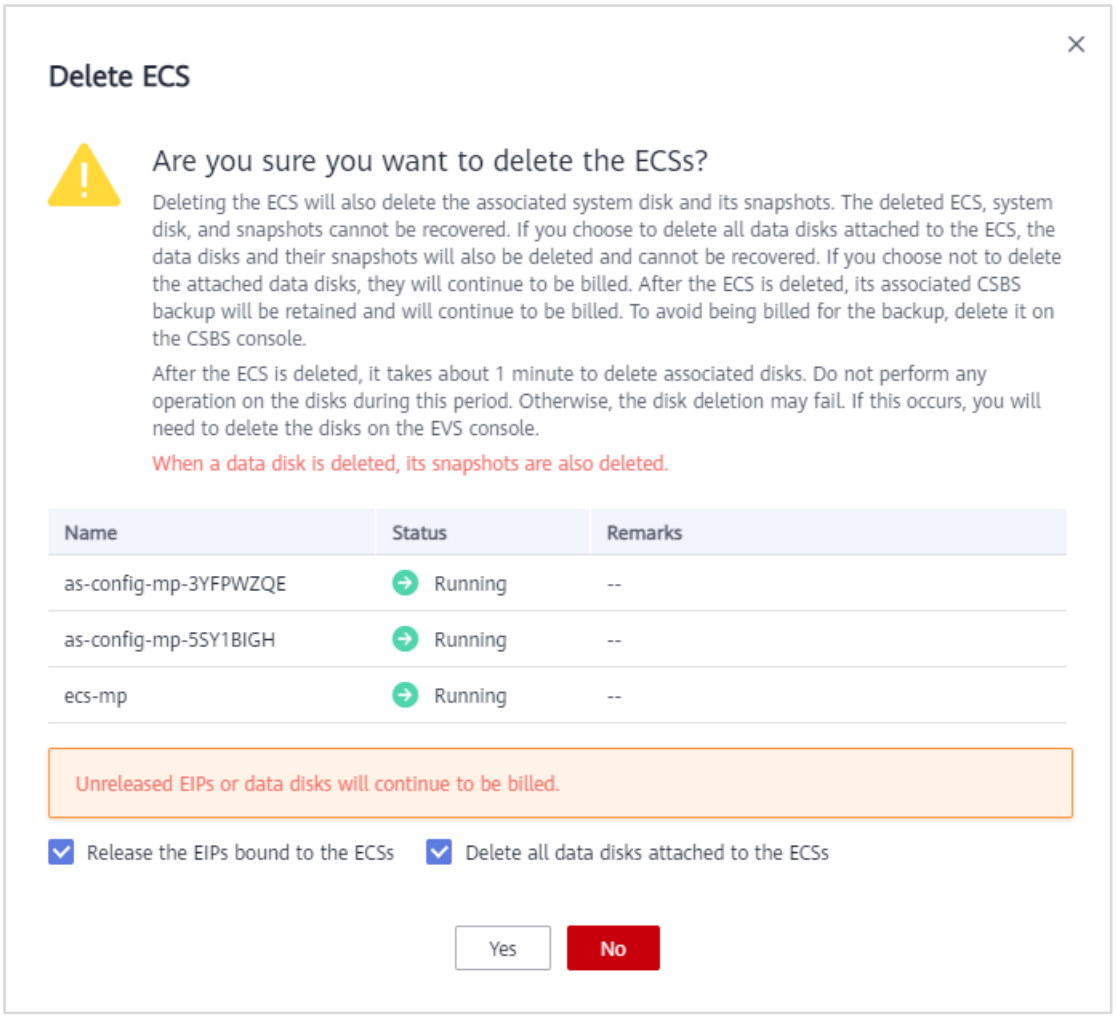


Figure 6-83 Confirming the deletion

6.8.2 Deleting the RDS DB Instance

Step 1 On the service list page, choose **Database** > **Relational Database Service**.

Step 2 Locate the RDS DB instance you want to delete and click **Delete** in the **Operation** column.

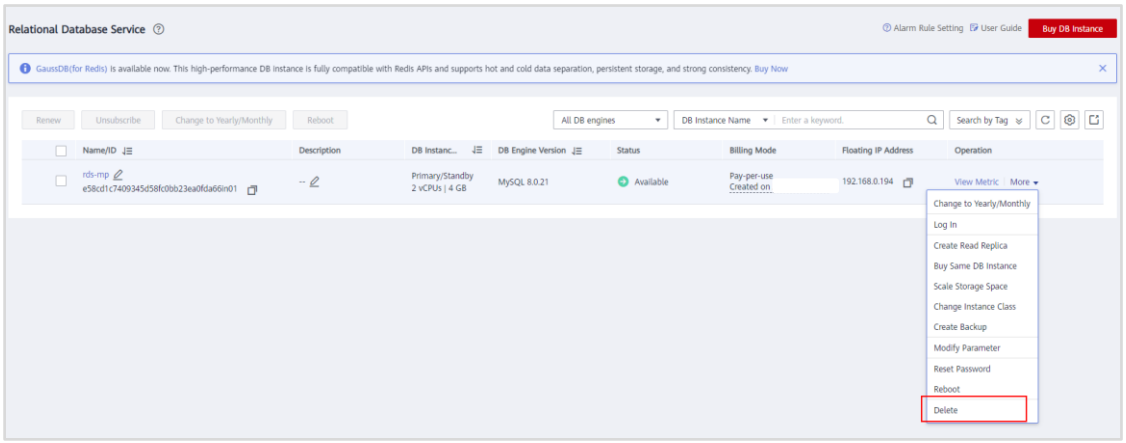


Figure 6-84 Deleting the RDS DB instance

6.8.3 Deleting the Image

Go to the IMS console. Locate the private image you want to delete and click **Delete**. In the displayed dialog box, click **Yes**.

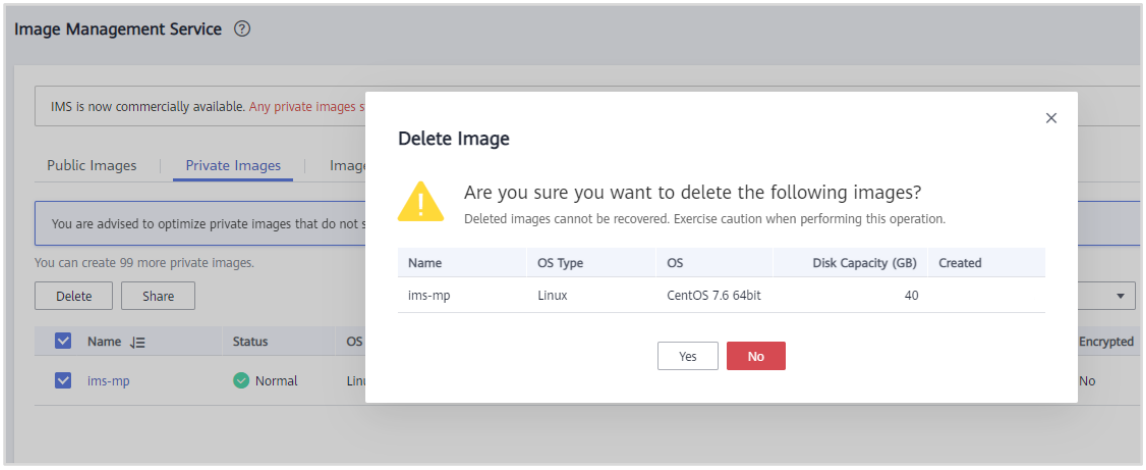


Figure 6-85 Deleting the private image

6.8.4 Deleting the Load Balancer

Step 1 Go to the ELB console, click the name of the shared load balancer. Under **Backend Server Groups**, locate the backend server group associated with the load balancer. Remove the ECSs from the group and then delete the listener. Once you have deleted the ECSs added by AS, you can delete the listener.

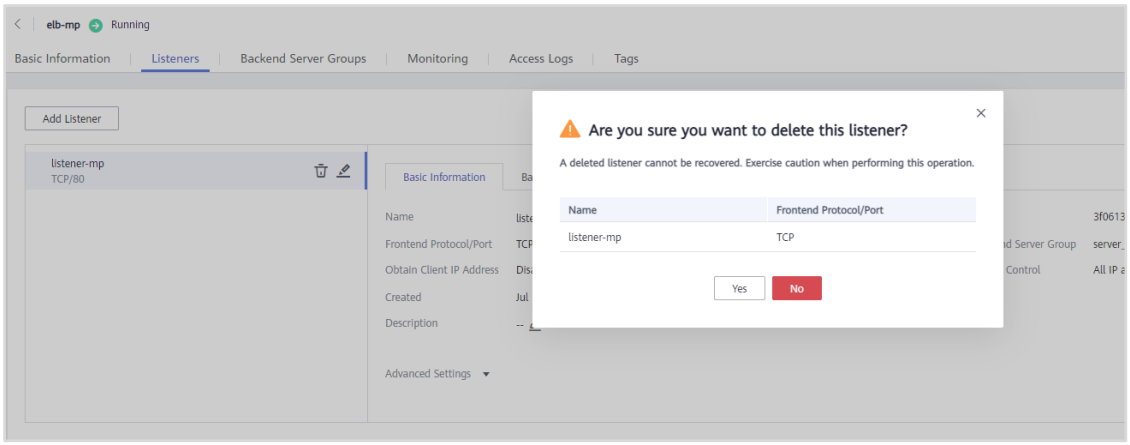


Figure 6-86 Deleting the listener

Step 2 Locate the load balancer and click **Delete**. In the displayed dialog box, click **Yes**.

Figure 6-87 Deleting the load balancer

6.8.5 Deleting AS Resources

Step 1 Locate the AS group you want to delete and click **Delete**. In the displayed dialog box, click **Yes**.

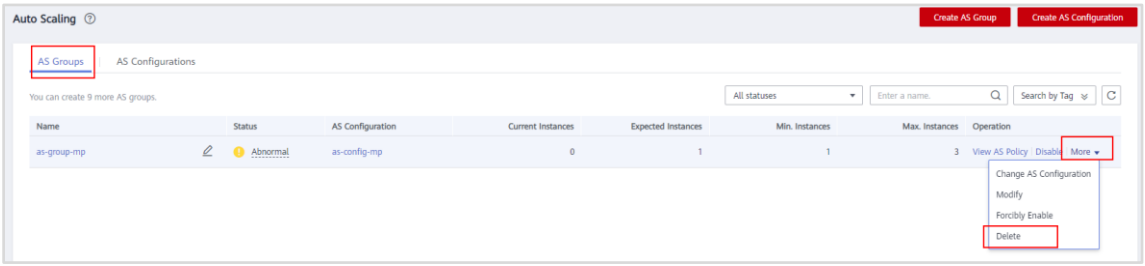


Figure 6-88 Deleting the AS group

Step 2 Locate the AS configuration you want to delete and click **Delete**. In the displayed dialog box, click **Yes**.

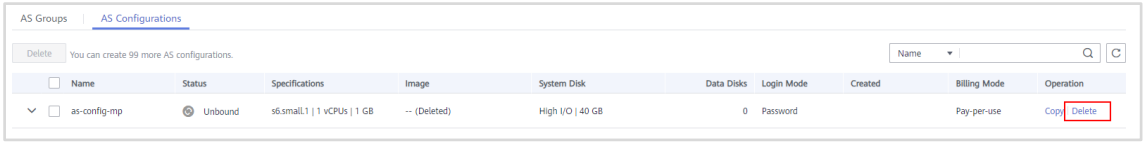


Figure 6-89 Deleting the AS configuration

6.8.6 Deleting VPC Resources

Step 1 In the left navigation pane, choose **Subnets** and then delete the subnet.

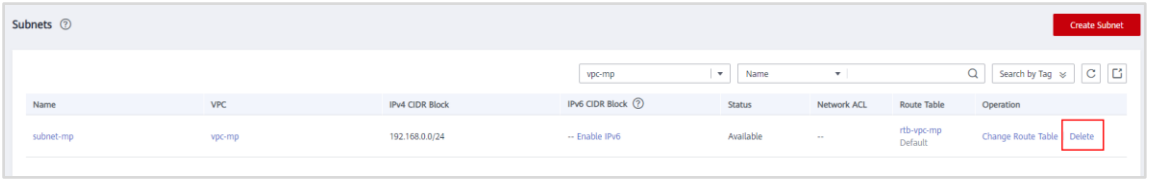


Figure 6-90 Deleting the subnet

Step 2 In the left navigation pane, choose **Access Control** > **Security Groups** and then delete the security group. Then delete the VPC.

Figure 6-91 Deleting the security group

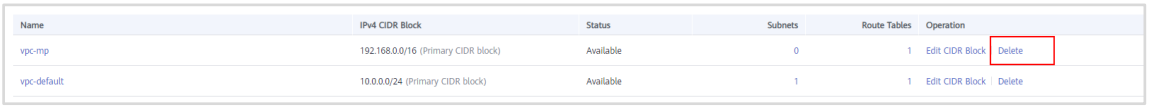


Figure 6-92 Deleting the VPC

Step 3 On the **Dashboard** page of the **Cloud Server Console** and **Network Console**, and on the IMS console, confirm that all of the purchased resources have been deleted in all regions.

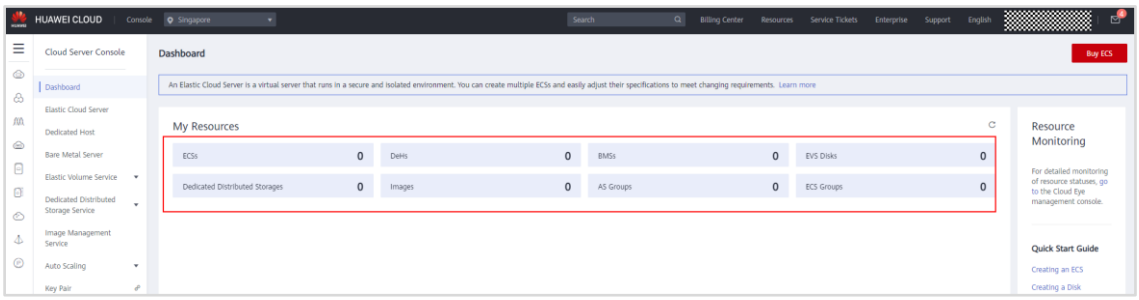


Figure 6-93 Checking ECS-related resources

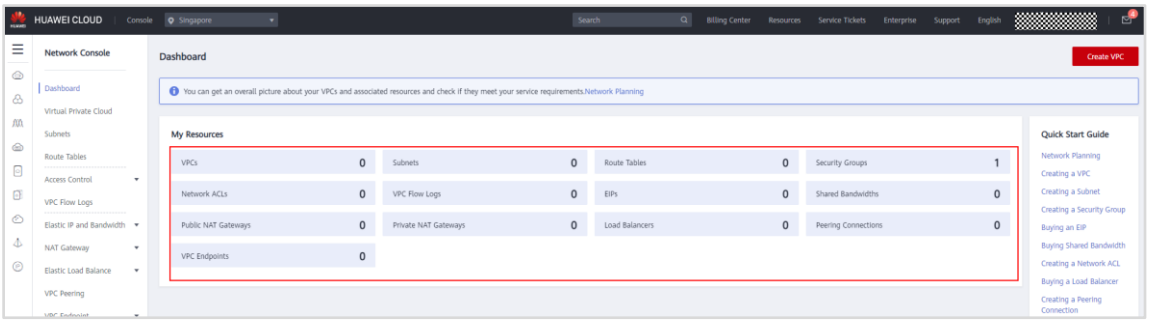


Figure 6-94 Checking network resources

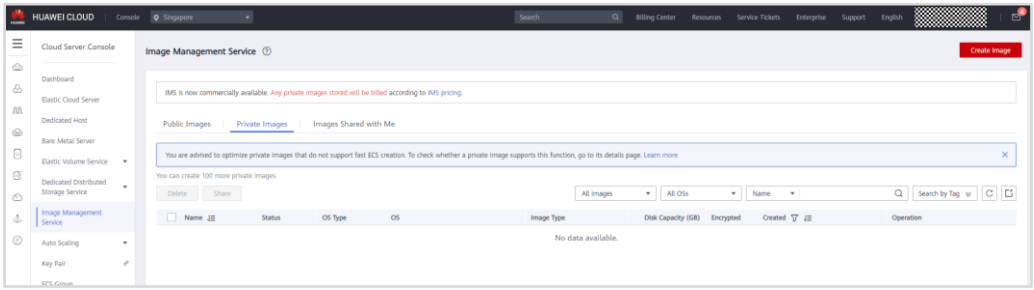


Figure 6-95 Viewing private images

Step 4 Hover your cursor over **Resources** and click **My Resources**. Check whether there are still billable cloud resources in the corresponding region. If there are such services, delete the resources in that region.

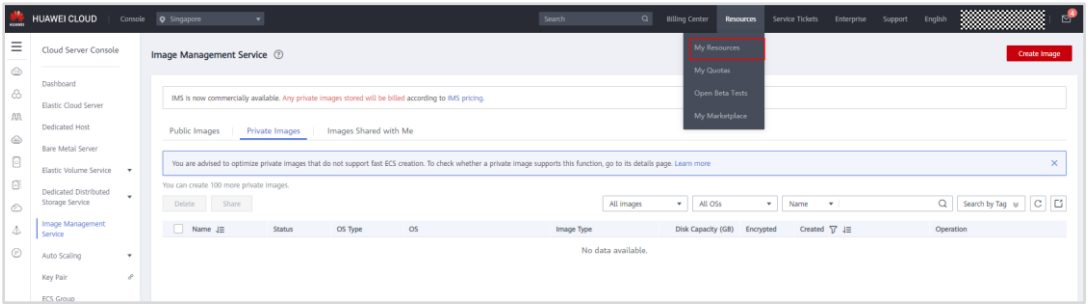


Figure 6-96 Resources

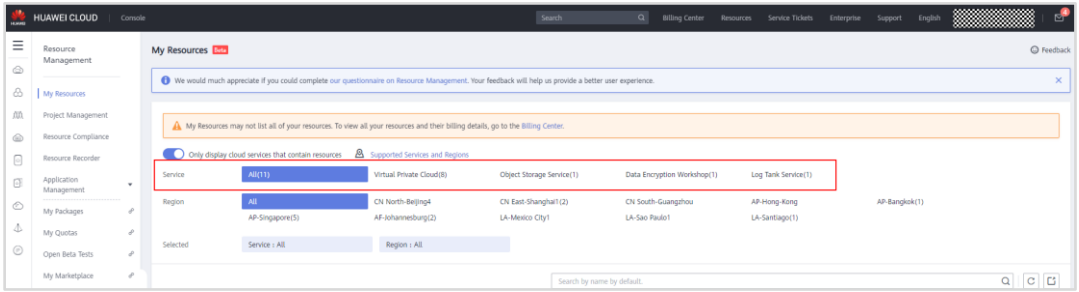


Figure 6-97 My Resources

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