

HCIA Cloud Service Certification Training

HCIA-Cloud Service

Lab Guide for HUAWEI

CLOUD Service Engineers

Version: V2.2



HUAWEI

Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: <http://e.huawei.com>



Huawei Certification System

Based on the "Platform+Ecosystem" strategy and the cloud-pipe-device synergy, the Huawei certification system covers Information and Communications Technology (ICT) architecture certification, platform and service certification, and industry ICT certification for all ICT technologies, which is unique in the industry.

The Huawei certification system offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). The certification covers all ICT fields and complies with the industry trend of ICT convergence. With its leading talent development system and certification standards, Huawei is committed to fostering new ICT talents in the digital era and building a sound ICT talent ecosystem.

HCIA-Cloud Service (Huawei Certified ICT Associate-Cloud Service) certification is designed for developing engineers who understand the cutting-edge Cloud information and who are familiar with eight HUAWEI CLOUD products. This document is intended for candidates who take the HCIA-Cloud Service exam or technical personnel who want to understand basic cloud services 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 cloud products such as computing, storage, network, management & governance, and relational database services in HUAWEI CLOUD.

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 Portfolio



Huawei Certification





About This Document

Overview

This document provides a training course for HCIA-Cloud Service certification. It is intended for candidates who are preparing for the HCIA-Cloud Service exam or readers who want to understand basic cloud services and technologies related to the use, management, and maintenance of HUAWEI CLOUD products.

Description

This document consists of six chapters, introducing operations on computing, storage, network, management, and relational database services, and scenario-specific operations. Those operations cover the usage of main cloud products in HUAWEI CLOUD and help you understand the functions and positions of these products in the HUAWEI CLOUD architecture.

experiment	Content
1	This chapter describes operations on Elastic Cloud Server (ECS), Image Management Service (IMS), and Auto Scaling (AS), including creating and logging in to an ECS, modifying the specifications of a Linux ECS and verifying the modification, creating a Windows system disk image from an ECS, modifying the system disk image, creating a shared image, adding or deleting tenants who share the image, replicating an image within a region, creating an AS configuration, an AS group, and an AS policy, and verifying the elastic scaling function. This chapter also describes operations on ECSs and containers, including creating and logging in to an ECS, performing basic container operations, building a container image using Dockerfile, and building a private registry.
2	This chapter describes operations on Elastic Volume Service (EVS), Object Storage Service (OBS), Scalable File Service (SFS), and Cloud Backup and Recovery (CBR)
3	This chapter presents network services, including verifying that two ECSs in a Virtual Private Cloud (VPC) can communicate with each other by default and that communication can be controlled by security groups, enabling Internet access after binding an EIP to the ECS, distributing traffic using Elastic Load Balance (ELB), creating a VPC peering connection to enable ECSs in different VPCs in the same region to communicate with each other, and creating a VPN connection to enable ECSs in different regions to communicate with each other.
4	This chapter introduces management services, including creating an IAM



experiment	Content
	user account and assigning permissions to the account, using Cloud Trace Service (CTS) to acquire operation records of resources, monitoring resources using Cloud Eye, and using Log Tank Service (LTS) to view and search for logs.
5	This chapter describes basic operations on Relational Database Service (RDS), including buying an RDS MySQL DB instance, and connecting to a MySQL through DAS, a private network, or a public network.
6	This chapter describes how to deploy a website with cloud resources. ECSs function as service nodes. VPC provides network resources for ECSs. AS can be used based on service requirements. AS dynamically adds and deletes ECSs using images of the service nodes to ensure stable and efficient running of services. ELB automatically distributes incoming traffic across multiple ECSs to balance their workloads. Cloud Eye monitors the status of services in real time.

Lab Environment Overview

All operations described in this document are performed on [HUAWEI CLOUD](https://www.huaweicloud.com/intl/en-us/) (<https://www.huaweicloud.com/intl/en-us/>). You need to register a HUAWEI CLOUD account and perform identity authentication in advance. All the products described in this document are operated and used on HUAWEI CLOUD. Obtain the latest product documentation from [HUAWEI CLOUD Help Center](#).



Contents

1 Compute Services.....	8
1.1 ECS, IMS, and AS	8
1.1.1 Introduction	8
1.1.2 Objectives	8
1.1.3 Tasks.....	8
1.1.4 ECS Lifecycle Management.....	8
1.1.5 Creating a Windows System Disk Image Using an ECS.....	21
1.1.6 AS Operations	33
1.2 Container Operations.....	43
1.2.1 Introduction	43
1.2.2 Objectives	43
1.2.3 Tasks.....	43
1.2.4 Basic Container Operations.....	44
1.2.5 (Optional) Building a Container Image Through Dockerfile	52
1.2.6 (Optional) Setting Up a Private Registry	54
1.3 Deleting Resources	56
2 Storage Services	58
2.1 EVS.....	58
2.1.1 Introduction	58
2.1.2 Objectives	58
2.1.3 Tasks.....	58
2.1.4 Attaching an EVS Disk to a Windows ECS.....	58
2.1.5 Attaching an EVS Disk to a Linux ECS.....	69
2.2 OBS.....	73
2.2.1 Introduction	73
2.2.2 Objectives	73
2.2.3 Tasks.....	73
2.2.4 Preparations.....	73
2.2.5 Using OBS Browser+	77
2.2.6 Versioning.....	78
2.2.7 OBS Permission Control Operations	83
2.2.8 Deleting Resources	86
2.3 SFS	86
2.3.1 Introduction	86



2.3.2 Objectives	86
2.3.3 Creating a File System	86
2.3.4 Mounting a File System to an ECS (Linux)	89
2.3.5 Mounting a File System to an ECS (Windows)	93
2.3.6 Deleting Resources	102
2.4 CBR	104
2.4.1 Introduction	104
2.4.2 Objectives	104
2.4.3 Tasks	104
2.4.4 Purchasing a Server Backup Vault	104
2.4.5 Restoring Data Using a Cloud Server Backup	106
2.4.6 Deleting Resources	109
3 Network Services.....	110
3.1 Introduction	110
3.1.1 Objectives	110
3.1.2 Tasks	110
3.2 Preparing Resources	111
3.2.1 Creating VPCs	111
3.2.2 Buying ECSs	114
3.3 Verifying Network Service Functions	117
3.3.1 Communication Between Two ECSs in a VPC	118
3.3.2 Traffic Control by Security Groups	119
3.3.3 Access to the Internet	120
3.3.4 Traffic Distribution	122
3.3.5 Communication Between ECSs in Different VPCs of the Same Region	130
3.3.6 (Optional) Communication Between ECSs in Different Regions	134
3.4 Deleting Resources	141
4 Management Services.....	143
4.1 Introduction	143
4.1.1 Objectives	143
4.1.2 Process	143
4.2 CTS	144
4.2.1 Enabling CTS and Viewing the Default Tracker	144
4.2.2 Creating a Key Event Notification	145
4.2.3 Viewing VPC Creation Records	150
4.3 Creating an IAM User Account and Performing Related Operations	151
4.3.1 Creating an IAM Account and Assigning Permissions	151
4.3.2 Buying an ECS Using the IAM User Account	155
4.4 Cloud Eye	157



4.4.1 Monitoring an ECS.....	157
4.4.2 Creating an Alarm Rule.....	160
4.5 LTS	162
4.5.1 Creating Log Groups and Log Streams.....	162
4.5.2 Installing the ICAgent.....	164
4.5.3 Configuring Log Collection Rules.....	166
4.6 Deleting Resources	168
5 RDS	169
5.1 Introduction.....	169
5.1.1 Objectives	169
5.1.2 Tasks.....	169
5.1.3 Exercise Architecture.....	169
5.2 Buying an RDS MySQL DB Instance and Performing Basic Operations.....	170
5.2.1 Logging In to the Management Console	170
5.2.2 Modifying the Automated Backup Policy for an RDS MySQL DB Instance.....	173
5.2.3 Changing the Database Port of an RDS MySQL DB Instance	174
5.3 Connecting to a MySQL DB Instance Through DAS.....	175
5.4 Connecting to a MySQL DB Instance Through a Private Network	179
5.5 Connecting to a MySQL DB Instance Through a Public Network.....	182
5.6 Deleting Resources	185
6 Comprehensive Exercises: HA Architecture for Enterprise ECSs	187
6.1 Application Scenario.....	187
6.2 Solution.....	187
6.3 Preparations	188
6.4 Setting Up the Apache HTTP Server	189
6.5 Configuring Server-Level HA.....	193
6.5.1 Configuring ELB.....	193
6.5.2 Creating an Image.....	196
6.5.3 Configuring AS.....	198
6.6 Visiting the Website.....	200
6.7 Monitoring Resources	201
6.8 Deleting Resources	202



1 Compute Services

1.1 ECS, IMS, and AS

1.1.1 Introduction

The ECS service provides scalable, on-demand cloud servers for secure, flexible, and efficient application environments, ensuring reliable, uninterrupted services.

IMS provides full lifecycle management for images to help users deploy services quickly.

AS automatically adjusts resources based on business requirements and configured AS policies. You can configure a scheduled, periodic, or alarm policy to change the number of user resources along with service traffic, reducing costs and ensuring stable service running.

This exercise involves the ECS, IMS and AS services, including creating and logging in to ECSs, modifying ECS specifications, creating Windows private images, creating shared images, and automatically scaling resources.

1.1.2 Objectives

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

- Create and log in to an ECS.
- Modify the specifications of an ECS.
- Create a Windows system disk image using an ECS.
- Modify image attributes and share images.
- Create an AS configuration, AS configuration group, and AS policy.

1.1.3 Tasks

ECSs are mainly used as web servers, small-sized database servers, and servers that handle a large number of I/Os. Generally, the ECS service is used together with other cloud products. In this exercise, ECS is used together with IMS and AS.

1.1.4 ECS Lifecycle Management

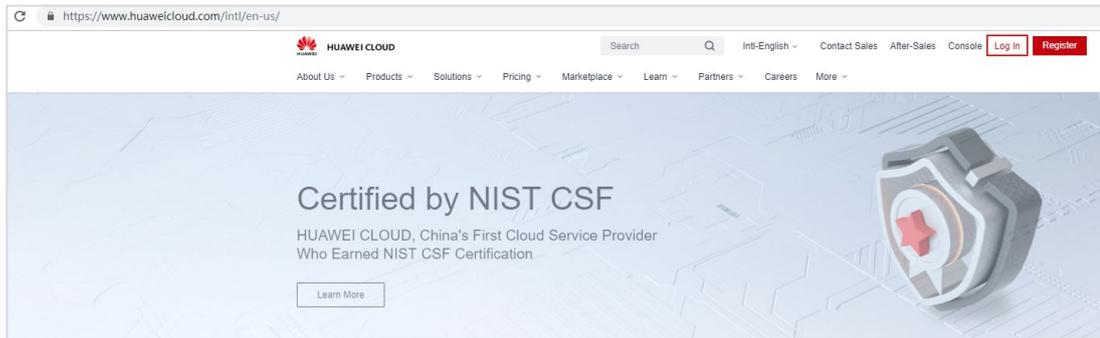
1.1.4.1 Creating Two ECSs Running Different OSs

Step 1 Open a browser and navigate to [HUAWEI CLOUD](#).

Step 2 [Register an account](#) and perform real-name authentication as prompted.



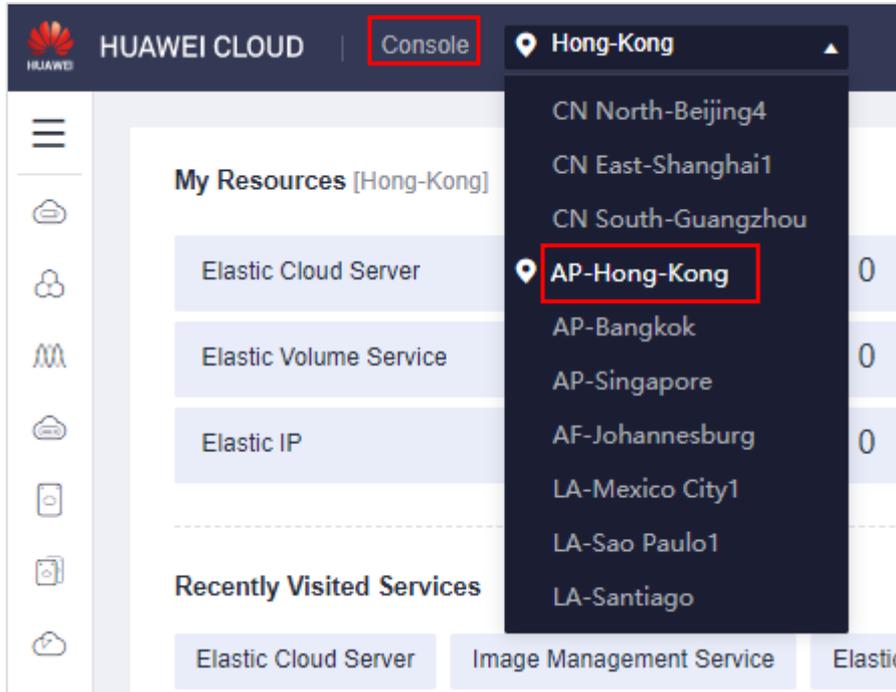
If you already have an account, click **Log In** in the top right corner of the page.



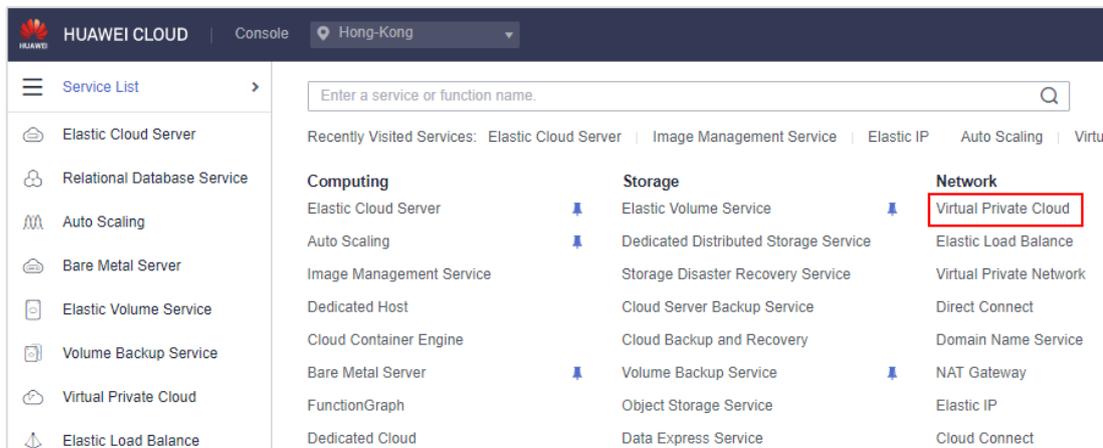
Step 3 Enter the username and password and click **Log In**.

A screenshot of the 'Account Login' form. The form has a white background and a red border. At the top, the title 'Account Login' is centered. Below the title, there are two input fields: 'Account name or email' and 'Password'. The 'Password' field has a small eye icon to its right. Below the input fields, there is a 'Mobile Number Login' option and a 'Remember me' checkbox which is checked. A large red button labeled 'Log In' is positioned below these options. At the bottom of the form, there are four links: 'Free Registration', 'Forgot Password', 'IAM User Login', and 'HUAWEI ID Login'. Below these links is a 'Use Another Account' dropdown menu.

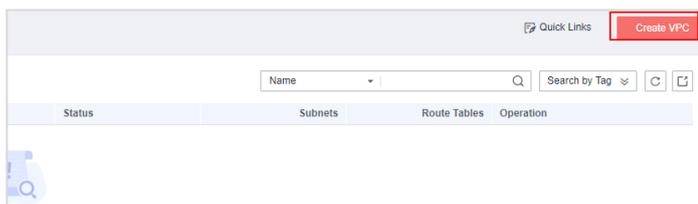
Step 4 On the management console, set the target region to AP-Hong Kong.



Step 5 In the **Service List**, click **Virtual Private Cloud** under **Network** to switch to **Network Console**.



Step 6 Click **Create VPC**, set the parameters, and click **Create Now**.



- **Region:** AP-Hong Kong



- **Name:** Enter a name.
- **Other parameters:** Retain their default settings.

Basic Information

Region: AP-Hong-Kong

Name: vpc-default

CIDR Block: 192.168.0.0/16

Default Subnet

Name: subnet-c408

CIDR Block: 192.168.0.0/24

Available IP Addresses: 251

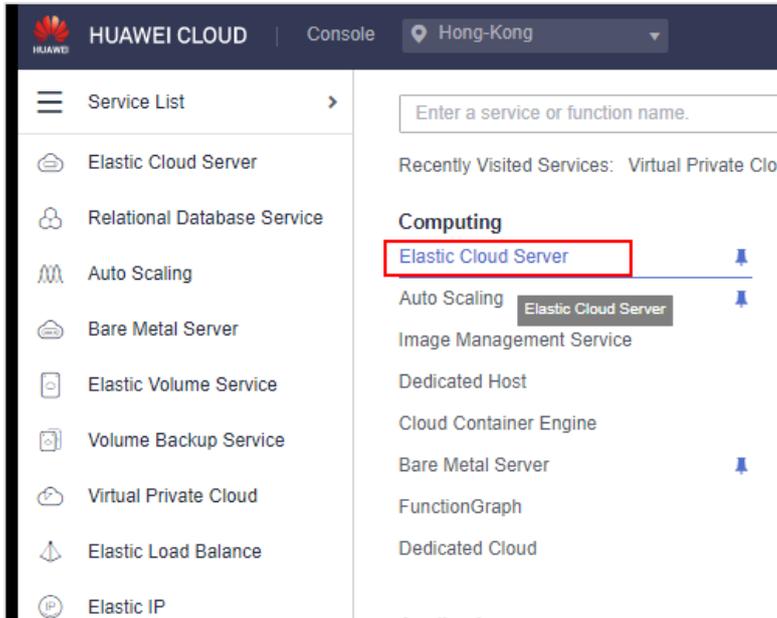
The CIDR block cannot be modified after the subnet has been created.

Free Create Now

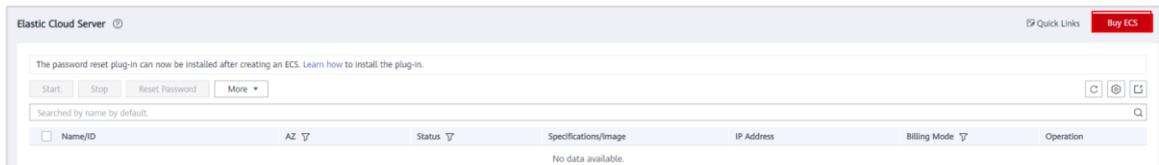
Step 7 Switch back to the VPC page to view the created VPC.

Status	Subnets	Route Tables	Operation
Available	0	1	Modify CIDR Block Delete

Step 8 Switch back to the console homepage. In the **Service List**, click **Elastic Cloud Server** under **Computing**.



Step 9 Click **Buy ECS** and configure basic settings.



- **Billing Mode: Pay-per-use**
- **Region: AP-Hong Kong**
- **AZ: Random**
- **CPU Architecture: x86**
- **Specifications: General computing | s6.small.1 | 1 vCPUs | 1 GB** (You can change the specifications by selecting a different flavor, if required.)



The screenshot shows the 'Elastic Cloud Server' configuration interface. It includes a progress bar with four steps: 1. Configure Basic Settings, 2. Configure Network, 3. Configure Advanced Settings, and 4. Confirm. Under 'Billing Mode', 'Pay-per-use' is selected. The 'Region' is set to 'AP-Hong-Kong'. Under 'AZ', 'Random' is selected. The 'CPU Architecture' is 'x86' with 'Kunpeng' selected. The 'Specifications' section shows a table of instance flavors. The 'General computing' category is selected, and the 's2.small.1' flavor is chosen.

Flavor Name	vCPUs Memory	CPU	Assured / Maximum Bandwidth
s2.small.1	1 vCPUs 1 GB	Intel E5-2680V4 2.4GHz	0.1/0.5 Gbit/s
s2.medium.2	1 vCPUs 2 GB	Intel E5-2680V4 2.4GHz	0.1/0.5 Gbit/s
s2.medium.4	1 vCPUs 4 GB	Intel E5-2680V4 2.4GHz	0.1/0.5 Gbit/s
s2.large.2	2 vCPUs 4 GB	Intel E5-2680V4 2.4GHz	0.2/0.8 Gbit/s
s2.large.4	2 vCPUs 8 GB	Intel E5-2680V4 2.4GHz	0.2/0.8 Gbit/s
s2.xlarge.2	4 vCPUs 8 GB	Intel E5-2680V4 2.4GHz	0.4/1.5 Gbit/s
s2.xlarge.4	4 vCPUs 16 GB	Intel E5-2680V4 2.4GHz	0.4/1.5 Gbit/s
s2.2xlarge.2	8 vCPUs 16 GB	Intel E5-2680V4 2.4GHz	0.8/3 Gbit/s

- **Image:** public image, CentOS 7.6 64bit (40GB)
- **System Disk:** high I/O, 40 GB

The screenshot shows the 'Image' and 'System Disk' configuration sections. Under 'Image', 'Public image' is selected, and 'CentOS 7.6 64bit(40GB)' is chosen. Under 'System Disk', 'High I/O' is selected, and the size is set to 40 GB. The IOPS limit is 1,440 and the burst limit is 5,000. There is a note about free package benefits for a 40 GB High I/O disk and an option to add more data disks.

Step 10 Click **Next: Configure Network**.

- **Network:** Select the VPC created in Step 5.
- **Extension NIC:** Default setting
- **Security Group:** Default or create a new one
- **EIP: Auto Assign**
- **EIP Type: Dynamic BGP**
- **Billed By: Bandwidth**
- **Bandwidth Size: 1 Mbit/s** (You can specify another bandwidth size, if required.)



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

Network:

Extension NIC: You can add 11 more NICs.

Security Group:

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

Security Group Rules

EIP: Auto assign Use existing Not required

EIP Type:

Greater than or equal to 99.95% service availability rate

Billed By:

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

Bandwidth Size: The bandwidth can be from 1 to

Free Anti-DDoS protection

Free package offers 20 GB of Dynamic BGP-based bandwidth billed by traffic. [Learn more](#)

Step 11 Click Next: Configure Advanced Settings.

- ECS Name: ecs-Linux
- Login Mode: Password
- Password: Enter a password, for example, Huawei@123.
- Confirm Password: Enter the password again.
- ECS Group (Optional): Default
- Advanced Options: Default



Elastic Cloud Server

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

ECS Name: Allow duplicate ECS names

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

Login Mode: Key pair Password Set password later

Username: root

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

Confirm Password:

ECS Group (Optional): ⓘ

ⓘ

Advanced Options Configure now

Step 12 Click **Next: Confirm**. After confirming parameter settings, read the service agreement, select the check box, and click **Next**.

Settings — ② Configure Network — ③ Configure Advanced Settings — ④ **Confirm**

Basic ⓘ

Billing Mode	Pay-per-use	Region	Hong-Kong	AZ	AZ2
Specifications	General computing s2.small.1 1 vCPUs 1 GB	Image	CentOS 7.6 64bit	System Disk	High I/O, 40 GB

Network ⓘ

VPC	vpc-default(192.168.0.0/16)	Security Group	default	Primary NIC	subnet-c4d8(192.168.0.0/24)
EIP	Dynamic BGP Billed By: Bandwidth Bandwidth: 1 Mbit/s				

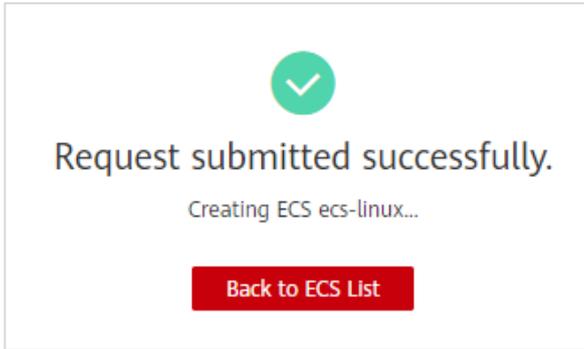
Advanced ⓘ

ECS Name	ecs-linux	Login Mode	Password	ECS Group	--
----------	-----------	------------	----------	-----------	----

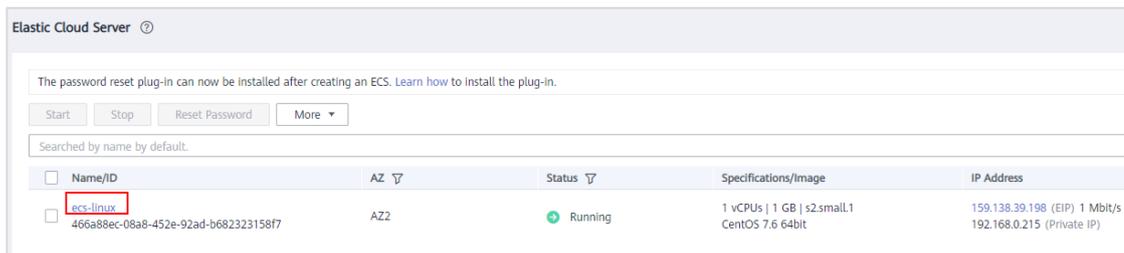
You can create 20 more ECSs. [Learn how to increase quota.](#)

I have read and agree to the [Service Level Agreement](#) and [Huawei Image Disclaimer](#).

JSD/hour ©
deducted preferentially. [Learn more](#)

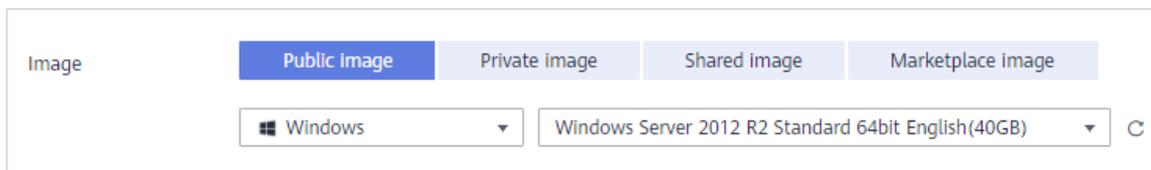


The purchased ECS is displayed on the **Elastic Cloud Server** page.



Step 13 Repeat the preceding operations to create another ECS with the following parameter settings:

- **Billing Mode:** Pay-per-use
- **Image:** public image, Windows Server 2012 R2 Standard 64bit English (40GB)



- **ECS Name:** ecs-Windows2012
- **Other parameters:** same as those of **ecs-Linux**



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

ECS Name: Allow duplicate ECS names

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

Login Mode:

Username: Administrator

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

Confirm Password:

ECS Group (Optional): ⓘ

ⓘ

[Create ECS Group](#)

Advanced Options Configure now

The purchased ECSs are displayed on the **Elastic Cloud Server** page.

Elastic Cloud Server ⓘ

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

Searched by name by default.

<input type="checkbox"/>	Name/ID	AZ	Status	Specifications/Image	IP Address
<input type="checkbox"/>	ecs-Windows2012 74817c7a-556c-47f6-89be-a095704a85fa	AZ2	Running	1 vCPUs 1 GB s2.small.1 Windows Server 2012 R2 Standard 64bit Eng...	119.8.33.27 (EIP) 1 Mbit/s 192.168.0.25 (Private IP)
<input type="checkbox"/>	ecs-linux 466a88ec-08a8-452e-92ad-b682323158f7	AZ2	Running	1 vCPUs 1 GB s2.small.1 CentOS 7.6 64bit	159.138.39.198 (EIP) 1 Mbit/s 192.168.0.215 (Private IP)

----End

1.1.4.2 Logging In to the ECSs

- Step 1 On the **Elastic Cloud Server** page, click **Remote Login** in the **Operation** column of each ECS.



Name/ID	AZ	Status	Specifications/Image	IP Address	Billing Mode	Operation
ecs-Windows2012 74817c7a-556c-4716-89be-a095704a85fa	AZ2	Running	1 vCPUs 1 GB s2.small.1 Windows Server 2012 R2 Standard 64bit Eng...	119.8.33.27 (EIP) 1 Mbit/s 192.168.0.25 (Private IP)	Pay-per-use Created on Aug 12, 2020 17:09:...	Remote Login
ecs-linux 466a88ec-08a8-452e-92ad-b682323158f7	AZ2	Running	1 vCPUs 1 GB s2.small.1 CentOS 7.6 64bit	159.138.39.198 (EIP) 1 Mbit/s 192.168.0.215 (Private IP)	Pay-per-use Created on Aug 12, 2020 17:03:...	Remote Login

Step 2 Enter login information.

- Linux

Username: root

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.12.1.el7.x86_64 on an x86_64

ecs-linux login: root
Password:

Welcome to Huawei Cloud Service

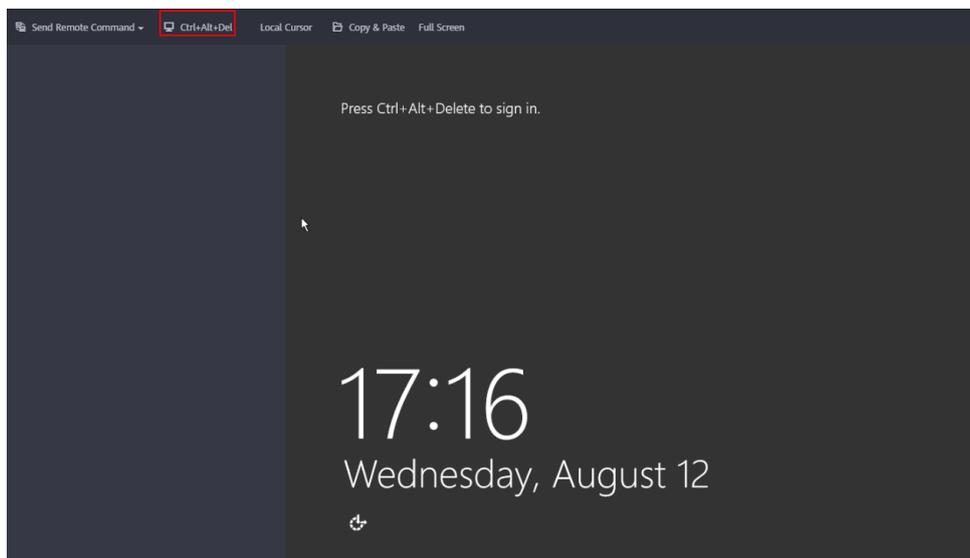
[root@ecs-linux ~]# _
```

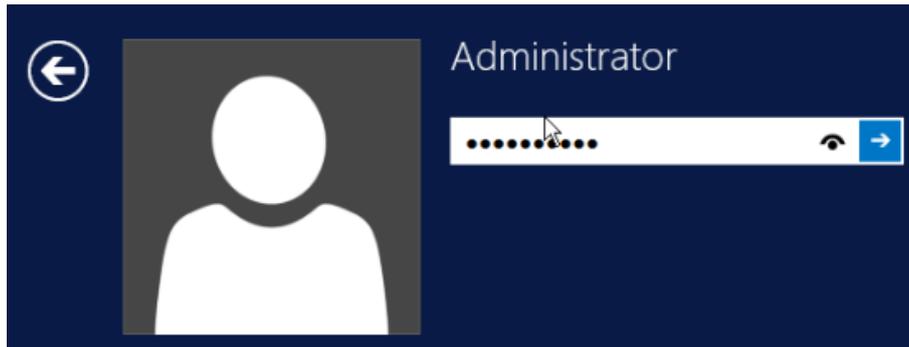
- Windows

Username: Administrator

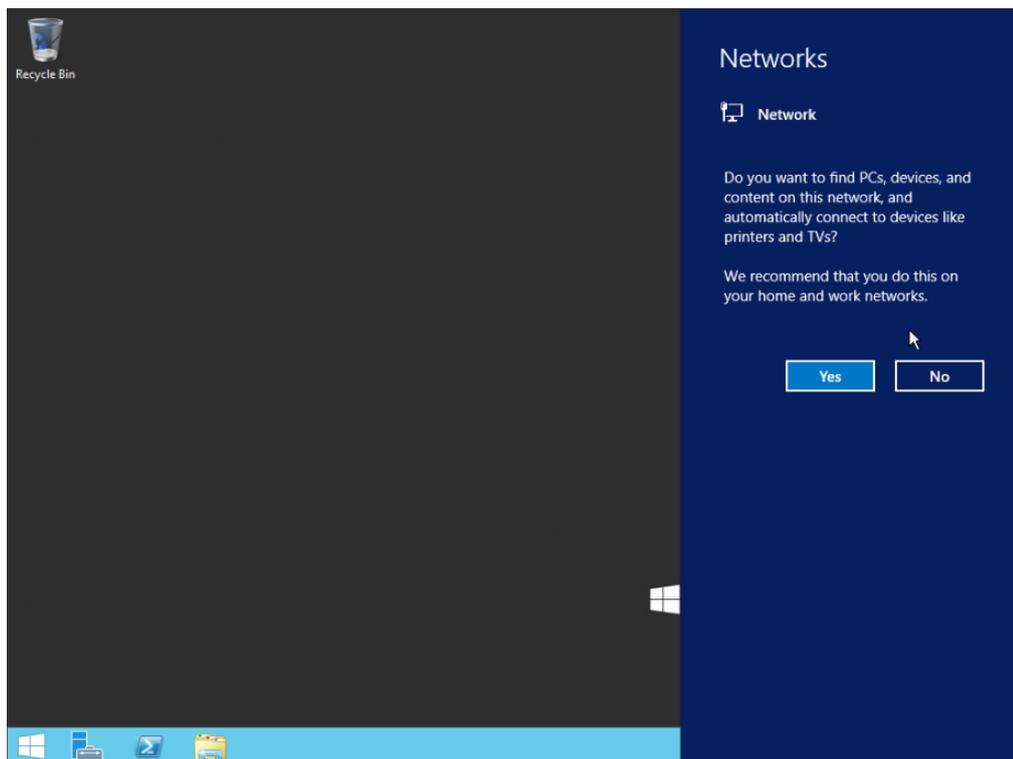
Password: Enter a password, for example, **Huawei@123**.

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





If a page similar to the following is displayed, the ECSs are logged in.



For more details about parameter settings, see [Purchasing an ECS](#).

----End

1.1.4.3 Modifying ECS Specifications (Linux)

If the specifications of an ECS fail to meet your service requirements, you can modify the ECS specifications at any time.

The following operations use a Linux ECS as an example.

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

Ensure that the ECS is stopped.



The screenshot shows the Elastic Cloud Server console. At the top, there are buttons for 'Start', 'Stop', 'Reset Password', and 'More'. Below this is a search bar and a table of ECS instances. The table has columns for Name/ID, AZ, and Status. Two instances are listed: 'ecs-Windows2012' (Running) and 'ecs-linux' (Running). The 'ecs-linux' instance is selected with a checkmark and highlighted with a red box.

Name/ID	AZ	Status
ecs-Windows2012 74817c7a-556c-47f6-89be-a095704a85fa	AZ2	Running
ecs-linux 466a88ec-08a8-452e-92ad-b682323158f7	AZ2	Running

Step 2 Click **More** in the **Operation** column and select **Modify Specifications**.

The screenshot shows the Elastic Cloud Server console with the 'More' dropdown menu open for the 'ecs-linux' instance. The menu options include: Buy Same ECS, Start, Stop, Restart, Reset Password, Modify Specifications (highlighted with a red box), Change Billing Mode, Delete, Manage Image/Disk, Manage Network, and Migrate ECS.

Step 3 On the **Modify ECS Specifications** page, select the desired ECS type, vCPUs, and memory and click **Next**. After confirming parameter settings, read the service agreement, select the check box, and click **Submit**.

The status of the ECS changes to **Resizing** on the **Elastic Cloud Server** page.

The screenshot shows the Elastic Cloud Server console. The 'ecs-linux' instance is now in a 'Resized' state, indicated by a blue 'R' icon and the text 'Resized' in a red box. The other instance, 'ecs-Windows2012', remains in a 'Running' state.

Name/ID	AZ	Status	Specifications/Image	IP Address
ecs-Windows2012 74817c7a-556c-47f6-89be-a095704a85fa	AZ2	Running	1 vCPUs 1 GB s2.small.1 Windows Server 2012 R2 Standard 64bit Eng...	119.8.33.27 (EIP) 1 Mbit/s 192.168.0.25 (Private IP)
ecs-linux 466a88ec-08a8-452e-92ad-b682323158f7	AZ2	Resized	1 vCPUs 1 GB s2.small.1 CentOS 7.6 64bit	159.138.39.198 (EIP) 1 Mbit/s 192.168.0.215 (Private IP)

Step 4 After the ECS status changes to **Running**, check whether its specifications have been modified.



Elastic Cloud Server

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

Searched by name by default.

Name/ID	AZ	Status	Specifications/Image	IP Address
<input type="checkbox"/> ecs-Windows2012 74817c7a-556c-47f6-89be-a095704a85fa	AZ2	Running	1 vCPUs 1 GB s2.small.1 Windows Server 2012 R2 Standard 64bit Eng...	119.8.33.27 (EIP) 1 Mbit/s 192.168.0.25 (Private IP)
<input checked="" type="checkbox"/> ecs-linux 466a88ec-08a8-452e-92ad-b682323158f7	AZ2	Running	1 vCPUs 2 GB s2.medium.2 CentOS 7.6 64bit	159.138.39.198 (EIP) 1 Mbit/s 192.168.0.215 (Private IP)

Step 5 (Optional) Log in to the modified ECS and check its specifications on the CLI.

- Run the `cat /proc/cpuinfo | grep "processor" | wc -l` command to view vCPUs (originally 1 vCPU).

Manually run this command. Pay attention to the command format if you copy-paste the command.

```
[root@ecs-linux ~]# cat /proc/cpuinfo | grep "processor" | wc -l
1
[root@ecs-linux ~]#
```

- Run the `cat /proc/meminfo` command to view memory.

MemTotal shows the total memory size.

```
[root@ecs-linux ~]# cat /proc/meminfo
MemTotal: 1881688 kB
MemFree: 1495316 kB
MemAvailable: 1591988 kB
Buffers: 17656 kB
Cached: 208056 kB
SwapCached: 0 kB
Active: 151236 kB
Inactive: 162560 kB
Active(anon): 88364 kB
Inactive(anon): 8460 kB
Active(file): 62872 kB
Inactive(file): 154100 kB
```

The specifications modification is successful.

----End

1.1.5 Creating a Windows System Disk Image Using an ECS

If you have created an ECS and configured it (such as by installing software and deploying an application environment) based on your business requirements, you can create a system disk image with the configured ECS. Then, the configurations will be applied to all the new ECSs created from this image.

For example, the process of creating a Windows system disk image using an ECS is as follows:

1. Log in to a Windows ECS.



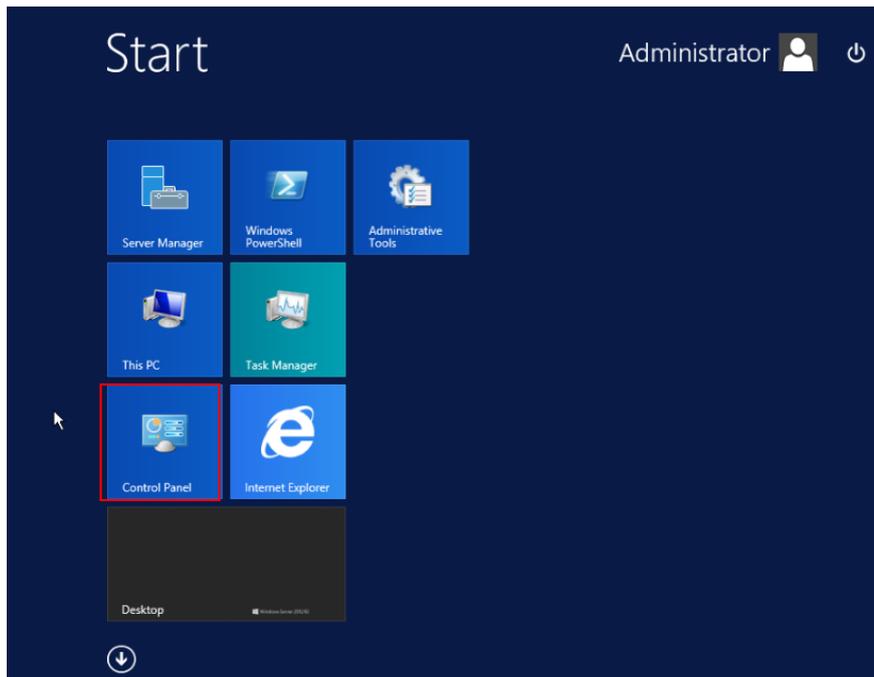
2. Configure the ECS.
3. Use the ECS to create a system disk image.

1.1.5.1 Configuring a Windows ECS

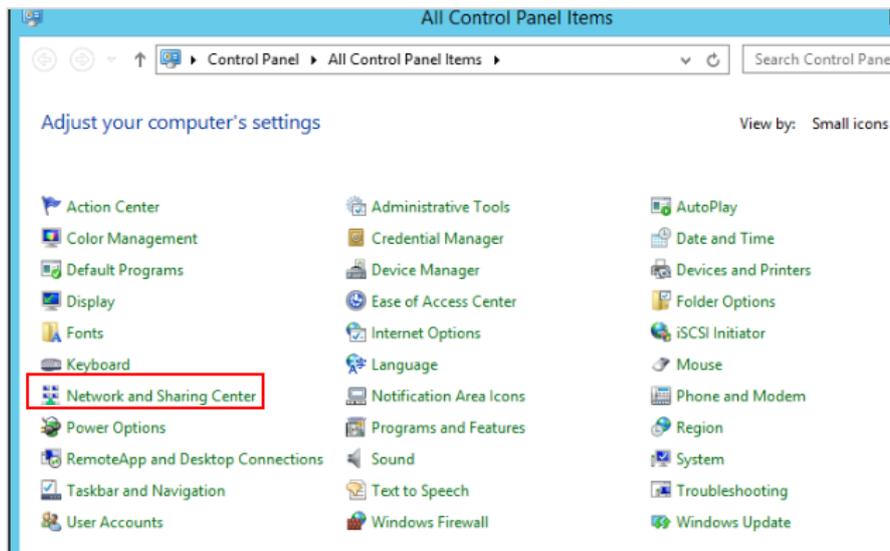
Step 1 Log in to the ECS (**ecs-Windows2012** is used as an example).

Step 2 Configure DHCP for the ECS NICs.

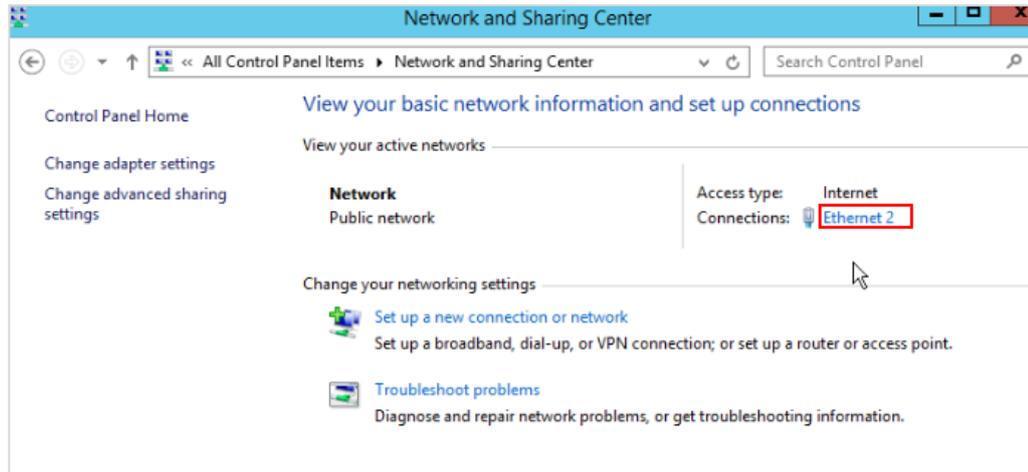
1. Choose **Start > Control Panel**.



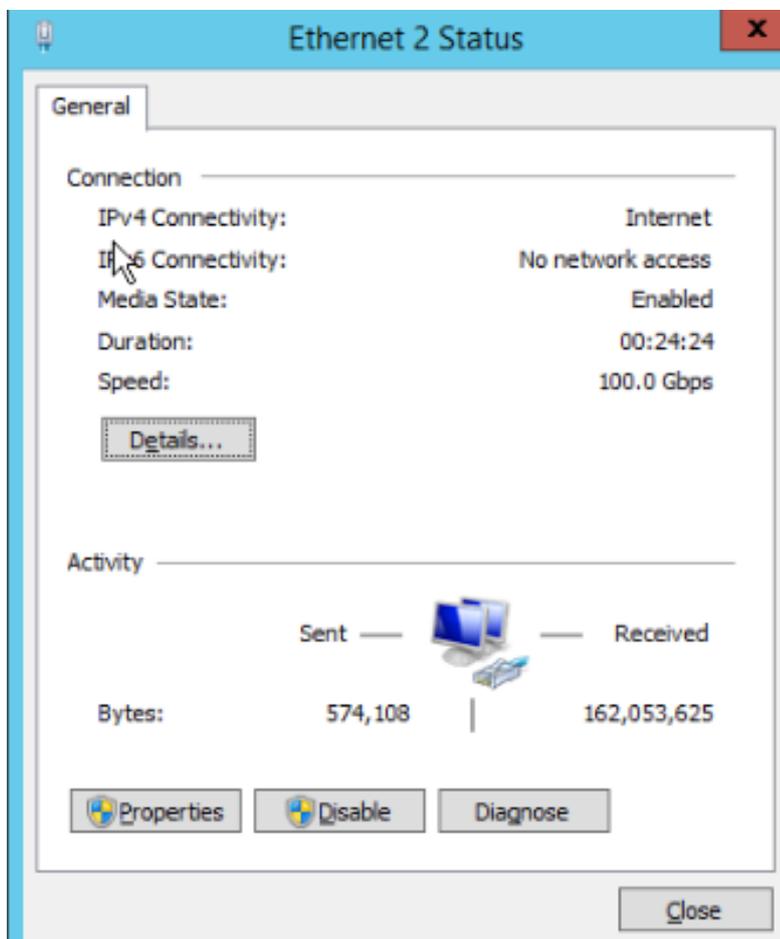
2. Click **Network and Sharing Center**.



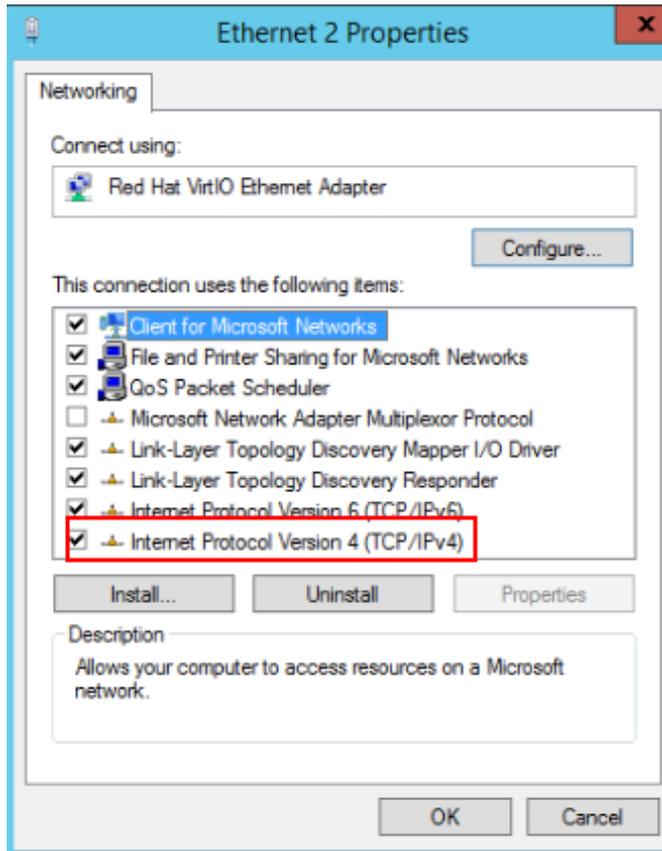
3. Click the connection (for example, **Ethernet 2**).



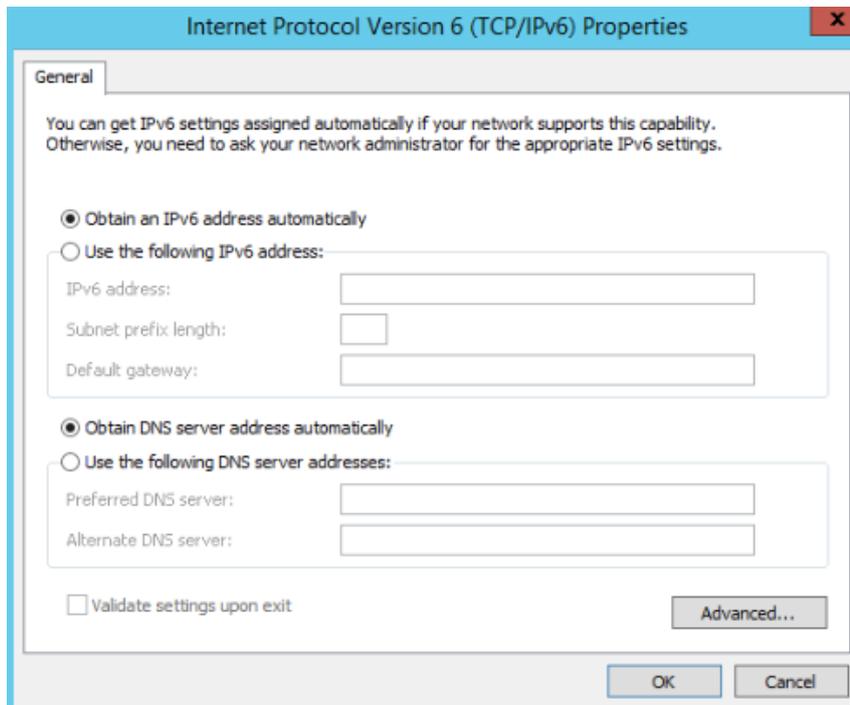
4. Click **Properties**.



5. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.

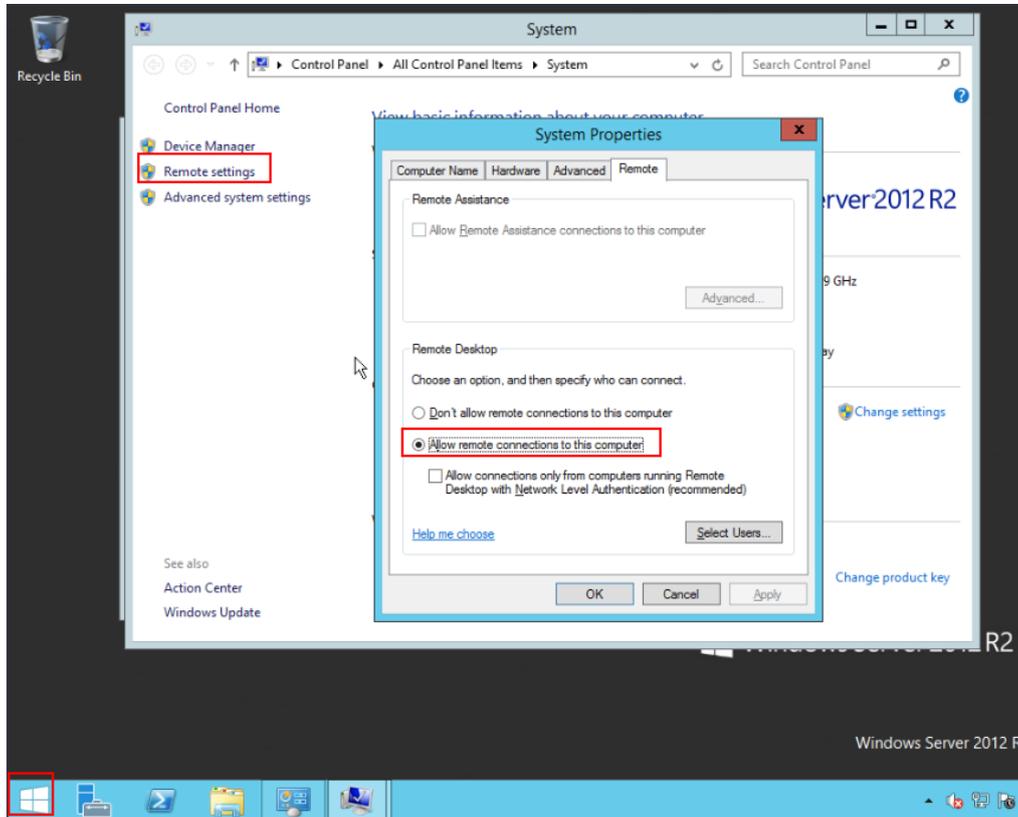


6. If **Obtain an IPv6 address automatically** and **Obtain DNS server address automatically** are selected, DHCP has been configured. Otherwise, select the two check boxes and click **OK**.

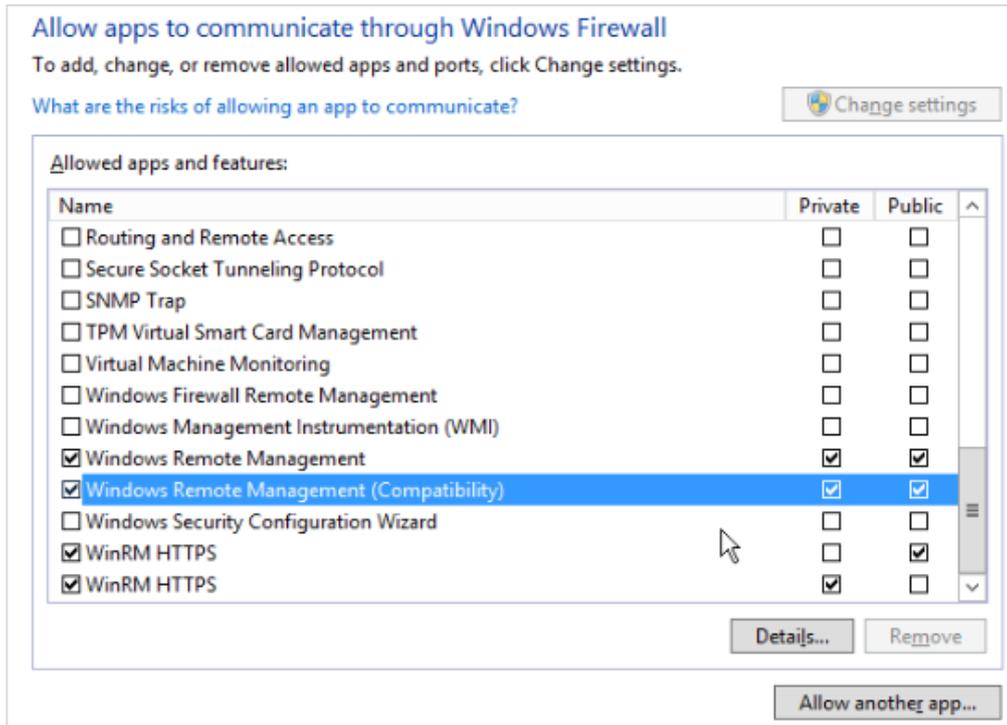




- Step 3 Click **Start**, right-click **Computer**, and choose **Properties**. In the left navigation pane of the **System** page, click **Remote settings**. Select **Allow remote connections to this computer**. Click **OK**.



- 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**.
- Step 5 Select apps that are allowed by Windows Firewall for **Remote Desktop** based on your network requirements and click **Allow another app...**

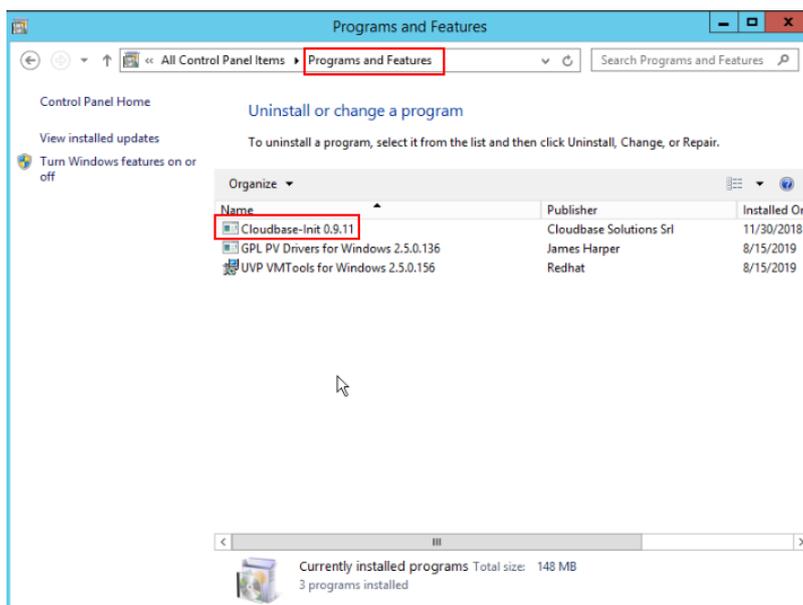


Step 6 Install Cloudbase-Init on the ECS.



If Cloudbase-Init is not configured for 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.

In this exercise, the ECS is created from public image **windows2012 R2** for which Cloudbase-Init is installed by default. You can go to **Control Panel > Programs and Features** to check whether Cloudbase-Init has been installed on the ECS.



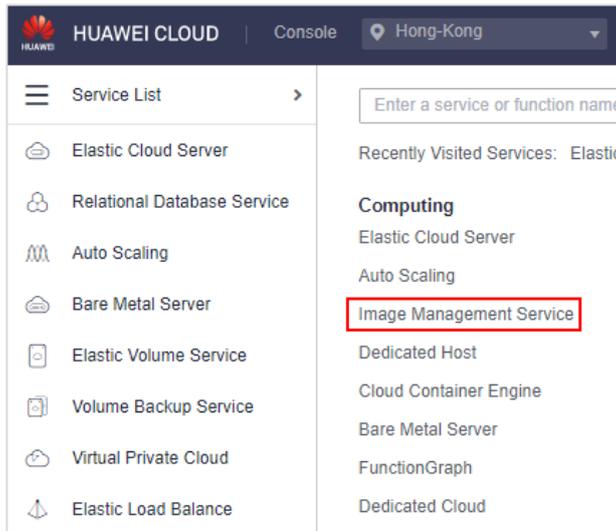


For the ECSs created from a private image or an external image file, install and configure Cloudbase-Init for them by referring to [IMS User Guide](#).

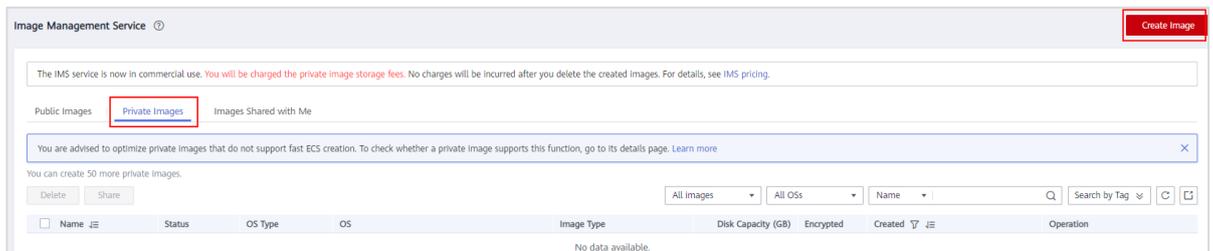
----End

1.1.5.2 Creating a Windows Private Image

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



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



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

- **Type:** Select **System Disk Image**.
- **Source:** Select **ECS** and then the desired ECS, for example, **ecs-Windows2012**.
- **Name:** Enter a name, for example, **image-windows2012**.



Create Image

The IMS service is now in commercial use. You will be charged the private image storage fees. For details, see [IMS pricing](#).

Image Type and Source

* Type: **System disk Image** | Full-ECS Image | Data disk image | ISO image

* Source: **ECS** | Image File

- You can only use a running or stopped ECS to create a private image.
- You need to first customize and optimize the ECS to suit your needs. For example, you need to install Cloud-Init if the ECS runs Linux and install Cloudbase-Init if the ECS runs Windows. [Learn more](#)
- Do not perform any operation on the selected ECS or associated resources during image creation.

Name	OS	Status	Private IP Address	Created
<input checked="" type="radio"/> ecs-Windows2012	Windows Server 2012 R2...	Running	192.168.0.25	Aug 12, 2020 17:09:06...
<input type="radio"/> ecs-linux	CentOS 7.6 64bit	Running	192.168.0.215	Aug 12, 2020 17:03:19...

Selected: ecs-Windows2012|OS: Windows Server 2012 R2 Standard 64bit|System Disk: High I/O | 40 GB
[Buy ECS](#)

Image Information

Encryption: Unencrypted ⓘ

* Name: **image-windows2012**

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

Tag key: Tag value:

You can add 10 more tags.

Description:

Next

Step 4 Confirm the settings. Then, select **I have read and agree to the Huawei 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 varies depending on the image file size. Generally, it takes about 10 to 20 minutes. The image is created successfully when its status changes to **Normal**.

Image Management Service

The IMS service is now in commercial use. You will be charged the private image storage fees. No charges will be incurred after you delete the created images. For details, see [IMS pricing](#).

Public Images | **Private Images** | Images Shared with Me

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

You can create 49 more private images.

Delete | Share | All Images | All OSs

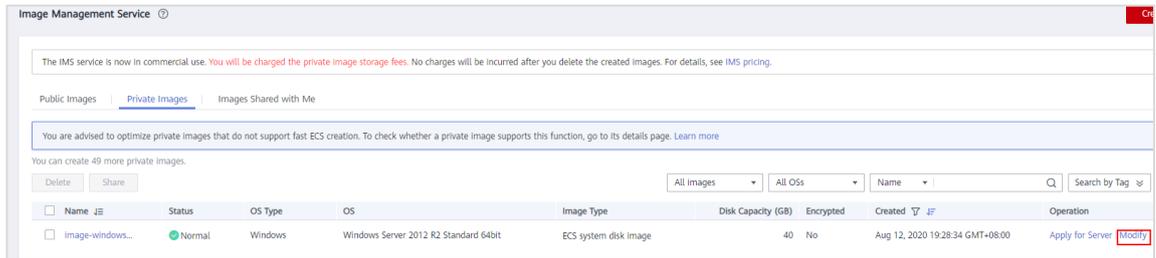
Name	Status	OS Type	OS	Image Type	Disk Capacity (GB)	Encrypted
image-windows...	Normal	Windows	Windows Server 2012 R2 Standard 64bit	ECS system disk image	40	No

----End



1.1.5.3 Modifying Image Information

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



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

Modify Image

* Name:

Description:

Minimum Memory: *If the minimum memory size of an image has been increased, it must be set back to the original size before you reinstall OSs of the ECSs that were created using the image.*

Unlimited	1 GB	2 GB	4 GB
8 GB	16 GB	32 GB	64 GB
128 GB			

Maximum Memory: **Unlimited** | 4 GB | 32 GB | 64 GB | 128 GB

NIC Multi-Queue: Supported | **Not supported**

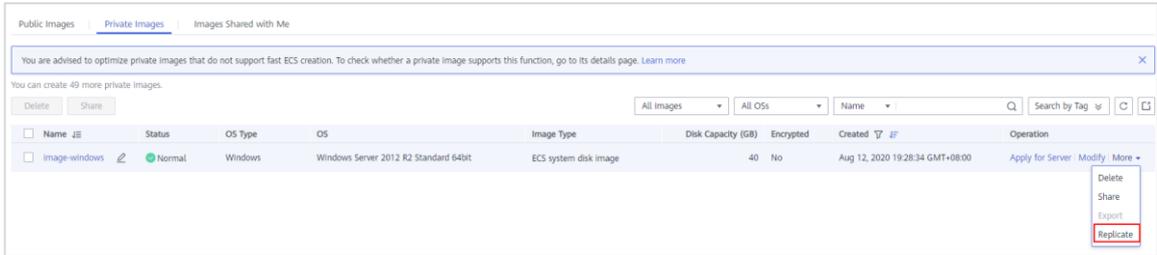
Boot Mode: BIOS | UEFI

OK Cancel

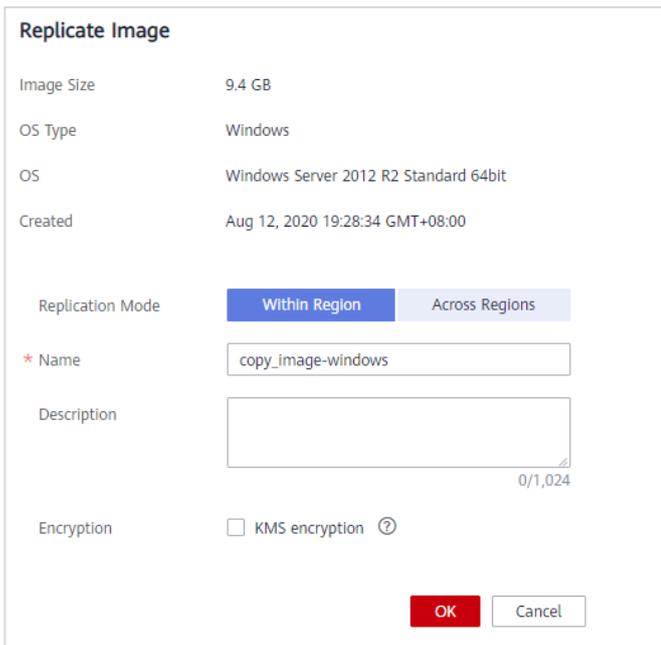
----End

1.1.5.4 In-Region Image Replication

Step 1 Locate the row that contains the image to be replicated and choose **More > Replicate** in the **Operation** column.



Step 2 In the displayed **Replicate Image** dialog box, enter a new name for the image and click **OK**.



The new image is displayed on the **Private Image** tab page and its status is **Creating**.



----End

1.1.5.5 Creating a Shared Image

You can share your images with another user. Before sharing the images, you need to obtain the account name of the user (if the user is a DeC or multi-project user, you also



need to obtain their project name). In this exercise, sharing a single image is used as an example.

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



- Step 2 Click the **Shared Images** tab, enter the account name of the target user and click **Add**.

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).

Share Image

Image Details

Image Name image-windows

OS Type Windows

OS Windows Server 2012 R2 Standard 64bit

Image Size 9.4 GB

[Shared Images](#) | [Stop Sharing](#)

Enter an account name of the recipient. [Learn how](#) to obtain an account name and a project name.

The recipient is a DeC user, so you must enter a project name.

* *

Account Name	Project Name	Project ID	Operation
--------------	--------------	------------	-----------

- Step 3 Go to the image details page to check whether the image has been successfully shared with the user. On this page, you can also add or remove users who can use the shared image.



Share Image

Image Details

Image Name image-windows
OS Type Windows
OS Windows Server 2012 R2 Standard 64bit
Image Size 9.4 GB

[Shared Images](#) | [Stop Sharing](#)

Enter an account name of the recipient. [Learn how](#) to obtain an account name and a project name.
The recipient is a DeC user, so you must enter a project name.

* *

Account Name	Project Name	Project ID	Operation
--------------	--------------	------------	-----------

-----End

1.1.5.6 Applying for an ECS Using a Private Image

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

Image Management Service ⓘ

The IMS service is now in commercial use. You will be charged the private image storage fees. No charges will be incurred after you delete the created images. For details, see [IMS pricing](#).

Public Images | **Private Images** | Images Shared with Me

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

You can create 48 more private images.

All Images All OSs Name Search by T

<input type="checkbox"/>	Name	Status	OS Type	OS	Image Type	Disk Capacity (GB)	Encrypted	Created	Operation
<input type="checkbox"/>	copy_image-win...	Normal	Windows	Windows Server 2012 R2 Standard 64bit	ECS system disk image	40	No	Aug 12, 2020 20:06:08 GMT+08:00	Apply for Server
<input type="checkbox"/>	image-windows	Normal	Windows	Windows Server 2012 R2 Standard 64bit	ECS system disk image	40	No	Aug 12, 2020 19:28:34 GMT+08:00	Apply for Server

Step 2 Set **Billing Mode** to **Pay-per-use** and **Image** to **Private image**. Set other parameters as needed.



The screenshot shows the configuration interface for an Elastic Cloud Server (ECS). The Billing Mode is set to 'Pay-per-use'. The Region is 'AP-Hong-Kong'. The CPU Architecture is 'x86'. Under Specifications, 'General computing' is selected, and 's2.medium.4' is chosen. The Image is set to 'image-windows(40GB)'.

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

Name/ID	AZ	Status	Specifications/Image	IP Address	Billing Mode	Operation
ecs-test 65515200-d59b-473b-8f75-5851fc782cba	AZ2	Running	1 vCPUs 4 GB s2.medium.4	159.138.30.102 (EIP) 2 Mbit/s 192.168.0.32 (Private IP)	Pay-per-use Created on Aug. 12, 2020, 20:30:...	Remote Login More
ecs-Windows2012 74817c7a-556c-47f6-89be-a095704a85fa	AZ2	Running	1 vCPUs 1 GB s2.small.1	119.8.33.27 (EIP) 1 Mbit/s 192.168.0.25 (Private IP)	Pay-per-use Created on Aug. 12, 2020, 17:09:...	Remote Login More
ecs-linux 466a88ec-08a8-452e-92ad-b682323158f7	AZ2	Running	1 vCPUs 2 GB s2.medium.2	159.138.39.198 (EIP) 1 Mbit/s 192.168.0.215 (Private IP)	Pay-per-use Created on Aug. 12, 2020, 17:03:...	Remote Login More

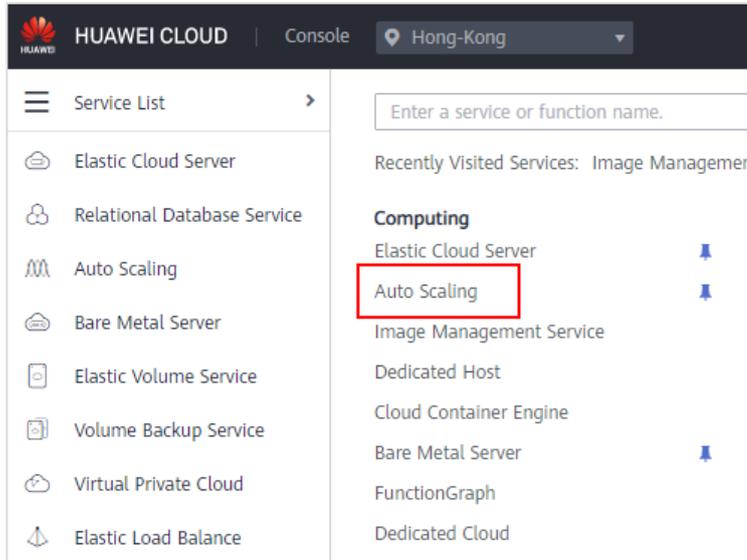
----End

1.1.6 AS Operations

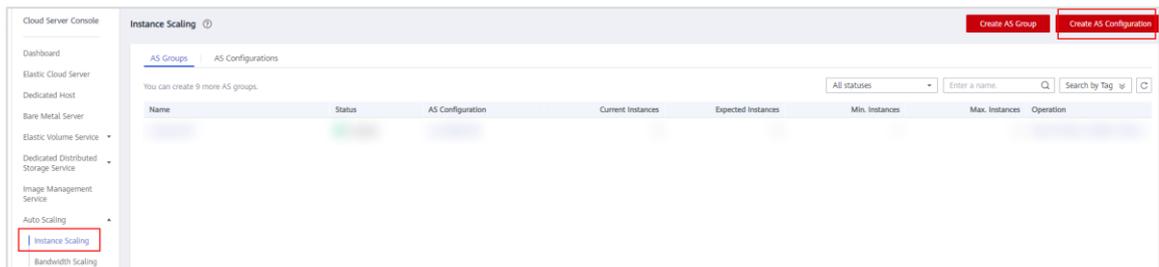
AS automatically adjusts resources based on your service requirements and configured AS policies. In this section, bandwidth scaling is performed.

1.1.6.1 Creating an AS Configuration

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



Step 2 Click **Create AS Configuration**.



Step 3 Set the following parameters:

- **Region:** AP-Hong Kong
- **Name:** Use the default name **as-config-f1e6** here.
- **Configuration Template:** Select **Use the specifications of an existing ECS**. Click **Select ECS**. In the **Select ECS** dialog box, select an existing ECS, for example, **ecs-Windows2012**.



Create AS Configuration

* Region: AP-Hong-Kong

* Name: as-config-f1e6

* Configuration Template: Use specifications of an existing ECS

Select ECS

You can only select an ECS in Running or Stopped state.

Name	Status	Specifications	Image	Created
<input type="radio"/> ecs-test	Running	s2.medium.4 1 vCPUs...	image-windows	Aug 12, 2020 20:30:45...
<input checked="" type="radio"/> ecs-Windows2012	Running	s2.small.1 1 vCPUs 1...	Windows Server 2012 ...	Aug 12, 2020 17:09:06...
<input type="radio"/> ecs-linux	Running	s2.medium.2 1 vCPUs...	CentOS 7.6 64bit	Aug 12, 2020 17:03:19...

OK Cancel

- **EIP: Automatically assign**
- **Type: Dynamic BGP**
- **Billed By: Bandwidth**
- **Bandwidth: 1 Mbit/s**
- **Login Mode: Password**
- **Password: Enter a desired password.**
- **Enter the password again for Confirm Password.**

EIP: Do not use | Automatically assign

* Type: Dynamic BGP

* Billed By: Bandwidth (For heavy/stable traffic)

* Bandwidth: 1 Mbit/s

* Login Mode: Key pair | Password

Username: Administrator

* Password: [Masked]

* Confirm Password: [Masked]

Advanced Settings: Do not configure | Configure now

ECS Price: \$0.04 USD/hour

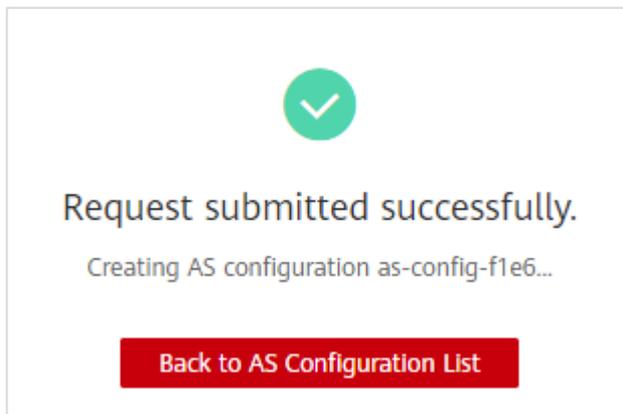
AS is free of charge. The fees are for the ECSs added based on the AS configuration for the AS group and are for reference only.

Create Now



Step 4 Click **Create Now**.

The following page is displayed.



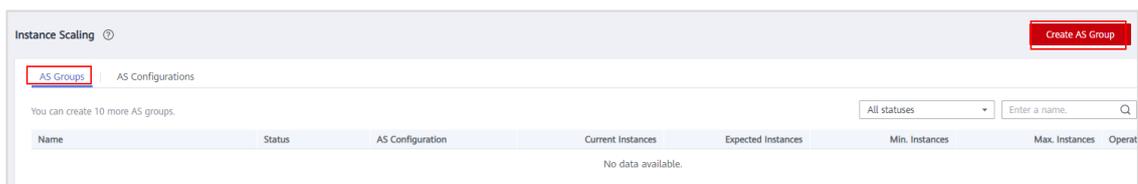
Step 5 In the AS Configuration list, view the created AS configuration **as-config-f1e6**.

Name	Status	Specifications	Image	System Disk	Data Disks	Login Mode	Created	Billing Mode	Operation
as-config-f1e6	Unbound	s2.small.1 1 vCPUs 1 GB	Windows Server 2012 R2 Stan...	High I/O 40 GB	0	Password	Aug 12, 2020 20:42:03 GMT...	Pay-per-use	Copy Delete

----End

1.1.6.2 Creating an AS Group

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



Step 2 Set the following parameters and then click **Create Now**.

- **Region:** AP-Hong Kong
- **AZ:** Select all AZs. All AZs in the same region can communicate with each other over an intranet.
- **Multi-AZ Expansion Policy:** Load-balanced
- **Name:** for example, **as-group-CB**
- **Max. Instances:** 3
- **Expected Instances:** 2
- **Min. Instances:** 1



Create AS Group

* Region
Regions are geographic areas isolated from each other. Resources are internal network connections. For low network latency and quick res

* AZ C

* Multi-AZ Extension Policy Load-balanced Sequenced

* Name

* Max. Instances

* Expected Instances

* Min. Instances

- **AS Configuration:** Select the created AS configuration **as-config-f1e6**.
- **VPC:** Select an existing VPC from the drop-down list for **VPC**. If no VPC is available, click **Create VPC**.
- **Subnet:** Retain the default value. The system automatically selects a subnet in the VPC.
- **Load Balancing:** Do not use
- **AS configuration Instance Removal Policy:** Oldest instance created from oldest AS configuration
- **EIP:** Release
- **Data Disk:** Release
- **Health Check Method:** ECS health check
- **Health Check Interval:** 5 minutes
- **Health Check Grace Period (s):** 600
- **Tag:** not required



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

* AS Configuration: as-config-f1e6 +

* VPC: vpc-default (192.168.0.0/16) Create VPC

* Subnet: subnet-c4d8 (192.168.0.0/24) This subnet is used by the primary NIC.
Add Subnet You can add 4 more subnets. Create Subnet

Load Balancing: Do not use | Elastic load balancer

* Instance Removal Policy: Oldest instance created from oldest AS c...
EIP: Release | Do not release
Data Disk: Release | Do not release

* Health Check Method: ECS health check
* Health Check Interval: 5 minutes
* Health Check Grace Period (s): 600

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

ECS Price \$0.01 USD/hour

Step 3 Click **Back to AS Group List** to view the created AS group **as-group-CB**.



Request submitted successfully.

Creating AS group as-group-CB...

After the AS group is created, add AS policies to it to trigger scaling actions.

[Add AS Policy](#) [Back to AS Group List](#)

Instance Scaling

AS Groups | AS Configurations

You can create 9 more AS groups. All statuses

Name	Status	AS Configuration	Current Instances	Expected Instances	Min. Instances
as-group-CB	Enabled	as-config-f1e6	0	2	1

Step 4 Locate the row that contains the target AS group and click **View AS Policy** in the **Operation** column.



Name	Status	AS Configuration	Current Instances	Expected Instances	Min. Instances	Max. Instances	Operation
as-group-CB	Enabled	as-config-f1e6	2	2	1	3	View AS Policy

Step 5 Click **Add AS Policy**.

< | as-group-CB

Overview | Monitoring | Instances | Scaling Actions | **AS Policies** | Notifications | Tags | Lifecycle Hooks

An AS policy defines the condition for triggering a scaling action. [Learn more](#)

Add AS Policy | Enable | Disable | Delete | You can add 10 more policies.

<input type="checkbox"/>	Name	Status	Policy Type	Trigger Condition	Scaling Action	Cooldown Perio...
No data available.						

Step 6 In the **Add AS Policy** dialog box, set the following parameters:

- **Policy Name:** for example, **as-policy-test1**
- **Policy Type:** **Periodic**
- **Interval:** **One day**
- **Triggered At:** **18:00**
- **Time Range:** Retain the default value.
- **Scaling Action:** **Add 1 instance**
- **Cooldown Period (s):** **900**



The screenshot shows the 'Add AS Policy' dialog box in the Huawei Cloud console. The dialog box is open over the 'AS Policies' tab. The 'Add AS Policy' button is highlighted with a red box. The dialog box contains the following fields:

- Policy Name: as-policy-test1
- Policy Type: Alarm, Scheduled, Periodic
- Interval: One day
- Time Zone: GMT+08:00
- Triggered At: 18:00
- Time Range: Aug 12, 2020 20:52:43 - Aug 13, 2020 20:52:43
- Scaling Action: Add, 1, instances
- Cooldown Period (s): 300

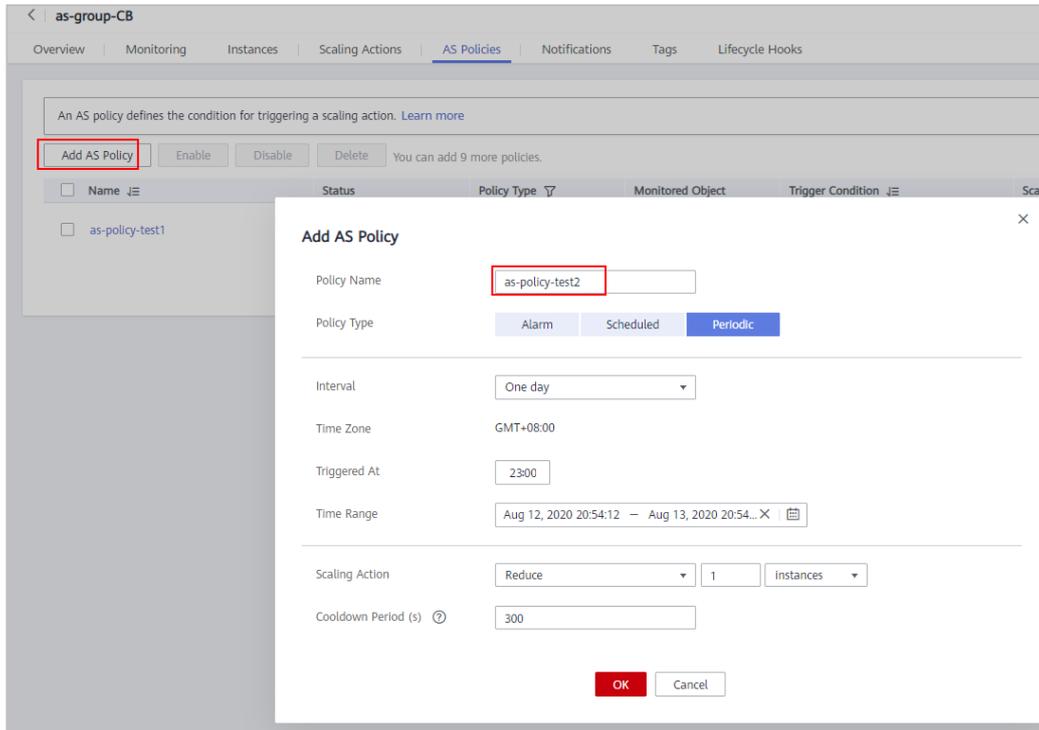
The OK button is highlighted with a red box.

Step 7 Click **OK** and then click **Add AS Policy** again.

The screenshot shows the 'AS Policies' tab in the Huawei Cloud console. The 'Add AS Policy' button is highlighted with a red box. The table below it is empty, showing 'No data available.'

Step 8 Set the following parameters:

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

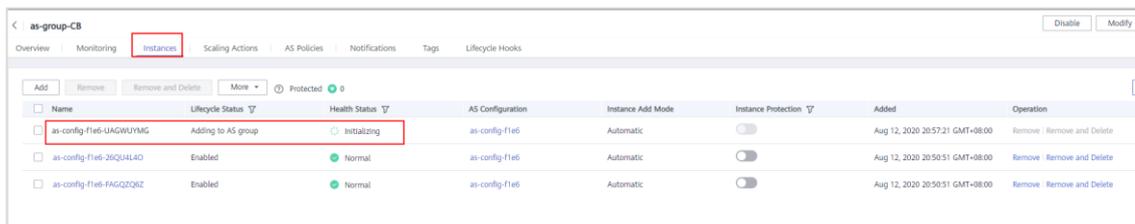
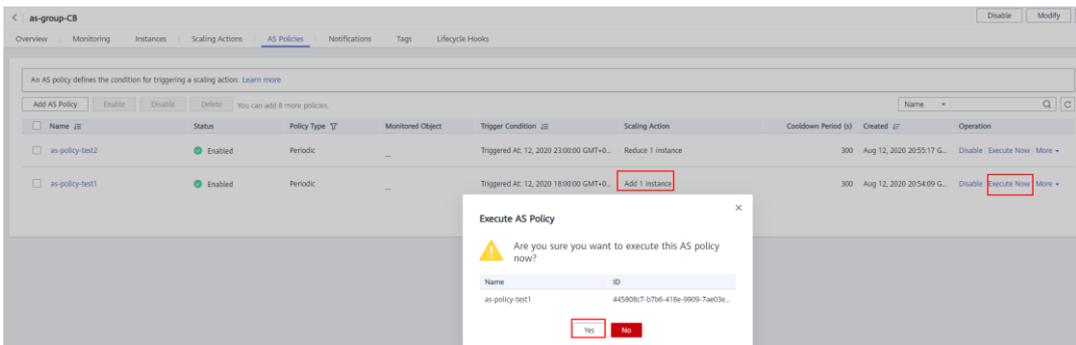


Step 9 Click **OK**.

Step 10 Wait till the triggering times of both AS policies expire.

Step 11 Click the **Monitoring** tab and reserve the changes in the number of instances triggered by the two periodic policies as shown in the following figure.

Considering time restrictions, you can click **Execute Now** to make the created policy **as-policy-test1** take effect immediately. A new instance is then added.



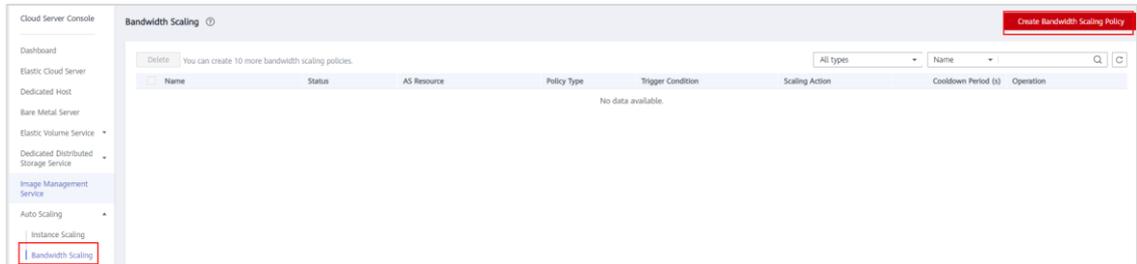
----End



1.1.6.3 (Optional) Creating a Bandwidth Scaling Policy

Step 1 On the management console, choose **Service List > Computing > Auto Scaling**.

Step 2 In the left navigation pane, choose **Bandwidth Scaling**. Click **Create Bandwidth Scaling Policy**.



Step 3 Set the following parameters:

- **Region:** AP-Hong Kong
- **Policy Name:** for example, **as-policy-test**
- **Resource Type:** EIP. Select an existing EIP or create a new one.
- **Policy Type:** Scheduled
- **Triggered On:** Retain the default setting. Generally, the value is several minutes later than the current time.
- **Scaling Action:** Set to 5 Mbit/s
- **Cooldown Period (s):** 300

Create Bandwidth Scaling Policy

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

Policy Name: as-policy-test

Resource Type: EIP (Selected) Shared bandwidth

EIP: 119.8.33.27 Buy EIP
Bandwidth Size: 1 Mbit/s Only pay-per-use shared bandwidths of EIPs can be scaled.

Policy Type: Alarm Scheduled (Selected) Periodic

Time Zone: GMT+08:00

Triggered On: Aug 12, 2020 20:39:22
The specified time must be later than the default time and the current system time.

Scaling Action: Set to 5 Mbit/s
The minimum added or reduced bandwidth value allowed varies depending on the bandwidth range. The adjusted bandwidth will be automatically set to a value closest to a multiple of the minimum added or reduced bandwidth value allowed.

Cooldown Period (s): 300

Create Now



Step 4 Click **Create Now**.

Step 5 Wait for a short while and then return to the page that displays the bandwidth scaling policy list.

Name	Status	AS Resource	Policy Type	Trigger Condition	Scaling Action
as-policy-test	Enabled	EIP 119.8.33.27	Scheduled	Triggered On: Aug 12, 2020 21:20:00 ...	Set to 5 Mbit/s

Step 6 Locate the row that contains the target policy and click the EIP.

On the page that displays the details about the EIP, the bandwidth has been changed to 5 Mbit/s.

Bandwidth Name	ecs-Windows2012-bandwidth-b1e1	Billing Mode	Pa
Bandwidth ID	ff240fa7-0458-452a-9866-1476f45889b4	Bandwidth (Mbit/s)	5
Billed By	Bandwidth		
Bandwidth Type	Dedicated		

----End

1.2 Container Operations

1.2.1 Introduction

This exercise involves ECSs and Docker containers, including creating and logging in to an ECS, creating, viewing, and running a Docker container, building a Docker image, and setting up a private registry.

1.2.2 Objectives

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

- Create, view, enter, and run a container.
- Build a container image.
- Set up a private registry.

1.2.3 Tasks

In this exercise, you will perform container-related operations on the ECS.



1.2.4 Basic Container Operations

1.2.4.1 Logging In to the ECS

Step 1 Create a Linux ECS. If an existing Linux ECS is available, skip this step.

Step 2 Log in to the ECS.

- **Username:** root
- **Password:** Enter the password you set when creating the ECS.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.12.1.el7.x86_64 on an x86_64

ecs-linux login: root
Password:
Login incorrect

ecs-linux login: root
Password:
Last failed login: Tue Jun  9 13:37:36 CST 2020 on tty1
There were 3 failed login attempts since the last successful login.

Welcome to Huawei Cloud Service

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

If information highlighted in the red box is displayed, you have logged in to the ECS successfully.

----End

1.2.4.2 Installing the Docker Environment

Step 1 Check the kernel version of the system.

```
uname -r
```

```
[root@ecs-linux ~]# uname -r
3.10.0-1062.12.1.el7.x86_64
```

Step 2 Log in to CentOS as user **root**. Update the Yellowdog Updater, Modified (YUM) package to the latest version.

```
sudo yum update
```

YUM is a free, open-source RPM package management tool in Linux. Enter **y** in the subsequent operations.

```
[root@ecs-linux ~]# sudo yum update
Loaded plugins: fastestmirror
Determining fastest mirrors
epel/x86_64/metalink | 7.6 kB 00:00:00
```



```
perl-Socket x86_64 2.010-5.el7 base 49 k
perl-libs x86_64 4:5.16.3-295.el7 base 689 k
perl-macros x86_64 4:5.16.3-295.el7 base 44 k
plymouth x86_64 0.8.9-0.33.20140113.el7.centos base 116 k
plymouth-core-libs x86_64 0.8.9-0.33.20140113.el7.centos base 108 k
plymouth-scripts x86_64 0.8.9-0.33.20140113.el7.centos base 39 k
policycoreutils x86_64 2.5-34.el7 base 917 k
polkit x86_64 0.112-26.el7 base 178 k
postfix x86_64 2:2.10.1-9.el7 base 2.4 M
procps-ng x86_64 3.3.10-27.el7 base 291 k
python x86_64 2.7.5-88.el7 base 96 k
python-firewall noarch 0.6.3-8.el7_8.1 updates 354 k
python-libs x86_64 2.7.5-88.el7 base 5.6 M
python-perf x86_64 3.10.0-1127.10.1.el7 updates 8.0 M
python-urlgrabber noarch 3.10-10.el7 base 108 k
rpm x86_64 4.11.3-43.el7 base 1.2 M
rpm-build-libs x86_64 4.11.3-43.el7 base 107 k
rpm-libs x86_64 4.11.3-43.el7 base 278 k
rpm-python x86_64 4.11.3-43.el7 base 84 k
rsyslog x86_64 8:24.0-52.el7 base 620 k
sed x86_64 4.2.2-6.el7 base 231 k
selinux-policy noarch 3.13.1-266.el7 base 497 k
selinux-policy-targeted noarch 3.13.1-266.el7 base 7.0 M
setup noarch 2.8.71-11.el7 base 166 k
sg3_utils x86_64 1:1.37-19.el7 base 646 k
sg3_utils-libs x86_64 1:1.37-19.el7 base 65 k
shared-mime-info x86_64 1.8-5.el7 base 312 k
sos noarch 3.8-8.el7.centos updates 517 k
strace x86_64 4.24-4.el7 base 901 k
sudo x86_64 1.8.23-9.el7 base 842 k
systemd x86_64 219-73.el7_8.6 updates 5.1 M
systemd-libs x86_64 219-73.el7_8.6 updates 416 k
systemd-sysv x86_64 219-73.el7_8.6 updates 94 k
teamd x86_64 1:29-1.el7 base 115 k
tuned noarch 2.11.0-8.el7 base 268 k
tzdata noarch 2020a-1.el7 updates 495 k
unzip x86_64 6.0-21.el7 base 171 k
util-linux x86_64 2.23.2-63.el7 base 2.0 M
yum noarch 3.4.3-167.el7.centos base 1.2 M
yum-plugin-fastestmirror noarch 1.1.31-54.el7_8 updates 34 k

Transaction Summary
-----
Install 3 Packages
Upgrade 142 Packages
Total download size: 293 M
Is this ok [y/d/N]: y
```

```
Total 8.0 MB/s | 293 MB 00:00:36
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importing GPG key 0xf40808e5:
Userid : "CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>"
Fingerprint: 6341 ab27 53d7 8a78 a7c2 7bb1 24c6 a8a7 f4a8 0eb5
Package : centos-release-7-6.1810.2.el7.centos.x86_64 (@anaconda)
From : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Is this ok [y/N]: y
```

```
libss.x86_64 0:1.42.9-17.el7
libuuid.x86_64 0:2.23.2-63.el7
libxml2-python.x86_64 0:2.9.1-6.el7.4
logrotate.x86_64 0:3.8.6-19.el7
mariadb-libs.x86_64 1:5.5.65-1.el7
numactl-libs.x86_64 0:2.0.12-5.el7
parted.x86_64 0:3.1-32.el7
perl.x86_64 4:5.16.3-295.el7
perl-libs.x86_64 4:5.16.3-295.el7
perl-macros.x86_64 4:5.16.3-295.el7
perl-Socket.x86_64 0:2.010-5.el7
perl-macros.x86_64 4:5.16.3-295.el7
plymouth-core-libs.x86_64 0:0.8.9-0.33.20140113.el7.centos
policycoreutils.x86_64 0:2.5-34.el7
postfix.x86_64 2:2.10.1-9.el7
python.x86_64 0:2.7.5-88.el7
python-libs.x86_64 0:2.7.5-88.el7
python-urlgrabber.noarch 0:3.10-10.el7
rpm-build-libs.x86_64 0:4.11.3-43.el7
rpm-python.x86_64 0:4.11.3-43.el7
sed.x86_64 0:4.2.2-6.el7
selinux-policy-targeted.noarch 0:3.13.1-266.el7
sg3_utils.x86_64 1:1.37-19.el7
shared-mime-info.x86_64 0:1.8-5.el7
strace.x86_64 0:4.24-4.el7
systemd.x86_64 0:219-73.el7_8.6
systemd-sysv.x86_64 0:219-73.el7_8.6
tuned.noarch 0:2.11.0-8.el7
unzip.x86_64 0:6.0-21.el7
yum.noarch 0:3.4.3-167.el7.centos
libteam.x86_64 0:1.29-1.el7
libxml2.x86_64 0:2.9.1-6.el7.4
linux-firmware.noarch 0:20191203-76.git0a0f4c.el7
lshw.x86_64 0:0.8.02.18-14.el7
microcode_ctl.x86_64 2:2.1-61.el7
pam.x86_64 0:1.1.8-23.el7
passwd.x86_64 0:0.79-6.el7
perl-Pod-Escapes.noarch 1:1.04-295.el7
perl-libs.x86_64 4:5.16.3-295.el7
plymouth.x86_64 0:0.8.9-0.33.20140113.el7.centos
plymouth-scripts.x86_64 0:0.8.9-0.33.20140113.el7.centos
polkit.x86_64 0:0.112-26.el7
procps-ng.x86_64 0:3.3.10-27.el7
python-firewall.noarch 0:0.6.3-8.el7_8.1
python-perf.x86_64 0:3.10.0-1127.10.1.el7
rpm.x86_64 0:4.11.3-43.el7
rpm-libs.x86_64 0:4.11.3-43.el7
rsyslog.x86_64 0:8.24.0-52.el7
selinux-policy.noarch 0:3.13.1-266.el7
setup.noarch 0:2.8.71-11.el7
sg3_utils-libs.x86_64 1:1.37-19.el7
sos.noarch 0:3.8-8.el7.centos
sudo.x86_64 0:1.8.23-9.el7
systemd-libs.x86_64 0:219-73.el7_8.6
teamd.x86_64 0:1.29-1.el7
tzdata.noarch 0:2020a-1.el7
util-linux.x86_64 0:2.23.2-63.el7
yum-plugin-fastestmirror.noarch 0:1.1.31-54.el7_8

Replaced:
iw17265-firmware.noarch 0:22.07.0-72.el7

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

Step 3 Install the required software package (yum-util provides yum-config-manager functionality).

```
sudo yum install -y yum-utils device-mapper-persistent-data lvm2
```



```
[root@ecs-linux ~]# sudo yum install -y yum-utils device-mapper-persistent-data lvm2
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.bit.edu.cn
 * epel: mirrors.bfsu.edu.cn
 * extras: mirror.bit.edu.cn
 * updates: mirrors.bfsu.edu.cn
Resolving Dependencies
--> Processing Dependency: libaio.so.1(LIBAIO_0.4)(64bit) for package: device-mapper-persistent-data-0.8.5-2.el7.x86_64
--> Processing Dependency: libaio.so.1(LIBAIO_0.1)(64bit) for package: device-mapper-persistent-data-0.8.5-2.el7.x86_64
--> Processing Dependency: libaio.so.1()(64bit) for package: device-mapper-persistent-data-0.8.5-2.el7.x86_64
--> Package lvm2.x86_64 7:2.02.186-7.el7_8.2 will be installed
--> Processing Dependency: lvm2-libs = 7:2.02.186-7.el7_8.2 for package: 7:lvm2-2.02.186-7.el7_8.2.x86_64
--> Processing Dependency: liblvm2app.so.2.2(Base)(64bit) for package: 7:lvm2-2.02.186-7.el7_8.2.x86_64
--> Processing Dependency: libdevmapper-event.so.1.02(Base)(64bit) for package: 7:lvm2-2.02.186-7.el7_8.2.x86_64
--> Processing Dependency: liblvm2app.so.2.2()(64bit) for package: 7:lvm2-2.02.186-7.el7_8.2.x86_64
--> Processing Dependency: libdevmapper-event.so.1.02()(64bit) for package: 7:lvm2-2.02.186-7.el7_8.2.x86_64
--> Package yum-utils.noarch 0:1.1.31-54.el7_8 will be installed
--> Processing Dependency: python-kitchen for package: yum-utils-1.1.31-54.el7_8.noarch
--> Running transaction check
--> Package device-mapper-event-libs.x86_64 7:1.02.164-7.el7_8.2 will be installed
--> Package libaio.x86_64 0:0.3.109-13.el7 will be installed
--> Package lvm2-libs.x86_64 7:2.02.186-7.el7_8.2 will be installed
--> Processing Dependency: device-mapper-event = 7:1.02.164-7.el7_8.2 for package: 7:lvm2-libs-2.02.186-7.el7_8.2.x86_64
--> Package python-kitchen.noarch 0:1.1.1-5.el7 will be installed
--> Processing Dependency: python-chardet for package: python-kitchen-1.1.1-5.el7.noarch
--> Running transaction check
--> Package device-mapper-event.x86_64 7:1.02.164-7.el7_8.2 will be installed
--> Package python-chardet.noarch 0:2.2.1-3.el7 will be installed
--> Finished Dependency Resolution

Installed:
  device-mapper-persistent-data.x86_64 0:0.8.5-2.el7    lvm2.x86_64 7:2.02.186-7.el7_8.2    yum-utils.noarch 0:1.1.31-54.el7_8

Dependency Installed:
  device-mapper-event.x86_64 7:1.02.164-7.el7_8.2    device-mapper-event-libs.x86_64 7:1.02.164-7.el7_8.2
  libaio.x86_64 0:0.3.109-13.el7                    lvm2-libs.x86_64 7:2.02.186-7.el7_8.2
  python-chardet.noarch 0:2.2.1-3.el7                python-kitchen.noarch 0:1.1.1-5.el7

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

Step 4 Set the **yum** source.

```
sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
```

```
[root@ecs-linux ~]# sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
Loaded plugins: fastestmirror
adding repo from: https://download.docker.com/linux/centos/docker-ce.repo
grabbing file https://download.docker.com/linux/centos/docker-ce.repo to /etc/yum/repos.d/docker-ce.repo
repo saved to /etc/yum/repos.d/docker-ce.repo
[root@ecs-linux ~]#
```

Step 5 View Docker versions in all repositories and select a specific version for installation.

```
yum list docker-ce --showduplicates | sort -r
```



```
[root@ecs-linux ~]# yum list docker-ce --showduplicates | sort -r
 * updates: mirrors.bfsu.edu.cn
Loading mirror speeds from cached hostfile
Loaded plugins: fastestmirror
 * extras: mirror.bit.edu.cn
 * epel: mirrors.bfsu.edu.cn
docker-ce.x86_64          3:19.03.9-3.e17          docker-ce-stable
docker-ce.x86_64          3:19.03.8-3.e17          docker-ce-stable
docker-ce.x86_64          3:19.03.7-3.e17          docker-ce-stable
docker-ce.x86_64          3:19.03.6-3.e17          docker-ce-stable
docker-ce.x86_64          3:19.03.5-3.e17          docker-ce-stable
docker-ce.x86_64          3:19.03.4-3.e17          docker-ce-stable
docker-ce.x86_64          3:19.03.3-3.e17          docker-ce-stable
docker-ce.x86_64          3:19.03.2-3.e17          docker-ce-stable
docker-ce.x86_64          3:19.03.1-3.e17          docker-ce-stable
docker-ce.x86_64          3:19.03.11-3.e17         docker-ce-stable
docker-ce.x86_64          3:19.03.10-3.e17         docker-ce-stable
docker-ce.x86_64          3:19.03.0-3.e17          docker-ce-stable
docker-ce.x86_64          3:18.09.9-3.e17          docker-ce-stable
docker-ce.x86_64          3:18.09.8-3.e17          docker-ce-stable
docker-ce.x86_64          3:18.09.7-3.e17          docker-ce-stable
docker-ce.x86_64          3:18.09.6-3.e17          docker-ce-stable
docker-ce.x86_64          3:18.09.5-3.e17          docker-ce-stable
docker-ce.x86_64          3:18.09.4-3.e17          docker-ce-stable
docker-ce.x86_64          3:18.09.3-3.e17          docker-ce-stable
docker-ce.x86_64          3:18.09.2-3.e17          docker-ce-stable
docker-ce.x86_64          3:18.09.1-3.e17          docker-ce-stable
docker-ce.x86_64          3:18.09.0-3.e17          docker-ce-stable
docker-ce.x86_64          18.06.3.ce-3.e17         docker-ce-stable
docker-ce.x86_64          18.06.2.ce-3.e17         docker-ce-stable
docker-ce.x86_64          18.06.1.ce-3.e17         docker-ce-stable
docker-ce.x86_64          18.06.0.ce-3.e17         docker-ce-stable
docker-ce.x86_64          18.03.1.ce-1.e17.centos  docker-ce-stable
docker-ce.x86_64          18.03.0.ce-1.e17.centos  docker-ce-stable
docker-ce.x86_64          17.12.1.ce-1.e17.centos  docker-ce-stable
docker-ce.x86_64          17.12.0.ce-1.e17.centos  docker-ce-stable
docker-ce.x86_64          17.09.1.ce-1.e17.centos  docker-ce-stable
docker-ce.x86_64          17.09.0.ce-1.e17.centos  docker-ce-stable
docker-ce.x86_64          17.06.2.ce-1.e17.centos  docker-ce-stable
docker-ce.x86_64          17.06.1.ce-1.e17.centos  docker-ce-stable
docker-ce.x86_64          17.06.0.ce-1.e17.centos  docker-ce-stable
docker-ce.x86_64          17.03.3.ce-1.e17         docker-ce-stable
docker-ce.x86_64          17.03.2.ce-1.e17.centos  docker-ce-stable
docker-ce.x86_64          17.03.1.ce-1.e17.centos  docker-ce-stable
docker-ce.x86_64          17.03.0.ce-1.e17.centos  docker-ce-stable
 * base: mirror.bit.edu.cn
Available Packages
[root@ecs-linux ~]#
```

Step 6 Install Docker. Enter **y** in the subsequent operations. (The installation duration depends on the bandwidth of the ECS. If a small bandwidth is used, you may need to wait for 5 to 10 minutes.)

```
sudo yum install docker-ce
```



```
--> Package docker-ce-cli.x86_64 1:19.03.11-3.el7 will be installed
--> Package libcgroupp.x86_64 0:0.41-21.el7 will be installed
--> Running transaction check
--> Package policycoreutils-python.x86_64 0:2.5-34.el7 will be installed
--> Processing Dependency: setools-libs >= 3.3.8-4 for package: policycoreutils-python-2.5-34.el7.x86_64
--> Processing Dependency: libsemanage-python >= 2.5-14 for package: policycoreutils-python-2.5-34.el7.x86_64
--> Processing Dependency: audit-libs-python >= 2.1.3-4 for package: policycoreutils-python-2.5-34.el7.x86_64
--> Processing Dependency: python-IPy for package: policycoreutils-python-2.5-34.el7.x86_64
--> Processing Dependency: libqpol.so.1(UEERS_1.4)(64bit) for package: policycoreutils-python-2.5-34.el7.x86_64
--> Processing Dependency: libqpol.so.1(UEERS_1.2)(64bit) for package: policycoreutils-python-2.5-34.el7.x86_64
--> Processing Dependency: libqpol.so.4(UEERS_4.0)(64bit) for package: policycoreutils-python-2.5-34.el7.x86_64
--> Processing Dependency: checkpolicy for package: policycoreutils-python-2.5-34.el7.x86_64
--> Processing Dependency: libqpol.so.1()(64bit) for package: policycoreutils-python-2.5-34.el7.x86_64
--> Processing Dependency: libqpol.so.4()(64bit) for package: policycoreutils-python-2.5-34.el7.x86_64
--> Running transaction check
--> Package audit-libs-python.x86_64 0:2.8.5-4.el7 will be installed
--> Package checkpolicy.x86_64 0:2.5-8.el7 will be installed
--> Package libsemanage-python.x86_64 0:2.5-14.el7 will be installed
--> Package python-IPy.noarch 0:0.75-6.el7 will be installed
--> Package setools-libs.x86_64 0:3.3.8-4.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package arch Version Repository Size
=====
Installing:
docker-ce x86_64 3:19.03.11-3.el7 docker-ce-stable 24 M
Installing for dependencies:
audit-libs-python x86_64 2.8.5-4.el7 base 76 k
checkpolicy x86_64 2.5-8.el7 base 295 k
container-selinux noarch 2:2.119.1-1.c57a6f9.el7 extras 48 k
containerd.io x86_64 1.2.13-3.2.el7 docker-ce-stable 25 M
docker-ce-cli x86_64 1:19.03.11-3.el7 docker-ce-stable 38 M
libcgroupp x86_64 0.41-21.el7 base 66 k
libsemanage-python x86_64 2.5-14.el7 base 113 k
policycoreutils-python x86_64 2.5-34.el7 base 457 k
python-IPy noarch 0.75-6.el7 base 32 k
setools-libs x86_64 3.3.8-4.el7 base 628 k
=====

Transaction Summary
=====
Install 1 Package (+10 Dependent packages)

Total download size: 89 M
Installed size: 365 M
Is this ok [y/d/N]: y_
```

```
Downloading packages:
(1/11): audit-libs-python-2.8.5-4.el7.x86_64.rpm | 76 kB 00:00:00
(2/11): container-selinux-2.119.1-1.c57a6f9.el7.noarch.rpm | 48 kB 00:00:00
(3/11): checkpolicy-2.5-8.el7.x86_64.rpm | 295 kB 00:00:00
warning: rpm:rsync.gpg/x86_64/7/docker-ce-stable/packages/docker-ce-19.03.11-3.el7.x86_64.rpm: Header V4 RSA/SHA512 Signature,
key ID 621e9f35: NOKEY
Public key for docker-ce-19.03.11-3.el7.x86_64.rpm is not installed
(4/11): docker-ce-19.03.11-3.el7.x86_64.rpm | 24 MB 00:00:05
(5/11): libcgroupp-0.41-21.el7.x86_64.rpm | 66 kB 00:00:00
(6/11): python-IPy-0.75-6.el7.noarch.rpm | 32 kB 00:00:00
(7/11): libsemanage-python-2.5-14.el7.x86_64.rpm | 113 kB 00:00:00
(8/11): setools-libs-3.3.8-4.el7.x86_64.rpm | 628 kB 00:00:00
(9/11): docker-ce-cli-19.03.11-3.el7.x86_64.rpm | 38 MB 00:00:05
(10/11): containerd.io-1.2.13-3.2.el7.x86_64.rpm | 25 MB 00:00:11
(11/11): policycoreutils-python-2.5-34.el7.x86_64.rpm | 457 kB 00:00:24

Total 2.9 MB/s | 89 MB 00:00:30
Retrieving key from https://download.docker.com/linux/centos/gpg
Importing GPG key 0x621E9F35:
Userid : "Docker Release (CE rpm) <docker@docker.com>"
Fingerprint: 0600 61c5 1b55 8a7f 742b 77aa c52f eb6b 621e 9f35
From : https://download.docker.com/linux/centos/gpg
Is this ok [y/N]: y
```

```
Installed:
docker-ce.x86_64 3:19.03.11-3.el7

Dependency Installed:
audit-libs-python.x86_64 0:2.8.5-4.el7
container-selinux.noarch 2:2.119.1-1.c57a6f9.el7
docker-ce-cli.x86_64 1:19.03.11-3.el7
libsemanage-python.x86_64 0:2.5-14.el7
python-IPy.noarch 0:0.75-6.el7
checkpolicy.x86_64 0:2.5-8.el7
containerd.io.x86_64 0:1.2.13-3.2.el7
libcgroupp.x86_64 0:0.41-21.el7
policycoreutils-python.x86_64 0:2.5-34.el7
setools-libs.x86_64 0:3.3.8-4.el7

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

If an error occurs during the installation, you can manually input the command. Pay attention to the command format and the space between commands. You can also install Docker in other methods.

Step 7 Start Docker and add it to the startup items list.

```
sudo systemctl start docker
sudo systemctl enable docker
```



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

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

- Step 8 Check whether the installation is successful. If the command output contains **client** and **service**, Docker is installed and started successfully.

docker version

```
[root@ecs-linux ~]# docker version
Client: Docker Engine - Community
 Version:           19.03.11
 API version:       1.40
 Go version:        go1.13.10
 Git commit:        42e35e61f3
 Built:             Mon Jun 1 09:13:48 2020
 OS/Arch:           linux/amd64
 Experimental:      false

Server: Docker Engine - Community
 Engine:
  Version:           19.03.11
  API version:       1.40 (minimum version 1.12)
  Go version:        go1.13.10
  Git commit:        42e35e61f3
  Built:             Mon Jun 1 09:12:26 2020
  OS/Arch:           linux/amd64
  Experimental:      false
 containerd:
  Version:           1.2.13
  GitCommit:        7ad184331fa3e55e52b890ea95e65ba581ae3429
 runc:
  Version:           1.0.0-rc10
  GitCommit:        dc9208a3383fcef5b3839f4323d9beb36df0a9dd
 docker-init:
  Version:           0.18.0
  GitCommit:        fec3683
```

----End

1.2.4.3 Running a Container

- Step 1 Create an httpd container named **huawei**.

docker create --name huawei httpd

```
[root@ecs-linux ~]# docker create --name huawei httpd
Unable to find image 'httpd:latest' locally
latest: Pulling from library/httpd
8559a31e96f4: Pull complete
bd517d441028: Pull complete
f67807e59c3c: Pull complete
83c578481926: Pull complete
f3cbcb88690d: Pull complete
Digest: sha256:f5edf1ab099b35909635f3340b0f0a2cd3f57bd797990b94b6bcd31cf202f219
Status: Downloaded newer image for httpd:latest
965afc7d0ae00b366e56888dcd1ea8a29bae3aaa22572b77e8eed6ba3c728bf4
```

- Step 2 View the container status.

docker ps -a



```
[root@ecs-linux ~]# docker ps -a
CONTAINER ID   IMAGE     COMMAND                  CREATED          STATUS          PORTS          NAMES
965afc7d8ae8   httpd    "httpd-foreground"     About a minute ago   Created
```

Step 3 Start the **huawei** container.

```
docker start huawei
```

```
[root@ecs-linux ~]# docker start huawei
```

Step 4 Check the **huawei** container status again. The status is **Up**.

```
docker container ls
```

```
[root@ecs-linux ~]# docker container ls
CONTAINER ID   IMAGE     COMMAND                  CREATED          STATUS          PORTS          NAMES
881ed6c71826   httpd    "httpd-foreground"     6 minutes ago   Up 14 seconds   80/tcp        huawei
[root@ecs-linux ~]#
```

Step 5 Stop the **huawei** container and verify that the container is in the **Exited** state.

```
docker stop huawei
```

```
docker ps -a
```

```
[root@ecs-linux ~]# docker stop huawei
huawei
[root@ecs-linux ~]# docker ps -a
CONTAINER ID   IMAGE     COMMAND                  CREATED          STATUS          PORTS          PORTS          NAMES
881ed6c71826   httpd    "httpd-foreground"     8 minutes ago   Exited(0)      About a minute ago
```

Step 6 Delete the **huawei** container and check the container information.

```
docker rm huawei
```

```
docker ps -a
```

```
[root@ecs-linux ~]# docker rm huawei
huawei
[root@ecs-linux ~]# docker ps -a
CONTAINER ID   IMAGE     COMMAND                  CREATED          STATUS          PORTS          NAMES
[root@ecs-linux ~]#
```

The container is deleted successfully.

----End

1.2.4.4 Entering a Container Using the **docker exec** Command

Step 1 Run an httpd container named **httpd1** at the backend and map its service port 80 to port 8080 of the host machine.

```
docker run --name httpd1 -d -p 8080:80 httpd
```



```
[root@ecs-linux ~]# docker run --name httpd1 -d -p 8080:80 httpd
1f1dcd65d2c0de40ad42c0f8e8d0ccfda98c85ba0f1630bdb556a1d4d1f0d4e0
```

Step 2 Access the container **httpd1**.

```
curl 127.0.0.1:8080
```

```
[root@ecs-linux ~]# curl 127.0.0.1:8080
<html><body><h1>It works!</h1></body></html>
```

Step 3 Enter the container **httpd1**.

```
docker exec -it httpd1 bash
```

```
[root@ecs-linux ~]# docker exec -it httpd1 bash
root@1f1dcd65d2c0:/usr/local/apache2# ls
bin build cgi-bin conf error htdocs icons include logs modules
```

Step 4 Modify the static files in the **httpd1** container and enter **exit** to exit.

```
cd htdocs
ls
echo "update to httpd" > index.html
exit
```

```
root@1f1dcd65d2c0:/usr/local/apache2# cd htdocs
root@1f1dcd65d2c0:/usr/local/apache2/htdocs# ls
index.html
root@1f1dcd65d2c0:/usr/local/apache2/htdocs# echo "update to httpd" > index.html
root@1f1dcd65d2c0:/usr/local/apache2/htdocs# exit
exit
[root@ecs-linux ~]#
```

Step 5 Access the container **httpd1** again. If the container can be accessed, the **exit** does not end the container process.

```
curl 127.0.0.1:8080
```

```
[root@ecs-linux ~]# curl 127.0.0.1:8080
update to httpd
[root@ecs-linux ~]# _
```

----End



1.2.5 (Optional) Building a Container Image Through Dockerfile

Step 1 Create a **dockerfile** folder in the **/root** directory.

```
mkdir dockerfile
```

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

Step 2 Create a Dockerfile file named **dockerfile1**.

```
cd dockerfile  
touch dockerfile1
```

```
[root@ecs-linux ~]# mkdir dockerfile  
[root@ecs-linux ~]# cd dockerfile/  
[root@ecs-linux dockerfile]# touch dockerfile1
```

Step 3 Edit the **dockerfile1** file using the vi editor.

```
vi dockerfile1
```

Enter the following content:

```
FROM httpd  
MAINTAINER Gale@Huawei.com  
RUN echo "dockerfile test"> /usr/local/apache2/htdocs/index.html
```

Press **Esc** and run the **:wq** command to save the configuration and exit.



```
1 httpd
MAINTAINER Gale@Huawei.com
RUN echo "dockerfile test" > /usr/local/apache2/htdocs/index.html
```

Step 4 Build an image named `httpd:v11`.

```
docker build -t httpd:v11 -f dockerfile1 /root/dockerfile
```

```
"dockerfile1" 5L, 185C written
[root@ecs-linux ~]# docker build -t httpd:v11 -f dockerfile1 /root/dockerfile
Sending build context to Docker daemon 1.641kB
Step 1/3 : FROM httpd
--> 9d2a0c6e5b57
Step 2/3 : MAINTAINER Gale@Huawei.com
--> Running in 89341eee29a8
Removing intermediate container 89341eee29a8
--> 5cb8e6cfec2d
Step 3/3 : RUN echo "dockerfile test" > /usr/local/apache2/htdocs/index.html
[21499.313776] docker0: port 2(veth38466bb) entered blocking state
[21499.314395] docker0: port 2(veth38466bb) entered disabled state
--> Running in 8048d7af2b30
[21499.321888] device veth38466bb entered promiscuous mode
[21499.322498] IPv6: ADDRCONF(NETDEV_UP): veth38466bb: link is not ready
[21499.323140] docker0: port 2(veth38466bb) entered blocking state
[21499.323718] docker0: port 2(veth38466bb) entered forwarding state
5722 docker0: port 2(veth38466bb) entered disabled state
"docker475530 5IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[21499.475530] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Sending 479306 cIPv6: ADDRCONF(NETDEV_CHANGE): veth38466bb: link becomes ready
Step 1/4800130Mdocker0: port 2(veth38466bb) entered blocking state
--> 9d80619e5docker0: port 2(veth38466bb) entered forwarding state e
Step 2/570130INDocker0: port 2(veth38466bb) entered disabled state
--> R585452 idocker0: port 2(veth38466bb) entered disabled state
Removing 586797rmeevice veth38466bb left promiscuous mode
--> 5587459fecocker0: port 2(veth38466bb) entered disabled state
Removing intermediate container 8048d7af2b30 d ndex.html
--> 66b9688dbd92
Successfully built 66b9688dbd92
Successfully tagged httpd:v11 p d ndex.html
[root@ecs-linux ~]#
```



Step 5 View the built image.

docker images

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

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
httpd	v11	66b9688dbd92	58 seconds ago	166MB
httpd	latest	9d2a8c6e5b57	6 days ago	166MB

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

Step 6 Run a container created from the image **httpd:v11**.

docker run -d -p 8081:80 httpd:v11

```
[root@ecs-linux ~]# docker run -d -p 8081:80 httpd:v11
1b057ac2bb6569ae1c8d3cf5458e8122542b6e77ceede772d9ea5154aa9268e5
```

Step 7 Access the container.

curl 127.0.0.1:8081

```
[root@ecs-linux ~]# curl 127.0.0.1:8081
dockerfile test
```

----End

1.2.6 (Optional) Setting Up a Private Registry

Step 1 Create a **myregistry** folder in the **/root** directory to store the private registry.

mkdir myregistry

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

Step 2 Run a registry container and map the host's port 1000 to the container's port 5000 and mount the folder created in the preceding step as the image storage folder.

docker run -d -p 1000:5000 -v /root/myregistry:/var/lib/registry registry



```
[root@ecs-linux ~]# docker run -d -p 8081:80 httpd:v11
144e58476db5dd2da4b71e8183285e8e4ff8f8ce5bd92ba8f35f3f856843726f5
[21586.525316] docker0: port 2(veth354e108) entered blocking state
[21586.526871] docker0: port 2(veth354e108) entered disabled state
[21586.533969] device veth354e108 entered promiscuous mode
[21586.534716] IPv6: ADDRCONF(NETDEV_UP): veth354e108: link is not ready
[21586.535477] docker0: port 2(veth354e108) entered blocking state
[21586.536187] docker0: port 2(veth354e108) entered forwarding state
[21586.548286] docker0: port 2(veth354e108) entered disabled state
[21586.693482] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[21586.696682] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[21586.697432] IPv6: ADDRCONF(NETDEV_CHANGE): veth354e108: link becomes ready
[21586.698269] docker0: port 2(veth354e108) entered blocking state
[21586.698987] docker0: port 2(veth354e108) entered forwarding state
[root@ecs-linux ~]# curl 127.0.0.1:8081
dockerfile test
[root@ecs-linux ~]# mkdir myregistry
[root@ecs-linux ~]# docker run -d -p 1000:5000 -v /root/myregistry:/var/lib/registry registry
Unable to find image 'registry:latest' locally
latest: Pulling from library/registry
c4db67a5bc2a: Pull complete
47112e65547d: Pull complete
46bcb632e586: Pull complete
c1cc712bcecd: Pull complete
3db6272dcbfa: Pull complete
Digest: sha256:8be26f81ffea54106bae812c6f349df70f4d5e7e2ec81b143c46e2c83b9e551d
Status: Downloaded newer image for registry:latest
a653968889d1d04fa838219df54191a0e381b1ea8fe0f8084444e89495f7e6ca
[root@ecs-linux ~]#
```

Step 3 Change the format of `httpd:v11` to the format required by the registry.

```
docker tag httpd:v11 127.0.0.1:1000/michael/httpd:v11
docker images
```

```
[root@ecs-linux ~]# docker tag httpd:v11 127.0.0.1:1000/michael/httpd:v11
[root@ecs-linux ~]# docker images
REPOSITORY          TAG          IMAGE ID          CREATED          SIZE
127.0.0.1:1000/michael/httpd  v11         66b9688dbd92     7 minutes ago   166MB
httpd                v11         66b9688dbd92     7 minutes ago   166MB
httpd                latest      9d2a8c6e5b57     6 days ago      166MB
registry             latest      2d4f4b5389b1     5 weeks ago     26.2MB
[root@ecs-linux ~]#
```

Step 4 Upload the `michael/httpd:v11` image to the registry.

```
docker push 127.0.0.1:1000/michael/httpd:v11
```

```
[root@ecs-linux ~]# docker push 127.0.0.1:1000/michael/httpd:v11
The push refers to repository [127.0.0.1:1000/michael/httpd]
e8624b4d9d6: Pushed
e6cfff37f35: Pushed
878e6411b28: Pushed
292ec64385a: Pushed
8b213d315e5: Pushed
5ef25a32843: Pushed
11: digest: sha256:295bd56858af35be482acfc5cda765631db8bc8636b6aacbc803cddf1dc49c10 size: 1574
[root@ecs-linux ~]#
```

Step 5 View the image in the registry.

```
curl 127.0.0.1:1000/v2/_catalog
```

```
[root@ecs-linux ~]# curl 127.0.0.1:1000/v2/_catalog
{"repositories":["michael/httpd"]}
```



Step 6 Delete the `httpd:v11` image from the host.

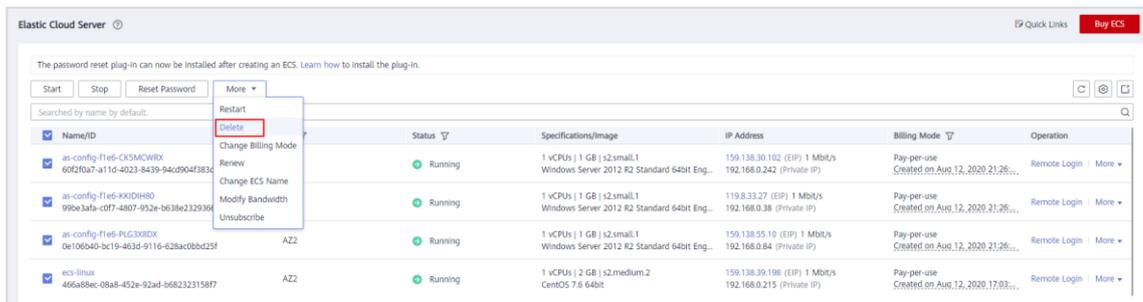
`docker rmi httpd:v11`

```
[root@ecs-linux sha256]# docker rmi httpd:v11
Untagged: httpd:v11
```

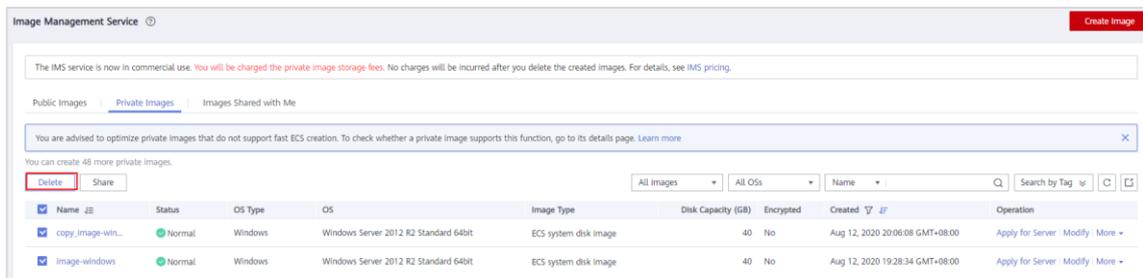
----End

1.3 Deleting Resources

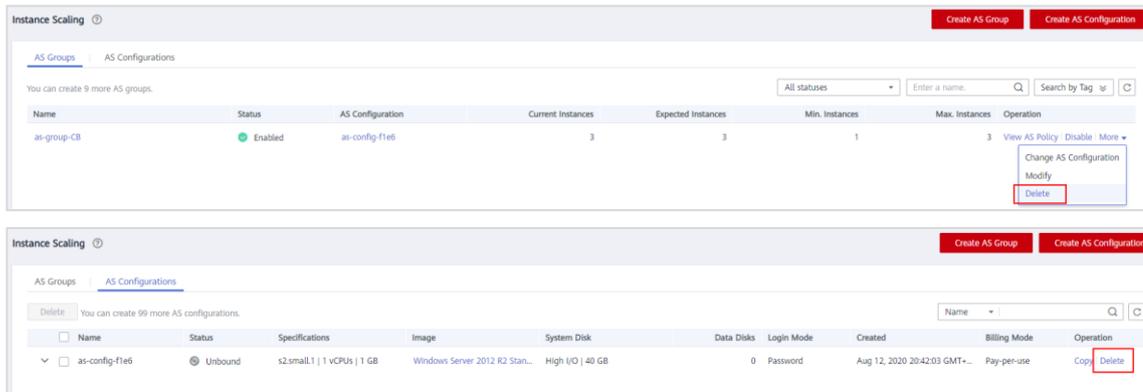
Step 1 Delete the ECSs.



Step 2 Delete the private images.



Step 3 Delete the AS group and configuration.





Step 4 Delete the subnet and then delete the VPC.

----End



2 Storage Services

2.1 EVS

2.1.1 Introduction

EVS provides persistent block storage for computing services such as ECS and BMS. EVS offers high availability and durability with extremely little latency thanks to advanced data redundancy and cache acceleration capabilities. You can format your EVS disks, create file systems on them, attach them to ECSs, and use them for persistent data storage. This section describes how to purchase an EVS disk and then attach the disk to an ECS.

2.1.2 Objectives

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

- Purchase an EVS disk.
- Attach an EVS disk to an ECS.
- Initialize the EVS disk (on a Windows or Linux server).
- Use snapshots.

2.1.3 Tasks

You can expand the capacity of an EVS disk to meet the requirements of the service system or production environment. You can attach an EVS disk to an ECS or detach it when it is no longer needed. This example describes how to attach an EVS disk to a Windows or Linux server.

- A system disk is automatically created and attached when an ECS is purchased. System disks cannot be purchased separately.
- If you purchase a data disk when creating an ECS, the system automatically attaches the data disk to the ECS. You can also purchase a data disk separately and attach it to the ECS later.

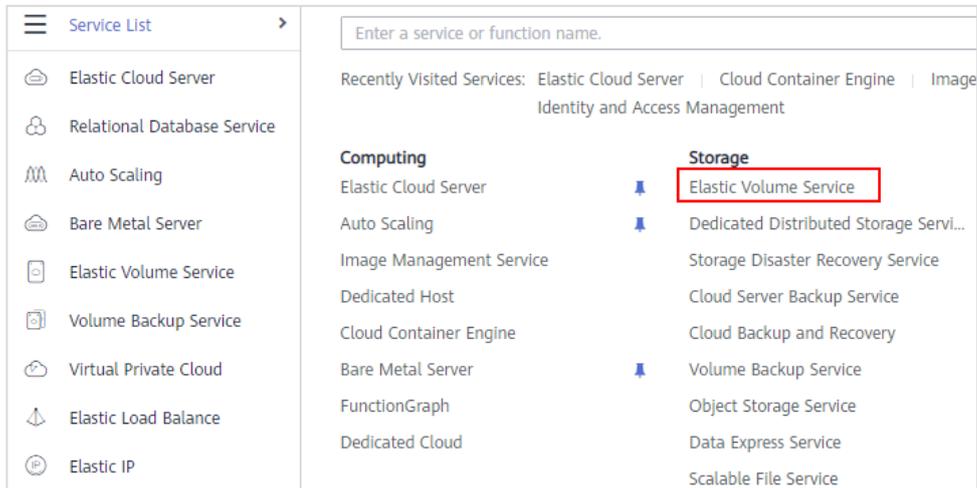
2.1.4 Attaching an EVS Disk to a Windows ECS

2.1.4.1 Purchasing an EVS Disk

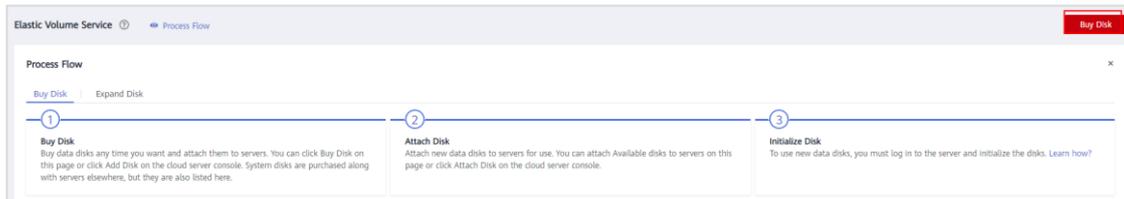
In this section, an ECS running Windows Server 2012 R2 Standard 64bit English (40GB) purchased in the AP-Hong Kong region will be used as an example to illustrate the process.



- Step 1 In the AP-Hong Kong region, buy an ECS running Windows Server 2012 R2 Standard 64bit English (40GB) by referring to instructions in section 1.1.4.1. You can also use an existing ECS running Windows Server 2012.
- Step 2 Log in to the management console and choose **Service List > Storage > Elastic Volume Service**.



- Step 3 Click **Buy Disk**.



- Step 4 Configure the basic information about the EVS disk.

- **Billing Mode: Pay-per-use**
- **Region: AP-Hong Kong**
- **AZ:** Select the AZ where the ECS is located.
- **Disk Specifications:** Select **Common I/O**. If **Common I/O** is unavailable, select an available one.
- **Capacity: 20 GB**
- **Auto Backup:** Deselect it.
- **More:** Skip this parameter.
- **Disk Name: volume-winadded** (user-defined)



Buy Disk

Billing Mode: Yearly/Monthly Pay-per-use
Disks are billed based on capacity and duration of use, and fees are paid after use. Select this option if your requirements may change over time.

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

AZ: AZ1 (3) AZ2
There are 3 servers in the current AZ.
Disks can only be attached to servers in the same AZ. Once a disk has been created, you cannot change the AZ of the disk.

Disk Specifications: GB
IOPS limit: 1,320, IOPS burst limit: 5,000

Auto Backup: Enable **Recommended**
It is recommended that you back up EVS data. The cost of backups will be included in the final bill. 1 GB of backed up data will cost \$0.046 USD per month.

More: Share | SCSI | Encryption | Tag

Disk Name:
If you buy multiple disks at a time, the value you entered will be used as the prefix of disk names, and one disk name will be composed of this value and a four-digit number. For example, if you enter my_disk and set the quantity to 2, the disk names will be my_disk-0001 and my_disk-0002.

Quantity: You can create 395 more disks. You can create a maximum of 100 disks at a time. [Increase Quota.](#)

Step 5 Click **Next**.

Step 6 On the **Details** page, confirm the disk configuration and click **Submit** to start the creation. If you need to modify the configuration, click **Previous** to modify parameters.

Buy Disk

Details

Resource	Configuration	Billing Mode	Quantity	Subtotal
	Region	Hong-Kong		
	AZ	AZ1		
	Data Source	Not required		
	Capacity (GB)	20		
Disk	Disk Type	High I/O	1	\$0.004 USD/hour
	Disk Encryption	No		
	Device Type	VBD		
	Disk Sharing	Disabled		
	Disk Name	volume-winadded		

Step 7 Return to the disk list and take note of the disk status on the **Elastic Volume Service** page. When the disk status changes to **Available**, the disk creation is complete.



The screenshot shows the Elastic Volume Service console. At the top, there is a 'Process Flow' section with three steps: 1. Buy Disk, 2. Attach Disk, and 3. Initialize Disk. Below this, there is a table of disks. The table has columns for Disk Name, Status, Disk Specification, Function, Server Name, Disk Sharing, Device Type, Encrypted, and AZ. Two disks are listed: 'volume-winaddfd' with status 'Available' and function 'Data disk', and 'ecs-windows2012' with status 'In-use' and function 'System disk'. The 'Data disk' and 'Available' status are highlighted with red boxes.

Disk Name	Status	Disk Specification	Function	Server Name	Disk Sharing	Device Type	Encrypted	AZ
volume-winaddfd	Available	High I/O 20 GB	Data disk	--	Disabled	VBD	No	AZ1
ecs-windows2012	In-use	High I/O 40 GB	System disk	ecs-windows2012 ECS	Disabled	VBD	No	AZ1

----End

2.1.4.2 Attaching an EVS Disk to an ECS

EVS disks purchased separately are automatically data disks. In the disk list, the function of such disks is displayed as **Data disk**, and the status is displayed as **Available**. Now you need to attach the data disk to an ECS.

A system disk is purchased and attached to an ECS automatically when you purchase the ECS. In the disk list, the function of such a disk is displayed as **System disk**, and the status is displayed as **In-use**. If a system disk is detached from an ECS, the disk function changes to **Bootable disk**, and the status changes to **Available**. A non-shared EVS disk is like an SSD or SATA disk purchased for a regular PC. After being attached to an ECS, it functions as regular hard drive, like a D or E drive on a PC.)

Step 1 Locate the disk in the list and click **Attach**. The **Attach Disk** dialog box is displayed.

The screenshot shows the Elastic Volume Service console, similar to the previous one. The table of disks is visible. The 'Data disk' and 'Available' status are highlighted with red boxes. The 'Attach' button in the 'Operation' column for the 'volume-winaddfd' disk is also highlighted with a red box.

Disk Name	Status	Disk Specification	Function	Server Name	Disk Sharing	Device Type	Encrypted	AZ	Billing Mode	Operation
volume-winaddfd	Available	High I/O 20 GB	Data disk	--	Disabled	VBD	No	AZ1	Pay-per-use Created on Aug. 13, 2016	Attach Expand

Step 2 Select the target Windows ECS and select a mount point from the drop-down list. Ensure that the EVS disk and ECS are in the same AZ.



Attach Disk

Disk: volume-winadded | Hong-Kong | AZ1 | VBD | Non-shareable

ECSs | BMSs

Name

Name	Mount Point	Status	Image	Private IP ...	EIP
ecs-windows2012	Data disk	Running	Windows ...	192.168.0.161	119.8.33.27

Step 3 Return to the disk list page. The status of the disk is **Attaching**, indicating that the disk is being attached to the ECS. When the disk status changes to **In-use**, the disk has been attached to the ECS, but will still need to be initialized before it can be used.

You can create 394 more disks. The disks can use up to 32,428 GB of storage space. To renew multiple disks at a time, switch to the Renewals page.

Delete

Disk Name	Status	Disk Specificat...	Function
volume-winadded	In-use	High I/O 20 GB	Data disk

The attaching process is NOT completed yet. You must initialize the disk before using it.

A new disk or the additional capacity of an expanded disk must be initialized after the disk has been attached. An initialized disk does not need to be reinitialized. [Learn how to initialize disks](#)

OK

Step 4 Switch to the ECS list, select the Windows ECS that the EVS disk was attached to, and click **Remote Login**.

Elastic Cloud Server

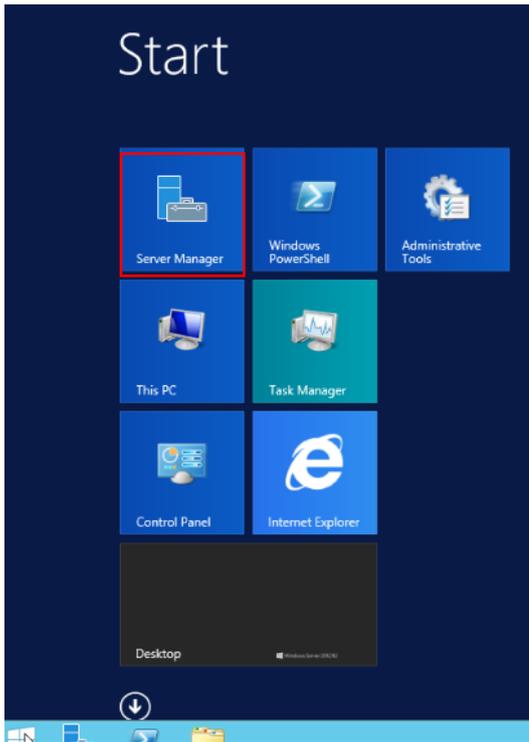
The password reset plug-in can now be installed after creating an ECS. [Learn how to install the plug-in.](#)

Start Stop Reset Password More

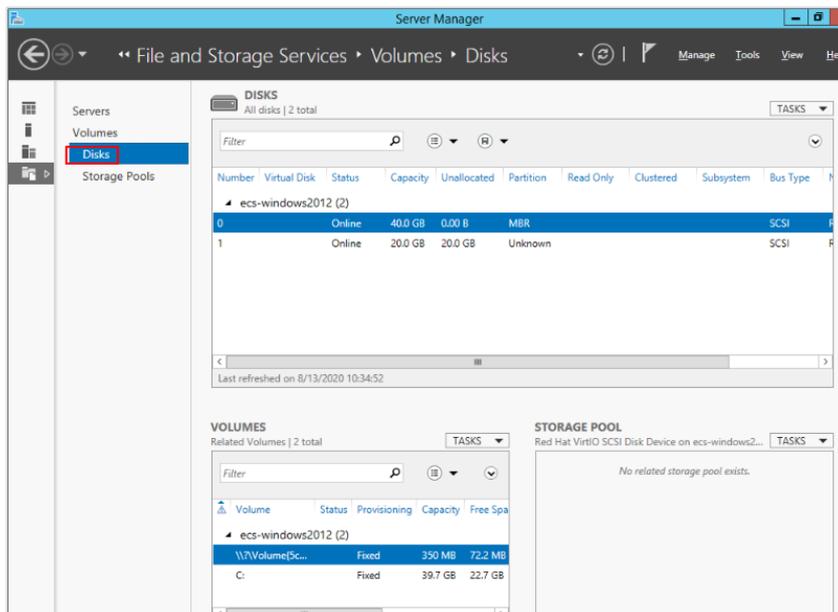
Searched by name by default.

Name/ID	AZ	Status	Specifications/Image	IP Address	Billing Mode	Operation
ecs-windows2012 f21b21ed-3886-4a74-8841-902d25763773	AZ1	Running	1 vCPUs 1 GB s2.small.1 Windows Server 2012 R2 Standard 64bit English	119.8.33.27 (EIP) 1 Mbit/s 192.168.0.161 (Private IP)	Pay-per-use Created on: Aug.13, 2020, 10:02:14	Remote Login

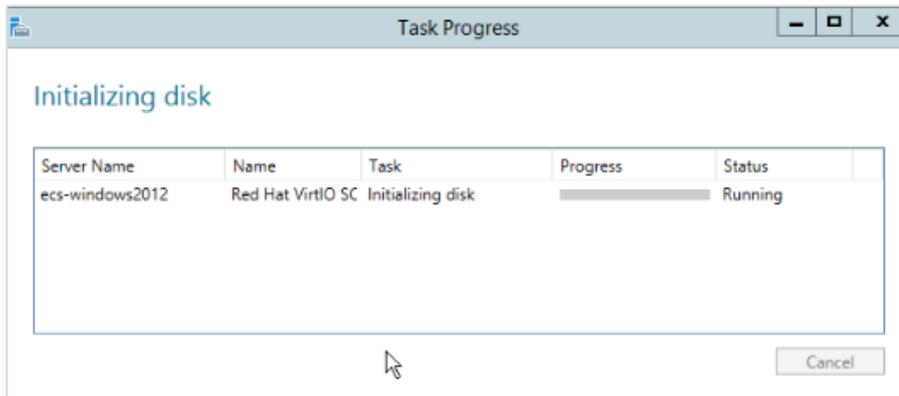
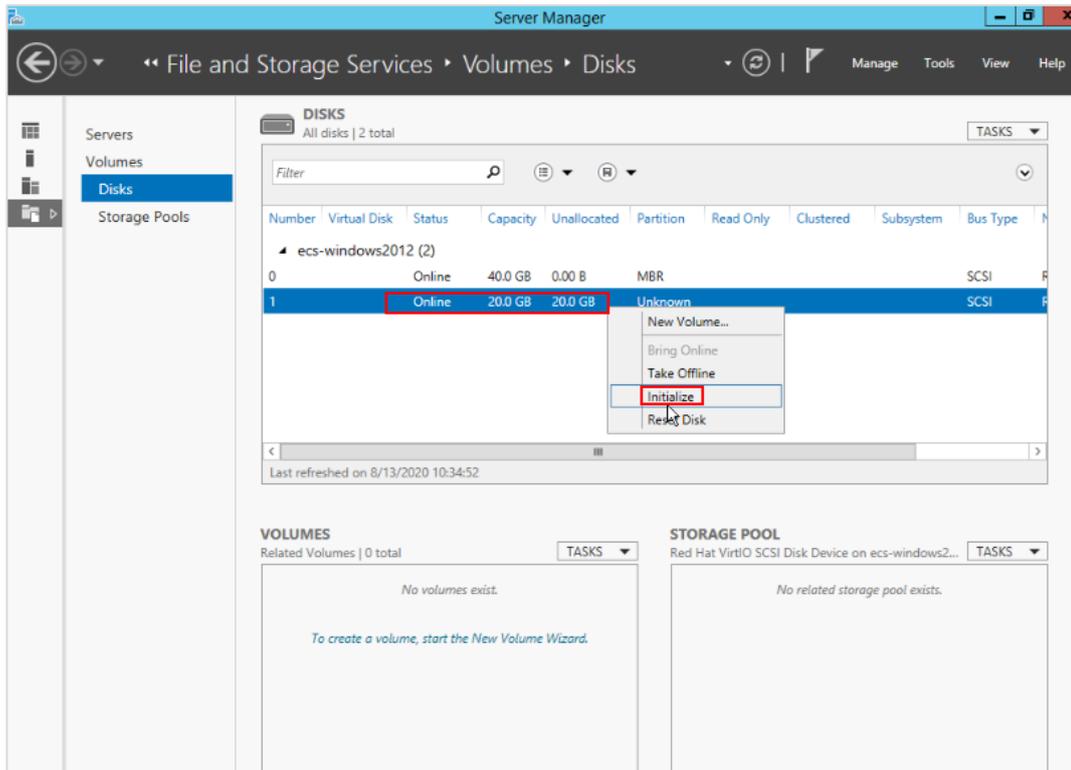
Step 5 On the ECS desktop, choose **Start > Server Manager**.



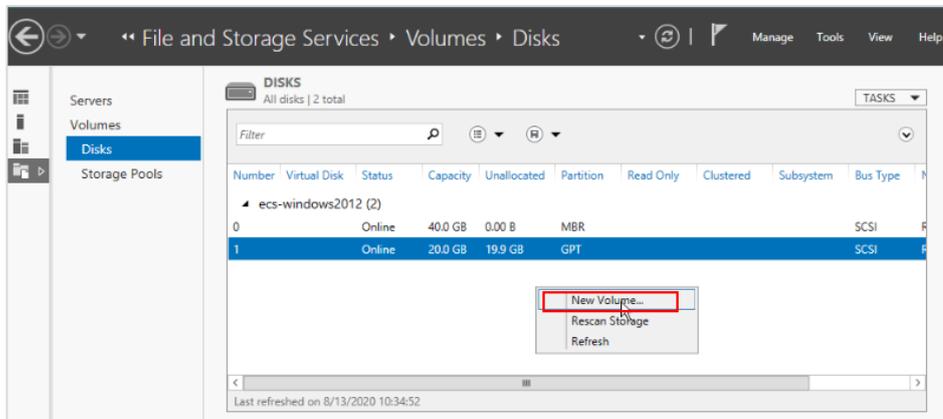
Step 6 In the left navigation pane, choose **File and Storage Services > Disks**.



Step 7 If the newly attached disk is in the **Offline** state, right-click in the disk and choose **Bring Online** from the shortcut menu. If the newly attached disk has not been initialized, right-click the disk and choose **Initialize** from the displayed menu.

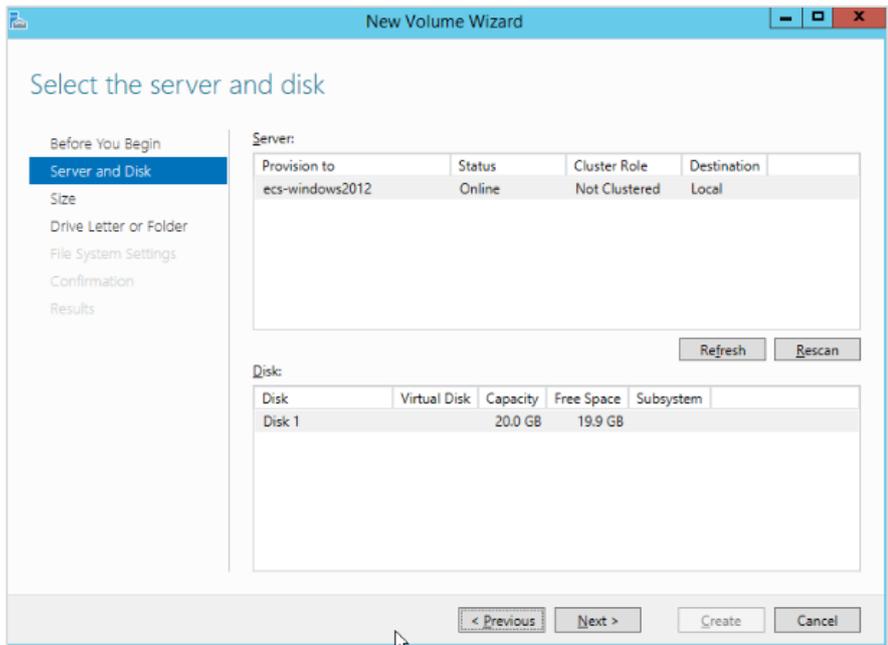
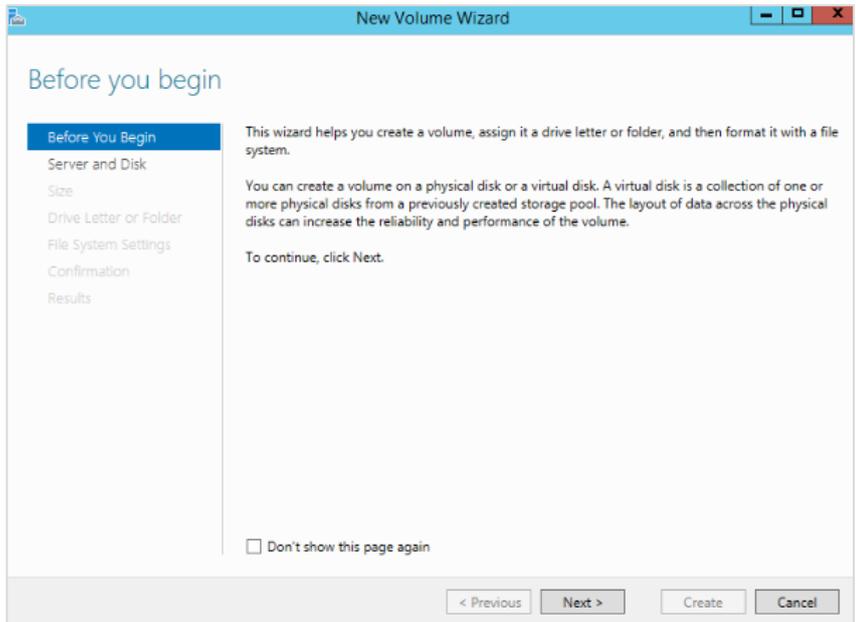


Step 8 Right-click at the unallocated partition and choose **New Volume** from the shortcut menu.

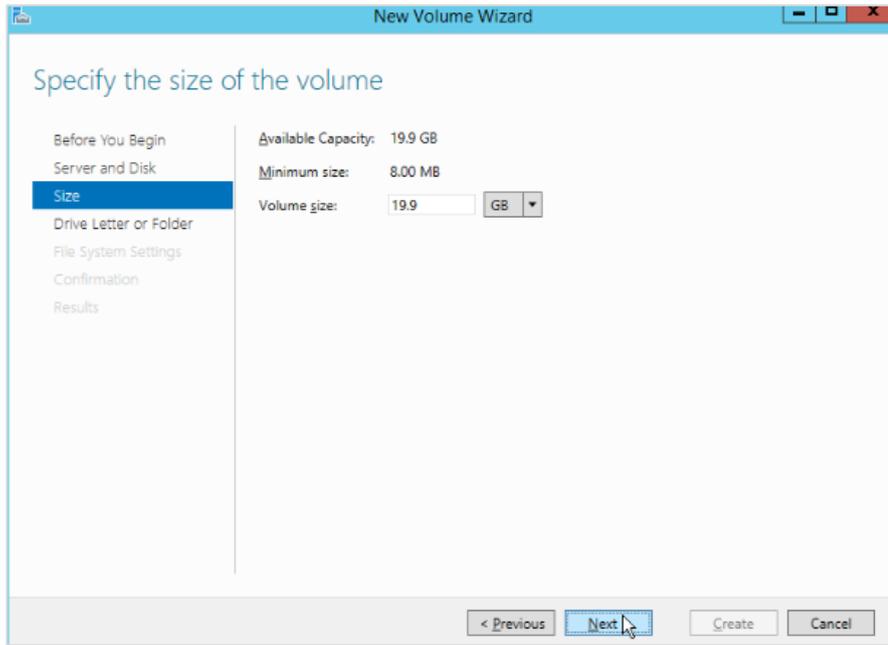




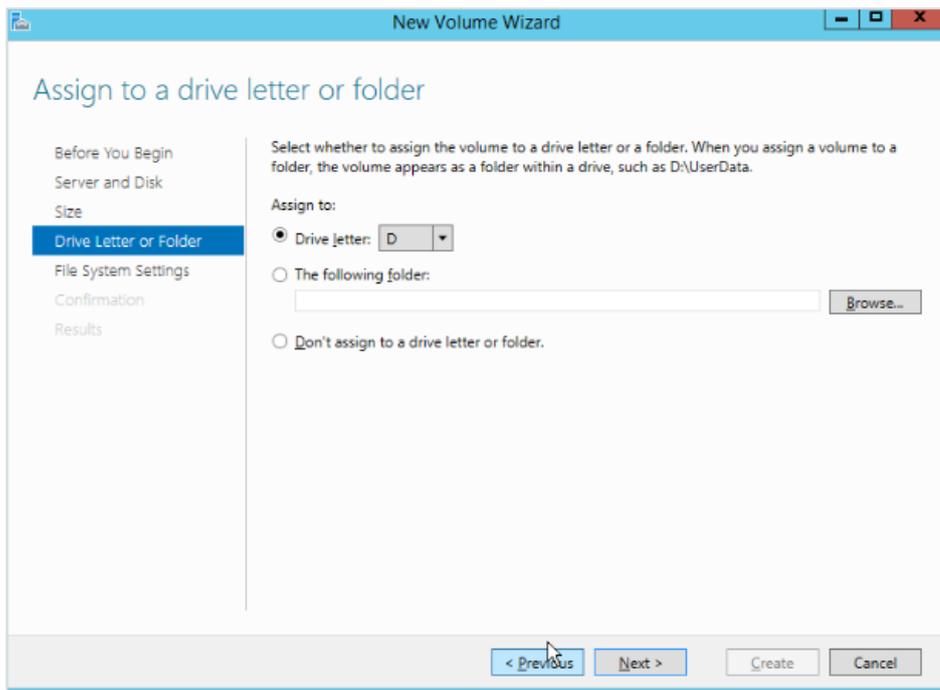
Step 9 On the displayed **New Volume Wizard**, click **Next**.



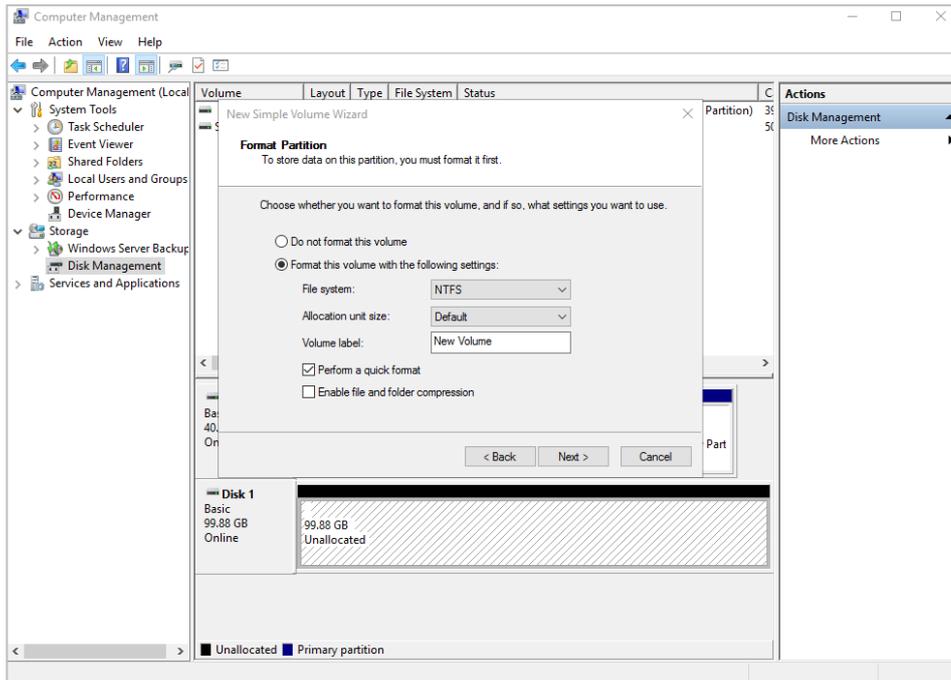
Step 10 Specify the volume size and click **Next**. The default value is the maximum size.



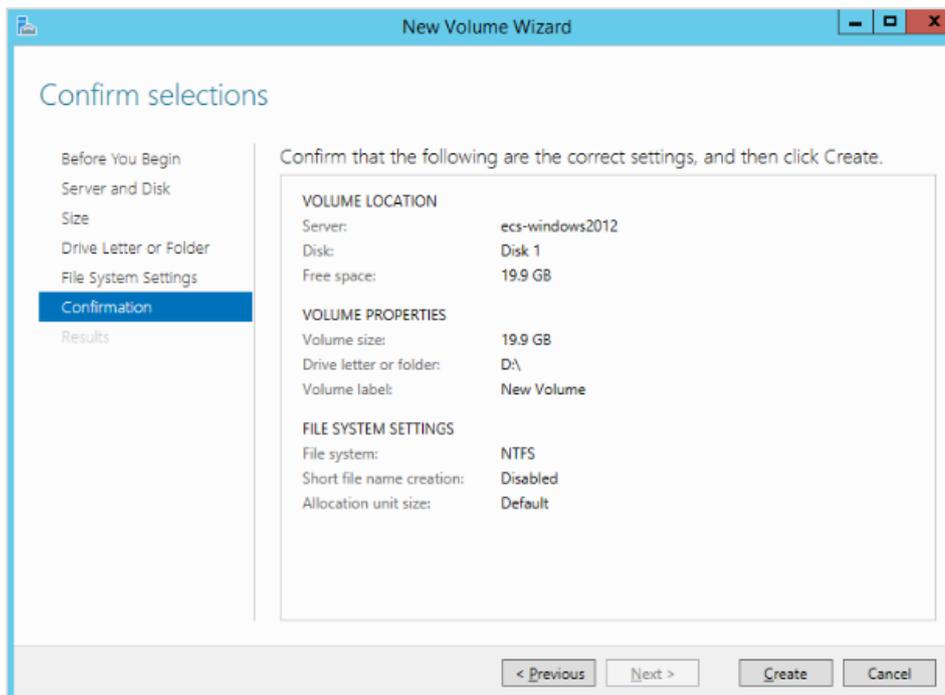
Step 11 Assign a drive letter and click **Next**.



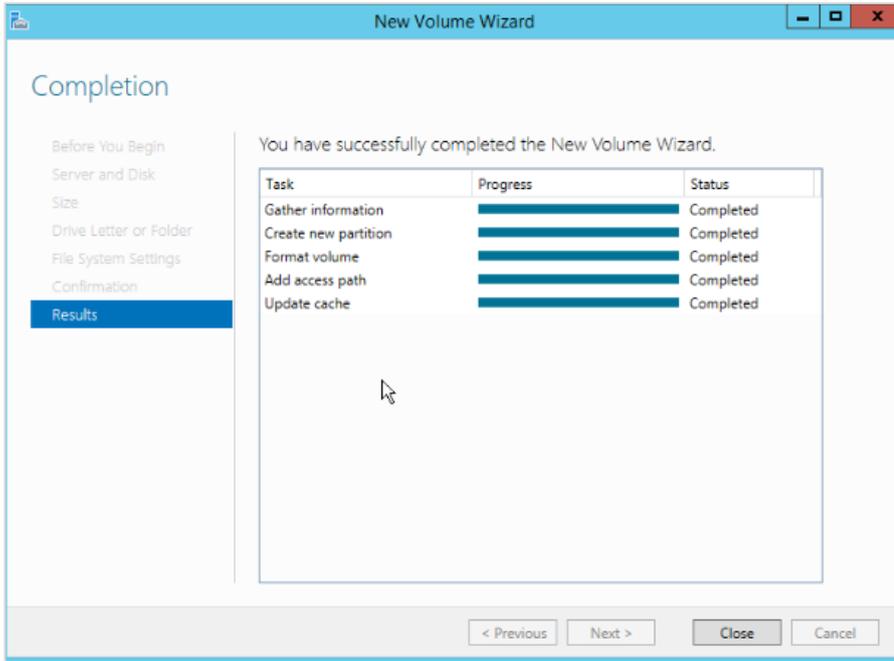
Step 12 Select **Format this volume with the following settings**, set parameters based on actual requirements, and select **Perform a quick format**. Then click **Next**.



Step 13 Confirm the settings and click **Create**.

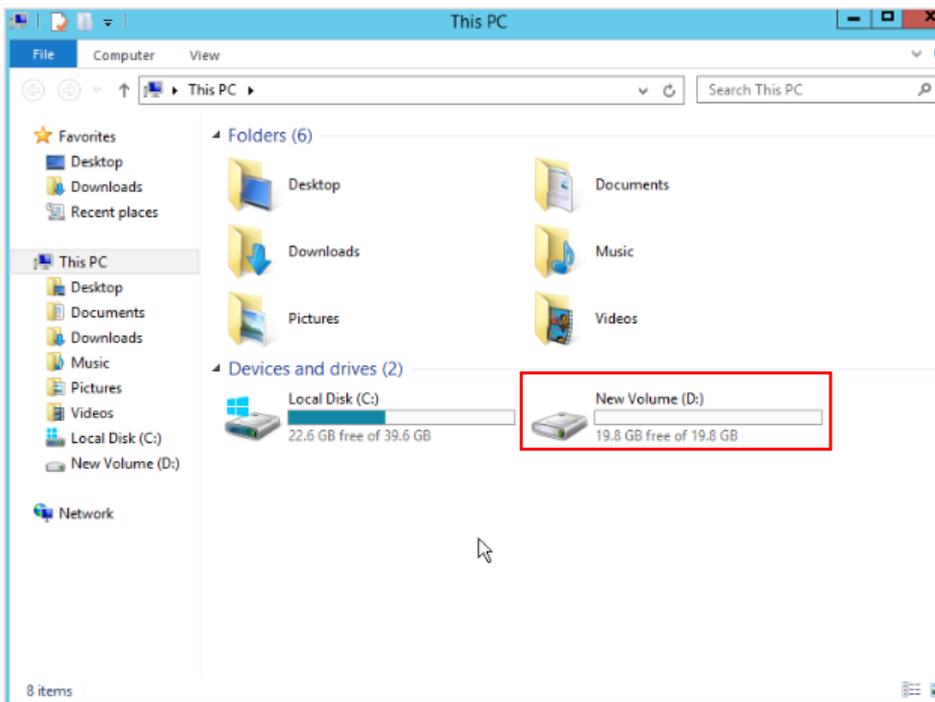


Step 14 After the creation is complete, click **Close**.



Step 15 Switch to **This PC**.

If a new drive is displayed, the disk has been successfully attached to the ECS.

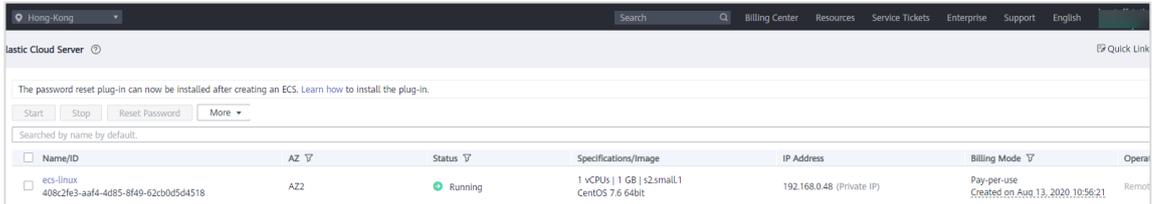


----End

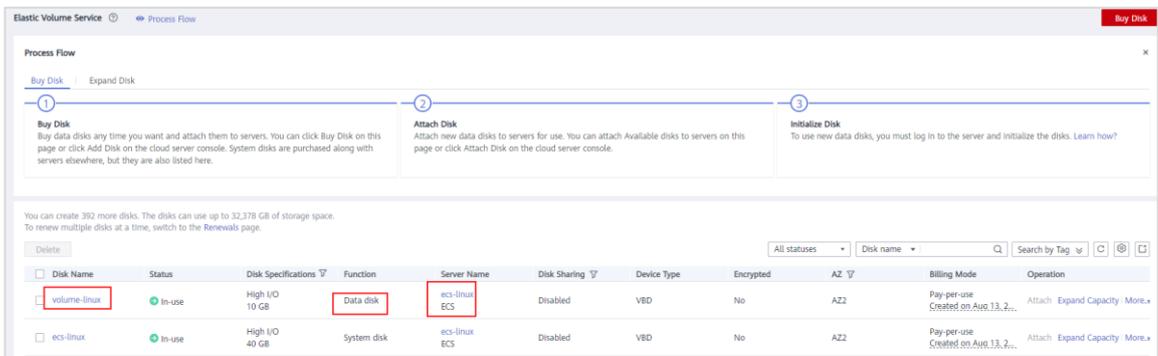


2.1.5 Attaching an EVS Disk to a Linux ECS

Step 1 Buy a Linux ECS by referring to instructions in section 1.1.4.1. In this example, an ECS running CentOS 7.6 64-bit is used, but the tool used, `fdisk`, should be the same regardless of which Linux distribution you select.



Step 2 Purchase a non-shared EVS disk and attach it to an ECS by referring to instructions in section 2.1.4. Ensure that the data disk is in the same AZ as the Linux ECS.



Step 3 Remotely log in to the Linux ECS and run the following command to view the newly added 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
```



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

- Step 4 Use **fdisk**, the disk partitioning tool, to partition the new data disk. In the example here, we are partitioning disk **/dev/vdb**, so the command is as follows:

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): █
```

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
Command (m for help): █
```

- Step 5 In this example, a primary partition is created. Therefore, enter **p** and press **Enter** to create a primary partition. Primary partition number 1 is used in this example. Enter **1** and press **Enter**.

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

First sector indicates the start cylinder number. The value range is **2048** to **20971519**, and the default value is **2048**.

- Step 6 Select the default first cylinder number **2048** and press **Enter**.

```
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): █
```

Last sector indicates the last cylinder number. The value range is **2048** to **20971519**, and the default value is **20971519**.



Step 7 Select the default last cylinder number **20971519** and press **Enter**.

```
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):
```

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

Step 8 Enter **p** and press **Enter** to view the details of 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):
```

Details about the **dev/vdb1** partition are displayed.

Step 9 Enter **w** and press **Enter** to write the changes to the partition table.

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

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

Note that if you want to exit fdisk without keeping the changes made before, input **q**.

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

```
partprobe
```



- Step 11 Run the following command to create an ext4 file system format for the created 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
```

The formatting takes little time. Do not exit until the task status changes to **done**.

- Step 12 Run the following command to create a mount point `/mnt/sdc`:

```
mkdir /mnt/sdc
```

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

- Step 13 Run the following command to mount the new partition to the mount point created in the previous step:

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

```
[root@ecs-linux ~]# mkdir /mnt/sdc
[root@ecs-linux ~]# mount /dev/vdb1 /mnt/sdc
[root@ecs-linux ~]#
```

- Step 14 Run the following command to view the results:

```
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
```

The new partition `/dev/xvdb1` is mounted to `/mnt/sdc`.

----End

2.2 OBS

2.2.1 Introduction

OBS is a stable, secure, efficient, and easy-to-use cloud storage service. It supports standard REST APIs, and can store unstructured data of any amount and types. This section describes how to use OBS Browser+ to manage object storage.

2.2.2 Objectives

Upon the completion of this section, 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.

2.2.3 Tasks

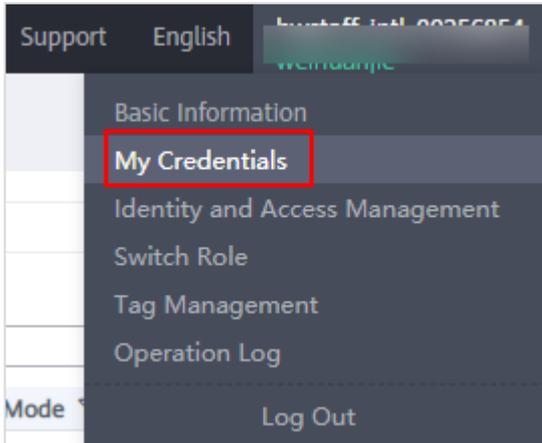
When you log in to the OBS console using your HUAWEI CLOUD account or as an IAM user, OBS authenticates your account or IAM user credentials.

When you access OBS using the tools (OBS Browser+ or obsutil), SDKs, or APIs, instead of your HUAWEI CLOUD account or IAM user account, OBS requires the access keys (AK and SK) for authentication. Therefore, you need to obtain the access keys (AK and SK) before you access OBS using any methods other than OBS Console.

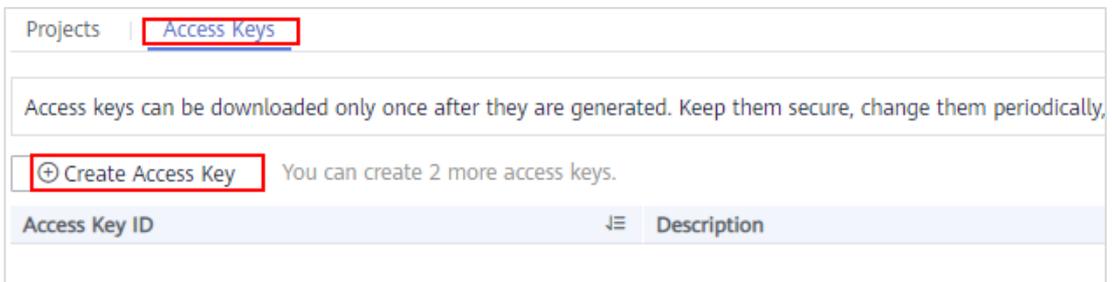
2.2.4 Preparations

2.2.4.1 Obtaining AK and SK

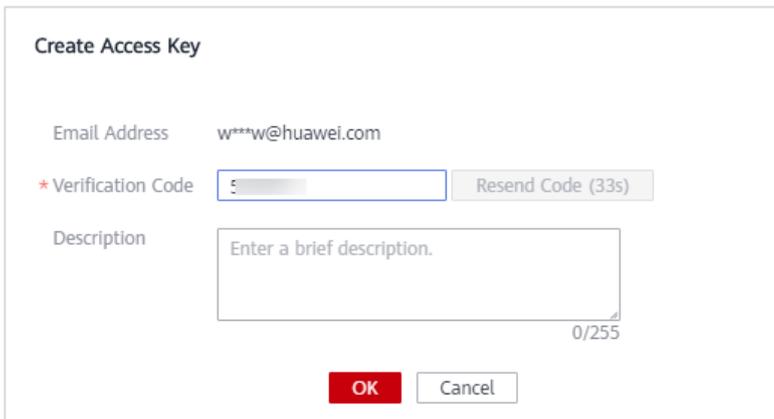
- Step 1 In the upper right corner of the console homepage, select **My Credentials** under the username.



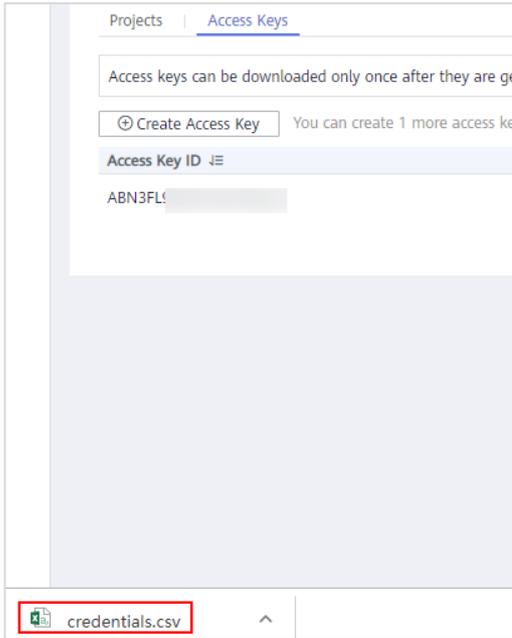
Step 2 Select **Access Keys** and then click **Create Access Key**.



Step 3 In the **Create Access Key** dialog box, enter the email or SMS verification code. Click **OK** to automatically download the file.



Step 4 Save the key file when prompted.



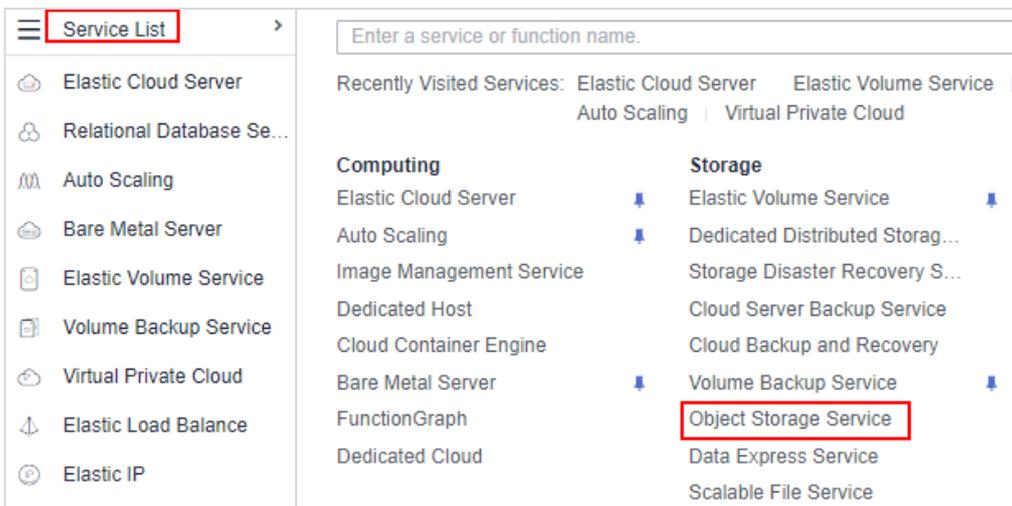
Keep the access keys properly.

Step 5 Open the downloaded file, **credentials.csv**, to obtain the AK and SK pair.

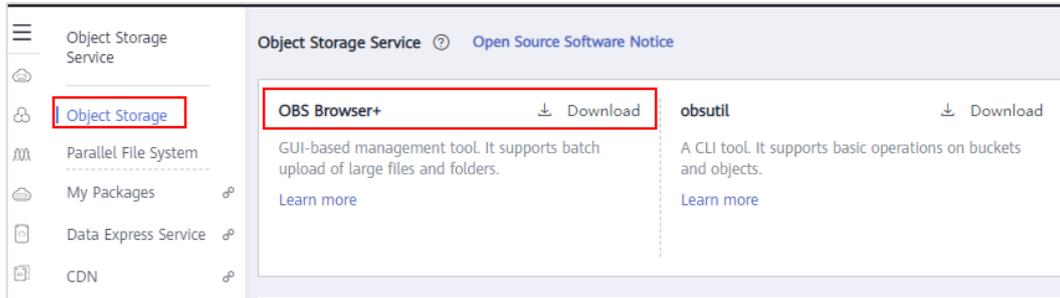
----End

2.2.4.2 Downloading and Initializing OBS Browser+

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



Step 2 On the OBS console, download the OBS Browser+ software package based on the operating system of your local PC.



 **OBS Browser+ Tool**

OBS Browser+ is a GUI-based desktop application for comprehensively managing OBS buckets and objects. OBS Browser+ is intuitive and easy to use. It allows you to easily manage OBS resources from your local end.

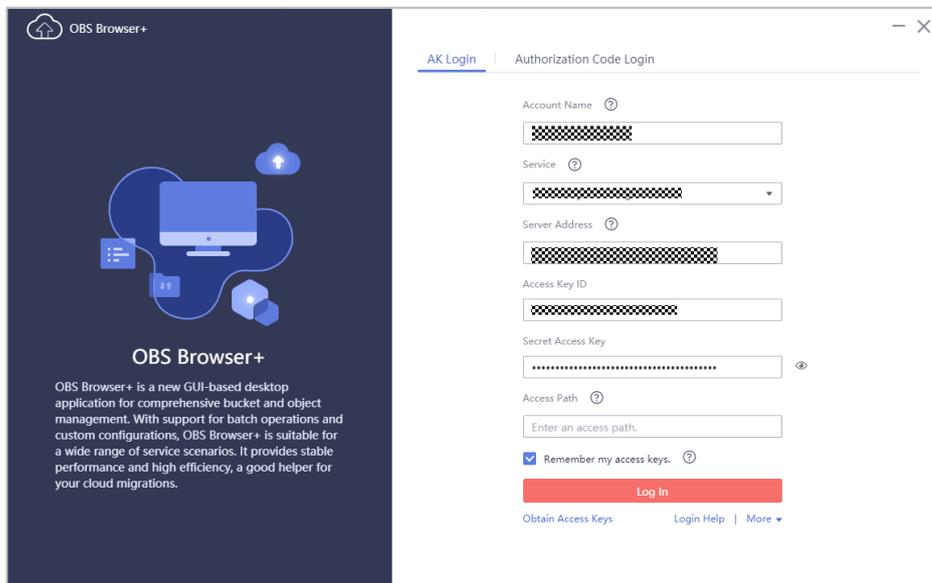
[Doc](#) [Windows \(32-bit\)](#) [Windows \(64-bit\)](#)

Step 3 Decompress the downloaded software package and install it.

----End

2.2.4.3 Logging In to OBS Browser+

Enter the account information and log in to OBS Browser+ using the AK.



OBS Browser+ can save the login details for up to 100 accounts. If a proxy is required to access your network environment, configure the network proxy before login.



2.2.5 Using OBS Browser+

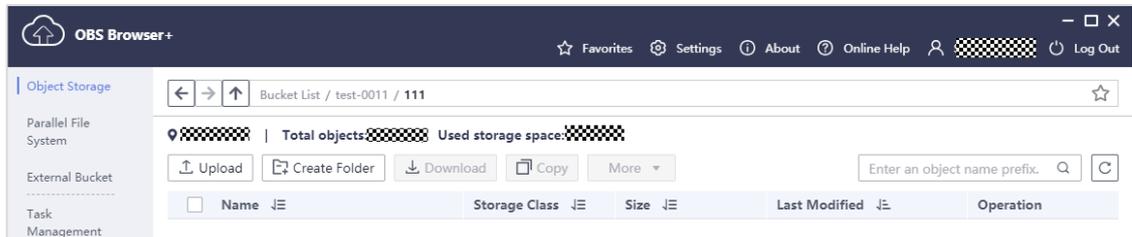
Step 1 Create a bucket.

The bucket name must be globally unique.

Step 2 Create a folder in the bucket.

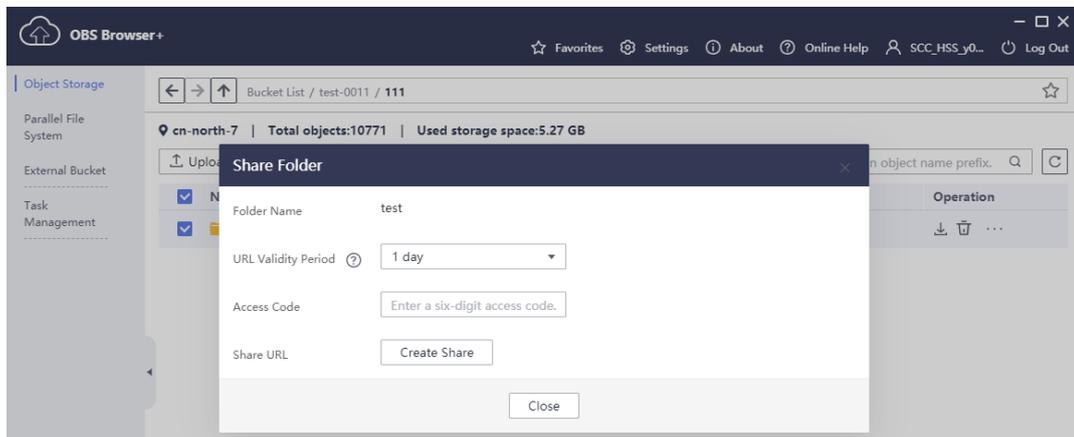
Step 3 Drag a file from a local path and drop it to the created folder.

OBS Browser+ supports drag-and-drop upload. Drag one or more files or folders into the object list of a bucket or a parallel file system on OBS Browser+. You can even drag a file or folder directly to a specified folder on OBS Browser+. This drag-and-drop functionality makes it easy to upload files to OBS. For details, see [OBS Best Practices](#).



Step 4 Share a folder with another account.

OBS Browser+ provides folder sharing and authorization code login functions, allowing you to easily share a folder with other accounts for a specific length of time. To share a folder, log in to OBS Browser+, right-click the folder you want to share and choose **Share**, or click **More > Share** in the operation column.

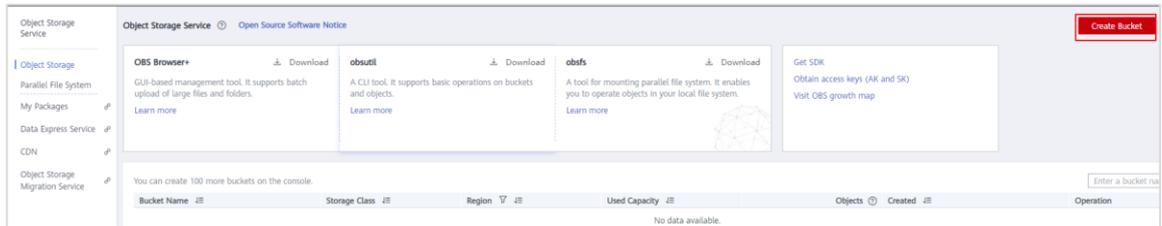


----End



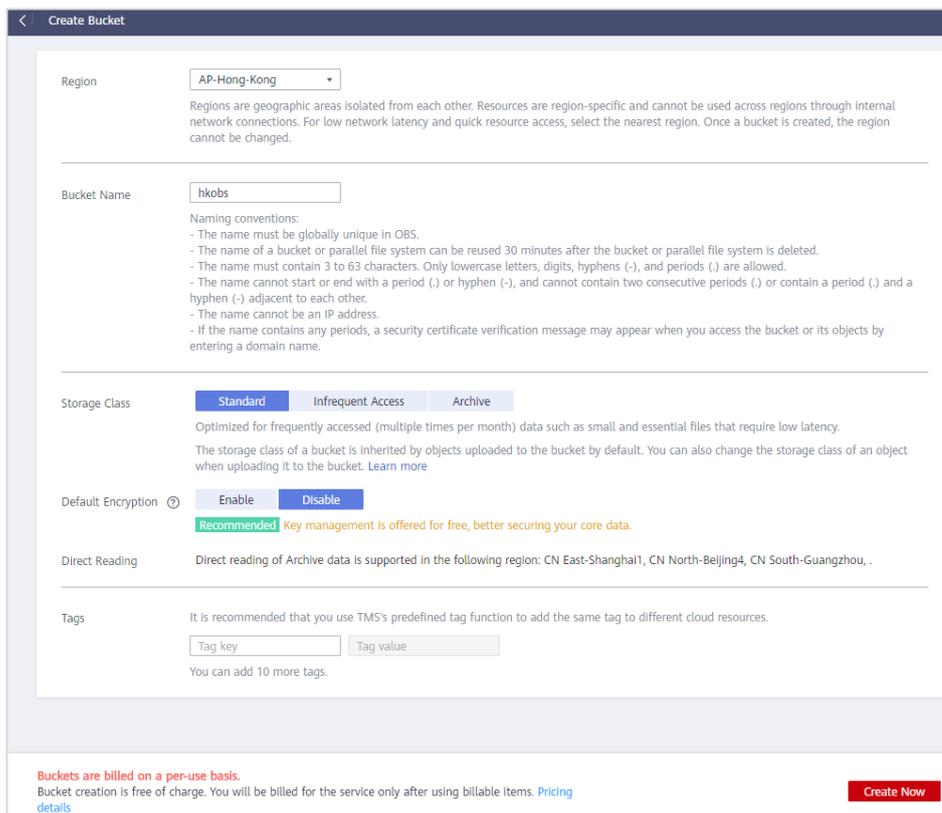
2.2.6 Versioning

Step 1 Log in to the OBS console and click **Create Bucket**.



Step 2 Set the bucket information as follows:

- **Region: AP-Hong Kong**
- **Bucket Name:** Enter a name that is globally unique.
- **Storage Class: Standard**
- **Default Encryption: Disable**



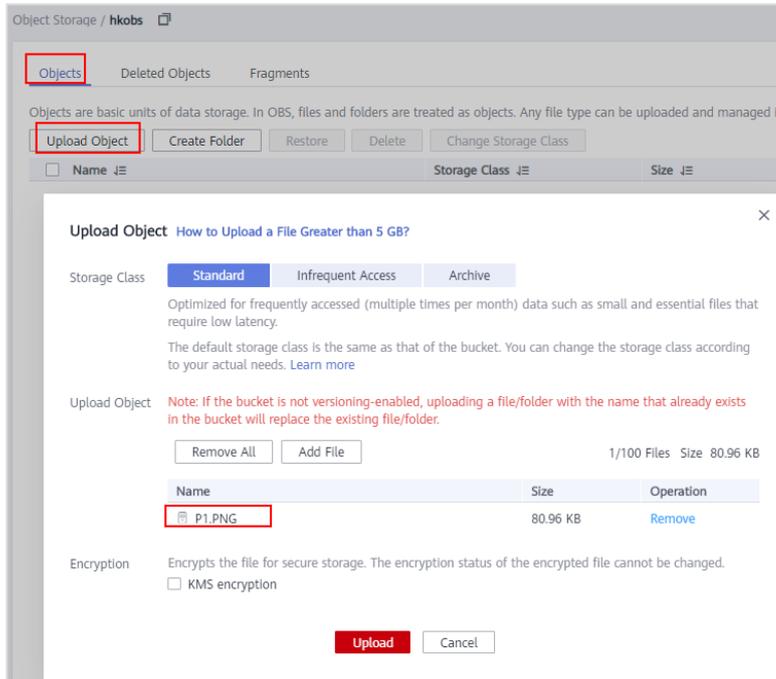
Step 3 Switch back to the bucket list and view the newly created bucket.

You can create 99 more buckets on the console.

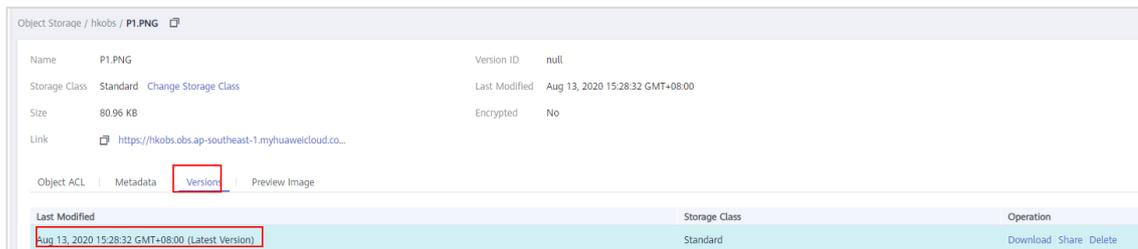
Bucket Name	Storage Class	Region	Used Capacity
hkobs	Standard	AP-Hong-Kong	0 byte



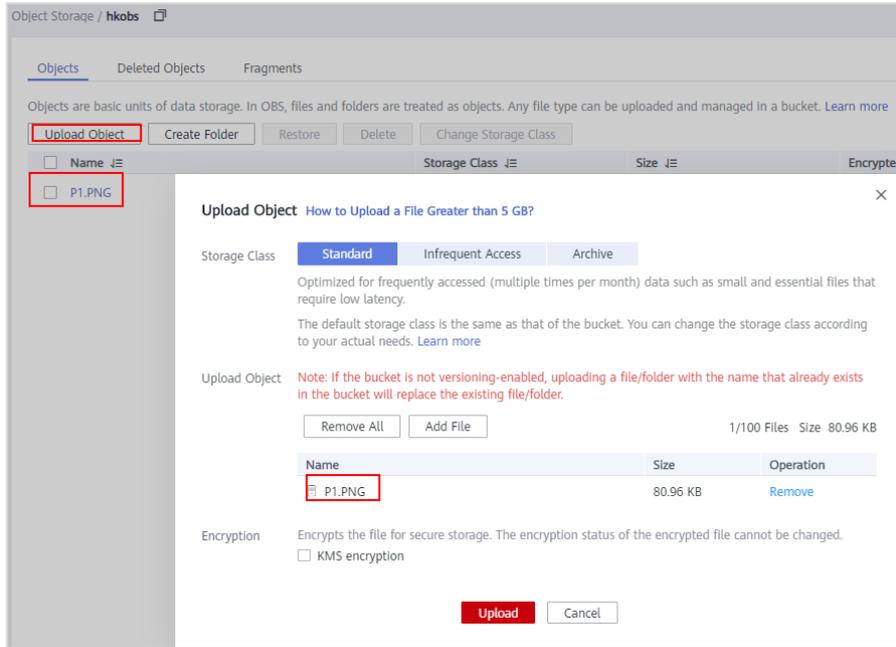
Step 4 Click the bucket name. On the **Objects** tab page, click **Upload Object** upload a file from a local path.



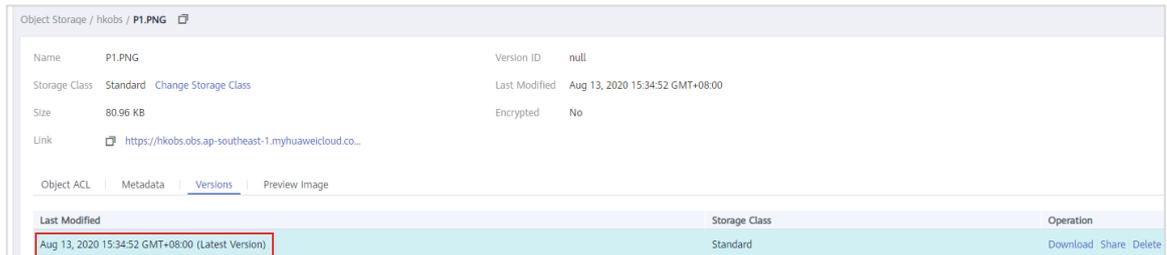
Step 5 Click the file name to go to the details page, where you can see any versions that exist.



Step 6 Return to the bucket list and upload a file with the same name to the bucket.



Step 7 Confirm that only one file is displayed in the object list of the bucket.
On the details page of the file, only the latest object version is displayed.



Step 8 On the **Overview** page of the bucket, click **Edit** next to **Versioning** in the **Basic Information** area to enable versioning.



The screenshot shows the 'Object Storage / hkobs' overview page. The left sidebar has 'Overview' highlighted. The main content area is divided into 'Basic Statistics' and 'Basic Information'. In the 'Basic Information' section, 'Versioning' is currently 'Disabled' with an 'Edit' button next to it. A 'Versioning' dialog box is open, showing two options: 'Enable' (selected) and 'Suspend'. The 'Enable' option includes the text: 'Multiple versions of objects can be stored in the same bucket. Each object version stored will incur a fee.' At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Basic Statistics	
Storage	Objects
Used Capacity: 80.96 KB	1
This month GET: 48	

Basic Information	
Bucket Name	hkobs
Storage Class	Standard
Bucket Version	3.0
Region	AP-Hong-Kong
Account ID	09859dfdc00107a0ff6c00aa79a1c20
Created	Aug 13, 2020 15:22:41 GMT+08:00
Versioning	Disabled Edit
Endpoint	obs.ap-southeast-1.myhuaweicloud.com
Access Domain Name	hkobs.obs.ap-southeast-1.myhuaweicloud.com

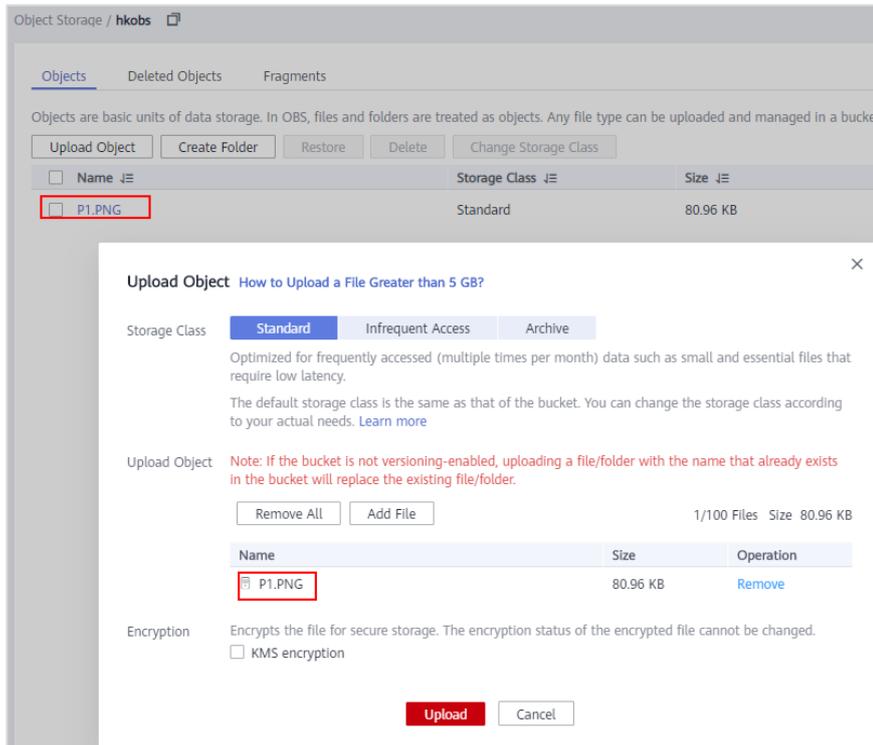
Versioning

Enable
Multiple versions of objects can be stored in the same bucket. Each object version stored will incur a fee.

Suspend

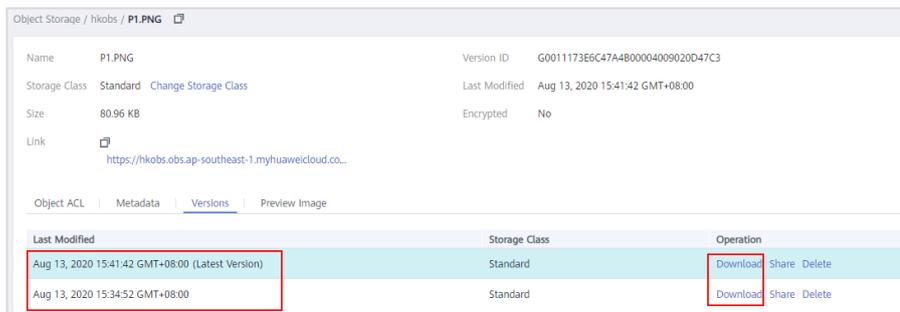
OK Cancel

Step 9 Upload two files with the same name.

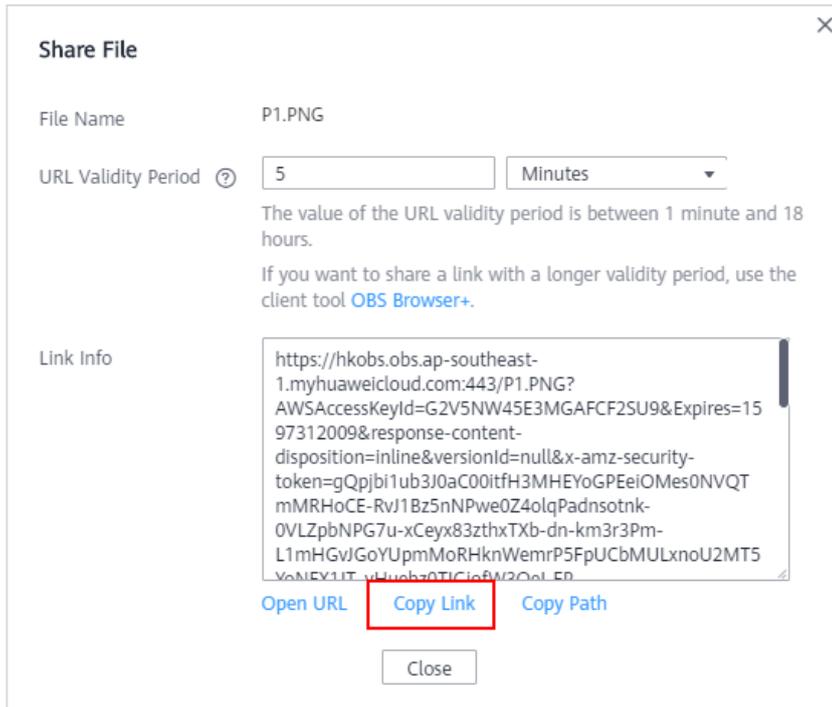


Step 10 Click the file name to go to its details page and view the file versions.

There are now two files, one for each of the two files you uploaded in the previous step. You can download, share, and delete different versions of that file.

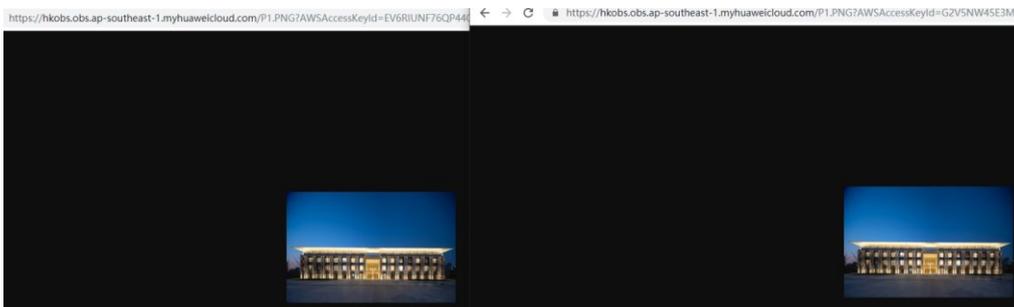


Step 11 Locate the target file, click **Share** in the operation column. In the displayed dialog box, enter the URL validity period and copy the URL to share the file.



Note that the maximum validity period is 18 hours.

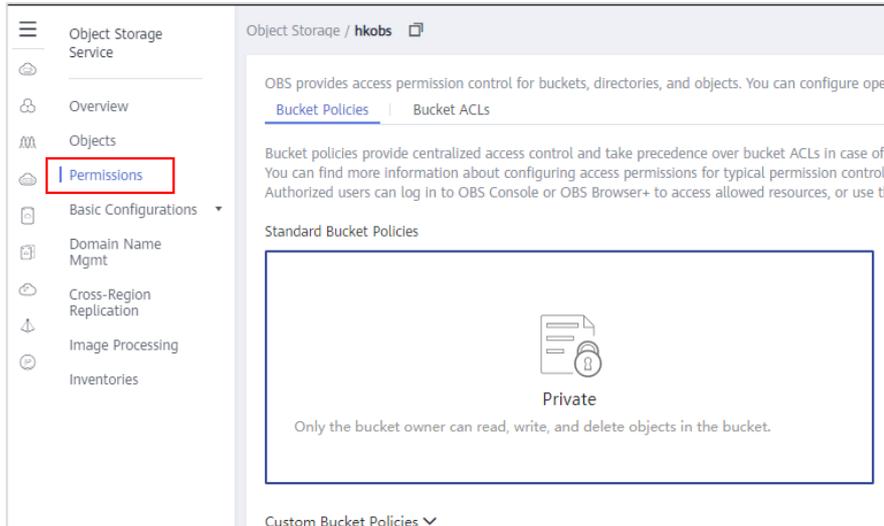
Two files with the same name (different versions) are displayed through the link.



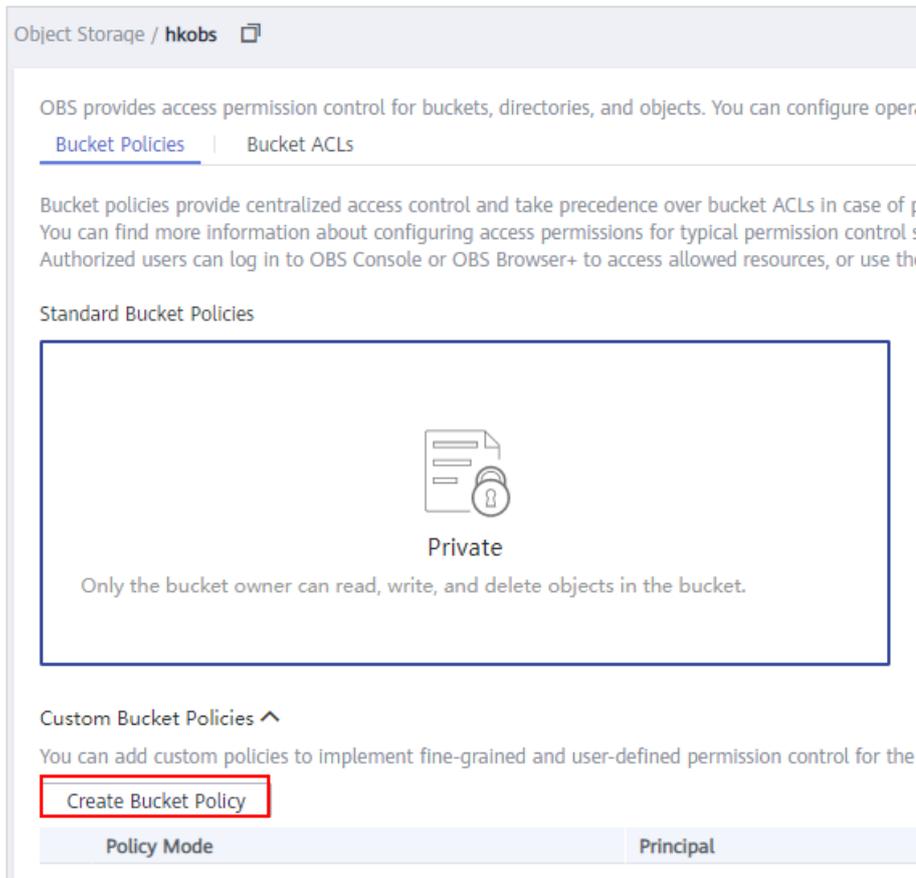
----End

2.2.7 OBS Permission Control Operations

Step 1 In the bucket list, click the destination bucket and click **Permissions**.



Step 2 Choose **Bucket Policies** > **Custom Bucket Policies**.



Step 3 Click **Create Bucket Policy**. The **Create Bucket Policy** dialog box is displayed. Configure the following parameters:

- **Bucket Name**



- **Policy Mode: Customized**
- **Effect: Allow**
- **Principal: Include**
- **Account ID: *** (indicating all anonymous users)
- **Resources: Include, Specific resources**
- **Actions: Include**
- **Conditions:**
 - **Conditional Operator: DateGreaterThan; Key: CurrentTime; Value: 2020-06-11T19:00:00Z**
 - **Conditional Operator: DateLessThan; Key: CurrentTime; Value: 2020-06-11T20:00:30Z**

If it is only for verification, you can shorten the interval as needed.

Create Bucket Policy [Learn how to configure.](#)

Bucket Name

Policy Mode
Provides users with customized operation permissions for the bucket and objects in the bucket.

Effect

Principal Include Exclude

Account ID

User ID

Resources Include Exclude

Resource Name

Actions Include Exclude

Action Name

Conditions	Conditional Operator	Key	Value	Operati...
	DateGreaterThan	CurrentTime	2020-08-	Delete
	DateLessThan	CurrentTime	2020-08-	Delete



Step 4 Verify the OBS permissions.

During the specified time period, any user can access the specified resources in the bucket. Outside the specified time period, only the bucket owner can access the bucket.

The following information will appear if users other than the bucket owner have accessed the bucket outside the specified time period.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Request has expired</Message>
  <RequestId>00000172A3713D6566D05DB94785FA89</RequestId>
  <HostId>
    5ft4U3+rIIca8PJY7u407TWZVgEyLP4vFCv4+JBenkAOpWKXDP06euLrFVNoLA50
  </HostId>
</Error>
```

----End

2.2.8 Deleting Resources

Delete all OBS resources on the console. You cannot delete a bucket with objects in it. You need to empty the bucket first.

2.3 SFS

2.3.1 Introduction

SFS is a network attached storage (NAS) service that provides scalable, high-performance file storage. With SFS, you can enjoy shared file access spanning ECSs, BMSs, and containers created on Cloud Container Engine (CCE) and Cloud Container Instance (CCI). This section describes basic operations of SFS.

2.3.2 Objectives

- Learn how to create a shared folder.
- Learn how to mount file systems to Linux ECSs and Windows ECSs.
- Learn how to share a file system across ECSs in different VPCs.

2.3.3 Creating a File System

Prerequisites

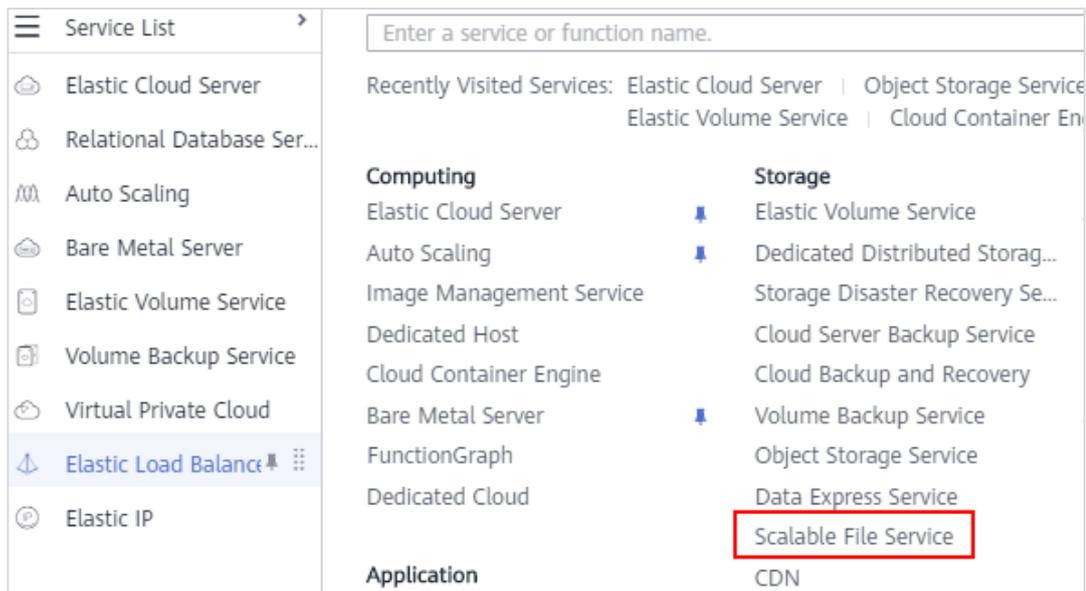
- Three VPCs have been created, one for a Linux ECS, one for a Windows ECS, and one for the file system that will be created.
 - VPCs: **vpc-test-linux**, **vpc-test-windows**, and a third VPC of your own choosing
 - Region: AP-Hong Kong



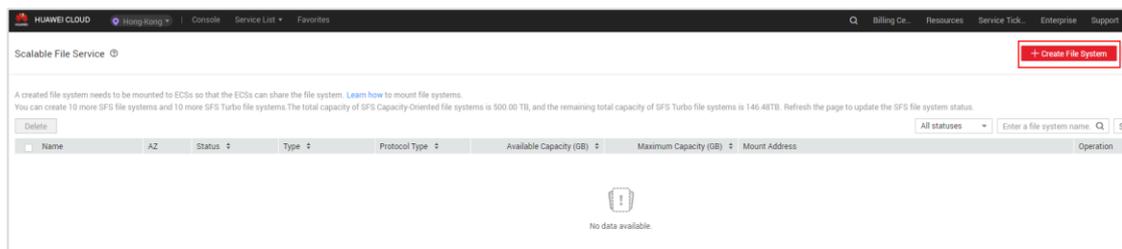
- Two ECSs have been purchased, one Linux and one Windows, each with an EIP bound. The Linux ECS runs CentOS 7.4 and will be deployed in **vpc-test-linux**, and the Windows ECS runs Windows Server 2012 and will be deployed in **vpc-test-windows**.

Procedure

- Step 1 Log in to the management console and choose **Service List > Storage > Scalable File Service**.



- Step 2 On the SFS console, click **Create File System**.



- Step 3 On the page displayed, enter the name, type, and VPC of the file system, confirm the settings, and click **Create Now**.

- **File System Type:** SFS
- **Region:** AP-Hong Kong
- **AZ:** Keep the default value.
- **Protocol Type:** NFS
- **VPC:** Use an existing VPC or create a new one. This VPC must be different from the VPCs of the two ECSs.
- **Maximum Capacity:** 1 GB



- **Name: sfs-sdcbb**
- **Quantity: 1**

Create File System

[Back to File System List](#)

* File System Type SFS SFS Turbo

* Region
File systems and ECSs in different regions cannot communicate with each other.

* AZ
File systems and ECSs in different AZs in the same region can communicate with each other.

* Protocol Type
The NFS protocol is recommended for a Linux client and the CIFS protocol is recommended for a Windows client.

* VPC [Create VPC](#)
ECSs cannot access file systems that reside on different VPCs. Select the VPCs where ECSs reside.

Maximum Capacity
Maximum capacity of a single file system. After the used capacity reaches this value, expand the file system. Otherwise, data can no longer be written to the file system.

Tag
It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#)

You can add 10 more tags.

Name
If you create multiple SFS file systems at the same time, the system automatically populates an SFS name (editable) and adds an incremental number to the end of each SFS name. For example, if the first SFS's name is sfs-share-001, the second SFS's name will be sfs-share-002.

Quantity
[You can create 10 more SFS file systems which can use up to 500.00 TB storage space. Increase quota](#)

[Create Now](#)

Step 4 Return to the SFS homepage and view the created SFS file system.

Scalable File Service

[Create File System](#) [Buy Storage Package](#)

A created file system needs to be mounted to ECSs so that the ECSs can share the file system. [Learn how to mount file systems.](#)
You can create 9 more SFS file systems and 10 more SFS Turbo file systems. The total capacity of SFS Capacity-Oriented file systems is 500.00 TB, and the remaining total capacity of SFS Turbo file systems is 146.46TB. Refresh the page to update the SFS file system status.

Name	AZ	Status	Type	Protocol Type	Available Capacity (GB)	Maximum Capacity (GB)	Mount Address	Operation
sfs-sdcbb	AZ1	Available	SFS Capacity-Oriented	NFS	1.00	1.00	sfs-nas01.ap-southeast-1a.myhuaweicloud.com/share-94561426	Resize Delete

Step 5 Grant permissions.

Normally, files can only be shared among ECSs within a single VPC. If you want to share the file system across multiple VPCs, you must specifically authorize access for those other VPCs.

On the SFS homepage, click the name of the file system name you want to grant access to. On the displayed page, choose **Basic Info** > **Authorizations** > **Add Authorized VPC** to authorize a VPC to access the file system. Add the two VPCs, **vpc-test-linux** and **vpc-test-windows**.



SFS File System List > sfs-sdcbb

Basic Info Mount Point Info

Name	sfs-sdcbb	ID	3c9d8def-
Protocol Type	NFS	Status	Available
Available Capacity (GB)	1.00	Maximum Capacity (GB)	1.00
Region	AP-Hong-Kong	AZ	AZ1
Created	Aug 13, 2020 19:43:47 GMT+08:00		

Authorizations Tags

Only ECSs on VPCs can access file systems. If there are no available VPCs, [apply for VPCs](#) first.

Add Authorized VPC You can add 19 more authorized VPCs and 399 more authorized addresses/segments.

Name

- vpc-default

Add Authorized VPC

VPC vpc-test-linux x Create VPC

You can add 19 more authorized VPCs.

OK Cancel

SFS File System List > sfs-sdcbb

Basic Info Mount Point Info

Name	sfs-sdcbb	ID	3c9d8def-5f98-4d73-b3c7-5a0512623d5c
Protocol Type	NFS	Status	Available
Available Capacity (GB)	1.00	Maximum Capacity (GB)	1.00
Region	AP-Hong-Kong	AZ	AZ1
Created	Aug 13, 2020 19:43:47 GMT+08:00		

Authorizations Tags

Only ECSs on VPCs can access file systems. If there are no available VPCs, [apply for VPCs](#) first.

Add Authorized VPC You can add 17 more authorized VPCs and 397 more authorized addresses/segments.

Name

- vpc-default
- vpc-test-linux
- vpc-test-windows

-----End

2.3.4 Mounting a File System to an ECS (Linux)

- Step 1 Log in to the ECS console. Locate the row that contains the Linux ECS you prepared for this exercise (CentOS 7.4) and click **Remote Login**.
- Step 2 Log in to the ECS as user **root**.



```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.12.1.el7.x86_64 on an x86_64

ecs-linux login: root
Password:

Welcome to Huawei Cloud Service

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

Step 3 Check whether the NFS software package has been installed in the OS.

rpm -qa|grep nfs

The NFS software package is usually included in the OS. If information similar to the following is displayed, the NFS software package is already installed. The command output varies according to operating systems.

```
[root@ecs-256845 ~]# rpm -qa|grep nfs
libnfsidmap-0.25-19.el7.x86_64
nfs-utils-1.3.0-0.66.el7.x86_64
```

If no command output is displayed, install the NFS software package.

```
[root@ecs-linux ~]# rpm -qa|grep nfs
[root@ecs-linux ~]#
```

As CentOS is used here, you can run the following command to install the package:

sudo yum -y install nfs-utils

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

Dependency Installed:
gssproxy.x86_64 0:0.7.0-28.el7          keyutils.x86_64 0:1.5.8-3.el7          libbasicobjects.x86_64 0:0.1.1-32.el7
libcollection.x86_64 0:0.7.0-32.el7     libevent.x86_64 0:2.0.21-4.el7         libini_config.x86_64 0:1.3.1-32.el7
libnfsidmap.x86_64 0:0.25-19.el7        libpath_utils.x86_64 0:0.2.1-32.el7         libref_array.x86_64 0:0.1.5-32.el7
libtirpc.x86_64 0:0.2.4-0.16.el7       libverto-libevent.x86_64 0:0.2.5-4.el7         quota.x86_64 1:4.01-19.el7
quota-nls.noarch 1:4.01-19.el7          rpcbind.x86_64 0:0.2.0-49.el7         tcp_wrappers.x86_64 0:7.6-77.el7

Complete!
```

For details about other OSs, see [Mounting an NFS File System to ECSs \(Linux\)](#).

Step 4 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!
```

Step 5 Log in to the SFS console, click the file system to be mounted, and view the mount address.

Name	AZ	Status	Type	Protocol Type	Available Capacity (GB)	Maximum Capacity (GB)	Mount Address
sfs-sdccb	AZ1	Available	SFS Capacity-Oriented	NFS	1.00	1.00	sfs-nas01.ap-southeast-1a.myhuaweicloud.com

The part of the address in the red box is the domain name of the file system.

Step 6 On the page for logging in to the Linux ECS, run the following command to check whether the file system domain name can be resolved:

`nslookup sfs-nas01.ap-southeast-1a.myhuaweicloud.com` (Replace it with the actual address.)

If the domain name can be resolved, information similar to the following is displayed:

```
root@ecs-linux ~# nslookup sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Server:      100.125.3.250
Address:     100.125.3.250#53

Non-authoritative answer:
Name:   sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Address: 100.125.96.42
Name:   sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Address: 100.125.96.44
Name:   sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Address: 100.125.96.45
Name:   sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Address: 100.125.96.52
Name:   sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Address: 100.125.96.40
Name:   sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Address: 100.125.96.43
Name:   sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Address: 100.125.96.51
Name:   sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Address: 100.125.96.46
Name:   sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Address: 100.125.96.50
Name:   sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Address: 100.125.96.49
Name:   sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Address: 100.125.96.47
Name:   sfs-nas01.ap-southeast-1a.myhuaweicloud.com
Address: 100.125.96.41

root@ecs-linux ~#
```



Step 7 Create a local directory for the mount.

```
mkdir [/i>Directory name]
```

Example:

```
mkdir /localfolder
```

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

Step 8 Mount the created file system to the local path.

```
mount -t nfs -o vers=3,nolock [SFS file system path] [Local path]
```

Example:

```
mount -t nfs -o vers=3,timeo=600,nolock sfs-nas01.ap-southeast-1a.myhuaweicloud.com:/share-a4661e26 /localfolder
```

```
[root@ecs-linux ~]# mount -t nfs -o vers=3,timeo=600,nolock sfs-nas01.ap-southeast-1a.myhuaweicloud.com:/share-a4661e26 /localfolder
[root@ecs-linux ~]#
```

Step 9 Check the mounted file system.

```
mount -l
```

```
[root@ecs-linux ~]# mount -l
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
devtmpfs on /dev type devtmpfs (rw,nosuid,size=496828k,nr_inodes=124285,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmoude=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,mode=755)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/usr/lib/ps-agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpuacct,cpu)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_prio,net_cls)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
configfs on /sys/kernel/config type configfs (rw,relatime)
/dev/vda1 on / type ext4 (rw,relatime,data=ordered)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=26,pgrp=1,timeout=0,minproto=5,maxproto=5)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=101436k,mode=700)
sfs-nas01.ap-southeast-1a.myhuaweicloud.com:/share-a4661e26 on /localfolder type nfs (rw,relatime,vers=3,rsize=131072,wbcs=255,hard,nolock,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=100.125.96.51,mountvers=3,mountudp,local_lock=all,addr=100.125.96.51)
[root@ecs-linux ~]#
```

----End



2.3.4.2 Creating a File in the Local Path

Step 1 Run the following commands to create the **new** file in the **localfolder** directory:

```
cd /localfolder
vim new
```

Step 2 Edit the **new** file, input **ecs**, and run the **:wq** command to save the file.

```
Hello HuaweiCloud SFS
```

Step 3 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]#
```

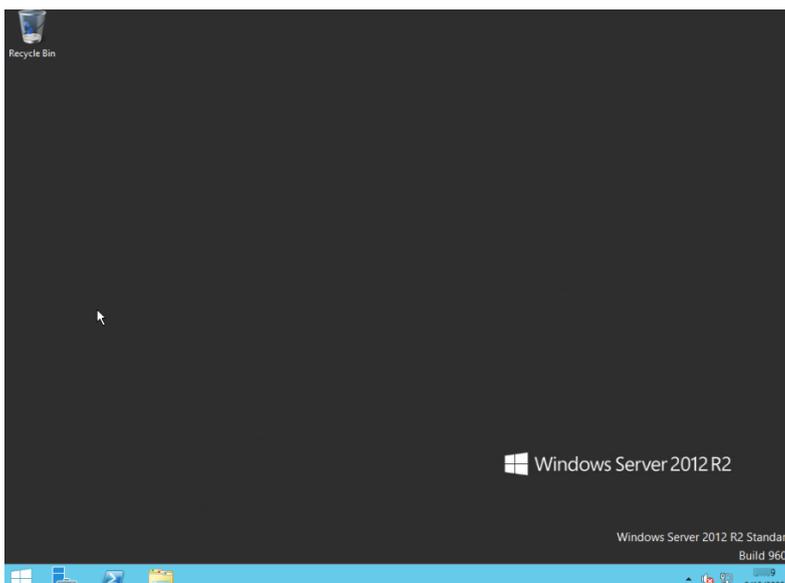
----End

2.3.5 Mounting a File System to an ECS (Windows)

2.3.5.1 Logging In to a Windows ECS

Log in to the ECS console. Locate the row that contains the ECS that you wish to mount the file system to and click **Remote Login**. In this example, **ecs-windows** is used.

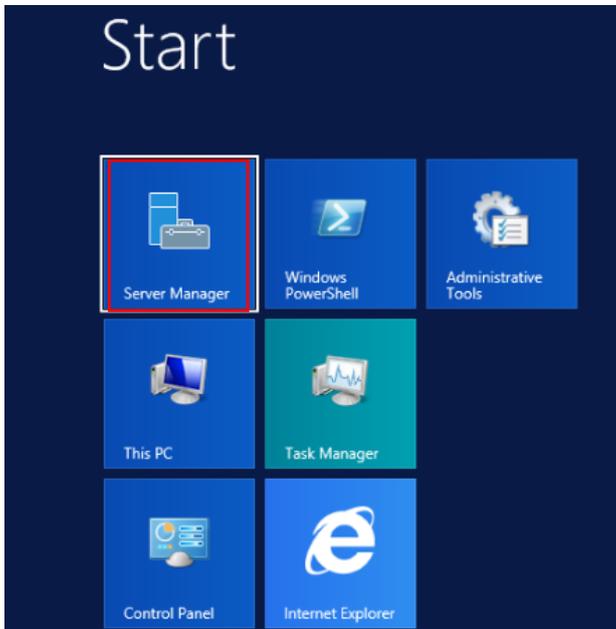
Name/ID	AZ	Status	Specifications/Image	IP Address	Billing Mode	Operation
vpc-test-windows c4c5b8a3-7206-4045-970f-f7d48e3ab29e	AZ2	Running	1 vCPUs 2 GB s2.medium.2 Windows Server 2012 R2 Standard 64bit Eng...	159.138.39.198 (EIP) 1 Mb/s 192.168.0.200 (Private IP)	Pay-per-use Created on Aug.13., 2020, 19:35:...	Remote Login



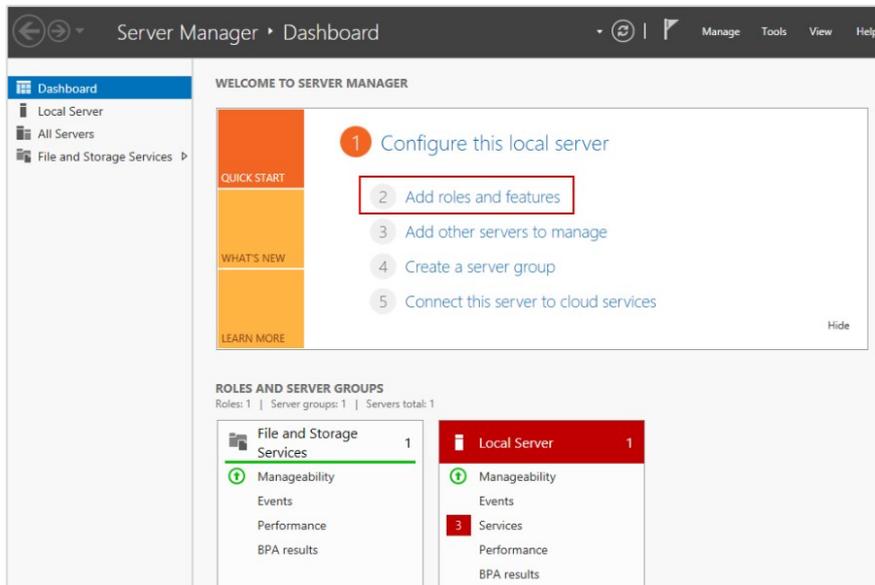


2.3.5.2 Installing the NFS client

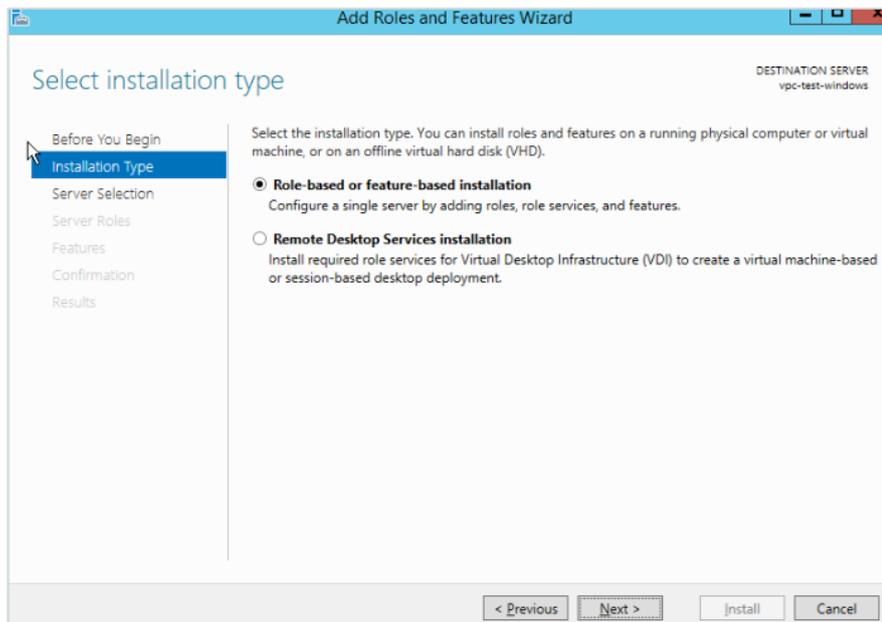
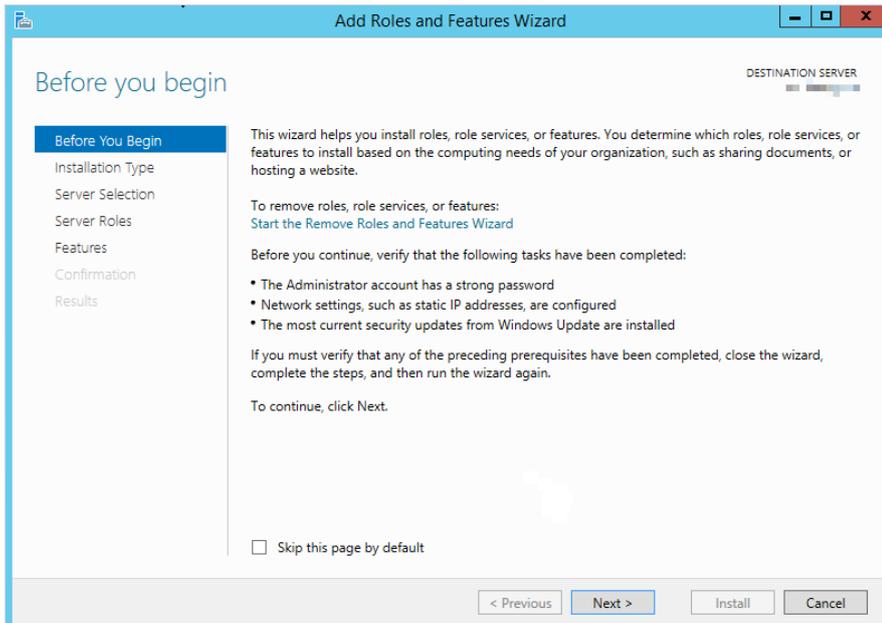
Step 1 Click **Server Manager** in the lower left corner.

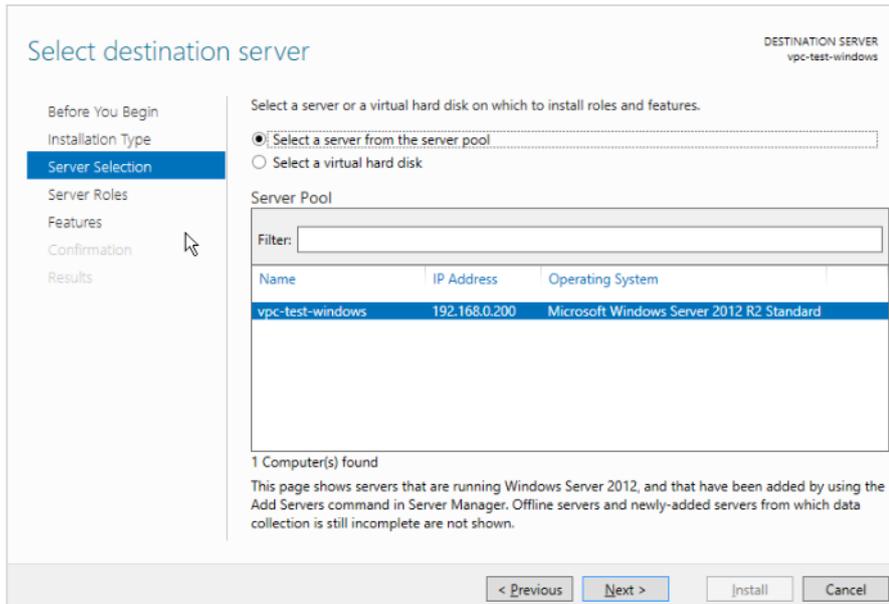


The **Server Manager** window is displayed.

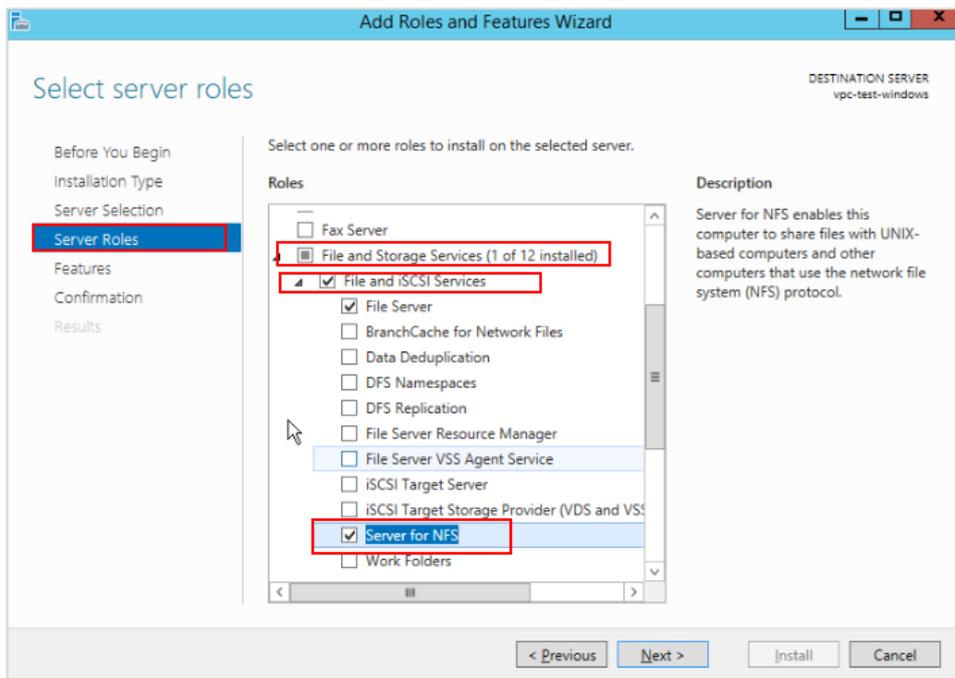


Step 2 Click **Next**.

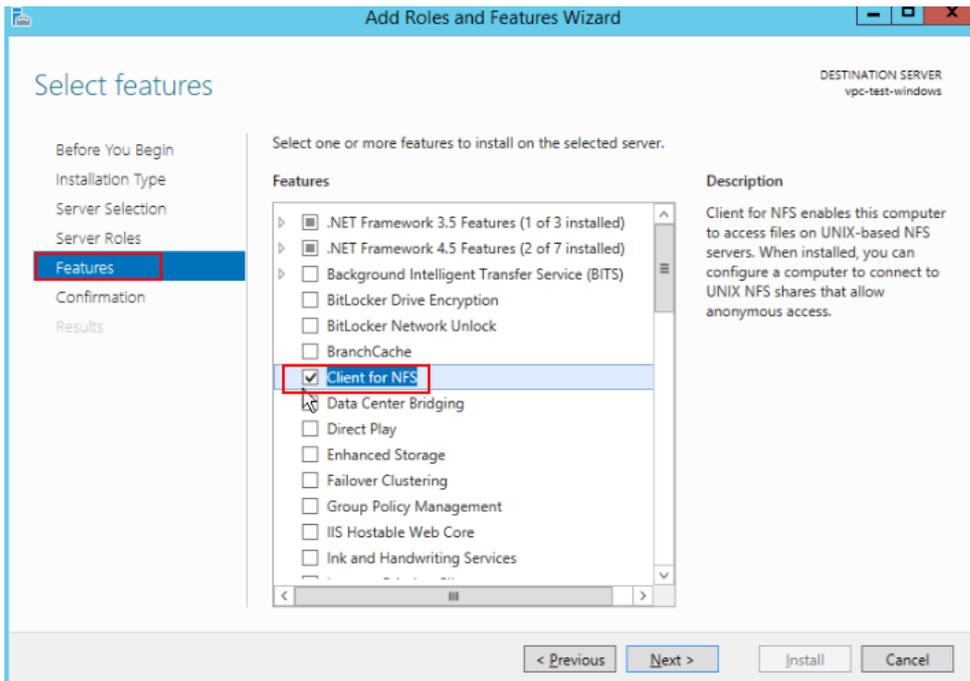




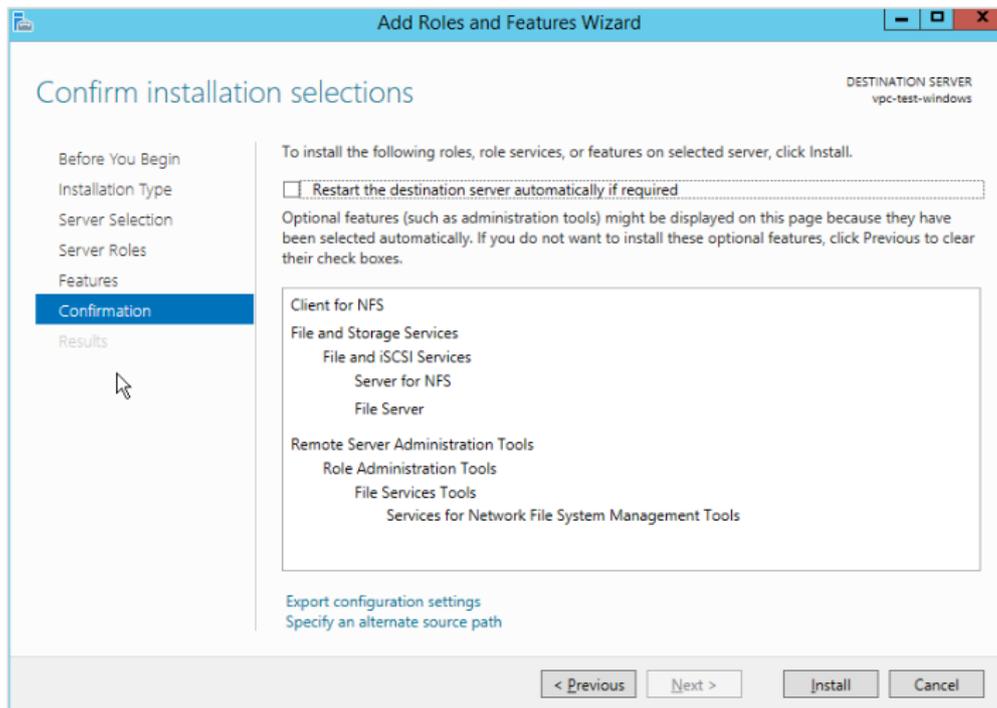
Step 3 Click **Next** when prompted, and on the **Server Roles** page, select **Server for NFS**.



Step 4 In the **Features** area, select **Client for NFS**.



Step 5 Confirm the settings and click **Install**.



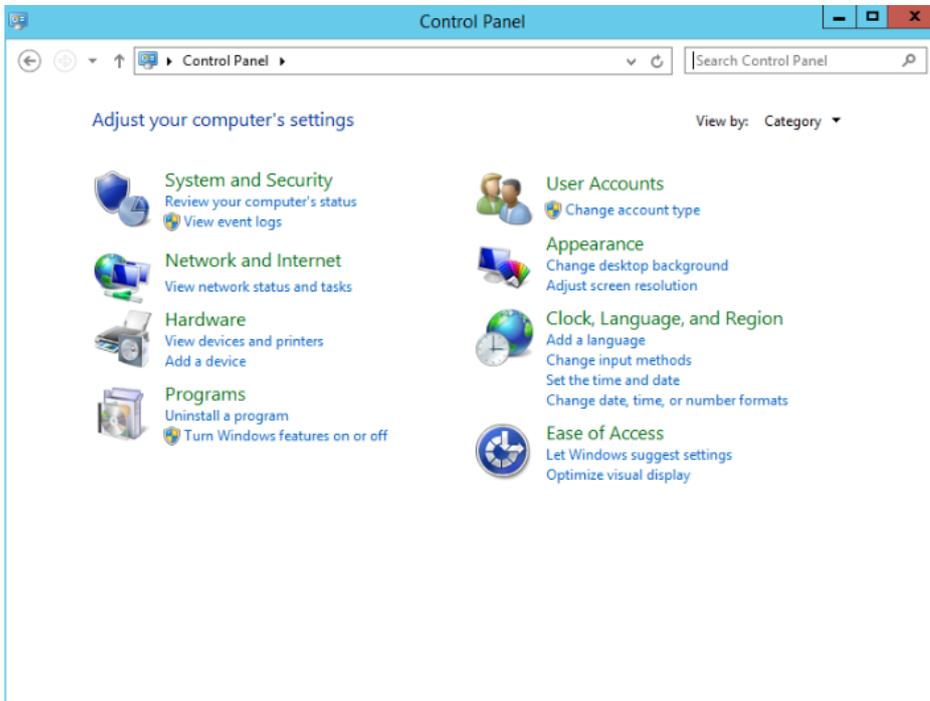
Step 6 If you are installing the NFS client for the first time, after the installation is complete, restart the client and log in to the ECS again when prompted.

-----End

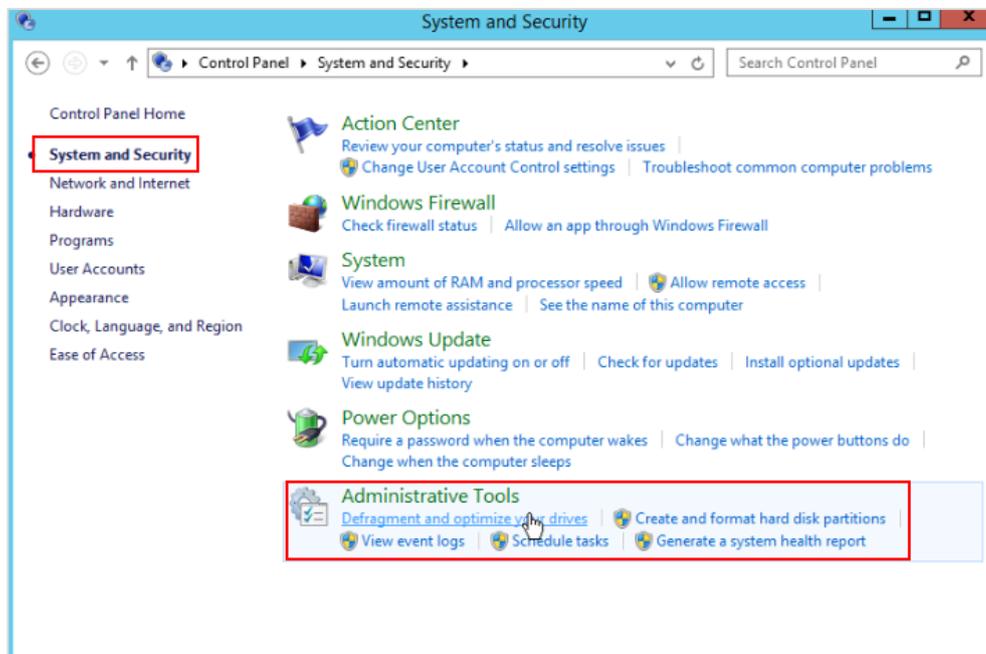


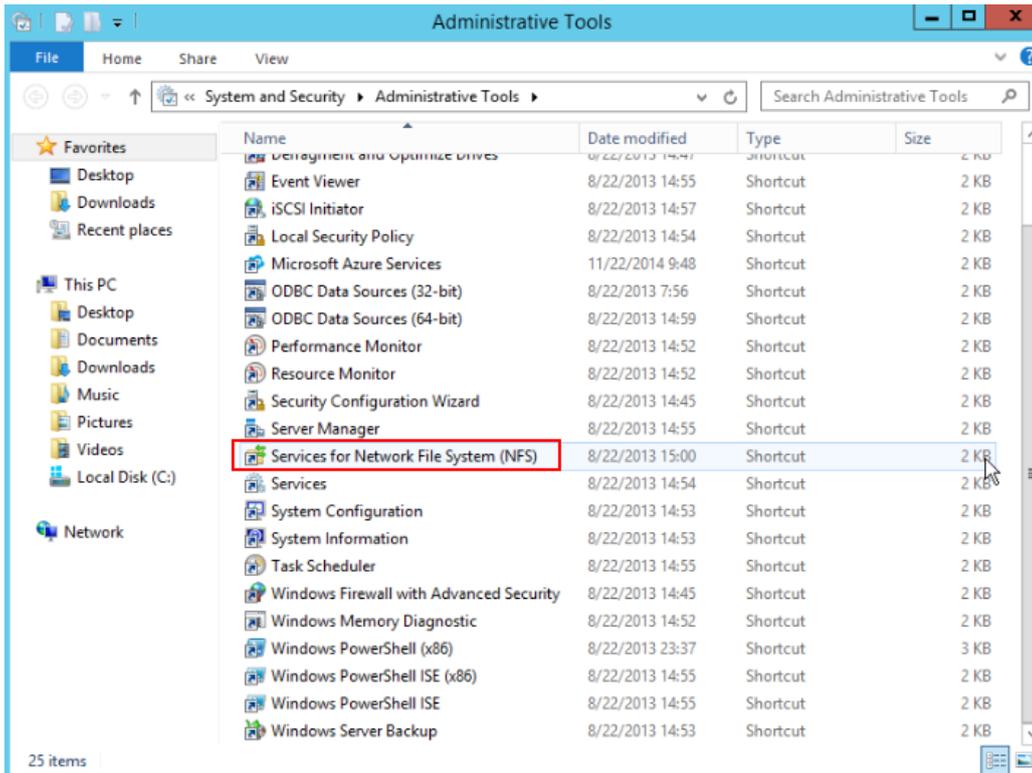
2.3.5.3 Mounting the File System

Step 1 Click **Control Panel** and select view by **Category**.

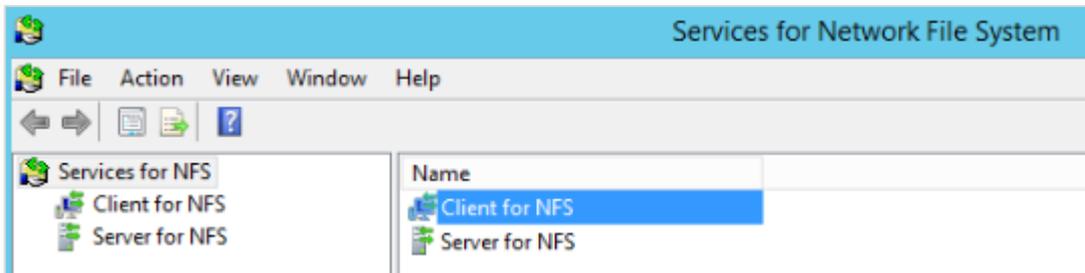


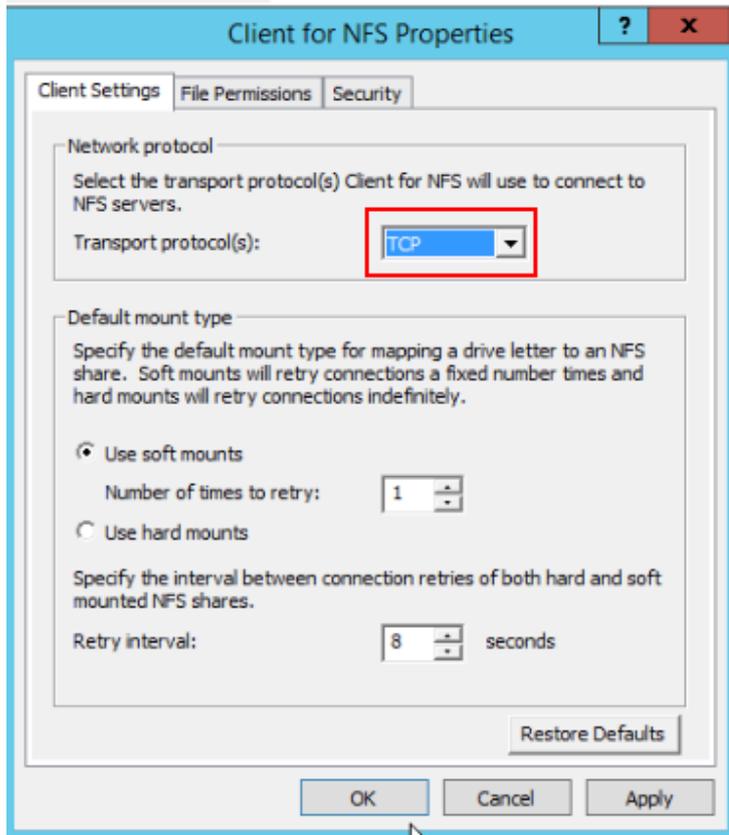
Step 2 Choose **System and Security > Administrative Tools**.





Step 3 Double-click **Services for Network File System (NFS)**. On the displayed window, right-click **Client for NFS**, select **Properties** from the shortcut menu, change the transport protocol to **TCP**, and select **Use hard mounts**.





Step 4 Run the following command in the Command Prompt of the Windows Server 2012 (X is the drive letter of the free disk).

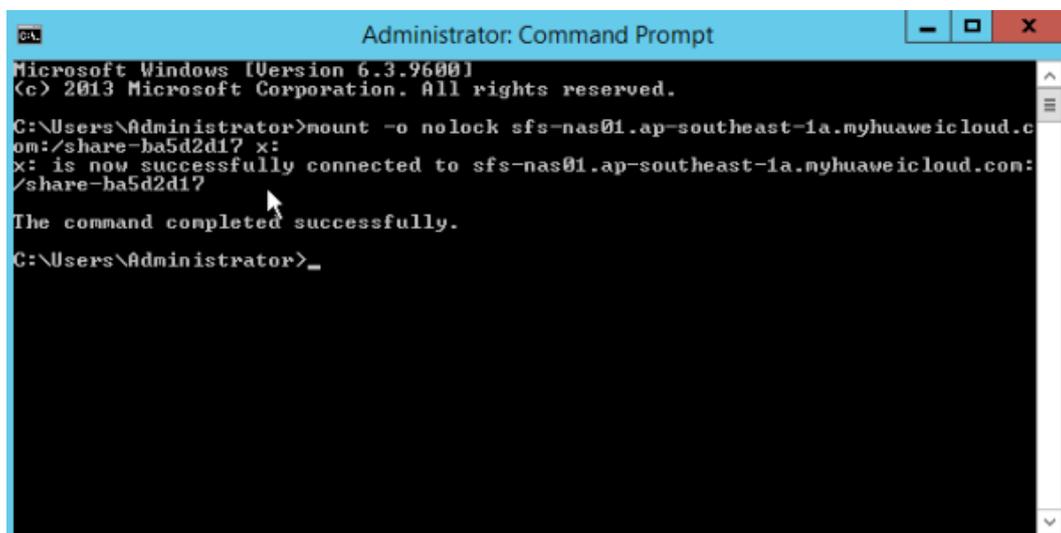
Run the following command in the SFS file system:

```
mount -o nolock [mount point] X
```

An example command is provided as follows:

```
mount -o nolock sfs-nas01.ap-southeast-1a.myhuaweicloud.com:/share-ba5d2d17 X
```

Obtain the mount point on the SFS file system details page.

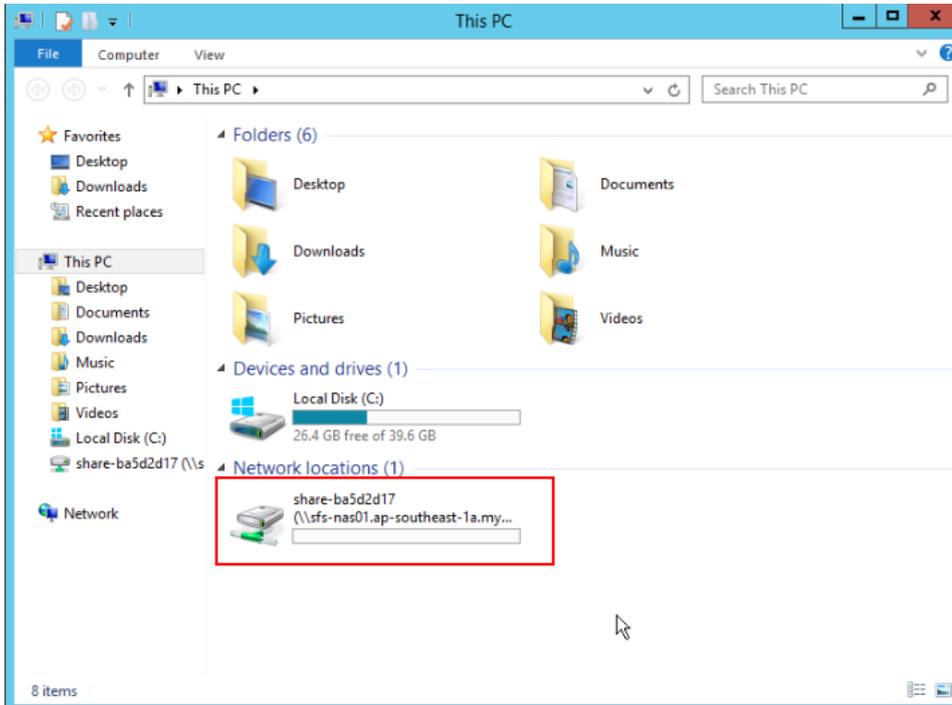




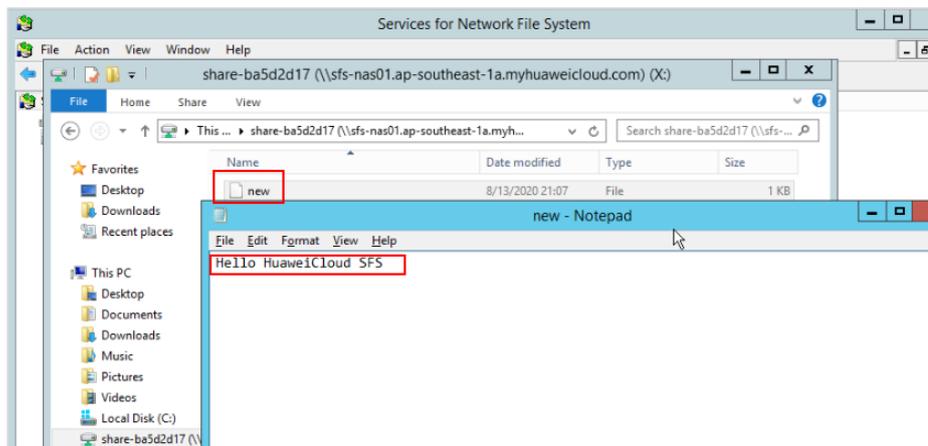
----End

2.3.5.4 Verification

Step 1 On the Windows ECS, click **This PC** to view the mounted file system.



Step 2 Access the file system and view the **new** file which was created on the Linux ECS, indicating that the file has been shared with the Windows system.



----End



2.3.6 Deleting Resources

2.3.6.1 Unmounting the File System (Linux)

- Step 1 Log in to Linux ECS and run the following command to confirm that the directory was successfully unmounted:

```
umount /localfolder
```

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

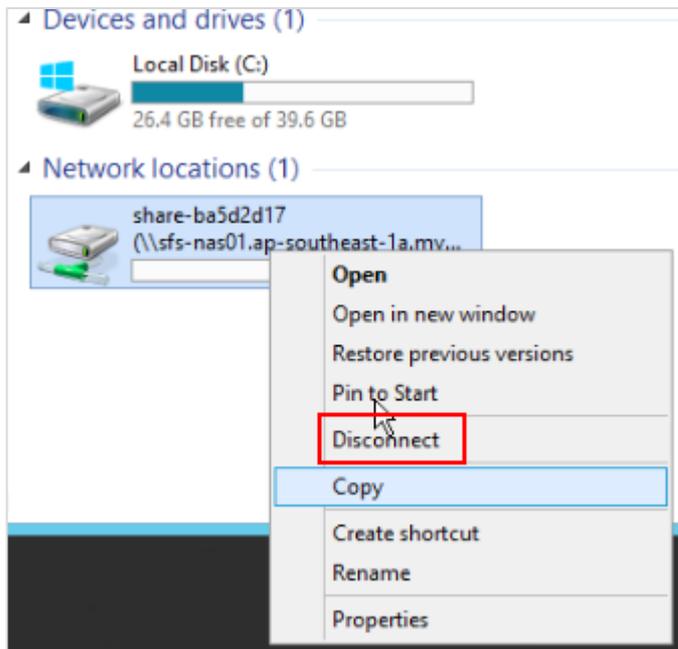
- Step 2 Run the following command to check whether the uninstallation is successful:

```
mount-l
```

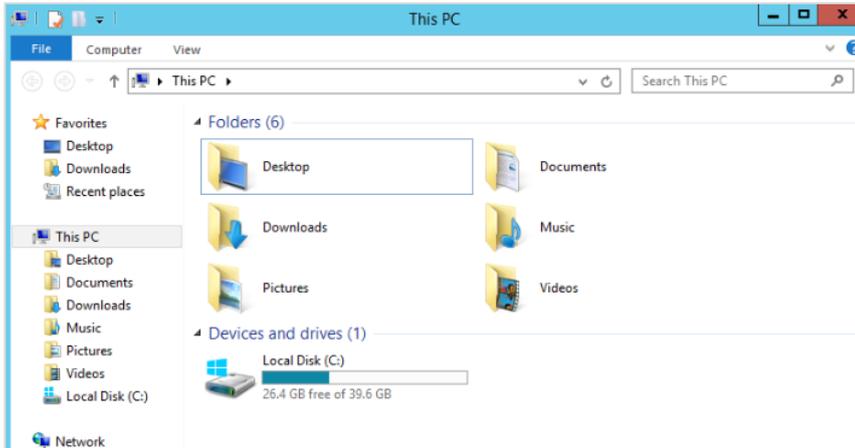
----End

2.3.6.2 Unmounting the File System (Windows)

- Step 1 Log in to ecs-windows. On the **This PC** page, right-click the file system to be unmounted and choose **Disconnect** from the shortcut menu.



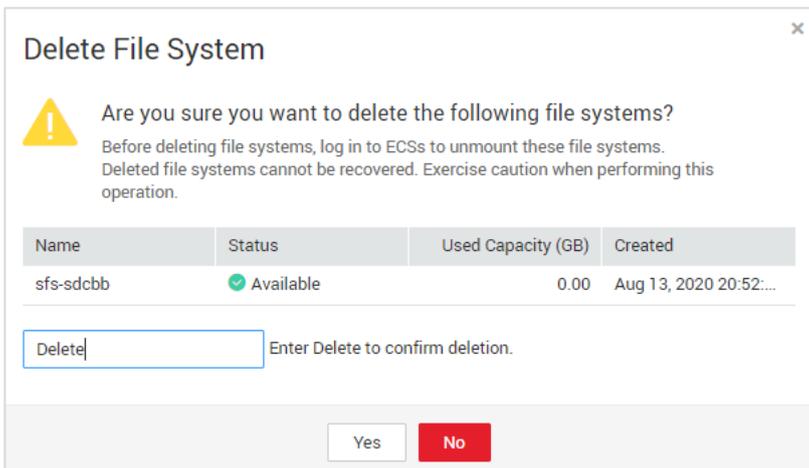
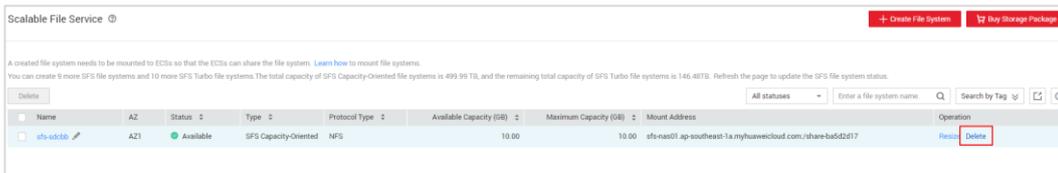
- Step 2 If the mounted file system is not shown as a network location anymore, the file system was successfully unmounted.



----End

2.3.6.3 Deleting the File System

- Step 1 Log in to the SFS console.
- Step 2 In the list of file systems, click **Delete** at the end of the row where the desired file system resides.



The status of the file system changes to **Deleting**. Refresh the page after a few moments. Once the file system has been deleted, it will no longer be displayed in the list.

- Step 3 Delete the Windows ECS and the VPCs you created and verify that the resources have been deleted. You can leave the Linux ECS for now as it will be used for subsequent exercises.



----End

2.4 CBR

2.4.1 Introduction

CBR enables you to back up ECSs, Hyper Elastic Cloud Servers (HECSs), BMSs, EVS disks, SFS Turbo file systems, and on-premises VMware virtual environments with ease. If there is a virus intrusion, accidental deletion, or software or hardware fault, you can restore data to any point in the past when the data was backed up.

CBR protects your services by ensuring the security and consistency of your data.

2.4.2 Objectives

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

- Purchase a vault.
- Create a cloud server backup.
- Use a cloud server backup to restore data.

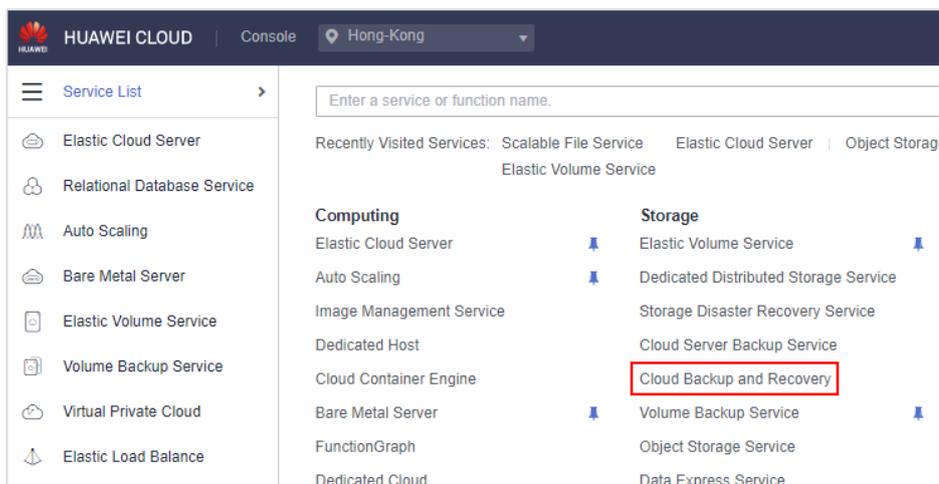
2.4.3 Tasks

Purchase a CBR vault on HUAWEI CLOUD and back up a cloud server to prevent data loss caused by disk faults or misoperations. Then use the created backup to restore data.

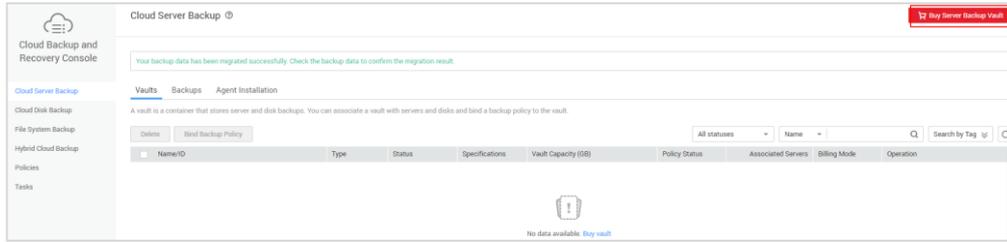
For this exercise, you must have a Linux server available.

2.4.4 Purchasing a Server Backup Vault

Step 1 Go to the CBR home page.

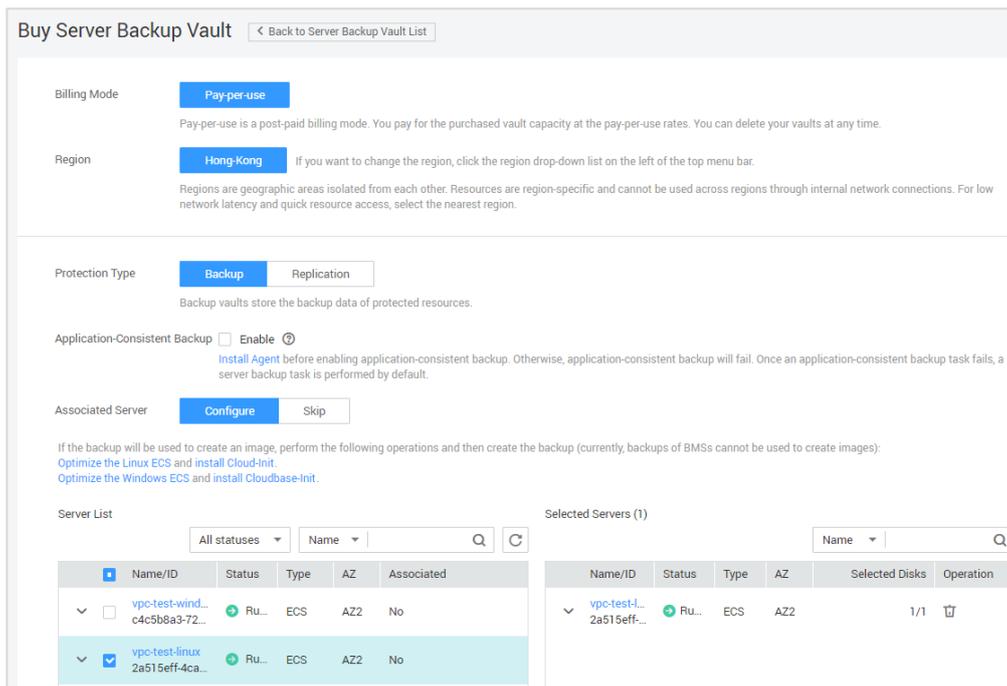


Step 2 Click **Buy Server Backup Vault**.



Step 3 Select the server to be backed up, configure other parameters based on your needs, confirm the settings, and submit the request.

- **Billing Mode: Pay-per-use**
- **Region: Hong-Kong**
- **Protection Type: Backup**
- **Associated Server:** In this example, select the Linux ECS purchased in section 2.3.
- **Capacity: 80 GB** (Adjust the value based on site requirements.)
- **Auto Backup:** Select **Configure** and create a backup policy.
- **Vault Name: vault-test**





* Capacity [Set the capacity to 40 GB to get a free package. Learn more](#)

The capacity of the selected disks is 40 GB. To ensure continuity, it is recommended that the vault space be greater than or equal to the space of the server to be backed up. **If the total backup capacity exceeds the vault capacity, the backup task fails.**

Auto Backup

After a vault is bound to a backup policy, automatic backup can be performed based on the policy.

Backup Policy

Tags

Tags here are for resource management only. It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#)

You can add 10 more tags.

* Vault Name

Price **\$0.004 USD**/hour
This price is an estimate and may differ from the final price. [Pricing details](#)

Step 4 Return to the **Cloud Server Backup** page. You can see the vault you created in the vault list.

Cloud Server Backup 17 My Server Backup Vault

Your backup data has been migrated successfully. [Check the backup data to confirm the migration result.](#)

Vaults Backups Agent Installation

A vault is a container that stores server and disk backups. You can associate a vault with servers and disks and bind a backup policy to the vault.

All statuses Name Search by Tag

Name/ID	Type	Status	Specifications	Vault Capacity (GB)	Policy Status	Associated Servers	Billing Mode	Operation
<input type="checkbox"/> vault-test 627abd93-d653-4e56b79d-c39086b13708	Backup	Available	Server backup	Used <input type="text" value="0"/> /80	Enabled	1	Pay-per-use	Associate Server More

----End

2.4.5 Restoring Data Using a Cloud Server Backup

If a disk on a server fails or server data is lost due to misoperations, you can use a backup to restore the server to its former state.

Prerequisites

- Disks on the server to be restored are running properly.
- The server to be restored has at least one backup.
- The backup status is **Available**.

Procedure

Step 1 Log in to Linux server and use **vim** to create a file.

vim /root/test

```
[root@ecs-linux ~]# vim /root/test
```



Step 2 Input `i` and enter **hello world!**, press **Esc**, input `:wq` to save the file and exit.

```
hello world_
```

Step 3 On the **Cloud Server Backup** page, click **Vaults** and locate the vault that the server is associated to.

Step 4 Choose **More > Perform Backup** in the **Operation** column. In the server list, select the server you want to back up. After the server is selected, it appears in the list of **Selected Servers**.

Name/ID	Type	Status	Specifications	Vault Capacity (GB)	Policy Status	Associated Servers	Billing Mode	Operation
vault-test b27abda3-d863-4e56b79d-c3508b613708	Backup	Available	Server backup	Used 0/80	Enabled	1	Pay-per-use	Associate Server More Perform Backup Create Replicas Bind Backup Policy Bind Replication Policy Change Specifications Expand Capacity Delete

Perform Backup

If the backup will be used to create an image, perform the following operations and then create the backup (currently, backups of BMSs cannot be used to create images):
[Optimize the Linux ECS and install Cloud-Init.](#)
[Optimize the Windows ECS and install CloudBase-Init.](#)

Server List

Name/ID	Status	Type	AZ	Associated
vpc-test-linux-2a515eff-4ca...	Ru...	ECS	AZ2	Yes(vault-test)

Selected Servers (1)

Name/ID	Status	Type	AZ	Selected Disks	Operation
vpc-test-li...-2a515eff...	Ru...	ECS	AZ2	1/1	

Name: manualbk_vault-test-1859

Description: 0/255

Full Backup Enable

OK

Step 5 Log back in to the server again and delete the file you created in Step 1.

```
rm -rf /root/test
```

Step 6 Confirm that the file has been deleted.

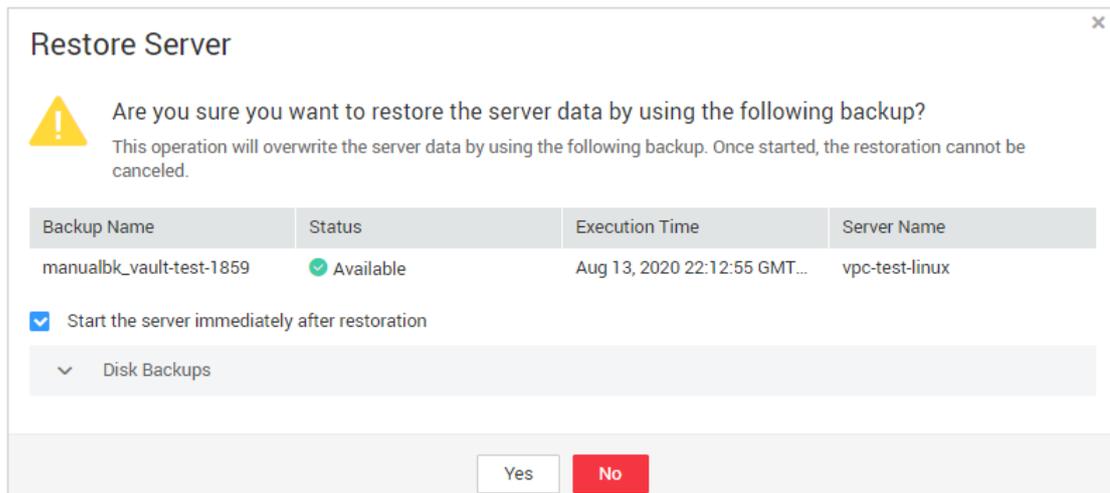
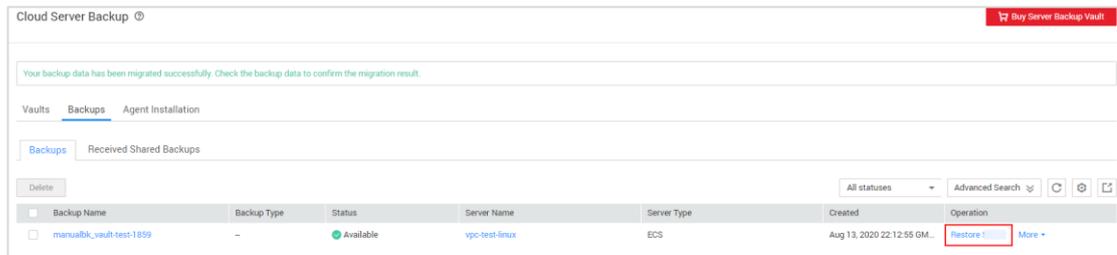
```
cat /root/test
```



```
[root@ecs-linux ~]# cat /root/test
cat: /root/test: No such file or directory
```

If the preceding message is displayed, the file has been deleted.

- Step 7 Log in to the CBR console. On the **Cloud Server Backup** tab page, click **Backups**, locate the backup of your server, and click **Restore Server** in the row where the backup resides. In the displayed **Restore Server** dialog box, click **Yes**.



- Step 8 Log in to the server and confirm that the file has been restored.

```
cat /root/test
```

```
[root@ecs-linux ~]# cat /root/test
hello world!
```

If the preceding message is displayed, the file has been restored.

----End



2.4.6 Deleting Resources

- Step 1 Delete the ECS and VPCs.
- Step 2 Delete the vault and backup.



Make sure that all the resources you created have been deleted.

----End



3 Network Services

3.1 Introduction

In this exercise, we will verify that two ECSs in a VPC can communicate with each other by default, security groups can be used to control communication between ECSs, ECSs can access the Internet after an EIP is bound to each, and that ELB can distribute traffic across backend servers. You 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.

3.1.1 Objectives

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

- Have a good command of VPC functions
- Understand how to use ELB to distribute traffic.
- Create a VPC peering connection to enable communication between ECSs in different VPCs of the same region.
- Create a VPN connection to enable ECSs in different regions to communicate with each other.

3.1.2 Tasks

- Prepare resources.
- Verify that two ECSs in a VPC can communicate with each other by default.
- Verify that security groups can be used to control communication.
- Access the Internet through ECS after an EIP is bound to the ECS.
- Use ELB to distribute traffic.
- Create a VPC peering connection to enable communication between ECSs in different VPCs of the same region.
- Create a VPN connection to enable ECSs in different regions to communicate with each other.

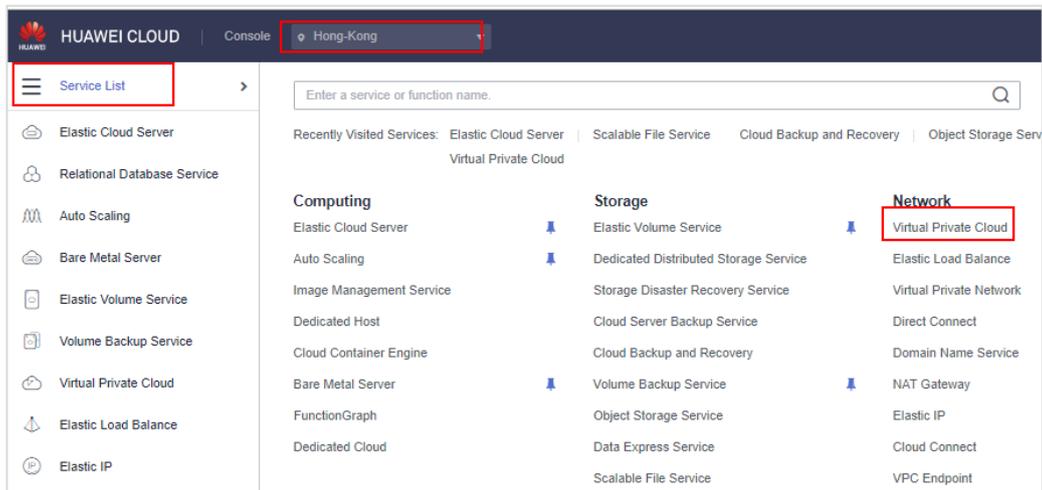


3.2 Preparing Resources

3.2.1 Creating VPCs

Create three VPCs, with two in AP-Hong Kong, and one in CN South-Guangzhou.

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



- Step 2 Click **Create VPC**.



Set the following parameters, and click **Create Now**.

- **Region:** AP-Hong Kong
- **Name:** VPC-01
- **CIDR Block:** Use the default CIDR block, for example, 192.168.0.0/16.
- **Default subnet name:** subnet-01
- **Other parameters:** Retain their default settings.



Step 3 View the created VPC in the VPC list.

Name	IPV4 CIDR Block	Status	Subnets	Route Tables	Operation
VPC-01	192.168.0.0/16	Available	0	1	Modify CIDR Block Delete

Step 4 Click **Create VPC** again and set the following parameters.

- **Region:** AP-Hong Kong
- **Name:** VPC-02
- **CIDR Block:** Set a CIDR block different from that of **VPC-01**, for example, 10.0.0.0/24.
- **Default subnet name:** subnet-02
- **Other parameters:** Retain their default settings.



Step 5 View the created VPC in the VPC list.

Name	IPv4 CIDR Block	Status	Subnets	Route Tables	Operation
VPC-02	10.0.0.0/24	Available	0	1	Modify CIDR Block Delete
VPC-01	192.168.0.0/16	Available	1	1	Modify CIDR Block Delete

Step 6 Switch the region to CN South-Guangzhou and create a VPC by setting the following parameters:

- **Name:** VPC-03
- **CIDR Block:** Set a CIDR block different from those of VPC-01 and VPC-02, for example, 172.16.0.0/24.
- **Default subnet name:** subnet-03
- **Other parameters:** Retain their default settings.

Basic Information

Region: CN South-Guangzhou

Name: VPC-03

CIDR Block: 172.16.0.0 / 24

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

Default Subnet

Name: subnet-03

CIDR Block: 172.16.0.0 / 24 Available IP Addresses: 251

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

Associated Route Table: Default

Free Create Now

Step 7 View the created VPC in the VPC list.

Name	IPv4 CIDR Block	Status	Subnets	Route Tables	Operation
VPC-03	172.16.0.0/24	Available	0	1	Edit CIDR Block Delete

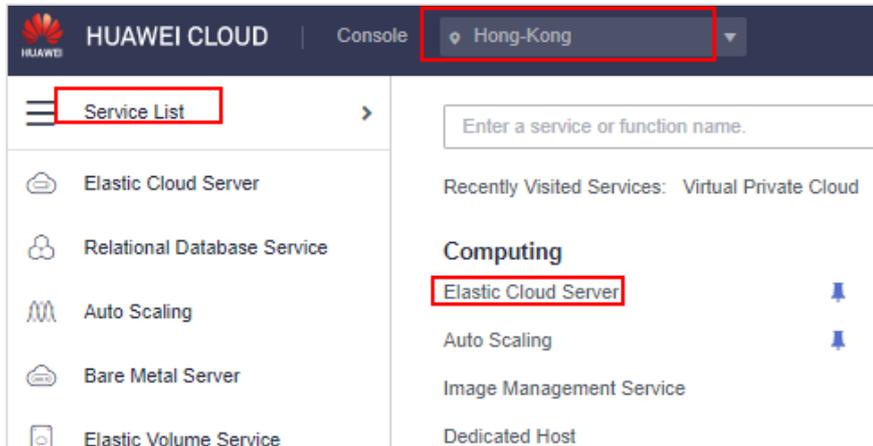
----End



3.2.2 Buying ECSs

Buy four Linux ECSs, two ECSs in **VPC-01**, one ECS in **VPC-02**, and one ECS in **VPC-03**. Do not buy EIPs when you purchase ECSs.

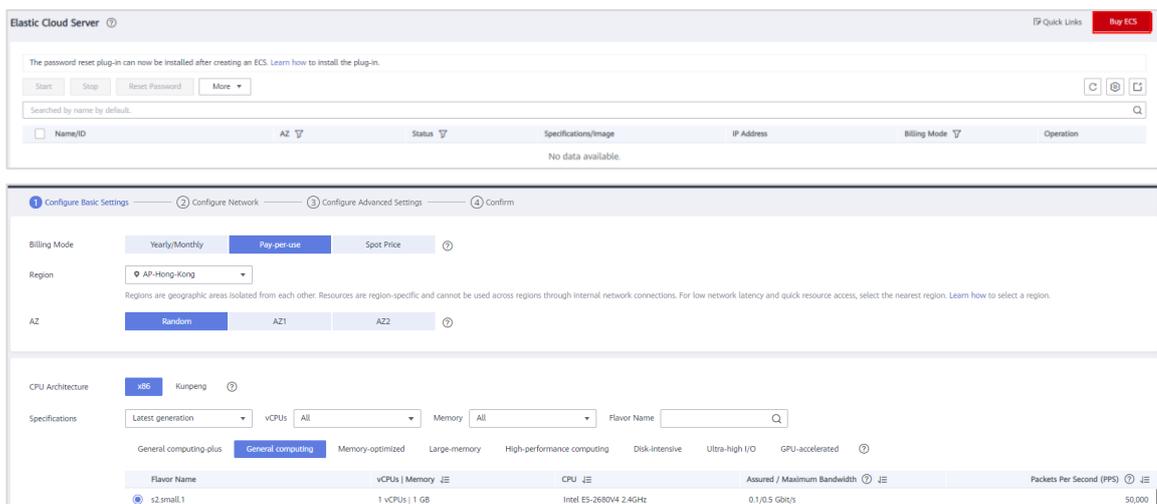
Step 1 Select the AP-Hong Kong region, click **Service List**. Under **Computing**, select **Elastic Cloud Server**.



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

Basic settings:

- **Billing Mode:** Pay-per-use
- **Region:** AP-Hong Kong
- **AZ:** any AZ
- **CPU Architecture:** x86
- **Specifications:** General computing, s6.small.1, 1 vCPU | 1 GB
- **Image:** public image, CentOS 7.6 64bit (40GB)
- **System Disk:** high I/O, 40 GB





Image

Public image Private image Shared image Marketplace image

CentOS CentOS 7.6 64bit(40GB)

System Disk

High I/O 40 GB IOPS limit: 1,440, IOPS burst limit: 5,000

Free package benefits are applied when you select a 40 GB of High I/O disk. [Learn more](#)

Add Data Disk You can attach 23 more disks.

Network configuration:

- **Network: VPC-01**
- **Security Group: sys-default**
- **EIP: Not required**

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

Network

VPC-01(192.168.0.0/16) subnet-01(192.168.0.0/24) Automatically-assigned IP address

Create VPC

Extension NIC

Add NIC You can add 11 more NICs.

Security Group

default (06e716b9-2ec5-4618-8b4f-b1ca4f6814e1) Create Security Group

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

Security Group Rules

EIP

Auto assign Use existing Not required

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

Advanced settings:

- **ECS Name: for example, ecs-HK**
- **Login Mode: Password, for example, Huawei@123!**
- **Quantity: 2**



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

ECS Name Allow duplicate ECS names

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

Login Mode

Username root

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

Confirm Password

ECS Group (Optional) ?

C

[Create ECS Group](#)

Advanced Options Configure now

Quantity ECS Price **\$0.036 USD**/hour ?
 Free quota will be deducted preferentially. [Learn more](#)

Step 3 Confirm the configuration and click **Buy Now**.

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

Note: The primary network interface does not have an EIP bound, and the ECS cannot access the Internet.

Configuration		Basic ✎					
Billing Mode	Pay-per-use	Region	Hong-Kong	AZ	AZ2		
Specifications	General computing s2.small.1 1 vCPUs 1 GB	Image	CentOS 7.6 64bit	System Disk	High I/O,40 GB		
Network ✎		Security Group		default	Primary NIC	subnet-01(192.168.0.0/24)	
VPC	VPC-01(192.168.0.0/16)	EIP		No EIP bound to the primary network interface			
Advanced ✎		ECS Name	ecs-HK	Login Mode	Password	ECS Group	--

Quantity You can create 20 more ECSs. [Learn how to increase quota.](#)

Agreement I have read and agree to the [Service Level Agreement](#) and [Huawei Image Disclaimer](#).

Step 4 View the purchased ECSs in the ECS list.

Two ECSs are automatically named by the system. One is **ecs-HK-0001**, and the other is **ecs-HK-0002**.



Name/ID	AZ	Status	Specifications/Image	IP Address
ecs-HK-0002 9172c89f-5b06-4a55-8350-a770aea1cf97	AZ2	Running	1 vCPUs 1 GB s2.small.1 CentOS 7.6 64bit	192.168.0.96 (Private IP)
ecs-HK-0001 90e35181-ea51-40b7-8b14-dd9c83a51b9b	AZ2	Running	1 vCPUs 1 GB s2.small.1 CentOS 7.6 64bit	192.168.0.81 (Private IP)

Step 5 Repeat Step 2 and Step 3 to buy an ECS named **ecs-HK-0003** in VPC-02.

Name/ID	AZ	Status	Specifications/Image	IP Address
ecs-HK-0003 a5896a61-1fe8-4944-aa28-bc628a57e38d	AZ2	Running	1 vCPUs 1 GB s2.small.1 CentOS 7.6 64bit	10.0.0.122 (Private IP)
ecs-HK-0002 9172c89f-5b06-4a55-8350-a770aea1cf97	AZ2	Running	1 vCPUs 1 GB s2.small.1 CentOS 7.6 64bit	192.168.0.96 (Private IP)
ecs-HK-0001 90e35181-ea51-40b7-8b14-dd9c83a51b9b	AZ2	Running	1 vCPUs 1 GB s2.small.1 CentOS 7.6 64bit	192.168.0.81 (Private IP)

Step 6 Switch the region to CN South-Guangzhou and repeat Step 2 and Step 3 to buy an ECS in **VPC-03**.

Name/ID	AZ	Status	Specifications/Image	IP Address	Billing Mode	Tag
ecs-GZ0001 4d313a9e-93e6-4873-bb42-ae92...	AZ2	Running	1 vCPUs 1 GB s2.small.1 CentOS 7.6 64bit	172.16.0.217 (Private IP)	Pay-per-use Created on Jan 20, 20...	--

-----End

3.3 Verifying Network Service Functions

- Verify that two ECSs in a VPC can communicate with each other by default.
- Verify that the security groups can control traffic from and to the ECSs in the VPCs.
- Verify that the ECS that has an EIP bound can access the Internet.
- Verify that ELB can distribute traffic across ECSs.
- Create a VPC peering connection to enable communication between ECSs in different VPCs of the same region.



- Buy a VPN connection to enable communication between ECSs in different regions.

3.3.1 Communication Between Two ECSs in a VPC

- Step 1 On the ECS console, Switch the region to AP-Hong Kong, record the private IP address of **ecs-HK-0001**, and log in to **ecs-HK-0002** remotely.

Name/ID	AZ	Status	Specifications/Image	IP Address	Billing Mode	Operation
ecs-HK-0003 a5896a61-1fe8-4944-aa28-bcc2ba57e38d	AZ2	Running	1 vCPUs 1 GB s2.small1 CentOS 7 6 64bit	10.0.0.122 (Private IP)	Pay-per-use Created on Aug 14, 2020 09:46:26	Remote Login More
ecs-HK-0002 9172d8f-9b06-4a55-8350-a770bae1d97	AZ2	Running	1 vCPUs 1 GB s2.small1 CentOS 7 6 64bit	192.168.0.96 (Private IP)	Pay-per-use Created on Aug 14, 2020 09:44:00	Remote Login More
ecs-HK-0001 9ba35181-a451-40b7-8b14-d8dc3a519b6	AZ2	Running	1 vCPUs 1 GB s2.small1 CentOS 7 6 64bit	192.168.0.81 (Private IP)	Pay-per-use Created on Aug 14, 2020 09:44:00	Remote Login More

- Step 2 Enter the username (**root** for Linux ECSs by default) and password.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.12.1.el7.x86_64 on an x86_64

ecs-hk-0002 login: root
Password:

Welcome to Huawei Cloud Service

[root@ecs-hk-0002 ~]# _
```

- Step 3 Ping the private IP address of **ecs-HK-0001**.

If **ecs-HK-0001** can be pinged, the two ECSs can communicate with each other, as shown in the following page.

```
[root@ecs-hk-0002 ~]# ping 192.168.0.81
PING 192.168.0.81 (192.168.0.81) 56(84) bytes of data:
64 bytes from 192.168.0.81: icmp_seq=1 ttl=64 time=1.13 ms
64 bytes from 192.168.0.81: icmp_seq=2 ttl=64 time=0.295 ms
64 bytes from 192.168.0.81: icmp_seq=3 ttl=64 time=0.272 ms
64 bytes from 192.168.0.81: icmp_seq=4 ttl=64 time=0.279 ms
64 bytes from 192.168.0.81: icmp_seq=5 ttl=64 time=0.268 ms
64 bytes from 192.168.0.81: icmp_seq=6 ttl=64 time=0.287 ms
64 bytes from 192.168.0.81: icmp_seq=7 ttl=64 time=0.286 ms
64 bytes from 192.168.0.81: icmp_seq=8 ttl=64 time=0.272 ms
64 bytes from 192.168.0.81: icmp_seq=9 ttl=64 time=0.298 ms
```

- Step 4 Ping the private IP address of **ecs-HK-0003**.

If the following page is displayed, **ecs-HK-0002** cannot communicate with **ecs-HK-0003** because the two ECSs are in different VPCs.

```
[root@ecs-hk-0002 ~]# ping 10.0.0.122
PING 10.0.0.122 (10.0.0.122) 56(84) bytes of data.
```



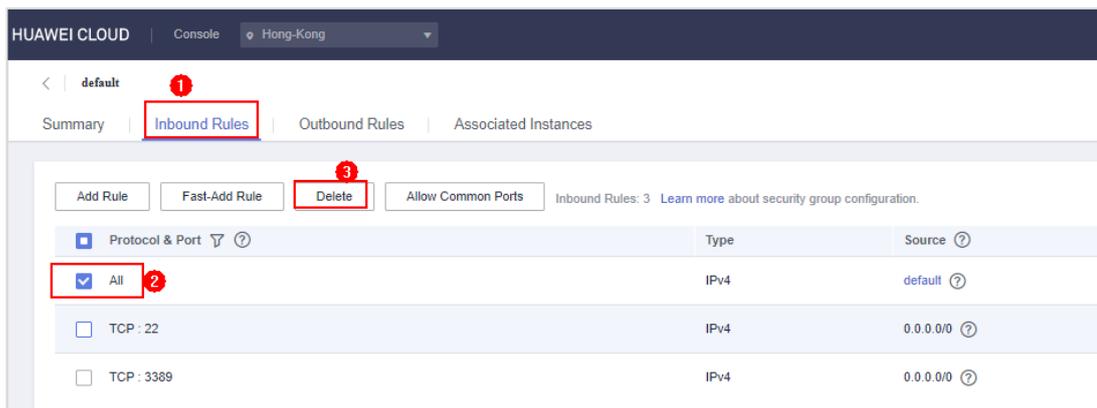
----End

3.3.2 Traffic Control by Security Groups

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



Step 2 Click the security group name and then delete the **All** rule.

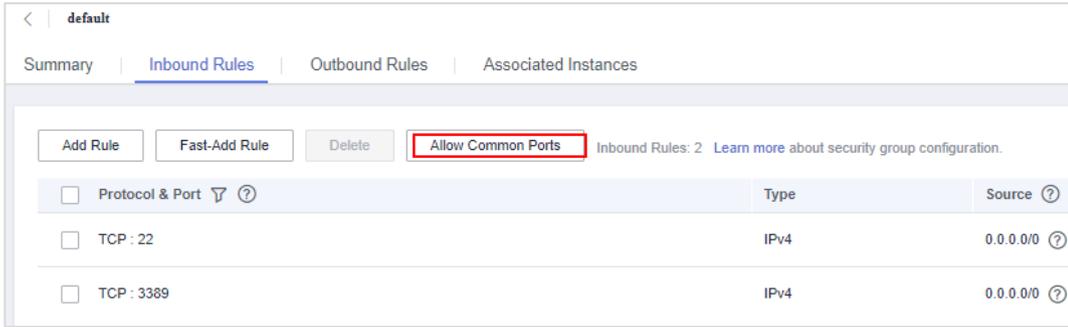


Step 3 Go back to the CLI of **ecs-HK-0002** and ping the private IP address of **ecs-HK-0001**.

You can see that the two ECSs cannot communicate with each other.

```
[root@ecs-hk-0002 ~]# ping 192.168.0.81
PING 192.168.0.81 (192.168.0.81) 56(84) bytes of data.
```

Step 4 Go back to the security group details page and add an inbound rule. Select **Allow Common Ports**.



Step 5 Go back to the CLI of **ecs-HK-0002** and ping the private IP address of **ecs-HK-0001**.

You can see that two ECSs can now communicate with each other, indicating that the added inbound security group rule has taken effect.

```
[root@ecs-hk-0002 ~]# ping 192.168.0.81
PING 192.168.0.81 (192.168.0.81) 56(84) bytes of data:
64 bytes from 192.168.0.81: icmp_seq=59 ttl=64 time=0.616 ms
64 bytes from 192.168.0.81: icmp_seq=60 ttl=64 time=0.285 ms
64 bytes from 192.168.0.81: icmp_seq=61 ttl=64 time=0.305 ms
64 bytes from 192.168.0.81: icmp_seq=62 ttl=64 time=0.329 ms
64 bytes from 192.168.0.81: icmp_seq=63 ttl=64 time=0.311 ms
64 bytes from 192.168.0.81: icmp_seq=64 ttl=64 time=0.383 ms
64 bytes from 192.168.0.81: icmp_seq=65 ttl=64 time=0.325 ms
64 bytes from 192.168.0.81: icmp_seq=66 ttl=64 time=0.325 ms
64 bytes from 192.168.0.81: icmp_seq=67 ttl=64 time=0.317 ms
```

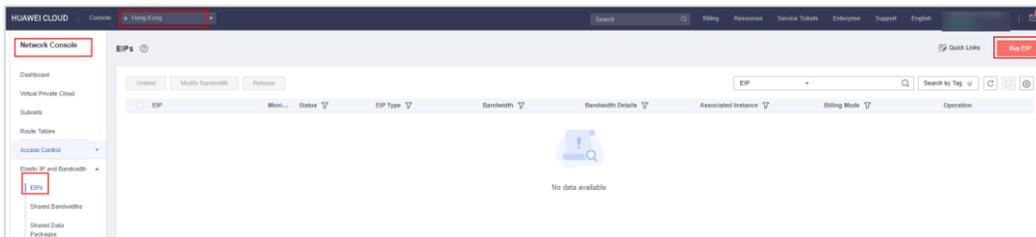
----End

3.3.3 Access to the Internet

Step 1 On the CLI of **ecs-HK-0002**, ping **baidu.com**. You can see that **ecs-HK-0002** fails to access the website.

```
[root@ecs-hk-0002 ~]# ping baidu.com
PING baidu.com (228.181.38.148) 56(84) bytes of data.
```

Step 2 Switch back to the network console, choose **Elastic IP > Buy EIP**.





Step 3 Set the following parameters, click **Buy Now**, confirm the configuration, and click **Submit**.

- **Billing Mode: Pay-per-use**
- **Region: AP-Hong Kong**
- **EIP Type: Dynamic BGP**
- **Billed By: Bandwidth**
- **Bandwidth: 1 Mbit/s**
- **Other parameters: Retain their default settings.**

Buy EIP

Billing Mode: Yearly/Monthly Pay-per-use

Region:

An EIP can only be associated with a cloud resource in its same region. After the purchase, the region cannot be changed. Exercise caution when selecting the region.

EIP Type: Dynamic BGP ?

Greater than or equal to 99.95% service availability rate

Billed By: Bandwidth Traffic Shared Bandwidth

For heavy/stable traffic For light/sharply fluctuating traffic For staggered traffic

Billed based on usage duration and bandwidth size.

Bandwidth: Custom

The bandwidth can be from 1 to 2,000 Mbit/s.

Free Anti-DDoS protection

Bandwidth Name:

Advanced Settings

Monitoring: Monitoring is enabled by default. **Free**

You can monitor network traffic at one-minute granularity, for free. You can monitor bandwidth fluctuations, and inbound/outbound bandwidth rates.

Quantity:

A maximum of 5 EIPs can be purchased at a time. You can buy 10 more EIPs. Increase quota

Step 4 On the **Elastic IP** page, locate the purchase EIP and click **Bind** in the **Operation** column. Select **ecs-HK-0002** and bind the EIP to it.

EIPs

Unbind Modify Bandwidth Release

EIP 159.138.39.198

EIP	Moni...	Status	EIP Type	Bandwidth	Bandwidth Details	Associated Instance	Billing Mode	Operation
159.138.39.198	<input type="checkbox"/>	Unbound	Dynamic BGP	bandwidth-c230	Bandwidth 1 Mbit/s	-	Pay-per-use Created on Aug 14, 2020 11:02:17	Bind Unbind More

Bind EIP

EIP: 159.138.39.198

Instance Type: ECS BMS Virtual IP address

All statuses Name Search by Tag

Name	Status	EIP	Private IP Address
ecs-HK-0003	Running	--	10.0.0.122
ecs-HK-0002	Running	--	192.168.0.96
ecs-HK-0001	Running	--	192.168.0.81

NIC

Selected Instance: ecs-HK-0002

NIC: IP: 192.168.0.96, MAC: fa-16-3e-09-b1-18 (Primary NIC)

OK Cancel



EIP	Mon.	Status	EIP Type	Bandwidth	Bandwidth Details	Associated Instance	Billing Mode	Operation
159.138.38.193		Bound	Dynamic BGP	bandwidth-c235	Bandwidth 1 Mbit/s	ecs-HK-0002 ECS	Pay per-use Created on Aug 14, 2020, 11:52:17	Bind Unbind More

Step 5 Go back to the CLI of **ecs-HK-0002** and ping **baidu.com**. You can see that **ecs-HK-0002** can now access the website.

```
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1661 ttl=45 time=7.15 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1662 ttl=45 time=7.13 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1663 ttl=45 time=7.12 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1664 ttl=45 time=7.09 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1665 ttl=45 time=7.08 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1666 ttl=45 time=7.03 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1667 ttl=45 time=7.14 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1668 ttl=45 time=7.05 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1669 ttl=45 time=7.08 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1670 ttl=45 time=7.11 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1671 ttl=45 time=7.02 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1672 ttl=45 time=7.03 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1673 ttl=45 time=7.07 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1674 ttl=45 time=7.03 ms
64 bytes from 39.156.69.79 (39.156.69.79): icmp_seq=1675 ttl=45 time=7.19 ms
```

----End

3.3.4 Traffic Distribution

Do as follows:

- Enable the HTTP service on **ecs-HK-0001** and **ecs-HK-0002**.
- Buy and configure a load balancer.
- Achieve load balancing when HTTP web pages of VMs are accessed through the load balancer.

Step 1 Remotely log in to **ecs-HK-0001** and **ecs-HK-0002**, and enable port 8889 used by the HTTP service.

- Run command `nohup python -m SimpleHTTPServer 8889 > /dev/null 2>&1 &` to enable the port.
- Run command `curl 127.0.0.1:8889` to verify that the port has been enabled.



```
[root@ecs-hk-0001 ~]# nohup python -m SimpleHTTPServer 8889 > /dev/null 2>&1 &
[1] 11654
[root@ecs-hk-0001 ~]# 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-hk-0001 ~]#

[root@ecs-hk-0002 ~]# 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-hk-0002 ~]#
```

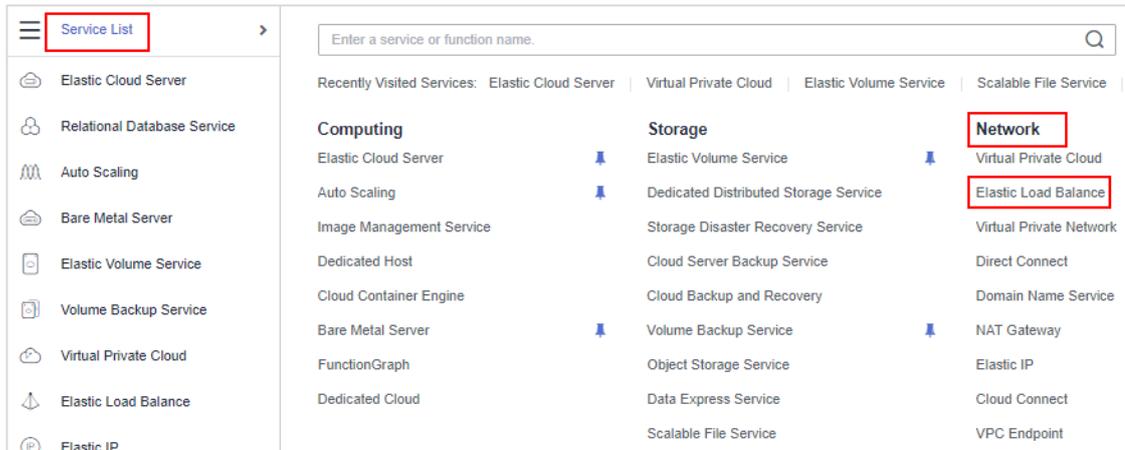
- Step 2 Run the **touch** command on **ecs-HK-0001** and **ecs-HK-0002** to create empty files named **SERVER1** and **SERVER2**, respectively. Run the **ll** command to check whether the files are created.

```
[root@ecs-hk-0001 ~]# touch SERVER1
[root@ecs-hk-0001 ~]# ll
total 0
-rw-r--r-- 1 root root 0 Aug 14 11:12 SERVER1
[root@ecs-hk-0001 ~]#

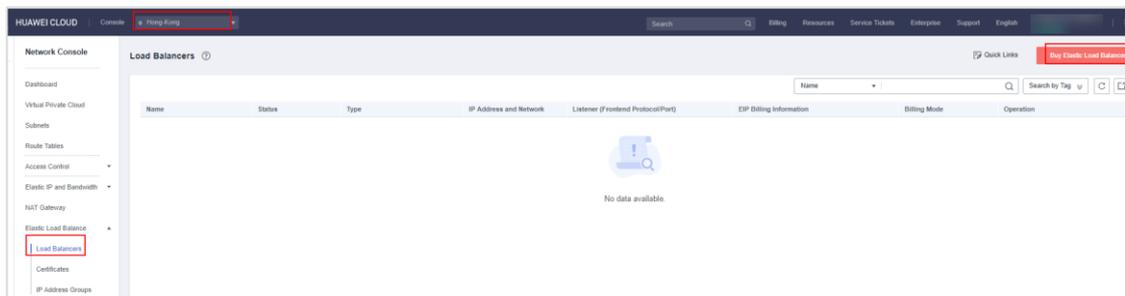
[root@ecs-hk-0002 ~]# touch SERVER2
[root@ecs-hk-0002 ~]# ll
total 0
-rw-r--r-- 1 root root 0 Aug 14 11:12 SERVER2
[root@ecs-hk-0002 ~]#
```



Step 3 Go back to the console, and choose **Service List > Network > Elastic Load Balance**.



Step 4 Click **Buy Elastic Load Balancer**.



Step 5 Set the following parameters, confirm the configuration, and click Submit.

- **Type:** Shared
- **Region:** AP-Hong Kong
- **Network Type:** Public network
- **VPC:** VPC-01
- **EIP:** New EIP
- **EIP Type:** Dynamic BGP
- **Billed By:** Bandwidth
- **Bandwidth:** 1 Mbit/s
- **Name:** for example, **elb-name**



Buy Elastic Load Balancer

Type: Shared

Region: AP-Hong-Kong

Network Type: Public network

VPC: VPC-01

Subnet: subnet-01 (192.168.0.0/24)

Private IP Address: Automatically-assigned IP ...

EIP: New EIP

EIP Type: Dynamic BGP

Billed By: Bandwidth (For heavy/stable traffic)

Bandwidth: 1

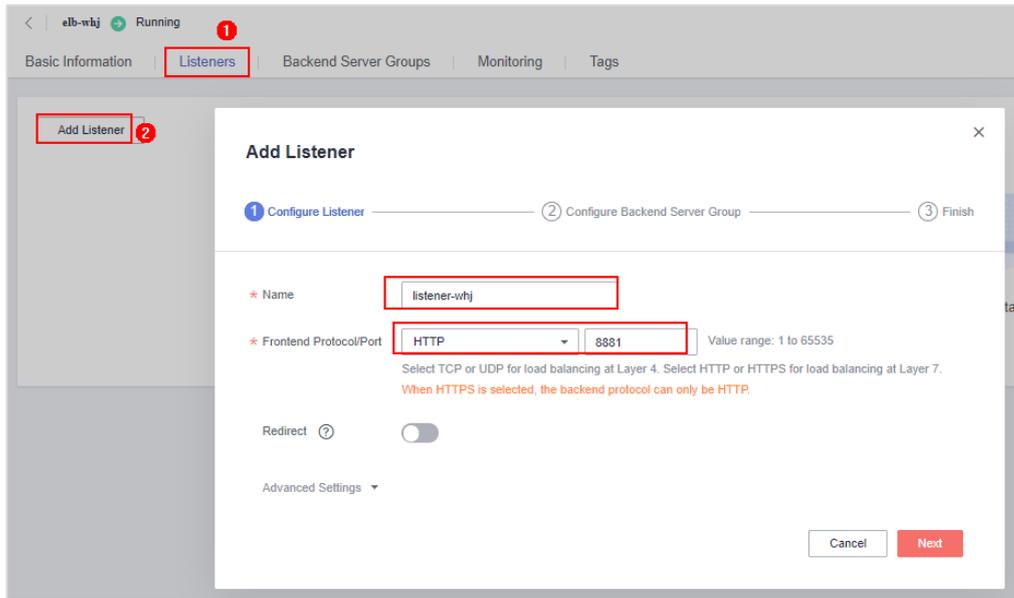
Name: elb-whj

Step 6 In the load balancer list, locate the purchase load balancer, click **Add listener**, and configure the listener.

Name	Status	Type	IP Address and Network	Listener (Frontend Protocol/Port)	EIP Billing Information	Billing Mode
elb-whj	Running	Shared	192.168.0.2 (Private IP addr... VPC-01 (VPC))	Add listener	--	--

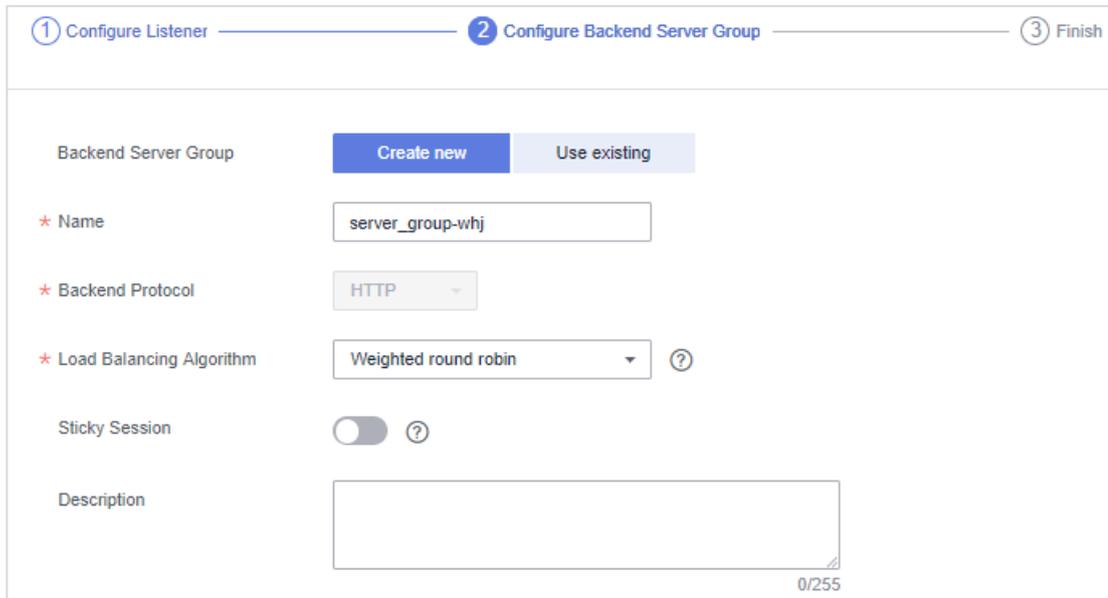
Set the following parameters to configure the listener:

- **Name:** Enter a name.
- **Frontend Protocol/Port:** HTTP/8881



Set the following parameters to configure a backend server group:

- **Backend Server Group: Create New**
- **Name:** Enter a name.
- **Load Balancing Algorithm: Weighted round robin**
- **Health check configuration:** Enable the health check function. Set **Protocol** to **HTTP** and **Port** to **8889**.





Health Check Configuration

Enable Health Check ?

* Protocol

Domain Name

Port ? Value range: 1 to 65535

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

Advanced Settings Default Custom

Step 7 Add **ecs-HK-0001** and **ecs-HK-0002** to the backend server group.

The screenshot shows the 'Add Backend Server' dialog box in the Huawei Cloud console. The dialog is titled 'Add Backend Server' and contains the following information:

- Health checks can be performed only if access from 100.125.0.0/16 is allowed in the security groups containing the servers. [Learn more](#)
- You can add 500 more backend servers. [Increase quota](#)
- Buy ECS: subnet-01 (192.168.0.0/24) | Name | Search | Clear
- Table of servers to be added:

Server	Specification	Private IP Address
<input checked="" type="checkbox"/> ecs-HK-0002	1 vCPUs 1 GB s2.small.1	192.168.0.96
<input checked="" type="checkbox"/> ecs-HK-0001	1 vCPUs 1 GB s2.small.1	192.168.0.81

Buttons:



The screenshot shows the 'Backend Server Groups' page for a server group named 'server_group-vhj'. The health check is enabled. Two ECS instances are listed:

Name	Status	Private IP Address	Health Check Result	Weight
ecs-HK-0002	Running	192.168.0.96	Unhealthy	1
ecs-HK-0001	Running	192.168.0.81	Unhealthy	1

Step 8 Check the health check result of the two ECSs. If the ECSs are detected unhealthy, troubleshoot the issue by referring to the [ELB documentation](#).

The health check result is **Unhealthy** because the security group denies communication through HTTP port 8889. Go to the VPC console, choose **Access Control > Security Groups**, click the security group name, and add an inbound rule.

The screenshot shows the 'Add Inbound Rule' dialog box. The 'Protocol & Port' section is selected, and the 'Protocol' is set to 'TCP' and the 'Port' is set to '8889'. The 'Source' is set to 'IP address' and the 'IP address' is '0.0.0.0/0'. The 'Add Rule' button is highlighted.

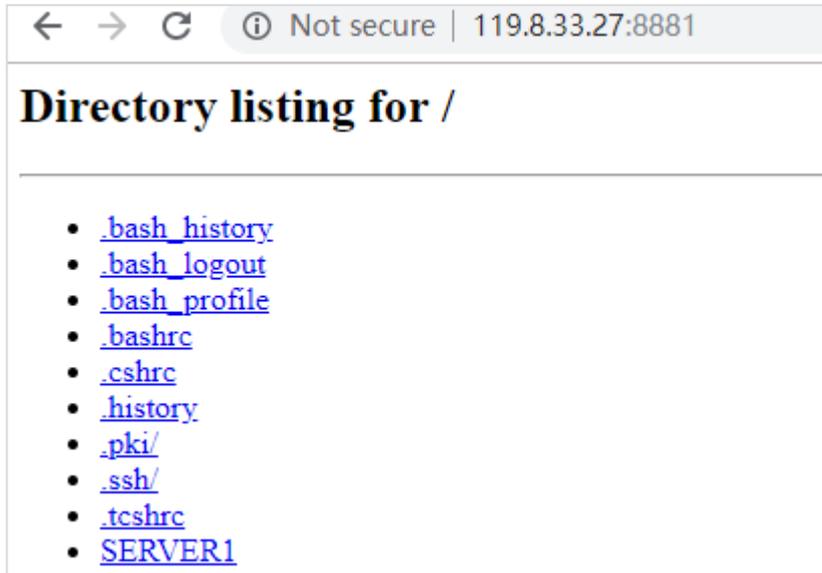
Step 9 Go back to the **Backend Server Groups** page, wait for 3 to 5 minutes, refresh the page, and check the health check result of the two ECSs. If the health check result changes to **Healthy**, the two ECSs can receive requests from the load balancer.

The screenshot shows the 'Backend Server Groups' page for the same server group. The health check is still enabled. The two ECS instances now show 'Healthy' health check results:

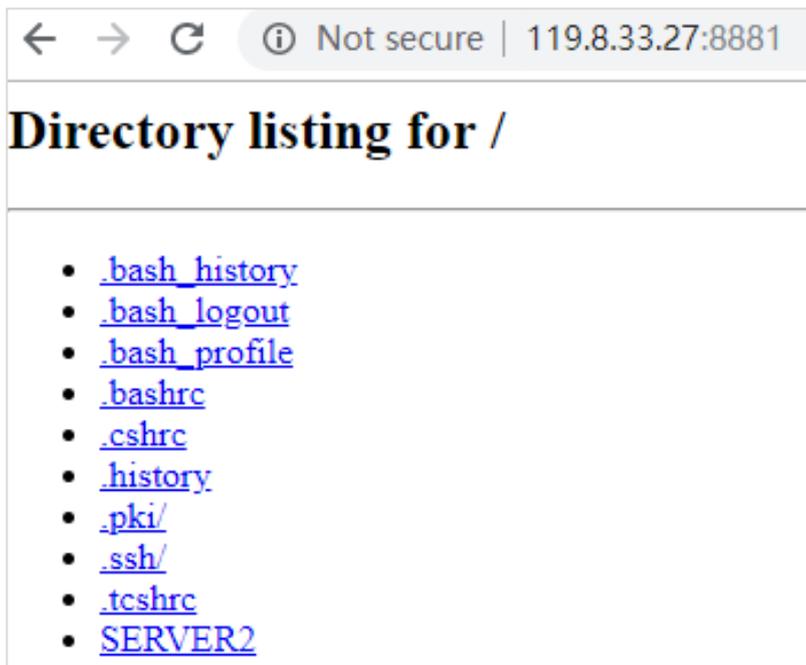
Name	Status	Private IP Address	Health Check Result	Weight
ecs-HK-0002	Running	192.168.0.96	Healthy	1
ecs-HK-0001	Running	192.168.0.81	Healthy	1



- Step 10 In the browser address box, enter **http://EIP bound to the load balancer:8881** to check whether the ECSs can be accessed. **SERVER1** in the following figure is the backend server corresponding to **ecs-hk-0001**.



- Step 11 Refresh the browser, verify that the two ECSs appear in turn.



Through this process, you can see that ELB can well distribute traffic across backend servers.

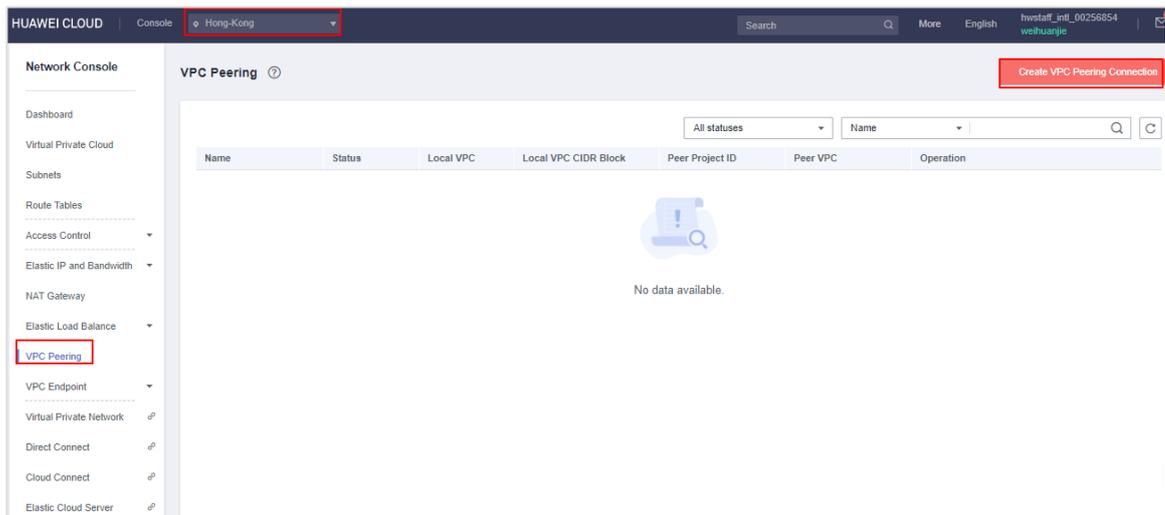
----End



3.3.5 Communication Between ECSs in Different VPCs of the Same Region

Create a VPC peering connection in AP-Hong Kong and configure VPC routes at both ends of the VPC peering connection.

- Step 1 In the navigation pane on the VPC console, choose **VPC Peering**. Click **Create VPC Peering Connection**.



- Step 2 Set the following parameters and click **OK**.

- **Name:** for example, **peering-name**
- **Local VPC:** **VPC-01**
- **Peer VPC:** **VPC-02**

Ensure that the two VPCs do not conflict with each other.



Create VPC Peering Connection

Local VPC Settings

* Name:

* Local VPC:

Local VPC CIDR Block: 192.168.0.0/16

Peer VPC Settings

* Account: My account Another account

* Peer Project:

* Peer VPC:

Peer VPC CIDR Block: 10.0.0.0/24

Step 3 In the VPC peering connection list, verify that the created VPC peering connection is in the **Accepted** state.

VPC Peering ? Create VPC Peering Connection

All statuses

Name	Status	Local VPC	Local VPC CIDR Block	Peer Project ID	Peer VPC	Operation
peering-whj	Accepted	VPC-01	192.168.0.0/16	09859dfddd0010...	VPC-02	Modify Delete

Step 4 Click the name of the VPC peering connection and view the routes. Under **Local Routes**, click **Route Tables** to add routes.

<

Name	peering-whj ↗	Status	Accepted
ID	4b6997a8-238f-4b49-83ac-8fbd1d2b791c ↗	Peer Project ID	09859dfddd00107a2ff9c00a37f0c015 ↗
Local VPC Name	VPC-01	Peer VPC Name	VPC-02
Local VPC ID	f7e9881f-a822-463c-bb32-2b435aab31f0 ↗	Peer VPC ID	80bc9ae4-f562-45ec-8e07-5d2658847a9b ↗
Local VPC CIDR Block	192.168.0.0/16	Peer VPC CIDR Block	10.0.0.0/24

Local Routes | Peer Routes

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

Destination	Next Hop Type	Next Hop	Route Table	Description
-------------	---------------	----------	-------------	-------------



Step 5 In route table **rtb-VPC-01**, click **Add Route**. Set **Destination** to the CIDR Block of **VPC-02** and **Next Hop Type** to **VPC peering connection**.

The screenshot shows the 'Add Route' dialog for route table **rtb-VPC-01**. The dialog is titled 'Add Route' and shows the route table name 'rtb-VPC-01(Default)'. The 'Destination' field is set to '10.0.0.0/24', the 'Next Hop Type' is 'VPC peering...', and the 'Next Hop' is 'peering-whj(4b6997a8-238f-4b49-83...'. There are 'OK' and 'Cancel' buttons at the bottom.

Step 6 In route table **rtb-VPC-02**, click **Add Route**. Set **Destination** to the CIDR Block of **VPC-01** and **Next Hop Type** to **VPC peering connection**.

The screenshot shows the 'Add Route' dialog for route table **rtb-VPC-02**. The dialog is titled 'Add Route' and shows the route table name 'rtb-VPC-02(Default)'. The 'Destination' field is set to '192.168.0.0/16', the 'Next Hop Type' is 'VPC peering...', and the 'Next Hop' is 'peering-whj(4b6997a8-238f-4b49-83...'. There are 'OK' and 'Cancel' buttons at the bottom.

Below the dialog, the 'Routes' section is visible, showing a table of routes:

Destination	Next Hop Type	Next Hop	Type	Description	Operation
Local	Local	Local	System	Default route that enables instance...	Modify Delete
192.168.0.0/16	VPC peering connect...	peering-whj	Custom	--	Modify Delete



Step 7 Switch to the ECS console, remotely log in to **ecs-HK-0002**, and access **ecs-HK-0003** in **VPC-02**.

If the following information is displayed, ECSs in **VPC-01** and **VPC-02** in the same region can communicate with each other after the VPC peering connection is created.

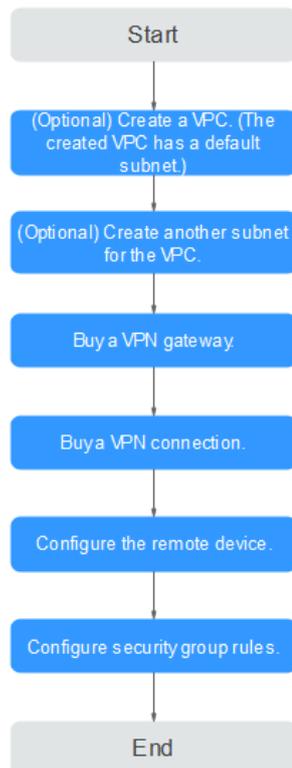
```
[root@ecs-hk-0002 ~]# ping 10.0.0.122
PING 10.0.0.122 (10.0.0.122) 56(84) bytes of data:
64 bytes from 10.0.0.122: icmp_seq=1 ttl=63 time=1.28 ms
64 bytes from 10.0.0.122: icmp_seq=2 ttl=63 time=0.455 ms
64 bytes from 10.0.0.122: icmp_seq=3 ttl=63 time=0.458 ms
64 bytes from 10.0.0.122: icmp_seq=4 ttl=63 time=0.455 ms
64 bytes from 10.0.0.122: icmp_seq=5 ttl=63 time=0.450 ms
64 bytes from 10.0.0.122: icmp_seq=6 ttl=63 time=0.446 ms
64 bytes from 10.0.0.122: icmp_seq=7 ttl=63 time=0.422 ms
64 bytes from 10.0.0.122: icmp_seq=8 ttl=63 time=0.437 ms
64 bytes from 10.0.0.122: icmp_seq=9 ttl=63 time=0.469 ms
```

----End



3.3.6 (Optional) Communication Between ECSs in Different Regions

By default, your on-premises data center or private network cannot communicate with ECSs on the cloud. To enable communication between them, you can create a VPN connection. In this example, the VPC in the CN South-Guangzhou region servers as the on-premises network.



Pay attention the following when configuring a VPN connection:

- Local and remote subnets cannot overlap.
- Different local subnets cannot overlap.
- Local and remote subnets use the same IKE and IPsec policies and PSK.
- The subnet and gateway configuration on the cloud must be the same as the subnet and gateway configuration on the on-premises network.
- The security groups containing the ECSs in the VPC that you want to access allow traffic from and to the on-premises network.
- After a VPN connection is created, its status changes to **Normal** only after the servers on both ends of the VPN connection communicate with each other.

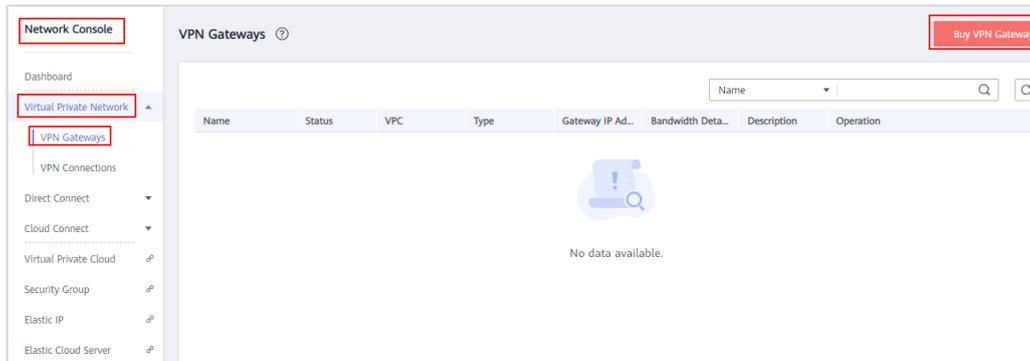
Do as follows:

- Buy a VPN gateway in AP-Hong Kong and CN South-Guangzhou, respectively.
- Configure the VPN connection.
- Modify security group rules.



- Enable communication between **ecs-HK-0001** in AP-Hong Kong and **ecs-GZ-0001** in CN South-Guangzhou.
- View the VPN connection status.

Step 1 Select the AP-Hong Kong region. On the network console, choose **Virtual Private Network > VPN Gateways**. Click **Buy VPN Gateway**.



Step 2 Set the following parameters and click **Buy Now**.

- **Billing Mode: Pay-per-use**
- **Name: vpngw-HK**
- **VPC: VPC-01**
- **Type: IPsec**
- **Billed By: Bandwidth**
- **Bandwidth: 5 Mbit/s**

★ Billing Mode **Pay-per-use**

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

★ Region **AP-Hong-Kong**

Regions are geographic areas isolated from each other. Resources are regionally isolated. For quick resource access, select the nearest region.

★ Name **vpngw-HK**

★ VPC **VPC-01** [Create VPC](#)

★ Type **IPsec**

★ Billed By **Bandwidth** Traffic

This is a one-time configuration and cannot be modified after the gateway is created.

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



Step 3 In the left navigation pane, choose **VPN Connections**. Click **Create VPN Connection**, set the parameters, and click **Buy Now**.

- **Name:** vpn-HK
- **Local Subnet:** Select the subnet of VPC-01.
- **Remote Gateway:** Enter any IP address and modify it after you have created the VPN connection in CN South-Guangzhou.
- **Remote Subnet:** Enter the subnet of VPC-03 (in CN South-Guangzhou).
- **PSK:** Enter a value.
- **Advanced Settings:** Retain their default settings.

The screenshot shows the configuration form for a VPN connection. The fields are as follows:

- Name:** vpn-HK
- VPN Gateway:** vpngw-HK
- Local Subnet:** Select subnet (selected) / Specify CIDR block. The selected subnet is subnet-01 (192.168...).
- Remote Gateway:** 1 . 2 . 2 . 1
- Remote Subnet:** 172.16.0.0/24. A note below states: "Using 100.64.0.0/10 as the customer subnet may cause services such as OBS".
- PSK:** [Redacted]
- Confirm PSK:** [Redacted]
- Advanced Settings:** Default (selected) / Custom

Step 4 Switch the region to CN South-Guangzhou, click **Buy VPN Gateway**, set the following parameters, and click **Buy Now**.

- **Billing Mode:** Pay-per-use
- **Name:** vpngw-GZ
- **VPC:** VPC-03
- **Type:** IPsec
- **Billed By:** Bandwidth
- **Bandwidth:** 5 Mbit/s



The screenshot shows a configuration form for a VPN connection. It includes the following fields and options:

- Billing Mode:** Pay-per-use
- Region:** CN South-Guangzhou
- Name:** vpngw-GZ
- VPC:** VPC-03
- Type:** IPsec
- Billed By:** Bandwidth and Traffic
- Bandwidth (Mbit/s):** 5, 10, 20, 50, 100, 200, 300

Step 5 In the left navigation pane, choose **VPN Connections**. Click **Create VPN Connection**, set the following parameters, and click **Buy Now**.

- **Name:** vpn-GZ
- **Local Subnet:** Select the subnet of VPC-03.
- **Remote Gateway:** Enter any IP address and modify it after you have created the VPN connection in CN South-Guangzhou.
- **Remote Subnet:** Enter the subnets of VPC-01.
- **PSK:** Set this to the value set for the VPN connection in AP-Hong Kong.
- **Advanced Settings:** Retain their default settings.

The screenshot shows the 'VPN Connection' configuration form with the following details:

- Name:** vpn-GZ
- VPN Gateway:** vpngw-GZ
- Local Subnet:** Select subnet (selected), Specify CIDR block
- Local Subnet:** subnet-03 (172.16...)
- Remote Gateway:** 1 . 1 . 1 . 1
- Remote Subnet:** 192.168.0.0/24
- PSK:**
- Confirm PSK:**
- Advanced Settings:** Default



Step 6 On the **VPN Connections** page, locate **vpn-GZ** and record its local gateway.

Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet
vpn-GZ	Creating	vpngw-GZ	139.159.222.123	172.16.0.0/24	1.1.1.1	192.168.0.0/24

Step 7 Switch back to the AP-Hong Kong region, locate **vpn-HK**, choose **More > Modify** in the **Operation** column, and set its remote gateway to the local gateway of **vpn-GZ**.

Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet	Operation
vpn-hk	Not connected	vpngw-hk	159.138.15.129	192.168.0.0/24	1.1.1.1	10.0.0.0/24	View Policy View Metric More

Modify VPN Connection

Basic Information

Name: vpn-hk

Local Subnet: subnet-8d43(192.16...)

Remote Gateway: 139 - 159 - 222 - 123

Remote Subnet: 172.16.0.0/24

Advanced Settings: PSK, IKE Policy, IPsec Policy

Buttons: OK, Cancel

Step 8 Record the local gateway of **vpn-HK**.

Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway
vpn-hk	Not connected	vpngw-hk	159.138.15.129	192.168.0.0/24	139.159.222.123

Step 9 Switch to the CN South-Guangzhou region, locate **vpn-GZ**, choose **More > Modify** in the **Operation** column, and set its remote gateway of to the local gateway of **vpn-HK**.



Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet	Operation
vpn-GZ	Not connected	vpngw-GZ	139.159.222.123	172.16.0.0/24	1.1.1.1	192.168.0.0/24	View Policy Modify Delete

Modify VPN Connection

Basic Information

Name: vpn-GZ Remote Gateway: 159.138.15.129

Local Subnet: subnet-03(172.16.0.0/24) Remote Subnet: 192.168.0.0/24

Advanced Settings: PSK, IKE Policy, IPsec Policy

OK Cancel

Step 10 Verify that the VPN connection status is **Not Connected**.

Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet
vpn-GZ	Not connected	vpngw-GZ	139.159.222.123	172.16.0.0/24	159.138.15.129	192.168.0.0/24

Step 11 Configure security group rules in AP-Hong Kong and CN South-Guangzhou to allow access from and to the peer end.

Add Inbound Rule

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

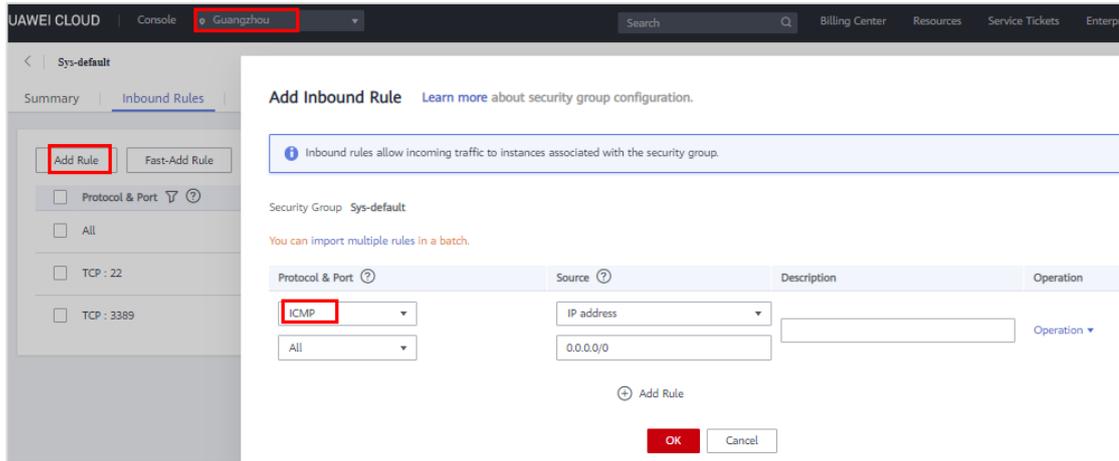
Security Group: default

You can import multiple rules in a batch.

Protocol & Port	Source	Description	Operation
ICMP	IP address		Operation
All	0.0.0.0		

Add Rule

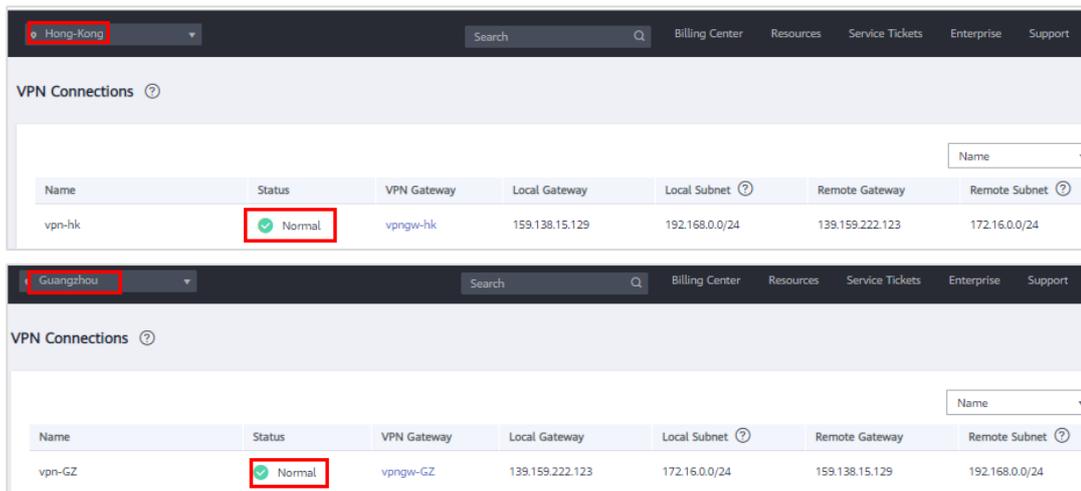
OK Cancel



Step 12 Remotely log in to **ecs-HK-0001** in **VPC-01** and ping **ecs-GZ-0001** in **VPC-03** of CN South-Guangzhou. ECSs in different regions can communicate with each other.

```
[root@ecs-hk-0001 ~]# ping 172.16.0.217
PING 172.16.0.217 (172.16.0.217) 56(84) bytes of data:
64 bytes from 172.16.0.217: icmp_seq=95 ttl=62 time=15.2 ms
64 bytes from 172.16.0.217: icmp_seq=96 ttl=62 time=14.0 ms
64 bytes from 172.16.0.217: icmp_seq=97 ttl=62 time=13.7 ms
64 bytes from 172.16.0.217: icmp_seq=98 ttl=62 time=13.9 ms
64 bytes from 172.16.0.217: icmp_seq=99 ttl=62 time=14.0 ms
64 bytes from 172.16.0.217: icmp_seq=100 ttl=62 time=13.8 ms
64 bytes from 172.16.0.217: icmp_seq=101 ttl=62 time=13.8 ms
64 bytes from 172.16.0.217: icmp_seq=102 ttl=62 time=13.7 ms
64 bytes from 172.16.0.217: icmp_seq=103 ttl=62 time=13.6 ms
64 bytes from 172.16.0.217: icmp_seq=104 ttl=62 time=13.8 ms
64 bytes from 172.16.0.217: icmp_seq=105 ttl=62 time=13.9 ms
64 bytes from 172.16.0.217: icmp_seq=106 ttl=62 time=13.9 ms
64 bytes from 172.16.0.217: icmp_seq=107 ttl=62 time=13.9 ms
64 bytes from 172.16.0.217: icmp_seq=108 ttl=62 time=14.0 ms
```

Step 13 Go to the **VPN Connections** page and check whether the statuses of the VPN connection in the two regions are normal.





Through this process, you can see that a VPN connection can be used to enable communication between the on-premises data center and the VPCs.

----End

3.4 Deleting Resources

Step 1 Delete the ECSs in the two regions.

Name/ID	AZ	Specifications/Image	IP Address	Billing Mo...	Operation
ecs-HK-0003 a5896a61-1fe8-4944-a...	AZ2	1 vCPUs 1 GB s2.sm... CentOS 7.6 64bit	10.0.0.122 (Pri...	Pay-per-use Created on Aug...	Remote Login More
ecs-HK-0002 9172c89f-5b06-4a55-8...	AZ2	1 vCPUs 1 GB s2.sm... CentOS 7.6 64bit	159.138.39.198 (...)	Pay-per-use Created on Aug...	Remote Login More
ecs-HK-0001 90e35181-aa51-40b7-...	AZ2	1 vCPUs 1 GB s2.sm... CentOS 7.6 64bit	192.168.0.81 (...)	Pay-per-use Created on Aug...	Remote Login More

Delete ECS

Are you sure you want to delete the ECSs?

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

After the ECS is deleted, it takes about 1 minute to delete associated disks. Do not perform any operation on the disks during this period. Otherwise, the disk deletion may fail. If this occurs, you will need to delete the disks on the EVS console.

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

Name	Status	Remarks
ecs-HK-0003	Running	--
ecs-HK-0002	Running	--
ecs-HK-0001	Running	--

Unreleased EIPs or data disks will continue to be billed.

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

Yes No

Step 2 Delete the load balancer in AP-Hong Kong. Remove the backend servers, delete the listener, and then delete the load balancer.

Name	Status	Private IP Address	Health Check Result	Weight	Backend Port	Operation
::	--	192.168.0.96	Deleted	1	8889	Remove
::	--	192.168.0.81	Deleted	1	8889	Remove



Load Balancers

Name	Status	Type	IP Address and Network	Listener (Fronten...	EIP Billing Inform...	Billing ...	Operation
elb-whj	Running	Shared	192.168.0.2 (Private IP addre... 119.8.33.27 (EIP) VPC-01 (VPC)	Add listener	1 Mbit/s Pay-per-use By bandwidth	--	Modify Bandwidth Delete More

Are you sure you want to delete this load balancer?

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

Name	Status	IP Address
elb-whj	Running	119.8.33.27 (EIP)

Release the EIP

Yes No

Step 3 Delete the VPC peering connection in AP-Hong Kong.

VPC Peering

Name	Status	Local VPC	Local VPC CIDR Blo...	Peer Project ID	Peer VPC	Operation
peering-whj	Accepted	VPC-01	192.168.0.0/16	09859dfddd...	VPC-02	Modify Delete

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

VPN Connections

Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet	Operation
vpn-HK	Normal	vpn-gw-HK	159.138.15.192	192.168.0.0/24	159.138.81.32	172.16.0.0/24	View Policy View Metric More

VPN Connections

Name	Status	VPN Gateway	Local Gateway	Local Subnet	Remote Gateway	Remote Subnet	Operation
vpn-GZ	Normal	vpn-gw-GZ	139.159.222.123	172.16.0.0/24	159.138.15.129	192.168.0.0/24	View Policy Modify Delete

Step 5 Delete the VPCs in the two regions. Delete the subnets in the VPCs and then delete the VPCs.

-----End



4 Management Services

4.1 Introduction

In this exercise, you will perform the following operations:

- View the CTS console and enable notification for key events.
- Use a HUAWEI CLOUD account to create an IAM user account, and use this IAM user account to buy an ECS and view logs.
- Increase the ECS CPU usage and then check whether an alarm is generated for the ECS.

4.1.1 Objectives

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

- Create an IAM user account and assign permissions to the account.
- Use CTS.
- Create an alarm rule to monitor ECSs on Cloud Eye.
- View cloud logs.

4.1.2 Process



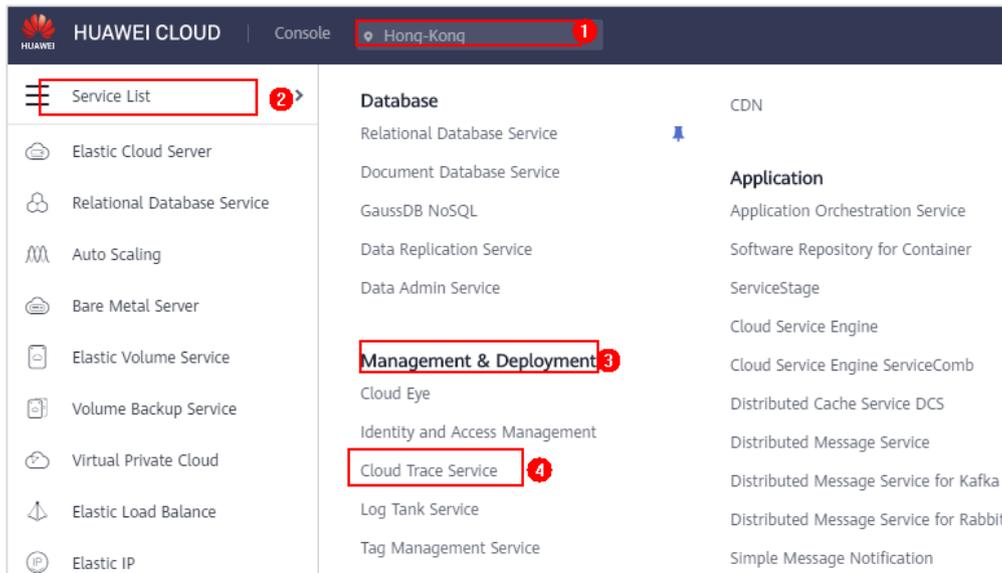


4.2 CTS

4.2.1 Enabling CTS and Viewing the Default Tracker

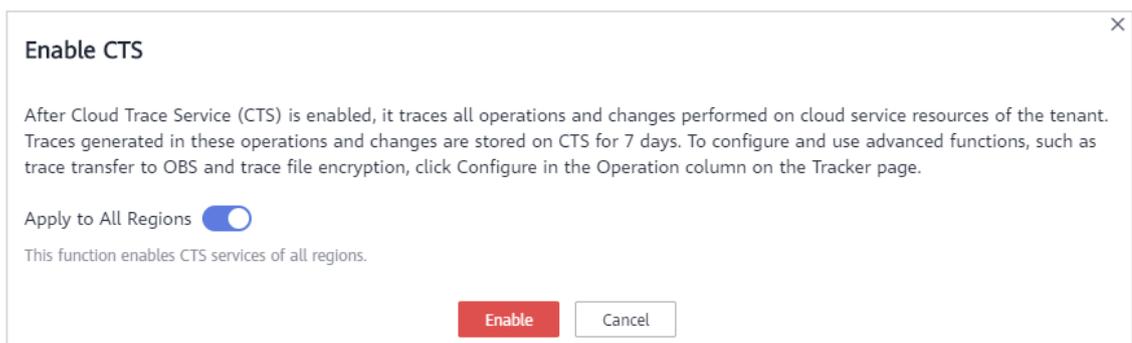
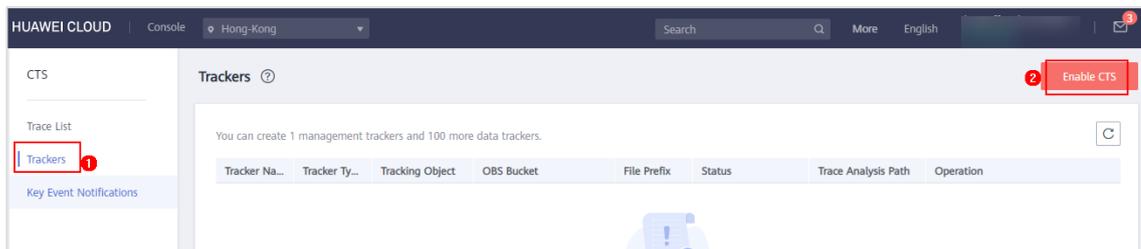
For this exercise, operations are performed in the AP-Hong Kong region.

- Step 1 Log in to the management console, select the AP-Hong Kong region, and click **Service List**. Under **Management & Deployment**, select **Cloud Trace Service**.



- Step 2 In the left navigation pane, choose **Trackers**, and click **Enable CTS** in the upper right corner. Enable **Apply to All Regions**. Click **Enable**.

A default tracker is created. The tracker will automatically identify and associate all of the cloud services that you use, and records all of your operations related to these services.





The tracker is now in the **Enabled** state.

Tracker Na...	Tracker Type	Tracking Object	OBS Bucket	File Prefix	Status	Trace Analysis Path	Operation
system	Management	--	--	--	Enabled	--	Configure Delete Disable

-----End

4.2.2 Creating a Key Event Notification

To be notified of key operations, you can configure key event notifications on CTS, and then Simple Message Notification (SMN) will send notifications when they occur. SMN can be configured to broadcast messages to email addresses, phone numbers, and HTTP/HTTPS servers.

Step 1 On the CTS console, click **Key Event Notifications**. In the left navigation pane, click **Create Key Event Notification**.

CTS

Key Event Notifications

Procedure for Using CTS ^

- 1 Create an SMN Topic
- 2 Create a Key Event Notification
- 3 A Specified Operation is Triggered
- 4 An SMN Notification is Received

You can create 100 more notifications. [Learn more](#)

Notification Name	Template Type	SMN Topic	Status	Operation
-------------------	---------------	-----------	--------	-----------

Step 2 On the displayed page, specify required parameters.

- **Notification Name:** Enter a notification name.
- **Operation Type:** Typical



Create Key Event Notification [← Back to Key Event Notification List](#)

Basic Information

Notification Name ?

Operation

SMN notifications will be sent when specified operations are performed.

Operation Type Typical All Custom

Delete Create Login

Select at least one operation. Notifications will be sent when login, create, and de

- **User Type: All users**

User

Notifications will be sent when specified users perform specified operations.

User Type All users Specified users

User List All users are selected by default.

- **Send Notification: Yes**
- **SMN Topic: Click Topic to create an SMN topic.**

Topic

Send Notification No Yes

SMN Topic ?

If no topic is available, switch to [Topic](#) and create a new one.

Step 3 On the displayed **Topics** page, click **Create Topic** in the upper right corner.

A topic is a specified event to publish messages and subscribe to notifications.

Topics ? [+ Create Topic](#)

SMN

Dashboard

Topic Management ^

- Topics
- Subscriptions
- Message Templates

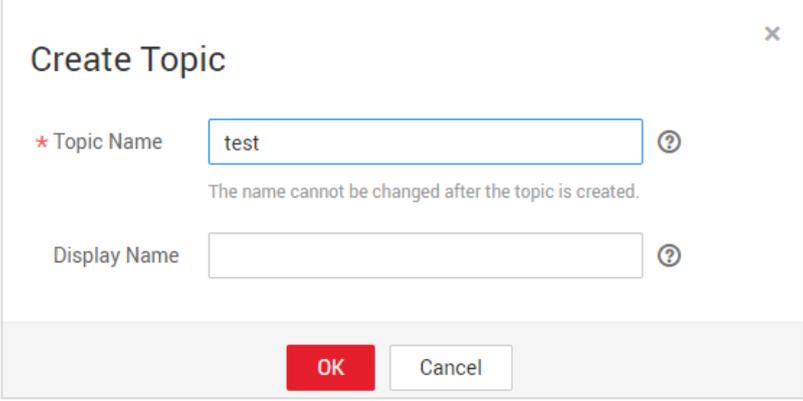
Mobile Push

Enter a name. ? ?

Name	URN ?	Display Name	Operation
No data available.			

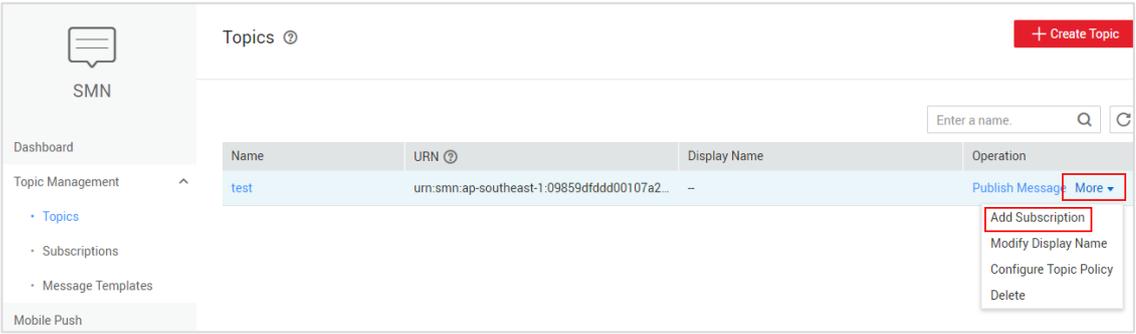


Step 4 Set the topic name and click **OK**.



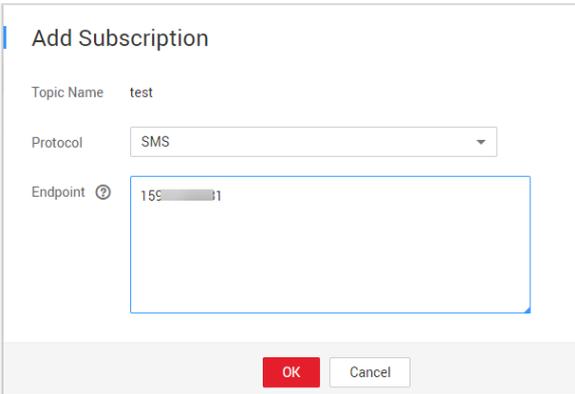
The image shows a 'Create Topic' dialog box. It has a title bar with a close button (X). The main content area contains two input fields: 'Topic Name' and 'Display Name'. The 'Topic Name' field is filled with the text 'test' and has a red asterisk to its left, indicating it is a required field. Below the 'Topic Name' field, there is a note: 'The name cannot be changed after the topic is created.' Both input fields have a help icon (question mark) to their right. At the bottom of the dialog, there are two buttons: a red 'OK' button and a white 'Cancel' button.

Step 5 To receive notifications for a specific topic, locate the topic, click **More** in the **Operation** column, and choose **Add Subscription**.



The image shows the 'Topics' management interface in the Huawei Cloud console. On the left is a navigation menu with 'SMN' selected. The main area shows a table of topics. The first row is highlighted in blue and contains the following data: Name: 'test', URN: 'urn:smn:ap-southeast-1:09859dfddd00107a2...', Display Name: '-', and Operation: 'Publish Message More'. A dropdown menu is open for the 'More' button, showing options: 'Add Subscription', 'Modify Display Name', 'Configure Topic Policy', and 'Delete'. The 'Add Subscription' option is highlighted with a red box. At the top right of the main area, there is a search bar with the placeholder text 'Enter a name.' and a '+ Create Topic' button.

Step 6 For **Protocol**, select **SMS** or **Email**. For **Endpoint**, enter your mobile number or email address. Click **OK**. The following uses **SMS** as an example.



The image shows an 'Add Subscription' dialog box. It has a title bar with a close button (X). The main content area contains three fields: 'Topic Name' (filled with 'test'), 'Protocol' (a dropdown menu with 'SMS' selected), and 'Endpoint' (a text input field with '159' entered). Below the 'Endpoint' field, there is a large empty text area. At the bottom of the dialog, there are two buttons: a red 'OK' button and a white 'Cancel' button.

Step 7 The entered mobile phone number will receive an SMS message from HUAWEI CLOUD. You can click the link to confirm the subscription.



After the confirmation, you will receive a message indicating that you have successfully subscribed to the topic.

The image shows two side-by-side screenshots. The left screenshot is an SMS message from a number starting with 1069138105. The message text is: "[HUAWEI](1/3)You are invited to subscribe to topic (urn:smn:ap-southeast-1:09859dfddd00107a2ff9c00a37f0c015:test) Click the following URL to confirm your subscription within 48 hours." Below this, a second message says: "[HUAWEI](2/3)URL is https://console-intl.huaweicloud.com/smn/c/confirm.html?id=ap-southeast-1:1:09859dfddd00107a2ff9c00a37f0c015:test". The URL is highlighted with a red box. The right screenshot is a web page from https://console-intl.huaweicloud.com/smn/c. It features the Huawei logo and a "Help Center" link. A green checkmark icon is followed by the heading "Subscription Successful". The text below reads: "You (+155...) have successfully subscribed to the following topic: test. If you do not want to subscribe to the topic, click here to cancel subscription." It then lists the "Topic URN" as urn:smn:ap-southeast-1:09859dfddd00107a2ff9c00a37f0c015:test and the "Subscription URN" as urn:smn:ap-southeast-1:09859dfddd00107a2ff9c00a37f0c015:05384c22996e726f2fc. A final note says: "Please bookmark this page so that you can unsubscribe from notifications for this topic in the future."

Step 8 Click **Publish Message** to check whether you can receive SMS messages.

The image shows a screenshot of the "Topics" management interface. At the top right, there is a red button labeled "+ Create Topic". Below this is a search bar with the placeholder text "Enter a name." and search and refresh icons. A table below the search bar lists the topics. The table has four columns: "Name", "URN", "Display Name", and "Operation". The first row in the table has the following values: "test", "urn:smn:ap-southeast-1:09859dfddd0010...", "--", and "Publish Message More". The "Publish Message" button is highlighted with a red box.

Name	URN	Display Name	Operation
test	urn:smn:ap-southeast-1:09859dfddd0010...	--	Publish Message More

Step 9 Enter a subject. Set **Message Format** to **Text** and **Message** to **hello**. Click **OK**.

If you receive an SMS message containing *hello* from HUAWEI CLOUD, you have successfully subscribed to the topic.



The 'Publish Message' dialog box shows the following configuration:

- Topic Name: test
- Subject: HUAWEI CLOUD Notice
- Message Format: Text (selected), JSON, Template
- Message: hello

Buttons: OK, Cancel

Preview: [HUAWEI]hello

Step 10 Go back to CTS console. On the **Create Key Event Notification** page, set **Topic** to the created SMN topic and click **Create Now**.

The 'Create Key Event Notification' page shows the following configuration:

- Operation Type: Typical, All, Custom
- Selected Operations: Delete, Create, Login
- User Type: All users, Specified users
- Send Notification: No, Yes
- SMN Topic: test

Buttons: Create Now

If the key event notification status is **Enabled**, the key event notification was successfully created.

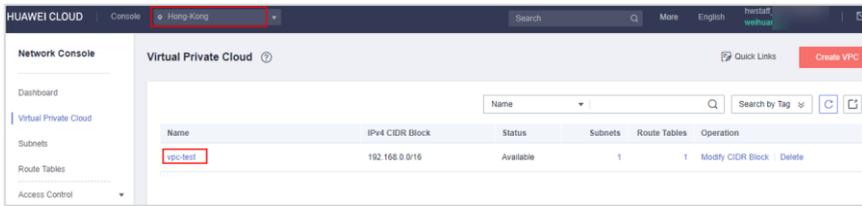
Notification Name	Template Type	SMN Topic	Status	Operation
keyOperate_info_whj	Typical	urn:smn:ap-southeast-1:09859dfddd00107a2ff9c00a37f0c015:test	Enabled	View Disable More

----End

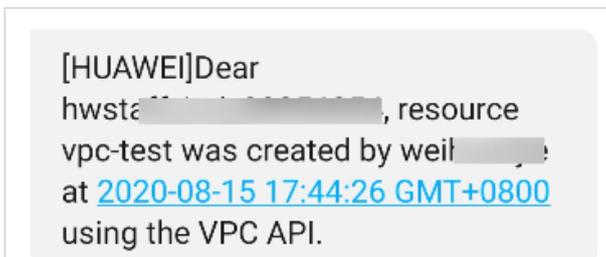


4.2.3 Viewing VPC Creation Records

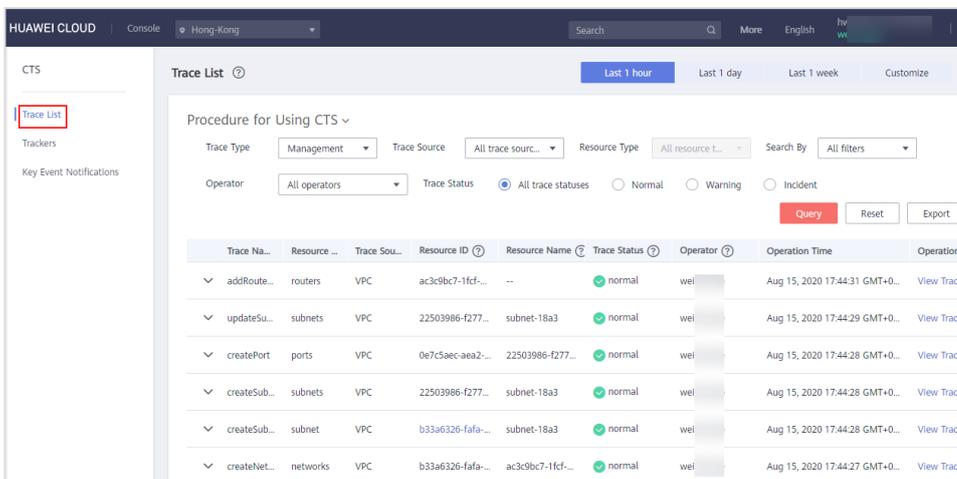
Step 1 Create a VPC in the AP-Hong Kong region by referring to section 3.2.1.



Step 2 Check whether you receive an SMS message from HUAWEI CLOUD indicating that the VPC has been created.



Step 3 Go back to CTS console and choose **Trace List**. In the trace list, view the VPC operation time and trace status.



----End



4.3 Creating an IAM User Account and Performing Related Operations

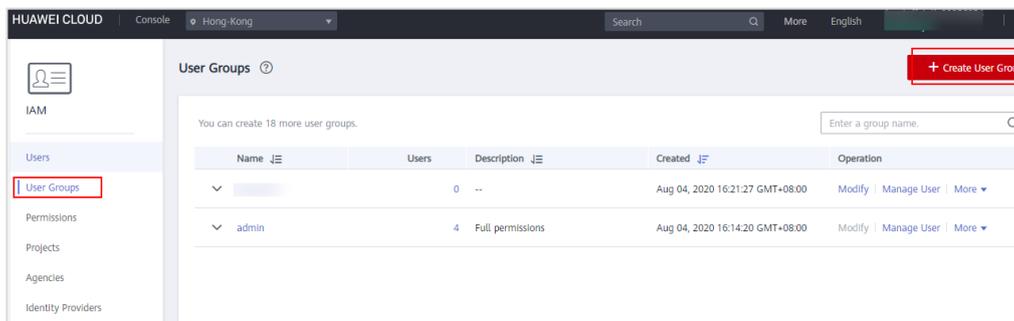
4.3.1 Creating an IAM Account and Assigning Permissions

IAM provides identity authentication and permissions management. With IAM, you can create users for employees, applications, or systems in your organization, and control the users' access to specified resources in your account.

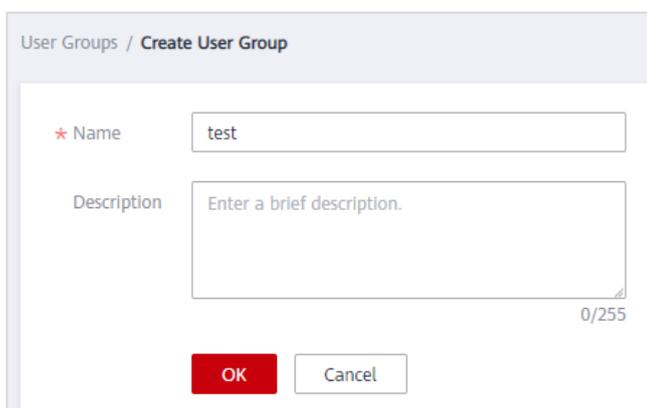
- Step 1 On the management console, under the username, click **Identity and Access Management**.



- Step 2 In the left navigation pane, choose **User Groups**, and click **Create User Group**. (A user group is a collection of users, and every user belonging to a user group has the permissions assigned to the user group.)



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





Step 4 Locate the created user group, in the **Operation** column, click **More**, and choose **Manage Permissions** to assign permissions to the user group.

Name	Users	Description	Created	Operation
test	0	--	Aug 15, 2020 18:29:38 GMT+08:00	Modify Manage User More
admin	4	Full permissions	Aug 04, 2020 16:14:20 GMT+08:00	Modify Manage Permissions Delete

Step 5 Click **Assign Permissions**.

Name: test | Group ID: 09a22ee8c2002563f47c00a5f452554

Description: -- | Created: Aug 15, 2020 18:29:38 GMT+08:00

Permissions | Users

Assign Permissions | Policy View | Project View

All policies/roles | All services | Enter a policy name, role name, or description

Policy/Role Name	Type	Description	Project [Region]	Operation
No data available.				

Step 6 For **Scope**, select **Region-specific projects**, select **AP-Hong Kong**. In the **Permissions** area, search for **IAM**, select **Tenant Guest** and **Tenant Administrator**, and click **OK**.

Scope

Global service project
Permissions for services, such as OBS, CDN, and TMS, can be assigned based on the global service project.

Region-specific projects
Permissions for services, such as ECS and DCS, can be assigned based on region-specific projects.

ap-southeast-1 [AP-Hong Kong]

Permissions

- cn-east-3 [CN East-Shanghai1]
- cn-south-1 [CN South-Guangzhou]
- ap-southeast-1 [AP-Hong Kong]**
- ap-southeast-2 [AP-Bangkok]
- ap-southeast-3 [AP-Singapore]
- af-south-1 [AF-Johannesburg]
- na-mexico-1 [LA-Mexico City1]
- sa-brazil-1 [LA-Sao Paulo1]
- la-south-2 [LA-Santiago]



The image shows two screenshots from the Huawei Cloud IAM console. The top screenshot is titled "Assign Permissions to test" and shows the "Region-based Authorization" section. Under "Scope", "Region-specific projects" is selected with the region "ap-southeast-1 [AP-Hong Kong]". Under "Permissions", a table lists several roles, with "Tenant Administrator" selected and highlighted by a red box. The bottom screenshot is titled "User Groups / test" and shows the "Permissions" tab for the "test" group. It displays a table of assigned permissions, including "Tenant Guest" and "Tenant Administrator", both of which are highlighted by red boxes.

Step 7 In the left navigation pane, choose **Users**, and click **Create User**.

The image shows the "Users" management page in the IAM console. The "Users" menu item in the left navigation pane is highlighted with a red box. In the top right corner, the "Create User" button is also highlighted with a red box. The main area displays a table of existing users with columns for Username, Description, Status, Last Login, Created, and Operation. The "Enterprise administrator" user is highlighted with a red box.

Step 8 Set the following parameters.

- **Username:** Set a username, for example, **test123**.
- **Credential Type:** Password
- **User Groups:** Select a created user group, for example, **test**.



Users / Create User

* Username: test123

* Credential Type: Password
 Access key

User Group	Description	Operation
test	--	Remove

Description: Enter a brief description. 0/255

Next Cancel

- **Password Type: Set now**
- **Password Reset: Deselect it.**
- **Password: Enter a password, for example, Huawei@123.**

* Password Type: Set now
 Set by user
 Automatically generated

Password Reset: Require user to set a new password upon first login

Email Address: [Empty]

Mobile Number: +852 (Hong Kong SAR, China)

* Password: [Masked]

* Confirm Password: [Masked]

Previous OK Cancel

If the following page is displayed, the account was successfully created.

Users + Create User

IAM User Login Link https://auth-intl.huaweicloud.com/authui/login?id=hwstaff_intl_00256854

You can create 45 more users.

Username	Description	Status	Last Login	Created	Operation
test123	--	Enabled		Aug 15, 2020 18:53:13 GMT+08:00	Set Credentials Delete Modify

-----End



4.3.2 Buying an ECS Using the IAM User Account

Step 1 Log out of the current account and log in again using the IAM user account.

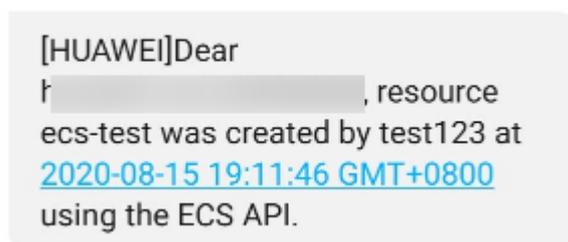
The image shows two side-by-side screenshots of the Huawei Cloud login interface. The left screenshot is titled 'Account Login' and features fields for 'Account name or email' and 'Password', along with a 'Remember me' checkbox and a 'Log In' button. Below the 'Log In' button are links for 'Free Registration', 'Forgot Password', 'IAM User Login' (highlighted with a red box), and 'HUAWEI ID Login'. The right screenshot is titled 'IAM User Login' and shows the same fields, but the password field contains 'test123' (highlighted with a red box) and the 'Log In' button is visible below.

Step 2 In the AP-Hong Kong region, create a Linux ECS named **ecs-test** by referring to section 1.1.4.

The screenshot shows the 'Elastic Cloud Server' page in the Huawei Cloud console. The page displays a table with the following data:

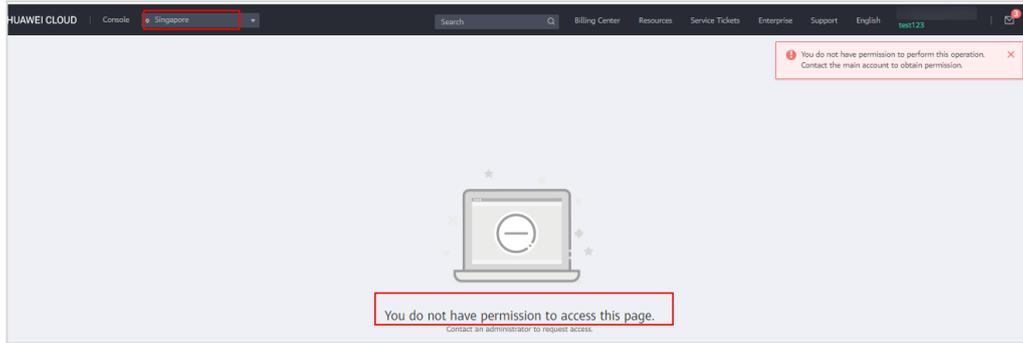
Name/ID	AZ	Status	Specifications/Image	IP Address	Billing Mode	Operation
ecs-test 6656d494-d458-42c1-9702-3c8f1bde...	AZ1	Running	2 vCPUs 4 GB c3.large.2 CentOS 7.4 64bit	192.168.0.157 (Private IP)	Pay-per-use Created on Aug 15, 2020...	Remote Login More

Step 3 After the ECS is created, check whether you have received an SMS message from HUAWEI CLOUD, indicating that the ECS creation operator is **test123**.

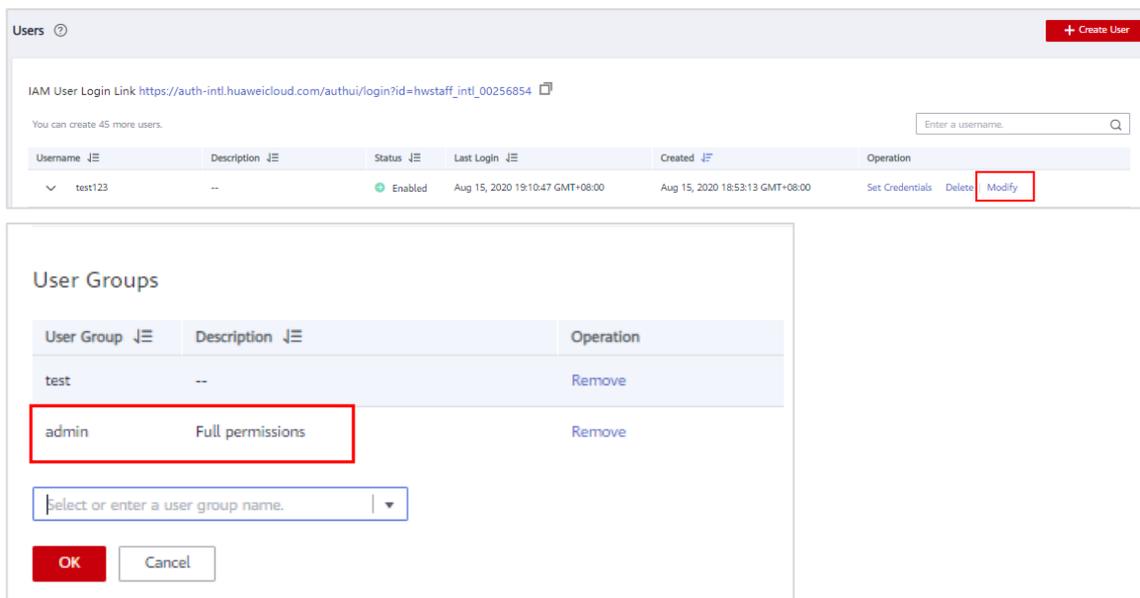


Step 4 Switch to another region and view the ECS list.

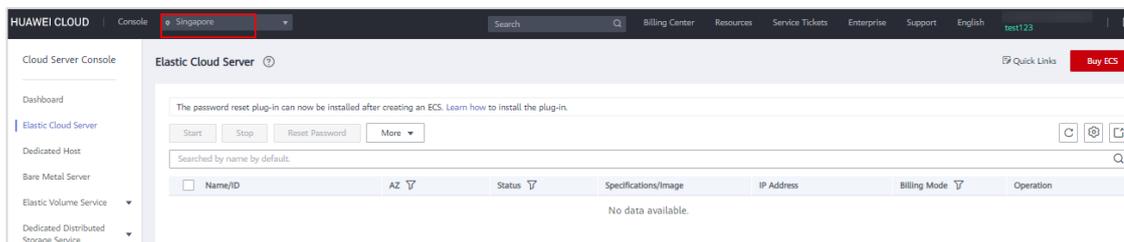
If the system displays a message saying "You do not have permission to access this page. Contact an administrator to request access", this account only has permissions in the AP-Hong Kong region.



Step 5 Switch to the HUAWEI Cloud account and add **test123** to the **admin** user group.



Step 6 Log in to the IAM console as user **test123**. Switch to another region, check whether you can access all of the ECSs.



----End

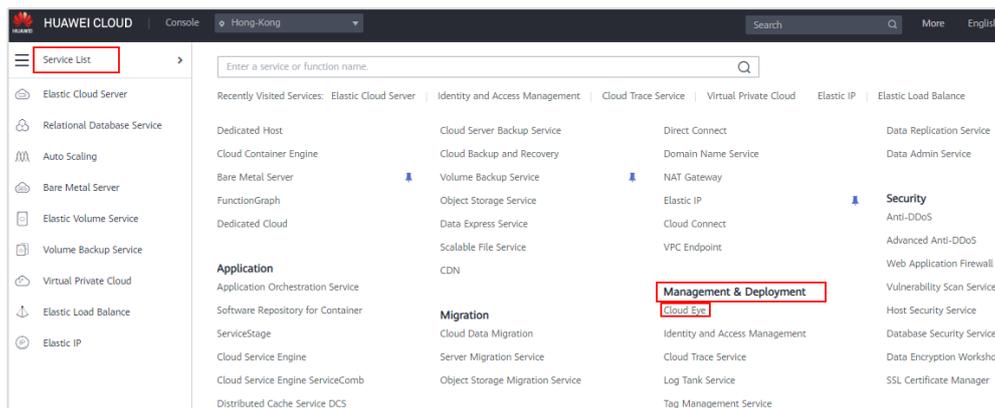


4.4 Cloud Eye

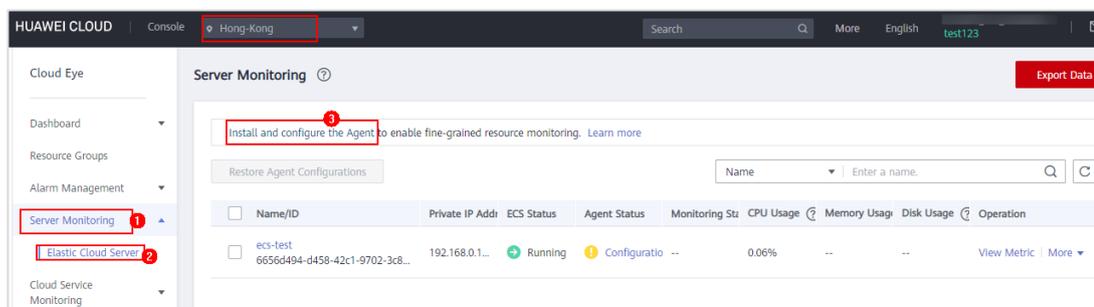
4.4.1 Monitoring an ECS

Cloud Eye is a multi-dimensional resource monitoring platform. In Cloud Eye, server monitoring performs basic monitoring, OS monitoring, and process monitoring for servers.

- Step 1 Log in to the management console as user **test123**, switch to the AP-Hong Kong region. Click **Service List**, and under **Management & Deployment**, select **Cloud Eye**.



- Step 2 In the left navigation pane, choose **Server Monitoring**, and click **Install and configure the Agent**.



- Step 3 On **Agent Installation and Configuration** page, install the Agent based on the ECS OS type.



Agent Installation and Configuration

Agent Installation

Linux OS (x86_64) | Linux OS (arm64) | Windows OS (64 bit)

OpenSUSE: 13.2, 42.2
Ubuntu: 14.04 server, 16.04 server
Fedora: 24, 25
Gentoo Linux: 13.0, 17.0

Debian: 7.5.0, 8.2.0, 8.8.0, 9.0.0
EulerOS: 2.2
Oracle Linux: 6.9, 7.4

CentOS: 6.3, 6.5, 6.8, 6.9, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
SUSE: Enterprise11 SP4, Enterprise12 SP1, Enterprise12 S...
CoreOS: 10.10.5

Mode 1: Normal Installation

* Before the installation, ensure that you have changed the DNS server address and added security group rules

1. Log in to an Elastic Cloud Server as user root.
2. Run the following command to install the Agent:

```
cd /usr/local && wget https://telescope-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/scripts/agentInstall.sh && chmod 755 agentInstall.sh && ./agentInstall.sh
```

Mode 2: Batch Installation (Recommended)

1. Perform the steps under mode 1 to install the Agent on a single Elastic Cloud Server. Use PuTTY to log in to the Elastic Cloud Server as user root.
2. Run the following command on the first Elastic Cloud Server to install the Python package:

```
cd /usr/local && wget https://telescope-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/scripts/agentBatchPackage.sh && chmod 755 agentBatchPackage.sh && ./agentBatchPackage.sh
```

3. Create iplist.txt in directory /user/local. Copy the private IP addresses of the target ECSs to iplist.txt, and ensure that each IP address is on a separate line.
4. Run the following command to install the Agent in batches:

```
cd /usr/local && ./batchInstall.sh spassword
```

Go back to ECS console and locate the Linux **ecs-test** created in section 4.3.2. This ECS is running Linux OS (x86_64), so **Mode 1** is used to install the Agent.

Step 4 Click **Remote Login** to log in to **ecs-test**.

Elastic Cloud Server

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

Start Stop Reset Password More

Searched by name by default.

Name/ID	AZ	Status	Specifications/Image	IP Address	Billing Mo...	Operation
ecs-test 6656d494-d458-42c1-...	AZ1	Running	2 vCPUs 4 GB c3.lar... CentOS 7.4 64bit	119.8.33.27 (El... 192.168.0.157 ...	Pay-per-use Created on Aug...	Remote Login

Step 5 Run the following command to install the Agent on **ecs-test**:

```
cd /usr/local && wget https://telescope-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/scripts/agentInstall.sh && chmod 755 agentInstall.sh && ./agentInstall.sh
```

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.12.1.el7.x86_64 on an x86_64

ecs-test login: root
Password:

Welcome to Huawei Cloud Service

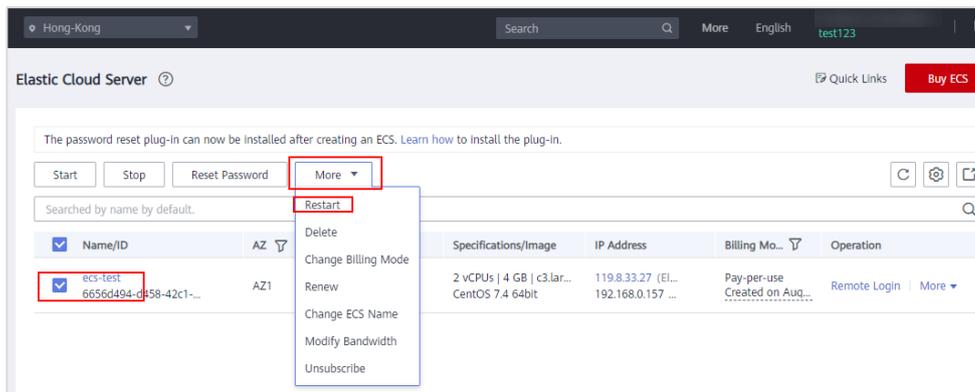
[root@ecs-test ~]# cd /usr/local && wget https://telescope-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/scripts/agentInstall.sh && chmod 755 agentInstall.sh && ./agentInstall.sh
```

Step 6 Press **Enter**.

If the following information is displayed, the Agent has been installed.

```
/bin/curl
ces flag NOT 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.
Starting telescope...
Telescope process starts successfully.
[root@ecs-test local]#
```

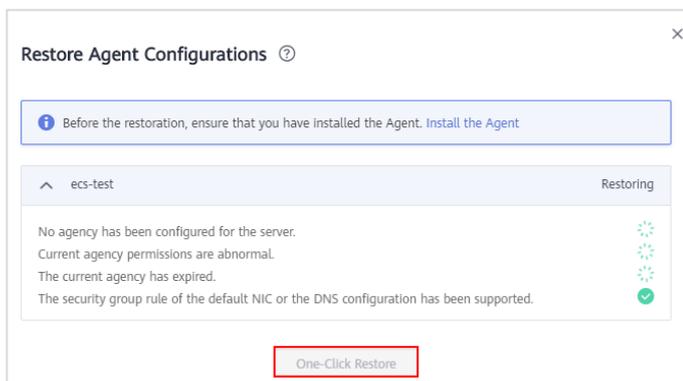
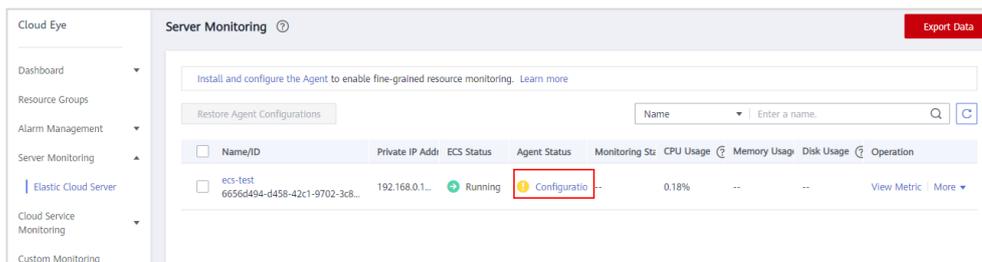
Step 7 Go back to ECS list, locate **ecs-test**, click **More** in the **Operation** column, and click **Restart**.



Step 8 After **ecs-test** is restarted, go back to the Cloud Eye **Server Monitoring** page and refresh the page.

The **Agent Status** will be **Configuration error**. Click **Configuration error**.

On the displayed **Restore Agent Configurations** dialog box, click **One-Click Restore**.





Restore Agent Configurations ?

Before the restoration, ensure that you have installed the Agent. [Install the Agent](#)

ecs-test Restoration Successful

- An agency has been configured for the server. ✓
- Current agency permissions are normal. ✓
- The current agency is within the validity period. ✓
- The security group rule of the default NIC or the DNS configuration has been supported. ✓

Restoration Completed

Step 9 Wait for 3 to 5 minutes.

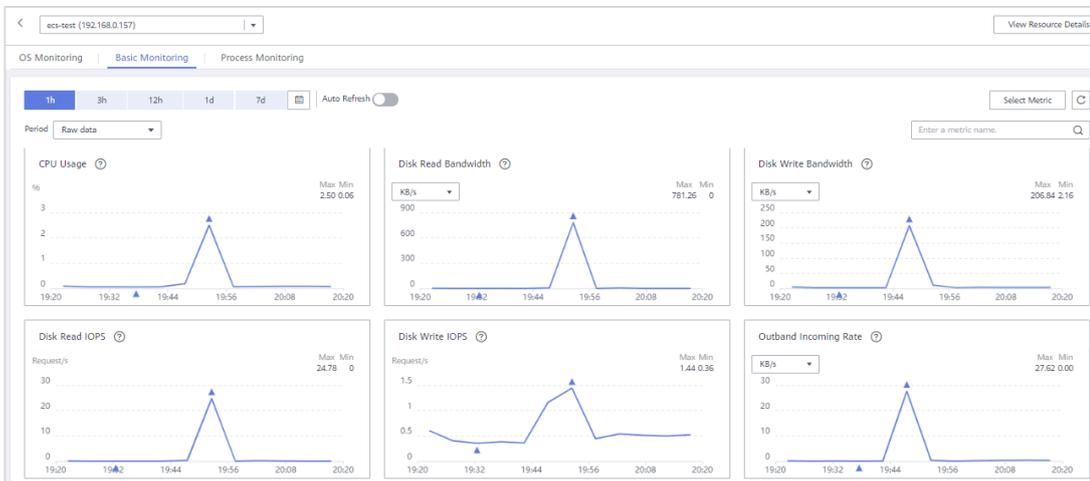
If the **Agent Status** changes to **Running** and **Monitoring Status** is enabled, the ECS is being monitored. Click **View Metric**.

Server Monitoring ?

Install and configure the Agent to enable fine-grained resource monitoring. [Learn more](#)

Name/ID	Private IP Address	ECS Status	Agent Status	Monitoring Status	CPU Usage ?	Memory Usage ?	Disk Usage ?	Operation
ecs-test 6656d494-d458-42c1-9702-3c8f1bdea7c4	192.168.0.157	Running	Running	On	0.05%	10.77%	5.23%	View Metric

On the displayed page, you can view the ECS status.



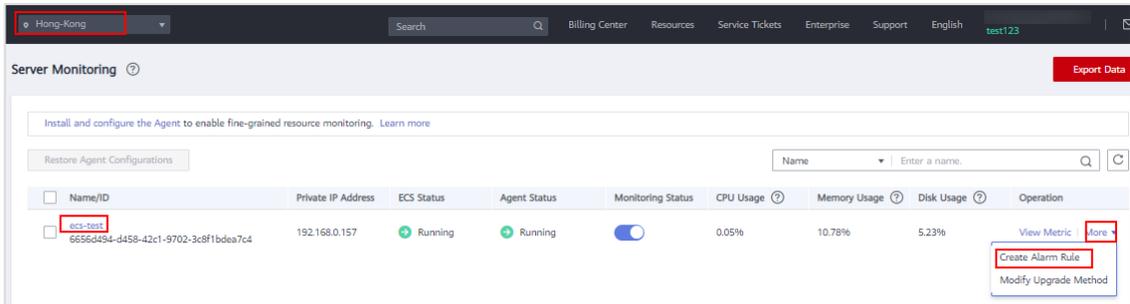
----End

4.4.2 Creating an Alarm Rule

You can flexibly configure alarm rules and notifications on Cloud Eye to learn about the resource running status and performance in a timely manner and to prevent potential service losses.



- Step 1 On the **Server Monitoring** page, locate **ces-test** in the ECS list. In the **Operation** column, choose **More > Create Alarm Rule**.



- Step 2 Set the following parameters:

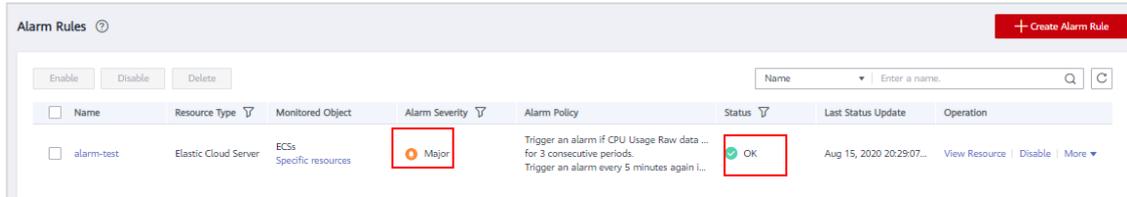
- **Name:** The system generates a name randomly but you can change it.
- **Method:** Create manually
- **Alarm Policy:** (Agent) CPU Usage (recommended), Raw data, 3 consecutive periods, \geq , 0.5, Every 5 minutes. In this exercise, set a small threshold to receive the alarm notifications as soon as possible.
- **Alarm Severity:** Major

The screenshot shows the 'Create Alarm Rule' configuration page. It has a dark blue header with a back arrow and the title 'Create Alarm Rule'. The form contains several sections:

- Name:** A text input field containing 'alarm-test'.
- Description:** A large text area, currently empty, with a character count '0/256'.
- Resource Type:** 'Elastic Cloud Server'
- Dimension:** 'ECS'
- Monitoring Scope:** 'Specific resources'
- Monitored Object:** 'ecs-test'
- Method:** Two buttons: 'Use template' and 'Create manually' (highlighted with a red box).
- Alarm Policy:** A row of dropdown menus and inputs: 'CPU Usage', 'Raw data', '3 consecutiv...', '>=', a percentage input field, and 'Every 5 minutes'.
- Alarm Severity:** Four radio buttons: 'Critical', 'Major' (selected), 'Minor', and 'Informational'.
- Alarm Notification:** A toggle switch, currently turned off.

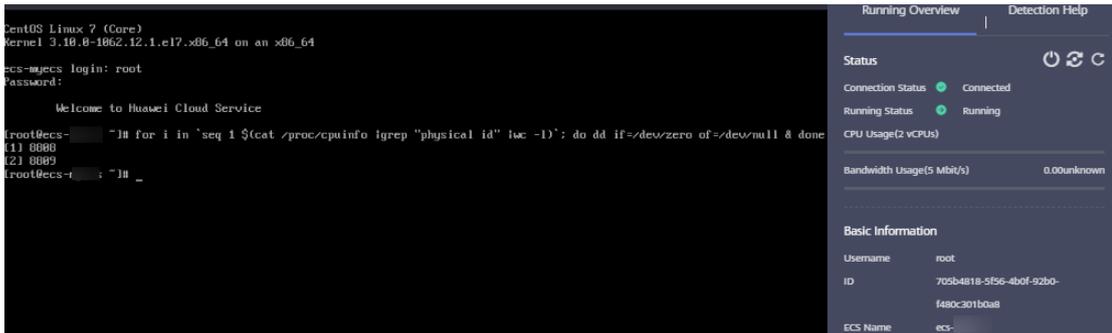
- Step 3 Go to the **Alarm Rules** page.

If the alarm rule is displayed in the alarm rule list, the alarm rule has been created.



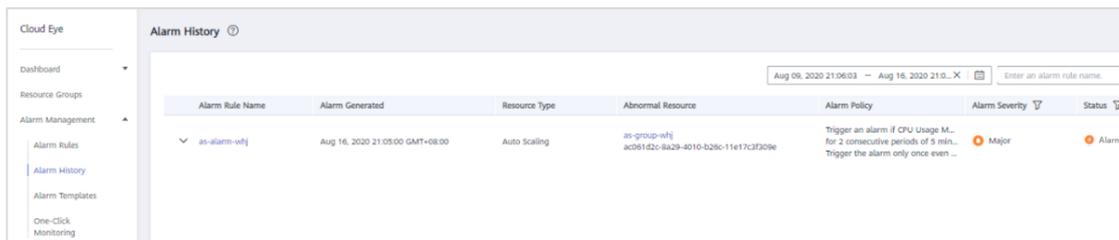
Step 4 Go back to ECS console, locate **ecs-linux**, and click **Remote Login**. Run the following command to increase the ECS CPU usage:

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



Wait for 5 to 10 minutes, then you can see the CPU increase.

Step 5 Refresh the **Alarm History** page to view the alarm rule status.



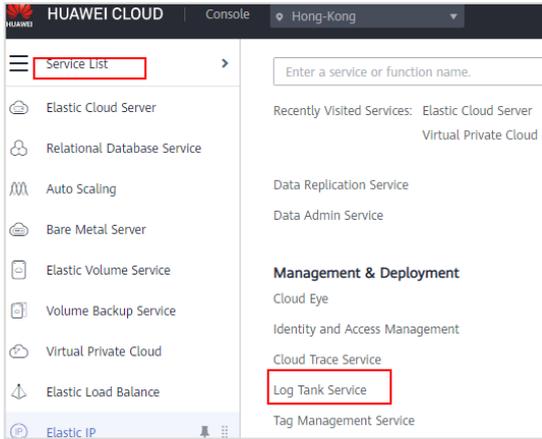
----End

4.5 LTS

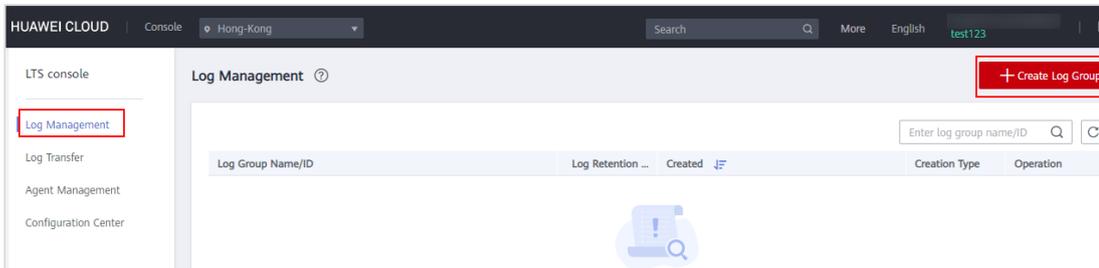
4.5.1 Creating Log Groups and Log Streams

A log group is a basic unit for managing logs. A log stream is a basic unit for reading and writing logs. Therefore, you must create a log group and a log stream before using LTS.

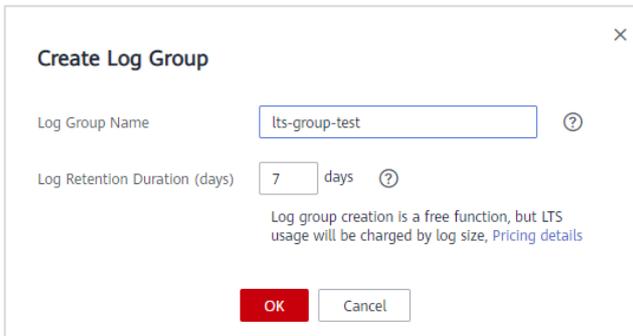
Step 1 Log in to the management console as user **test123**. Click **Service List**. Under **Management & Deployment**, select **Log Tank Service**.



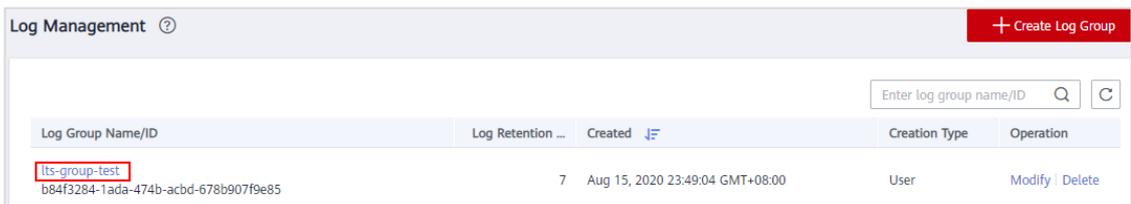
Step 2 In the left navigation pane, choose **Log Management**. In the upper right corner, click **Create Log Group**.



Step 3 Set **Log Group Name** and **Log Retention Duration (days)**, and click **OK**.

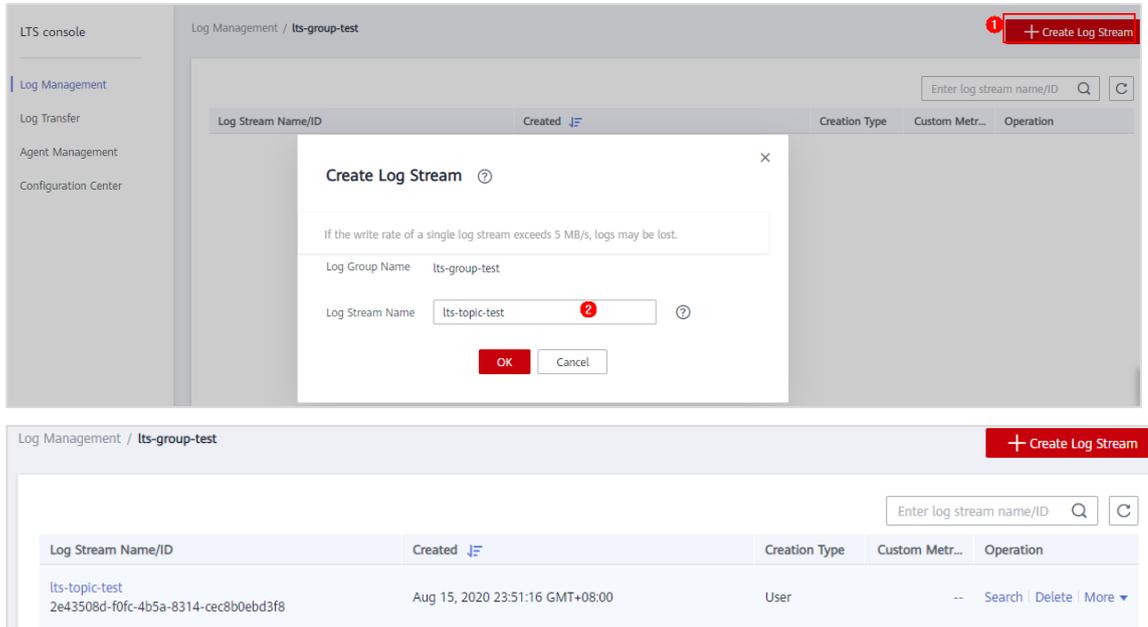


Step 4 On the **Log Management** page, click the name of the created log group.





Step 5 In the upper right corner, click **Create Log Stream**, enter the log stream name, and click **OK**.

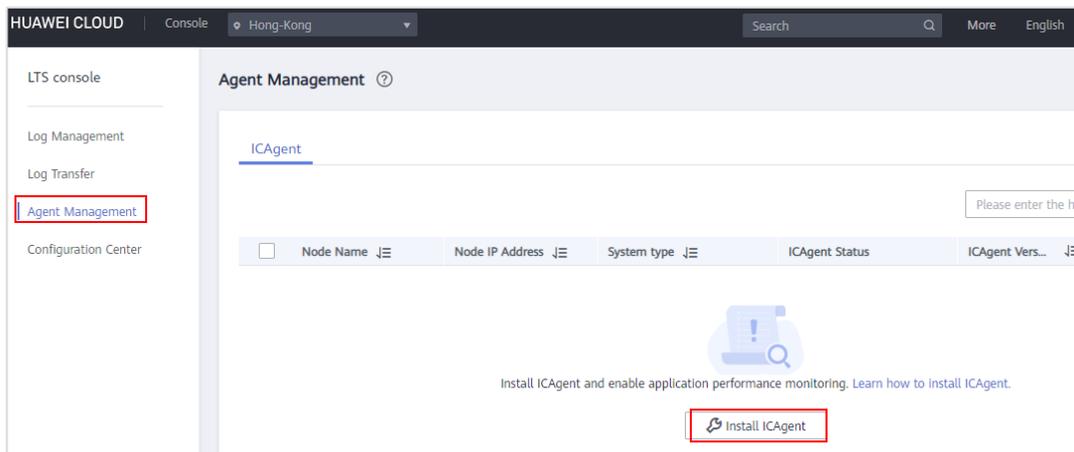


----End

4.5.2 Installing the ICAgent

ICAgent is a tool used by LTS to collect logs. It runs on servers where logs are collected.

Step 1 In the left navigation pane, choose **Agent Management**, and click **Install ICAgent**.



Step 2 Set the following parameters.

- **OS:** Linux
- **Installation Mode:** Obtain AK/SK
- **AK/SK:** Enter the AK/SK.



Install ICAgent

OS: Linux Windows

Installation Mode: Obtain AK/SK Create an Agency

You can install ICAgent in two ways. If you have a one-click installation for multiple hosts, please refer to [Inherited Batch Installation](#).

Step 1: Enter the AK/SK to generate the installation command. [How to Obtain an AK/SK?](#)

AK:

SK:

Step 2: Copy the ICAgent installation command.

Command Generated ✔ [Copy Command](#)

```
curl http://icagent-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/ICAgent_linux/apm_agent_install.sh >
apm_agent_install.sh && REGION=ap-southeast-1 bash apm_agent_install.sh -ak 4E06IZ3ROKN7D0IQIEXH -sk
cZI3V43yErL2SYuucCSmRDOxezlsL8LA5YRWefds -region ap-southeast-1 -projectid 09859dfddd00107a2ff9c00a37f0c015
-accessip 100.125.6.104 -obsdomain obs.ap-southeast-1.myhuaweicloud.com;
```

Step 3: Use a remote login tool (such as PuTTY) to log in to the node as the root user and run the copied command. If the message "ICAgent install success" is displayed, the installation is successful. After the installation is successful, choose Agent Management from the left navigation pane to view the ICAgent status.

If installation fails, uninstall ICAgent by referring to [Uninstalling ICAgent](#), and then install ICAgent again. If the installation fails

Step 3 Copy the ICAgent installation command and run it on **ecs-test**.

If the following information is displayed, the installation was successful.

```

[root@ecs-test ~]# curl http://icagent-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/ICAgent_linux/apm_agent_install.sh >
apm_agent_install.sh && REGION=ap-southeast-1 bash apm_agent_install.sh -ak 4E06IZ3ROKN7D0IQIEXH -sk cZI3V43yErL2SYuucCSmRDOxezlsL8LA5YRWefds -region ap-southeast-1 -projectid 09859dfddd00107a2ff9c00a37f0c015 -accessip 100.125.6.104 -obsdomain obs.ap-southeast-1.myhuaweicloud.com;
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 7851 100 7851 0 0 127k 0 --:--:-- --:--:-- --:--:-- 129k
start to install ICAgent.
begin to download install package from icagent-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com.
##### 100.0%
download success.
start install package.
start install ICAgent...
##### 100.0%
no crontab for root
starting ICAgent...
[CAgent install success.]
[root@ecs-test ~]#

```

Step 4 Refresh the ICAgent page.

When the ICAgent status changes to **Running**, the ICAgent has been installed.

Agent Management ?

[ICAgent](#)

Install ICAgent
Upgrade ICAgent
Uninstall ICAgent
Please enter the host name or host IP Q C

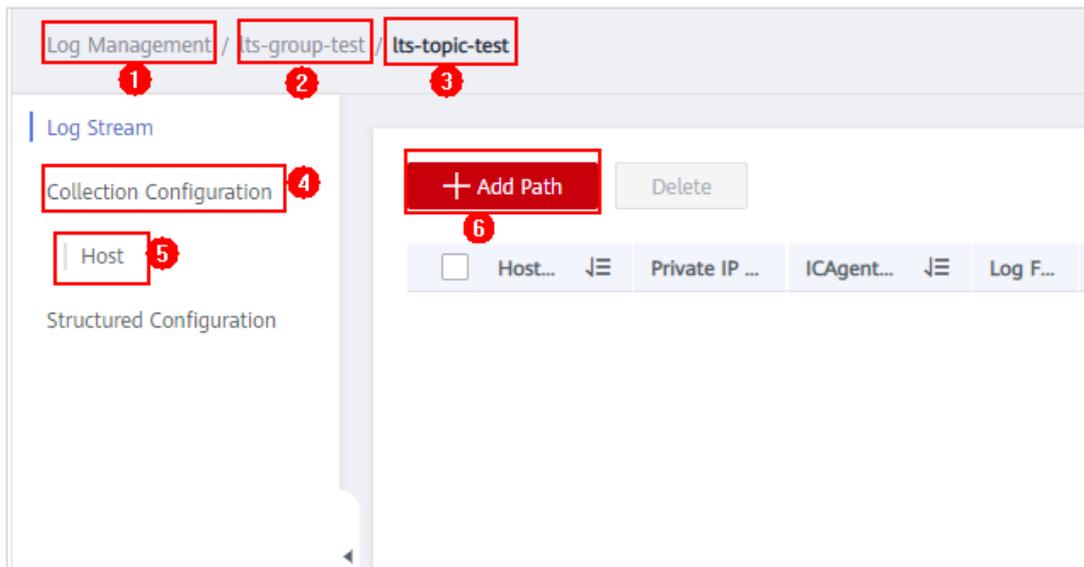
	Node Name	Node IP Address	System type	ICAgent Status	ICAgent Vers...	Updated At
<input type="checkbox"/>	ecs-test	192.168.0.157	Linux	✔ Running	5.12.57	2020/8/16 00:02:37 GMT+0...



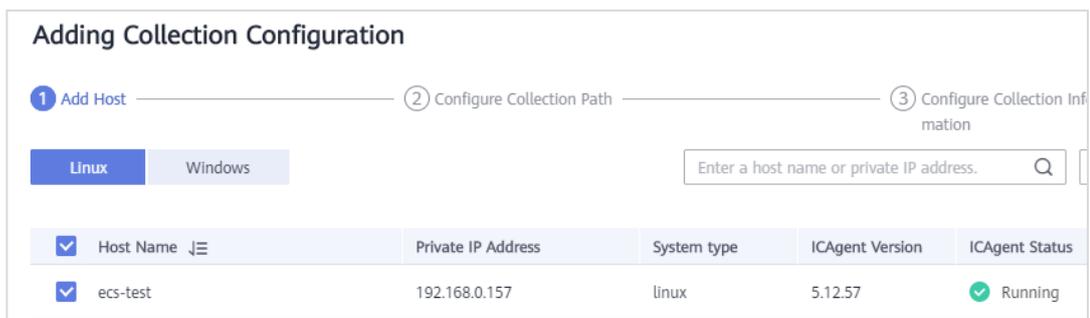
----End

4.5.3 Configuring Log Collection Rules

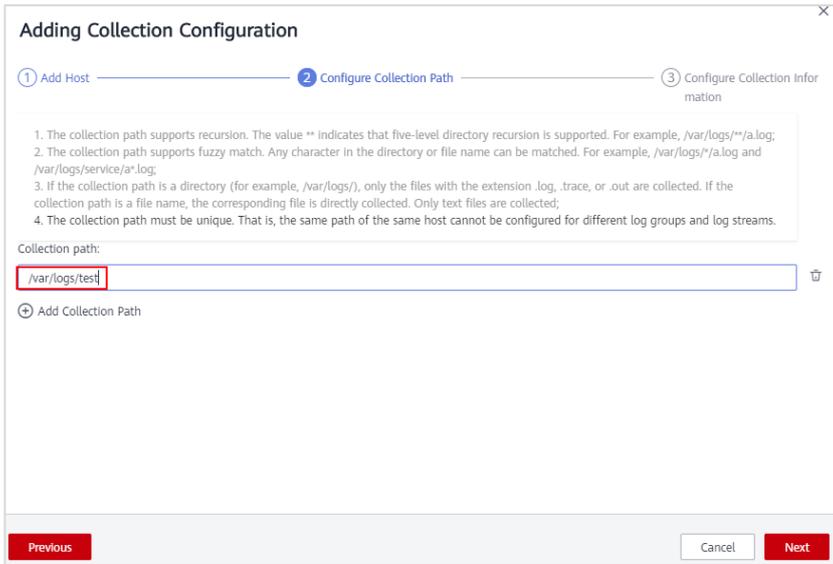
- Step 1 Go to the **Log Management** page, click the name of the created log group and the name of the created log stream. On the displayed **Log Stream** page, choose **Collection Configuration > Host**, and click **Add Path**.



- Step 2 In **Adding Collection Configuration** dialog box, select **ces-test**.

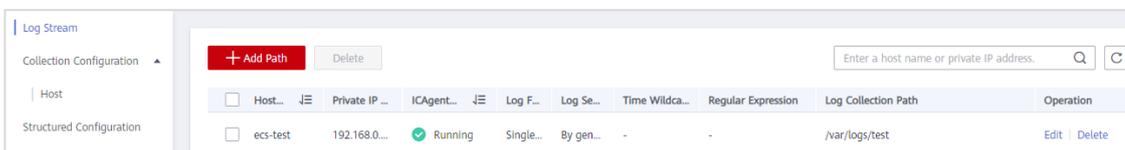
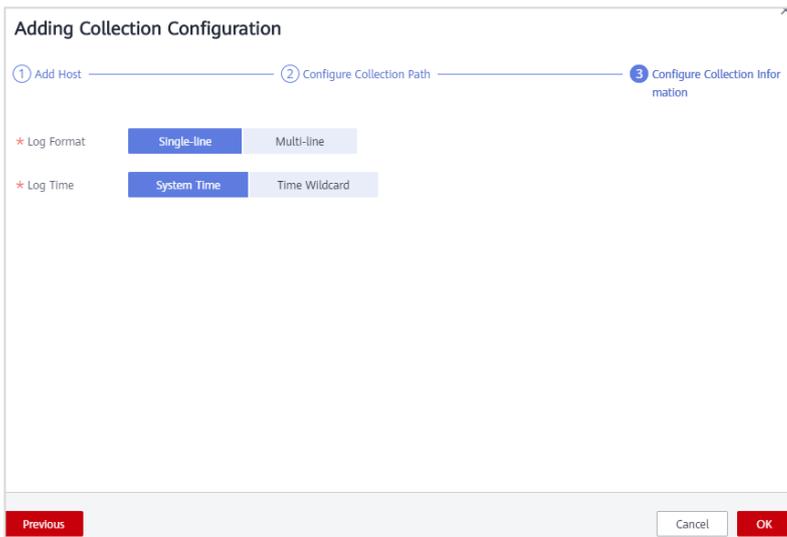


- Step 3 Configure the collection path by entering one ECS log path.



Step 4 Set the following parameters and then click **OK**.

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



Step 5 Wait for about 1 minute. On the **Log Stream** page, select the **Real-Time Logs** tab and view related logs.



```
Jun 4 19:20:53 ecs-myeecs NetworkManager[530]: <info> [1591269653.2951] device (eth0): state change: secondaries -> activated (reason 'none', sys-iface-state: 'managed')
Jun 4 19:20:53 ecs-myeecs NetworkManager[530]: <info> [1591269653.2965] manager: NetworkManager state is now CONNECTED_LOCAL
Jun 4 19:20:53 ecs-myeecs dhclient[602]: bound to 192.168.0.29 - renewal in 15386851 seconds.
Jun 4 19:20:53 ecs-myeecs NetworkManager[530]: <info> [1591269653.2993] manager: NetworkManager state is now CONNECTED_SITE
Jun 4 19:20:53 ecs-myeecs NetworkManager[530]: <info> [1591269653.2994] policy: set 'System eth0' (eth0) as default for IPv4 routing and DNS
Jun 4 19:20:53 ecs-myeecs NetworkManager[530]: <info> [1591269653.3038] device (eth0): Activation: successful, device activated.
Jun 4 19:20:53 ecs-myeecs NetworkManager[530]: <info> [1591269653.3042] manager: NetworkManager state is now CONNECTED_GLOBAL
Jun 4 19:20:53 ecs-myeecs NetworkManager[530]: <info> [1591269653.3045] manager: startup complete
```

----End

4.6 Deleting Resources

- Step 1 Delete all of the resources created for these exercises using the IAM user account (for example, **test123**). That includes any ECSs, alarm rules, cloud logs, and VPCs.
- Step 2 Use the HUAWEI CLOUD account to log in to the management console and delete all of the resources used for these exercises, such as user groups and IAM user accounts, trackers and key event notifications in CTS, and also the VPC.

----End



5 RDS

5.1 Introduction

RDS is a cloud-based web service that is reliable, scalable, easy to manage, and ready for immediate use out of the box. This exercise introduces how to buy RDS for MySQL databases, how to perform basic operations, and how to connect to DB instances.

5.1.1 Objectives

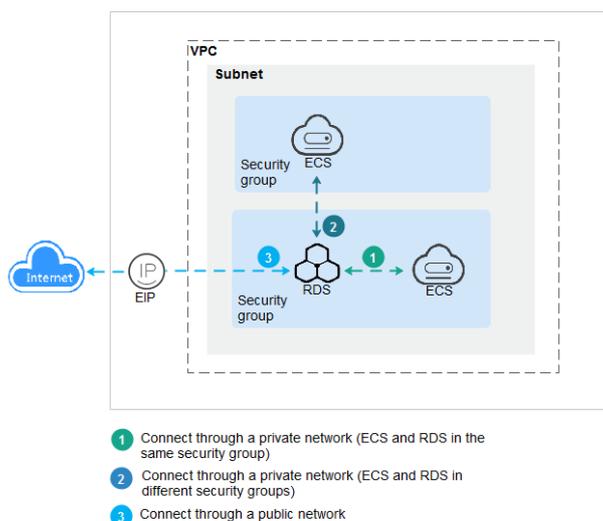
Upon completion of this exercise, you will be able to:

- Buy an RDS MySQL DB instance and perform basic operations.
- Master the method for changing the RDS MySQL database port.
- Master the method for connecting to an RDS MySQL DB instance.

5.1.2 Tasks

- Buy an RDS MySQL DB instance.
- Connect to a MySQL DB instance through DAS.
- Connect to a MySQL DB instance through a private network.
- Connect to a MySQL DB instance through a public network.

5.1.3 Exercise Architecture



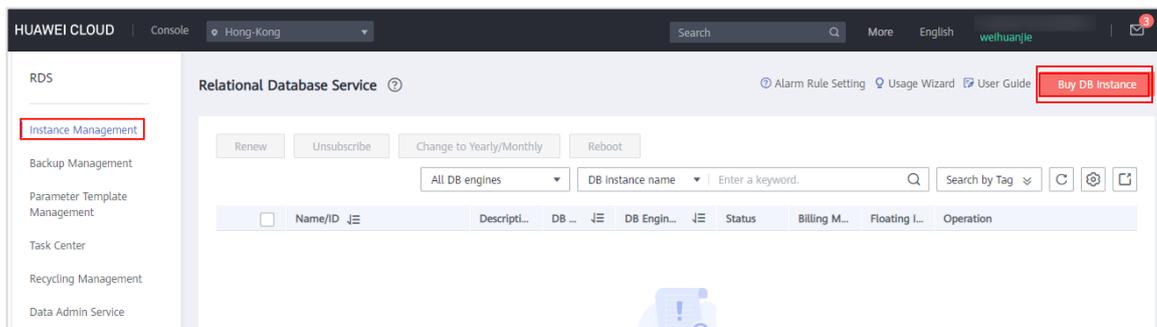


5.2 Buying an RDS MySQL DB Instance and Performing Basic Operations

RDS provides a comprehensive performance monitoring system, multiple layers of security, and a professional database management platform, allowing you to easily set, operate, and scale a relational database in the cloud. On the RDS console, you can execute all necessary tasks without any programming. This console simplifies the O&M process, and reduces routine O&M workload. Therefore, engineers can focus on application and business development.

5.2.1 Logging In to the Management Console

- Step 1 Log in to HUAWEI CLOUD, click **Console** in the upper right corner of the menu bar, and select AP-Hong Kong.
- Step 2 Choose **Service List > Database > Relational Database Service** to go to the RDS console. On the displayed page, click **Buy DB Instance**.



- Step 3 Set the following parameters:
 - **Billing Mode: Pay-per-use**
 - **Region: CN North-Beijing4**
 - **DB Instance name: rds-test**
 - **DB Engine: MySQL**
 - **DB Engine Version: 5.7**
 - **DB Instance Type: Single**
 - **Storage Type: Ultra-high I/O**
 - **AZ: optional**
 - **Time Zone: by default**



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

Region: AP-Hong-Kong
Regions are geographic areas isolated from each other. Resources are region-specific to the nearest region.

DB Instance Name: rds-test ⓘ
If you buy multiple DB instances at a time, they will be named with four digits after the instance name, such as instance-0001, the second as instance-0002, and so on.

DB Engine: **MySQL** | PostgreSQL | Microsoft SQL Server

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

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

Storage Type: **Recommended Ultra-high I/O** | Learn more about storage types.

AZ: **az1** | az2

Time Zone: UTC+08:00

- **Instance Class: General-enhanced** (1 vCPU and 2 GB memory, minimal specifications on the page)
- **Storage Space: 40 GB**
- **Disk Encryption: Disable**

Instance Class ⓘ: **General-enhanced** | General-enhanced II

vCPU Memory	Maximum Connections	TPS/QPS ⓘ
<input checked="" type="radio"/> 1 vCPU 2 GB	800	295 5,905
<input type="radio"/> 1 vCPU 4 GB	1,500	494 9,880
<input type="radio"/> 2 vCPUs 4 GB	1,500	466.35 9,327.04
<input type="radio"/> 2 vCPUs 8 GB	2,500	614.7 12,293.97
<input type="radio"/> 4 vCPUs 8 GB	2,500	969.14 19,382.91
<input type="radio"/> 4 vCPUs 16 GB	5,000	1,738.30 34,607.81

DB Instance Specifications: General-enhanced | 1 vCPU | 2 GB , Maximum Connections : 800 , TPS/QPS: 295 | 5905

Storage Space (GB): **40 GB** | 40 | 800 | 1,550 | 2,300 | 4,000 | - 40 + ⓘ

We provide free backup space the same size as the storage space of the primary DB instance. After the free backup space is used up, 40 GB is recommended. Enjoy more benefits of free packages. [Learn more](#)

Disk Encryption: **Disable** | Enable ⓘ | **Recommended** Use KMS to secure your data for free



- **VPC:** Select an existing VPC. Alternatively, create a VPC, refresh the page later, and add the created VPC.
- **Security Group:** sys-default
- **Administrator:** root
- **Database Port:** 3306 (default value)
- **Administrator Password:** user-defined
- **Parameter Template:** by default
- **Quantity:** 1
- **Read Replica:** Skip

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

VPC ?

⚠ After the RDS instance is created, the VPC cannot be changed. ECSs in different VPCs cannot communicate with each other by c

Security Group ? [View Security Group](#)

Inbound: -- | Outbound: --
In a security group, rules that authorize connections to DB instances apply to all DB instances associated with the security group.

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

Password

Administrator

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

Confirm Password

Parameter Template [View Parameter Template](#)

Tag It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predef](#)

You can add 10 more tags.

Quantity ? The total number of primary DB instances and read replicas cannot exceed 50. [Increase quota](#)

Read Replica ?

Step 4 Click **Next**. On the displayed page, confirm the specifications and click **Submit**. If you need to modify your settings, click **Previous**.



Step 5 Creating a DB instance takes about 5 to 9 minutes. During the process, the instance status displayed in the DB instance list is **Creating**. You can periodically refresh the list to see if the creation is finished. Once the DB instance is ready, the status changes to **Available**.

----End

5.2.2 Modifying the Automated Backup Policy for an RDS MySQL DB Instance

Step 1 Click a DB instance to view its details.



- Step 2 On the **Backup & Restoration** page, click **Modify Backup Policy** and modify the backup policy based on service requirements.

The screenshot shows the Huawei Cloud console interface. On the left, the 'Backups & Restorations' menu item is highlighted. In the center, the 'Modify Backup Policy' dialog box is open. The dialog box contains the following information:

- Automated Backup:** A toggle switch is currently turned off.
- Retention Period:** Set to 7 days. Below it, a note says 'Enter an integer from 1 to 732.'
- Time Zone:** Set to GMT+08:00.
- Time Window:** Set to 02:00 - 03:00. Below it, a note says 'The backup time is stored based on UTC time and will not change during daylight change. Time in local time however might change over daylight change according to the change.'
- Backup Cycle:** A dropdown menu is set to 'All'. Below it, checkboxes are shown for All, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday, all of which are checked. A note below says 'A minimum of one day must be selected.'
- Footer:** A note says 'If you require a fined-grained backup policy, log in to the database.' Below this are 'OK' and 'Cancel' buttons.

-----End

5.2.3 Changing the Database Port of an RDS MySQL DB Instance

After a MySQL DB instance is created, the default database port is 3306. You can change the database port if needed.

- Step 1 On the **Instance Management** page, click the target DB instance.
- Step 2 In the **Connection Information** area on the **Basic Information** page, click  in the **Database Port** field to change the database port if needed.



The screenshot shows the configuration page for an RDS instance named 'rds-test'. The left sidebar contains navigation options: Basic Information, Backups & Restorations, EIPs, Connection Management, Accounts, Databases, Logs, SQL Audits, Parameters, Advanced O&M, Tags, and CloudDBA. The main content area is divided into two sections: 'DB Information' and 'Connection Information'. The 'DB Information' section includes fields for DB Instance Name (rds-test), DB Instance ID, DB Engine Version (MySQL 5.7.29), DB Instance Type (Single), Instance Class (rds.mysql.c2.medium), Administrator (root), and AZ (az1). The 'Connection Information' section includes Floating IP Address (192.168.0.135), VPC (default_vpc), Subnet (default_subnet), Private Domain Name, Database Port (3306), Recommended Max. Connections (800), and Security Group (default_securitygroup). The Database Port field is highlighted with a red box.

-----End

5.3 Connecting to a MySQL DB Instance Through DAS

Step 1 Go back to the RDS instance list, locate the target DB instance you want to log in and click **Log In** in the **Operation** column.

The screenshot shows the 'Relational Database Service' instance list. At the top, there are buttons for Renew, Unsubscribe, Change to Yearly/Monthly, and Reboot. Below these are filters for 'All DB engines' and a search box for 'DB instance name'. A table lists the instances with columns: Name/ID, Description, DB Instance, DB Engine Version, Status, Billing Mode, Floating IP Address, and Operation. One instance is listed with Name/ID 'rds-test' and a 'Log In' button highlighted in red in the Operation column.

Step 2 Provide the username and password. The username is **root**. The password is the one you set when the instance was created.



Database Login

* Username :

Password :

Remember Password
Agree that the username and password are recorded in the DAS system and can be deleted from the DAS connection list page if it is no longer needed.

Metadata Collection ⓘ
If this item is not enabled, DAS can only query the database to query these structure definition data in real time, which has a certain impact on the real-time performance of your database.

SQL Execution Record ⓘ
After turning this on, you can easily view your SQL window execution history in the DAS, and you can execute it directly without repeating the input.

Data Admin Service MySQL SQL Operations Database Management Import and Export Structure Management Data Scheme Background Tasks CloudDBA **MySQL**

Home

DB Instance Name: **rds-test** DB Engine Version: mysql 5.7.29

Database List

Database Name	Table Quantity	Table Size	Index Size	Character Set	Operation
 You have not created any databases. Click Create Database to create one.					

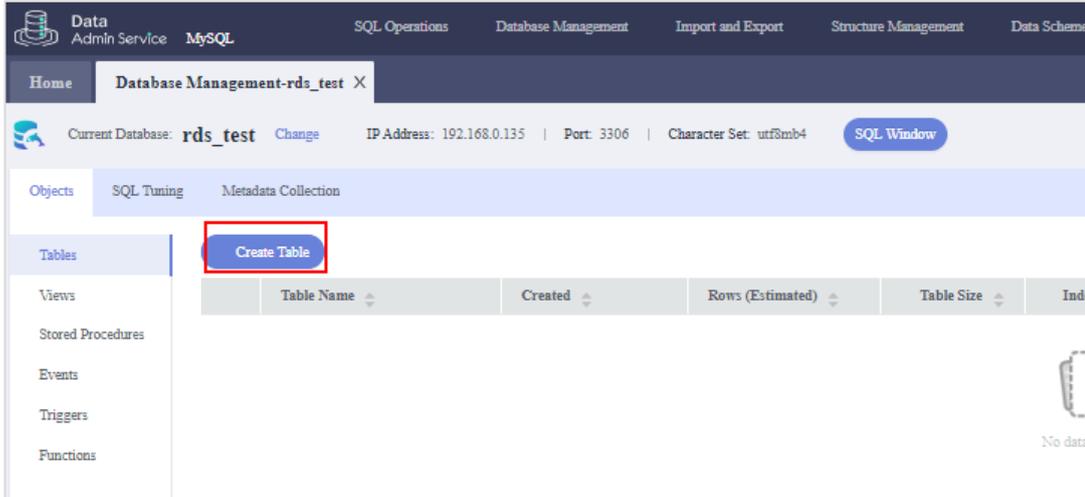
Step 3 Click **Create Database**, specify **Name**, and click **OK**.

Create Database

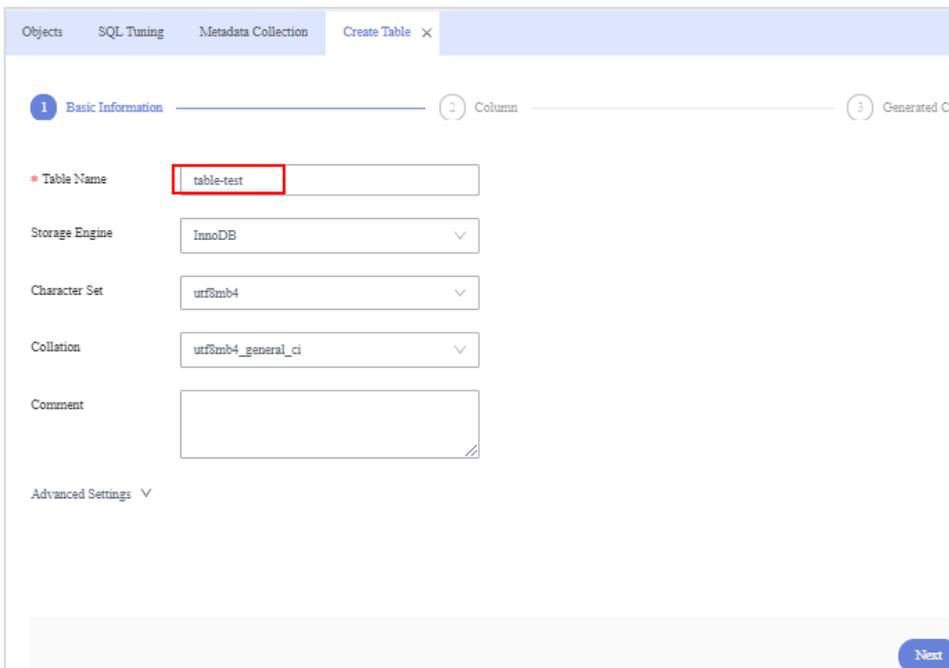
* Name

Character Set

Step 4 Click the name of the created database. On the displayed page, click **Create Table**.



Step 5 Enter the basic information when prompted and click **Next**.



Step 6 Specify **Column Name, Type**, and other information. Click **Create**.



Home Database Management-rds_test X

Current Database: rds_test Change IP Address: 192.168.0.135 | Port: 3306 | Character Set: utf8mb4 SQL Window

Objects SQL Tuning Metadata Collection Create Table X

1 Basic Information 2 Column 3 Generated Column(Optional)

Add Insert Delete Move Up Move Down

No.	Column Name	Type	Length	Nullable	Primary Key	Comment
1	123	int	11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Previous Next Create

Current Database: rds_test Change IP Address: 192.168.0.135 | Port: 3306 | Character Set: utf8mb4 SQL Window

Objects SQL Tuning Metadata Collection Alter Table: table-test X

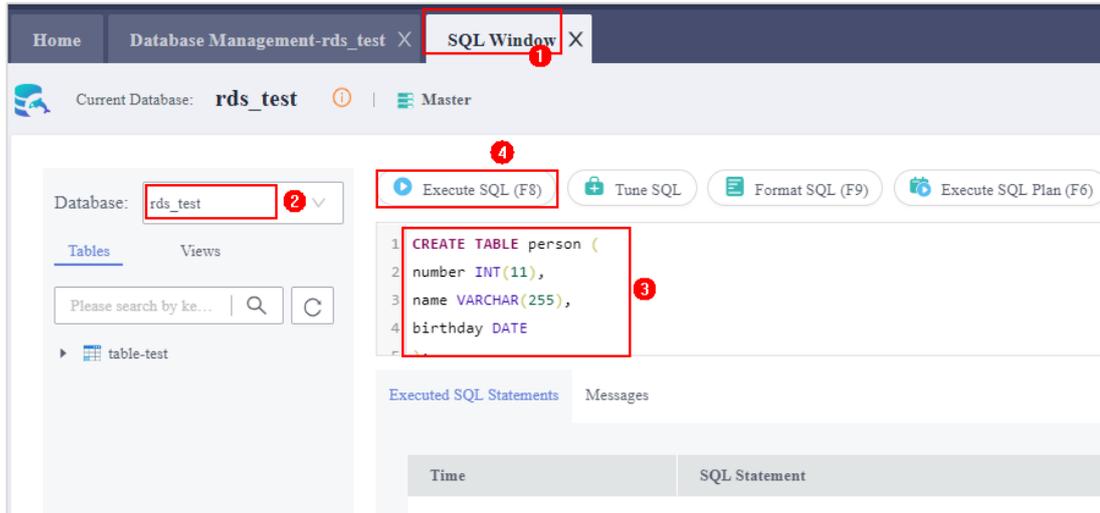
Tables Create Table

Table Name	Created	Rows (Estimated)	Table Size	Index Size
table-test	2020-08-16 12:24:55	0	16KB	0B

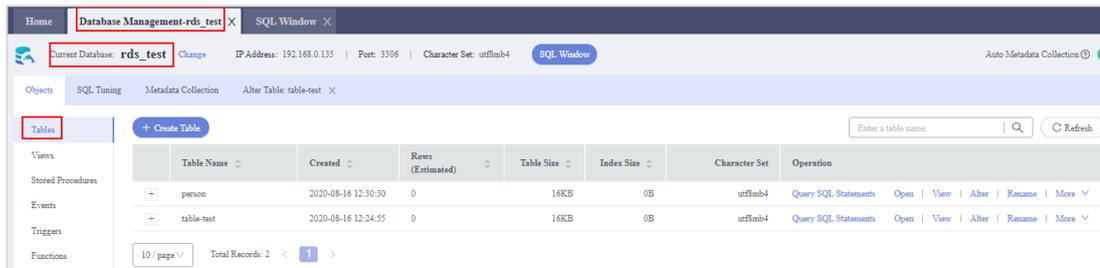
10 / page Total Records: 1 < 1 >

Step 7 You can also use SQL statements to create a table. An example is illustrated in the following figure. Click **SQL Window**, select database **rds_test**, clear any existing SQL statements, and copy the following statements into the window to create a table named **person**. Then, click **Execute** to create the table.

```
CREATE TABLE person (  
  number INT(11),  
  name VARCHAR(255),  
  birthday DATE  
);
```



Step 8 Go back to the table list and check that table **person** has been created.

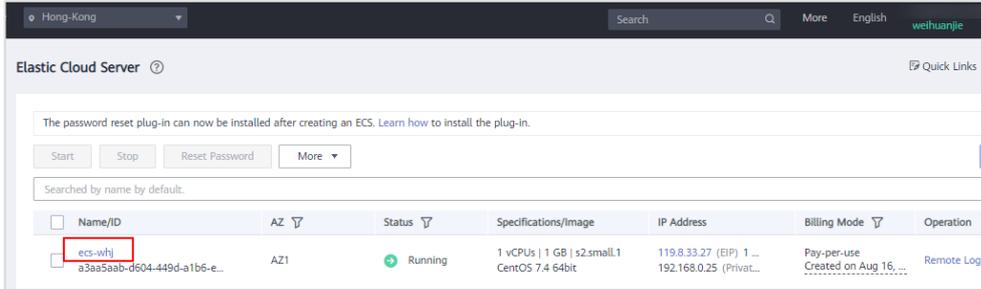


Step 9 Click **More** in the **Operation** column and drop or maintain the table as required. In this exercise, the table is not dropped.

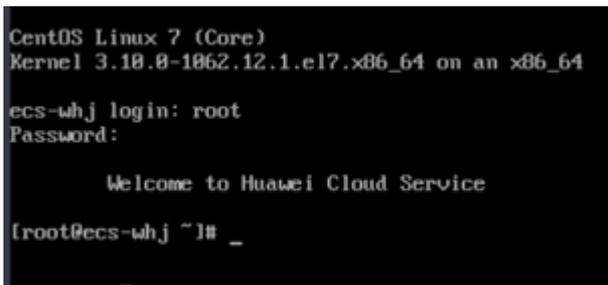
----End

5.4 Connecting to a MySQL DB Instance Through a Private Network

Step 1 Go back to the HUAWEI CLOUD console, select AP-Hong Kong. Click **Service List** and choose **Elastic Cloud Server** In the left navigation pane. Buy a Linux ECS (with an EIP) by referring to section 1.1.4. The following uses an ECS running CentOS as an example. Ensure that the VPC and security group of the ECS are the same as those of the RDS DB instance.



Step 2 Enter the username and password to log in to the ECS.



Step 3 Run the following command to install the MySQL client. The installation is complete if information in the following figure is displayed.

`yum install mysql -y`



Step 4 Run the following command to connect to the MySQL database on the target host:
(Note: If the ECS and RDS DB instance are in the same security group, the ECS and RDS DB instance can communicate with each other by default. You do not need to set security group rules. You can ping the RDS private IP address on the ECS for verification. If the



ECS and RDS DB instance are in different security groups, you need to set security group rules for the ECS and RDS DB instance, respectively.)

`mysql -h RDS private IP address -uroot -p RDS instance password`

```
[root@ecs-whj ~]# mysql -h 192.168.0.136 -uroot -phuawei@123!
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 64594
Server version: 5.7.29-2-log MySQL Community Server - (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> [ 253.592196] psmouse serial: UMmouse at isa0060/serial/input0 lost sync at byte 1
[ 253.632212] psmouse serial: UMmouse at isa0060/serial/input0 - driver resynced.
```

- Step 5 Run the following command to view the databases. You can see the default database and the database created on the DAS console. (Operations on MySQL databases must comply with the standard SQL syntax and end with semicolons (;).)

`show databases;`

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| rds_test |
| sys |
+-----+
5 rows in set (0.01 sec)

MySQL [(none)]>
```

- Step 6 Run the following command to use the database:

`use rds_test` #the database created on DAS

```
MySQL [(none)]> use rds_test
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [rds_test]>
```

- Step 7 Run the following command to view the tables created on the DAS in the database:

`show tables;`



```
MySQL [rds_test]> show tables;
+-----+
| Tables_in_rds_test |
+-----+
| person              |
| table-test          |
+-----+
2 rows in set (0.00 sec)

MySQL [rds_test]>
```

Step 8 Run the following command to exit:

```
exit;
```

```
MySQL [rds_test]> exit;
Bye
[root@ecs-whj ~]#
```

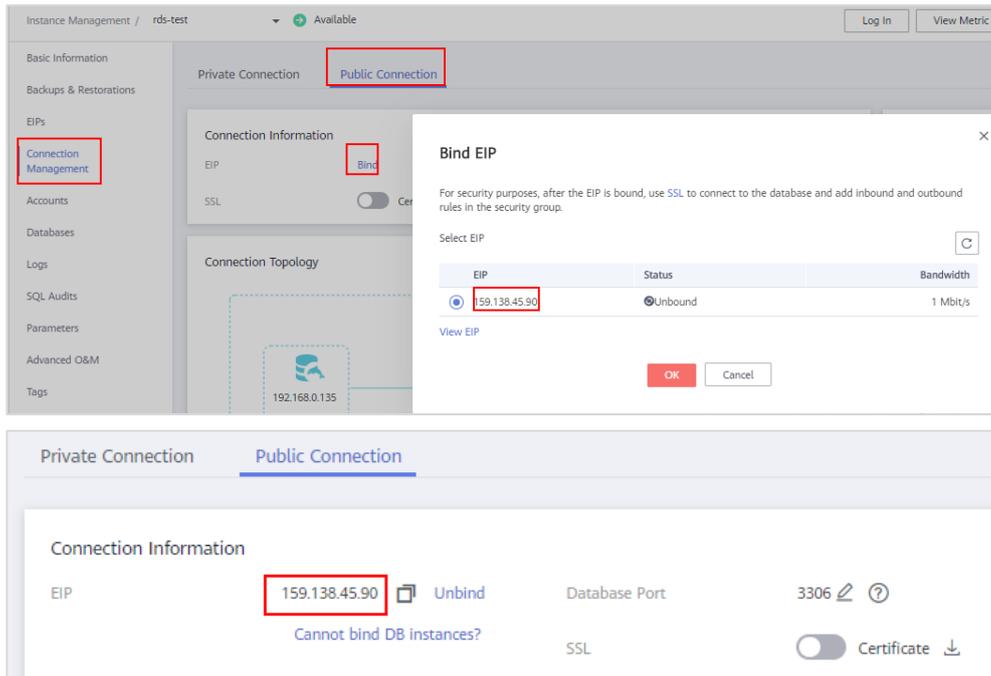
----End

5.5 Connecting to a MySQL DB Instance Through a Public Network

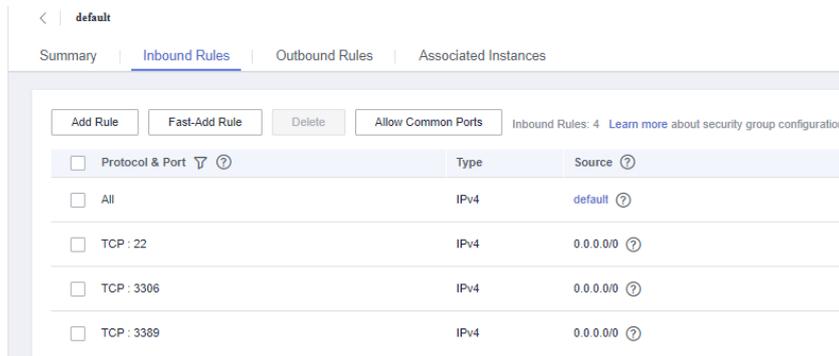
Step 1 Buy an EIP on the network console by referring to section 3.2.

EIP	Moni...	Status	EIP Type	Bandwidth	Bandwidth ...	Associated In...	Billing Mode	Operation
159.138.45.90		Unbo...	Dynamic BGP	bandwidth-316f	Bandwidth 1 Mbit/s	--	Pay-per-use Created on Aug 16, ...	Bind Unbind More
119.8.33.27		Bound	Dynamic BGP	ecs-whj-bandwid...	Bandwidth 1 Mbit/s	ecs-whj ECS	Pay-per-use Created on Aug 16, ...	Bind Unbind More

Step 2 Go back to the RDS console. On the **Instance Management** page, click the target DB instance. On the displayed page, choose **Connection Management > Public Connection**, and click **Bind** in the **EIP** field.



Step 3 Click the security group. On the **Inbound Rules** page, add an inbound rule for port 3306.



Step 4 On the ECS, check whether the RDS DB instance can connect to the MySQL database through the EIP bound to the RDS DB instance. If information similar to the following figure is displayed, the connection was successful. If the connection failed, check whether they are in the same security group and whether the security group policy is configured correctly.)

ping RDS-EIP



```
[root@ecs-whj ~]# ping 121.36.46.92
PING 121.36.46.92 (121.36.46.92) 56(84) bytes of data.
64 bytes from 121.36.46.92: icmp_seq=34 ttl=55 time=3.08 ms
64 bytes from 121.36.46.92: icmp_seq=35 ttl=55 time=2.48 ms
64 bytes from 121.36.46.92: icmp_seq=36 ttl=55 time=2.52 ms
64 bytes from 121.36.46.92: icmp_seq=37 ttl=55 time=2.42 ms
64 bytes from 121.36.46.92: icmp_seq=38 ttl=55 time=2.44 ms
64 bytes from 121.36.46.92: icmp_seq=39 ttl=55 time=2.39 ms
64 bytes from 121.36.46.92: icmp_seq=40 ttl=55 time=2.75 ms
64 bytes from 121.36.46.92: icmp_seq=41 ttl=55 time=2.51 ms
64 bytes from 121.36.46.92: icmp_seq=42 ttl=55 time=2.54 ms
64 bytes from 121.36.46.92: icmp_seq=43 ttl=55 time=2.39 ms
64 bytes from 121.36.46.92: icmp_seq=44 ttl=55 time=2.59 ms
64 bytes from 121.36.46.92: icmp_seq=45 ttl=55 time=2.39 ms
64 bytes from 121.36.46.92: icmp_seq=46 ttl=55 time=2.43 ms
64 bytes from 121.36.46.92: icmp_seq=47 ttl=55 time=2.80 ms
64 bytes from 121.36.46.92: icmp_seq=48 ttl=55 time=2.38 ms
64 bytes from 121.36.46.92: icmp_seq=49 ttl=55 time=2.45 ms
```

Step 5 Run the following command to connect to the RDS DB instance again:

```
mysql -h RDS-EIP -P 3306 (database port number) -uroot -p RDS instance password
```

```
[root@ecs-whj ~]# mysql -h 192.168.0.135 -P 3306 -uroot -phuawei@123!
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 11374
Server version: 5.7.29-5-log MySQL Community Server - (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Step 6 Run the following command to view the databases. You can see the default database and the database created on the DAS console. (Operations on MySQL databases must comply with the SQL statement standard and end with semicolons (;).)

```
show databases;
```

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| rds_test |
| sys |
+-----+
5 rows in set (0.00 sec)

MySQL [(none)]>
```



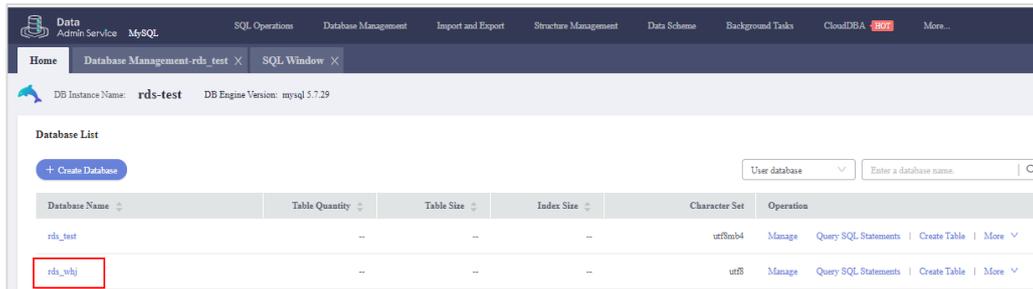
Step 7 Run the following command to create another database:

create database rds_whj; #rds_whj is the name of the created database.

```
MySQL [(none)]> create database rds_whj;
Query OK, 1 row affected (0.00 sec)

MySQL [(none)]>
```

Step 8 Go back to the DAS console. You can see the created database is already in the database list.



Step 9 Go back to the ECS login page and run the following command to exit:

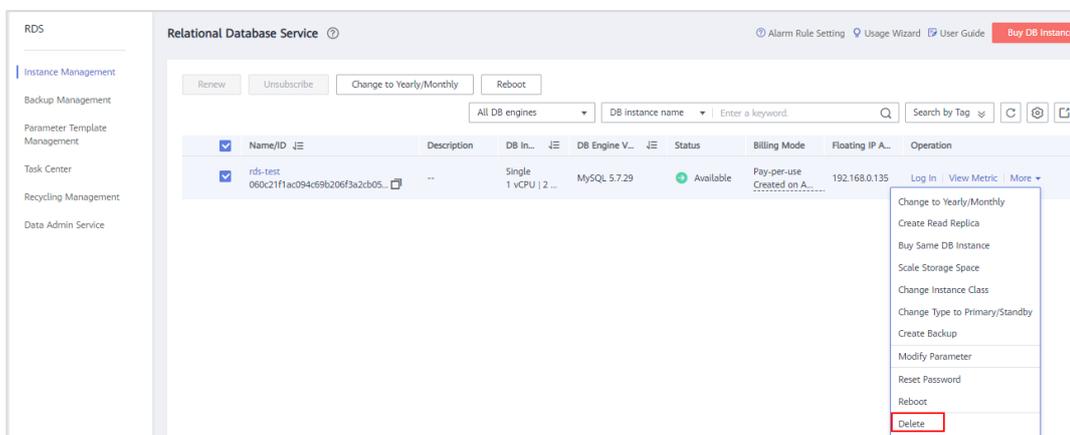
exit;

```
MySQL [(none)]> exit;
Bye
[root@ecs-whj ~]#
```

----End

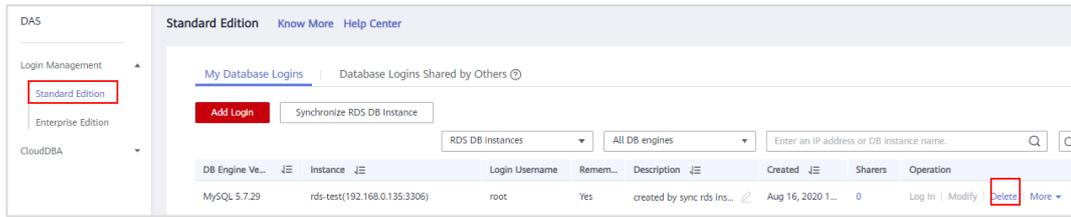
5.6 Deleting Resources

Step 1 Delete the RDS DB instance created in this exercise.

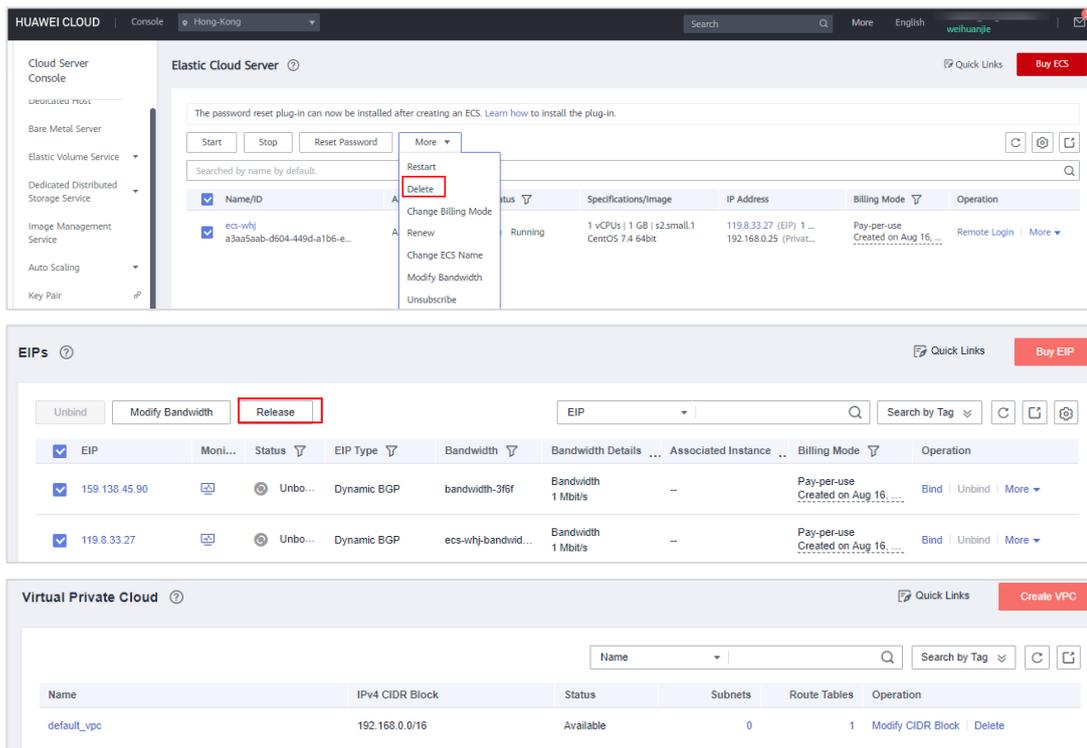




Step 2 Delete DAS resources.



Step 3 Delete the ECS and related EIP and VPC resources.



Check whether there are still any resources that have not been deleted in the account. If there are, delete them. Make sure that all resources created in this exercise are deleted.



6 Comprehensive Exercises: HA Architecture for Enterprise ECSs

6.1 Application Scenario

An enterprise intends to deploy their website on HUAWEI CLOUD with the following requirements:

- Data nodes and service nodes are deployed separately, and service nodes are deployed on ECSs.
- The number of ECSs can be dynamically adjusted based on service traffic.
- Service traffic can be automatically distributed to the ECSs.
- Service statuses can be monitored.

6.2 Solution

Requirement	Solution	Involved Services
Service nodes are deployed on ECSs.	Buy ECSs as service nodes. Use the VPC service to provide network resources for the ECSs.	ECS and VPC
The number of ECSs can be dynamically adjusted based on service traffic.	Use AS to dynamically increase or decrease the number of ECSs based on service traffic to ensure stable service running. ECSs are created based on the existing AS configuration (service node configuration).	AS and IMS
Service traffic can be automatically distributed across the ECSs.	Use ELB to automatically distribute service traffic across multiple ECSs for better fault tolerance.	ELB
Service statuses can be monitored.	Use Cloud Eye to monitor service statuses.	Cloud Eye



6.3 Preparations

Step 1 Create a VPC.

- Visit the [HUAWEI CLOUD official website](#) and click **Log In** in the upper right corner. Enter username and password, and then click **Login**.
- On the management console, switch the region to AP-Hong Kong. In the left navigation pane, choose **Service List > Network > Virtual Private Cloud**. Create a VPC. For details, see section 3.2.1.

Name	IPv4 CIDR Block	Status	Subnets	Route Tables	Operation
vpc-whj	192.168.0.0/16	Available	0	1	Modify CIDR Block Delete

Step 2 Create and configure a security group.

1. On the network console, choose **Access Control > Security Groups** and create a security group.

Name	Security Group Rules	Associated Instances	Description	Operation
sg-whj	7	0	The security group is for general-p...	Manage Rule More
default	4	0	default	Manage Rule More

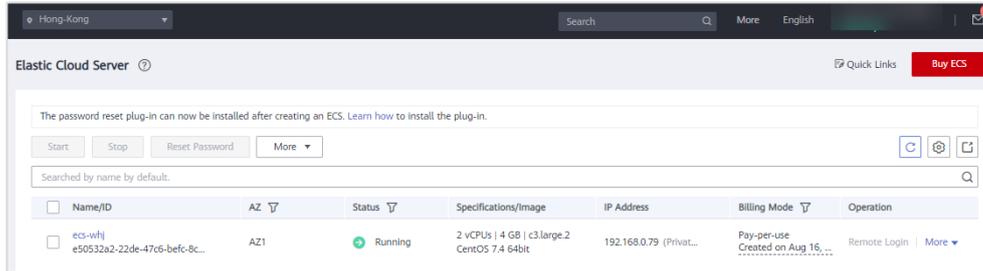
2. Click the security group name. On the page that is displayed, click **Inbound Rules** and then **Add Rule** to add an inbound rule with the following parameter settings:
 - **Protocol & Port: All**
 - **IP address in Source: 0.0.0.0/0**

Protocol & Port	Type	Source	Description
<input type="checkbox"/> All	IPv4	sg-whj	Allow ECSs in the same security group to commu...
<input type="checkbox"/> ICMP - All	IPv4	0.0.0.0/0	Used to test the ECS connectivity with the ping co...
<input type="checkbox"/> TCP - 22	IPv4	0.0.0.0/0	Used to remotely connect to Linux ECSs
<input type="checkbox"/> TCP - 80	IPv4	0.0.0.0/0	Used to access websites over HTTP
<input type="checkbox"/> TCP - 443	IPv4	0.0.0.0/0	Used to access websites over HTTPS
<input type="checkbox"/> TCP - 3389	IPv4	0.0.0.0/0	Used to remotely connect to Windows ECSs

Step 3 Buy a Linux ECS in the AP-Hong Kong region.



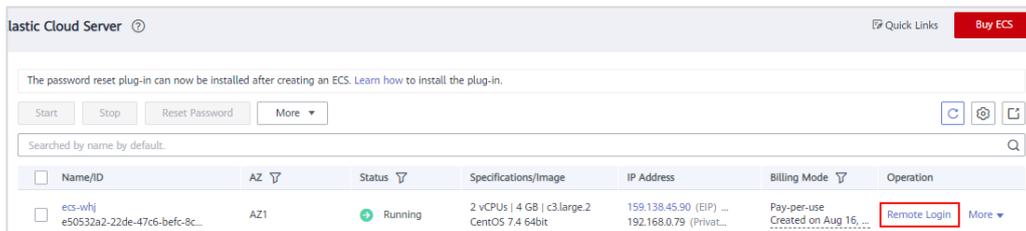
When setting parameters for the ECS, select the VPC and security group created in Step 1 and Step 2 of this procedure.



----End

6.4 Setting Up the Apache HTTP Server

Step 1 Switch back to the **Elastic Cloud Server** page and click **Remote Login** in the **Operation** column of the purchased ECS.



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



Step 3 Run the following command to install LAMP and enable desired processes:

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

```
(root@ecs-whj ~)# yum install -y httpd php php-fpm php-server php-mysql mysql
```

After the command is successfully executed, "Complete!" is displayed.



```
Installed:
  httpd.x86_64 0:2.4.6-93.el7.centos mariadb.x86_64 1:5.5.65-1.el7 php.x86_64 0:5.4.16-48.el7 php-fpm.x86_64 0:5.4.16-48.el7
  php-mysql.x86_64 0:5.4.16-48.el7

Dependency Installed:
  apr.x86_64 0:1.4.8-5.el7 apr-util.x86_64 0:1.5.2-6.el7 httpd-tools.x86_64 0:2.4.6-93.el7.centos
  libzip.x86_64 0:0.10.1-8.el7 mailcap.noarch 0:2.1.41-2.el7 php-cli.x86_64 0:5.4.16-48.el7
  php-common.x86_64 0:5.4.16-48.el7 php-pdo.x86_64 0:5.4.16-48.el7

Dependency Updated:
  mariadb-libs.x86_64 1:5.5.65-1.el7

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

Step 4 Run the following command to configure httpd:

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

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

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 code:

```
ServerName localhost:80
```

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



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

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

- Step 7 Run the following command to download the WordPress installation software:

```
wget -c https://hciacloud.obs.ap-southeast-1.myhuaweicloud.com/wordpress-5.3.1.tar.gz
```

If information similar to the following is displayed, the WordPress installation package has been downloaded.

```
root@ecs-whj ~]# wget -c https://hciacloud.obs.ap-southeast-1.myhuaweicloud.com/wordpress-5.3.1.tar.gz
--2020-08-16 18:44:23-- https://hciacloud.obs.ap-southeast-1.myhuaweicloud.com/wordpress-5.3.1.tar.gz
Resolving hciacloud.obs.ap-southeast-1.myhuaweicloud.com (hciacloud.obs.ap-southeast-1.myhuaweicloud.com)... 100.125.100.3, 100.125.100.2
Connecting to hciacloud.obs.ap-southeast-1.myhuaweicloud.com (hciacloud.obs.ap-southeast-1.myhuaweicloud.com)|100.125.100.3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12388850 (12M) [application/octet-stream]
Saving to: 'wordpress-5.3.1.tar.gz'

100%[=====] 12,388,850 --.-K/s in 0.05s

2020-08-16 18:44:23 (225 MB/s) - 'wordpress-5.3.1.tar.gz' saved [12388850/12388850]
root@ecs-whj ~]#
```

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

```
tar -zxvf wordpress-5.3.1.tar.gz -C /var/www/html
```

```
wordpress/wp-admin/widgets.php
wordpress/wp-admin/setup-config.php
wordpress/wp-admin/install.php
wordpress/wp-admin/admin-header.php
wordpress/wp-admin/post-new.php
wordpress/wp-admin/themes.php
wordpress/wp-admin/options-reading.php
wordpress/wp-trackback.php
wordpress/wp-comments-post.php
[root@ecs-whj ~]#
```

- Step 9 Run the following command to grant the read and write permissions to the directory where the file locates:

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

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

- Step 10 Run the following command to enable httpd:

```
systemctl start httpd.service
```

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



Step 11 Run the following command to enable php-fpm:

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

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

Step 12 Run the following command to check the httpd status, which is **active (running)**:

```
systemctl status httpd
```

```
■ httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
  Active: active (running) since Wed 2020-06-17 15:36:31 CST; 2min 35s ago
    Docs: man:httpd(8)
          man:apachectl(8)
  Main PID: 1442 (httpd)
  Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"
  CGroup: /system.slice/httpd.service
          └─1442 /usr/sbin/httpd -DFOREGROUND
            └─1444 /usr/sbin/httpd -DFOREGROUND
              └─1445 /usr/sbin/httpd -DFOREGROUND
                └─1446 /usr/sbin/httpd -DFOREGROUND
                  └─1447 /usr/sbin/httpd -DFOREGROUND
                    └─1448 /usr/sbin/httpd -DFOREGROUND

Jun 17 15:36:31 ecs-whj systemd[1]: Starting The Apache HTTP Server...
Jun 17 15:36:31 ecs-whj systemd[1]: Started The Apache HTTP Server.
[root@ecs-whj ~]#
```

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

```
systemctl status php-fpm
```

```
[root@ecs-whj ~]# systemctl status php-fpm
■ php-fpm.service - The PHP FastCGI Process Manager
  Loaded: loaded (/usr/lib/systemd/system/php-fpm.service; disabled; vendor preset: disabled)
  Active: active (running) since Wed 2020-06-17 15:37:50 CST; 4min 32s ago
  Main PID: 1455 (php-fpm)
  Status: "Processes active: 0, idle: 5, Requests: 0, slow: 0, Traffic: 0req/sec"
  CGroup: /system.slice/php-fpm.service
          └─1455 php-fpm: master process (/etc/php-fpm.conf)
            └─1457 php-fpm: pool www
              └─1458 php-fpm: pool www
                └─1459 php-fpm: pool www
                  └─1460 php-fpm: pool www
                    └─1461 php-fpm: pool www

Jun 17 15:37:50 ecs-whj systemd[1]: Starting The PHP FastCGI Process Manager...
Jun 17 15:37:50 ecs-whj systemd[1]: Started The PHP FastCGI Process Manager.
[root@ecs-whj ~]#
```

Step 14 Run the following command to set httpd to automatically start upon system startup:

```
systemctl enable httpd
```

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

Step 15 Run the following command to set php-fpm to automatically start upon system startup:

```
systemctl enable php-fpm
```



```
[root@ecs2-00] ~]#
C:\> ping 159.138.45.90
[root@ecs2-00] ~]#
```

Step 16 In the browser, enter the EIP bound to the ECS.

If the following information is displayed, LAMP has been installed.

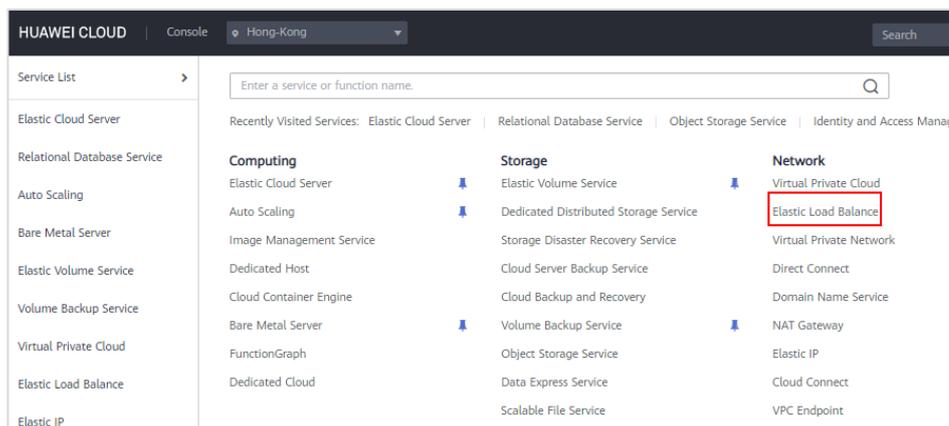


----End

6.5 Configuring Server-Level HA

6.5.1 Configuring ELB

Step 1 Log in to the management console and choose **Service List > Network > Elastic Load Balance**.



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

Step 3 Set parameters as follows:

- **Type:** Shared
- **Region:** AP-Hong Kong



- **Network Type: Public network**
- **VPC:** Select the created VPC from the drop-down list.
- **Subnet:** Select the created subnet from the drop-down list.

* Type: Shared

* Region: AP-Hong-Kong

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

* Network Type: Public network Private network

* VPC: vpc-whj View VPC

* Subnet: subnet-77af (192.168.0.0/24) View Subnet Available private IP addresses: 247

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

- **EIP: New EIP**
- **EIP Type: Dynamic BGP**
- **Billed By: Bandwidth**
- **Bandwidth: 1 Mbit/s**
- **Name:** Enter a name.

* EIP: New EIP Use existing

* EIP Type: Dynamic BGP

* Billed By: Bandwidth (For heavy/stable traffic) Traffic (For light/sharply fluctuating traffic)

Billed based on usage duration and bandwidth size.

* Bandwidth: 1 2 5 10 100 200 Custom 1 +

Anti-DDoS protects resources from network and application layer DDoS attacks and sends notifications the instant attacks are detected. DDoS Console | Advanced Anti-DDoS Console

* Name: elb-whj

Advanced Settings Description Tag

Step 4 Click **Next**, confirm parameter settings, and click **Submit**.

Step 5 Switch back to the network console and verify that the created load balancer is in the **Running** state.

Name	Status	Type	IP Address and Network	Listener (Frontend Prot...	EIP Billing Information	Billing Mode	Operation
elb-whj	Running	Shared	192.168.0.2 (Private IP addr... 159.138.42.217 (EIP) vpc-whj (VPC)	Add listener	1 Mbit/s Pay-per-use By bandwidth	--	Modify Bandwidth Delete More



Step 6 Click the name of the load balancer to view its details. Click **Listeners** and then **Add Listener**. Set the **Name** and **Frontend Protocol/Port** and click **Next**.

elb-whj Running

Basic Information Listeners Backend Server Groups Monitoring Tags

Add Listener

Add Listener

1 Configure Listener 2 Configure Backend Server Group 3 Finish

* Name listener-whj

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

Select TCP or UDP for load balancing at Layer 4. Select HTTP or HTTPS for load balancing at Layer 7.
When HTTPS is selected, the backend protocol can only be HTTP.

Obtain Client IP Address

Advanced Settings

Cancel Next

Step 7 Configure the backend server group.

- **Backend Server Group: Create New**
- **Name:** Enter a name.
- **Health check configuration:** Keep the health check function disabled.
- **Other parameters:** Retain their default settings.

Add Listener

1 Configure Listener 2 Configure Backend Server Group 3 Finish

Backend Server Group Create new Use existing

* Name server_group-whj

* Backend Protocol TCP

* Load Balancing Algorithm Weighted round robin

Sticky Session

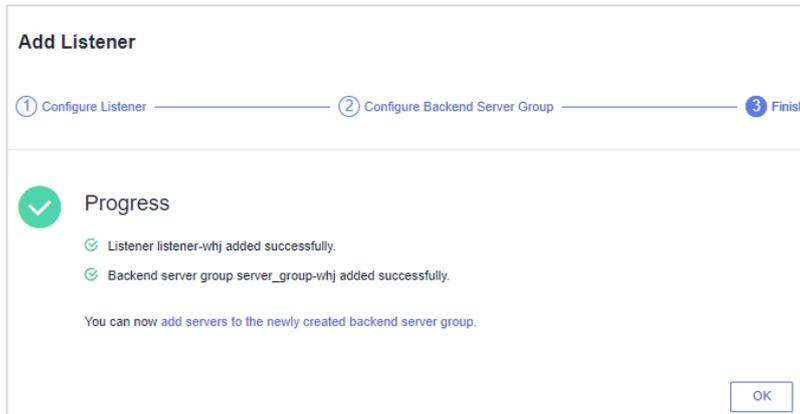
Description 0/255

Health Check Configuration

Enable Health Check



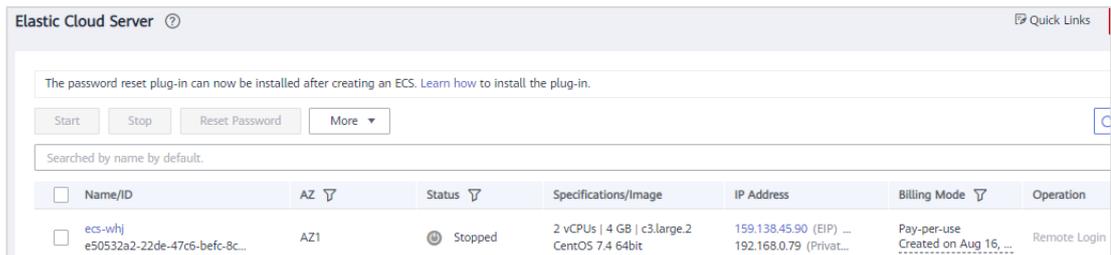
Step 8 Click **OK**.



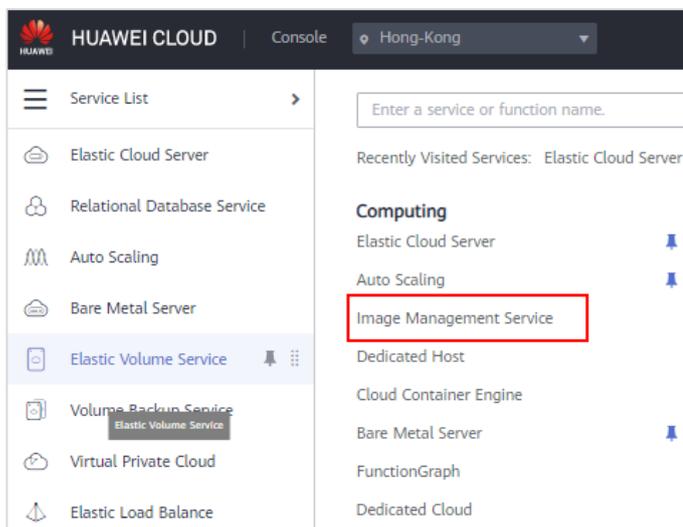
----End

6.5.2 Creating an Image

Step 1 Switch back to the **Elastic Cloud Server** page and stop the ECS.



Step 2 In the left navigation pane, choose **Service List > Computing > Image Management Service**.





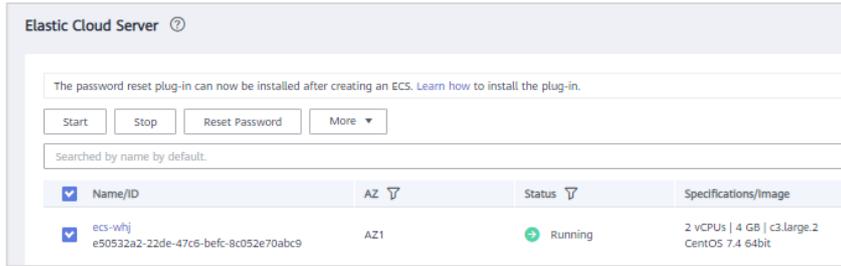
Step 3 Click **Create Image** in the upper right corner of the page.

- **Type:** System disk image
- **Source:** Click **ECS** and then select the purchased ECS.
- **Name:** Enter a name.

The screenshot shows the 'Create Image' interface. At the top, there is a notification: 'The IMS service is now in commercial use. You will be charged the private image storage fees. For details, see [IMS pricing](#).' Below this, the 'Image Type and Source' section has 'System disk image' selected under 'Type' and 'ECS' selected under 'Source'. A blue box contains instructions: 'You can only use a running or stopped ECS to create a private image. You need to first customize and optimize the ECS to suit your needs. For example, you need to install Cloud-init if the ECS runs Linux and install Cloudbase-init if the ECS runs Windows. [Learn more](#). Do not perform any operation on the selected ECS or associated resources during image creation.' Below the instructions is a table of ECS instances. The selected instance is 'ecs-whj' with OS 'CentOS 7.4 64bit' and status 'Stopped'. Below the table, it says 'Selected: ecs-whj|OS: CentOS 7.4 64bit|System Disk: High I/O | 40 GB' and 'Buy ECS'. In the 'Image Information' section, 'Encryption' is 'Unencrypted' and 'Name' is 'ims-whj'.

Step 4 Wait until the image status becomes **Normal**. Then, switch back to the **Elastic Cloud Server** page and start the ECS.

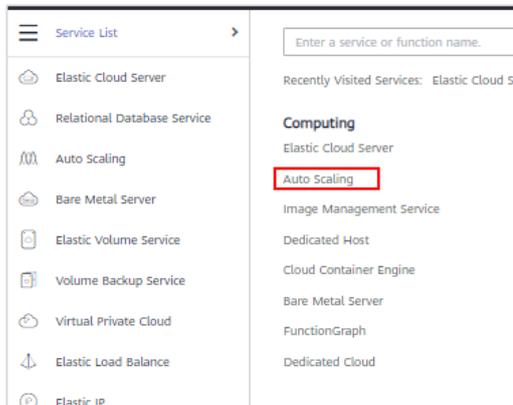
The screenshot shows the 'Image Management Service' page. At the top right is a 'Create' button. Below is a notification: 'The IMS service is now in commercial use. You will be charged the private image storage fees. No charges will be incurred after you delete the created images. For details, see [IMS pricing](#).' Below this are tabs for 'Public Images', 'Private Images', and 'Images Shared with Me'. A blue box contains a warning: 'You are advised to optimize private images that do not support fast ECS creation. To check whether a private image supports this function, go to its details page. [Learn more](#).' Below the warning is a table of private images. The image 'ims-whj' is listed with a status of 'Normal', OS Type 'Linux', OS 'CentOS 7.4 64bit', Image Type 'ECS system disk image', Disk Capacity (GB) '40', Encrypted 'No', and Created 'Aug 16, 2020 20:32:44 GMT+08:00'. The 'Operation' column for this image shows 'Apply for Server | Modify | More'.



-----End

6.5.3 Configuring AS

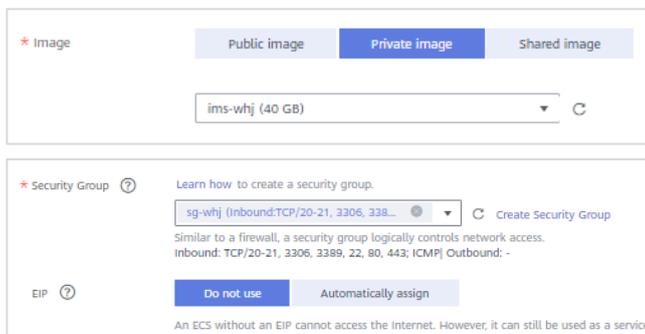
Step 1 In the left navigation pane, choose **Service List > Computing > Auto Scaling**.



Step 2 Click **Create AS Configuration**.

Step 3 Set AS configuration parameters.

- **Image:** Select the created system disk image from the drop-down list.
- **Security Group:** Select the created security group, which is the same as that of the ECS.
- **EIP: Do not use**
- **Other parameters:** Set them as required.



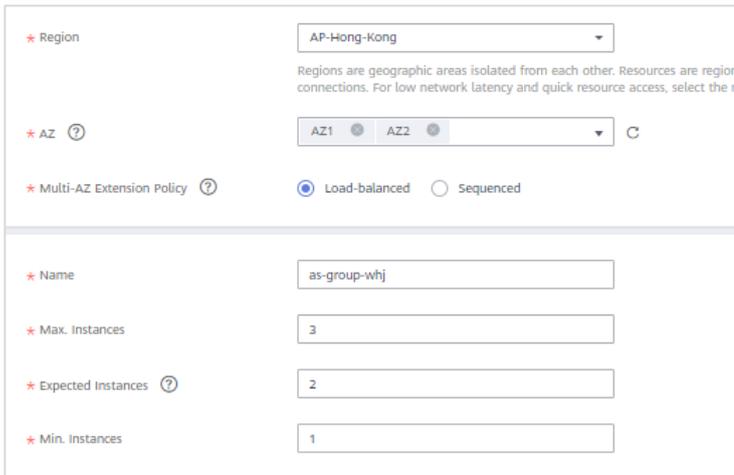


Step 4 Click **Create Now**.



Name	Status	Specifications	Image	System Disk	Data Disks	Login Mode	Created	Billing Mode	Operation
as-config-whj	Unbound	s2.small1 1 vCPU 1 GB	ims-whj	High I/O 40 GB	0	Password	Aug 16, 2020 20:51...	Pay-per-use	Copy Delete

Step 5 Click **Create AS Group**, set the parameters as shown in the following figures, and click **Create Now**.



* Region: AP-Hong-Kong

Regions are geographic areas isolated from each other. Resources are region-connections. For low network latency and quick resource access, select the ne

* AZ: AZ1, AZ2

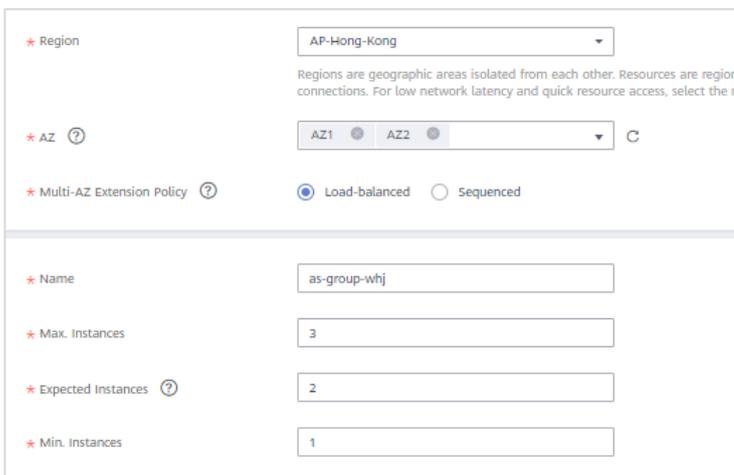
* Multi-AZ Extension Policy: Load-balanced Sequenced

* Name: as-group-whj

* Max. Instances: 3

* Expected Instances: 2

* Min. Instances: 1



* Region: AP-Hong-Kong

Regions are geographic areas isolated from each other. Resources are region-connections. For low network latency and quick resource access, select the ne

* AZ: AZ1, AZ2

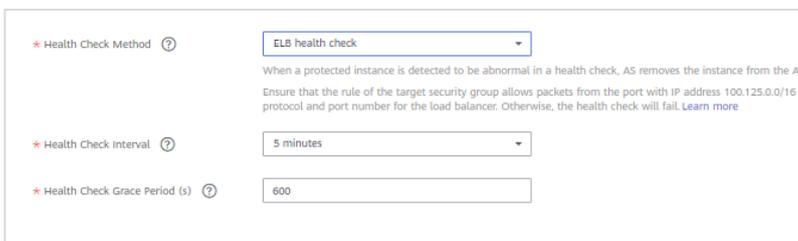
* Multi-AZ Extension Policy: Load-balanced Sequenced

* Name: as-group-whj

* Max. Instances: 3

* Expected Instances: 2

* Min. Instances: 1



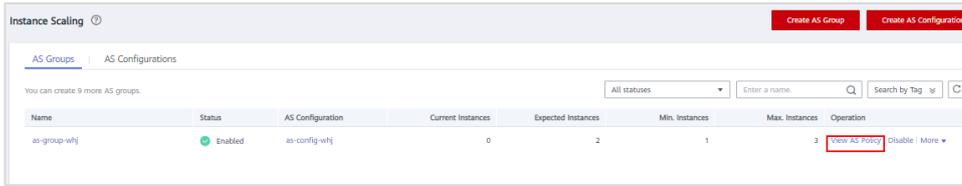
* Health Check Method: ELB health check

When a protected instance is detected to be abnormal in a health check, AS removes the instance from the AS. Ensure that the rule of the target security group allows packets from the port with IP address 100.125.0.0/16 to the instance on the port and protocol and port number for the load balancer. Otherwise, the health check will fail. [Learn more](#)

* Health Check Interval: 5 minutes

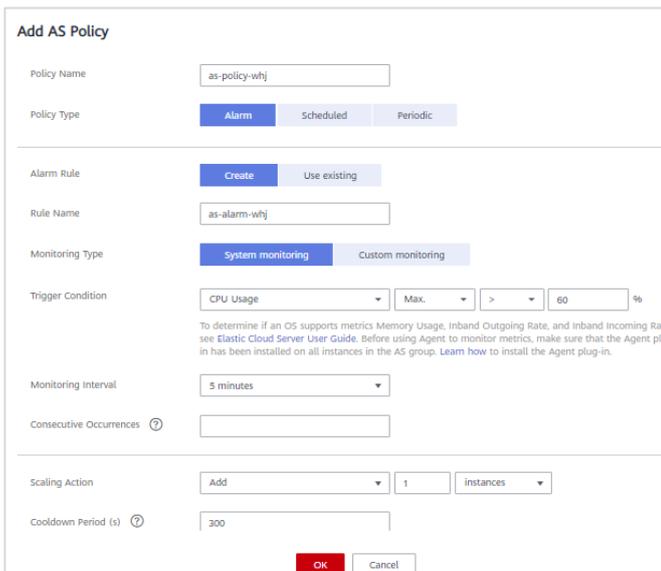
* Health Check Grace Period (s): 600

Step 6 Click **View AS Policy**.



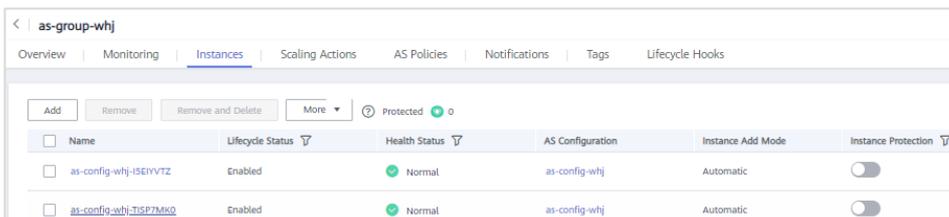
Step 7 Click Add AS Policy.

For example, when **CPU Usage** is greater than or equal to **60**, AS automatically adds 1 instance.



Step 8 Go back to the Instances tab on the AS group page and check whether the number of instances is changed.

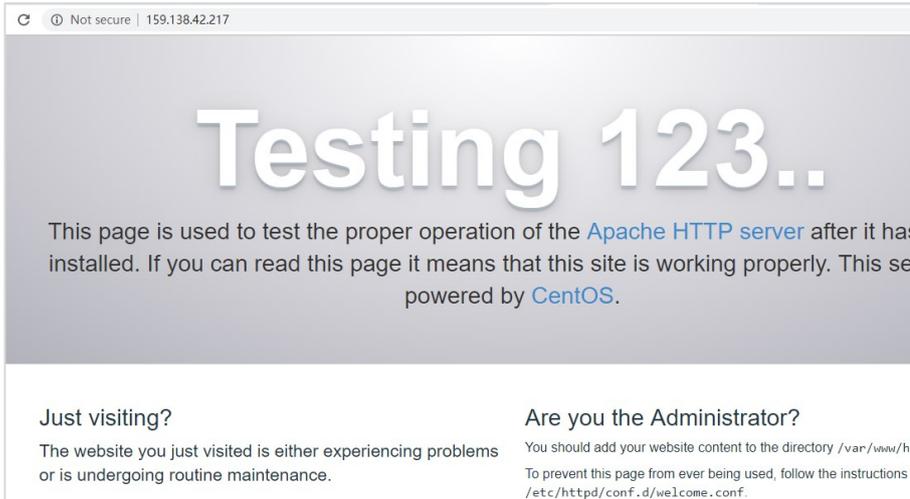
On the **AS Policies** tab on the AS group page, click **Execute Now** in the **Operation** column of the created AS policy to trigger the AS policy.



----End

6.6 Visiting the Website

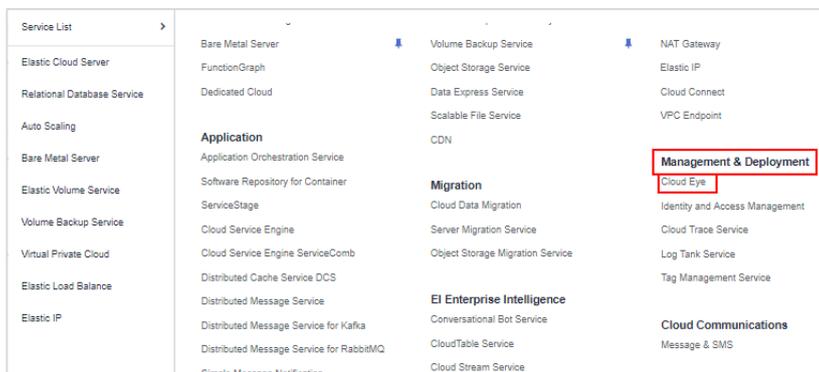
In the address box of the browser, enter **http://EIP bound to the load balancer/Port number** to access the website.



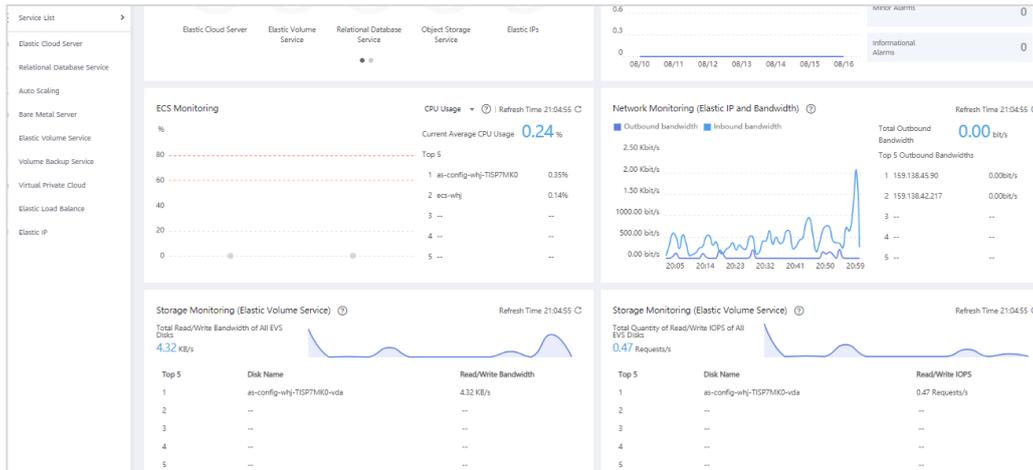
When the preceding page is displayed, server-level HA has been configured.

6.7 Monitoring Resources

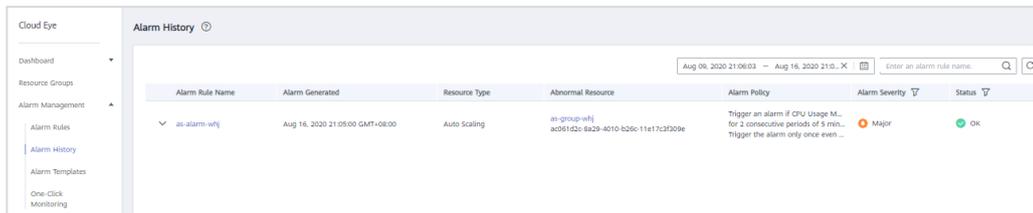
Step 1 Switch back to the management console and choose **Service List > Management & Deployment > Cloud Eye**.



Step 2 View resource usage.



Step 3 In the left navigation pane, choose **Alarm Management > Alarm History** to view alarms and handle them.



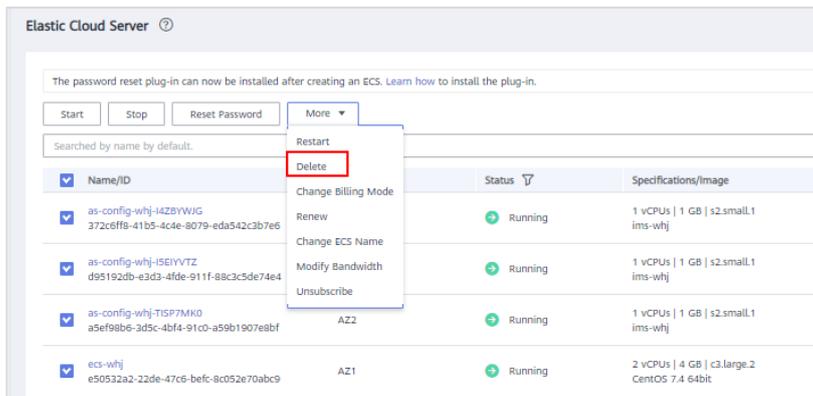
Step 4 In the left navigation pane, click **Server Monitoring** or **Cloud Service Monitoring** to view monitoring information.

Before monitoring an ECS, make sure that the Agent has been installed on the target ECS. For details, see 4.4.1.

----End

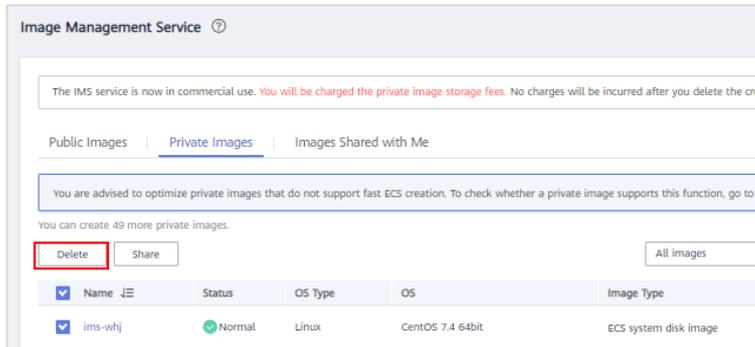
6.8 Deleting Resources

Step 1 Delete the ECSs used in these exercises.



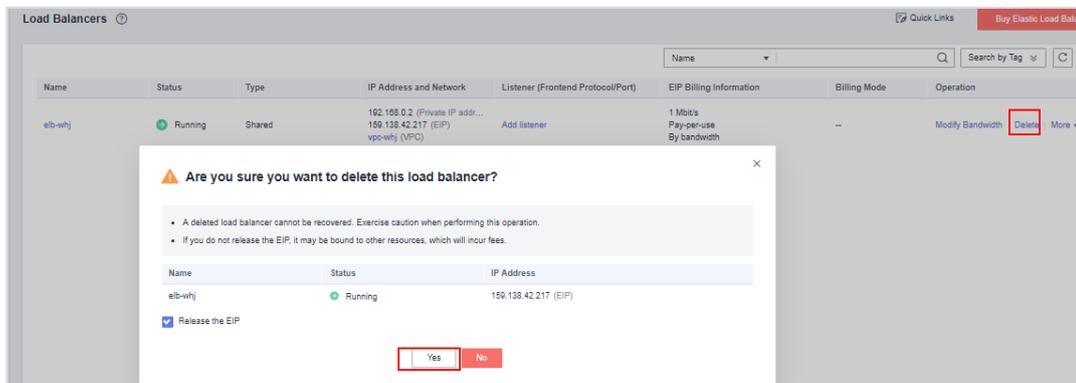


Step 2 Go to the IMS console and delete the private image.



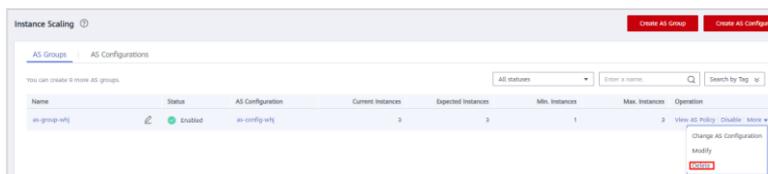
Step 3 Delete the load balancer.

Access the network console, choose **Elastic Load Balance > Load Balancers**, and click **Delete** in the **Operation** column of the target load balancer.



Step 4 Delete AS resources.

- Delete the AS group.



- Delete the AS configuration.



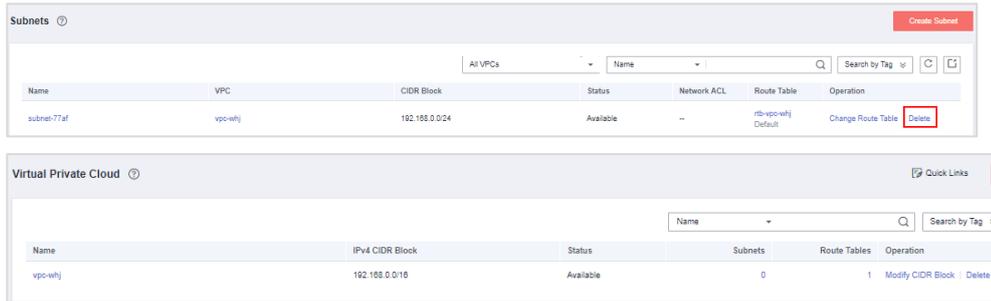
Step 5 Delete VPC resources.



- Delete the security group.



- Delete the subnet and VPC.



Step 6 Go back to the management console, choose **Resources > My Resources** in the upper part of the page, and verify that all the resources you purchased have been deleted.

----End