Huawei Cloud Service Certification Training

HCIA-Cloud Service Lab Guide for Cloud service Engineers

ISSUE:2.0

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2018. 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

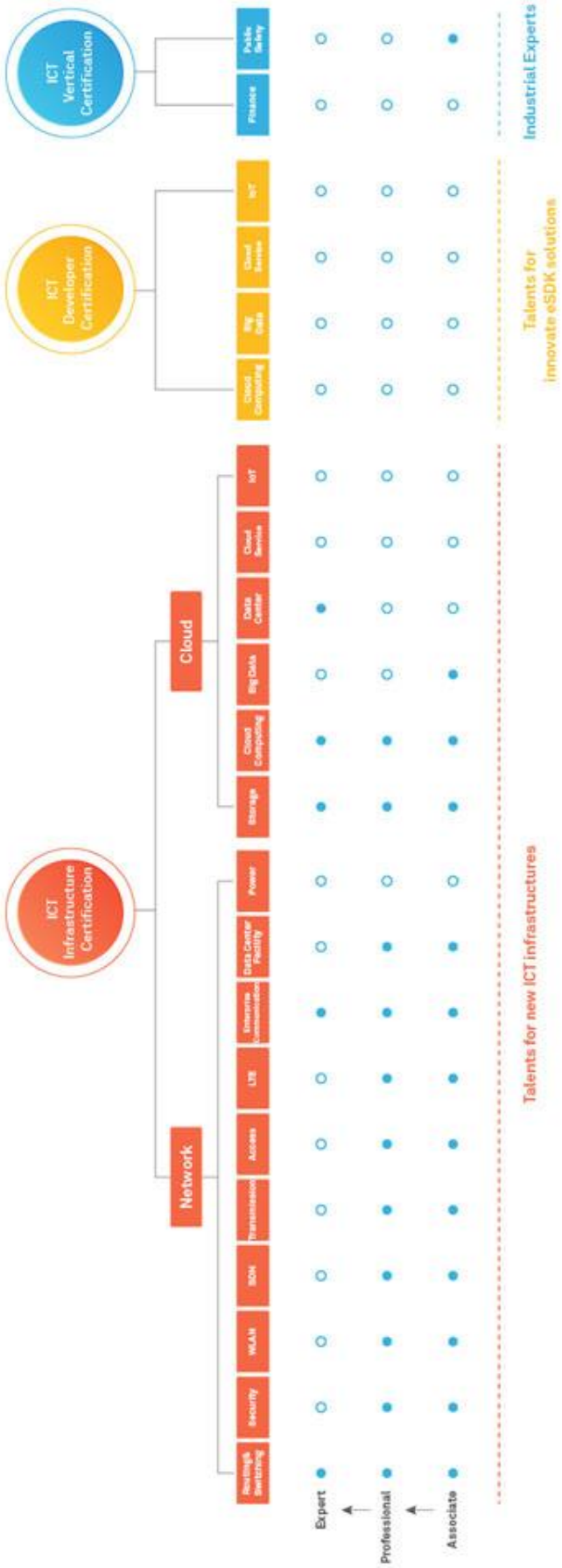
Huawei Certification Program

Relying on the strong technical strength and professional training system, Huawei provides a practical and professional three-level certificate system in the three directions of cloud architects, cloud administrators and cloud developers to meet various customer requirements on different Cloud Service technologies.

HCIA-Cloud Service is an ICT convergence certification, intended for engineers who use Huawei cloud service products and technologies, Huawei internal engineers, Huawei channel engineers, college students, and ICT professionals. HCIA-Cloud Service training covers the basic knowledge and hands-on skills of prevailing public cloud services across IaaS, PaaS, and SaaS. The curriculum includes but is not limited to the following parts: Concept and Value of Cloud Service, Architecture and Ecosystem of Huawei Cloud, Operation/Management/Application of Huawei Cloud Computing Service, Storage Service, Network Service, Security Service, Cloud Eye Service, RDS Service, API Service and EI.

An HCIA-Cloud Service certificate proves that the holder has a comprehensive understanding of prevailing cloud service products and technologies in the marketplace and is capable of independently using various Huawei Cloud service products.

Companies hiring HCIA-Cloud Service V2.0 certified engineers can demonstrate their commitment to public cloud technology and showcase their ability to design, architecture and implement Huawei cloud solutions.


ICT Infrastructure Certification
Network
Cloud
Routing&Switching
Security
WLAN
SDN
Transmission
Access
LTE
Enterprise Communication
Data Center Facility
Power
Storage
Cloud Computing
Big Data
Data Center
Cloud Service
IoT
ICT Developer Certification
Cloud Computing
Big Data
Cloud Service
ICT
ICT Vertical Certification
Finance
Public Safety
Expert
Professional
Associate
Talents for new ICT infrastructures
Talents for innovate eSDK solutions
Industrial Experts
Released
In progress

About This Document

Overview

This document is intended for certification candidates to prepare the HCIA-Cloud Service exam and for trainees to learn cloud service basics, as well as the operation, management, and maintenance of Huawei's cloud service products.

Description

This lab guide consists of thirteen lab exercises, covering basic operation and management of eight mainstream HUAWEI cloud products. Upon completion of these lab exercises, trainees can grasp basic technical skills of major public cloud services across IaaS, PaaS and SaaS.

- Lab 1: This System Management lab introduces the operation of HUAWEI ClOUD website and console.
- Lab 2 and 3: These two cloud computing labs include the basic operation of Elastic Cloud Server and Auto Scaling.
- Lab 4 to 7: Four storage service labs include the basic operation of Elastic Volume Service, Volumn Backup Service, Object Storage Service and Scalable File Service. You will learn how to create, attach/detach and delete different storage systems.
- Lab 8 and 9: Two network service labs include the basic operation of Virtual Private Cloud and Elastic Load Balance. You will learn the operation of VPC and how to load-balance backend ECS.
- Lab 10: This cloud security service lab introduces basic operations of anti-DDoS
- Lab 11: this lab introduces the basic operation for Cloud Eye Service.
- Lab 12: this lab introduces how to use ModelArts and quickly build an AI model with ExeML.
- Lab 13: this lab introduces how to control service requests through the API gateway to ensure service stability.

Background Knowledge Required

- basic network knowledge
- basic storage and server knowledge
- basic knowledge of Windows/Linux

Lab Environment Overview

All lab exercises in this guide are based on production HUAWEI cloud platform, and you can conduct them via the official website: http://www.huaweicloud.com/. Unlike traditional IT labs, there is no-need to buy any physical equipment in advance, instead, you login to huaweicloud.com website and do all exercises pay-as-you-go. We also provide a deep-discounted HCIA lab package for trainees. For more lab information, please enquire your local HALP (Huawei authorized Learning Partner).

When you have any questions during the learning process, you can also go to HUAWEI cloud help center https://intl.huaweicloud.com/.

Contents

About This Document **5**
Overview 5
Description 5
Background Knowledge Required 6
Lab Environment Overview 6
1 System Management **13**
1.1 Introduction 13
1.1.1 About This Lab 13
1.1.2 Objectives 13
1.1.3 List of Lab Tasks 13
1.2 Access the Console 14
1.2.1 Operation Procedures 14
1.2.2 Result Verification 16
1.3 Consult the Console 16
1.3.1 Operation Procedures 16
1.3.2 Result Verification 17
2 Elastic Cloud Server **19**
2.1 Introduction 19
2.1.1 About This Experiment 19
2.1.2 Objectives 19
2.1.3 Planning 19
2.2 Configuration 19
2.2.1 Prerequisites 19
2.2.2 Configuration Roadmap 20
2.2.3 Configuration Process 20
3 Auto Scaling **28**
3.1 Introduction 28

3.1.1 About This Hands-On Exercise 28
3.1.2 Objective 28
3.1.3 Product Description 29
3.1.4 Prerequisites 29
3.1.5 Tasks 29
3.2 Creating an AS Group that Expands Resources at Scheduled Time 31
3.2.1 Procedure 31
3.2.2 Creating an AS Group 31
3.2.3 Creating an AS Configuration 36
3.2.4 Creating an AS Policy 39
3.2.5 Expected Results 42
3.2.6 Verification 42
3.3 Creating a Scheduled Bandwidth Scaling Policy 43
3.3.1 Creating a Bandwidth Scaling Policy 43
3.3.2 Expected Results 46
3.3.3 Verification 46
3.4 Summary 46
3.5 Questions 46
4 Image Management Service 47
4.1 Introduction 47
4.1.1 About This Exercise 47
4.1.2 Objectives 47
4.1.3 Prerequisites 47
4.1.4 Task List 47
4.2 Creating a System Disk Image Using a Windows ECS 49
4.2.1 Configuring a Windows ECS 49
4.2.2 Installing and Configuring Cloudbase-Init 52
4.2.3 Creating a System Disk Image 57
4.3 Modifying Image Attributes 58
4.3.1 Scenarios 58
4.3.2 Procedure 58

4.4 Sharing Images 60
4.4.1 Sharing One or More Images 60
4.4.2 Adding Tenants Who Can Use Shared Images 61
4.4.3 Deleting Tenants Who Can Use Shared Images 62
4.5 Replicating an Image Within a Region 63
4.5.1 Scenarios 63
4.5.2 Restrictions and Limitations 63
4.5.3 Prerequisites 63
4.5.4 Procedure 63
5 Volume Backup Service 65
5.1 Introduction 65
5.1.1 About This Exercise 65
5.1.2 Objective 65
5.1.3 Prerequisites 65
5.1.4 List of Tasks 65
5.2 Performing Basic Operations 66
5.2.1 Creating Backups 66
5.2.2 Deleting Backups 68
5.2.3 Restoring Data from a Backup 70
5.3 Managing Backup Policies 72
5.3.1 Creating a Backup Policy 72
5.3.2 Editing a Backup Policy 73
5.3.3 Associating EVS Disks with a Backup Policy 74
5.3.4 Executing a Backup Policy 75
5.3.5 Viewing Backup Jobs 76
5.3.6 Deleting a Backup Policy 77
6 Object Storage Service 78
6.1 Introduction 78
6.1.1 About This Exercise 78
6.1.2 Objective 78
6.1.3 Service Overview 78

6.1.4 Prerequisites 78
6.1.5 List of Tasks 79
6.2 Preparing the OBS Browser Environment 79
6.2.1 Scenarios 79
6.2.2 Restrictions 79
6.2.3 Subtasks 80
6.3 Using OBS Browser 83
6.3.1 Scenarios 83
6.3.2 Prerequisites 83
6.3.3 Subtasks 84
7 Scalable File Service 90
7.1 About This Exercise 90
7.1.1 Objective 90
7.1.2 Prerequisites 90
7.1.3 List of Tasks 90
7.2 Creating File Systems 91
7.2.1 Creating a File System 91
7.2.2 Creating File Systems in a Batch 93
7.3 Deleting File Systems 93
7.3.1 Deleting a File System 93
7.3.2 Deleting File Systems in a Batch 94
7.4 Mounting a File System on an ECS 95
7.5 Unmounting a File System 99
8 Virtual Private Cloud 101
8.1 Introduction 101
8.1.1 About This Exercise 101
8.1.2 Objectives 101
8.1.3 Prerequisites 101
8.1.4 VPC Service Overview and Topology 102
8.1.5 Task List 102
8.2 Creating a VPC and a Subnet 103

8.3 Creating a Security Group and Adding Rules 104
8.4 Buying an EIP and Binding It to an ECS 105
8.4.1 Scenario 105
8.4.2 Configuration Step 106
8.4.3 Verification 107
8.5 Controlling ECS Access Using a Security Group 108
8.5.1 Scenario 108
8.5.2 Configuration Step 108
8.5.3 Verification 110
9 Elastic Load Balance 111
9.1 Introduction 111
9.1.1 About This Exercise 111
9.1.2 Objective 111
9.1.3 Networking 111
9.1.4 Prerequisites 112
9.1.5 Exercise Planning 112
9.1.6 Task List 113
9.2 Procedure 113
9.2.1 Creating a Load Balancer 113
9.2.2 Adding a Listener 114
9.2.3 Adding Backend Servers 116
9.2.4 Enabling the HTTP Service on Backend Servers 116
9.3 Verification 118
10 Security Service 120
10.1 Introduction 120
10.1.1 About the Exercises 120
10.1.2 Objectives 120
10.1.3 Prerequisites 120
10.1.4 Lists of Tasks 121
10.2 Configuration for Anti-DDoS 121
10.2.1 Enabling Anti-DDoS 121

10.2.2 Enabling Alarm Notifications 122

11 Cloud Eye 125

11.1 Introduction 125

11.1.1 About This Hands-On Exercise 125

11.1.2 Objectives 125

11.1.3 Prerequisites 125

11.1.4 List of Tasks 125

11.2 Tasks 126

11.2.1 Monitoring ECSs 126

11.2.2 Installing and Configuring the Agent (Linux) 132

11.2.3 Setting an AS Policy to Trigger Bandwidth Scaling 137

12 Enterprise Intelligence 141

12.1 ModelArts 141

12.1.1 Introduction 141

12.1.2 Getting Familiar with the ModelArts Management Console 142

12.1.3 Building an AI Model with ExeML from Scratch 145

13 API Gateway Mobile Number Location Lookup 149

13.1 Introduction 149

13.1.1 About This Experiment 149

13.1.2 Objectives 149

13.2 Building a Mobile Number Location Lookup API 149

13.2.1 Opening an API 149

13.2.2 Calling the API 155

13.2.3 Binding a Request Throttling Policy 156

13.2.4 Viewing Metrics 157

1 System Management

1.1 Introduction

1.1.1 About This Lab

Introduction the functions of console, including website login, access to ECS and EVS management page.

1.1.2 Objectives

- Upon completion of this task, you will be able to:
- How to log-onto HUAWEI CLOUD website.
- How to manage the console.
- How to view ECS/EVS management page.

1.1.3 List of Lab Tasks

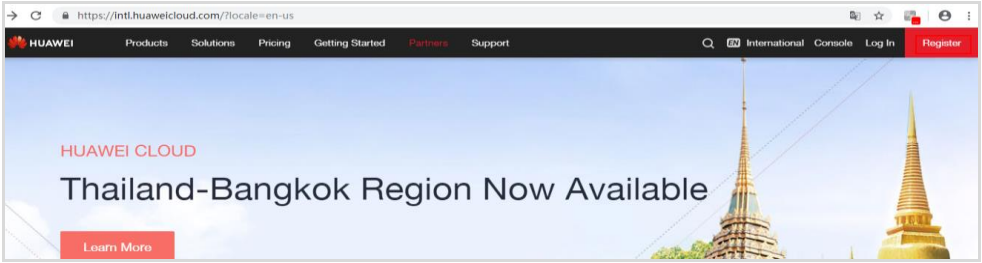
Number	Application scenario	Task	Sub-task
1	After checking the information on the official website of Huawei Enterprise Cloud, access console and save ECS/EVS as frequently used services.	Log into the console	Access Huawei Enterprise Cloud website
			Website registration
			Access console interface
			Save ECS/EVS services (set favorites)
2	View ECS/EVS details.	View ECS/EVS management	Access console interface
			View ECS management

		page.	page
			View EVS management page

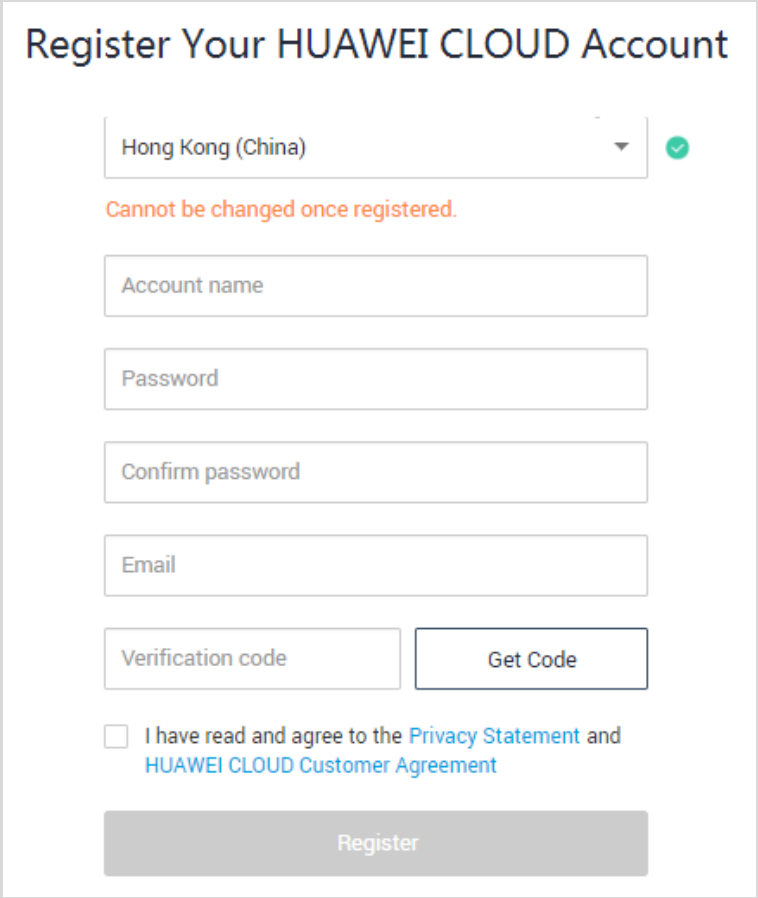
1.2 Access the Console

1.2.1 Operation Procedures (user is created already just read this part)

Step 1 **Access HUAWEI CLOUD website: https://intl.huaweicloud.com/**



Step 2 **Click "Register" on the top-right of the page, as indicated below:**



Step 3 **On the registration page, enter Account name,Password,Confirm password,Email, Verification code.**

Step 4 **I have read and agree to the Privacy Statement and HUAWEI CLOUD Customer Agreement.**

Step 5 **Click "Register".**

Step 6 **After the registration is done, click "console" on the top-right of the page.**

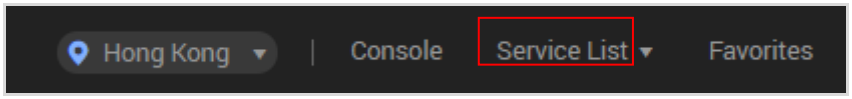
Step 7 **On the login page, fill in the user information and click "login".**

There are two types of user for HUAWEI CLOUD console, please choose the corresponding login method according to actual user type.

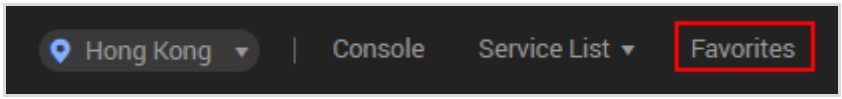
- Individual user please enter user name and password.
- Enterprise multi-tenants please enter user name, email, password and verification code.

Step 8 **Click "log in". Access console.**

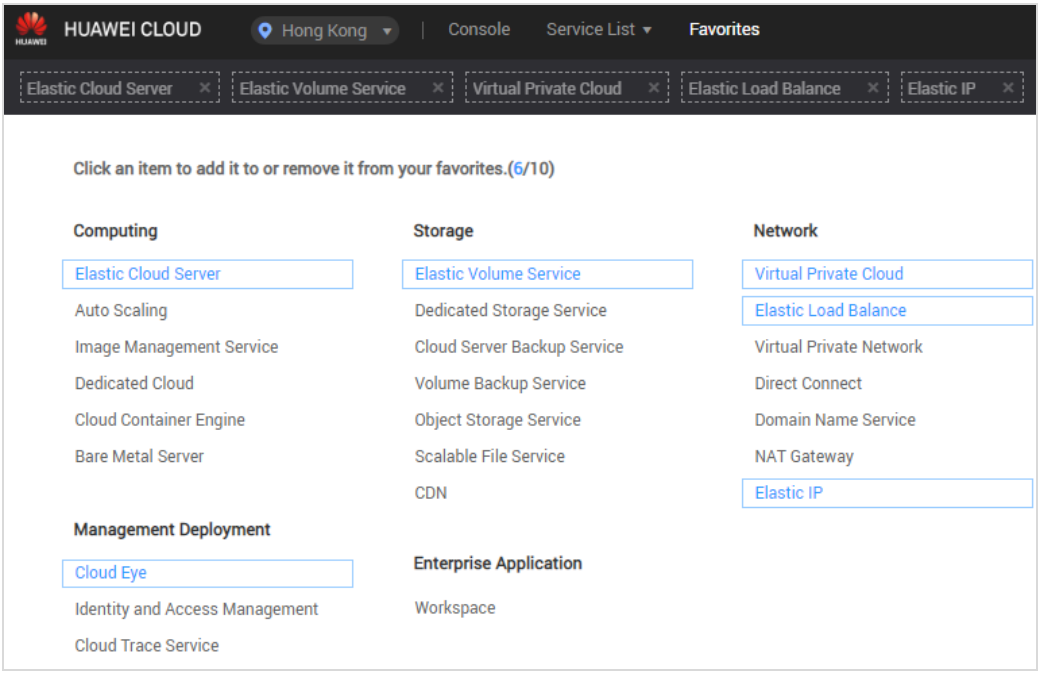
Step 9 **Click "Service List" on the top of the console's home page.**



Step 10 **Click "Favorites" on the top of the console's home page.**

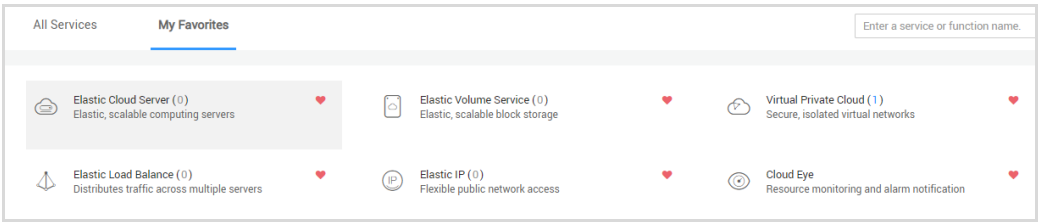


Step 11 **In the expanded List, choose services to be added to "Favorites".**



1.2.2 Result Verification

Click "My Favorites" inside the console to check the favorite services.



1.3 Consult the Console

1.3.1 Operation Procedures

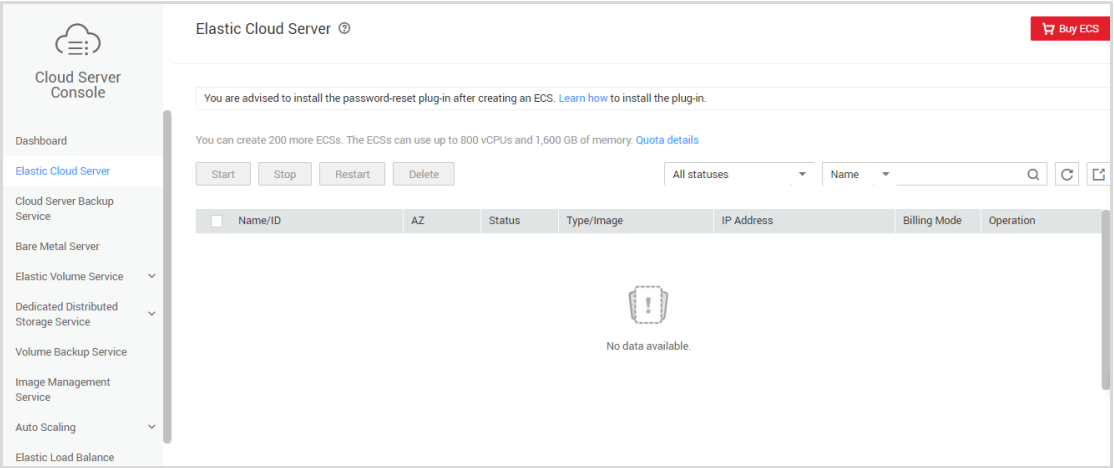
Step 1 **Access HUAWEI CLOUD website: https://intl.huaweicloud.com/**

Step 2 **Click "console" on the top-right of the page.**

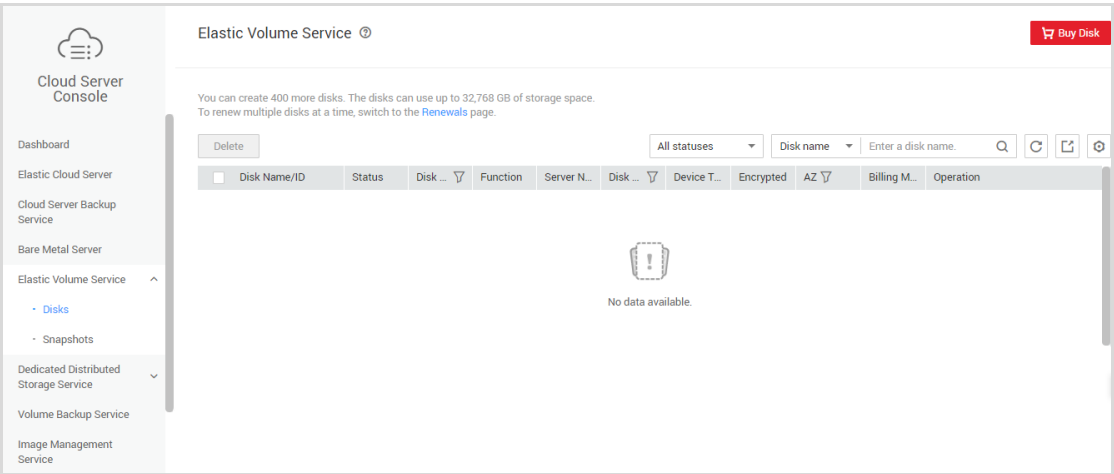
Step 3 **Log into the console.**

Step 4 **Click "log in". Access console.**

Step 5 **Go to "Computing > ECS" on the console's home page. Access ECS management page**

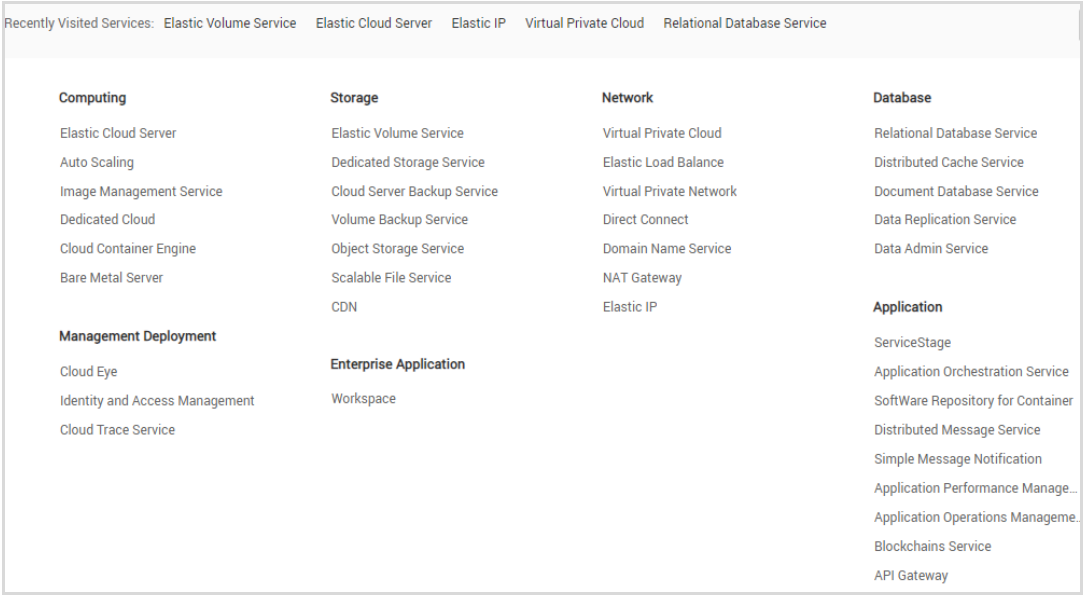


Step 6 **Go to "Storage > EVS" on the console´s home page. Access EVS management page.**



1.3.2 Result Verification

You can view the list of ECS and EVS in your account.


Recently Visited Services: Elastic Volume Service Elastic Cloud Server Elastic IP Virtual Private Cloud Relational Database Service
Computing
Elastic Cloud Server
Auto Scaling
Image Management Service
Dedicated Cloud
Cloud Container Engine
Bare Metal Server
Management Deployment
Cloud Eye
Identity and Access Management
Cloud Trace Service
Storage
Elastic Volume Service
Dedicated Storage Service
Cloud Server Backup Service
Volume Backup Service
Object Storage Service
Scalable File Service
CDN
Enterprise Application
Workspace
Network
Virtual Private Cloud
Elastic Load Balance
Virtual Private Network
Direct Connect
Domain Name Service
NAT Gateway
Elastic IP
Database
Relational Database Service
Distributed Cache Service
Document Database Service
Data Replication Service
Data Admin Service
Application
ServiceStage
Application Orchestration Service
SoftWare Repository for Container
Distributed Message Service
Simple Message Notification
Application Performance Manage...
Application Operations Manageme...
Blockchains Service
API Gateway

2 Elastic Cloud Server

2.1 Introduction

2.1.1 About This Experiment

This document describes basic operations on Elastic Cloud Servers (ECSs).

2.1.2 Objectives

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

- Create an ECS.
- Log in to the ECS.
- Adjust ECS specifications.

2.1.3 Planning

No.	Task	Description
1	Creating an ECS	Create a Linux ECS on HUAWEI CLOUD.
2	Logging In to an ECS	Log in to the ECS using VNC.
3	Modifying ECS Specifications	Modify the ECS specifications if they do not meet service requirements.

2.2 Configuration

2.2.1 Prerequisites

PuTTY has been installed if the target ECS is to be logged in using SSH.

2.2.2 Configuration Roadmap

- Register yourself on HUAEI CLOUD.
- Log in to the management console.
- Purchase a password-authenticated Linux ECS.
- Log in to the ECS using VNC.
- Upgrade the vCPU and memory configuration of the ECS.

2.2.3 Configuration Process

2.2.3.1 Creating an ECS

2.2.3.1.1 Scenarios

ECSs are more cost-effective than physical servers. Within minutes, you can obtain ECS resources from HUAWEI CLOUD. ECS resources are flexible and on-demand. This section describes how to create an ECS.

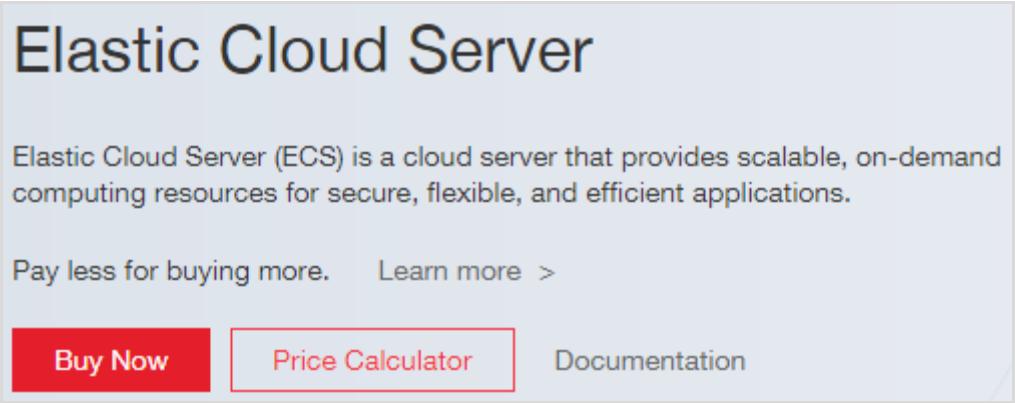
2.2.3.1.2 Procedure

Step 1 **Log in to the HUAWEI CLOUD website** https://intl.huaweicloud.com/

Step 2 **Click Register.**

Enter required information according to the prompts to register an account. Then, log in to HUAWEI CLOUD.

Step 3 **On the HUAWEI CLOUD homepage, click the Products tab. Under Computing, click Elastic Cloud Server. Then, click Buy Now.**



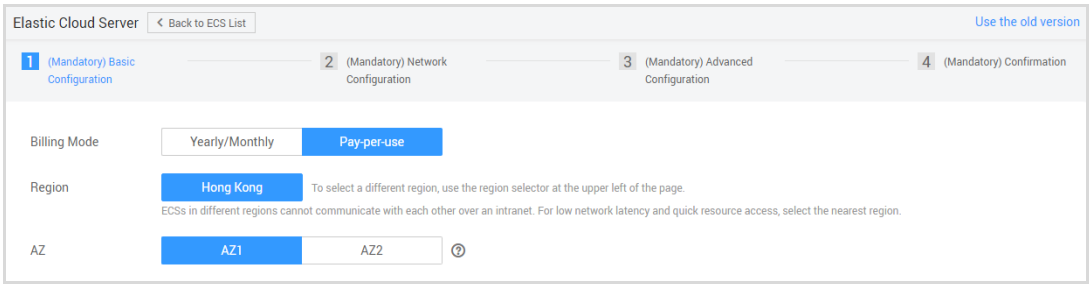
Step 4 **Set ECS parameters.**

Parameter	Example Value

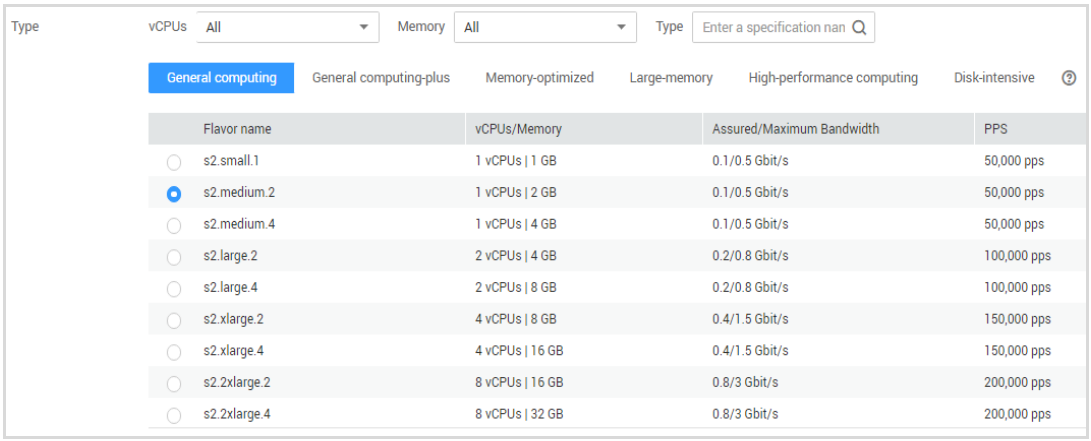
Parameter	Example Value
Billing Mode	Pay-per-use
Region	São Paulo
AZ	AZ1
Type	General computing
vCPUs	1
Memory	2 GB
Image	Public image
OS	CentOS 7.6 64bit
Disk	System disk: ultra-high I/O, 40 GB
VPC	Default
Security Group	Default
NIC	Default
EIP	Automatically assign
Type	Dynamic BGP
Bandwidth Type	Exclusive bandwidth
Billed By	Bandwidth
Bandwidth	5 Mbit/s
Login Mode	Password
Password	Test@123
Advanced Settings	Do not configure
ECS Name	ecs-myserver
Quantity	1

- Perform basic configurations.

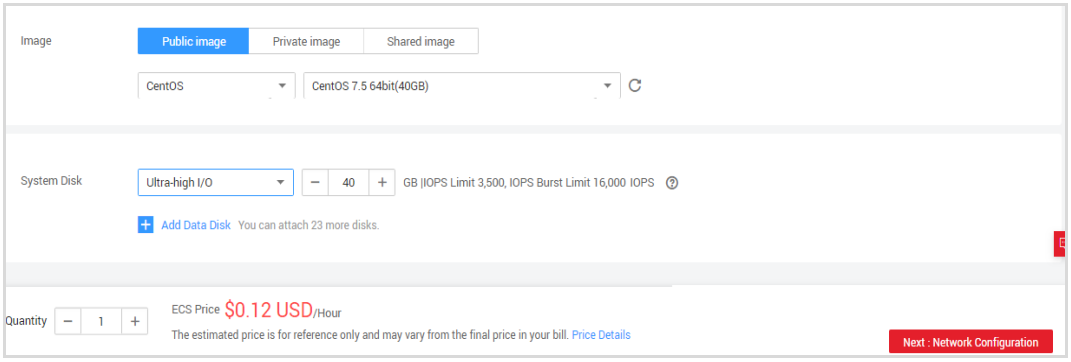
ECSs in different regions cannot communicate with each other over an intranet. For low network latency and quick resource access, select the nearest region.



- When purchasing an ECS, you are not allowed to select sold-out CPU and memory resources.



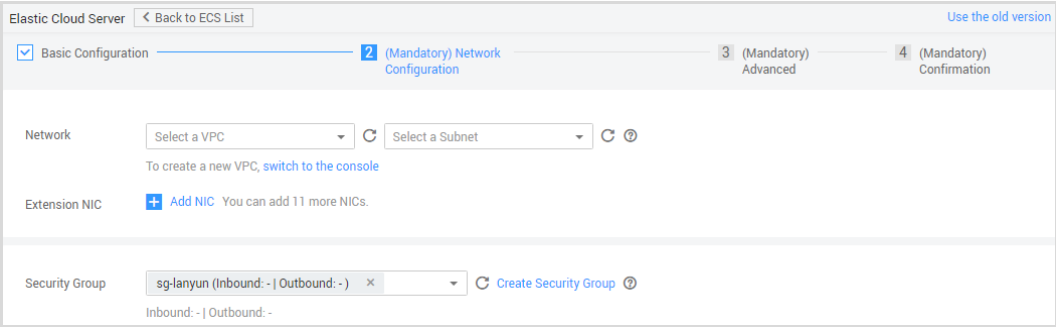
- During ECS creation, you can add up to 24 disks with customized sizes to it. After the ECS is created, you can add up to 60 disks to it.



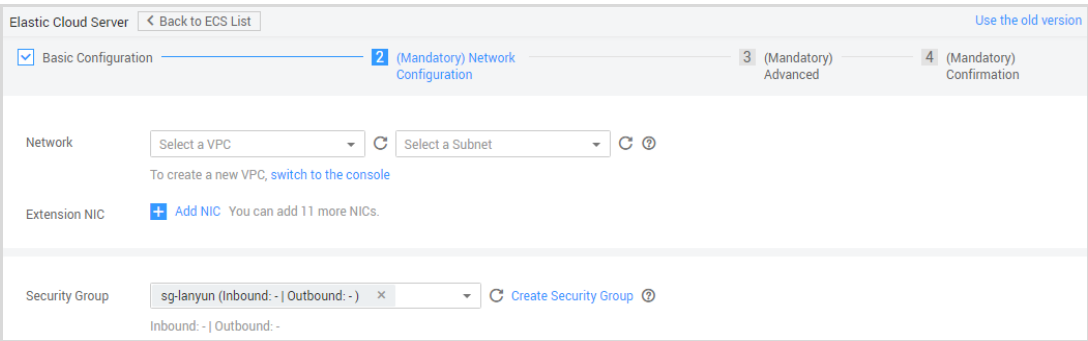
- Perform network configurations.

Step 5 **Click Next: Network Configuration.**

- Set **Network** by selecting an available VPC and subnet from the drop-down list and adding NICs as required.



- When you use VPC for the first time, the system automatically creates a VPC for you, including the security group and NIC.

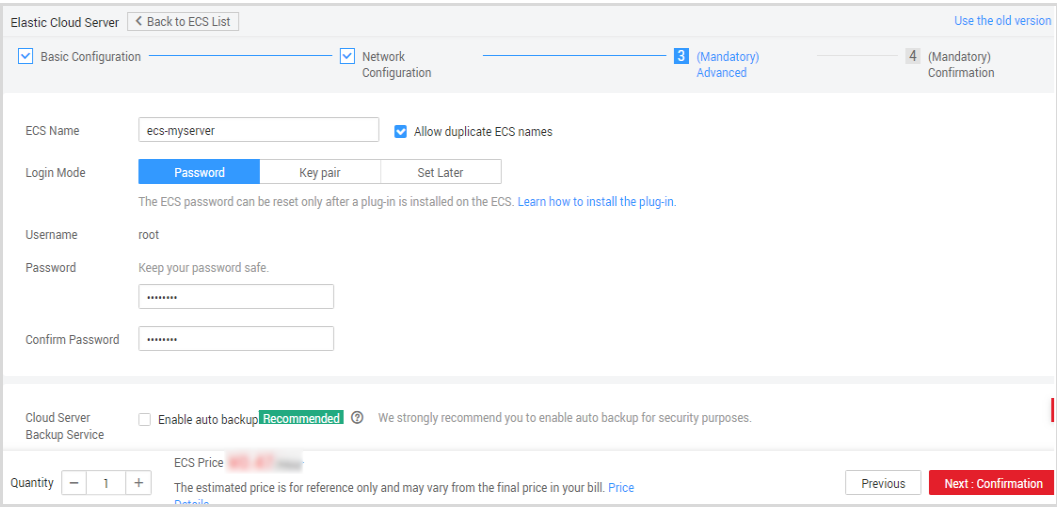


- Perform advanced configurations.

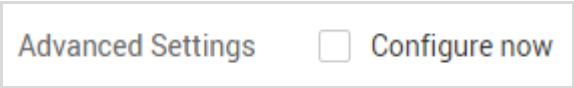
Step 6 **Click Next: Advanced Configuration.**

A key pair or password can be used for authenticating logins. In password authentication, the initial password of user **root** is used for authentication in Linux, while that of user **Administrator** is used for authentication in Windows.

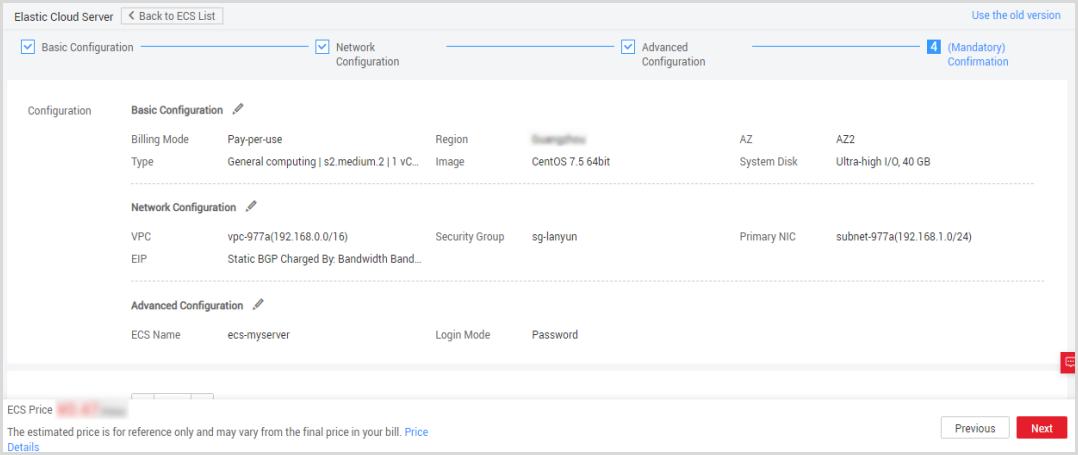
- Set **Login Mode** to **Password** and enter password **Test@123**.
- Set the ECS name and the number of ECSs to be purchased.



- Skip Advanced Settings.



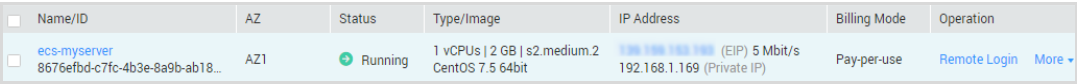
- Confirm the configuration.



Step 7 **Click Next.**

- Agree to the service agreement and click **Submit**.

Step 8 **Switch back to the ECS list and view the created ECS.**



----End

2.2.3.2 Logging In to the ECS

2.2.3.2.1 Scenarios

A Linux ECS can be logged in using either VNC or SSH.

- Logging in to an ECS using VNC

  If no EIP is bound to an ECS, you can remotely log in to the ECS on the management console.

- Logging in to an ECS using SSH

  This method applies only to Linux ECSs. You can use a remote login tool, such as PuTTY (provided for you in a ZIP student file), to log in to the ECS. Ensure that the ECS has an EIP bound.

  This section describes how to use the remote login function (VNC) available on HUAWEI CLOUD to log in to the ECS.

2.2.3.2.2 Prerequisites

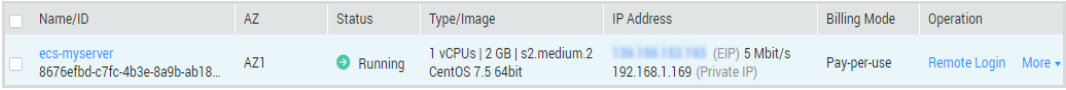
- You can only log in to a running ECS.

2.2.3.2.3 Procedure

Step 1 **Log in to the management console.**

Step 2 **Under Computing, click Elastic Cloud Server.**

Step 3 **In the search box above the upper right corner of the ECS list, enter the ECS name, IP address, or ID, and click .**

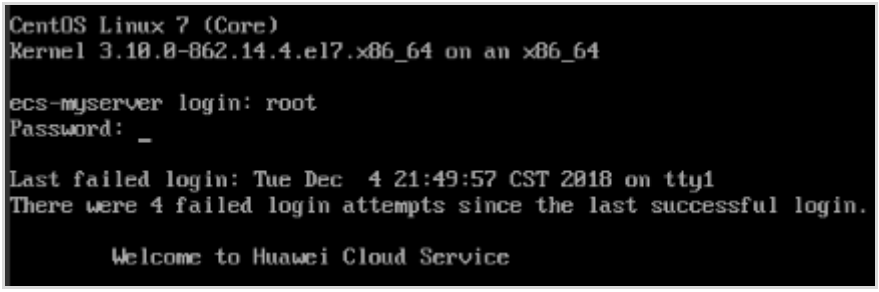


Step 4 **Locate the row containing the ecs-myserver ECS and click Remote Login in the Operation column.**

Step 5 **If the system displays "Press CTRL+ALT+DELETE to log on", click Send CtrlAltDel in the upper right corner of the remote login page to log in to the ECS.**

Step 6 **Enter the account information.**

- Username: **root**
- Password: **Test@123**



----End

2.2.3.3 Modifying ECS Specifications

2.2.3.3.1 Scenarios

If the ECS specifications do not meet service requirements, you can modify the ECS specifications, including vCPUs and memory. Certain ECSs allow you to change their types when you modify their specifications.

2.2.3.3.2 Notes

- When modifying the specifications of an ECS, you are not allowed to select sold-out CPU and memory resources.
- If ECS specifications are downgraded, the ECS performance is deteriorated.

2.2.3.3.3 Procedure

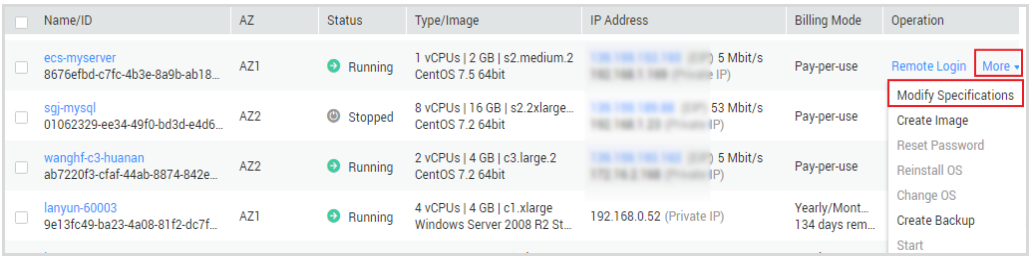
Step 1 **Log in to the management console.**

Step 2 **Under Computing, click Elastic Cloud Server.**

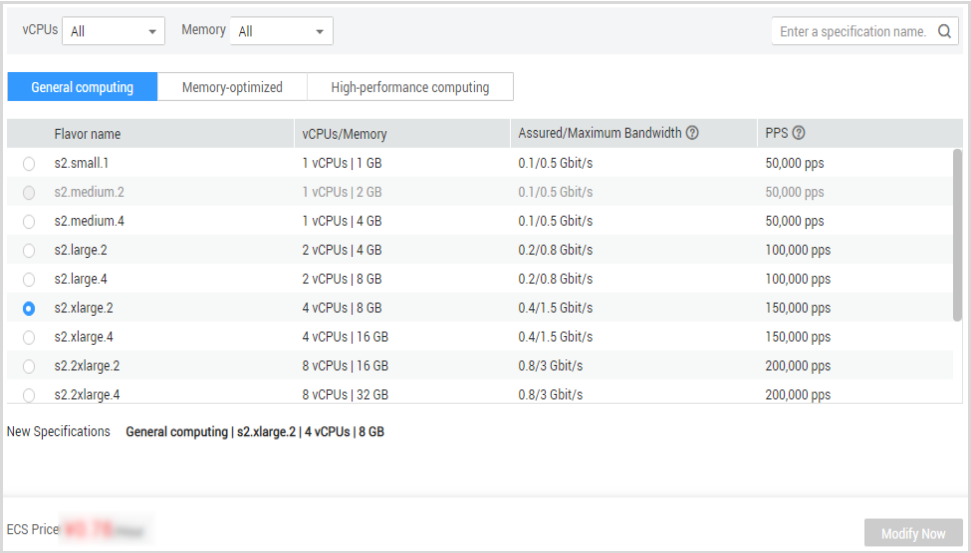
Step 3 **On the Elastic Cloud Server page, check the status of the target ECS.**

Step 4 **Stop ECS and wait for Status Stooped**

Step 5 **Click More in the Operation column and select Modify Specifications.**



Step 6 **Select the new ECS type, vCPUs, and memory as prompted.**



Step 7 **Click Modify Now.**

After the modification, view the modified ECS in the ECS list.

----End

3 Auto Scaling

3.1 Introduction

3.1.1 About This Hands-On Exercise

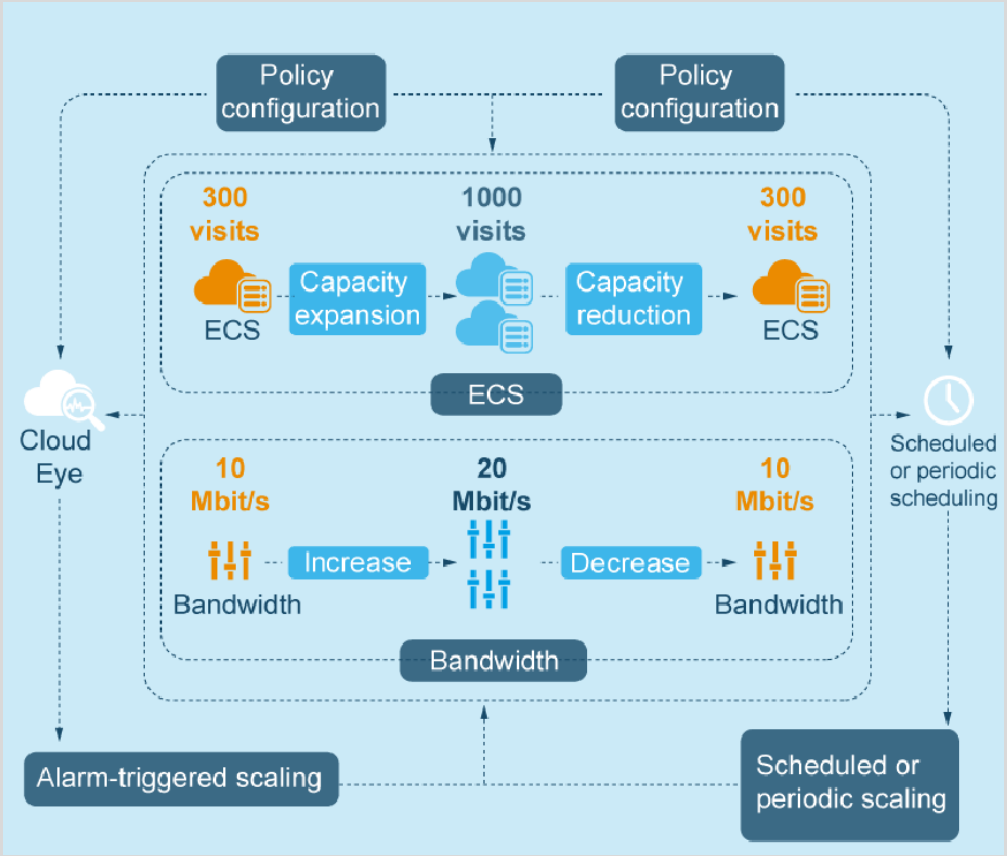
This guide describes how to perform elastic resource scaling, specifically, to automatically adjust the number of instances in an AS group as required, and adjust the public network bandwidth.

3.1.2 Objective

Learn how to:

- Create an AS group and configure the related parameters.
- Create an AS configuration and configure the related parameters.
- Create an AS policy.
- Create an AS bandwidth scaling policy.

3.1.3 Product Description



3.1.4 Prerequisites

- You have obtained the username and password for logging in to the environment.
- The username has available AZs, VPCs, subnets, security group, and ECSs.
- Information about the vCPU, memory, image, and disk of the existing ECSs has been provided for the user.

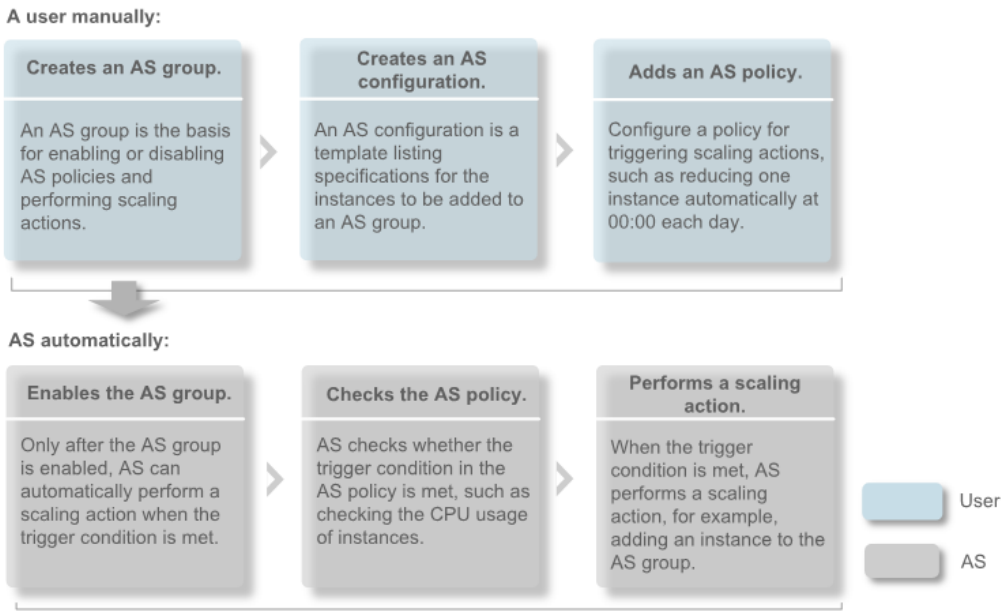
3.1.5 Tasks

No.	Hands-On Exercise Name	Application Scenario	Task	Sub-task
1	Creating an AS group	Visits to a shopping website sharply	Create an AS group	Creating an AS group

No.	Hands-On Exercise Name	Application Scenario	Task	Sub-task
	that expands resources at scheduled time	increase during a fixed period every day. Therefore, ECSs for this website need to be added or deleted accordingly.	so that the number of ECSs in the AS group increases or decreases at scheduled time every day.	Creating an AS configuration
				Creating an AS policy
2	Creating a scheduled bandwidth scaling policy	The public network of a live video website is overloaded every day when a program with a high audience rating is on the show, and video freezing will occur. To resolve this problem, the public network bandwidth must be increased to 10 Mbit/s when the program is on the show.	Create an AS bandwidth scaling policy so that the public network bandwidth will be increased to the target value right before the program with a high audience rating is on the show.	Creating a bandwidth scaling policy

3.2 Creating an AS Group that Expands Resources at Scheduled Time

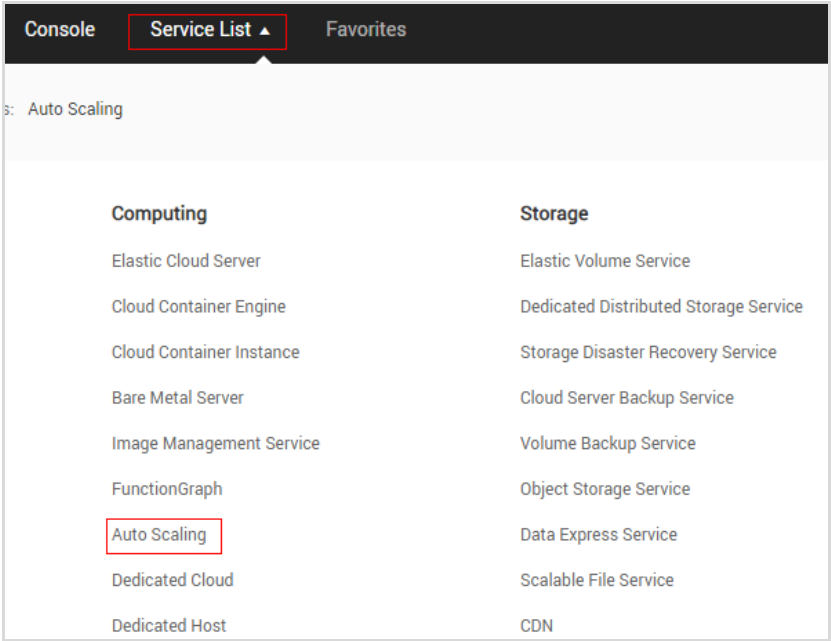
3.2.1 Procedure



3.2.2 Creating an AS Group

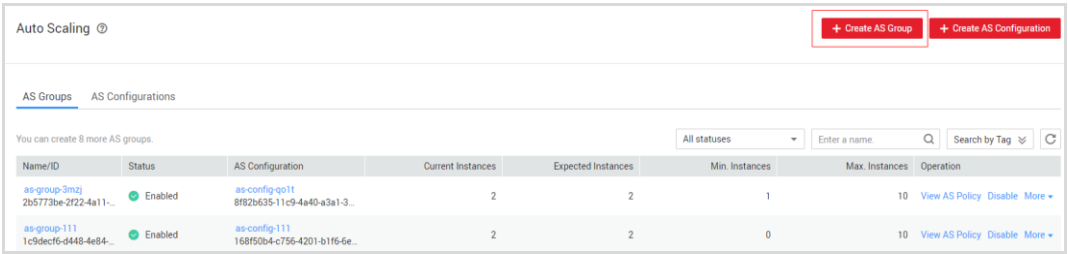
Step 1 **Log in to the management console.**

Step 2 **Choose Service List > Auto Scaling.**

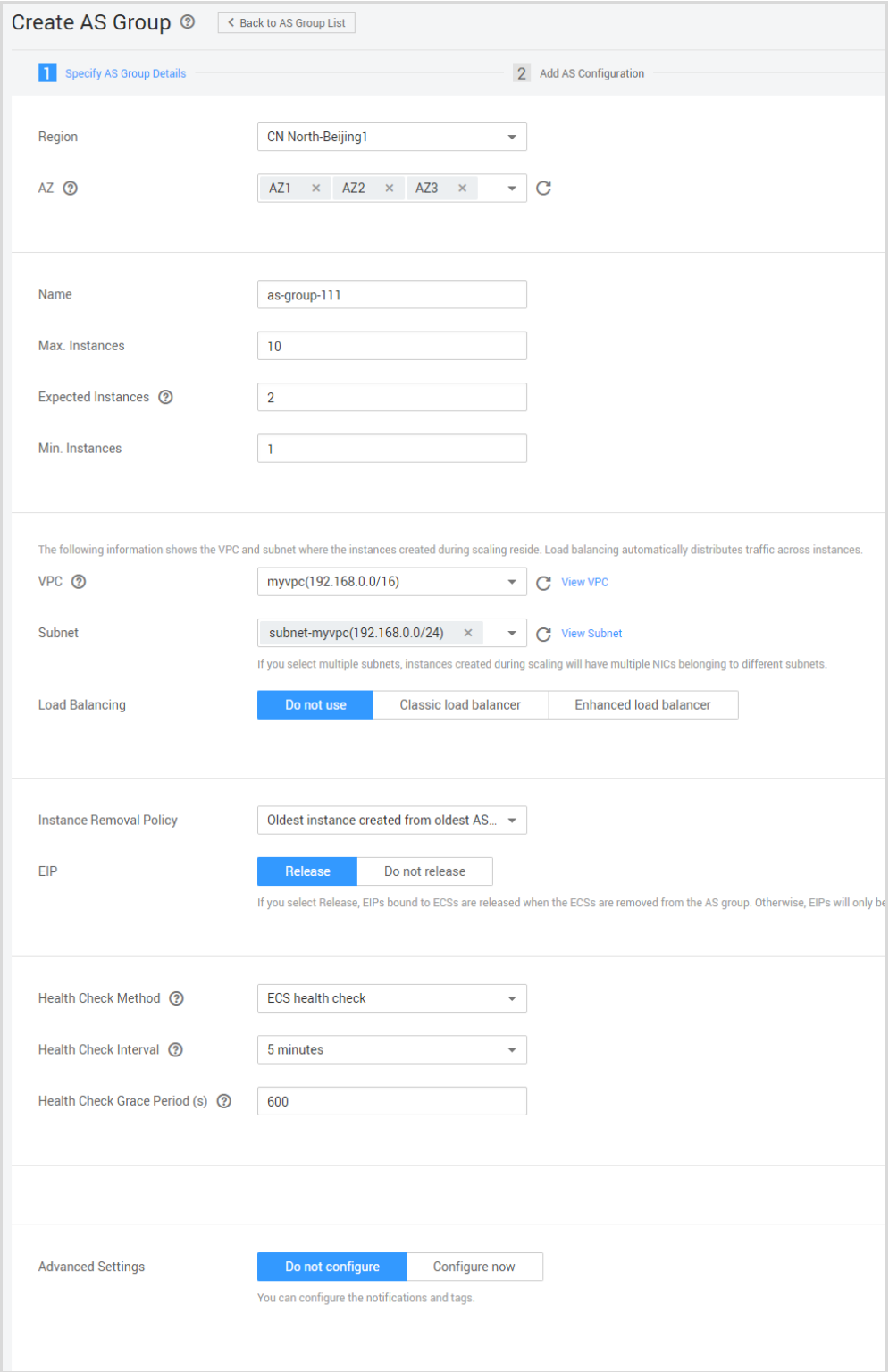


Step 3 **Click Auto Scaling. In the navigation pane on the left, choose Instance Scaling.**

Step 4 **Click Create AS Group.**



Step 5 **Set the parameters as required.**



Parameter	Description	Example Value
Region	Specifies the region where the AS group resides.	Sao Paulo

Parameter	Description	Example Value
AZ	A physical region where resources use independent power supplies and networks. AZs are physically isolated but interconnected through an internal network. To enhance application availability, the system evenly distributes your ECSs to AZs if multiple AZs have been selected.	AZ1, AZ2, AZ3
Name	Specifies the name of the AS group to be created. The name contains 1 to 64 characters and consists of only letters, digits, underscores (_), and hyphens (-).	as-group-111
Max. Instances or Min. Instances	Specifies the maximum or minimum number of instances in an AS group.	**10** max **1 min**
Expected Instances	Specifies the expected number of ECS instances in an AS group.	2
VPC	Specifies the VPC of the ECS network. Select the target VPC from the drop-down list.	None
Subnet	Select a subnet.	None
Load Balancing	This parameter is optional. A load balancer automatically distributes access traffic to all ECSs in an AS group to balance their service load. It enables higher levels of fault tolerance in your applications and expands application service capabilities.	Do not use

Parameter	Description	Example Value
Instance Removal Policy	Specifies the priority for removing an ECS instance. If required conditions are met, scaling actions are triggered to remove instances.	Oldest instance created from oldest AS configuration
EIP	If the AS configuration of an AS group uses an EIP, the system binds the EIP to the newly created ECS instance when the scaling action is performed. If you select **Release**, the EIP bound to the ECS instance is released when the instance is removed from the AS group. Otherwise, the system reserves the EIP.	Release
Health Check Method	Once the health check detects a faulty ECS, the system removes the faulty ECS from the AS group and adds a new one. The health check is implemented using any of the following methods: **ECS health check**: checks the ECS running status. If an ECS is stopped or deleted, it is considered as abnormal. **ELB health check**: determines ECS running status based on the health check result obtained using ELB.	ECS health check
Health Check Interval	Specifies the health check period for an AS group. You can set a proper health check interval, such as 10 seconds, 1 minute, 5 minutes, 15 minutes, 1 hour, and 3 hours based on the site requirements.	5 minutes

Parameter	Description	Example Value
Health Check Grace Period (s)	Specifies the grace period for instance health check. The unit is second and value range is 0 to 86,400. The default value is **600**.	600
Advanced Settings	Configure notifications and tags. You can select **Do not configure** or **Configure now**.	Do not configure

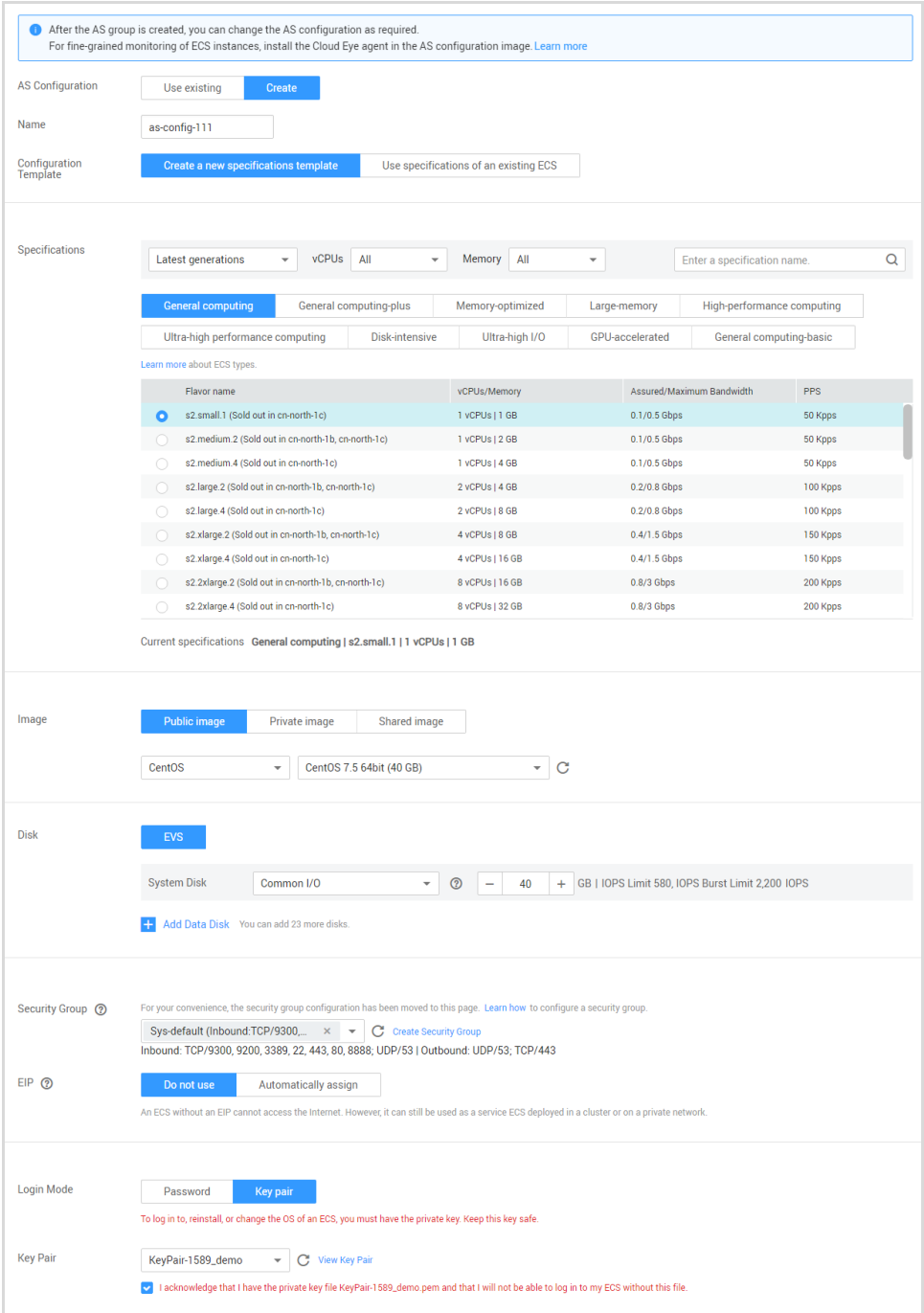
Step 6 **After the configuration, click Next.**

----End

3.2.3 Creating an AS Configuration

Step 1 **On the Create AS Group page, at AS Configuration box choose Create**

Step 2 **Set the parameters as required.**



Parameter	Description	Example Value
Name	Specifies the name of an AS configuration.	as-config-111
Configuration Template	Select an AS configuration template. If an ECS already exists, select **Use specifications of an existing ECS**. If you need to	Create a new specifications template

Parameter	Description	Example Value
	create a specifications template, click **Create a new specifications template** and configure the parameters, such as the ECS type, **vCPUs**, **Memory**, **Image**, and **Disk** to create an AS configuration.	
Specifications	The public cloud provides various ECS types for you to select based on application scenarios.	General computing
Image	Select the image used to create an ECS.	Public image, CentOS, CentOS 7.6 64bit (40 GB)
Disk	Includes the system disk and data disk. You can select **EVS**.	Select **Common I/O** for **System Disk**.
Security Group	Controls ECS access within or between logical groups by defining access rules.	Select the default security group.
EIP	Specifies a static public IP address bound to an ECS in a VPC. Using the EIP, the ECS provides services externally.	Do not use
Login Mode	An ECS can be authorized using a key pair or password. **Key pair**: You can use a key pair for login authentication. If you select this mode, create or import a key pair on the **Key Pair** page. **Password**: The initial password of user **root** (for Linux) or user **Administrator** (for Windows) is used for authentication. You can	Key Pair

Parameter	Description	Example Value
	log in to an ECS using the username and its initial password.	
Advanced Settings	This parameter allows you to configure **File Injection**, **User Data Injection**, and **ECS Group**. You can select **Do not configure** or **Configure now**.	Do not configure

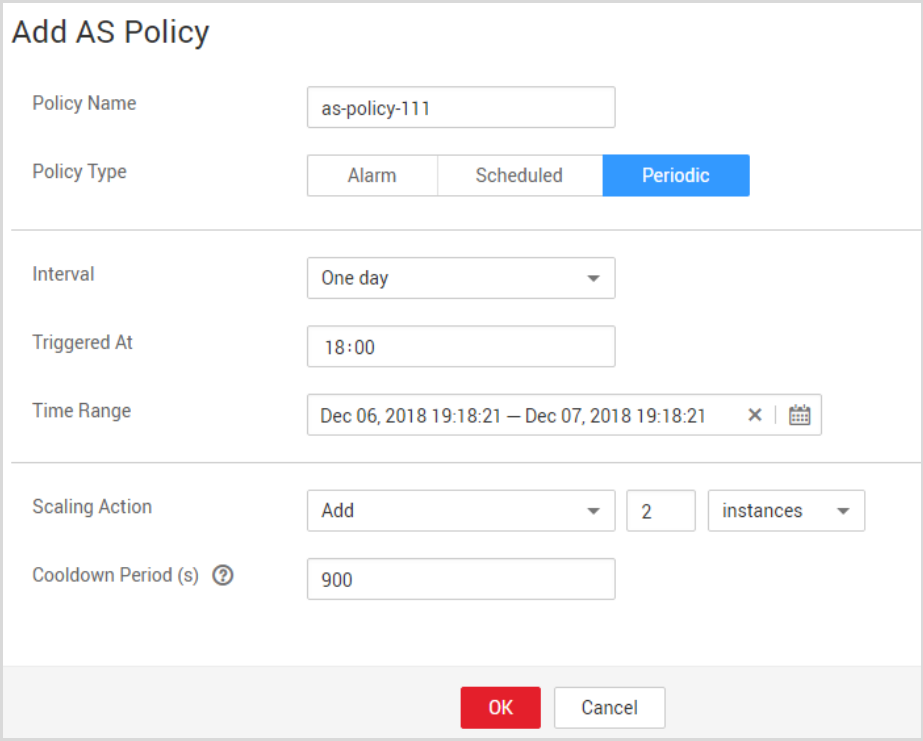
Step 3 **After the configuration, click Next.**

----End

3.2.4 Creating an AS Policy

Step 1 **On the Create AS Group page, click Add AS Policy.**

Step 2 **On the Add AS Policy page, configure the AS policy parameters. In the following example, an AS policy that two instances are added at the scheduled time every day is created.**

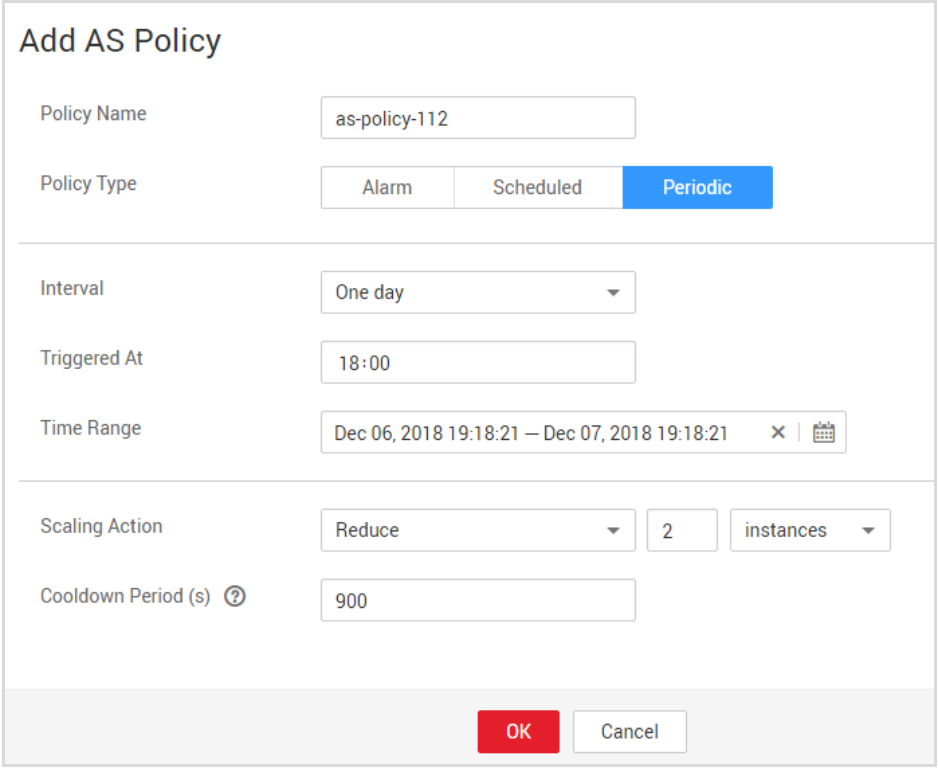


Parameter	Description	Example Value
Policy Name	Specifies the name of an AS policy.	as-policy-111
Policy Type	You can set Policy Type to Alarm, Scheduled, or Periodic. Based on the excise scenario requirement, the instances need to be added and deleted at scheduled time. Therefore, select Periodic. Adding and deleting instances require one AS policy each. In the following procedure, the AS policy for adding instances (AS policy 1) is added first.	Periodic
Interval	Specifies the repetition period of the periodic policy. Select One day.	One day
Triggered At	Specifies the time when the AS policy is triggered.	Set near time to see working at the lab
Time Range	Specifies the time range during which the AS policy takes effect.	Retain the default value.
Scaling Action	Specifies an action and the expected number of instances. In this scenario, two instances need to be added. Adjust the number of instances based on site requirements.	Add, 2
Cooldown Period (s)	Indicates the period of time after each a scaling action is complete.	900

Step 3 **Click OK.**

Step 4 **On the Create AS Group page, click Add AS Policy to create another AS policy (AS policy 2).**

Step 5 **On the Add AS Policy page, configure the AS policy parameters as the following figure shows. This AS policy is used to delete two instances at the scheduled time every day. Ensure to select Reduce 2 for Scaling Action.**



Step 6 **Click OK.**

Step 7 **Then, click Create Now.**

Step 8 **On the Details page, confirm the parameter configuration and then click Submit.**

Step 9 **Click Back to AS Group List.**

----End

Edit expected instances setting 3 instances plus and verify the results

Edit expected instances setting 2 instances minus and verify the results

Manually remove all instances (use ecs menu) and verify the results after a few minutes

Manually add 2 instances (use AS instance Add or policy submenu Execute now) and verify the results after a few minutes

3.2.5 Expected Results

Based on the configuration of expected instances and AS policies, the following actions are expected to be performed for the AS group:

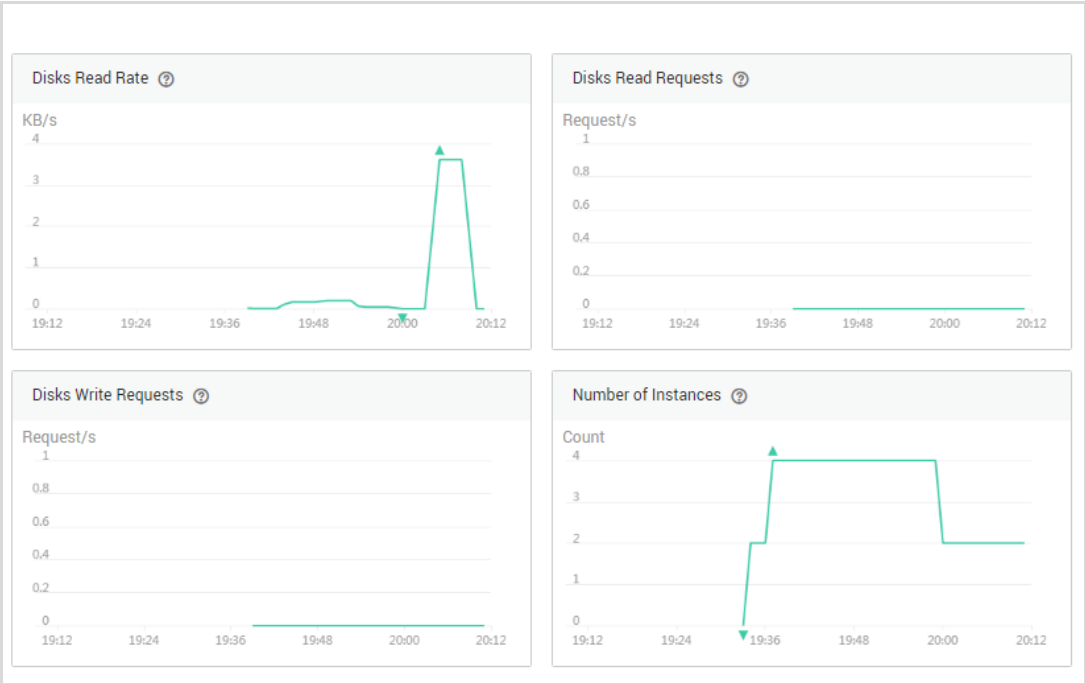
- Two instances are added to the AS group, which is triggered by the configuration of expected instances (2).
- Two instances are added to the AS group, which is triggered by the AS policy 1.
- Two instances are deleted from the AS group, which is triggered by the AS policy 2.

3.2.6 Verification

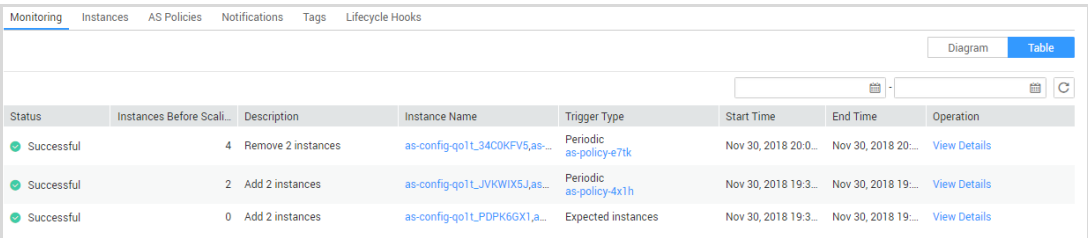
Step 1 **Wait till the triggering time of both the two AS policies passes.**

Step 2 **Click the name of the created AS group to switch to the AS group details page.**

Step 3 **In the Monitoring tab, view the instance changes triggered by the two periodic AS policies. The number of instances changes during the time ranges of the two periodic AS policies each day.**



Step 4 **Click Table in the upper right corner of the Monitoring tab to view scaling action records of the AS group. As the following figure shows, the scaling actions of the AS group are as expected, and the instances are added and deleted periodically.**



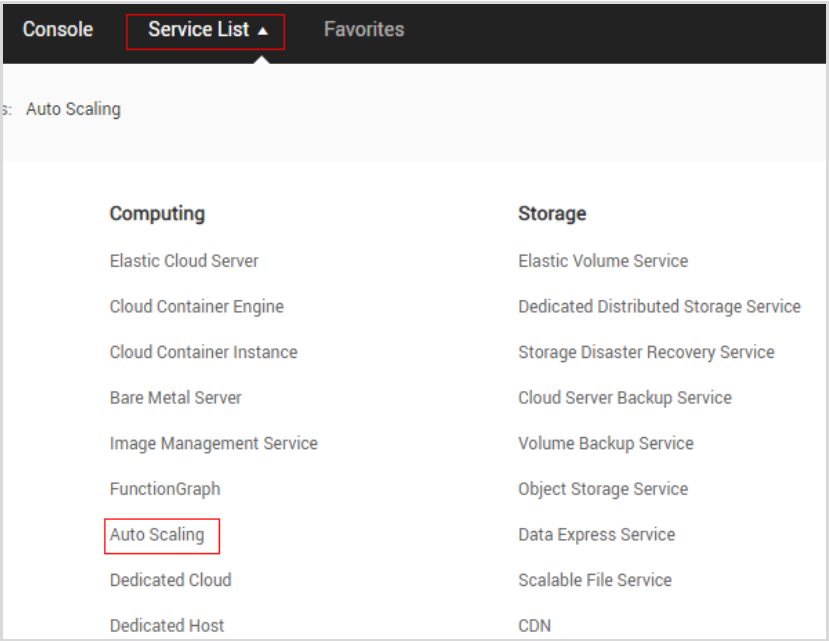
----End

3.3 Creating a Scheduled Bandwidth Scaling Policy

3.3.1 Creating a Bandwidth Scaling Policy

Step 1 **Log in to the management console.**

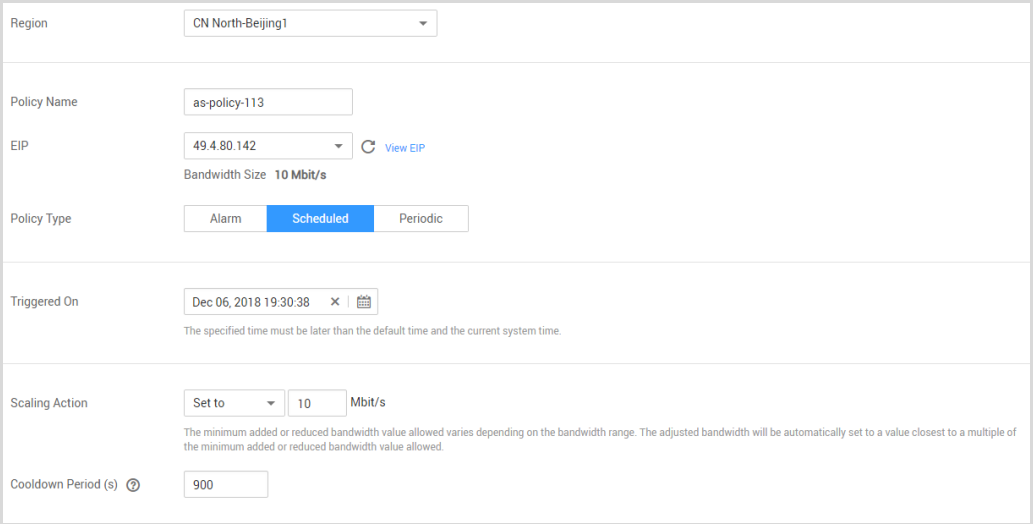
Step 2 **Choose Service List > Auto Scaling.**



Step 3 **Click Auto Scaling. In the navigation pane on the left, choose Bandwidth Scaling.**

Step 4 **Click Create Bandwidth Scaling Policy.**

Step 5 **Configure the parameters, such as Policy Name, EIP, Policy Type, and Trigger Condition.**



Parameter	Description	Example Value
~~Region~~	~~Specifies the region where the AS group resides.~~	~~Sao Paulo~~
Policy	Specifies the name of the	as-policy-113

Parameter	Description	Example Value
Name	bandwidth scaling policy. The name consists of only letters, digits, underscores (_), and hyphens (-).	
EIP	Specifies the public network IP address whose bandwidth needs to be scaled.	None
Policy Type	The value can be **Alarm**, **Scheduled**, or **Periodic**.	Scheduled
Triggered On	Specifies the time when the AS policy is triggered.	None
Scaling Action	Specifies the action in a scaling action. The following AS action options are available: Add When a scaling action is triggered, the bandwidth is increased. Reduce When a scaling action is triggered, the bandwidth is decreased. Set to The bandwidth is set to a fixed value.	Set to 2 Mbit/s
Cooldown Period (s)	Indicates the period of time after each a scaling action is complete.	900

Step 6 **Then, click Create Now.**

----End

3.3.2 Expected Results

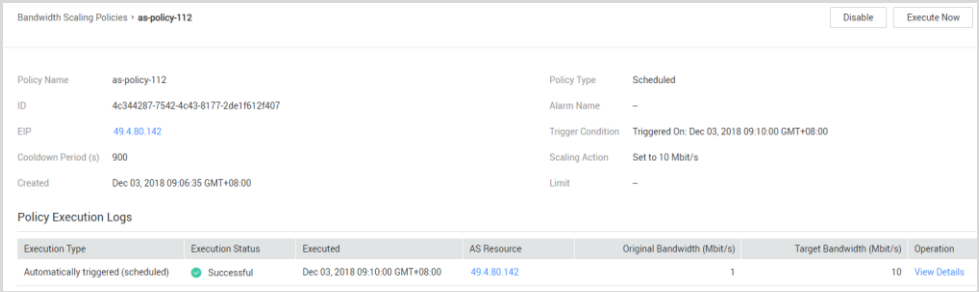
The public network bandwidth is increased to 10 Mbit/s at the preset triggering time.

3.3.3 Verification

Step 1 **Wait till the triggering time of the bandwidth scaling policy passes.**

Step 2 **On the Bandwidth Scaling page, click the new bandwidth scaling policy name to switch to the bandwidth scaling policy details page.**

Step 3 **On the Policy Execution Logs page, view the policy execution records. The public network bandwidth is increased to 2 Mbit/s after the scaling action is triggered as expected.**



----End

3.4 Summary

- The key step in these two hands-on exercises is to determine the target policy type and number of policies.
- When you create an AS group that expands resources at scheduled time, be aware that an AS action can be triggered when the configured policy condition is met and when the number of expected instances is different from the current number of instances.

3.5 Questions

- Can different types of AS policies be enabled for one AS group?
- Can instances that have been added based on an AS policy be automatically deleted when they are not required?

4 Image Management Service

4.1 Introduction

4.1.1 About This Exercise

This exercise describes some basic operations of Image Management Service (IMS).

4.1.2 Objectives

With this exercise, you can master basic operations of IMS. The details are as follows:

- Create a system disk image using a Windows ECS.
- Modify image attributes.
- Share images.
- Replicate images.

4.1.3 Prerequisites

You have registered a HUAWEI CLOUD account.

4.1.4 Task List

SN	Task	Subtask	Application Scenario
1	Create a system disk image using a Windows ECS.	Configure a Windows ECS.	Before you use a Windows ECS to create an image, you must enable DHCP on its NICs.
		Check whether Cloudbase-Init has been installed on the ECS.	To ensure that a new ECS created using a private image can be customized (for example, changing the

SN	Task	Subtask	Application Scenario
			ECS password), install Cloudbase-Init before creating the private image.
		Create a system disk image.	Create an image using the Windows ECS.
2	Modify image attributes.	Modify the name, description, minimum and maximum memory, or NIC multi-queue of a private image.	Only private images in **Normal** state can be modified. You can modify the name, description, minimum memory, or NIC multi-queue of a private image.
3	Share images.	Share specified images.	After obtaining the project ID from user B, user A can share a specified private image with user B.
		Add or delete a tenant who can use shared images.	You can add or delete a tenant who can use shared images.
4	Replicate images.	Replicate images within a region.	You can use the image replication function to convert an encrypted to an unencrypted image, or the other way around.

4.2 Creating a System Disk Image Using a Windows ECS

4.2.1 Configuring a Windows ECS

4.2.1.1 Scenarios

- If the Windows ECS that will be used to create a private image is using a static IP address, configure the ECS NIC to obtain an IP address using DHCP.

  Windows Server 2008 R2 is used as an example to describe how to configure DHCP. For details, see Configuring DHCP for NICs. For how to configure DHCP on ECSs running other OSs, see relevant OS documentation.

- You need to enable Remote Desktop Connections if you want to connect to the ECS using Remote Desktop later.

  For details, see (Optional) Enabling the Remote Desktop Connection.

4.2.1.2 Prerequisites

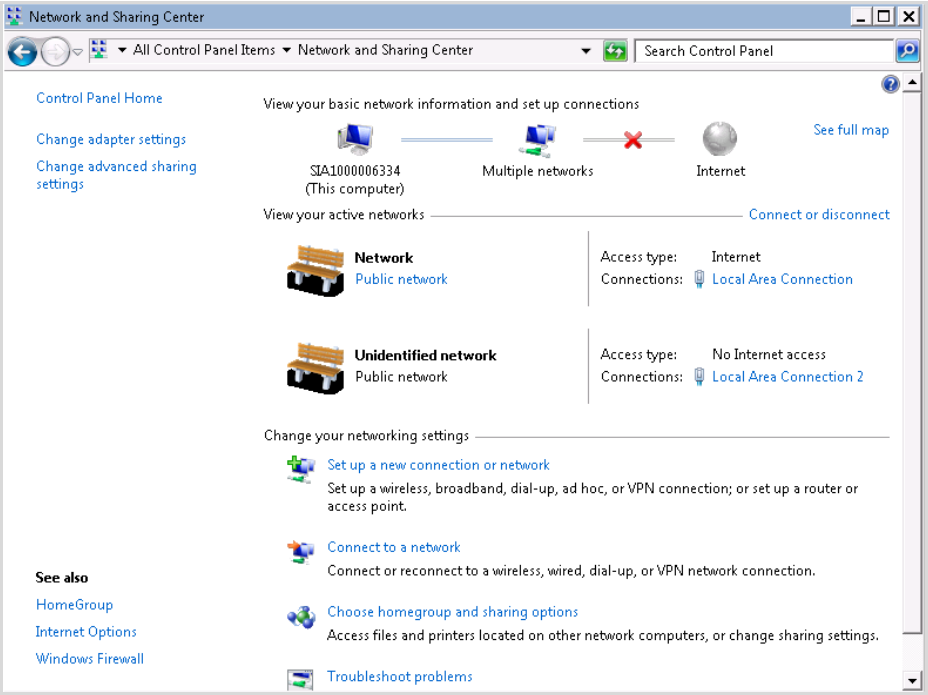
You have logged in to the ECS that will be used to create the private Windows image.

4.2.1.3 Configuring DHCP for NICs

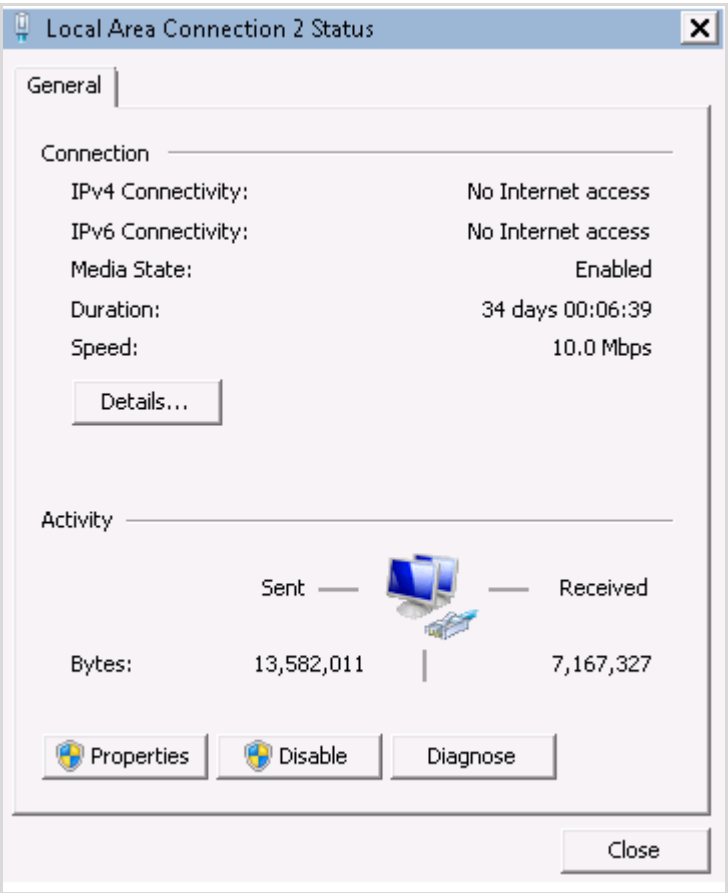
Step 1 **Choose Start > Control Panel.**

Step 2 **Click Network and Internet Connections.**

Step 3 **Click Network and Sharing Center.**



Step 4 **Select the connection using the static IP address. For example, click Local Area Connection 2.**

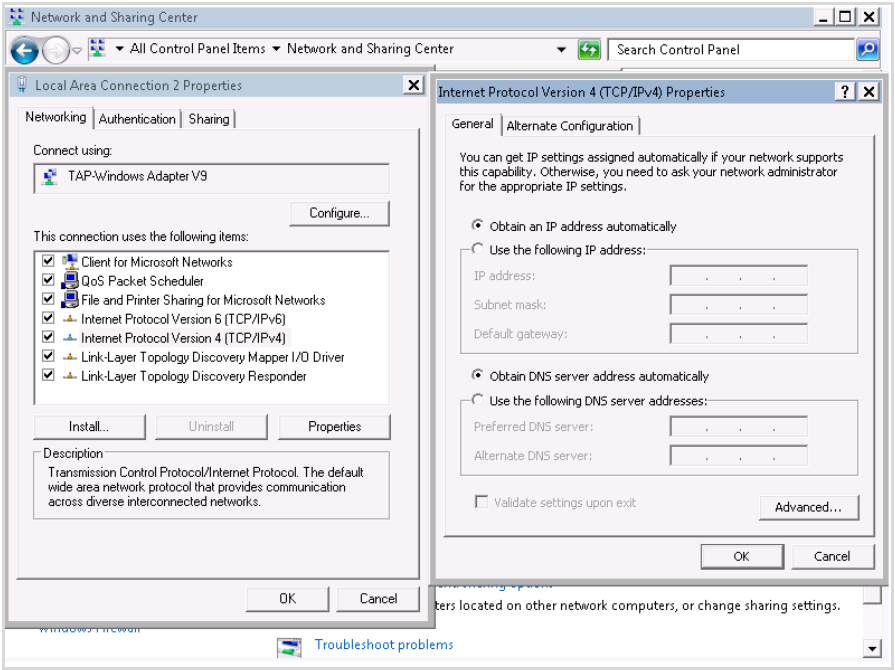


Step 5 **Click Properties and select the configured Internet protocol version.**

Step 6 **In the General tab, select Obtain an IP address automatically and Obtain DNS server address automatically and click OK.**

NOTE

You are advised to record the original network information so that you can restore the network if necessary.



4.2.1.4 (Optional) Enabling the Remote Desktop Connection

You need to enable Remote Desktop Connections if you want to connect to the ECS using Remote Desktop later. This function must be enabled for GPU-optimized ECSs.

Step 1 **Choose Start, right-click Computer, and choose Properties from the shortcut menu.**

Step 2 **Click Remote settings.**

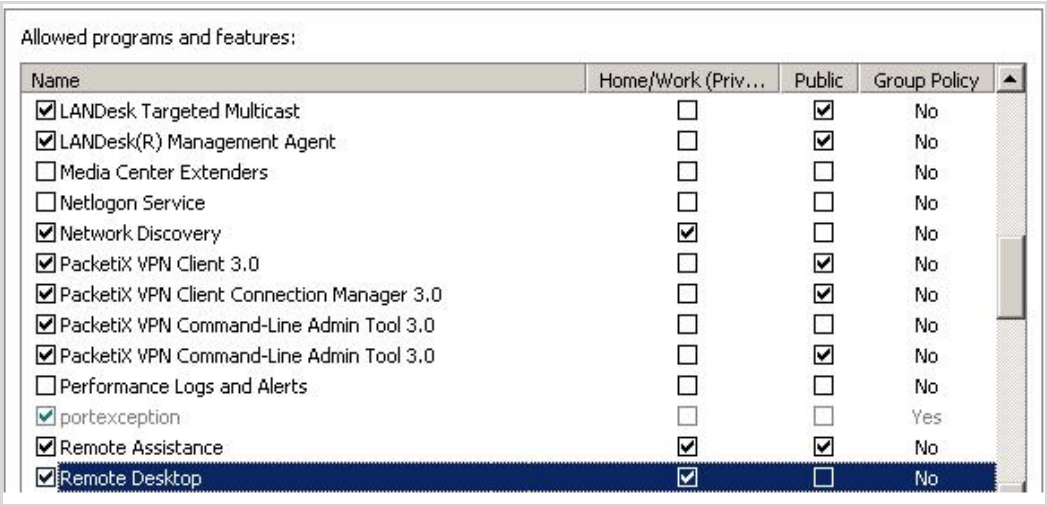
Step 3 **On the Remote page, select Allow connections from computers running any version of Remote Desktop (less secure).**

Step 4 **Click OK.**

Step 5 **On the Properties page, choose Start > Control Panel and navigate to Windows Firewall.**

Step 6 **Choose Allow a program or feature through Windows Firewall in the left pane.**

Step 7 **Select programs and features that are allowed by the Windows firewall for Remote Desktop based on your network requirements and click OK in the lower part.**



4.2.2 Installing and Configuring Cloudbase-Init

4.2.2.1 Scenarios

- If you do not install Cloudbase-Init, you can log in to the ECS with the original image password. However, you cannot customize ECS configurations.
- On the ECS created using the public images, the Cloudbase-Init has been installed by default. You do not need to install Cloudbase-Init or configure ECS.
- For ECSs created using an image file you imported, you must install and configure Cloudbase-Init by following the instructions in this section.

4.2.2.2 Prerequisites

- An elastic IP address has been bound to the Windows ECS.
- You have logged in to the Windows ECS.
- DHCP has been configured for the NICs.
- You have installed the one-click password reset plug-in. If the ECS is restarted during Cloudbase-Init installation, the password may be changed to a random one. Therefore, you need to install the one-click password reset plug-in.

4.2.2.3 Installing Cloudbase-Init

Step 1 **On the Windows Start menu, choose Control Panel > Programs > Programs and Features to check whether Cloudbase-Init is installed.**

- If yes, run Configuring Cloudbase-Init.
- If no, go to the next step.

Step 2 **Check whether a Windows desktop version is used as the OS:**

- If yes, go to Step3.
- If the OS is Windows Server, go to Step4.

Step 3 **Perform the following operations to ensure that the administrator account is enabled (Windows 7 is used as an example):**

a. Click **Start** and choose **Control Panel** > **System and Security** > **Administrative Tools**.

b. Double-click **Computer Management.**

c. Choose **System Tools** > **Local Users and Groups** > **Users**.

d. Right-click **Administrator** and select **Properties**.

e. Deselect **Account is disabled**.

Step 4 **Download the Cloudbase-Init installation package.**

The version of Cloudbase-Init may vary depending on the OS bits. You can download the version your need from the official website at http://www.cloudbase.it/cloud-init-for-windows-instances/.

Cloudbase-Init has two available versions, the stable version and the beta version.

- To obtain the stable version, visit the following paths:
  - 64-bit: https://www.cloudbase.it/downloads/CloudbaseInitSetup_Stable_x64.msi
  - 32-bit: https://www.cloudbase.it/downloads/CloudbaseInitSetup_Stable_x86.msi
- To obtain the beta version, visit the following paths:
  - 64-bit: https://www.cloudbase.it/downloads/CloudbaseInitSetup_x64.msi
  - 32-bit: https://www.cloudbase.it/downloads/CloudbaseInitSetup_x86.msi

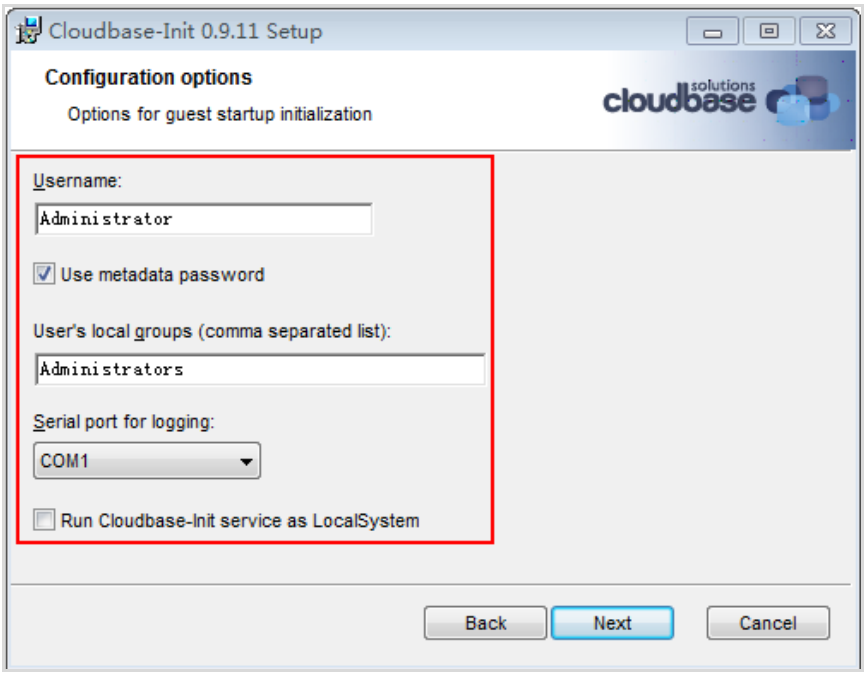
Step 5 **Double-click the Cloudbase-Init installation package.**

Step 6 **Click Next.**

Step 7 **Select I accept the terms in the License Agreement, and click Next.**

Step 8 **Retain the default path and click Next.**

Step 9 **In the Configuration options window, enter Administrator for Username, select COM1 for Serial port for logging, and ensure that Run Cloudbase-Init service as LocalSystem is not selected.**



NOTE

The version shown in the figure is for reference only. Use the latest version.

Step 10 **Click Next.**

Step 11 **Click Install.**

Step 12 **In the Files in Use dialog box, retain the default selection of Close the application and attempt to restart them and click OK.**

Step 13 **Check whether a Windows desktop version is used as the OS:**

- If yes, go to 15.
- If no, go to 14.

Step 14 **In the Completed the Cloudbase-Init Setup Wizard window, ensure that neither of the two options is selected.**

NOTE

The version shown in the figure is for reference only. You must use the latest version.

Step 15 **Click Finish.**

4.2.2.4 Configuring Cloudbase-Init

Step 1 **Add configuration item netbios_host_name_compatibility=false to the last row in C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf. This will allow the hostname to contain a maximum of 63 characters.**

NOTE

NetBIOS contains no more than 15 characters due to Windows system restrictions.

Step 2 **Enable the agent to access the IaaS OpenStack data source by adding configuration item metadata_services=cloudbaseinit.metadata.services.httpservice.HttpService to the cloudbase-init.conf configuration file in the C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\ directory.**

Step 3 **(Optional) When the Cloudbase-Init version is 0.9.12 or later, you can customize the length of the password. To set the password length, change the value of user_password_length in C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf.**

Step 4 **(Optional) When you log in to the ECS using password injection for the first time, you will be forced to change the password. If you do not want to change the password, you can disable this function. Add configuration item first_logon_behaviour=no to the cloudbase-init.conf configuration file in the C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\ directory to disable the function of changing the password.**

Step 5 **Release the current DHCP address so that created ECSs can obtain the correct addresses.**

Step 6 **In the Windows command line, run the following command to release the current DHCP address:**

```
ipconfig /release
```

NOTE

This operation will interrupt network connection and adversely affect the use of the ECS. After the ECS is restarted, network connections will automatically recover.

Step 7 **For a Windows ECS used to create an ECS image, you must set the SAN policy of the ECS to OnlineAll. Otherwise, the EVS disks may be offline.**

Windows has three types of SAN policies: **OnlineAll**, **OfflineShared**, and **OfflineInternal**.

Type	Description
OnlineAll	Indicates that all disks are automatically brought online.
OfflineShared	Indicates that all disks on sharable buses, such as iSCSI and FC, are left offline by default, while disks on non-sharable buses are kept online.
OfflineInternal	Indicates that all newly detected disks are left offline as default.

a. Run the following command on DiskPart to query the current SAN policy of the ECS:

```
diskpart
```

b. Run the following command to view the SAN policy of the ECS:

```
san
```

- If the SAN policy is **OnlineAll**, run the **exit** command to exit DiskPart.
- If no, go to Step7.c.

c. Run the following command to change the SAN policy to **OnlineAll**:

```
san policy=onlineall
```

4.2.3 Creating a System Disk Image

4.2.3.1 Scenarios

After the ECS configuration is complete, use the ECS to create a system disk image.

4.2.3.2 Prerequisites

- The IP address obtaining mode of the Windows ECS NIC has been set to DHCP.
- Cloudbase-Init has been installed and configured.

4.2.3.3 Procedure

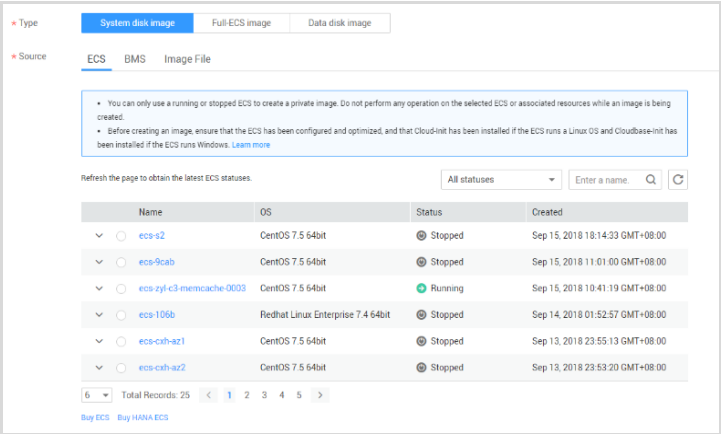
Step 1 **Log in to the management console.**

Step 2 **Choose Computing > Image Management Service from the main menu.**

Step 3 **On the Image Management Service page, click Create Private Image.**

Step 4 **In the Image Type and Source area, select System disk image for Type.**

Step 5 **By default, ECS is selected for Source, and you can select an ECS from the list.**



Step 6 **In the Image Information area, set basic information, such as the image name and description.**

Step 7 **Click Next.**

Step 8 **Confirm the image parameters as prompted. Select I have read and agree the Statement of Commitment of Image Creation, and click Submit.**

Step 9 **After submitting the task, switch back to the Image Management Service page to view the image status.**

The time required for creating an image varies depending on the image file size. Generally, it takes about 20 minutes to create an image. The image is successfully created when its image status changes to **Normal**.

NOTE

- Do not perform any operation on the selected ECS or associated resources during image creation.
- An ECS created using an encrypted image is an encrypted ECS. The key of the encrypted ECS is the same as that of the encrypted image.
- An image created from an encrypted ECS is also encrypted. The key of this image is the same as that of the ECS.

4.3 Modifying Image Attributes

You can modify the name, description, minimum memory, or NIC multi-queue of a private image.

4.3.1 Scenarios

Only private images in **Normal** state can be modified. You can modify the name, description, minimum memory, or NIC multi-queue of a private image.

4.3.2 Procedure

You can modify the name, description, minimum memory, or NIC multi-queue of a private image using either of the following methods:

Method 1:

Step 1 **Log in to the management console.**

Step 2 **Under Computing, click Image Management Service.**

Step 3 **Click Private Images to display the image list.**

Step 4 **Locate the row that contains the image and click Modify in the Operation column.**

Step 5 **Modify the image name and description.**

Method 2:

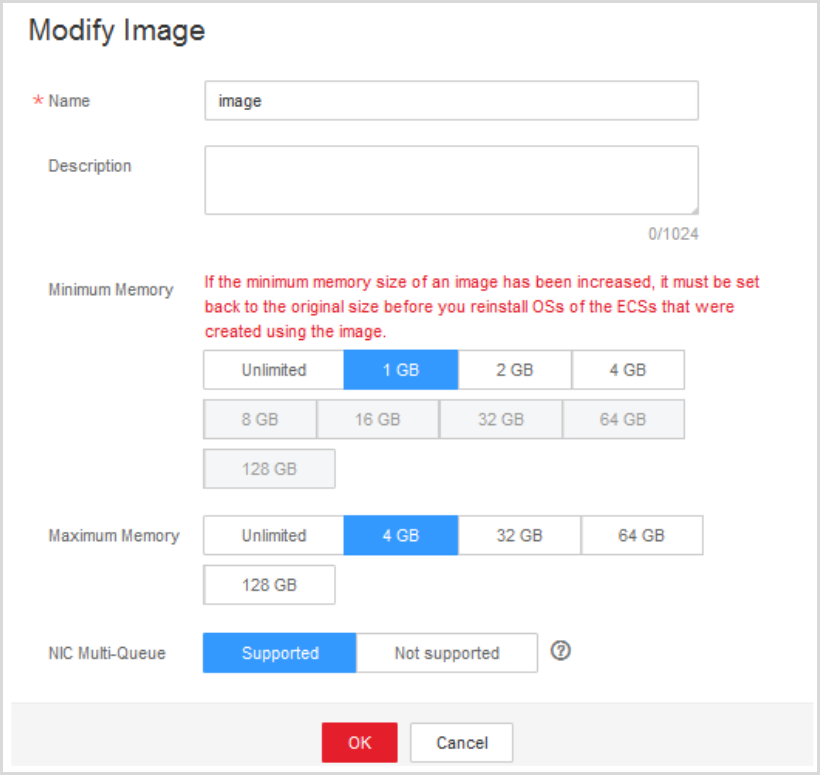
Step 1 **Log in to the management console.**

Step 2 **Under Computing, click Image Management Service.**

Step 3 **Click Private Images to display the image list.**

Step 4 **On the image list, click the name of the target image.**

Step 5 **On the image details page, click Modify. In the displayed Modify Image dialog box, modify the image attributes.**



4.4 Sharing Images

4.4.1 Sharing One or More Images

4.4.1.1 Scenarios

Suppose you are user A, and you want to share images with another user. You can use image sharing. After obtaining the Account Name=Domain Name (example= aluno16-huaweicloud from user B, you can perform the operations in this section to share specified images with user B. If user B is a DeC user or multi-project user, you must also obtain the project name. You can share a single image at a time or multiple images in batches as needed.

4.4.1.2 Prerequisites

You have obtained the Account Name of user B (ask for another student). If user B is a DeC or multi-project user, you need to obtain both the project ID and project name of user B. (look at the botton of My credential page)

4.4.1.3 Procedure

Share images in batches (need to created previously another images)

Step 1 **Log in to the management console.**

Step 2 **Under Computing, click Image Management Service.**

Step 3 **On the Image Management Service page, click Private Images to display the image list.**

Step 4 **Select the private images to share and click Share on top of the image list.**

Step 5 **In the Share Image dialog box, enter the project ID of user B. If user B is a DeC user or a multi-project user, select the corresponding project IDs**

Step 6 **Click OK.**

To Share a single image.

Step 1 **Log in to the management console.**

Step 2 **Under Computing, click Image Management Service.**

Step 3 **On the Image Management Service page, click Private Images to display the image list.**

Step 4 **Locate the row that contains the private image you are to share, click More in the Operation column and select Share.**

Step 5 **In the Share Image dialog box, enter the project ID of user B and click Add. If user B is a DeC user or a multi-project user, select the corresponding project name and click Add.**

NOTE

To add multiple image recipients, enter the project IDs and project names of these recipients.

Step 6 **Click OK.**

4.4.2 Adding Tenants Who Can Use Shared Images

4.4.2.1 Scenarios

You can add tenants who can use the shared images. (look inside of link of image)

4.4.2.2 Prerequisites

- You have shared private images.
- You have obtained the project ID of the tenant to be added and project name if the tenant is a DeC or multi-project user.

4.4.2.3 Procedure

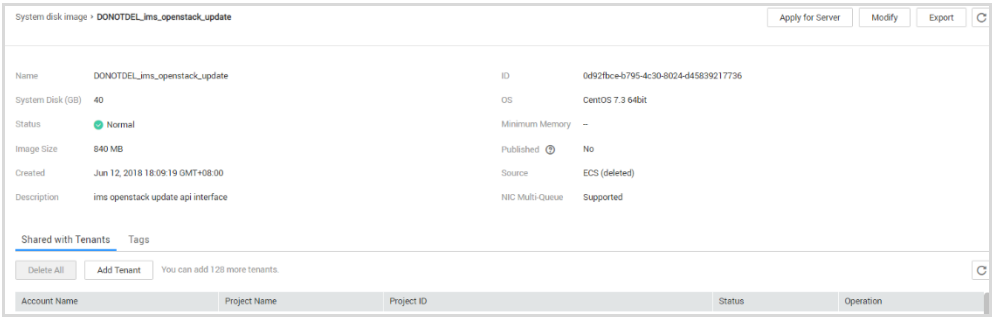
Step 1 **Log in to the management console.**

Step 2 **Under Computing, click Image Management Service.**

Step 3 **On the Image Management Service page, click Private Images to display the image list.**

Step 4 **Click the image name to view image details.**

Step 5 **In the image details area, click Add Tenant.**



Step 6 **In the Add Tenant dialog box, enter the project ID (and project name if the tenant to be added is a DeC or multi-project user) and click Ok.**

Step 7 **Your partner needs to accept this share, make sure that this procedure was done. In this same page you can see the status of sharing.**

4.4.3 Deleting Tenants Who Can Use Shared Images

4.4.3.1 Scenarios

You can delete tenants who can use shared images if you do not want to share images with them.

4.4.3.2 Prerequisites

- You have shared private images.
- You have obtained the Account Name of the tenant to be deleted.

4.4.3.3 Procedure

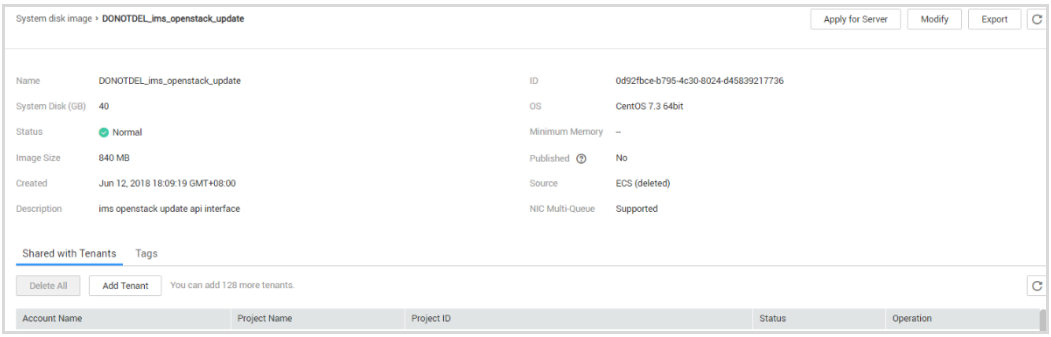
Step 1 **Log in to the management console.**

Step 2 **Under Computing, click Image Management Service.**

Step 3 **On the Image Management Service page, click Private Images to display the image list.**

Step 4 **Click the image name to view image details.**

Step 5 **View the shared tenant on the image details page.**



Step 6 **Determine the operation to perform based on how many tenants you want to delete:**

- To delete a single tenant, click **Delete** in the row that contains the tenant.
- To delete all tenants, click **Delete All** on top of the tenant list.

Step 7 **Click OK.**

4.5 Replicating an Image Within a Region

You can use the image replication function to convert an encrypted to an unencrypted image, or the other way around.

4.5.1 Scenarios (try all these cases)

You may need to replicate an image in the following scenarios:

- Replicate an encrypted image to an unencrypted image.

  Encrypted images cannot be shared with other tenants or published as a marketplace image. If you want to publish or share an encrypted image, you can replicate it to an unencrypted one.

- Replicate an encrypted image to an encrypted image.

  Keys for encrypting the images cannot be changed. If you want to change the key of an encrypted image, you can replicate this image to a new one and encrypt the new image using an encryption key.

- Replicate an unencrypted image to an encrypted image. (try to create another new key instead to use the default key)

  If you want to store an unencrypted image in an encrypted way, you can replicate this image to a new one and encrypt the new image using an encryption key.

4.5.2 Restrictions and Limitations

You can replicate a private image in **Normal** or **Normal (Uninitialized)** state.

A full-ECS image cannot be replicated within the same region.

4.5.3 Prerequisites

The image to be replicated is in **Normal** or **Normal (Uninitialized)** state.

4.5.4 Procedure

Step 1 **Log in to the management console.**

Step 2 **Under Computing, click Image Management Service.**

Step 3 **On the Image Management Service page, click Private Images to display the image list.**

Step 4 **Locate the row that contains the image to be replicated and click More in the Operation column.**

Step 5 **Select Replicate.**

Step 6 **In the displayed Replicate Image dialog box, enter a name and description for the image.**

Step 7 **Encrypt the image.**

Step 8 **If you want to encrypt the image or change a key, enable encryption and select a key from the drop-down list.**

Step 9 **Click OK.**

5 Volume Backup Service

5.1 Introduction

5.1.1 About This Exercise

This exercise describes common operations and backup policy management of Volume Backup Service (VBS).

5.1.2 Objective

- Create VBS backups.
- Delete VBS backups.
- Restore and create Elastic Volume Service (EVS) disks from VBS backups.
- Create, edit, and delete backup policies as well as associate EVS disks with backup policies.

5.1.3 Prerequisites

- You have registered an account with HUAWEI CLOUD.
- Create an EVS disk or ECS for BKPS

5.1.4 List of Tasks

No.	Task	Sub-Task	Application Scenario
1	Perform basic operations.	Create backups.	Create an EVS disk on HUAWEI CLOUD and then back up the disk.
		Delete backups.	Delete one or more backups at a time.
		Restore data from a	Restore data of an EVS disk or create an EVS disk from

No.	Task	Sub-Task	Application Scenario
		backup.	a backup.
2	Manage backup policies.	Create a backup policy.	Create a backup policy.
		Edit a backup policy.	Edit a backup policy.
		Associate EVS disks with a backup policy.	Associate EVS disks with a backup policy.
		Execute a backup policy.	Execute a backup policy.
		View backup jobs.	View backup jobs.
		Delete a backup policy.	Delete a backup policy.

5.2 Performing Basic Operations

5.2.1 Creating Backups

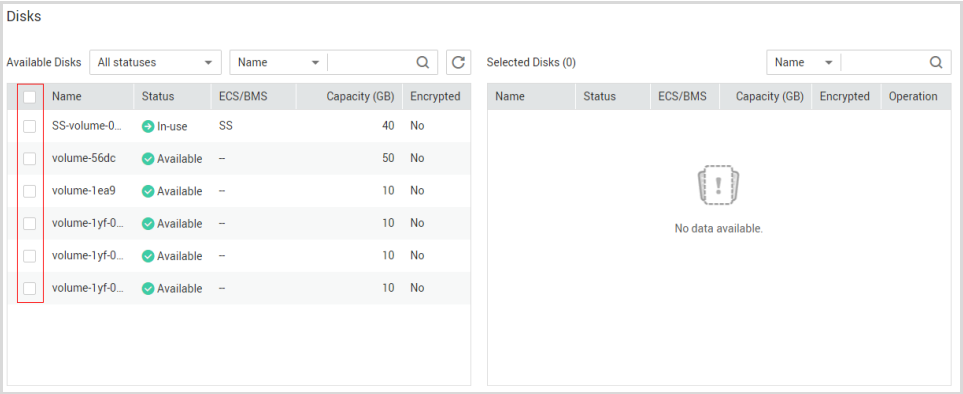
Step 1 **Create an EVS disk by referring to the Elastic Volume Service Hands-on Exercises.**

Step 2 **Create backups either on the VBS page or EVS page.**

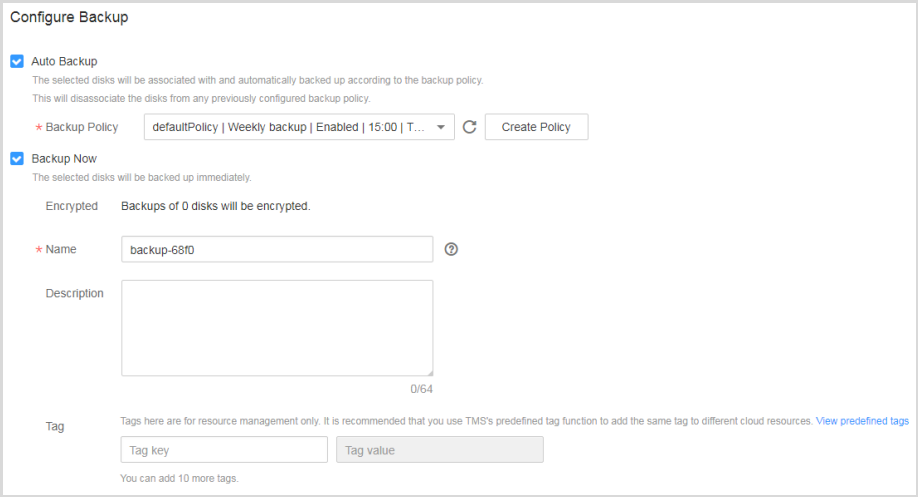
Method 1: Create backups on the VBS page.

1. Go to the VBS page.
2. Click

.
3. Select ☐ in the rows of the disks you want to back up.



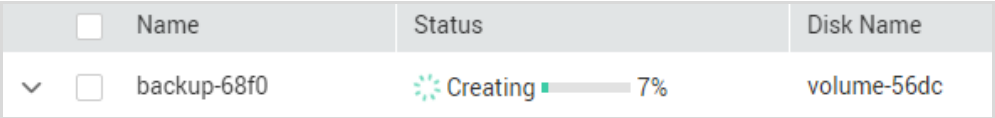
4. In the **Configure Backup** area, select **Auto Backup** or **Backup Now**, or both of them.



5. Click **Next**.

6. Confirm the configuration and click **Submit**.

7. Return to the **Backups** tab page and you can view the created backups in the backup list.



8. Wait a period of time and then refresh the page. When the status of a backup is **Available**, the backup creation is complete.

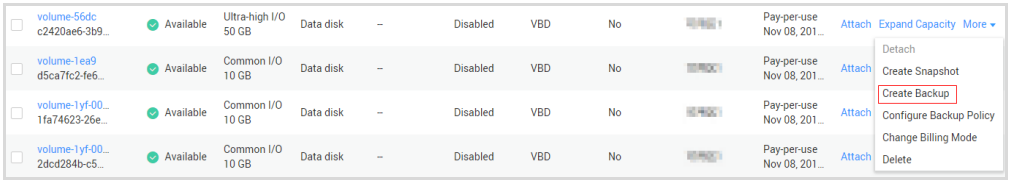
NOTE

The waiting time depends on the amount of data to be backed up. It takes approximately 35 minutes to back up 50 GB data.

----End

Method 2: Create a backup on the EVS page.

1. Go to the EVS page.
2. In the list of EVS disks, choose **More** > **Create Backup** in the row of the disk you want to back up.



3. On the page that is displayed, click **Next**.
4. Refer to step 5 to step 8 in the operation procedure performed on the VBS page to complete the creation.

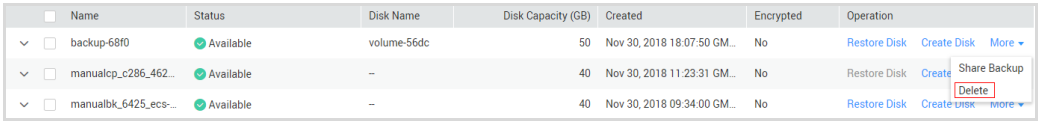
----End

5.2.2 Deleting Backups

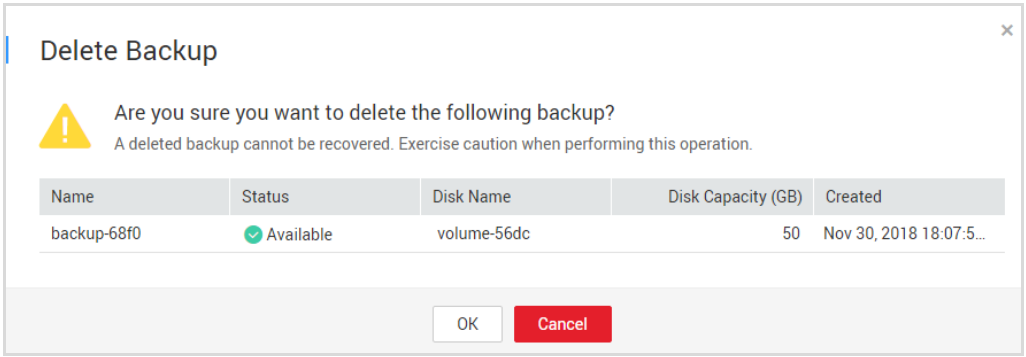
5.2.2.1 Deleting a Single Backup

Step 1 **Go to the VBS page.**

Step 2 **In the list of backups, choose More > Delete in the row of the backup you want to delete.**



Step 3 **In the dialog box that is displayed, click OK.**



Step 4 **The status of the backup changes to Deleting. Refresh the page later. When the backup is removed from the list, it is deleted successfully.**

NOTE

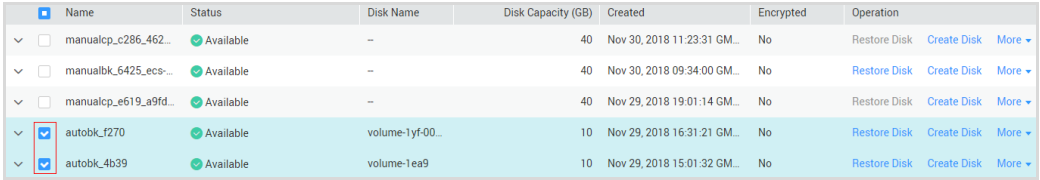
The time spent on deleting a backup varies with the backup size.

----End

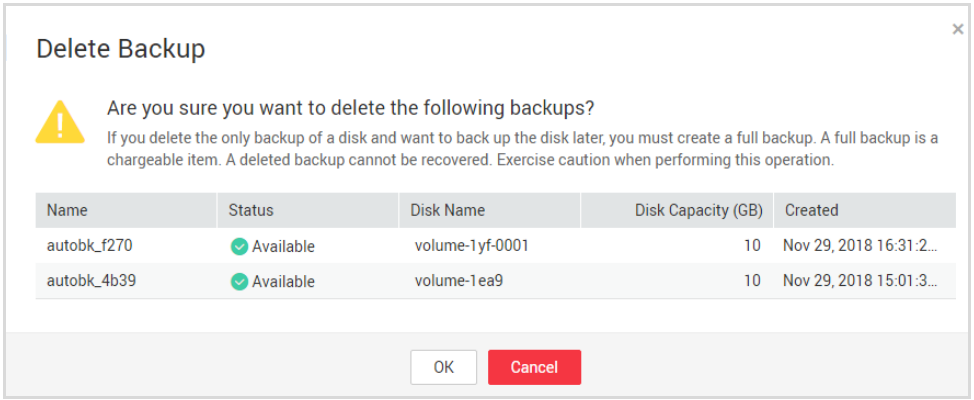
5.2.2.2 Deleting Backups in a Batch

Step 1 **Go to the VBS page.**

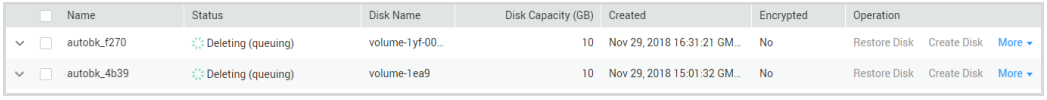
Step 2 **Select backups you want to delete or select all backups by ticking the box in the header of the list.**



Step 3 **In the upper left corner, click Delete. In the confirmation dialog box that is displayed, click OK.**



Step 4 **The status of the backups changes to Deleting. Refresh the page later. When those backups do not exist in the list, they are deleted successfully.**



NOTE

The time spent on deleting a backup varies with the backup size.

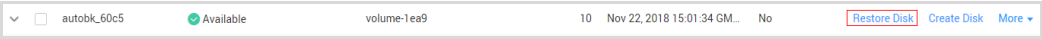
----End

5.2.3 Restoring Data from a Backup

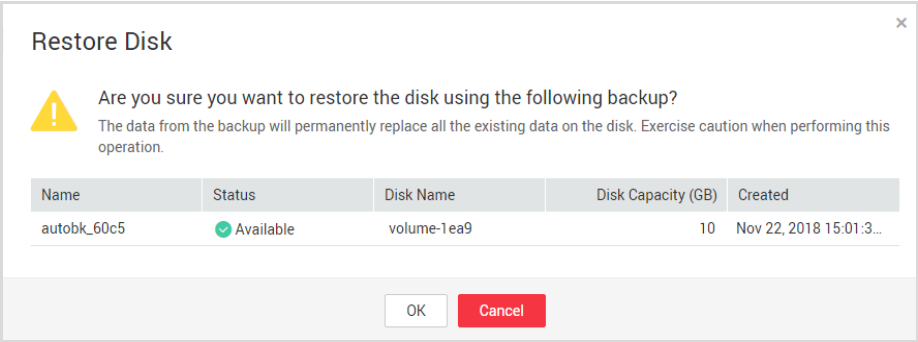
5.2.3.1 Restoring an EVS Disk from a Backup

Step 1 **Go to the VBS page.**

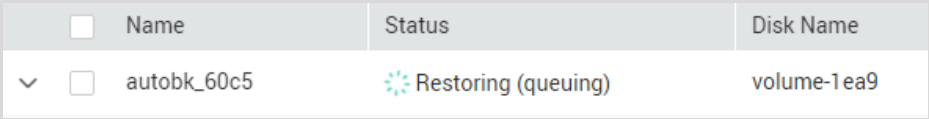
Step 2 **In the list of backups, click Restore Disk in the row of the desired backup.**



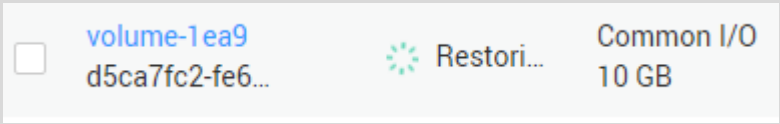
Step 3 **In the dialog box that is displayed, click OK.**



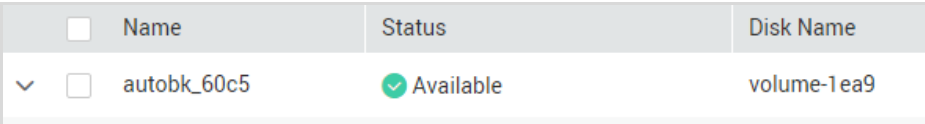
Step 4 **Refresh the VBS page. The status of the backup changes to Restoring.**

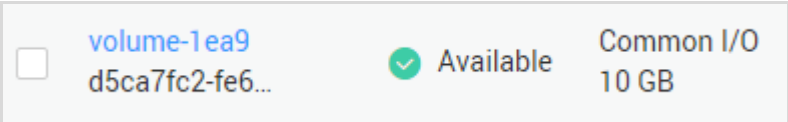


Step 5 **Go to the EVS page. The status is Restoring for the EVS disk corresponding to the backup.**



Step 6 **After a period of time, go to the VBS page and then the EVS page to check the status of the backup and the EVS disk. When they are both in the Available state, the EVS disk is restored successfully.**





NOTE

The time spent on restoring data from a backup varies with the backup size.

----End

5.2.3.2 Creating an EVS Disk from a VBS Backup

Step 1 **Go to the VBS page.**

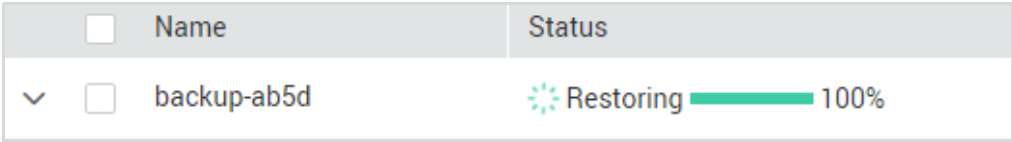
Step 2 **In the list of backups, click Create Disk in the row of the desired backup.**

Step 3 **On the displayed dialog box, select Pay-per-use for Billing Mode and click Next.**

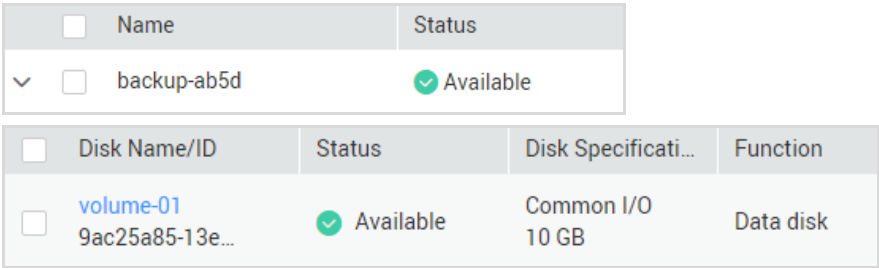
Step 4 **On the page that is displayed, click Submit.**

Step 5 **Go to the EVS page. The newly created EVS disk is displayed in the list. Refresh the page later, and the status of the EVS disk changes to Creating.**

Step 6 **Go to the VBS page. The status is Restoring for the EVS disk corresponding to the backup.**



Step 7 **After a period of time, go to the VBS page and then the EVS page to check the status of the backup and the EVS disk. When they are both in the Available state, the EVS disk is created successfully.**



NOTE

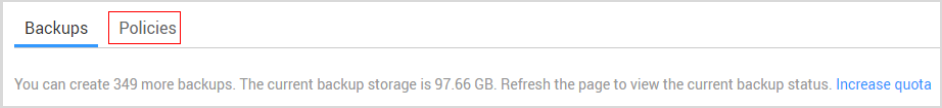
The time spent on creating an EVS disk from a backup varies with the backup size.

----End

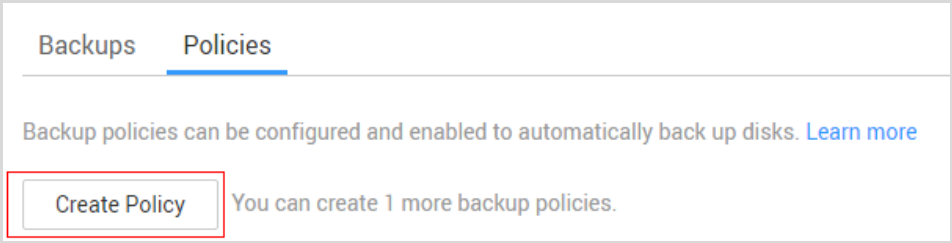
5.3 Managing Backup Policies

5.3.1 Creating a Backup Policy

Step 1 **Go to the VBS page and click the Policies tab to go to the Policies tab page.**

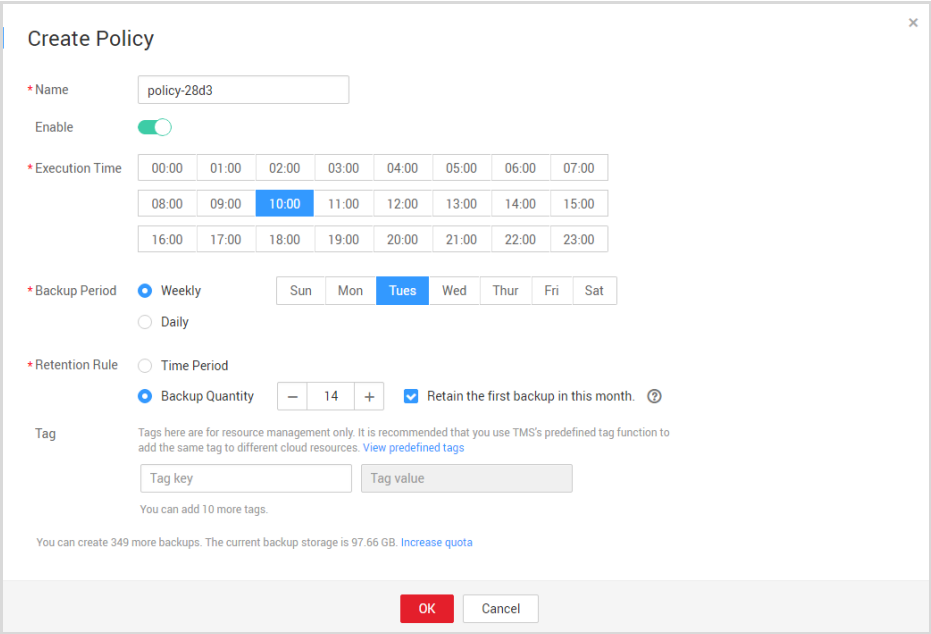


Step 2 **Click Create Policy.**

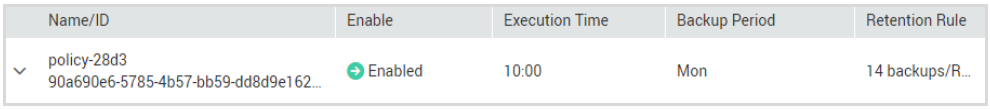


Step 3 **Set the backup parameters and click OK. The following example is for your reference.**

- Set Name to policy-28d3.
- Set **Enable** to .
- Set Execution Time to 10:00.
- Select **Weekly** for **Backup Period** and then select **Tues**.
- Select Backup Quantity for Retention Rule and then set the number to 14 and select Retain the first backup in this month.



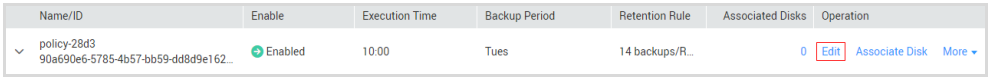
Step 4 **The newly created backup policy is displayed in the list of backup policies.**



----End

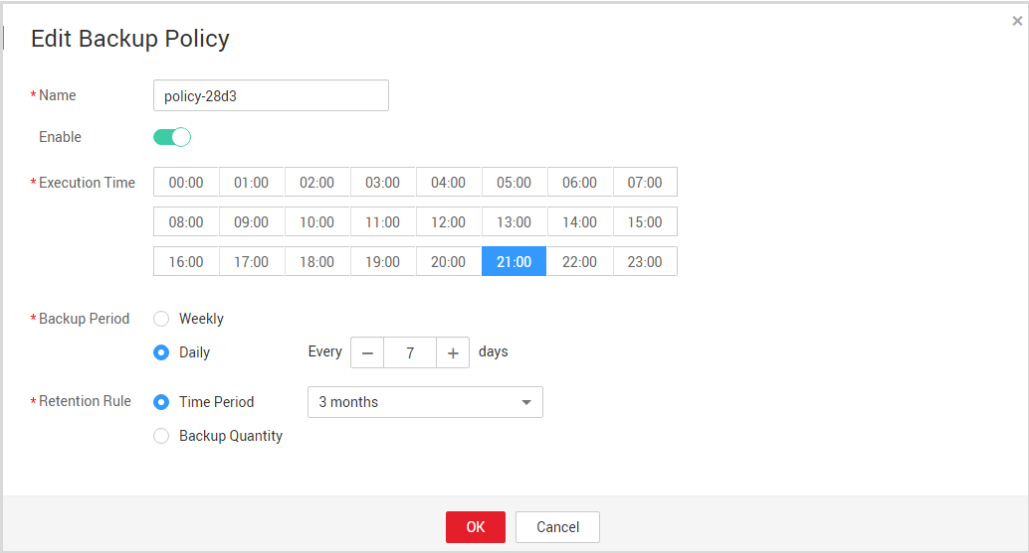
5.3.2 Editing a Backup Policy

Step 1 **Go to the Policies tab page and click Edit in the row of the desired policy.**



Step 2 **In the dialog box that is displayed, edit the backup policy and click OK. The following example is for your reference.**

- Keep Name to policy-28d3.
- Keep **Enable** to .
- Change Execution Time to 21:00.
- Select **Daily** for **Backup Period** and set the period to every 7 days.
- Select **Time Period** for **Retention Rule** and set the time period to **3 months**.



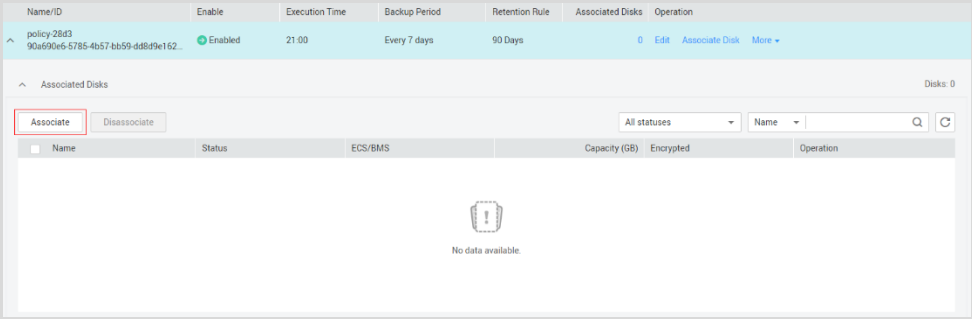
Step 3 **Parameter values are changed to those set in the preceding step.**

Name/ID	Enable	Execution Time	Backup Period	Retention Rule
policy-28d3 90a690e6-5785-4b57-bb59-dd8d9e162...	Enabled	21:00	Every 7 days	90 Days

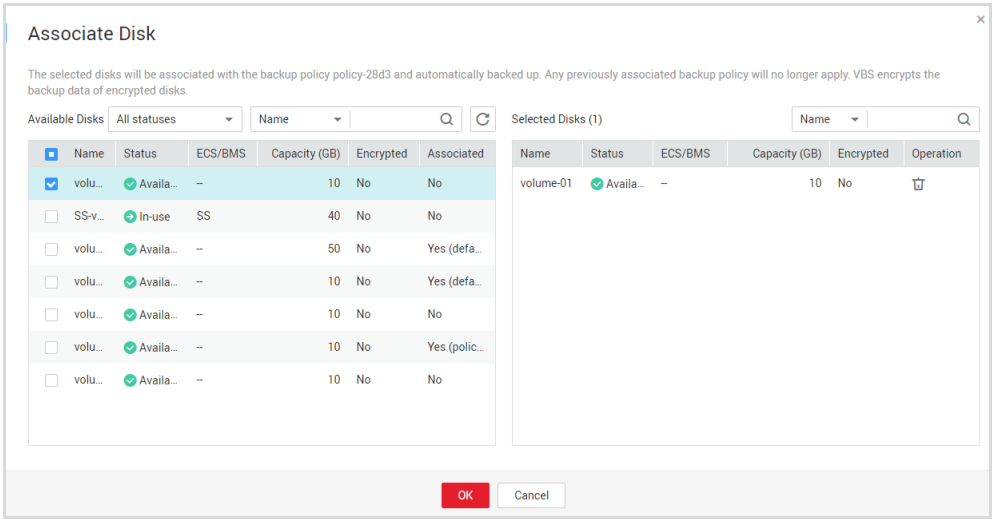
----End

5.3.3 Associating EVS Disks with a Backup Policy

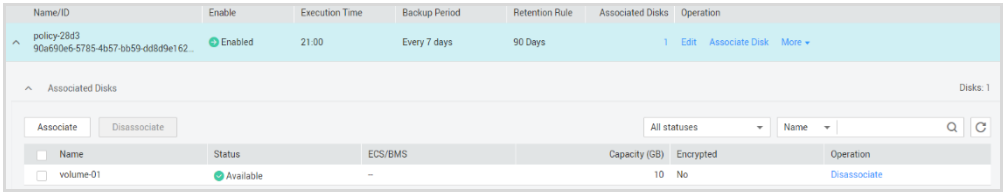
Step 1 **Go to the Policies tab page and click the policy name to expand the policy details. In the Associated Disks panel, click Associate.**



Step 2 **In the dialog box that is displayed, select the wanted disks and click OK.**



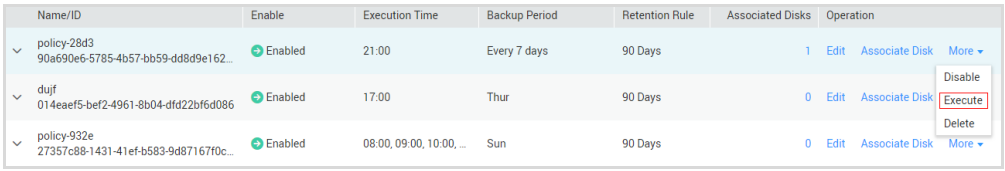
Step 3 **The selected EVS disks are displayed in the Associated Disks panel.**



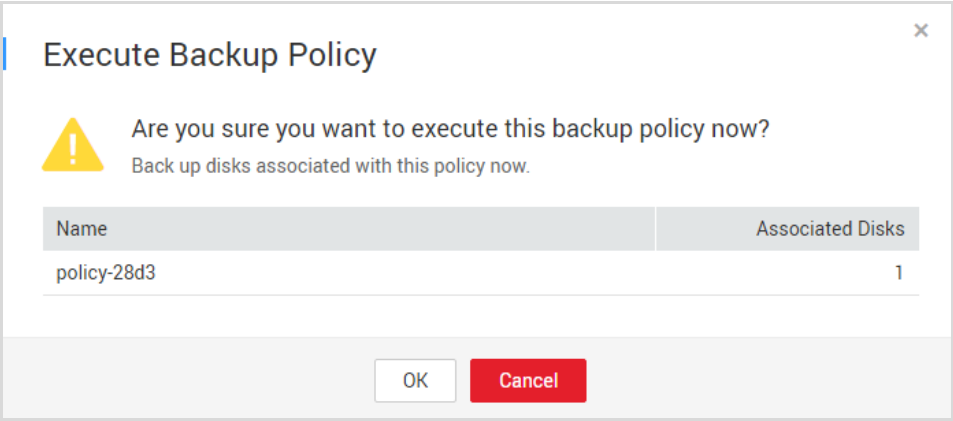
----End

5.3.4 Executing a Backup Policy

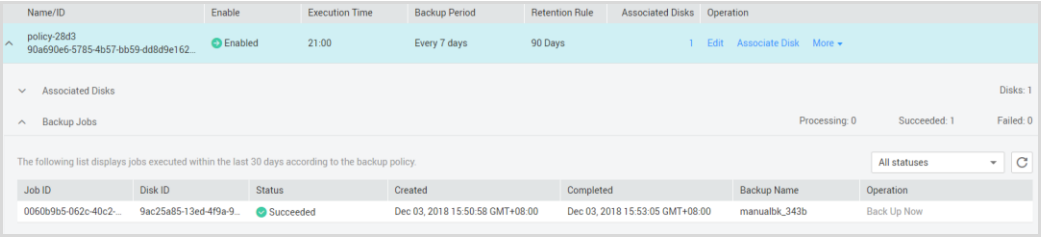
Step 1 **Go to the Policies tab page and choose More > Execute in the row of the policy.**



Step 2 **In the dialog box that is displayed, click OK.**



Step 3 **The newly started backup job is displayed in the Backup Jobs panel.**

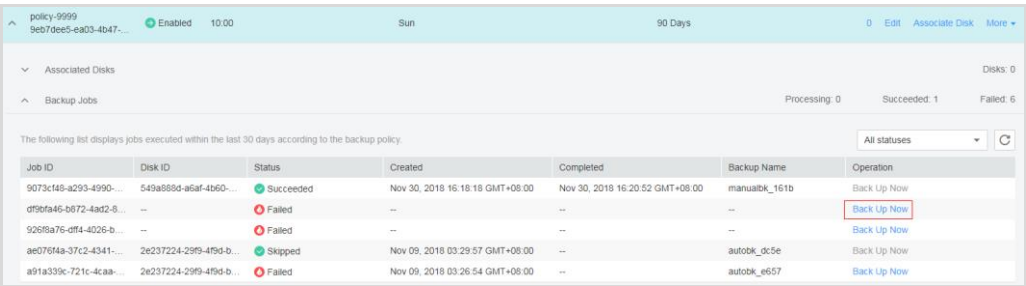


----End

5.3.5 Viewing Backup Jobs

Step 1 **Go to the Policies tab page and click the policy whose backup jobs you want to view.**

Step 2 **Click Backup Jobs to view the backup jobs executed within the last 30 days according to the backup policy.**

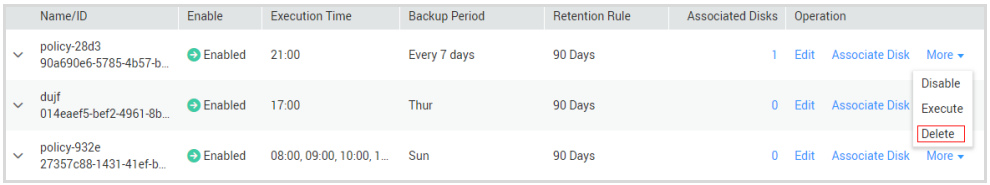


Step 3 **If there are failed backup jobs, you can click Back Up Now in the row of each failed one to manually back up them.**

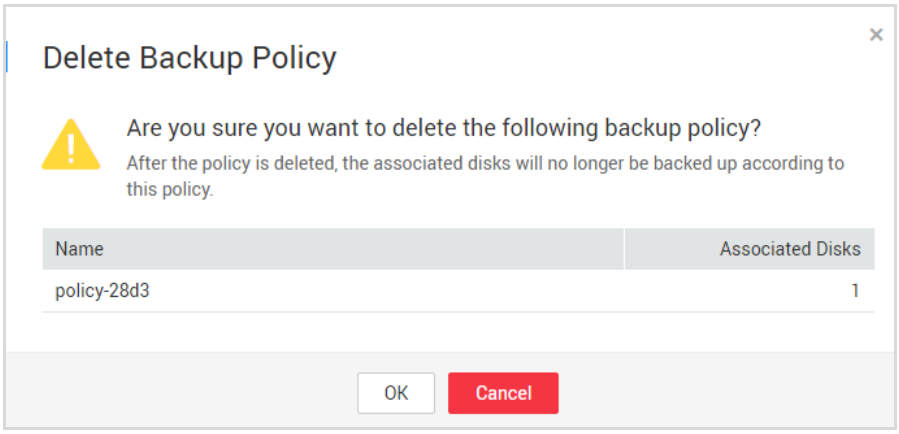
----End

5.3.6 Deleting a Backup Policy

Step 1 **Go to the Policies tab page and choose More > Delete in the row of the policy you want to delete.**



Step 2 **In the dialog box that is displayed, click OK.**



The deleted policy is not displayed in the page any more.

----End

6 Object Storage Service

6.1 Introduction

6.1.1 About This Exercise

This exercise describes how to use OBS Browser to perform basic OBS operations.

6.1.2 Objective

After completing this exercise, you will be able to:

- Know how to install OBS Browser. https://developer.huaweicloud.com/intl/tools
- Know how to use basic OBS Browser functions, such as creating buckets and folders, uploading, downloading, and deleting files or folders, and deleting buckets.

6.1.3 Service Overview

OBS is an object-based massive storage service. It provides abundant, secure, highly reliable, and low-cost data storage capabilities. OBS applies to a broad range of data storage scenarios such as enterprise backup/archiving, video on demand, and video surveillance.

OBS Browser is a client tool provided by OBS for Windows operating systems. It enables customers to manage object storage on PCs.

6.1.4 Prerequisites

You have obtained an account for logging in to HUAWEI CLOUD.

6.1.5 List of Tasks

No.	Task	Subtask	Application Scenario:
1	Prepare the OBS Browser environment.	Download OBS Browser. https://developer.huaweicloud.com/intl/tools	An enterprise needs to store a large number of files but does not want to purchase storage devices. Therefore, the enterprise uses OBS for storing and managing the files.
		Obtain access keys.	
		Log in to OBS Browser.	
2	Use OBS Browser.	Create a bucket.	
		Create a folder.	
		Upload a file or folder.	
		Download a file or folder.	
		Delete a file or folder.	
		Delete a bucket.	

6.2 Preparing the OBS Browser Environment

6.2.1 Scenarios

Before using OBS Browser, you need to download the software package from OBS Console and obtain your access keys for logging in to OBS Browser.

6.2.2 Restrictions

For details about required specifications of the Windows and Mac operating systems, see https://support-intl.huaweicloud.com/clientogw-obs/en-us_topic_0045853837.html

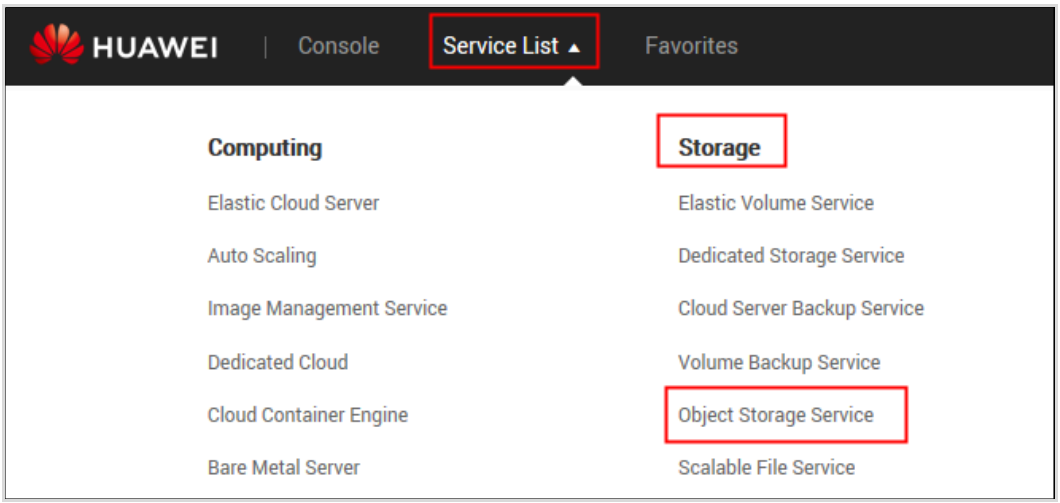
6.2.3 Subtasks

6.2.3.1 Downloading OBS Browser

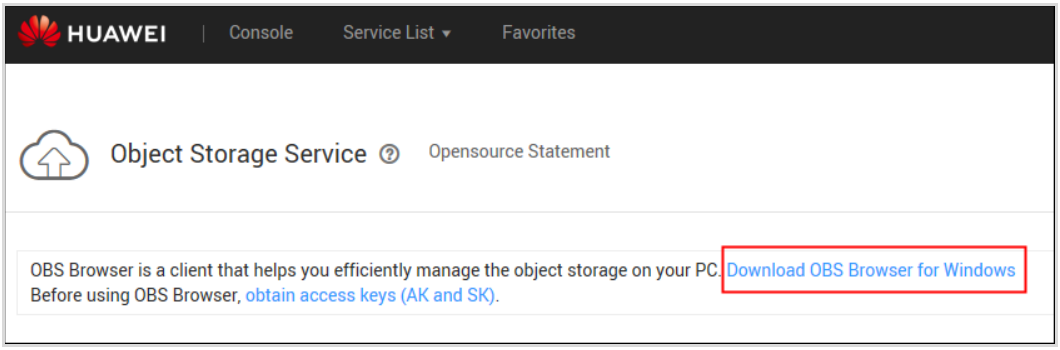
https://developer.huaweicloud.com/intl/tools

Step 1 **Log in to the HUAWEI CLOUD management console.**

Step 2 **On the home page of the console, choose Service List > Storage > Object Storage Service to access OBS Console.**



Step 3 **On the OBS Console home page, download the OBS Browser software package to the local path based on the operating system.**

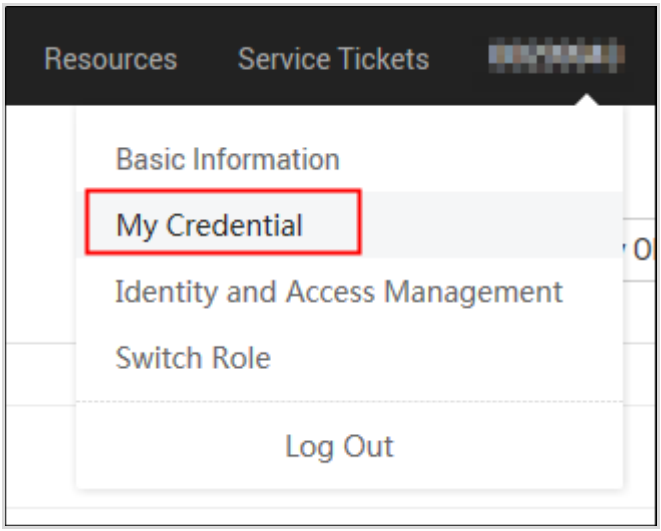


Step 4 **Decompress the downloaded software package on the local PC.**

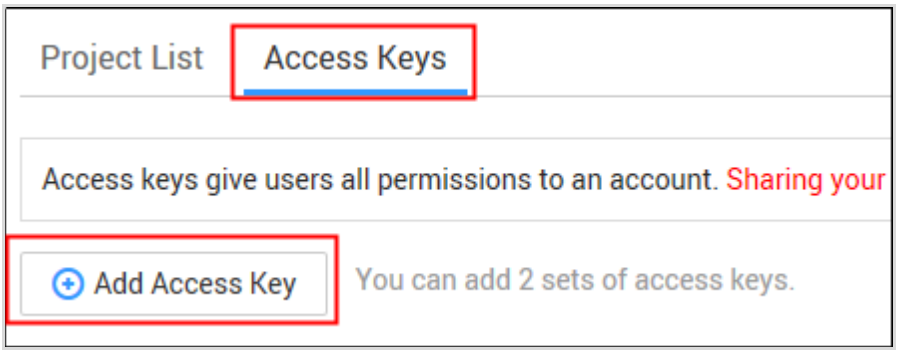
----End

6.2.3.2 Obtaining an Access Key (AK and SK)

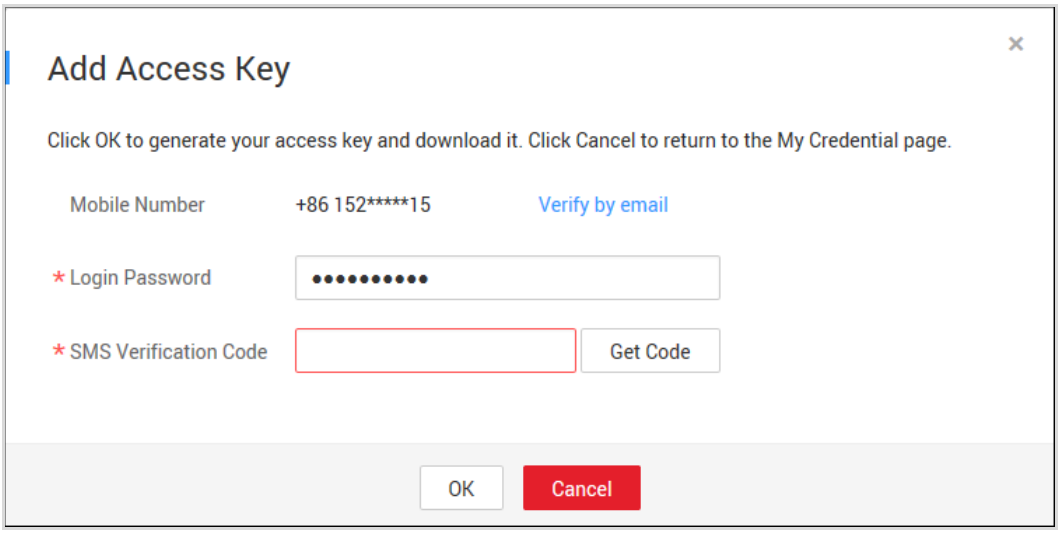
Step 1 **On the HUAWEI CLOUD console, click the username in the upper right corner and choose My Credential.**



Step 2 **On the My Credential page, click Add Access Key on the Access Keys tab page.**



Step 3 **In the Add Access Key dialog box that is displayed, enter the login password and verification code.**



Step 4 **Click OK.**

Step 5 **Save the key file as prompted.**

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

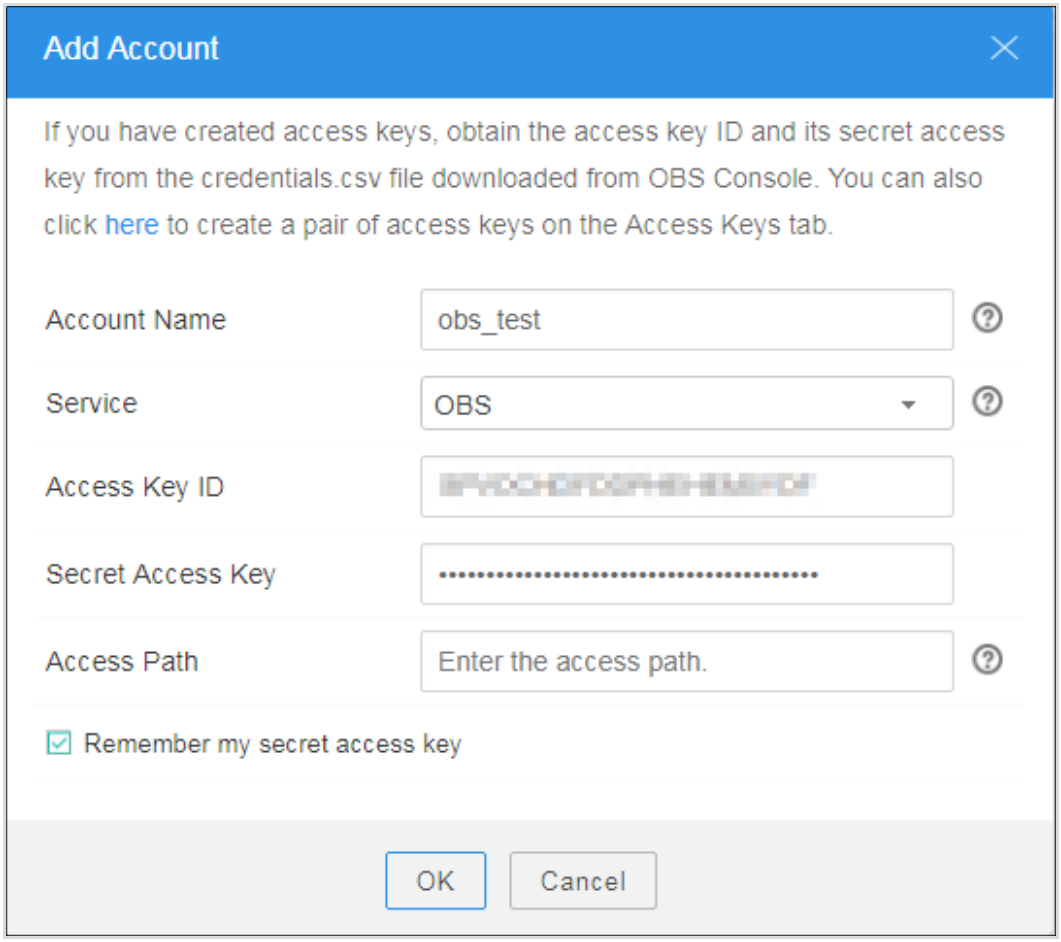
----End

6.2.3.3 Logging in to OBS Browser

Step 1 **In the decompressed OBS Browser file, double-click obs.exe to run OBS Browser.**

Step 2 **Enter the account information in the Add Account dialog box that is displayed.**

- **Account Name**: Enter **obs_test** for example.
- **Service**: Select **OBS**. OBS Browser automatically sets the server domain name to the service domain name of HUAWEI CLOUD OBS.
- **Access Key ID**: Obtain the value from the file downloaded in Obtaining an Access Key (AK and SK). ~~alunox-huaweicloud,~~**OCK4UYEPEOP79RRRRM9W**~~,0u3dX4MvvvvnkqVI0a0gMVxeFs3H5sz60jMxLpsk~~
- **Secret Access Key**: Obtain the value from the file downloaded in Obtaining an Access Key (AK and SK) sample… get only the red part after comma ~~alunox-huaweicloud,OCK4UYEPEOP79RRRRM9W,~~**0u3dX4MvvvAnkqVI0a0gMVxeFs3H5sz60jMxLpsk**
- **Access Path**: Leave this parameter blank.



Step 3 **Click OK to log in to OBS Browser.**

----End

6.3 Using OBS Browser

6.3.1 Scenarios

The following uses OBS Browser running on Windows as an example to introduce basic OBS operations.

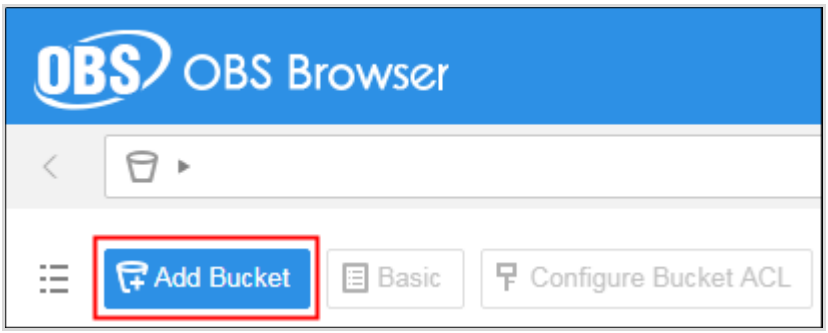
6.3.2 Prerequisites

You have downloaded and logged in to OBS Browser. For details, see Preparing the OBS Browser Environment.

6.3.3 Subtasks

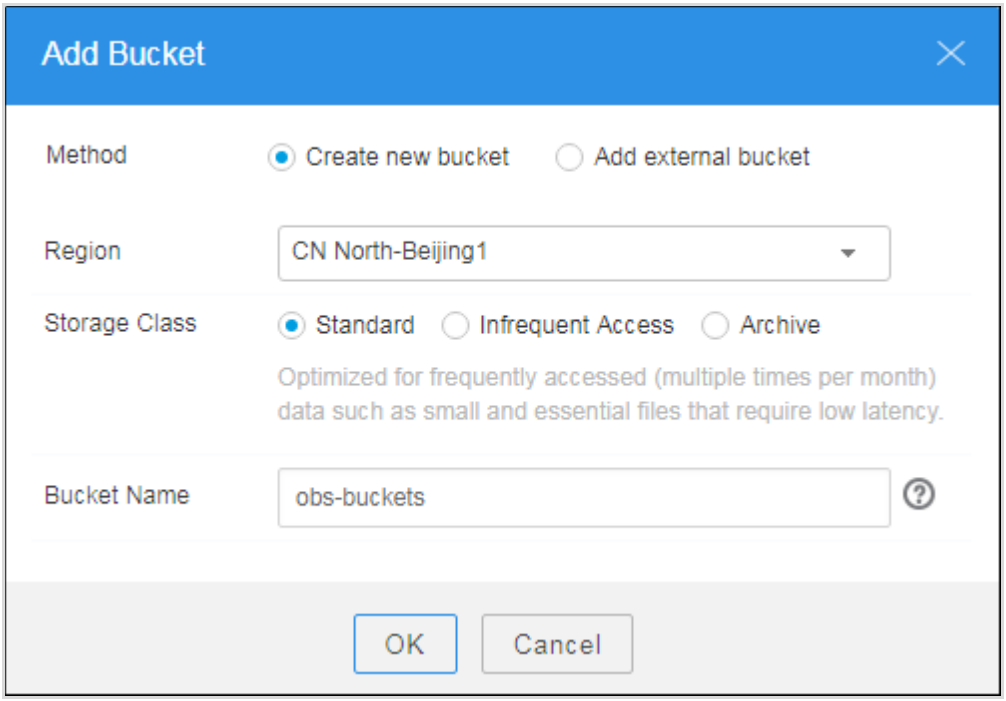
6.3.3.1 Creating a Bucket

Step 1 **Click Add Bucket on the upper left of the OBS Browser page.**

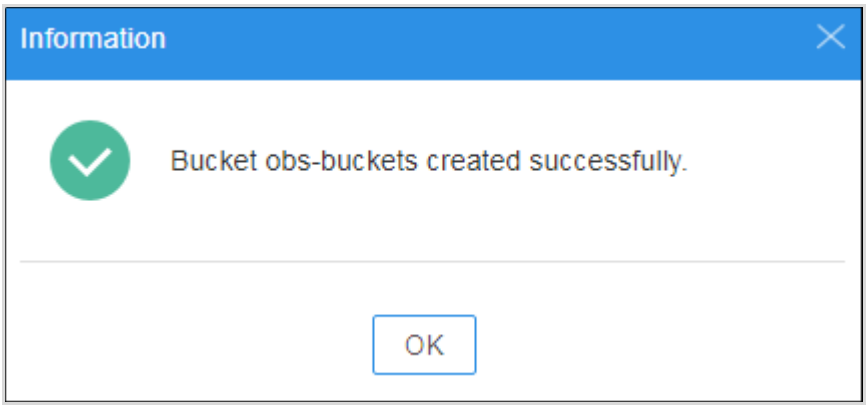


Step 2 **In the Add Bucket dialog box that is displayed, set the following parameters:**

- Method: Choose Create new bucket.
- **Region**: Select a region name from the drop-down list box, for example, **CN North-Beijing1**.
- Storage Class: Select Standard.
- **Bucket Name**: You can click next to the text box to view the bucket naming rule. **obs-buckets** is used as an example here.



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



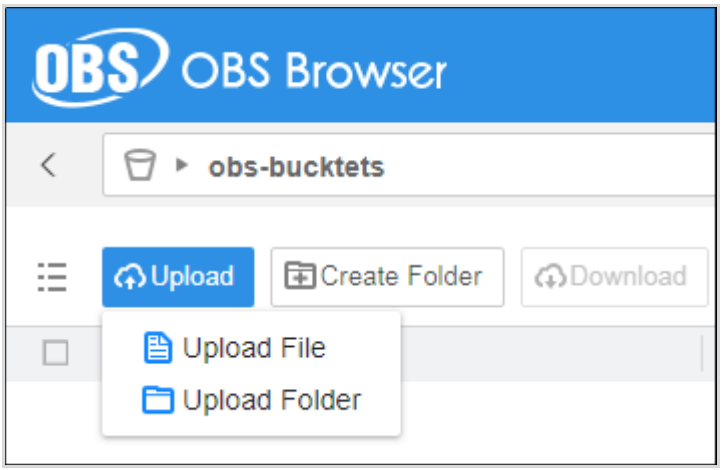
Step 4 **In the displayed dialog box, click OK.**

----End

6.3.3.2 Uploading a File or Folder

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

Step 2 **Click Upload and select Upload File or Upload Folder.**



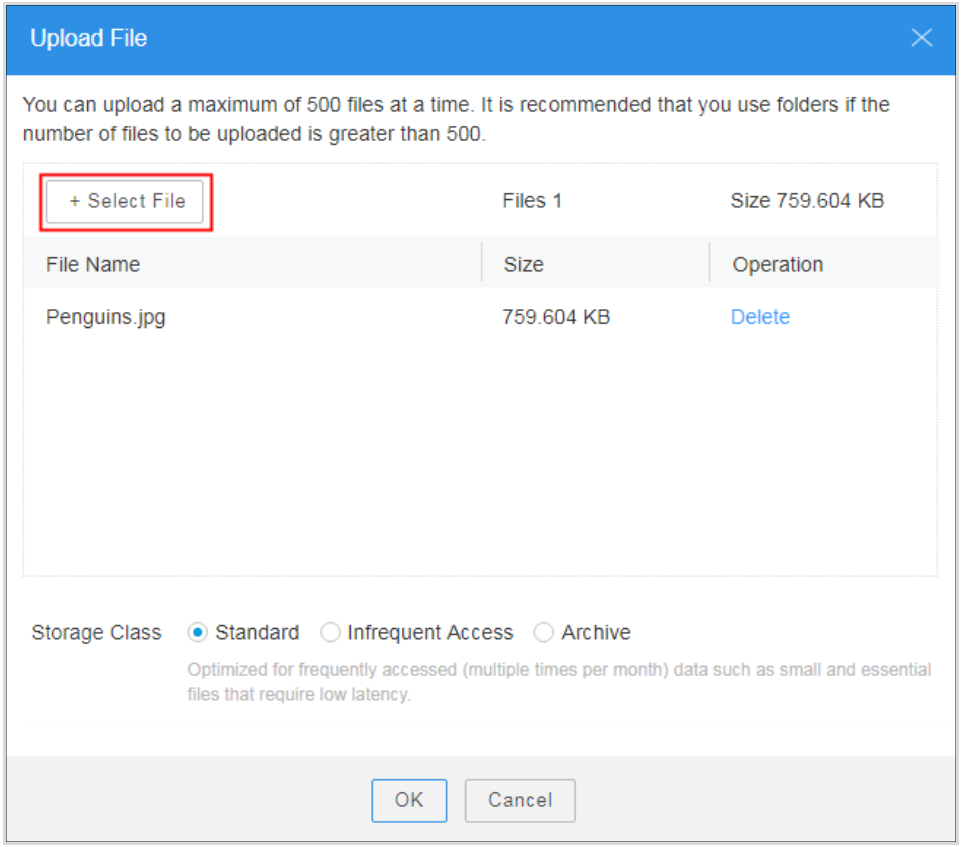
Step 3 **Upload a file.**

- In the **Upload File** dialog box, click **Select File** to select the file to be uploaded, and click **Open**.

NOTE

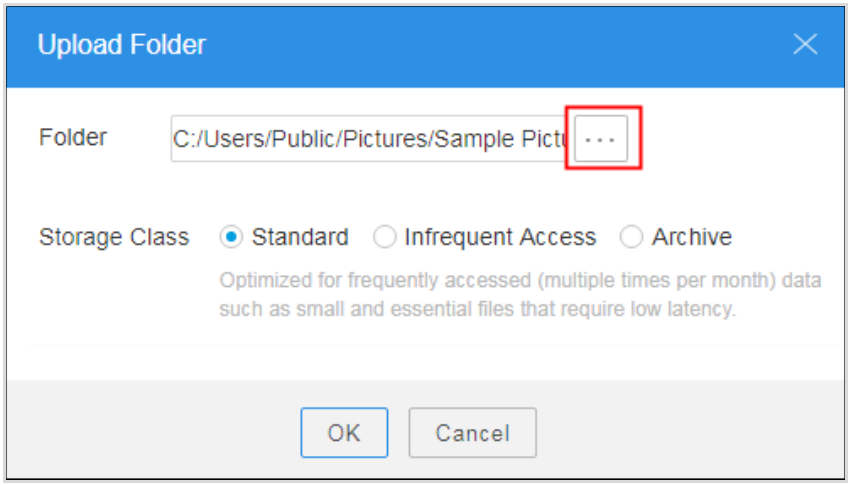
OBS Browser allows multiple files to be uploaded at a time. You can hold down **Ctrl** or **Shift** to select multiple files and batch upload them. You can also select all files by

pressing **Ctrl**+**A**. The operations are consistent with those on the Windows operating system.



- Upload a folder.

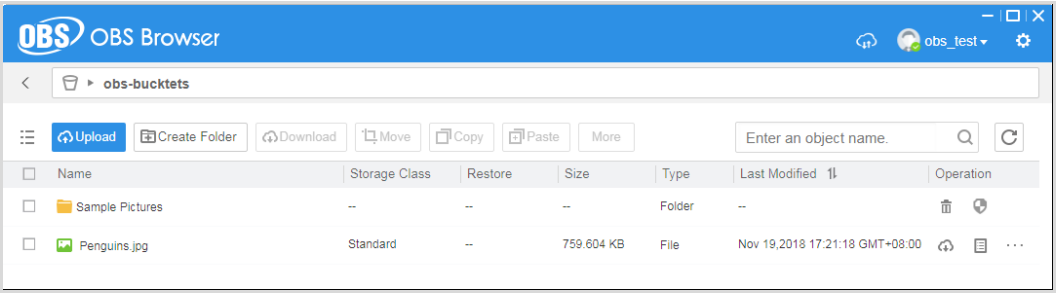
Step 4 **In the Upload Folder dialog box, click ..., select the folder to be uploaded, and click OK.**



Step 5 **After selecting the file or folder to be uploaded, click OK.**

Step 6 **(Optional) Click in the upper right corner of the page to access the task management page. The file or folder upload progress is displayed on the page. You can suspend, delete, or cancel an upload task based on site requirements.**

Step 7 **View the uploaded file or folder in the object list.**



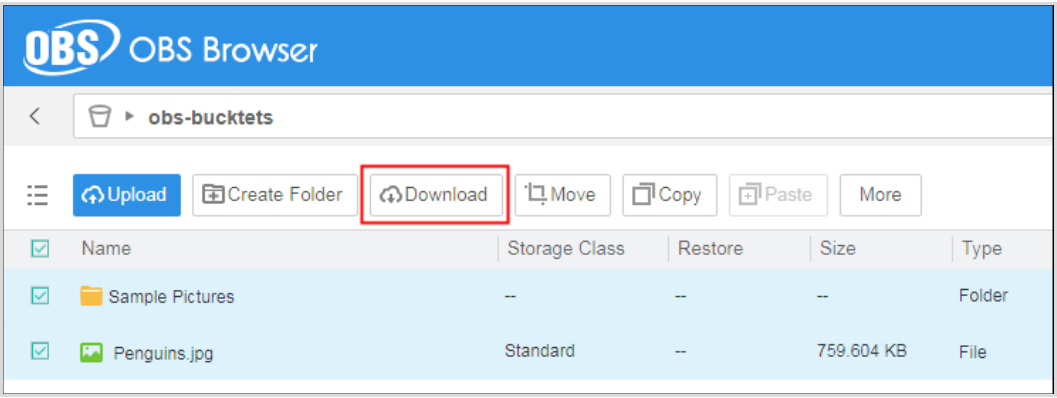
----End

6.3.3.3 Downloading a File or Folder

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

NOTE

You can hold down **Ctrl** or **Shift** to select files or folders and batch download them. You can also select all the files or folders on the current page by pressing **Ctrl+A**. The operations are consistent with those on the Windows operating system.



Step 2 **In the dialog box that is displayed, select a path for saving the file or folder, and then click OK.**

Step 3 **(Optional) Click in the upper right corner of the page to access the task management page. The file or folder download progress is displayed on the**

page. You can suspend, delete, or cancel a download task based on site requirements.

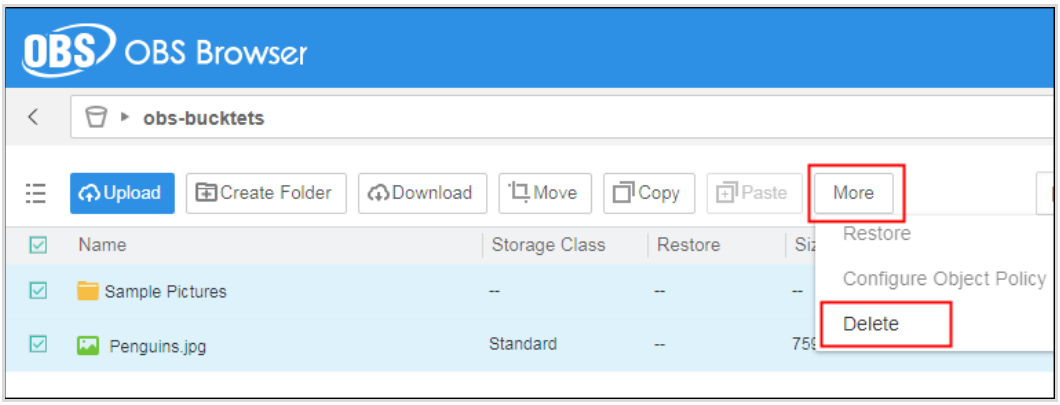
----End

6.3.3.4 Deleting a File or Folder

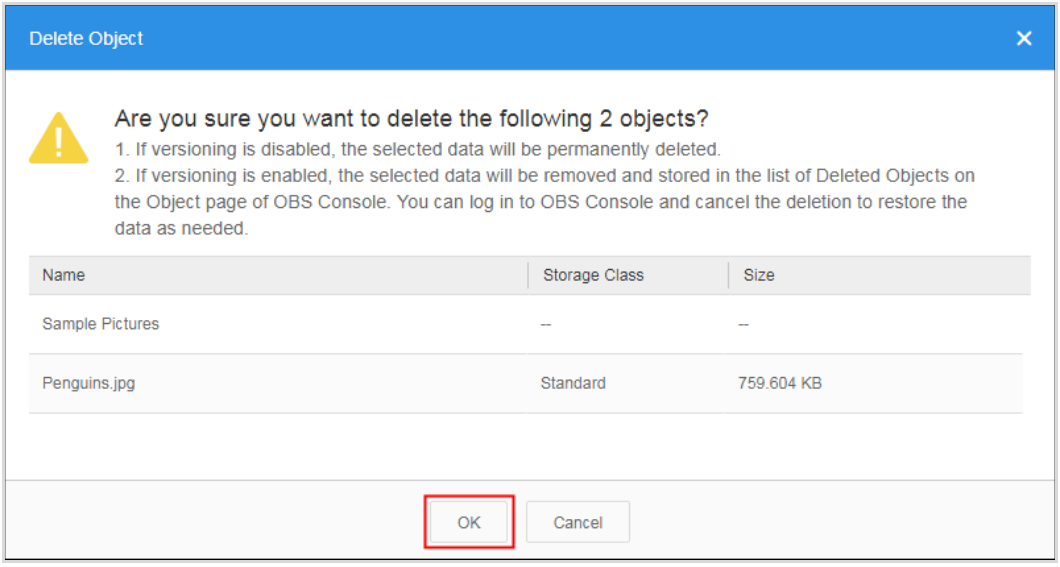
Step 1 **On the object list page, select the file or folder to be deleted, and choose More > Delete.**

NOTE

You can hold down **Ctrl** or **Shift** to select multiple files or folders and batch delete them. You can also select all the files or folders on the current page by pressing **Ctrl+A**. The operations are consistent with those on the Windows operating system.



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

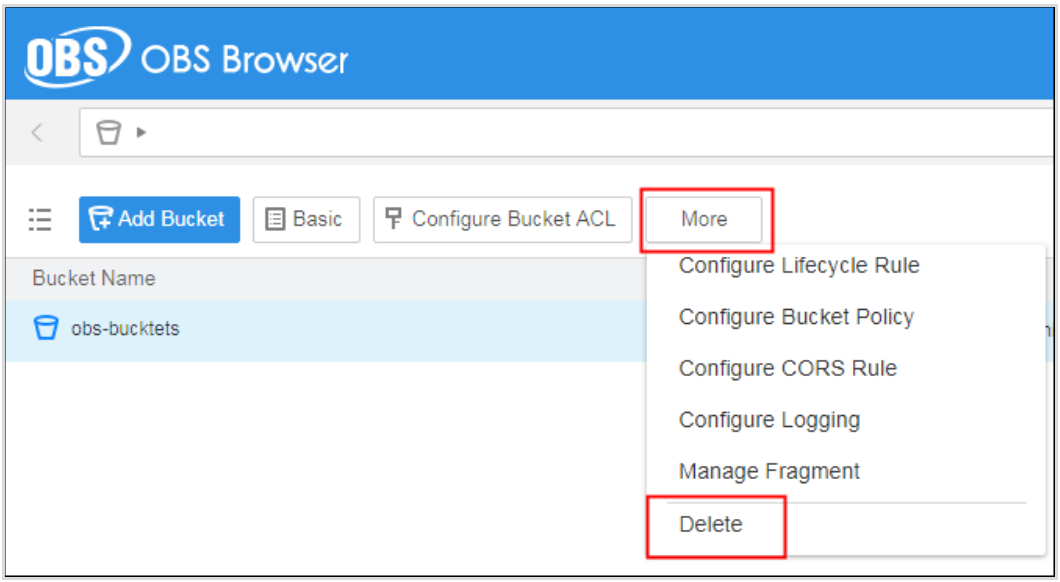


Step 3 **(Optional) Click in the upper right corner of the page to access the task management page. The file or folder deletion progress is displayed on the page. You can suspend, delete, or cancel a deletion task based on site requirements.**

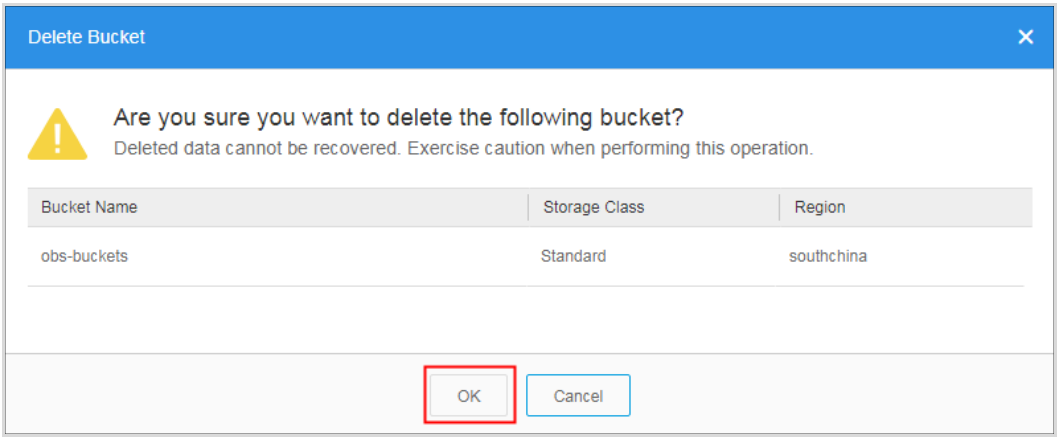
----End

6.3.3.5 Deleting a Bucket

Step 1 **Select the bucket to be deleted and choose More > Delete.**



Step 2 **In the Delete Bucket confirm dialog box, click OK.**



Step 3 **Check whether the bucket exists on the bucket list page. If not, it is successfully deleted.**

----End

7 Scalable File Service

7.1 About This Exercise

This experiment describes basic operations of Scalable File Service (SFS).

7.1.1 Objective

- Create shared file systems.
- Delete shared file systems.
- Mount a shared file system on an elastic cloud server (ECS).

7.1.2 Prerequisites

You have registered an account with HUAWEI CLOUD.

A Linux ECS bound with an elastic IP address (EIP) has been obtained.

7.1.3 List of Tasks

No.	Task	Sub-Task	Application Scenario
1	Creating shared file systems	Creating a file system	Creating a file system
		Creating file systems in a batch	Creating file systems in a batch
2	Deleting shared file systems	Deleting a file system	Deleting a file system
		Deleting	Deleting file systems in a batch

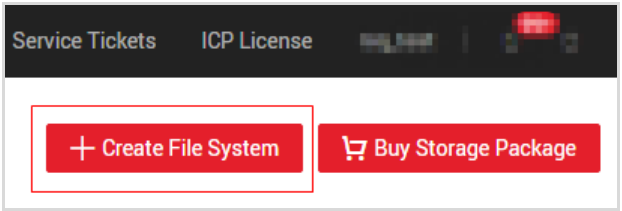
No.	Task	Sub-Task	Application Scenario
		file systems in a batch	
3	Mounting a shared file system	Mounting a shared file system	Mount a shared file system on an ECS.
		Unmounting a shared file system	Unmounting a shared file system from an ECS.

7.2 Creating File Systems

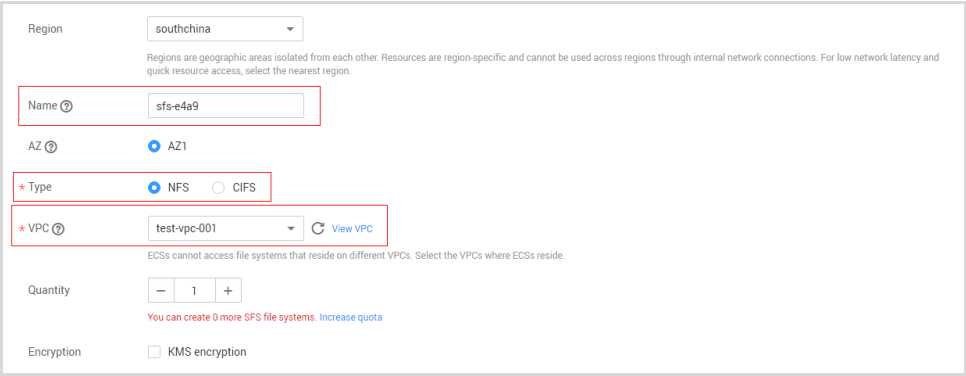
7.2.1 Creating a File System

Step 1 **Log in to SFS Console.**

Step 2 **On SFS Console, click Create File System.**

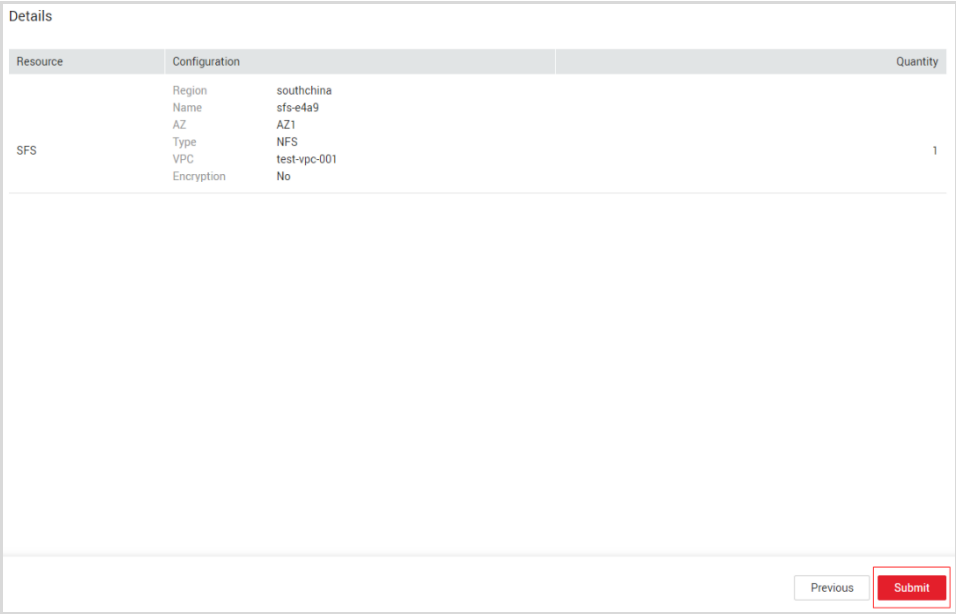


Step 3 **On the page that is displayed, enter the file system name, file system type, and the VPC where the file system resides.**

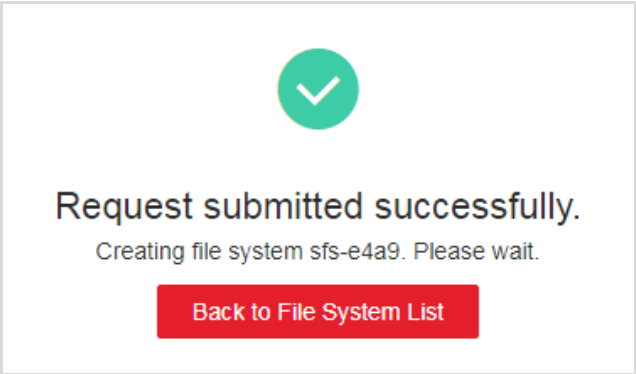


Step 4 **Click Create Now.**

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



Step 6 **A message is displayed, indicating that the request is submitted successfully.**



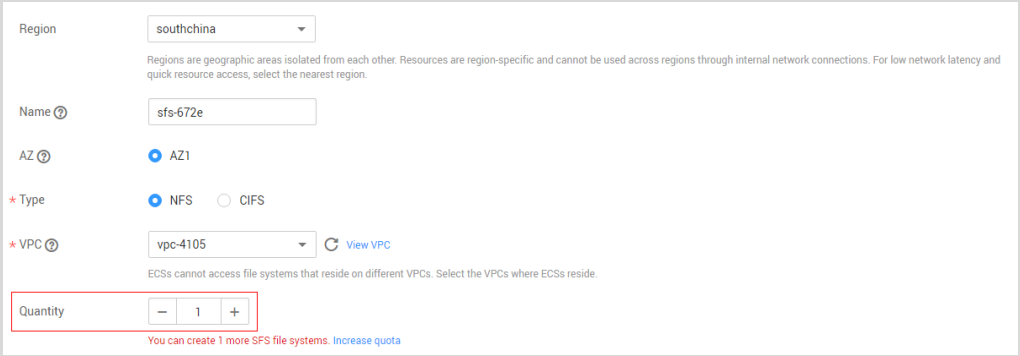
Step 7 **Go back to the file system list and view whether the file system is created.**

Name	AZ	Status	Type	Share Protocol
sfs-e4a9	AZ1	Available	SFS Capacity-Ori...	NFS

----End

7.2.2 Creating File Systems in a Batch

Step 1 **The procedure for creating SFS shared file systems in a batch is similar to that for creating a shared file system. The number of shared file systems that can be created is subject to the remaining system quota.**



----End

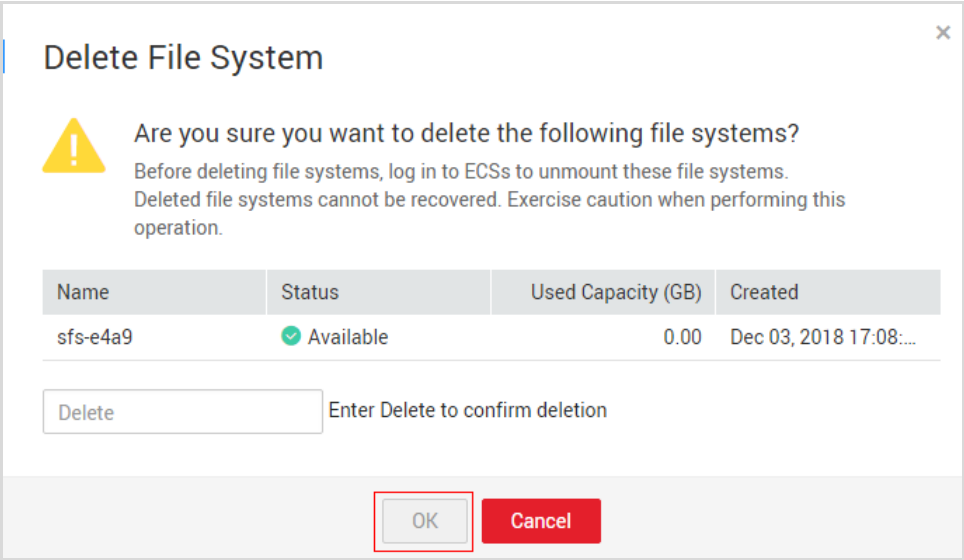
7.3 Deleting File Systems

7.3.1 Deleting a File System

Step 1 **Log in to SFS Console.**

Step 2 **In the list of file systems, click Delete at the end of the row where an SFS Capacity-Oriented file system resides, or Unsubscribe at the end of the row where an SFS Turbo file system resides.**

Step 3 **For an SFS Capacity-Oriented file system, confirm the information in the displayed dialog box, enter Delete in the text box, and then click OK. For an SFS Turbo file system, complete the unsubscription procedure as prompted.**



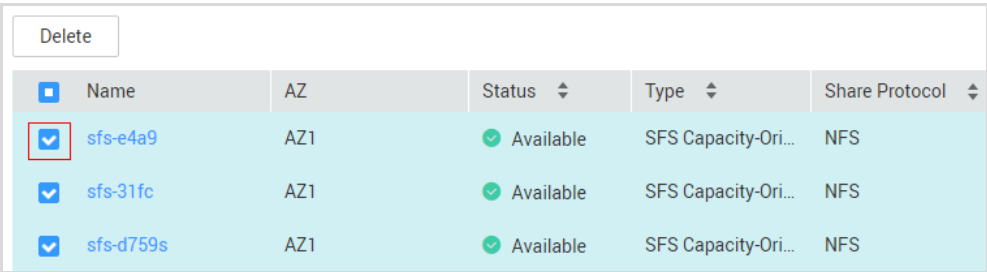
Step 4 **The status of the file system changes to Deleting. Refresh the page later. When the file system is no longer displayed in the list, it is deleted successfully.**

----End

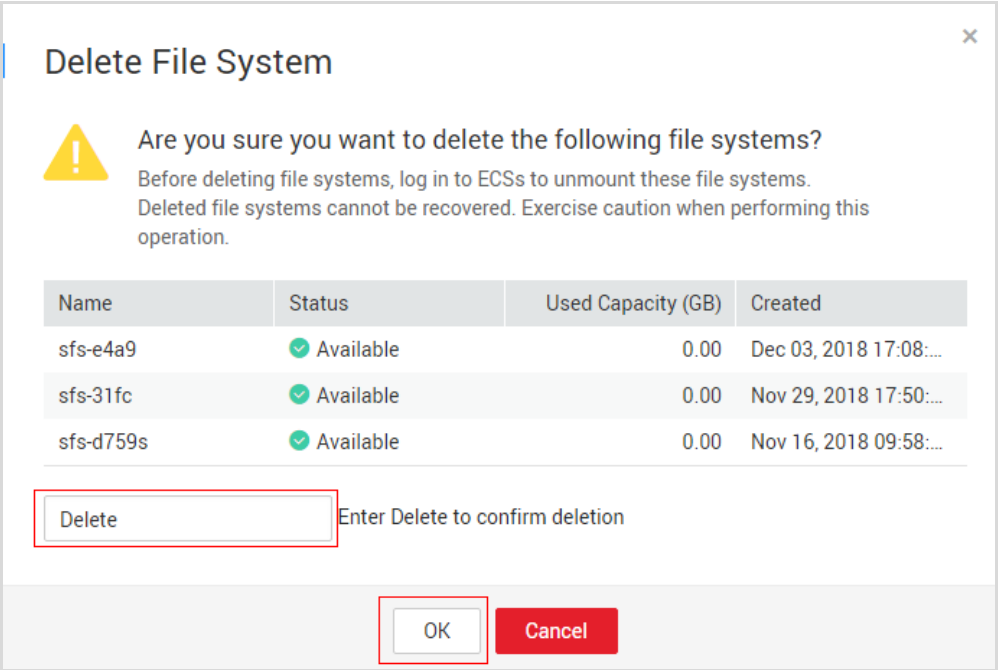
7.3.2 Deleting File Systems in a Batch

Step 1 **Log in to SFS Console.**

Step 2 **Select file systems you want to delete or select all file systems by ticking the box in the header of the list.**



Step 3 **At the upper left corner, click Delete. Enter Delete and then click OK in the displayed confirmation dialog box.**



Step 4 **The status of the selected file systems changes to Deleting. Refresh the page later. When the file systems are no longer displayed in the list, they are deleted successfully.**

----End

7.4 Mounting a File System on an ECS

Step 1 **Log in to ECS Console.**

Step 2 **Click Remote Login on the row of an ECS.**

Step 3 **Log in to the ECS using the root account and password (for example, Huawei@12).**

```
CentOS Linux 7 (Core)
Kernel 3.10.0-327.el7.x86_64 on an x86_64

ecs-be39 login: root
Password:
  ##############################################################################
  #                              Notice                                        #
  #                                                                            #
  #  1. Please create unique passwords that use a combination of words,#
  #   numbers, symbols, and both upper-case and lower-case letters.            #
  #   Avoid using simple adjacent keyboard combinations such as                #
  #   "Qwert!234","Qaz2wsx",etc.                                               #
  #                                                                            #
  #  2. Unless necessary, please DO NOT open or use high-risk ports,           #
  #   such as Telnet-23, FTP-20/21, NTP-123(UDP), RDP-3389,                    #
  #   SSH/SFTP-22, Mysql-3306, SQL-1433,etc.                                   #
  #                                                                            #
  #                                                                            #
  #                      Any questions please contact 4000-955-988             #
  ##############################################################################
[root@ecs-be39 ~]#
```

Step 4 **Run the following command to check whether the NFS software package has been installed in the operating system (generally available in the operating system).**

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

Step 5 **If information similar to the following is displayed, the NFS software package has been successfully installed. The command output varies according to operating systems.**

```
libnfsidmap-0.25-11.x86_64
nfs-utils-1.3.0-0.9.x86_64
```

Step 6 **If the NFS software package is not installed, install it by following instructions as follows:**

- For operating systems CentOS, Red Hat, Euler OS, Fedora, and Oracle Enterprise Linux, run the following command:

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

- For operating systems Debian and Ubuntu, run the following command:

```
sudo apt-get install nfs-common
```

- For operating systems SUSE and OpenSUSE, run the following command:

```
zypper install nfs-client
```

Step 7 **Configure the DNS server for resolving domain names of file systems. For the IP address of the DNS server, see the HUAWEI CLOUD intranet DNS addresses.**

NOTE

By default, the IP address of the DNS server used to parse the domain names of file systems is automatically configured on the ECS when the ECS is created, except when the resolution fails due to a change in the DNS server IP address.

Step 8 **On the ECS, configure the DNS server IP address. (do this only if error occour)**

- Run the **vi /etc/resolv.conf** command to edit the **/etc/resolv.conf** file.
- Prior to the two Internet IP addresses, add a line and input the DNS server IP address. (depends on the actual situation)
- Input a pound key (#) in front of the two public IP addresses to comment them out.

- Press **Esc** and input **:wq** to save and exit.
- Run the following command to check whether the IP address has been added successfully.

```
cat /etc/resolv.conf
```

Step 9 **Run the following command to check whether an IP address can be resolved from the file system domain name.**

```
nslookup File system domain name
Type this => nslookup sfs-nas1.sa-brazil-1.myhuaweicloud.com
```

NOTE

Obtain the file system domain name from the file system shared path. If the **nslookup** command fails to be executed, run the **yum install bind-utils** command.

Information similar to the following is displayed if the domain name is successfully resolved:

```
[root@ecs-be39 ~]# nslookup sfs.cn-north-1.hwclouds.com
Server:         100.125.1.250
Address:        100.125.1.250#53

Non-authoritative answer:
Name:   sfs.cn-north-1.hwclouds.com
Address: 100.125.13.32
Name:   sfs.cn-north-1.hwclouds.com
Address: 100.125.13.35
Name:   sfs.cn-north-1.hwclouds.com
Address: 100.125.13.33
Name:   sfs.cn-north-1.hwclouds.com
Address: 100.125.13.28
Name:   sfs.cn-north-1.hwclouds.com
Address: 100.125.13.24
Name:   sfs.cn-north-1.hwclouds.com
Address: 100.125.13.29
Name:   sfs.cn-north-1.hwclouds.com
Address: 100.125.13.25
Name:   sfs.cn-north-1.hwclouds.com
Address: 100.125.13.26
Name:   sfs.cn-north-1.hwclouds.com
Address: 100.125.13.31
Name:   sfs.cn-north-1.hwclouds.com
Address: 100.125.13.34
Name:   sfs.cn-north-1.hwclouds.com
Address: 100.125.13.30
Name:   sfs.cn-north-1.hwclouds.com
Address: 100.125.13.27
```

Step 10 **Run the mkdir/local path command to create a local directory for the mounting, for example, mkdir /local_path or mkdir /sfs.**

Type this => sudo mkdir /sfs

Step 11 **Run the following command to mount the created file system to the local path:**

mount -t nfs -o vers=3,timeo=600,nolock *Shared path* ***/sfs***
example => sudo mount -t nfs -o vers=3,timeo=600,nolock sfs-nas1.sa-brazil-1.myhuaweicloud.com:/share-52fcb6f9 /sfs

For an SFS Capacity-Oriented file system, the format of the shared path is *File system domain name*:/Path. For example, **example.com:/share-***xxx.* For an SFS Turbo file system, the format of the shared path is *File system IP address*:/. For example, **192.168.0.0:/**. You can obtain the shared path of a file system in the file system list.

Name	AZ	Status	Type	Share Protocol	Used Capacity (G...	Encrypted	Enterprise Pr...	Share Path	Operation
sfs-fa98	AZ1	Available	SFS Capacity-O...	NFS	0.00	No	default	sfs-nas1 /share-6872b26b	Resize Delete
sfs-name-c650	AZ1	Available	SFS Capacity-O...	CIFS	0.00	Yes	default	\\sfs-nas1 \share-c4158baa	Resize Delete

Step 12 **Run the mount –l command to check the mounted file system.**

Example => sudo mount -l

```
[root@ecs-be39 /]# mount -t nfs -o vers=3,timeo=600,nolock sfs-nas1.cn-north-1.myhuaweicloud.com:/share-7b88e5d0 /local_path
[root@ecs-be39 /]# 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=490808k,nr_inodes=124528,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=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/systemd/systemd-cgrou
ps-agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
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/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpuacct,cpu)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
configfs on /sys/kernel/config type configfs (rw,relatime)
/dev/vda1 on / type ext3 (rw,relatime,data=ordered)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=28,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=9665
)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw,relatime)
nfsd on /proc/fs/nfsd type nfsd (rw,relatime)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=101588k,mode=700)
sfs-nas1.cn-north-1.myhuaweicloud.com:/share-7b88e5d0 on /local_path type nfs (rw,relatime,vers=3,rsize=1048576,wsize=1048576,na
mlen=255,hard,nolock,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=100.125.16.91,mountvers=3,mountport=2050,mountproto=udp,loc
al_lock=all,addr=100.125.16.91)
```

Step 13 **Create a document named new in the local /sfs and edit it through vim.**

Step 14 **cd /sfs**

Step 15 **vim new**

Step 16 **Edit the document new and save it.**

```
Hello HuaweiCloud SFS
~
~
~
~
~
~
~
~
~
~
```

Step 17 **Run the cat /sfs/new to view the document content.**

----End

7.5 Unmounting a File System

Step 1 **Log in to ECS Console.**

Step 2 **In the ECS list, click Remote Login on the row of the ECS from which the file system is to be unmounted.**

Step 3 **In the displayed ECS window, run the following command to unmount the shared file system:**

umount /sfs of the file system
sample => **sudo umount /sfs**

----End

8 Virtual Private Cloud

8.1 Introduction

8.1.1 About This Exercise

This exercise introduces the Virtual Private Cloud (VPC) service and describes how to create a VPC and related resources, how to create an Elastic Cloud Server (ECS) and bind an elastic IP address (EIP) to the ECS, and how to use security groups to control communication between two ECSs in a VPC.

8.1.2 Objectives

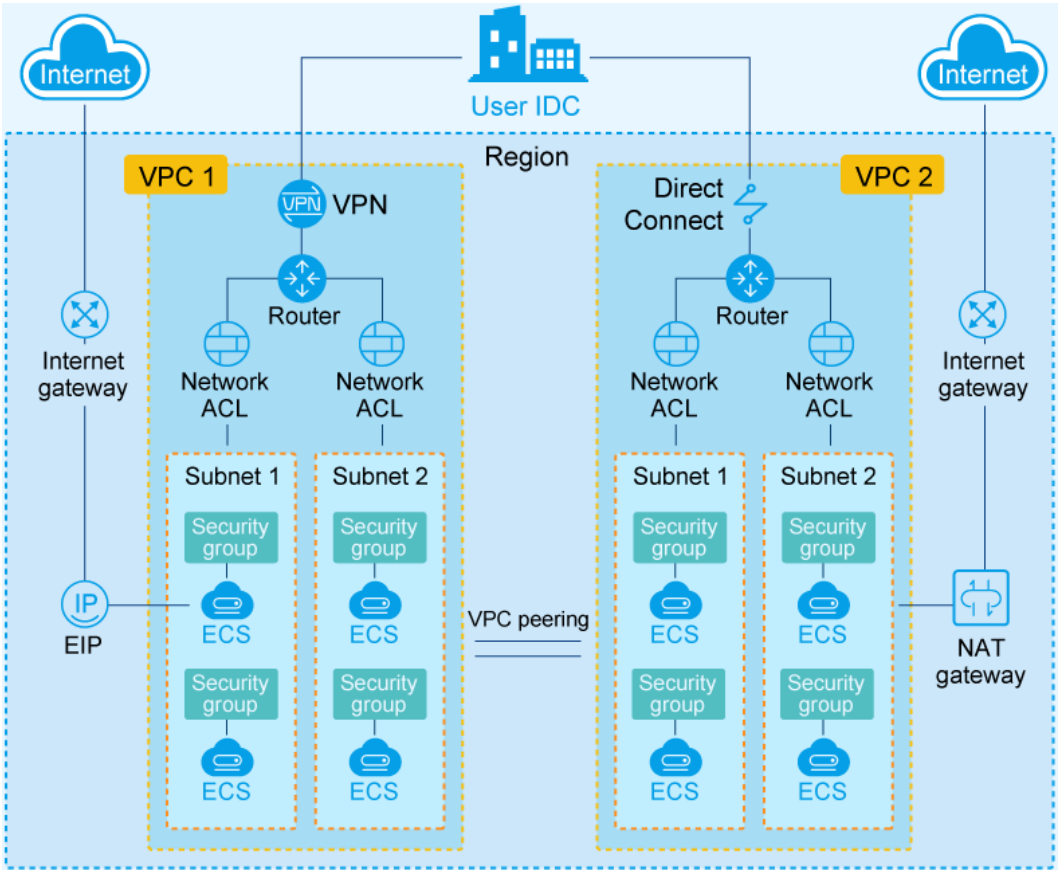
- Have a good command of VPC operations and related resources
- Learn how to bind an EIP.
- Know how access traffic from the Internet to ECSs will be directed.
- Understand security group functions and know how to perform required operations on security groups.

8.1.3 Prerequisites

You have registered a HUAWEI CLOUD account.

Create an ECS called **ecs-myserver (without EIP)**

8.1.4 VPC Service Overview and Topology



8.1.5 Task List

SN	Task	Subtask
1	Creating a VPC and a subnet	Creating a VPC
		Creating a subnet
2	Creating a security group and adding rules	Creating a security group
		Adding security group rules
3	Buying an EIP and binding it to an ECS	Buying an EIP
		Binding an EIP to an ECS

4	Controlling ECS access using a security group	Deleting a security group rule to interrupt communication between ECSs in the security group and other resources
		Adding a security group rule to enable communication between ECSs in the security group and other resources

8.2 Creating a VPC and a Subnet

Step 1 **Log in to the management console.**

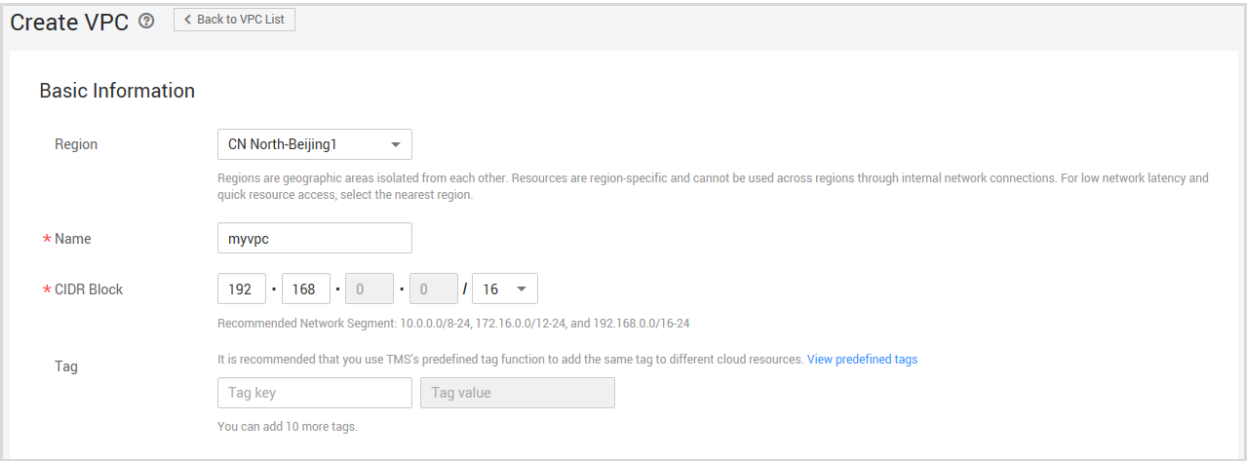
Step 2 **Choose Service List > Virtual Private Cloud.**

Step 3 **Click Create VPC.**

Step 4 **Configure VPC parameters.**

Basic Information

- Set Region to AP-Hong Kong.
- Set **Name** to **myvpc**.
- Set CIDR Block to 192.168.0.0/16.

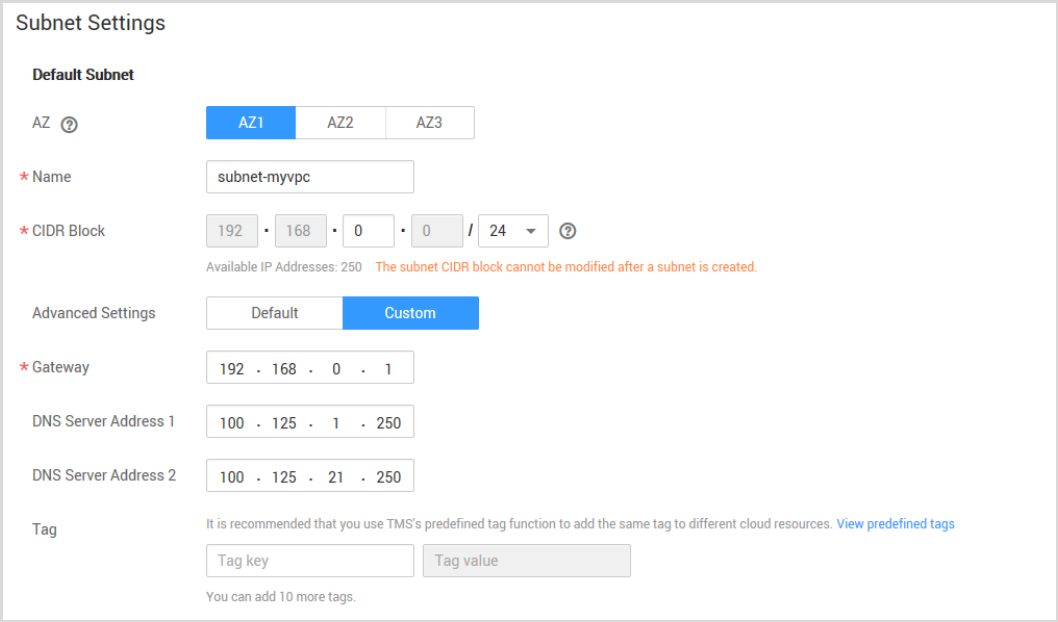


Subnet Settings

You can click **Advanced Settings (custom)** to configure the gateway and DNS server addresses.

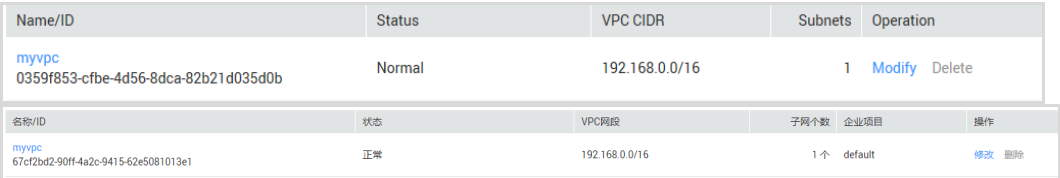
-

- Set Name to subnet-myvpc.
- Set CIDR Block to 192.168.0.0/24.
- Set Gateway to 192.168.0.1.
- Retain the default value for **DNS Server Address 1**.
- Retain the default value for **DNS Server Address 2**.



Step 5 **Click Create Now.**

Step 6 **View the created VPC in the VPC list.**



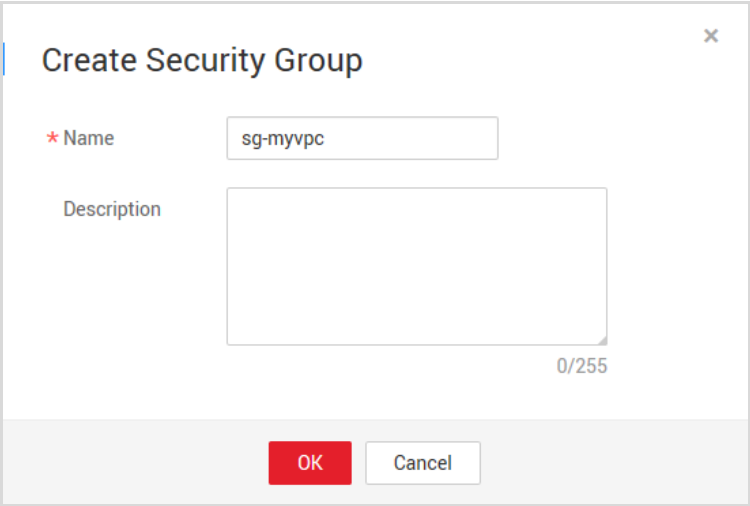
----End

8.3 Creating a Security Group and Adding Rules

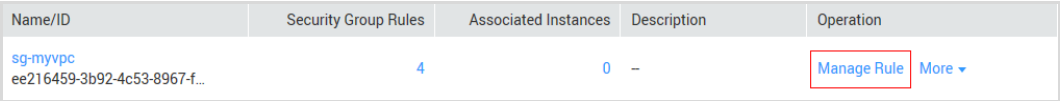
Step 1 **In the navigation pane on the left, choose Security Group.**

Step 2 **Click Create Security Group.**

Step 3 **Set Name to sg-myvpc.**

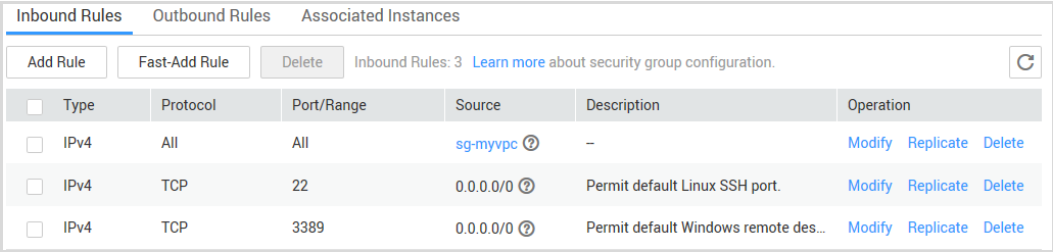


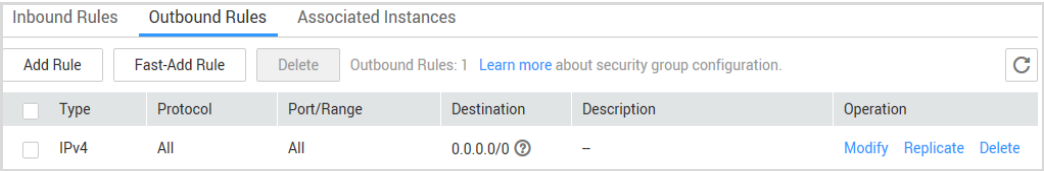
Step 4 **Locate the created security group and click Manage Rule.**



Step 5 **Add rules on the Inbound Rules and Outbound Rules tabs.**

- In this exercise, the default security group rules are used.





----End

8.4 Buying an EIP and Binding It to an ECS

8.4.1 Scenario

An ECS has been created for this exercise. You need to buy an EIP and bind it to the ECS to enable the ECS to access the Internet through this EIP.

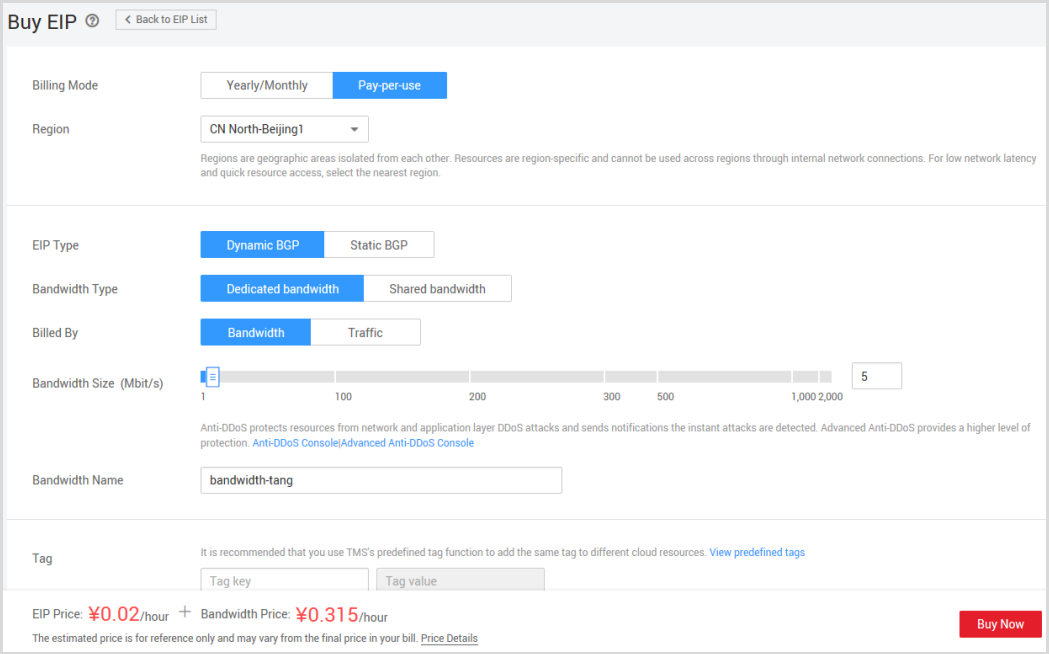
8.4.2 Configuration Step

Step 1 **Choose Service List > Elastic IP.**

Step 2 **Click Buy EIP.**

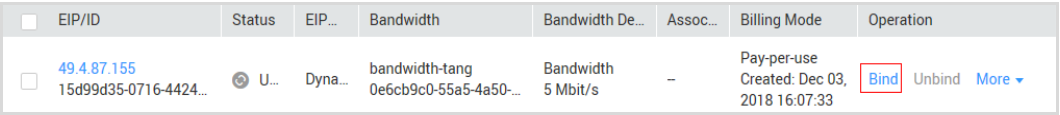
Step 3 **Configure EIP parameters.**

- Set Billing mode to Pay-per-use.
- Set Region to AP-Hong Kong
- Set EIP Type to Dynamic BGP.
- Set Bandwidth Type to Dedicated bandwidth.
- Set Billed By to Bandwidth.
- Set Bandwidth Size to 5 Mbit/s.
- Set Bandwidth Name to bandwidth-defb.
- Set **Quantity** to **1**.



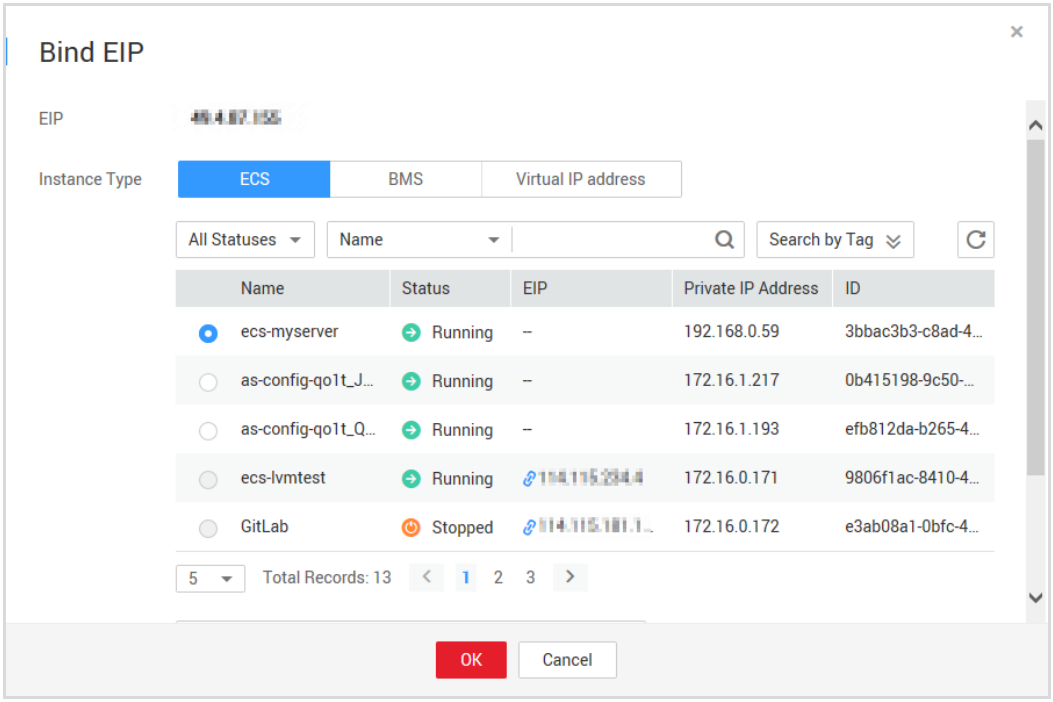
Step 4 **Click Buy Now.**

Step 5 **Locate the target EIP in the EIP list, and click Bind in the Operation column.**

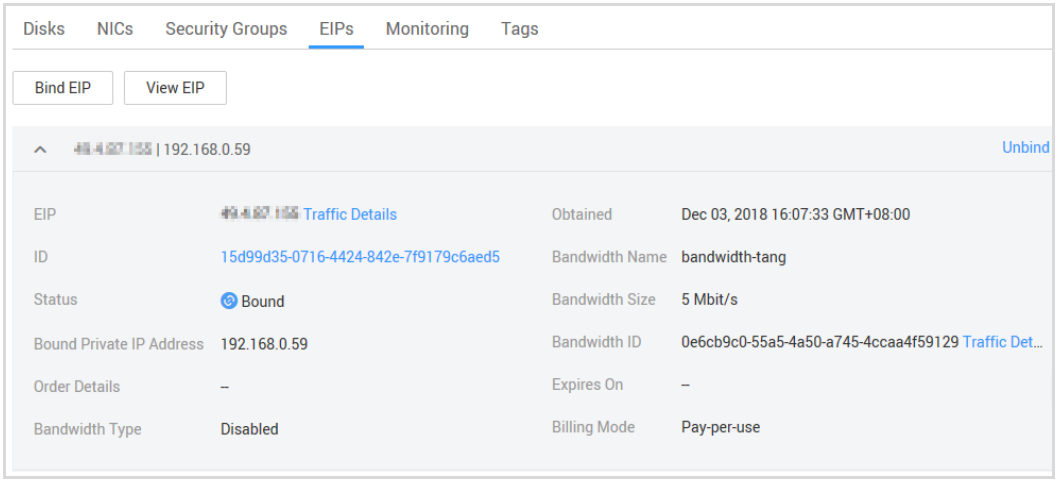


Step 6 **Bind the EIP to the ECS.**

- Select ECS **ecs-myserver**.
- Select the primary NIC, for example, the NIC whose IP address is **192.168.0.59**.



Step 7 **Choose Service List > Elastic Cloud Server. On the displayed page, check the EIP bound to ECS ecs-myserver.**



----End

8.4.3 Verification

Log in to the ECS remotely and run the following command to check whether the communication between the ECS and the Internet is normal:

- ping www.huawei.com

```
[root@ecs-myserver ~]# ping www.huawei.com
PING huawei.dtwscache.ourwebcdn.com (103.254.188.61) 56(84) bytes of data.
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=1 ttl=48 time=3.34 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=2 ttl=48 time=3.40 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=3 ttl=48 time=3.04 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=4 ttl=48 time=3.03 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=5 ttl=48 time=2.94 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=6 ttl=48 time=3.03 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=7 ttl=48 time=3.00 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=8 ttl=48 time=3.07 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=9 ttl=48 time=2.93 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=10 ttl=48 time=3.08 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=11 ttl=48 time=2.99 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=12 ttl=48 time=2.98 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=13 ttl=48 time=2.90 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=14 ttl=48 time=3.55 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=15 ttl=48 time=3.03 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=16 ttl=48 time=3.89 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=17 ttl=48 time=3.02 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=18 ttl=48 time=3.00 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=19 ttl=48 time=2.85 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=20 ttl=48 time=2.97 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=21 ttl=48 time=3.03 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=22 ttl=48 time=3.68 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=23 ttl=48 time=2.99 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=24 ttl=48 time=2.95 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=25 ttl=48 time=3.04 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=26 ttl=48 time=2.97 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=27 ttl=48 time=3.09 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=28 ttl=48 time=3.91 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=29 ttl=48 time=3.04 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=30 ttl=48 time=2.96 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=31 ttl=48 time=2.93 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=32 ttl=48 time=3.03 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=33 ttl=48 time=2.94 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=34 ttl=48 time=3.63 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=35 ttl=48 time=2.99 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=36 ttl=48 time=3.13 ms
64 bytes from 103.254.188.61 (103.254.188.61): icmp_seq=37 ttl=48 time=2.91 ms
^C
--- huawei.dtwscache.ourwebcdn.com ping statistics ---
37 packets transmitted, 37 received, 0% packet loss, time 36057ms
rtt min/avg/max/mdev = 2.856/3.119/3.917/0.278 ms
```

8.5 Controlling ECS Access Using a Security Group

8.5.1 Scenario

Create a VPC and create two Linux ECSs in the VPC. Bind EIPs to the ECSs, and then configure security group rules to control ECS access.

8.5.2 Configuration Step

Step 1 **Create two ECSs in the same VPC and bind EIPs to the two ECSs.**

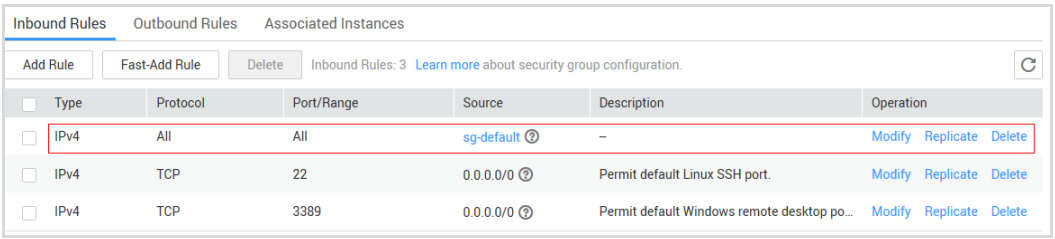
ecs-myserver-0001 9806f1ac-8410-4bcc-afbc-f92d3ed81408	AZ1	Running	1 vCPUs | 1 GB | s2.small.1 CentOS 7.4 64bit	117.78.50.186 (EIP) 5 Mbit/s 192.168.2.204 (Private IP)
ecs-myserver-0002 1b51cfb9-14e6-4350-aaff-c92f195189b8	AZ1	Running	1 vCPUs | 1 GB | s2.small.1 CentOS 7.4 64bit	117.78.50.169 (EIP) 5 Mbit/s 192.168.2.123 (Private IP)

You can run the following command to verify that the default security group rules allow communication between the two ECSs in the same VPC:

- ping 192.168.2.123

```
[root@ecs-myserver-0001 ~]# ping 192.168.2.123
PING 192.168.2.123 (192.168.2.123) 56(84) bytes of data.
64 bytes from 192.168.2.123: icmp_seq=1 ttl=64 time=0.864 ms
64 bytes from 192.168.2.123: icmp_seq=2 ttl=64 time=0.435 ms
64 bytes from 192.168.2.123: icmp_seq=3 ttl=64 time=0.545 ms
64 bytes from 192.168.2.123: icmp_seq=4 ttl=64 time=0.406 ms
64 bytes from 192.168.2.123: icmp_seq=5 ttl=64 time=0.462 ms
64 bytes from 192.168.2.123: icmp_seq=6 ttl=64 time=0.288 ms
```

Step 2 **Delete the inbound security group rule with Type set to IPv4, Protocol set to All, Port/Range set to All, Source set to the current security group sg-default.**



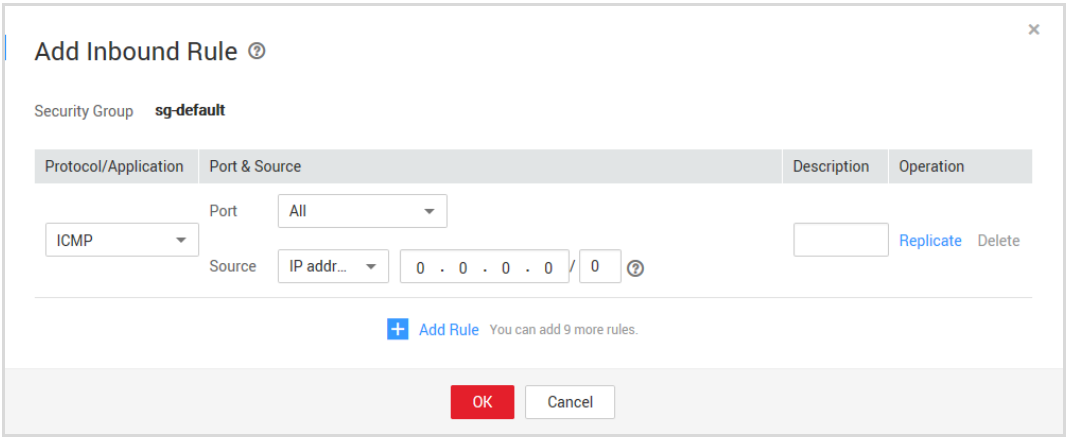
- Verify that the two ECSs cannot communicate with each other.

```
[root@ecs-myserver-0001 ~]# ping 192.168.2.123
PING 192.168.2.123 (192.168.2.123) 56(84) bytes of data.
^C
--- 192.168.2.123 ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 10999ms

[root@ecs-myserver-0001 ~]# _
```

Step 3 **Configure the following parameters to add an inbound security group rule.**

- Set Protocol to ICMP.
- Set **Port** to **All**.
- Set Source to IP address and 0.0.0.0/0.



----End

8.5.3 Verification

Check network communication.

- Run the **ping *ECS private IP address*** command to verify internal network communication of the ECS. For example, run the **ping 192.168.2.123** command.

```
[root@ecs-myserver-0001 ~]# ping 192.168.2.123
PING 192.168.2.123 (192.168.2.123) 56(84) bytes of data.
64 bytes from 192.168.2.123: icmp_seq=1 ttl=64 time=0.630 ms
64 bytes from 192.168.2.123: icmp_seq=2 ttl=64 time=0.474 ms
64 bytes from 192.168.2.123: icmp_seq=3 ttl=64 time=0.578 ms
64 bytes from 192.168.2.123: icmp_seq=4 ttl=64 time=0.426 ms
64 bytes from 192.168.2.123: icmp_seq=5 ttl=64 time=0.584 ms
64 bytes from 192.168.2.123: icmp_seq=6 ttl=64 time=0.327 ms
64 bytes from 192.168.2.123: icmp_seq=7 ttl=64 time=0.302 ms
64 bytes from 192.168.2.123: icmp_seq=8 ttl=64 time=0.292 ms
```

- Run the **ping *ECS EIP*** command to verify public network communication of the ECS. For example, run the **ping 117.78.50.169** command.

```
[root@ecs-myserver-0001 ~]# ping 117.78.50.169
PING 117.78.50.169 (117.78.50.169) 56(84) bytes of data.
64 bytes from 117.78.50.169: icmp_seq=1 ttl=55 time=1.71 ms
64 bytes from 117.78.50.169: icmp_seq=2 ttl=55 time=2.12 ms
64 bytes from 117.78.50.169: icmp_seq=3 ttl=55 time=1.21 ms
64 bytes from 117.78.50.169: icmp_seq=4 ttl=55 time=1.05 ms
```

9 Elastic Load Balance

9.1 Introduction

9.1.1 About This Exercise

This exercise describes how to use Elastic Load Balance (ELB) to access the HTTP service on VMs.

9.1.2 Objective

After this exercise, you will be able to:

- Perform basic operations on the ELB console.
- Know how to create a load balancer.
- Configure load balancers and associated resources.

9.1.3 Networking

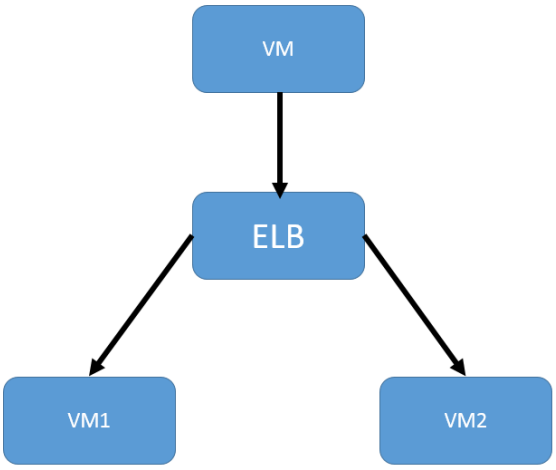


Figure 9-1 Topology

9.1.4 Prerequisites

- You have registered an account on HUAWEI CLOUD.
- A load balancer has been created.
- Two ECSs that run a Linux OS are available.

9.1.5 Exercise Planning

Table 9-1 Resource configurations

SN	Item	Configuration
1	Load balancer	Network type: public network IP address: 114.116.115.1 Load balancing protocol and port: HTTP/8881 Server protocol and port: HTTP/8889
2	Backend server (VM 1)	Specifications: 2 vCPUs, 4 GB memory, Linux CentOS Private IP address: 192.168.0.20 (Optional) EIP: 10.154.75.139
3	Backend server (VM 2)	Specifications: 2 vCPUs, 4 GB memory, Linux CentOS Private IP address: 192.168.0.21 (Optional) EIP: 10.154.75.142
4	Client	Local PC

9.1.6 Task List

SN	Task	Subtask	Remarks
1	Create a load balancer.	Create a load balancer.	ELB provides a cost-effective and transparent method to expand the bandwidth of network devices and servers, increase the throughput, enhance the network processing capability, and improve the flexibility and availability of the network.
		Add a listener.	A listener is configured with a protocol and port for receiving requests from the client, a protocol and port for routing the requests to backend servers, and other configurations for routing the requests, such as load balancing algorithm.
		Add backend servers.	Add the two ECSs to the listener.
2	Enable the HTTP service on backend servers.	Configure the security group.	Add security group rules.
		Enable the HTTP service.	Run the **touch** command to create separate files on two backend servers.

9.2 Procedure

9.2.1 Creating a Load Balancer

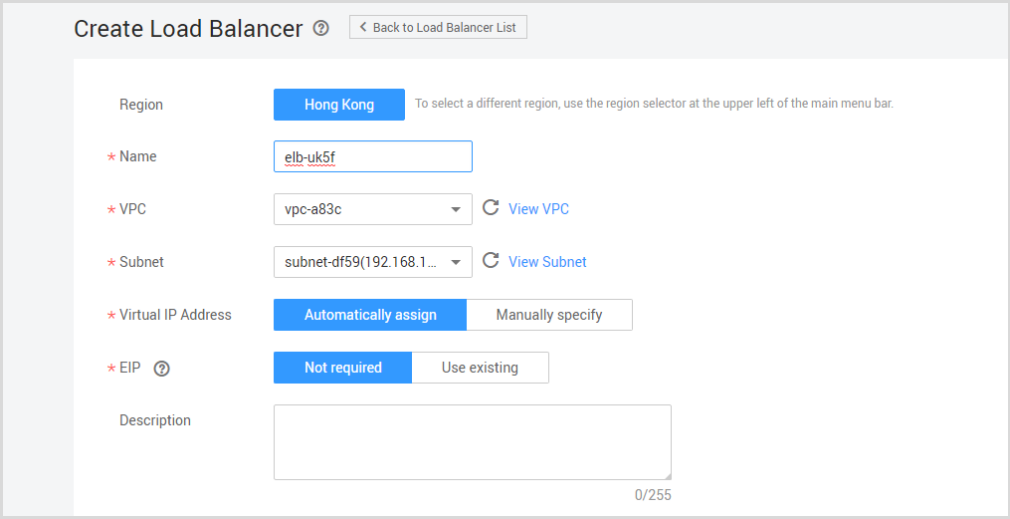
Step 1 **Log in to the management console.**

Step 2 **Click Service List. Under Network, click Elastic Load Balance.**

Step 3 **On the Elastic Load Balance page, click Create Load Balancer.**

Step 4 **On the Create Load Balancer page, set parameters as needed and click Next.**

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



----End

9.2.2 Adding a Listener

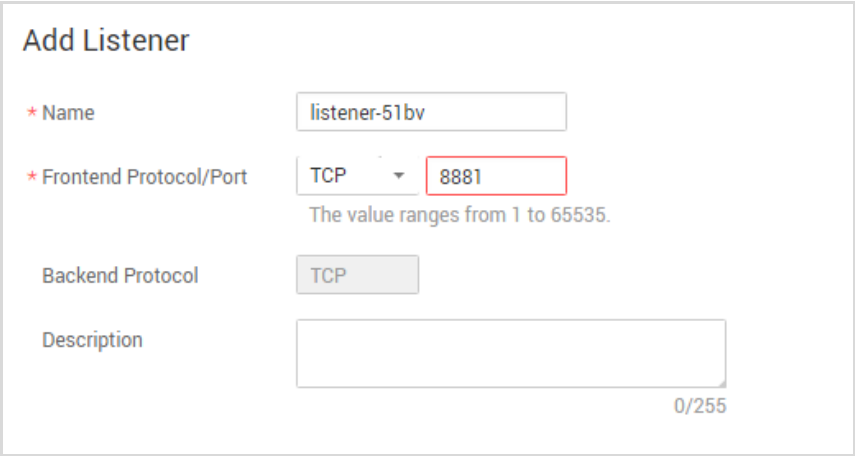
Step 1 **Log in to the management console.**

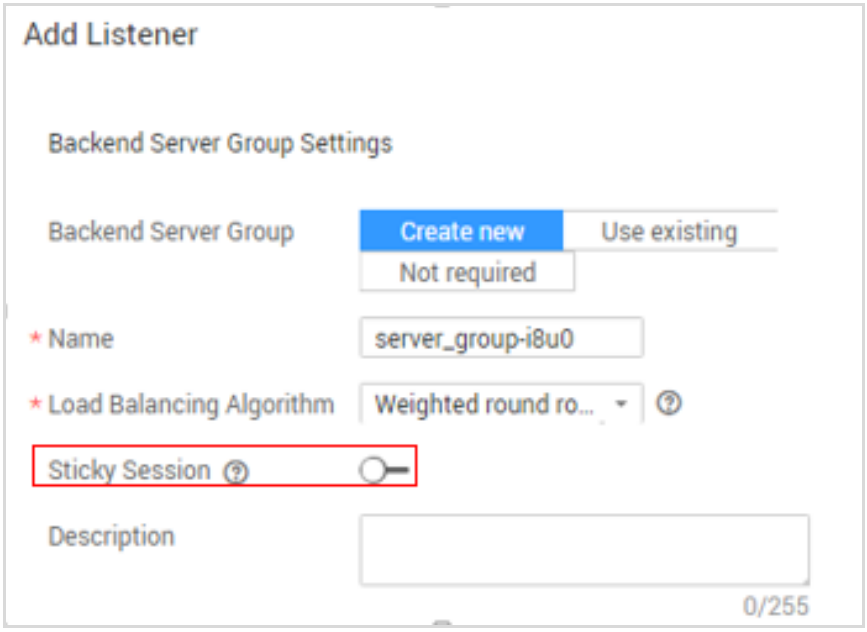
Step 2 **Click Service List. Under Network, click Elastic Load Balance.**

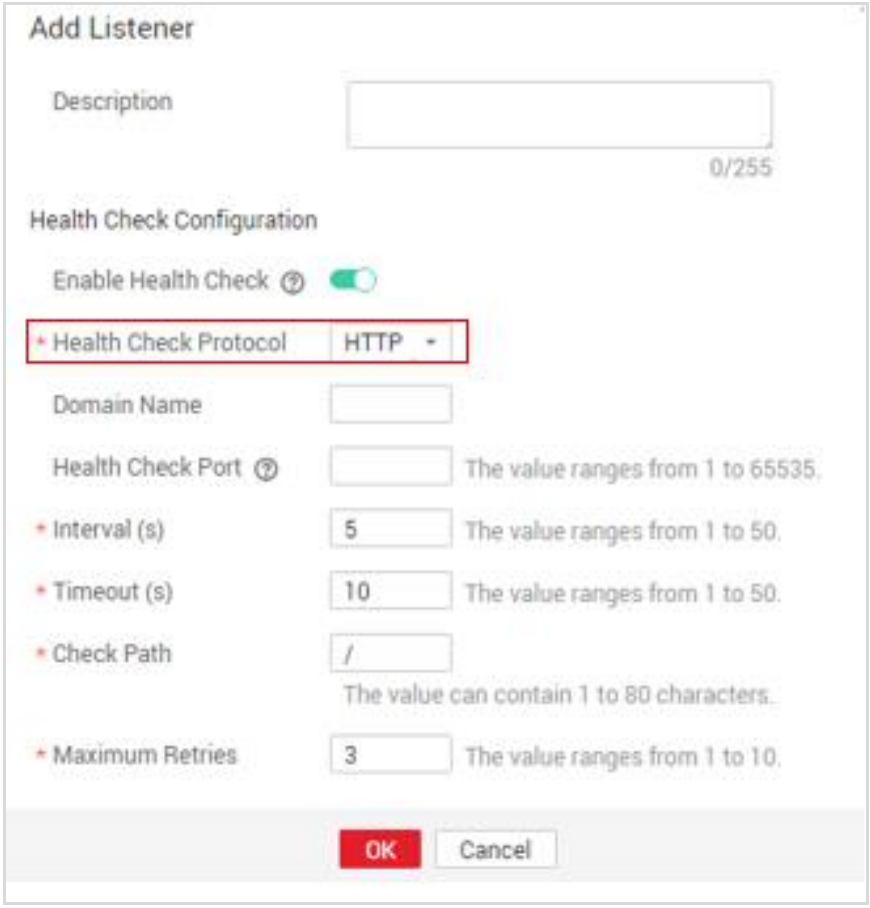
Step 3 **On the Elastic Load Balance page, locate the target load balancer and click its name.**

Step 4 **Under Listeners, click Add Listener.**

Step 5 **In the Add Listener dialog box, set parameters based on Table 9-1 and click Next. Backend Protocol need to be set to TCP 8889, Frontend to TCP 8881**







NOTE

Disable the sticky session feature. Health check port need to be set to HTTP 8889

----Click ok

9.2.3 Adding Backend Servers

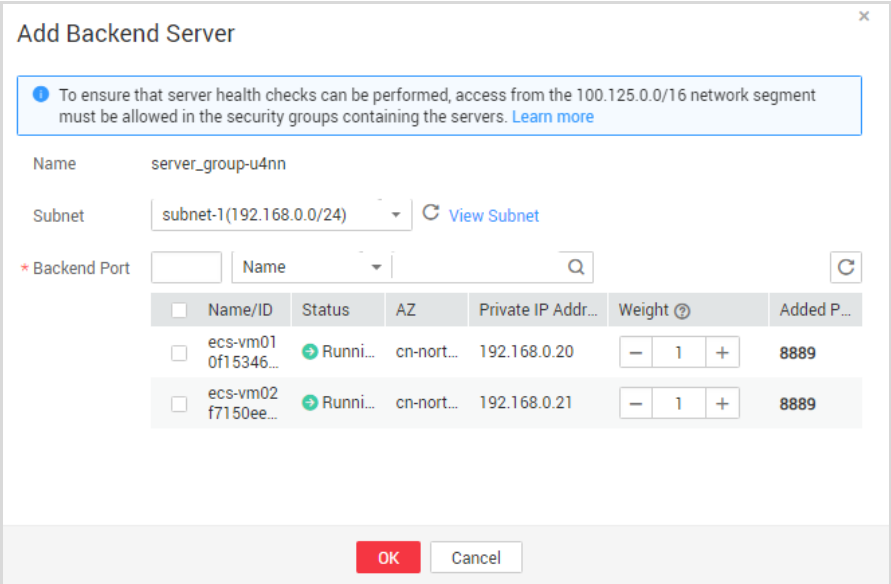
Step 1 **Log in to the management console.**

Step 2 **Click Service List. Under Network, click Elastic Load Balance.**

Step 3 **On the Elastic Load Balance page, click the name of the target load balancer.**

Step 4 **Under Backend Server Groups, locate the target backend server group and choose More > Add Backend Server in the Operation column.**

Step 5 **Select the target servers, set 8889 as backend port and click OK.**



----End

9.2.4 Enabling the HTTP Service on Backend Servers

Step 1 **On the VPC console, add port 8889 to the security group of the two backend servers.**

Step 2 **Log in to the two backend servers and enable the HTTP service on port 8889.**

Run the command nohup python -m SimpleHTTPServer %s > /dev/null 2>&1 & to enable the HTTP service. **%s** in the command indicates port 8889.

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

Run the command curl 127.0.0.1:8889 to verify the HTTP service is enabled.

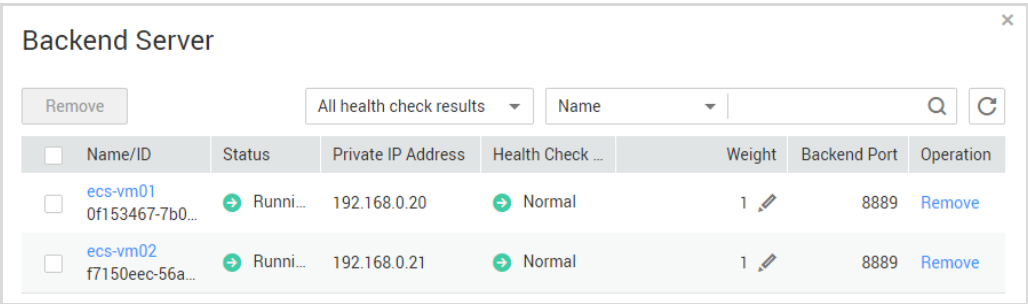
```
[root@ecs-vm01 ~]# nohup python -m SimpleHTTPServer 8889 > /dev/null 2>&1 &
[1] 1301
[root@ecs-vm01 ~]# curl 127.0.0.1:8889
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</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=".cache/">.cache/</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".oracle_jre_usage/">.oracle_jre_usage/</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
<li><a href=".tcshrc">.tcshrc</a>
<li><a href="nohup.out">nohup.out</a>
</ul>
<hr>
</body>
</html>
[1]+  Exit 1                  nohup python -m SimpleHTTPServer 8889 > /dev/null 2>&1
[root@ecs-vm01 ~]#
```

Step 3 **Run the touch command to create an empty file on each server.**

Example => touch SERVER1 (at backend1) and touch SERVER2 (at backend2)

```
[root@ecs-vm01 ~]# touch SERVER1
[root@ecs-vm01 ~]# ll
total 560
-rw------- 1 root root 572202 Dec  6 21:03 nohup.out
-rw-r--r-- 1 root root      0 Dec  6 21:03 SERVER1
[root@ecs-vm01 ~]#
```

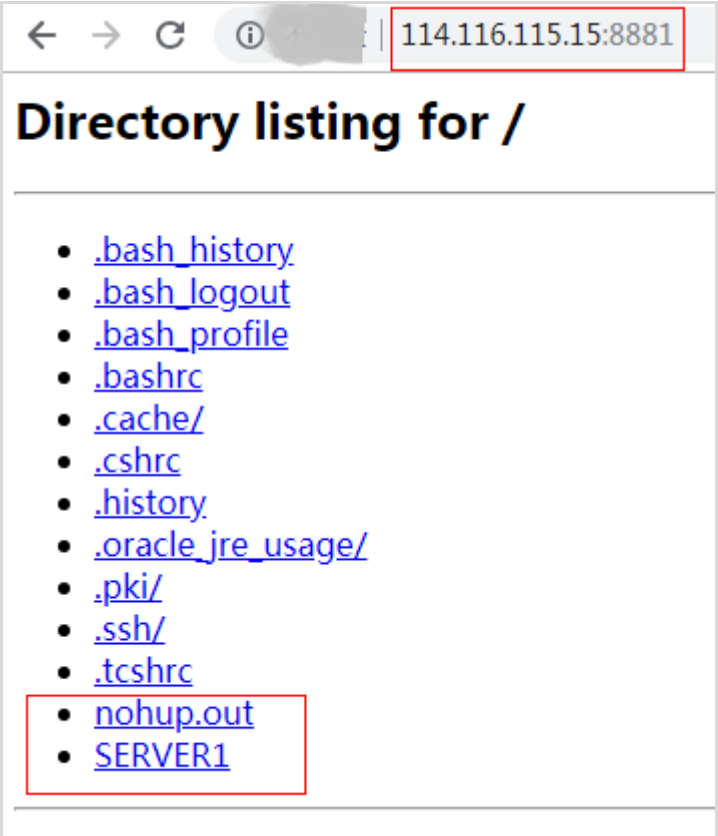
Step 4 **Check the health status of the two backend servers.**



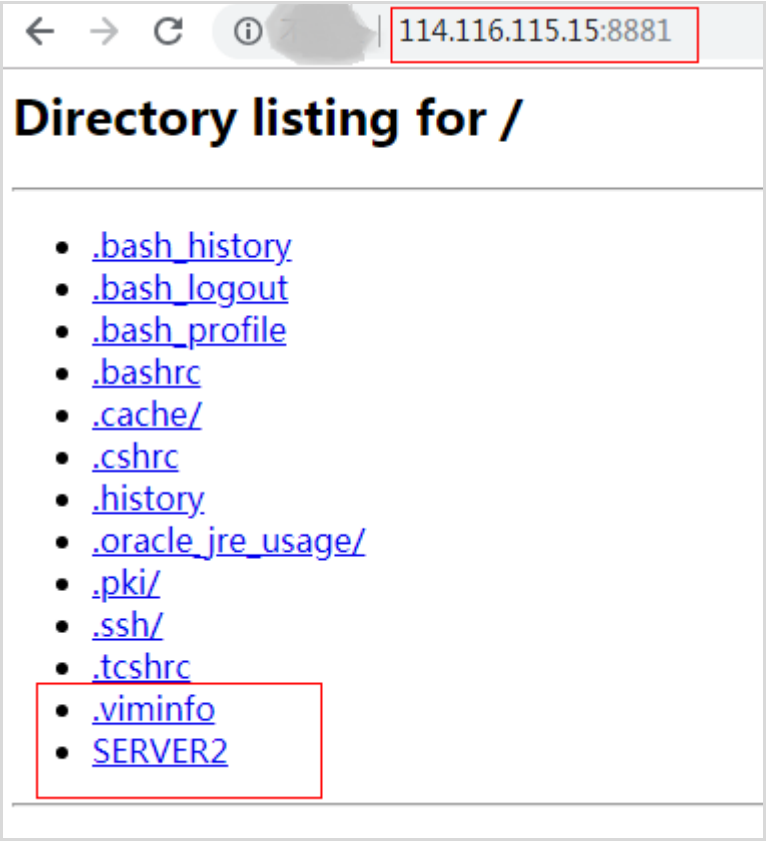
----End

9.3 Verification

Enter "**http://Load_Balance_IP:8881/**"in browser to see if the following result is in a browser address bar on the local PC and check whether the following is displayed.



When you refresh the browser, you can see that the two servers appear on the page in turn, indicating that the load balancer can route traffic between two servers.


114.116.115.15:8881
Directory listing for /
.bash_history
.bash_logout
.bash_profile
.bashrc
.cache/
.cshrc
.history
.oracle_jre_usage/
.pki/
.ssh/
.tcshrc
.viminfo
SERVER2

10 Security Service

10.1 Introduction

10.1.1 About the Exercises

The exercises introduce basic operations of Anti-DDoS

10.1.2 Objectives

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

- Enable Anti-DDoS.
- Enable alarm notifications on the Anti-DDoS console.

10.1.3 Prerequisites (try Hong Kong region)

- You have registered an account with HUAWEI CLOUD.
- You have bought Elastic Cloud Servers (ECSs)

You have obtained the elastic IP addresses (EIPs) of two ECSs and password of user **Administrator**.

ECS Name	Requirement	Task
ECS1	Associates with an EIP and runs on 64-bit Windows 2008.	Enable Anti-DDoS
ECS1	Associates with an EIP (optional) and runs on Windows 2008.	Set an IP blacklist.

10.1.4 Lists of Tasks

No.	Task	Subtask	Applicable Scenario
1	Configuration for Anti-DDoS	Set the maximum service traffic	The protected ECS is hit by DDoS attacks.
		Enable alarm notifications.	The protected ECS is hit by DDoS attacks.

10.2 Configuration for Anti-DDoS

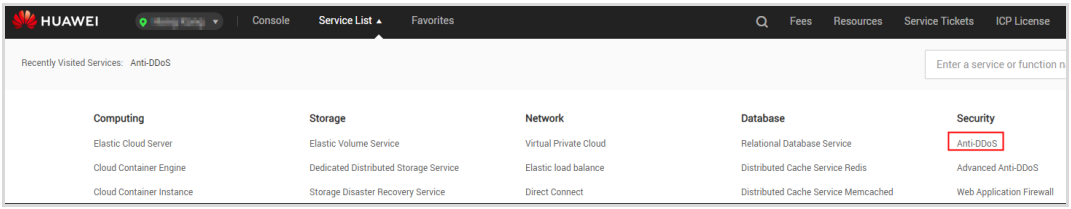
10.2.1 Enabling Anti-DDoS

Enabling Anti-DDoS for an IP address defends the IP address against DDoS attacks.

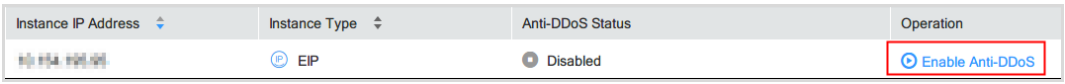
This section introduces how to enable Anti-DDoS for ECS1.

Step 1 **Log in to the management console.**

Step 2 **In the service list, choose Security > Anti-DDoS. The management console is displayed.**

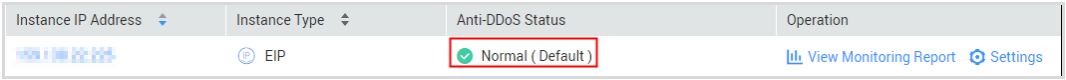


Step 3 **Choose Anti-DDoS > Instances, locate the row containing the IP address of the instance to be protected, and click Enable Anti-DDoS.**



Step 4 **In the dialog box that is displayed, click OK.**

Step 5 **You can view the Anti-DDoS defense status of the IP address on the Instances page.**

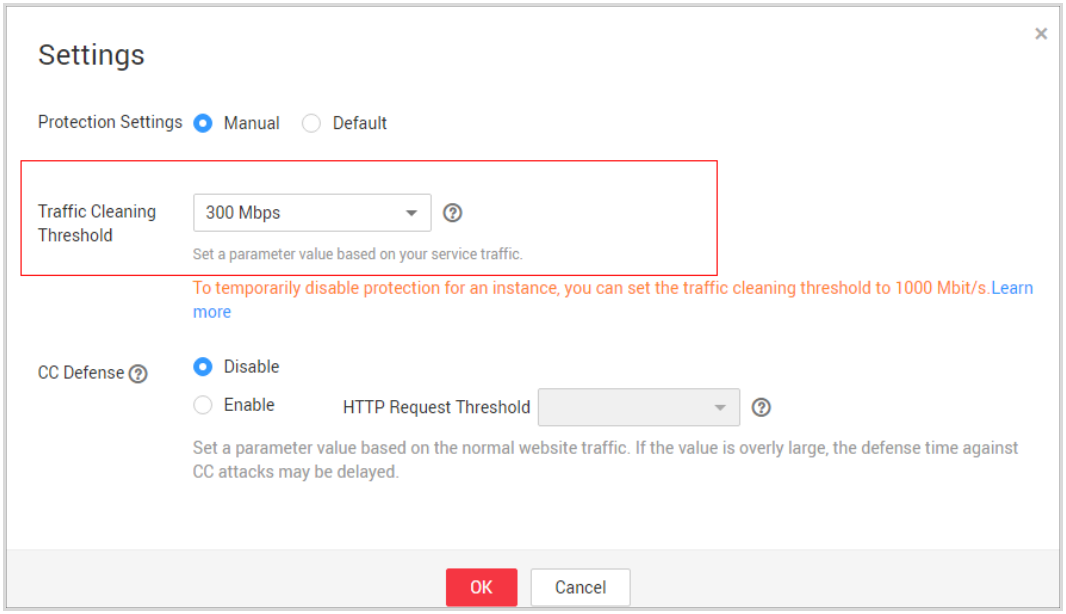


Step 6 **Click Settings and set the traffic cleaning threshold.**

If the service bandwidth purchased for ECS1 is 100 Mbit/s, the value of **Traffic Cleaning Threshold** can be set to 70 Mbit/s.

NOTE

If service traffic triggers Anti-DDoS, only attack traffic is intercepted. If service traffic does not trigger Anti-DDoS, no traffic is intercepted.



Step 7 **Click OK to save the configurations and enable defense.**

----End

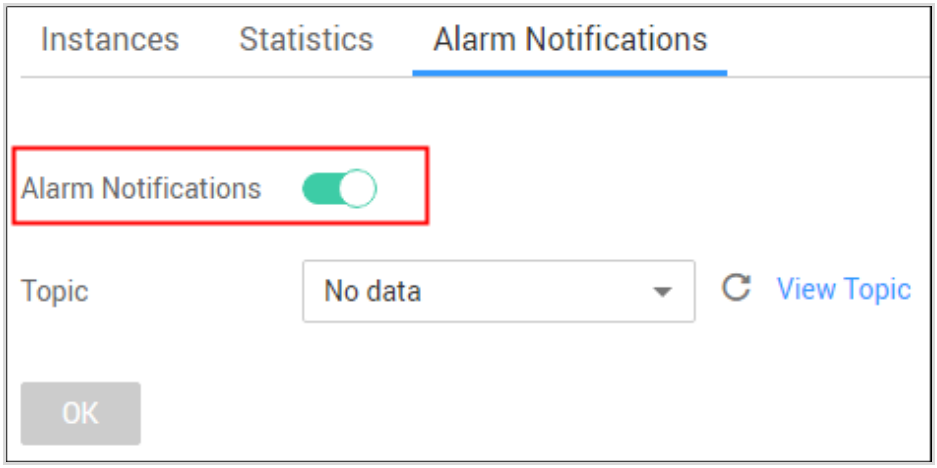
10.2.2 Enabling Alarm Notifications (try Hong Kong Region)

The alarm notifications function sends you alarm notifications (by SMS or email) if a DDoS attack is detected. If you do not enable this function, you have to log in to the management console to view alarms.

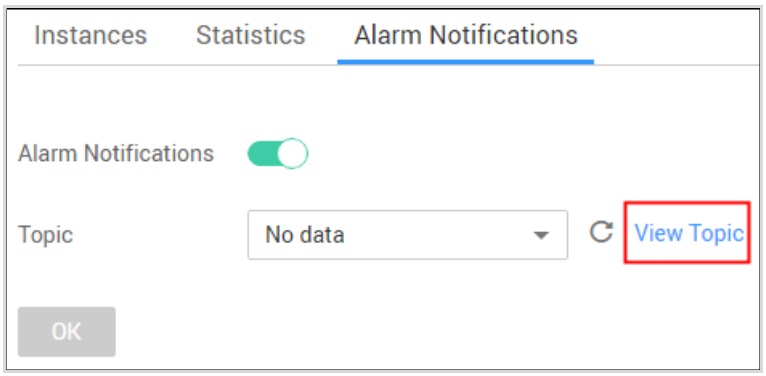
Step 1 **Log in to the management console.**

Step 2 **In the service list, choose Security > Anti-DDoS. The management console is displayed.**

Step 3 **Click the Alarm Notifications tab, and enable the Alarm Notifications function.**

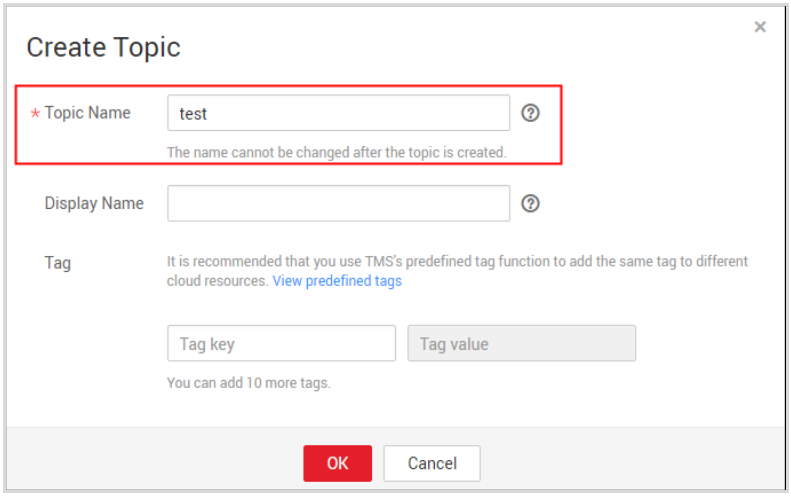


Step 4 **Click View Topic.**



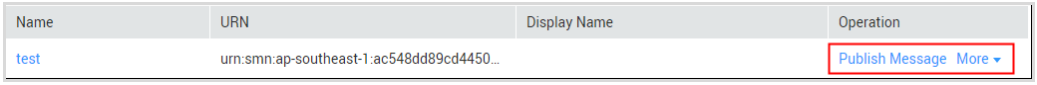
Step 5 **Click Create Topic at the upper right corner.**

Step 6 **In the Create Topic dialog box, enter the name of a topic.**

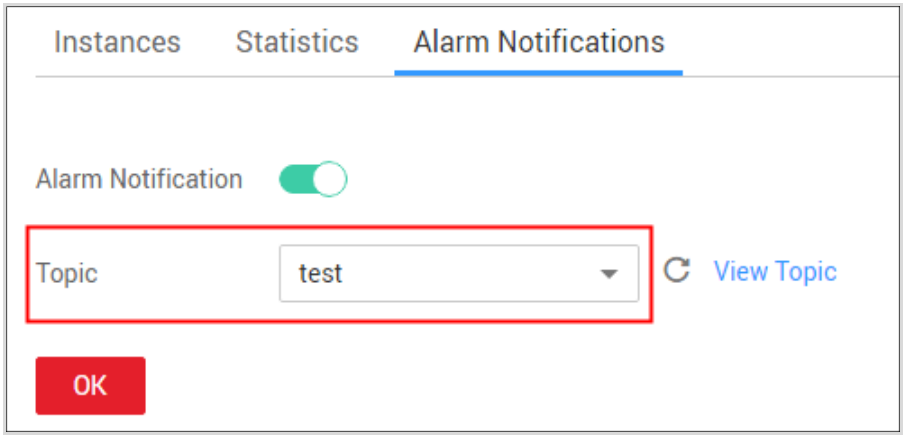


Step 7 **Click OK.**

Step 8 **In the row containing the topic, you can perform operations such as Publish Message and Add Subscription.**



Step 9 **Go back to the Alarm Notifications page, and select the created topic. (You need first to enable one email subscription to allow the drop-box below)**



Step 10 **Click OK to enable alarm notifications.**

11 Cloud Eye

11.1 Introduction

11.1.1 About This Hands-On Exercise

This section describes basic Cloud Eye operations.

11.1.2 Objectives

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

- Use Cloud Eye to monitor Elastic Cloud Servers (ECSs).
- Install and configure the Agent.

11.1.3 Prerequisites

You have obtained an account for logging in to HUAWEI CLOUD.

11.1.4 List of Tasks

No.	Task	Subtask
1	Monitor ECSs.	Create an alarm rule.
		Create a topic and add a subscription.
		View the ECS running status.
2	Install and configure the Agent (Linux). It takes about 3 min to change the agent status	Install the Agent.
		Restore the Agent configurations.
		Manually configure the Agent.
3	Set an Auto Scaling (AS) policy to trigger bandwidth	Scale bandwidth.

No.	Task	Subtask
	scaling.	

11.2 Tasks

11.2.1 Monitoring ECSs

11.2.1.1 Creating an Alarm Rule

11.2.1.1.1 Scenarios

Creating ECS alarm rules helps you track the ECS running status at any time.

This section describes how to set alarm rules, including alarm rule names, monitoring objects, metrics, alarm policies, alarm severities, and notifications.

For details about how to monitor other cloud services, you can also see this section.

11.2.1.1.2 Procedure

Step 1 **Install the agent on ECS (go to task 11.2.2)**

Step 2 **Log in to the management console.**

Step 3 **Under Management & Deployment, select Cloud Eye.**

Step 4 **In the navigation pane on the left, choose Server Monitoring.**

Step 5 **Locate the target ECS. In the Operation column, choose More > Create Alarm Rule.**

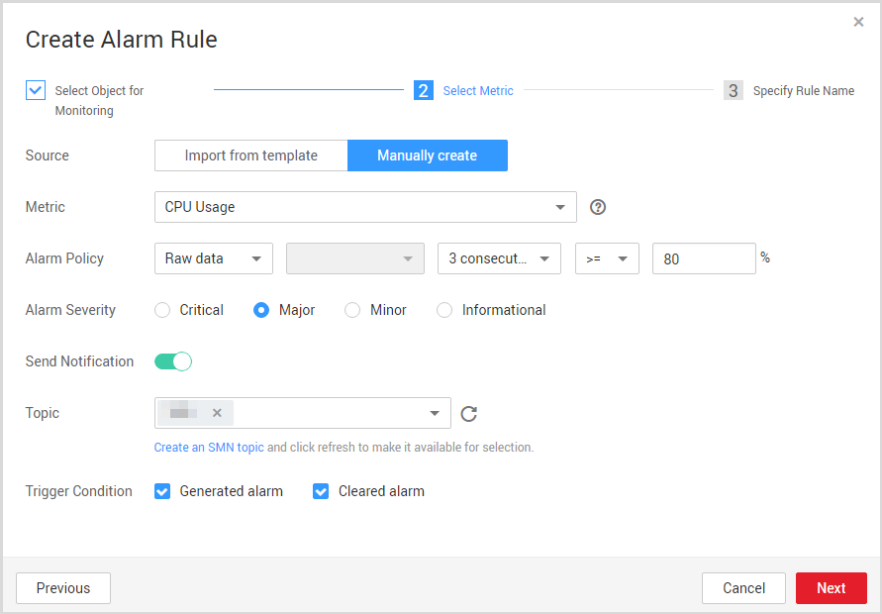
Step 6 **In the Create Alarm Rule dialog box, follow the prompts to set the parameters.**

- You do not need to set the monitored object because it is the current ECS.
- For **Source**, select **Manually create**. Configure parameters based on Table 11-1.
-

Table 11-1 Parameters

Parameter	Description	Example Value
Source	Specifies the means by which you create an alarm rule.	Manually create
Metric	Metrics are the core concept in Cloud Eye. A metric refers to a quantitative value of a resource dimension on the cloud platform, such as the ECS CPU usage and memory usage.	CPU Usage
Alarm Policy	Specifies the policy that triggers an alarm. For example, trigger an alarm if the metric raw data equals to or is greater than 80% for 3 consecutive 5-minute periods.	N/A
Alarm Severity	Specifies the severity of the alarm. Valid values are Critical, Major, Minor, and Informational.	Major
Send Notification	Specifies whether to notify users when alarms are generated or cleared. Notifications can be sent by email or text message, or HTTP/HTTPS request. You can enable (recommended) or disable this function.	Yes
Topic	Specifies the name of the topic to which the alarm notification is sent. If you enable this function, you need to select a topic. If no desired topics are available, you need to create one first, whereupon the Simple Message Notification (SMN) service is invoked. For details about how to create a topic, see the *Simple Message Notification User*	N/A

Parameter	Description	Example Value
	Guide.	
Trigger Condition	Specifies the condition for triggering the alarm notification. You can select Generated alarm, Cleared alarm, or both.	N/A



Step 7 **Click Next. In the Specify Rule Name step, set Name and Description of the alarm rule, and click Finish.**

After the alarm rule is created, if the specified metric reaches the specified threshold, Cloud Eye will immediately inform you that an error has occurred.

11.2.1.2 Creating a Topic and Adding a Subscription

11.2.1.2.1 Scenarios

A topic is a specified event to publish messages and subscribe to notifications. It serves as a message sending channel, where publishers and subscribers can interact with each other.

11.2.1.2.2 Procedure

Step 1 **Log in to the management console.**

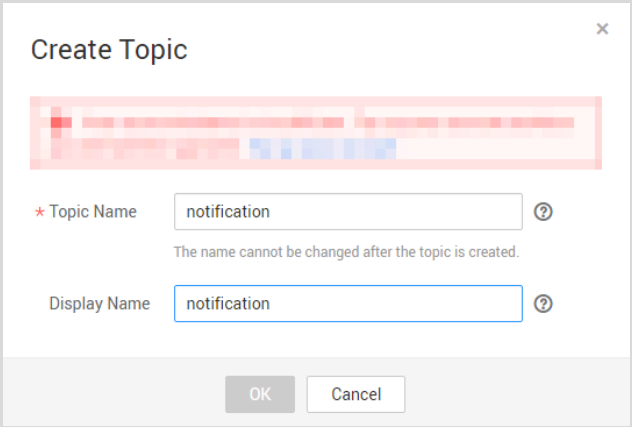
Step 2 **Under Application, select Simple Message Notification.**

Step 3 **In the navigation pane of the SMN console, choose Topic Management > Topics, and click Create Topic in the upper right corner.**

Step 4 **Enter a topic name and display name.**

Table 11-2 Parameters

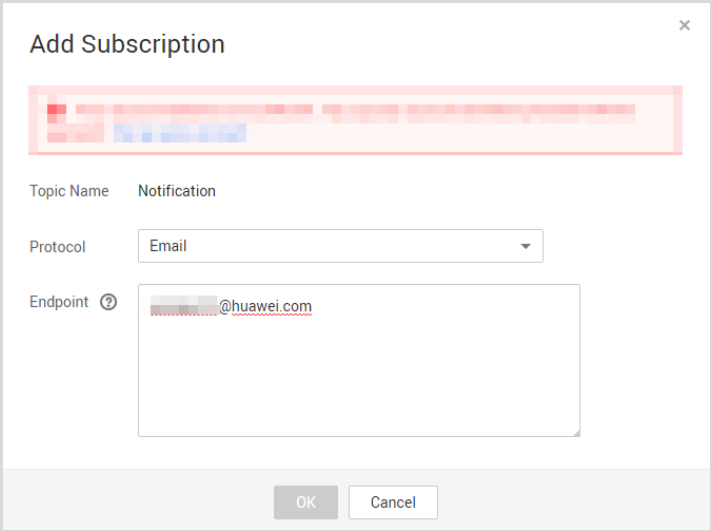
Parameter	Description
Topic Name	Specifies the topic name, which Contains only upper or lower case letters, numerals, hyphens (-), and underscores (_) and must start with a letter or a numeral. Must be 1-256 characters long. Must be unique and cannot be modified once the topic is created.
Display Name	Specifies the message sender name, which must be less than 192 bytes. Note: After you specify a display name, the sender in email messages will be presented as *Display name*<username@example.com>. Otherwise, the sender will be username@example.com.



Step 5 **Click OK.**

Step 6 **Locate the topic to which you want to add a subscription, click More under Operation, and select Add Subscription.**

Step 7 **Specify the subscription protocol and endpoints. You can enter 10 endpoints at most, each in one line.**



- Email **(try this)**

Enter a valid email address, for example, **username@example.com**.

Subscribers will receive a subscription confirmation email valid in 48 hours and must confirm the subscription to receive messages published to the topic.

- HTTP/HTTPS

Enter a public network URL, for example, **http://example.com/notification/action**. HTTP/HTTPS subscribers must confirm their subscriptions. For details about HTTP/HTTPS messages, see Introduction in the *Simple Message Notification User Guide*.

- SMS

Enter a valid mobile phone number. Only phone numbers in the Chinese mainland are supported, for example, **18512345678**.

Subscribers will receive a subscription confirmation message valid in 48 hours and must confirm the subscription to receive messages published to the topic.

- DMS

Subscription endpoints are message queues. This type of subscriptions does not need confirmation. Click + to select subscription endpoints. Ensure that the queue policy grants the **DMS:ProduceMessages** permission to SMN. For details, see "Managing Queue Policies" in the *Distributed Message Service User Guide*.

Step 8 **Click OK. The subscriptions you added is displayed in the subscription list.**

11.2.1.3 Viewing the ECS Running Status

11.2.1.3.1 Scenarios

Cloud Eye can monitor the ECS running status. You can obtain the metrics of each ECS on the Cloud Eye management console.

11.2.1.3.2 Prerequisites

Cloud Eye does not display the metrics of a stopped, faulty, or deleted ECS. The status of a stopped or faulty ECS can be displayed only after it is started or recovered.

11.2.1.3.3 Procedure

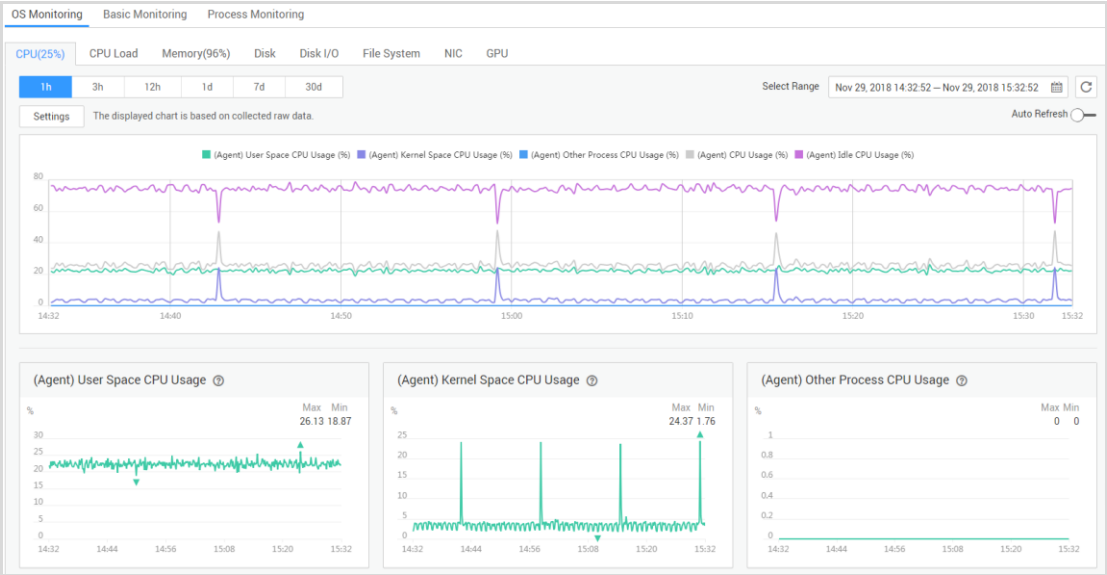
Step 1 **Log in to the management console.**

Step 2 **Under Management & Deployment, select Cloud Eye.**

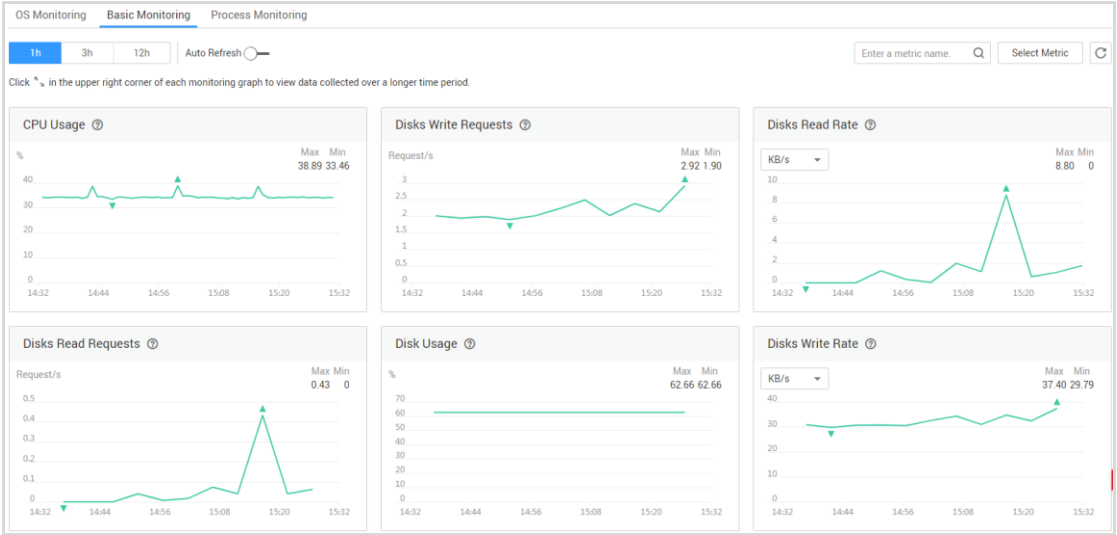
Step 3 **In the navigation pane on the left, choose Server Monitoring.**

Step 4 **On the Server Monitoring page, locate the row that contains the target ECS and click View Metric to go to the OS Monitoring page.**

OS monitoring requires the Agent to be installed. For details, see Installing and Configuring the Agent (Linux).



Step 5 **To view the ECS metrics, click Basic Monitoring.**



Step 6 **Hover your mouse over a graph, click in the upper right corner to enlarge the graph for viewing detailed data.**

In the upper left corner, you can see six default monitoring periods: **1h**, **3h**, **12h**, **1d**, **7d**, and **30d**. You can also view the alarm history for any period during the last six months by customizing the monitoring period.

In the upper left of the graph, you can click **Settings** to configure the rollup method.

11.2.2 Installing and Configuring the Agent (Linux)

11.2.2.1 Installing the Agent

11.2.2.1.1 Scenarios

This section describes how to manually install the Agent on an ECS or a BMS.

11.2.2.1.2 Prerequisites

- The installation directories in Procedure have the read and write permissions.
- The Telescope process is not stopped by other software after the installation.

11.2.2.1.3 Procedure

Step 1 **Log in to the ECS or BMS as user root.**

Step 2 **Run the following command to install the Agent:**

- Asia Pacific-Hong Kong: (use this option)

```
cd /usr/local && wget
https://telescope-ap-southeast-1.obs.ap-southeast-1.myhwclouds.com/scripts/agentInstall.sh &&
chmod 755 agentInstall.sh && ./agentInstall.sh
```

- CN North-Beijng1: (do not use this in this lab)

```
cd /usr/local && wget http://telescope.obs.cn-north-1.myhwclouds.com/scripts/agentInstall.sh &&
chmod 755 agentInstall.sh && ./agentInstall.sh
```

- CN South-Guangzhou: (do not use this in this lab)

```
cd /usr/local && wget
http://telescope-cn-south-1.obs.cn-south-1.myhwclouds.com/scripts/agentInstall.sh && chmod
755 agentInstall.sh && ./agentInstall.sh
```

- CN East-Shanghai2: (do not use this in this lab)

```
cd /usr/local && wget
http://telescope-cn-east-2.obs.cn-east-2.myhwclouds.com/scripts/agentInstall.sh && chmod 755
agentInstall.sh && ./agentInstall.sh
```

The Agent is installed if the following command output is displayed:

```
telescope_linux_amd64/
telescope_linux_amd64/uninstall.sh
telescope_linux_amd64/install.sh
telescope_linux_amd64/bin/
telescope_linux_amd64/bin/conf.json
telescope_linux_amd64/bin/telescope
telescope_linux_amd64/bin/conf_ces.json
telescope_linux_amd64/bin/conf_lts.json
telescope_linux_amd64/bin/record.json
telescope_linux_amd64/bin/logs_config.xml
telescope_linux_amd64/bin/agent
telescope_linux_amd64/telescoped
telescope_linux_amd64/telescope-1.0.12-release.json
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-74e5-7 local]#
```

NOTE

If the Agent installation package fails to be downloaded, the Domain Name Service (DNS) and security group configurations are incorrect. Change the DNS server address and add security group rules based on Changing the DNS Server Address and Adding Security Group Rules.

Step 3 **After the installation is complete, configure the Agent based on Restoring the Agent Configurations or Manually Configuring the Agent. (details below)**

11.2.2.2 Restoring the Agent Configurations

11.2.2.2.1 Scenarios

This section describes how to restore the Agent configurations after the Agent is installed.

11.2.2.2.2 Procedure

Step 1 **Log in to the management console.**

Step 2 **Under Management & Deployment, select Cloud Eye. In the navigation pane on the left, choose Server Monitoring.**

Step 3 **On the Server Monitoring page, select the target ECSs and click Restore Agent Configurations. On the displayed page, click One-Click Restore to complete the configuration.**

11.2.2.3 Manually Configuring the Agent

11.2.2.3.1 Scenarios

After successfully installing the Agent, you need to modify related configuration files to report monitoring data and heartbeat data.

11.2.2.3.2 Prerequisites

- The Agent has been installed.

11.2.2.3.3 Procedure

Step 1 **Log in to the ECS or BMS as user root.**

Step 2 **Run the following command to go to the bin directory of the Agent installation package:**

```
cd /usr/local/telescope/bin
```

Step 3 **Modify the configuration file conf.json.**

- Run the following command to open **conf.json**:

```
vi conf.json
```

- Modify the parameter in the file. For details, see Table 11-33.

```
{
    "InstanceId":"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "ProjectId": "b5b92ee0xxxxxxxxxxxxxxxxcab92396",
    "AccessKey": "QZ0XGJXFxxxxxxxxT65R",
    "SecretKey": "lEv2aXAGwxxxxxxxxxxxxxxxxxxxxxF8t0Bf18Tn2",
    "RegionId": "cn-north-1",
    "ClientPort": 0,
    "PortNum": 200
}
```

Table 11-3 Public configuration parameters

Parameter	Description
InstanceId	Specifies the ECS ID. You can log in to the management console and view the ECS ID in the ECS list. NOTE You do not need to configure **InstanceId**. Retain **"InstanceId":""**. If you choose to configure **InstanceId**, see the following instructions: The ECS ID must be unique in all sites, that is, in the same region, **InstanceId** used by the Agent cannot be the same. Otherwise, errors may occur. The **InstanceId** value must be consistent with the actual ECS ID. Otherwise, you cannot see the **OS Monitoring** data on Cloud Eye.
ProjectId	Specifies the project ID. You do not need to configure **ProjectId**. Retain **"ProjectId": ""**. If you do wish to configure it, a project ID can be obtained by performing the following steps: 1. Log in to the Cloud Eye console, click the username in the upper right corner, and select **My Credential**. 2. Under **Projects**, view the ECS project ID in the corresponding

Parameter	Description
	region.
AccessKey/ SecretKey	Specifies the Access Keys, which can be obtained by performing the following operations: Log in to the Cloud Eye console, click the username in the upper right corner, select **My Credential**, and click **Access Keys**. If you have obtained the access key, obtain the **AccessKey** value and the **SecretKey** value in the **credentials.csv** file saved when you create **Access Keys**. If **Access Keys** is not available, you can click **Add Access Key** to create one. Save the **credentials.csv** file and obtain the **AccessKey** value and the **SecretKey** value in it. **NOTE** For security purposes, it is recommended that the user be an Identity and Access Management (IAM) user and the rights of the user be **CES Administrator** and **LTS Administrator**. The configured access key must be within the **Access Keys** list on the **My Credential** page. Otherwise its authentication will fail and you cannot view **OS Monitoring** data on Cloud Eye.
RegionId	Specifies the region ID. For example, if the ECS is located in the CN North-Beijing1 region, the value of **RegionId** is **cn-north-1**. For region IDs of other regions, log in at https://developer-intl.huaweicloud.com/endpoint.
ClientPort	Specifies the start port number used by the Agent. **NOTE** The default value is **0,** indicating that the Agent will randomly use any port. Ports 1 to 1023 are reserved. You are advised not to specify a port in this range for the Agent.
PortNum	Specifies the number of ports configured for the Agent. **NOTE** The default value is **200**. If the value of **ClientPort** is **5000**, the port range will be 5000 to 5199.

Step 4 **Modify configuration file conf_ces.json for the Cloud Eye metric collection module.**

- Run the following command to open **conf_ces.json**:

```
vi conf_ces.json
```

- Modify the parameter in the file. For details, see Table 11-44.

```
{
  "Endpoint": "https://ces.cn-north-1.myhuaweicloud.com"
}
```

Table 11-4 Parameter setting of the metric collection module

Parameter	Description
Endpoint	Specifies the Cloud Eye endpoint URL in the region of the ECS. For example, if the ECS is in the CN North-Beijing1 region, the URL is ces.cn-north-1.myhuaweicloud.com. For the endpoint values of other regions, log in at Regions and Endpoints.

11.2.3 Setting an AS Policy to Trigger Bandwidth Scaling

11.2.3.1 Scaling Bandwidth

11.2.3.1.1 Scenarios

The AS service automatically adjusts the EIP bandwidth within a specified range (between the minimum and maximum bandwidths you configure) based on the EIP monitoring data (inbound and outbound traffic) or bandwidth policies.

You can create an AS bandwidth policy based on your service requirements. When the trigger condition is met, the AS service automatically increases, decreases, or set the bandwidth of an EIP to a specified value based on the action you configured.

11.2.3.1.2 Procedure

Step 1 **Log in to the management console.**

Step 2 **Under Computing, click Auto Scaling. In the navigation pane on the left, choose Auto Scaling > Bandwidth Scaling.**

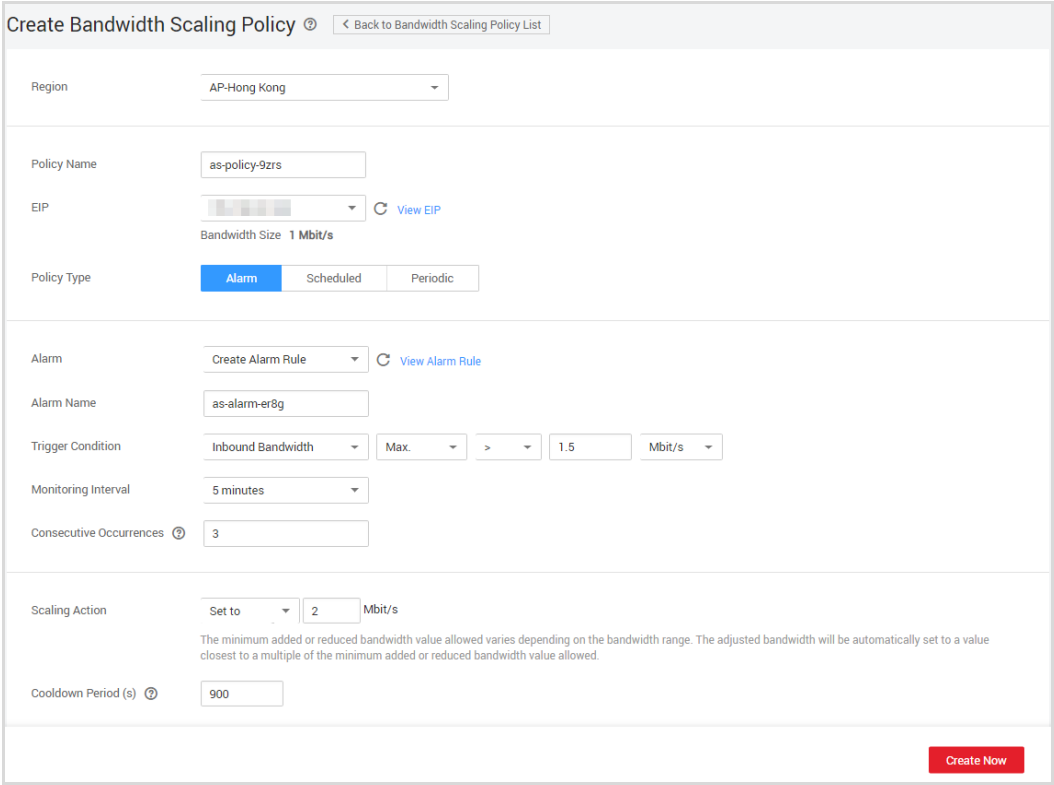
Step 3 **Click Create Bandwidth Scaling Policy. Configure the parameters in Table 11-55.**

Table 11-5 Parameters

Parameter	Description	Example Value
Region	Specifies the region where the AS group resides.	N/A
Policy Name	Specifies the name of the bandwidth scaling policy. The name consists of only letters, digits, underscores (_), and hyphens (-).	N/A
EIP	Specifies the public network IP address whose bandwidth needs to be scaled.	N/A
Policy Type	Select Alarm.	Alarm
Alarm	You can use an existing alarm rule or create an alarm rule. To create an alarm rule, configure the following parameters: Alarm Name Specifies the name of the new alarm rule (example: as-alarm-7o1u). Trigger Condition Specifies a metric and condition for triggering a scaling action. For example, when the outbound bandwidth MAX becomes greater than 100 bit/s, AS automatically triggers the scaling action. Monitoring Interval 5 min Consecutive Occurrences 1 Specifies the number of consecutive times for triggering a scaling action during a monitoring interval.	N/A
Scaling	Specifies the execution action in the AS policy.	N/A

Parameter	Description	Example Value
Action	The following AS action options are available: Add When a scaling action is triggered, the bandwidth is increased. Reduce When a scaling action is triggered, the bandwidth is decreased. Set to The bandwidth is set to a fixed value. NOTE The step (minimum unit for bandwidth adjustment) varies depending on the bandwidth value range. The bandwidth will be automatically adjusted to the nearest value according to the actual step. If the bandwidth is less than or equal to 300 Mbit/s, the default step is 1 Mbit/s. If the bandwidth ranges from 300 Mbit/s to 1000 Mbit/s, the default step is 50 Mbit/s. If the bandwidth is greater than 1000 Mbit/s, the default step is 500 Mbit/s.	
Limit	Specifies the maximum and minimum bandwidth allowed (Mbit/s). When Scaling Action is set to Add, this parameter specifies the maximum bandwidth allowed. When Scaling Action is set to Reduce, this parameter specifies the minimum bandwidth allowed. NOTE This parameter is unavailable if Scaling Action is	50 Mbit/s

Parameter	Description	Example Value
	Set to.	
Cooldown Period (s)	Specifies a period of time after a scaling action starts and before any further scaling actions can be triggered. The cooling duration prevents alarm-triggered scaling actions. Scaling actions triggered at a scheduled time or periodically will not be affected. However, the AS service recounts the cooling duration in the unit of second after a scheduled or periodic scaling action is performed.	300s



Step 4 **Click Create Now.**

The newly created bandwidth scaling policy is displayed on the **Bandwidth Scaling** page and is in **Enabled** state by default.

When the trigger condition is met, the AS service automatically increases, decreases, or set the bandwidth of an EIP to a specified value based on the action you configured.

12 Enterprise Intelligence

12.1 ModelArts

12.1.1 Introduction

12.1.1.1 About This Exercise

This exercise describes how to use ModelArts and quickly build an AI model with ExeML.

12.1.1.2 Objectives

After completing this exercise, you will be able to:

- Add an access key on the **Settings** page.
- Build an AI model with ExeML from scratch.
- Import the preset datasets in **Marketplace** to **Dataset** under **Data Management**.
- Create an ExeML project.
- Upload and label images in **Object Detection** on the **ExeML** page.
- Add images to test a service after the service is deployed in **Object Detection** on the **ExeML** page.

12.1.1.3 Prerequisites (try Hong Kong region)

You have registered an account for logging in to HUAWEI CLOUD and have applied for the open beta test of ModelArts. For details about how to apply for ModelArts, see section "Applying for ModelArts" in the *ModelArts User Guide*.

12.1.1.4 List of Tasks

No.	Task	Subtask
1	Get familiar with the ModelArts	On the Dashboard page, click Quick Start to learn about how to use ModelArts and basic

No.	Task	Subtask
	management console.	functions of each functional module.
2	Build an AI model with ExeML from scratch.	Import the preset datasets in Marketplace to Dataset under Data Management.
		Create a project in Object Detection on the ExeML page.
		Label the images for object detection.
		Release training.
		Deploy the model as a service and add an image to test the service.

12.1.2 Getting Familiar with the ModelArts Management Console

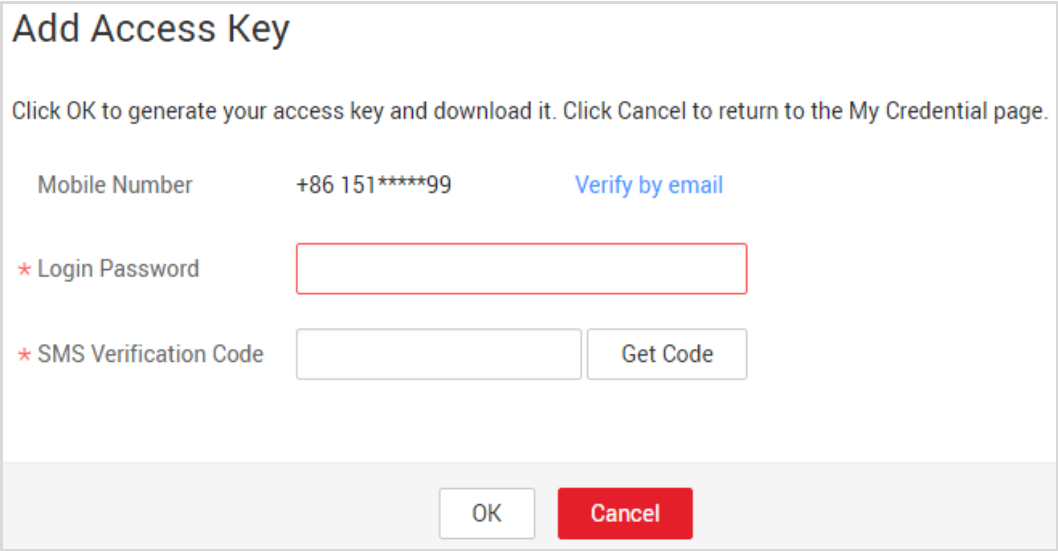
This section describes how to log in to the ModelArts management console, add an access key, and quickly learn about ExeML, AI development lifecycle, and Marketplace of ModelArts with **Quick Start** on **Dashboard**.

Step 1 **Log in to the management console.**

Step 2 **Choose Service List > EI Enterprise Intelligence > ModelArts. The ModelArts management console is displayed.**

Step 3 **Choose Settings Add an access key.**

- Create an access key.
  a. Log in to HUAWEI CLOUD and go to the **My Credential** page.
  b. Click the **Access Keys** tab.
  c. On the **Access Keys** tab page, click **Add Access Key**.
  d. In the **Add Access Key** dialog box that is displayed, enter the login password of the current user and the SMS or **email verification code (in this lab it will enable email option)**.



e. Click **OK** and save the access key as prompted. The key is directly saved to the default download folder of the browser.

f. Open the downloaded **credentials.csv** file to obtain the access key (AK and SK).

- Add an access key.

a. On the ModelArts management console, click **Settings** in the left navigation pane.

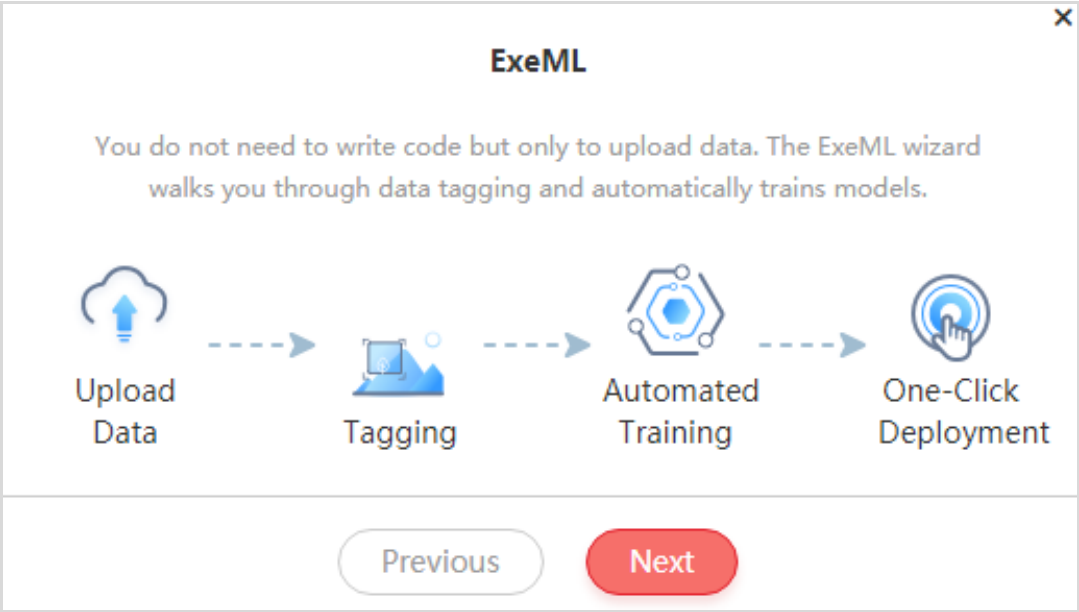
b. On the **Settings** page, click **Add Access Key**. In the dialog box that is displayed, enter the obtained access key. Set **AK** to the access key ID and **SK** to the secret access key.

c. Click **OK**. The access key is added.

Step 4 **Click Quick Start. In the dialog box that is displayed, click Start Now.**

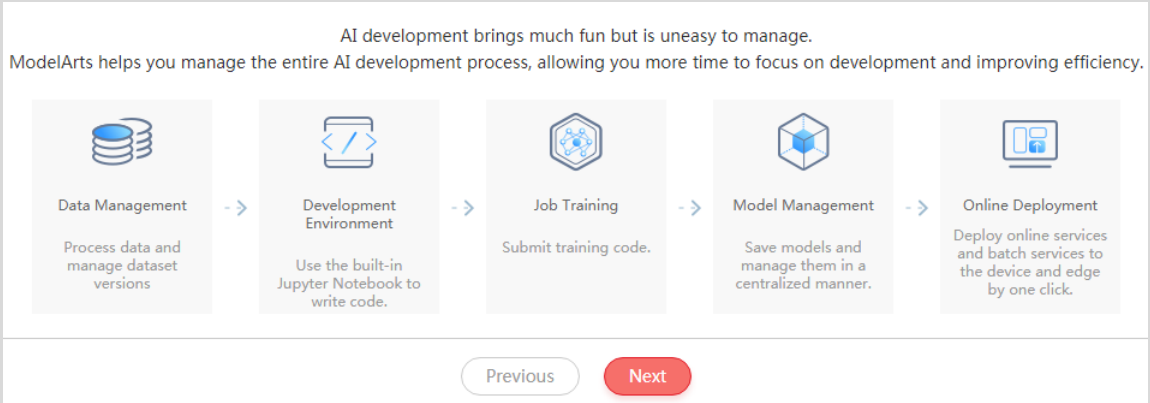
1. ExeML

ExeML frees you from coding. The wizard-based GUI walks you through data labeling, model training, and service deployment.



AI development lifecycle

The **Data Management** module supports data processing and dataset management. **DevEnviron** provides online code development environment, that is, Notebook. **Training Job** allows you to create training jobs to train models and manage the models. **Service Deployment** helps you deploy the models as online services, batch services, or edge services.



12.1.3 Building an AI Model with ExeML from Scratch

This section describes how to use ExeML to quickly build an object detection application.

This section describes how to use ExeML to train the preset Yunbao (the mascot of HUAWEI CLOUD) dataset to quickly build a Yunbao detection application. The detailed operations are as follows:

Step 1 **Prepare data.**

Step 2 **Create an object detection project.**

Step 3 **Label the data.**

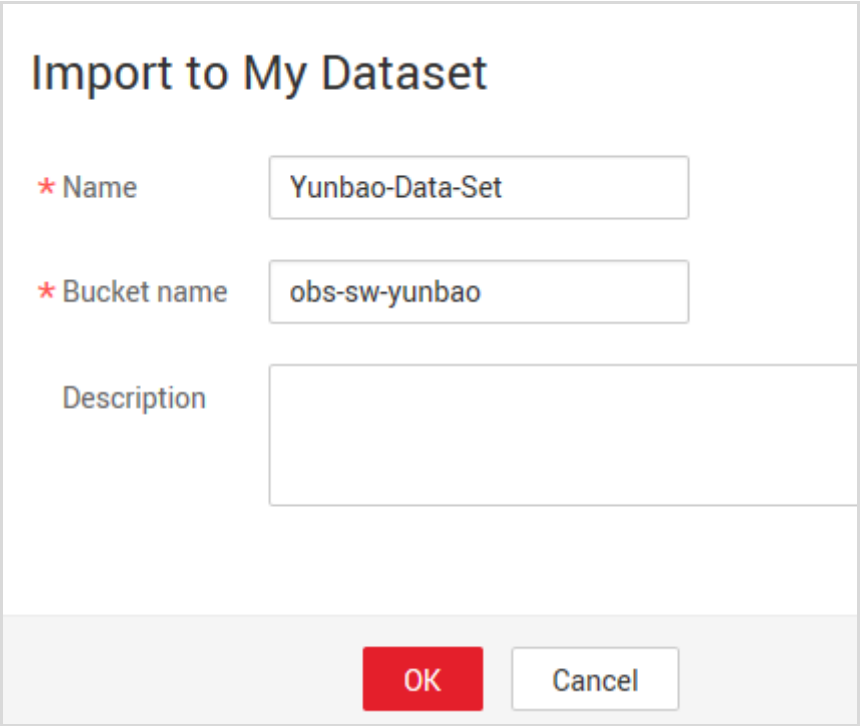
Step 4 **Perform automatic model training.**

Step 5 **Deploy a service.**

12.1.3.2 Preparing Data

Step 1 **Log in to the ModelArts management console and click Marketplace in the left navigation pane. On the Datasets tab page, find the preset Yunbao-Data-Set dataset for ExeML.**

Step 2 **Click the dataset to access its details page. Click Import to My Dataset. In the dialog box that is displayed, set a dataset name and an OBS bucket name.**



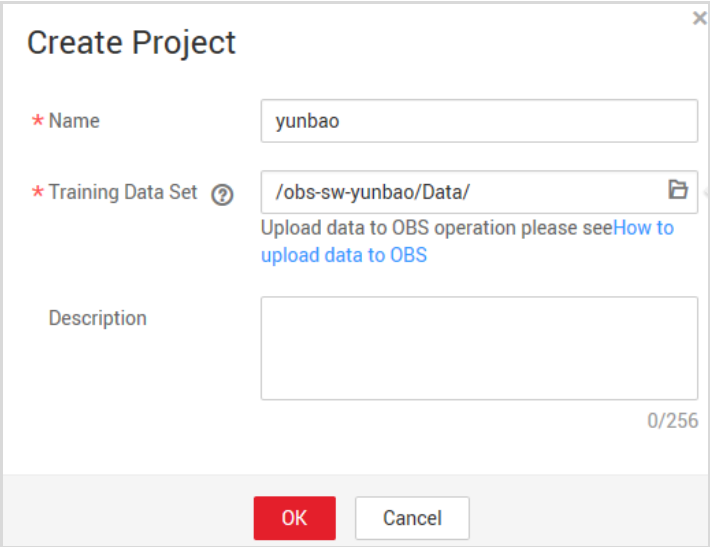
Step 3 **Click OK. In the dialog box that is displayed, click OK.**

----End

12.1.3.3 Creating an Object Detection Project

Step 1 **On the ModelArts management console, click ExeML in the left navigation pane.**

Step 2 **In the Object Detection box, click Create Project. In the dialog box that is displayed, enter the project name and select the OBS path of Yunbao-Data-Set.**



Step 3 **Click OK. The object detection project is created.**

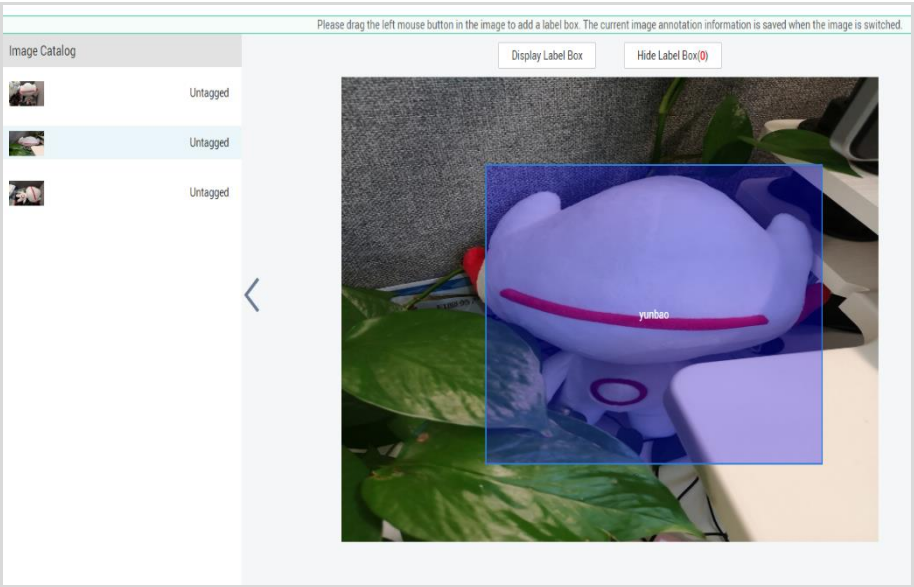
----End

12.1.3.4 Labeling the Data

Step 1 **Click the project name in the ExeML project list. The Tag Data tab page is displayed.**

Step 2 **Click the Untagged tab, and then click the Tagging icon on an image. The page for labeling the image is displayed.**

Step 3 **Drag the mouse to select an area containing Yunbao in the image, enter yunbao as the label name in the dialog box that is displayed, and click OK.**



Step 4 **After labeling all Yunbaos in the current image, select another unlabeled image in the left image catalog and repeat the previous operation to label it.**

Step 5 **Click Save and Return. Data labeling is completed.**

----End

12.1.3.5 Performing Automatic Model Training

Step 1 **After labeling data, set training parameters on the Tag Data tab page.**

Step 2 **Click Train to start automatic model training.(important: it will not work if you label just one image item, all itens labeled must have at least 5 images each)**

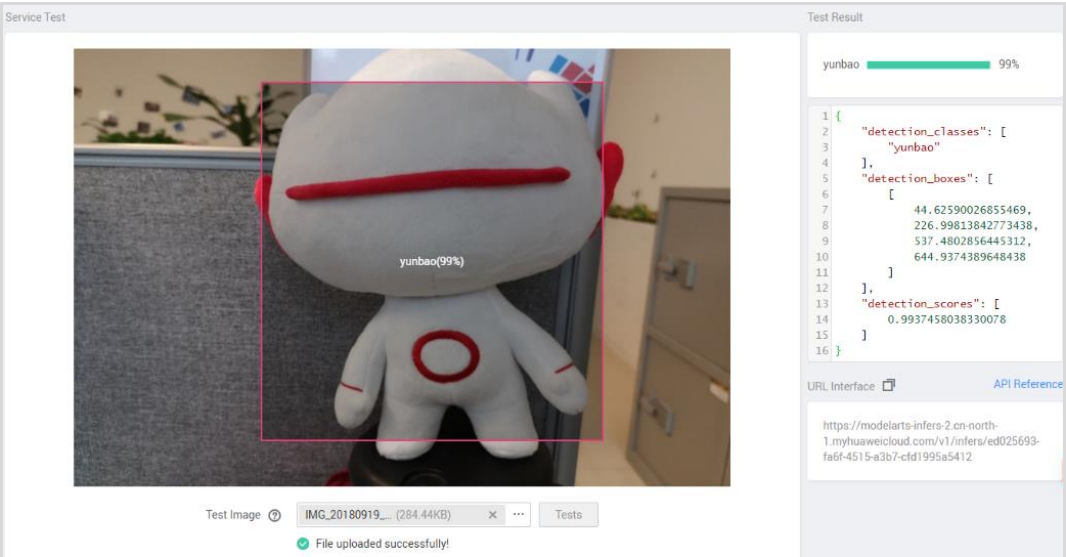
----End

12.1.3.6 Deploying a Service

Step 1 **When the training status on the Train Model tab page is Running Success, click Deploy to deploy the object detection model.**

Step 2 **After the deployment is successful, upload an image on the Deployment Online tab page for test.**

If the model accuracy does not meet your expectation, add images on the **Tag Data** tab page, label the images, and train and deploy the model again.



----End

13 API Gateway Mobile Number Location Lookup

13.1 Introduction

13.1.1 About This Experiment

This experiment guides you through the process of opening a mobile number location lookup API and publishing the API in the RELEASE environment. You can bind request throttling policies to the API to control service requests and ensure stable services.

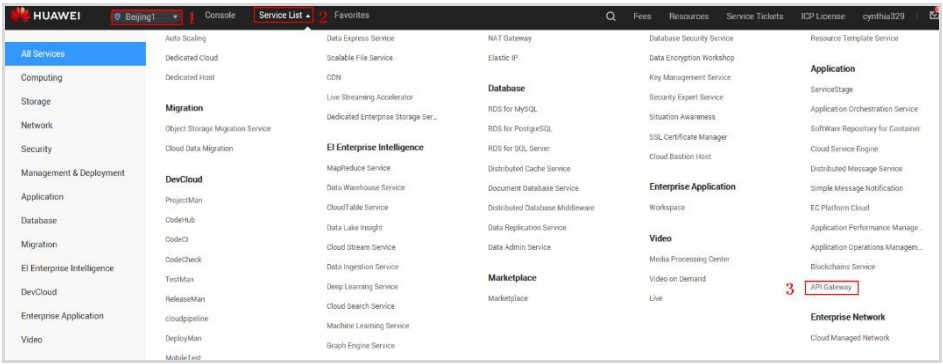
13.1.2 Objectives

- Learn about the functions of API Gateway.
- Understand how to open an API on API Gateway.

13.2 Building a Mobile Number Location Lookup API

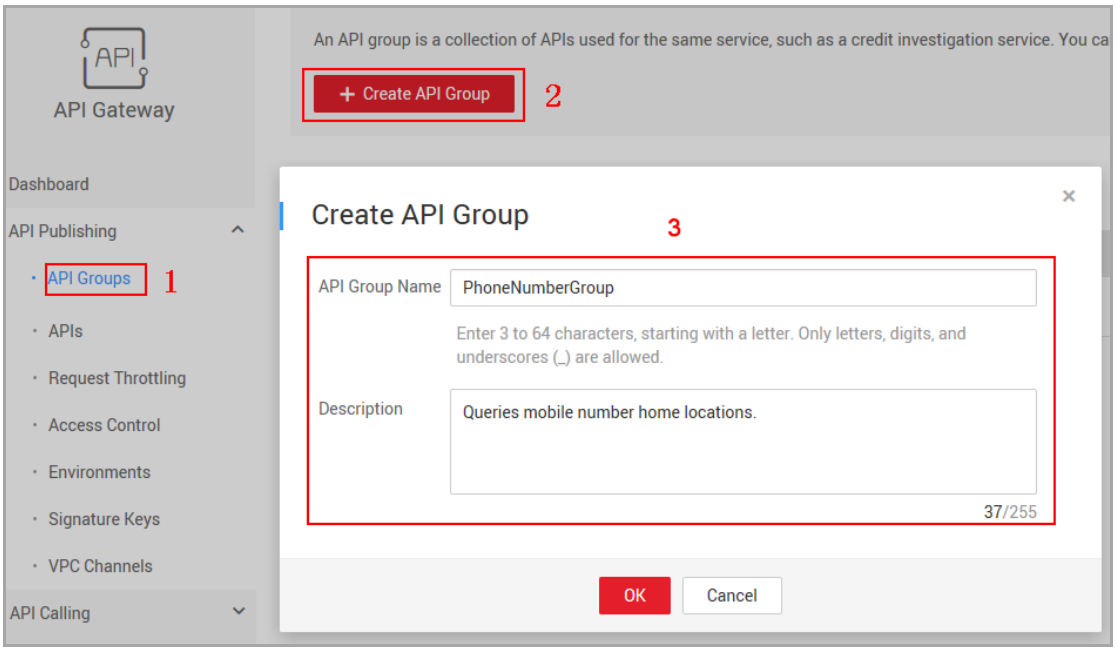
13.2.1 Opening an API (Try Hong Kong region)

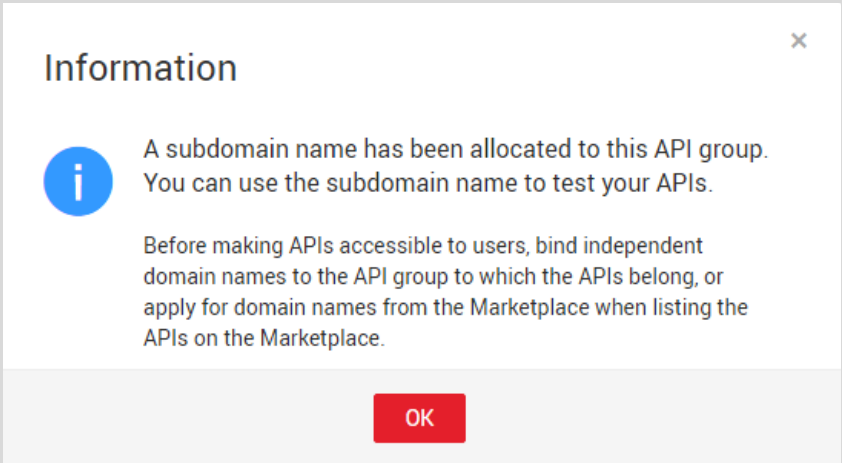
Step 1 **Log in to the HUAWEI CLOUD management console, select a region in the upper left corner, and choose Service List > Application > API Gateway.**



Click API Publishing

Step 2 **Create an API group and configure the parameters.**

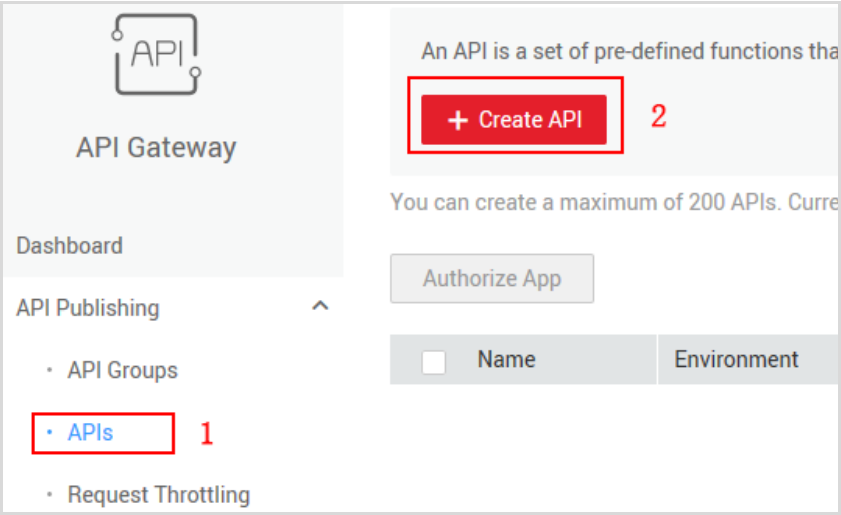


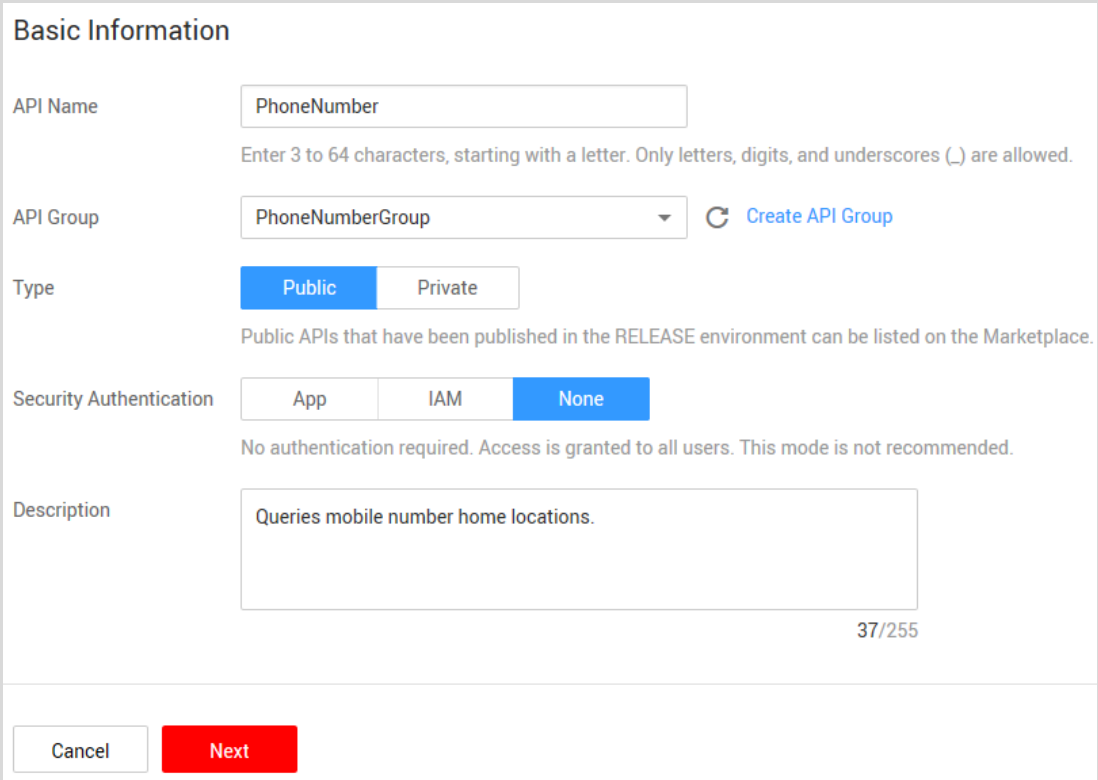


Step 3 **Select APIs on the left pane and click on Create an API.**

a. Set the basic information of the API

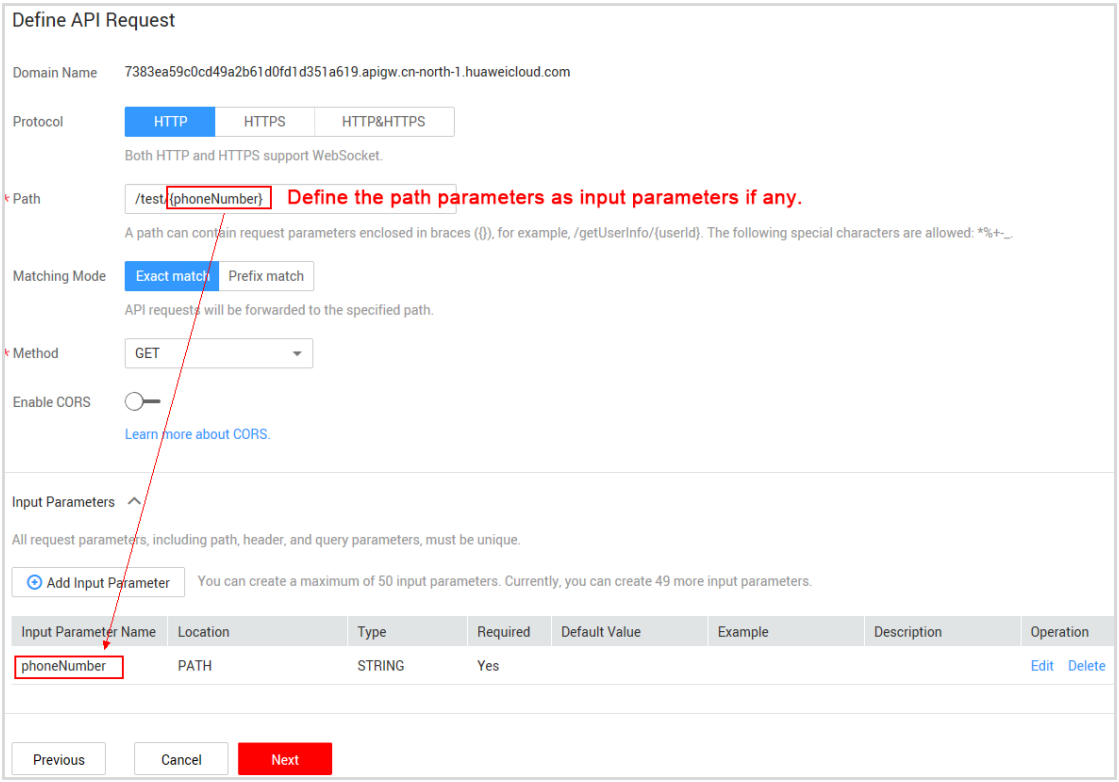
For details about the parameters, see the API Gateway User Guide.





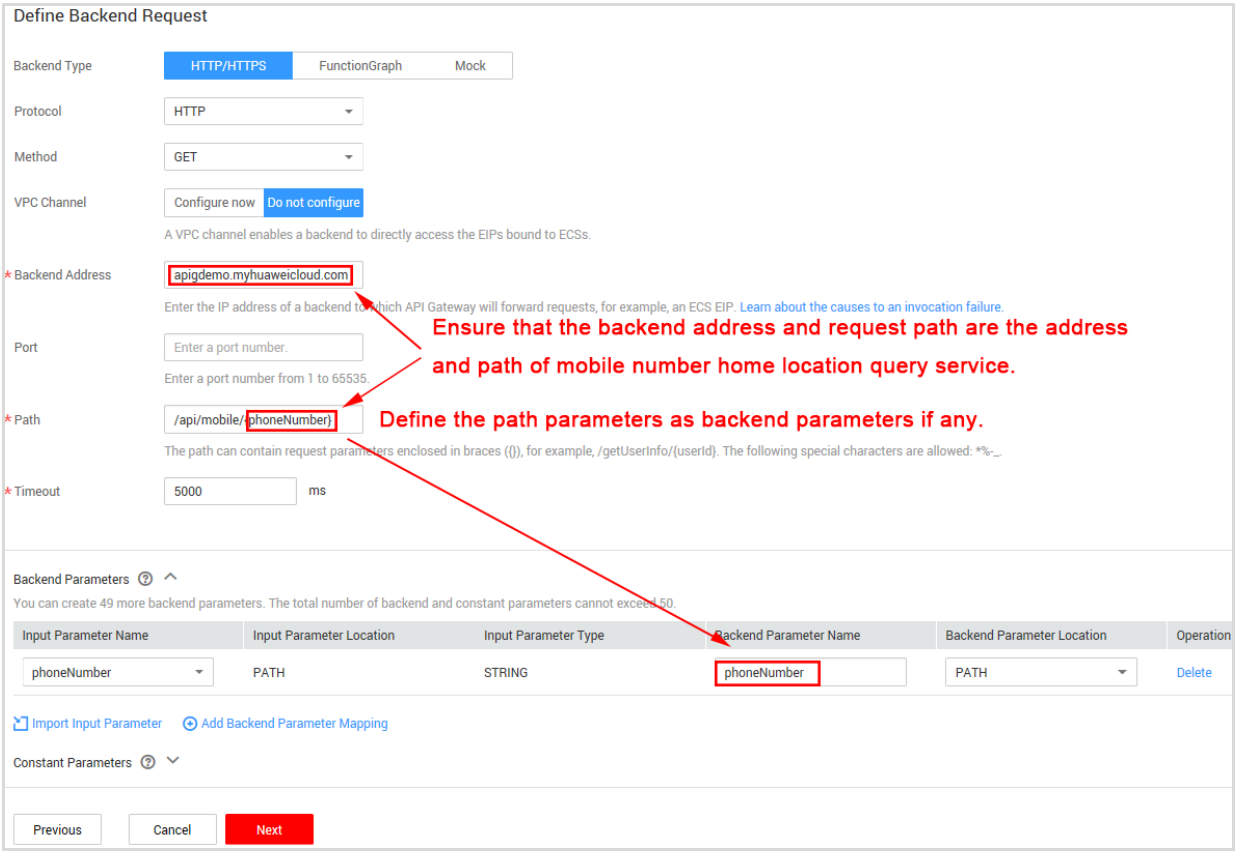
b. On the **Define API Request** page, set the API request information.

For details about the parameters, see the API Gateway User Guide.

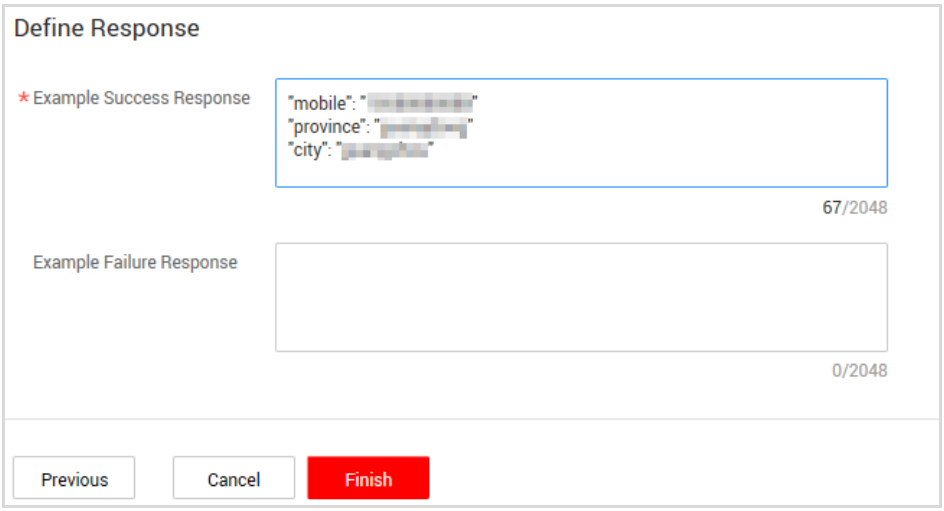


c. On the **Define Backend Request** page, set the backend request information.

For details about the parameters, see the API Gateway User Guide.

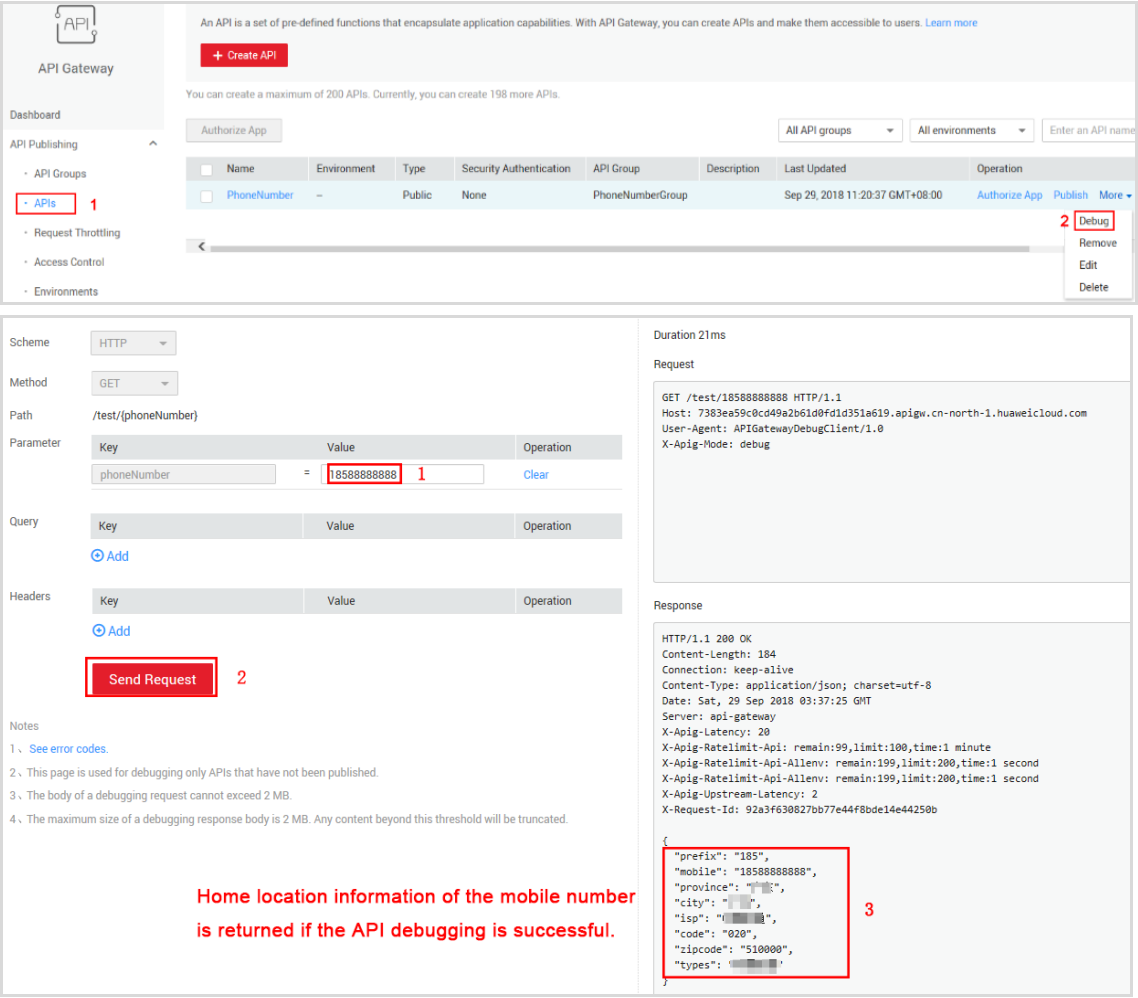


d. On the **Define Response** page, set the example success response.

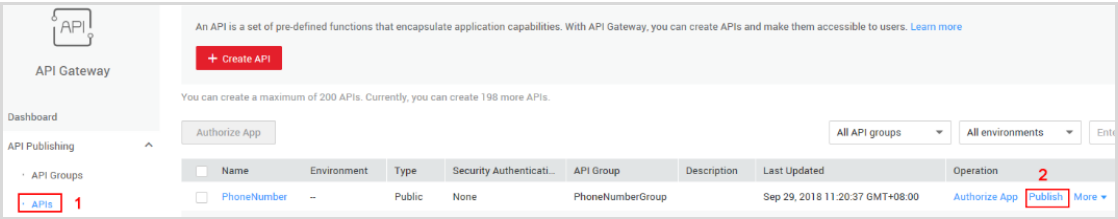


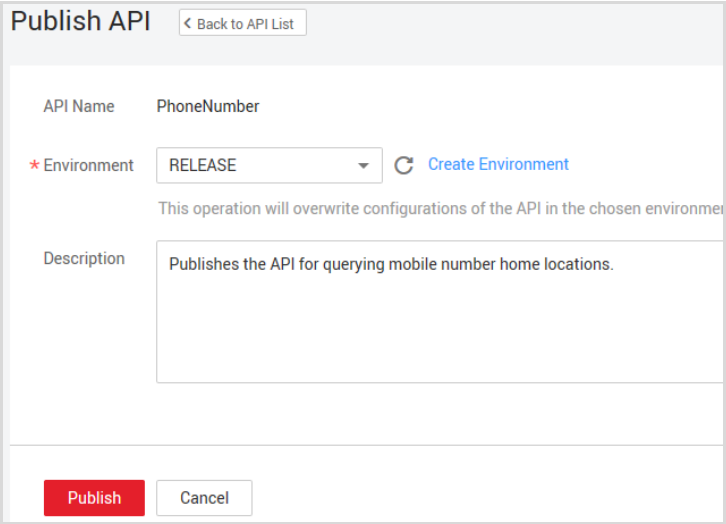
e. Click **Finish**.

Step 4 **Debug the API. Try the phoneNumber 18588888888**



Step 5 **Publish the API.**

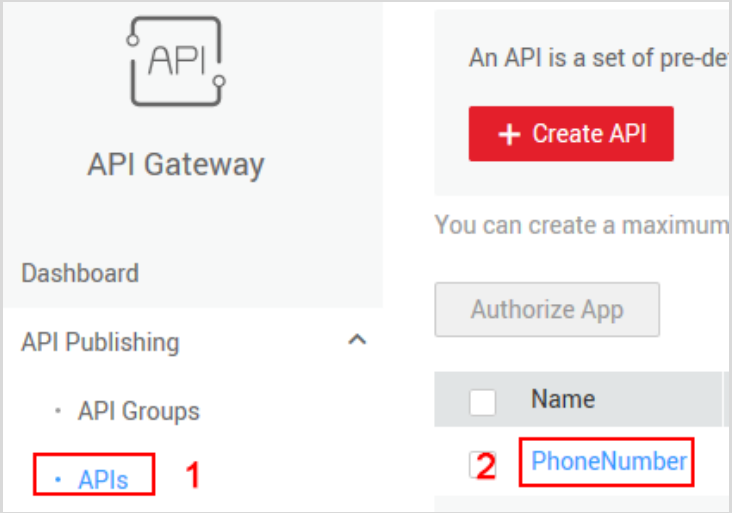


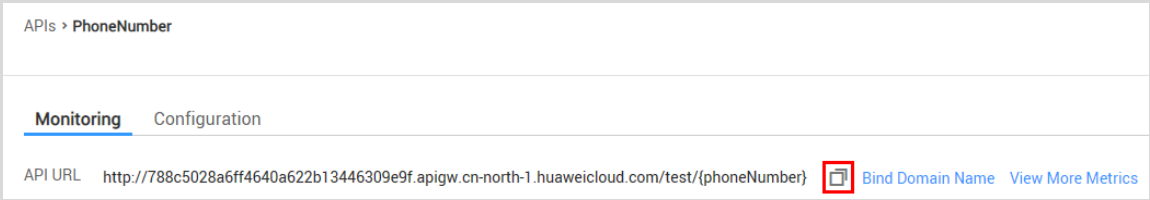


----End

13.2.2 Calling the API

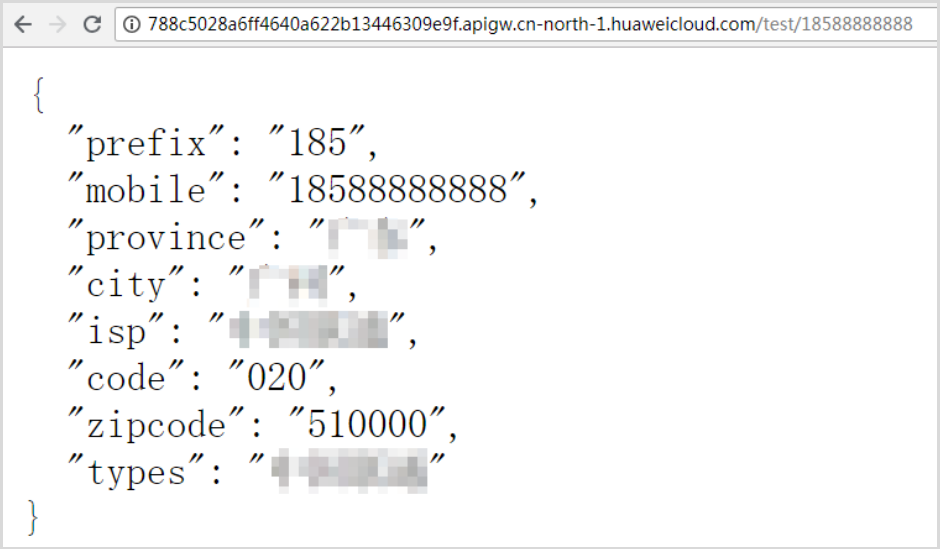
Step 1 **In the API list, click the created API, and then copy the API URL.**





Step 2 **Paste the URL of the API on the address bar of a browser, and replace *{phoneNumber}* with the mobile number you want to look up.**

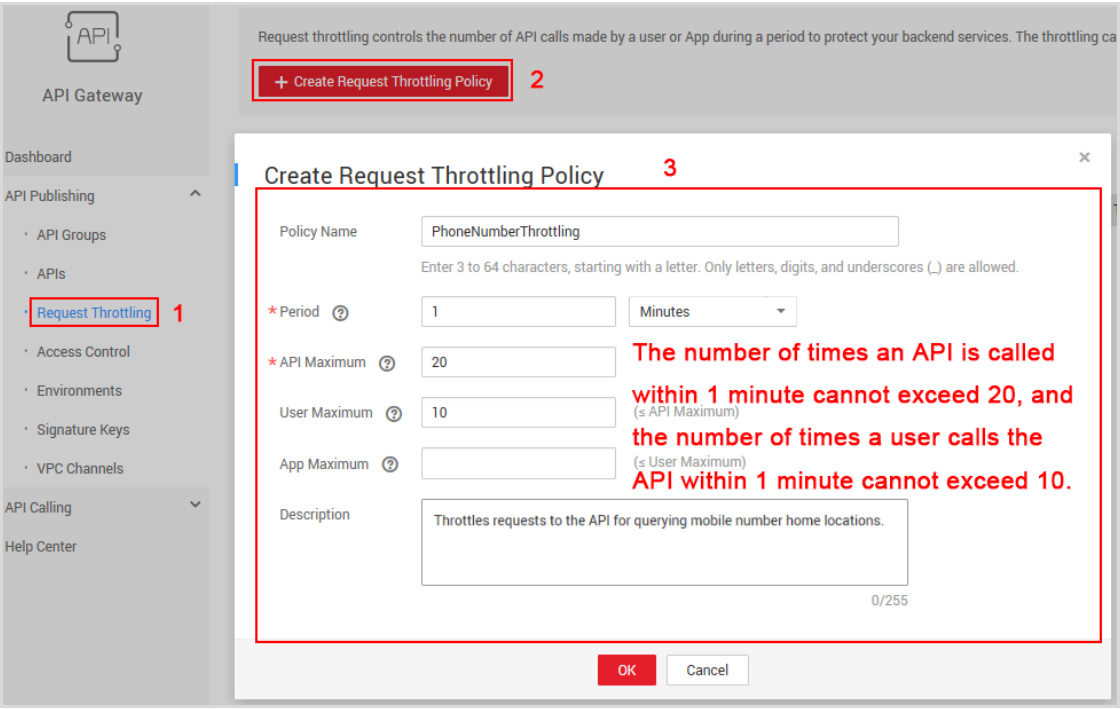
Information on the mobile number's origin will be returned if the API is called successfully.



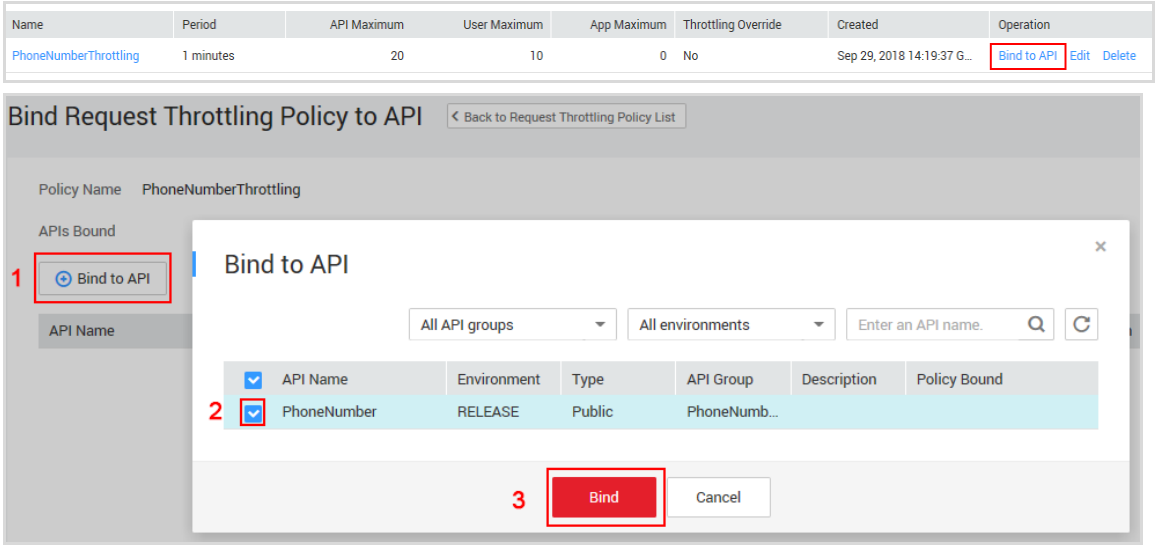
----End

13.2.3 Binding a Request Throttling Policy

Step 1 **Create a request throttling policy.**



Step 2 **Bind the request throttling policy to the API.**



Step 3 **Call the API by copying its URL to a browser. For details, see Calling the API.**

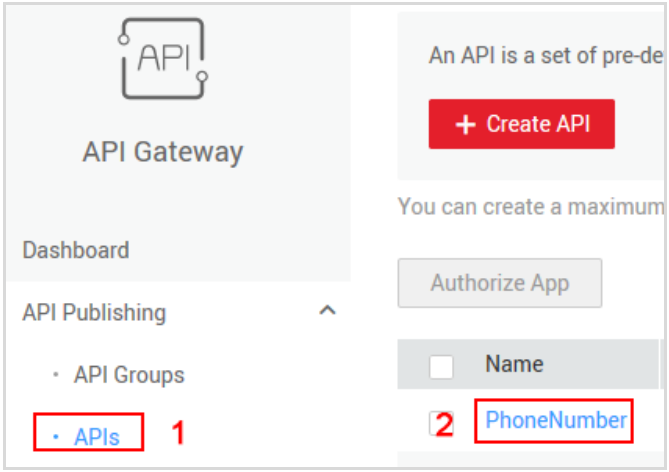
If the API is called more than 20 times within one minute, an error will be reported.

```
{"error_msg":"The maximum request receiving rate is exceeded:
policy api_control over ratelimit:20\/1
minute","error_code":"APIG.0308","request_id":"ca1857c0dfe9f48
2ea49aea16720005b"}
```

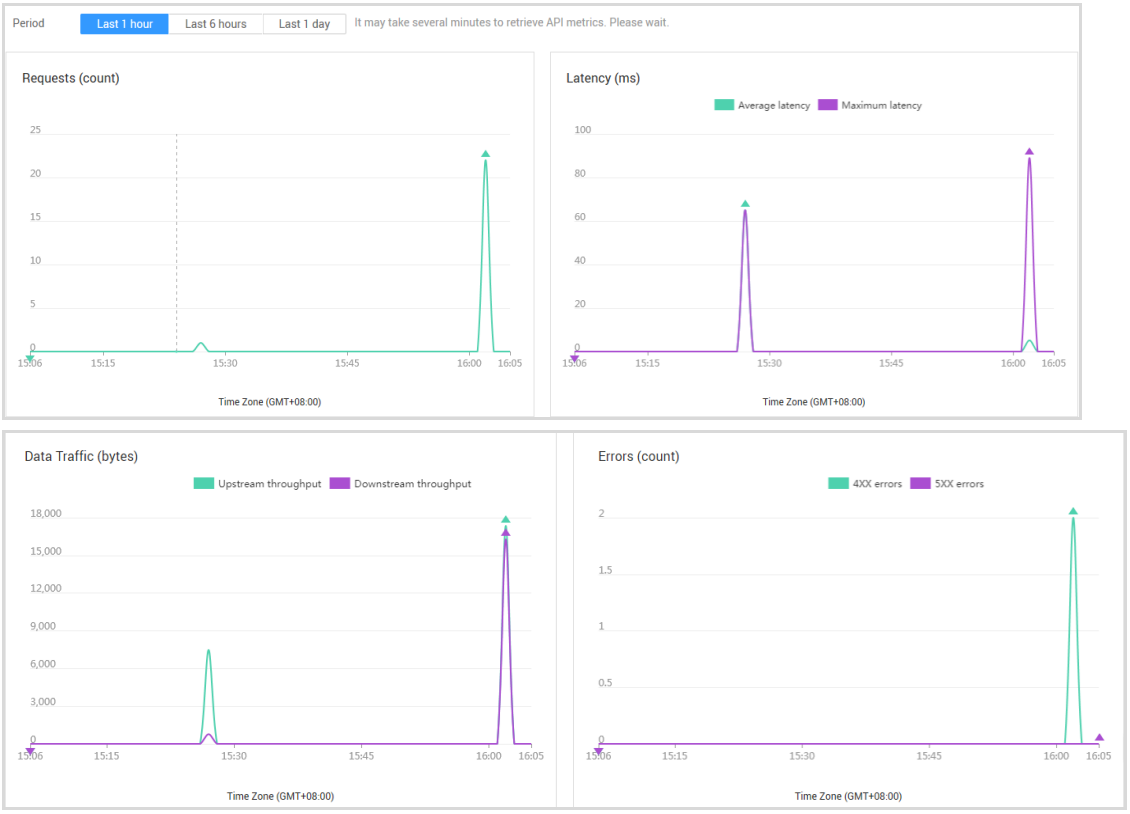
----End

13.2.4 Viewing Metrics

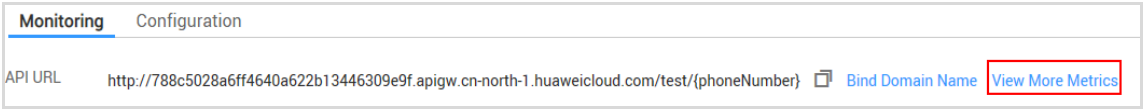
Step 1 **On the APIs page, click the API to display the details page.**



Step 2 **On the Monitoring tab page, view the API metrics, including requests, latency, data traffic, and errors.**



Step 3 **Click View More Metrics to view complete metrics on the Cloud Eye console.**



NOTE

Metrics data is retained for two days. For longer retention periods, save data to an OBS bucket.

----End