User Guide

Version: ZStack Cloud 4.3.12

Issue: V4.3.12

ZStack

Copyright Statement

Copyright © 2022 Shanghai Yunzhou Information and Technology Ltd. All rights reserved.

Without prior written consent of Shanghai Yunzhou Information and Technology Ltd., any organization and any individual do not have the right to extract, copy any part of or all of, and are prohibited to disseminate the contents of this document in any manner.

Trademark

Shanghai Yunzhou Information and Technology Ltd. reserves all rights to its trademarks, including , but not limited to ZStack and other trademarks in connection with Shanghai Yunzhou Information and Technology Ltd.

Other trademarks or registered trademarks presented in this document are owned or controlled solely by its proprietaries.

Notice

The products, services, or features that you purchased are all subject to the commercial contract and terms of Shanghai Yunzhou Information and Technology Ltd., but any part or all of the foregoing displayed in this document may not be in the scope of your purchase or use. Unless there are additional conventions, Shanghai Yunzhou Information and Technology Ltd. will disclaim any statement or warranty, whether implicit or explicit, on the contents of this document.

In an event of product version upgrades or other reasons, the contents of this document will be irregularly updated and released. Unless there are additional conventions, this document, considered solely as a reference guide, will not make any warranty, whether implicit or explicit, on all the statements, information, or suggestions.

Contents

Copyright Statement I
1 Introduction 1
2 Overview 2
3 Configuration Requirements 3
3.1 Network Environment 3
3.2 Hardware Requirements 4
4 Installation and Deployment 7
4.1 Environment Preparations 7
4.1.1 Network Bonding (Optional) 18
4.2 Install ZStack Cloud 26
4.2.1 ZStack Cloud Management Node Mode 28
4.2.2 ZStack Cloud Compute Node Mode 29
4.2.3 ZStack Cloud Expert Mode 29
4.3 Manage ZStack Cloud 30
4.4 Upgrade ZStack Cloud 31
5 License Management 38
5.1 What is License? 38
5.2 Install a License 46
5.2.1 Install a License by Using an USB Key 46
5.2.2 Install a License by Using a Request Key 47
5.3 Manage a License 49
6 Initialization by Wizard 54
6.1 Create a Zone 54
6.2 Create a Cluster 55
6.3 Add a Host 55
6.4 Add a Backup Storage 57
6.4.1 ImageStore 57
6.4.2 Ceph 59
6.5 Add a Primary Storage 60
6.5.1 LocalStorage 61
6.5.2 NFS 62
6.5.3 Shared Mount Point 64
6.5.4 Ceph 65
6.6 Create an Instance Offering 67
6.7 Add an Image 72
6.8 Create an L2 Network 77
6.9 Create an L3 Network 79
7 Resource Center 81
7.1 Resource Pool 81

7.1.1 VM Instance....81
7.1.1.1 What is VM Instance?....81
7.1.1.2 Create a VM Instance (Fast Creation)....85
7.1.1.3 Create a VM Instance (Standard Creation)....90
7.1.1.4 Manage a VM Instance....109
7.1.1.5 VM Details....134
7.1.1.5.1 VM Configurations....134
7.1.1.5.2 Advanced Settings....142
7.1.1.5.3 External Monitoring....143
7.1.1.5.4 Internal Monitoring....146
7.1.1.5.5 Internal Monitoring Agent....149
7.1.1.5.6 SSH Key Management....154
7.1.1.5.7 Resize the Root Volume....156
7.1.2 Volume....167
7.1.2.1 What is Volume?....167
7.1.2.2 Create a Volume....168
7.1.3 Image....176
7.1.3.1 What is Image?....176
7.1.3.2 Add an Image....178
7.1.3.3 Manage an Image....185
7.1.4 Instance Offering....188
7.1.4.1 What is Instance Offering?....188
7.1.4.2 Create an Instance Offering....188
7.1.4.3 Manage an Instance Offering....193
7.1.5 Disk Offering....194
7.1.5.1 What is Disk Offering?....194
7.1.5.2 Create a Disk Offering....194
7.1.5.3 Manage a Disk Offering....197
7.1.6 GPU Specification....198
7.1.6.1 What is GPU Specification?....198
7.1.7 Auto-Scaling Group....198
7.1.7.1 What is Auto-Scaling Group?....198
7.1.7.2 Create an Auto-Scaling Group....199
7.1.8 Snapshot....212
7.1.8.1 What is Snapshot?....212
7.1.8.2 Snapshot Fundamentals....213
7.1.8.3 Create a Snapshot....219
7.1.9 Affinity Group....222
7.1.9.1 What is Affinity Group?....222
7.1.9.2 Create an Affinity Group....223
7.2 Hardware....224
7.2.1 Zone....224
7.2.1.1 What is Zone?....224
7.2.1.2 Create a Zone....226

7.2.1.3 Manage a Zone....226
7.2.2 Cluster....227
7.2.2.1 What is Cluster?....227
7.2.2.2 Create a Cluster....231
7.2.2.3 Manage a Cluster....236
7.2.3 Host....238
7.2.3.1 What is Host?....238
7.2.3.2 Add a Host....238
7.2.3.3 Manage a Host....243
7.2.4 Primary Storage....247
7.2.4.1 What is Primary Storage?....247
7.2.4.2 Add a Primary Storage....249
7.2.4.3 Manage a Primary Storage....260
7.2.5 Backup Storage....262
7.2.5.1 What is Backup Storage?....262
7.2.5.2 Add a Backup Storage....265
7.2.5.3 Manage a Backup Storage....271
7.2.6 SAN Storage....273
7.2.6.1 What is SAN Storage?....273
7.2.6.2 Add an iSCSI Storage....274
7.3 Network Resource....275
7.3.1 L2 Network....276
7.3.1.1 What is L2 Network?....276
7.3.1.2 Create an L2 Network....279
7.3.1.3 Manage an L2 Network....285
7.3.2 VXLAN Pool....287
7.3.2.1 What is VXLAN Pool?....287
7.3.2.2 Create a VXLAN Pool....288
7.3.2.3 Manage a VXLAN Pool....291
7.3.3 L3 Network....292
7.3.3.1 Public Network....296
7.3.3.1.1 Create a Public Network....296
7.3.3.1.2 Manage a Public Network....306
7.3.3.2 Flat Network....307
7.3.3.2.1 Create a Flat Network....307
7.3.3.2.2 Manage a Flat Network....316
7.3.3.3 VPC Network....317
7.3.3.3.1 Create a VPC Network....317
7.3.3.3.2 Manage a VPC Network....326
7.3.3.4 Management Network....327
7.3.3.4.1 Create a Management Network....327
7.3.3.4.2 Manage a Management Network....330
7.3.3.5 Flow Network....331
7.3.3.5.1 Create a Flow Network....331

7.3.3.5.2 Manage a Flow Network....333
7.3.4 VPC vRouter....333
7.3.4.1 What is VPC vRouter?....333
7.3.4.2 Create a VPC vRouter....334
7.3.5 VPC HA Group....337
7.3.5.1 What is VPC HA Group?....337
7.3.5.2 Create a VPC vRouter HA Group....337
7.3.6 vRouter Image....340
7.3.6.1 What is vRouter Image?....340
7.3.6.2 Add a vRouter Image....340
7.3.7 vRouter Offering....343
7.3.7.1 What is vRouter Offering?....343
7.3.7.2 Create a vRouter Offering....344
7.3.8 SDN Controller....345
7.3.8.1 What is SDN Controller?....345
7.3.8.2 Add an SDN Controller....346
7.4 Network Service....347
7.4.1 Security Group....351
7.4.1.1 What is Security Group?....351
7.4.1.2 Create a Security Group....353
7.4.2 Virtual IP....354
7.4.2.1 What is Virtual IP?....354
7.4.2.2 Create a Virtual IP....356
7.4.3 Elastic IP....358
7.4.3.1 What is Elastic IP?....358
7.4.3.2 Create an Elastic IP....360
7.4.4 Port Forwarding....362
7.4.4.1 What is Port Forwarding?....362
7.4.4.2 Create a Port Forwarding Rule....365
7.4.5 Load Balancing....367
7.4.5.1 What is Load Balancer?....367
7.4.5.2 Load Balancer....369
7.4.5.2.1 Create a Load Balancer....369
7.4.5.3 Listener....373
7.4.5.3.1 Create a Listener....373
7.4.5.3.2 Create a Forwarding Rule....378
7.4.5.4 Backend Server Group....380
7.4.5.4.1 Create a Backend Server Group....380
7.4.5.5 Certificate....383
7.4.5.5.1 Create a Certificate....383
7.4.5.6 Load Balancing Configurations....385
7.4.5.6.1 Create a Load Balancer Instance Offering....385
7.4.6 Firewall....386
7.4.6.1 What is Firewall?....386

7.4.6.2 Create a Firewall....387
7.4.6.3 Rule Set....388
7.4.6.3.1 Create a Rule Set....388
7.4.7 IPsec Tunnel....389
7.4.7.1 What is IPsec Tunnel?....389
7.4.7.2 Create an IPsec Tunnel....389
7.4.8 OSPF Area....392
7.4.8.1 What is OSPF Area?....392
7.4.8.2 Create an OSPF Area....392
7.4.9 NetFlow....393
7.4.9.1 What is NetFlow?....393
7.4.9.2 Create a Netflow....393
7.4.10 Port Mirroring....395
7.4.10.1 What is Port Mirroring?....395
7.4.10.2 Create a Port Mirroring....395
7.4.11 Route Table....396
7.4.11.1 What is Route Table?....396
7.4.11.2 Create a Route Table....397
7.5 CloudFormation....397
7.5.1 What is CloudFormation?....397
7.6 Baremetal Management....398
7.6.1 What is Baremetal Management?....398
7.7 Elastic Baremetal Management....402
7.7.1 What is Elastic Baremetal Management?....402
7.7.2 Quick Start....409
7.8 vCenter....431
7.8.1 What is vCenter?....431
7.9 Hybrid Cloud Management....433
7.9.1 What is Hybrid Cloud Management?....433
8 Platform O&M....439
8.1 Network Topology....439
8.1.1 Global Network Topology....439
8.2 Cloud Monitoring....441
8.2.1 Performance Analysis....441
8.2.2 Capacity Management....441
8.2.3 MN Monitoring....441
8.2.4 Monitoring and Alarm....441
8.2.4.1 Alarm....443
8.2.4.1.1 Create an Alarm....443
8.2.4.2 One-click Alarm....448
8.2.4.3 Alarm Template....448
8.2.4.3.1 Create an Alarm Template....448
8.2.4.4 Resource Group....449
8.2.4.4.1 Create a Resource Group....449

8.2.4.5 Message Template....450
8.2.4.5.1 Create a Message Template....450
8.2.4.6 Message Source....454
8.2.4.6.1 Create a Message Source....454
8.2.4.7 Endpoint....455
8.2.4.7.1 Create an Endpoint....455
8.3 Message Log....460
8.3.1 Alarm Message....460
8.3.2 Operation Log....460
8.3.3 Audit....460
8.4 Backup Management....460
8.4.1 Backup Service....460
8.4.1.1 What is Backup Service?....460
8.4.1.2 Backup Job....465
8.4.1.2.1 Create a Backup Job....465
8.4.1.2.2 Manage a Backup Job....476
8.4.2 Continuous Data Protection (CDP)....478
8.4.2.1 What is CDP?....478
8.4.2.2 CDP Task....481
8.4.2.2.1 Create a CDP Task....481
8.4.2.2.2 Manage a CDP Task....483
8.5 Scheduled O&M....484
8.5.1 Scheduled Job....484
8.5.1.1 What is Scheduled O&M?....484
8.5.1.2 Create a Scheduled Job....485
8.6 Tag Management....486
8.6.1 What is Tag?....486
8.6.2 Create a Tag....487
8.7 Migration Service....488
8.7.1 What is Migration Service?....488
9 Operational Management....490
9.1 Enterprise Management....490
9.1.1 What is Enterprise Management?....490
9.2 Billing Management....490
9.2.1 What is Billing Management?....490
9.2.2 Pricing List....492
9.2.2.1 Create a Pricing List....492
9.3 Access Control....495
9.3.1 Console Proxy....495
9.3.2 AccessKey Management....496
9.3.3 IP Allowlist/Blocklist....496
9.4 Application Center....496
9.4.1 What is Application Center?....496
9.4.2 Add an Application....496

10 Settings.....498
10.1 Sub-Account Setting.....498
10.1.1 What is Sub-Account?.....498
10.1.2 Create a Sub-Account.....499
10.2 Theme and Appearance.....500
10.2.1 What is Theme and Appearance?.....500
10.3 Email Server.....500
10.3.1 What is Email Server?.....500
10.3.2 Add an Email Server.....500
10.4 Log Server.....502
10.4.1 What is Log Server?.....502
10.4.2 Add a Log Server.....502
10.5 Global Setting.....503
10.6 Scenario Template.....503
Glossary.....504

1 Introduction

Product Version

This document applies to ZStack Cloud 4.3.12.

Intended Audience

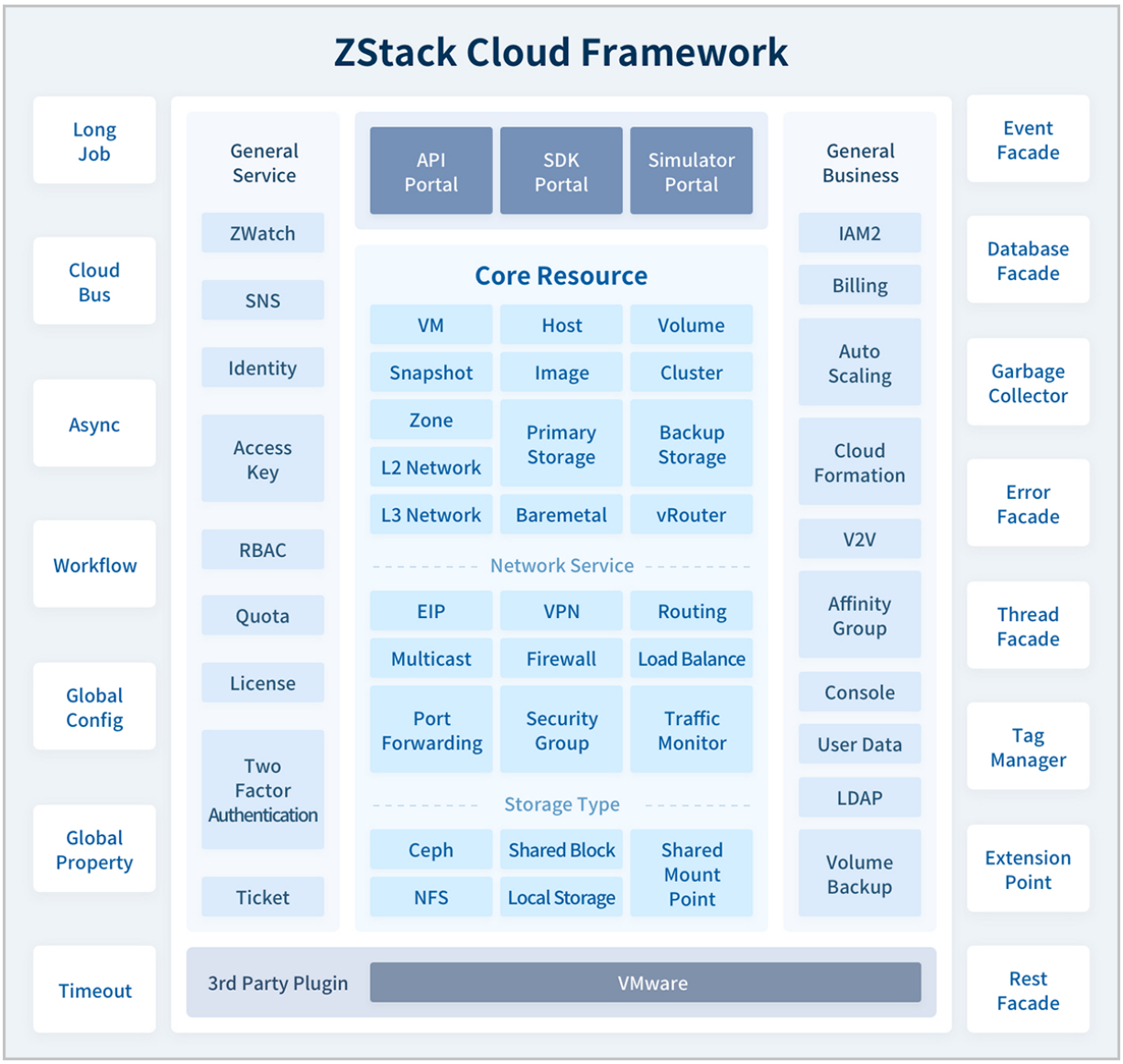
This document describes how to install, deploy, and use ZStack Cloud 4.3.12. The intended audience are as follows:

- Technical support engineers
- Maintenance engineers
- Product consulting engineers
- People who are interested in ZStack Cloud

2 Overview

ZStack Cloud is the next-generation, open-source IaaS software designed mainly for future-oriented, smart data centers. Also, it manages multiple data center resources of compute, storage, and network by providing flexible and comprehensive APIs. You can quickly set up your own smart cloud data center by using ZStack Cloud, and construct flexible cloud usage scenarios, such as VDI, PaaS, and SaaS, on the stable ZStack Cloud.

Figure 2-1: ZStack Cloud Framework



3 Configuration Requirements

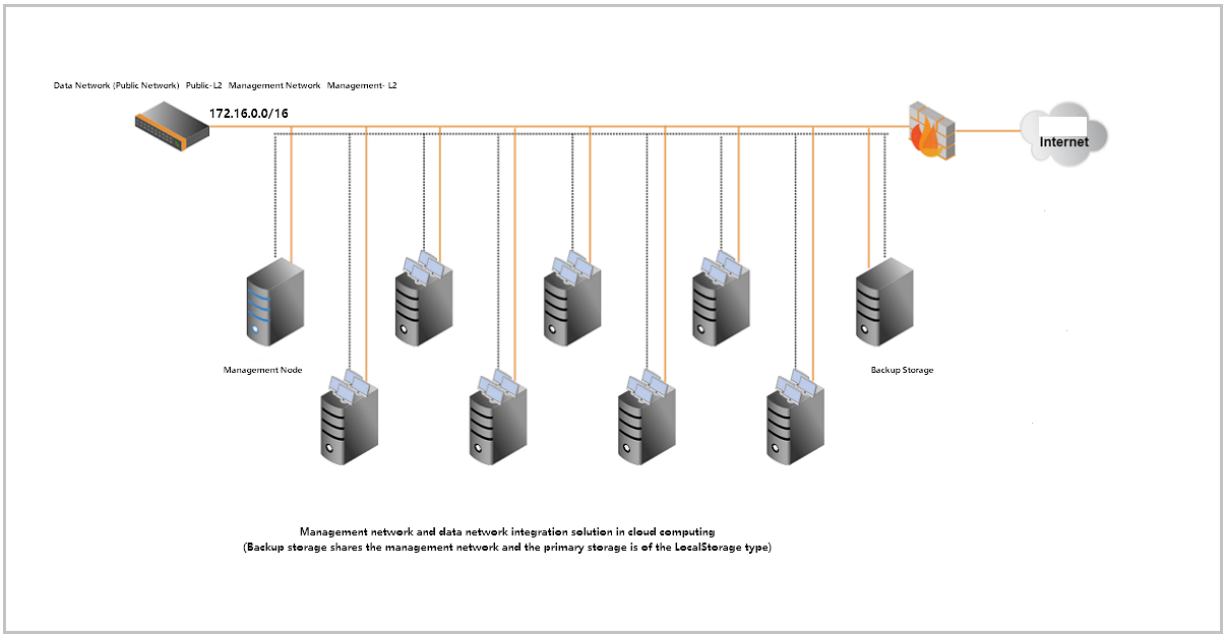
This topic describes the basic environment configurations required for the operation of ZStack Cloud.

3.1 Network Environment

Cloud computing environment is an essential IT infrastructure of enterprises. Before you install ZStack Cloud, you must prepare the basic hardware and software environments based on the required configuration settings. Incorrect environmental configurations may make you unable to complete environment deployment or encounter exceptions during usage.

The following figure shows a typical cloud environment built in a small data center. This environment consists of servers that are deployed for different usage and two independent networks.

Figure 3-1: Network Environment Diagram



As shown in the preceding figure, one server is used as the management node of ZStack Cloud and one server is used to store VM images. The other servers are used as the hosts of VM instances. Note that in small data centers, one server can serve as the management node and backup storage. In large physical environments, you can configure multiple management nodes to achieve high availability and configure multiple backup storages to extend backup storage space and throughput.

Every server is connected to the management network and data network. The data network can access the Internet through the firewall. The management network is used for the management node to manage hosts, VM instances, volumes, and other cloud resources. The data network is used for VM instances to provide data services. Note that the IP address in the preceding figure is used only for illustration.

Note:

- You need to assign static IP addresses to the servers that connect to the management network.
- You do not need to assign IP addresses to NICs of servers that connect to the data network. However, the name of the server NIC that connects to the data network must be consistent, for example, eth0.

3.2 Hardware Requirements

Hardware Configuration Requirements

The following table describes the configuration requirements over servers and other hardware devices for the installation and deployment of ZStack Cloud.

Device	Component	Configuration Requirements
Server	CPU	x86-64, with the support for Intel VT or AMD V virtualization hardware extensions, such as Intel VMX or AMD SVM
	Memory	No special requirements, DDR4 or higher-performance memory recommended
	Motherboard	Dual socket server motherboard
	RAID	SAS/SATA RAID 0/1/10 and support for pass-through mode
	Hard Disk	No special requirements, hard disk drive (HDD) or solid state disk (SSD)
	NIC Port	• One NIC port of a gigabit for connecting to the management network, such as 1 Gb RJ45 Ethernet NIC port • One NIC port of a ten-gigabit for connecting to the business network, such as 10GbE SFP+ port

Device	Component	Configuration Requirements
Network Switch	/	• At least a one-gigabit switch, ten-gigabit switch recommended • Several Category 5 jumpers

When you configure hardware settings, note that:

- Make sure that CPU virtualization is enabled in the server BIOS. In addition, make sure that the CPU model of all servers is consistent. This avoids inconsistency of CPU instruction sets of the servers.
- Make sure that storage configurations are complete in advance:
  - If you use LocalStorage, we recommend that you apply backup storage redundancy. For example, you can configure a RAID 10 array by using four disks. This makes the primary storage and backup storage more reliable. If higher read/write performance of VM instances is required, we recommend that you configure a RAID array by using SSD disks. If higher read performance of VM instances is required, we recommend that you configure a RAID array by using a mix of SSD and HDD disks.
  - If you use NFS, Ceph, or other distributed network storage that supports Shared Mount Point, you need to configure a relevant storage system or file system in advance. If you configure a Ceph backup storage, you need to configure a Ceph primary storage.
- Make sure that you complete network configurations in advance. We recommend that you configure identical names for NICs on all hosts and use the NICs that share the same name for data communications of the same type. For example, you can configure the name em1 for NICs that are used for management traffic transfers.
- Make sure that you complete network switch configurations in advance:
  - To use VLAN network environments, configure VLAN network communications on the switch in advance.
  - ZStack Cloud automatically assigns IP addresses to VM instances. You need to reserve an IP address range that does not conflict with the system and does not conflict with the existing DHCP service.
- The CPU, memory, storage, and NIC settings decide the business performance of ZStack Cloud:

- Minimum-configuration environment (All In One): requires a minimum of 4 CPU cores and 8 GB memory. This configuration is used only for demonstrations and is not recommended for production environments.
- Production environment: management node configurations decided based on your deployment scale and compute node configurations decided based on your business scale. For more information, contact the official technical support.

Management Node Configurations

The following table describes the hardware server resources that a management node occupies in different deployment scales.

Configuration Item	**Deployment Scale (Number of Hosts)**			
	=1 (Non-Production Environment)	**<=50**	**<=500**	**<=1000**
	Minimum Configuration	**Recommended Configuration**	**Recommended Configuration**	**Recommended Configuration**
CPU	4 cores	16 cores	32 cores	64 cores
Memory	8 GB	32 GB	64 GB	128 GB
Storage	60 GB	120 GB	480 GB	960 GB
Note: The preceding configurations are used for reference only. Required configurations vary depending on your demand and environment. For more information, contact the official technical support.				

4 Installation and Deployment

4.1 Environment Preparations

Prerequisites

To install or upgrade ZStack Cloud, you need to prepare the custom ISO of ZStack Cloud:

1. Two custom ISO editions of ZStack Cloud are available:
   - c76: ZStack-Cloud-x86_64-DVD-4.3.12-c76.iso
   - c74: ZStack-Cloud-x86_64-DVD-4.3.12-c74.iso

   Note:

   - The custom ISO of the c76 edition inherits all features of the c74 edition. In addition, it uses the updated operating system core and supports NVIDIA vGPU.
   - **For the first installation of ZStack Cloud, we recommend that you use ISO of the c76 edition.**. If you have deployed ZStack Cloud, you can upgrade the Cloud to the latest version of the same edition. For more information, see Upgrading Tutorial.
   - Starting from 3.7.1, ZStack Cloud custom ISO of the c72 edition is no longer available. If you have deployed the ISO of the c72 edition, contact the technical support for upgrading.
2. ZStack Cloud allows for offline installation. You do not need to connect to the public network or configure the local repo.
3. The following installation modes are available: Enterprise Management Node , Community Management Node, Compute Node, Expert Mode. You can select a mode based on your business needs.
4. Default settings: **DATE&TIME**: Asia/Shanghai timezone. **LANGUAGE SUPPORT**: English(United States). **KEYBOARD**: English(US).

The initial installation of c74 ISO and c76 ISO basically is the same. This topic takes c76 ISO as an example to describe the installation process.

1. Prepare files.
2. Write the image.
3. Install the operating system.

Procedure

1. Prepare files.

Before you install ZStack Cloud, prepare the following packages for installation and deployment:

- ZStack Cloud custom ISO:
  - C76: ZStack-Cloud-x86_64-DVD-4.3.12-c76.iso
  - C74: ZStack-Cloud-x86_64-DVD-4.3.12-c74.iso
  - Download address: *Click here*
- ZStack Cloud installation package:
  - Software: ZStack-Cloud-installer-4.3.12.bin
  - Download address: *Click here*

Note:

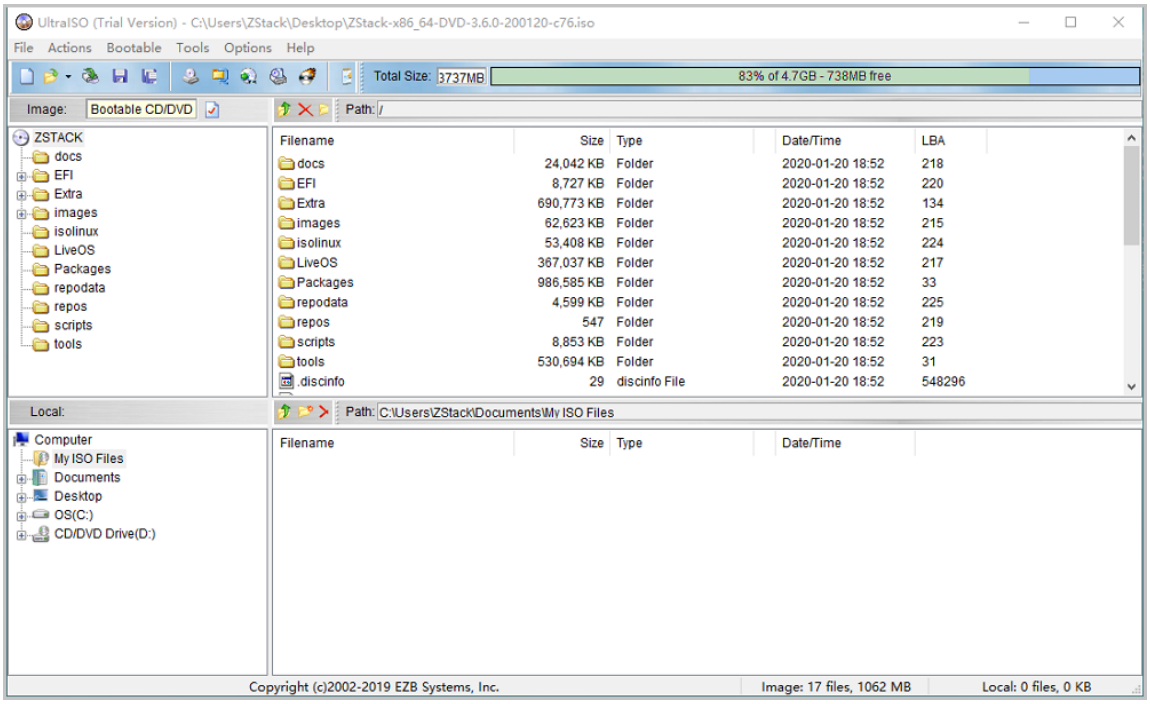
After you download the software packages, check the MD5 hash by using a MD5 checker to verify software integrity.

2. Use UltraISO to burn the image file to a U disk.

   a) Use UltraISO to open the ISO image file.

   Open UltraISO, click the **File** button, and open the downloaded ISO image file.

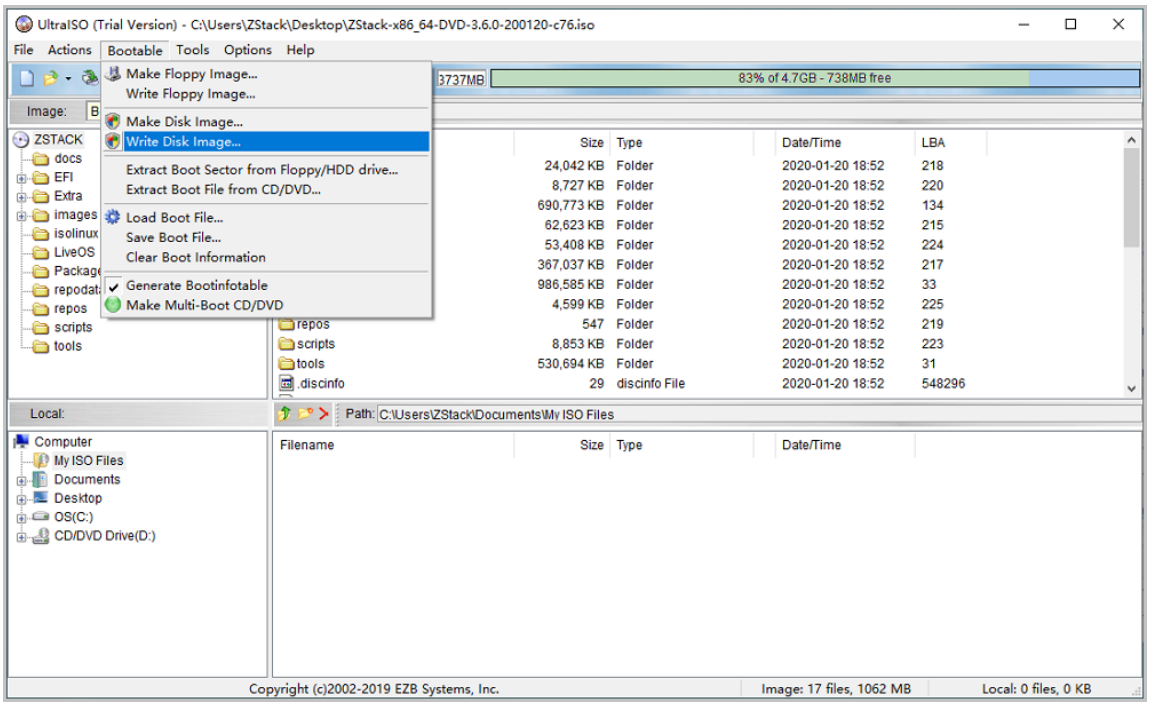
   Figure 4-1: Use UltraISO to Open ISO Image File



   b) Write the Image.

In UltraISO, choose **Bootable** > **Write Disk Image**.

Figure 4-2: Write Disk Image on UltraISO

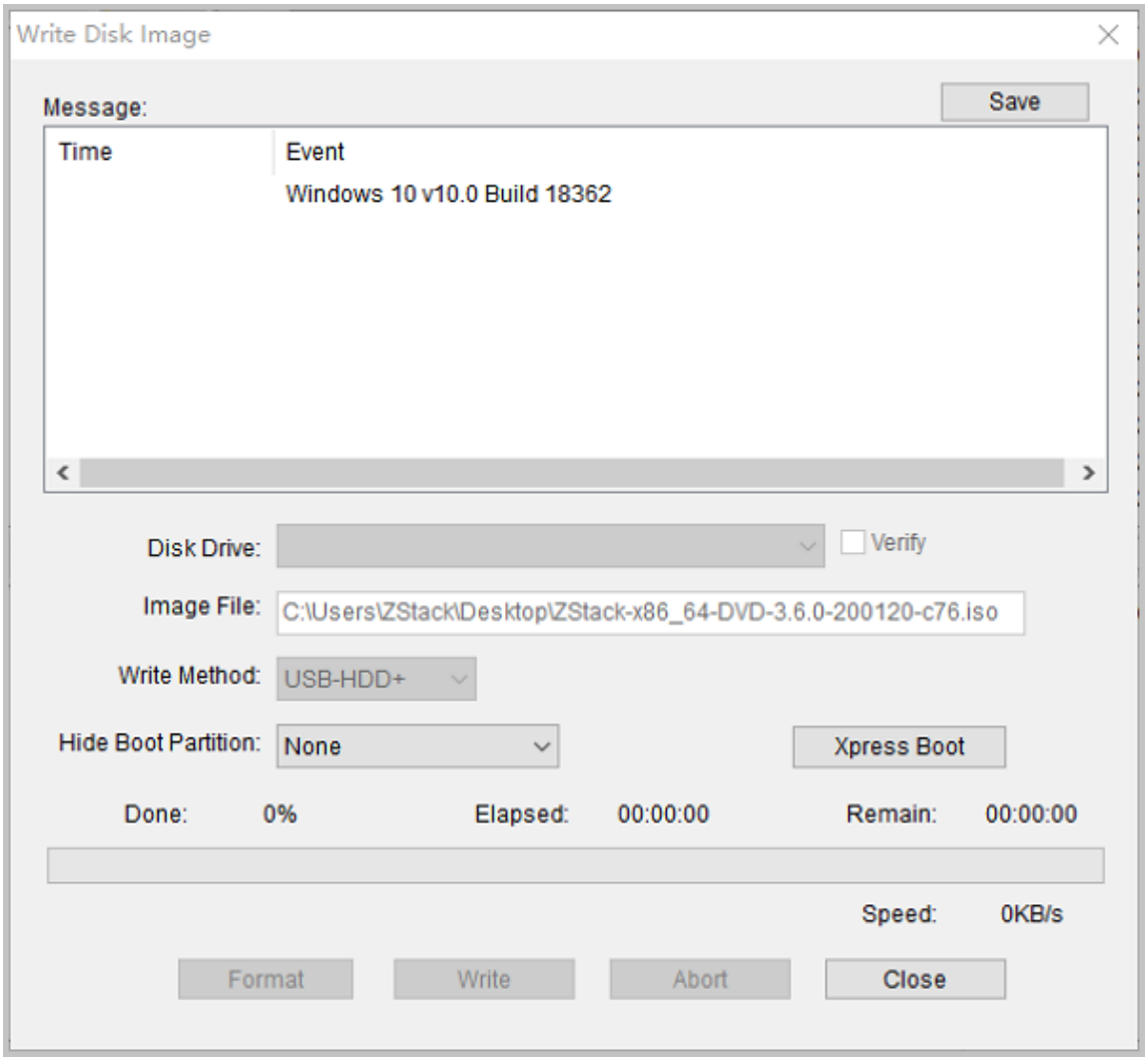


c) Select a U disk from the **Disk Drive** drop list to burn the image file.

Note:

- If only one U disk is available, the U disk is used to burn the image file by default. Note that before you burn the image file, **backup the data on the U disk**.
- Use the default settings for the other parameters and then click **Write**.

Figure 4-3: Confirm to Write ISO Image on UltraISO



d) On the page that appears, click **Yes**. Then UltraISO burns the ISO image file to the U disk.

e) Then the U disk is used as the startup disk. This disk supports the Legacy and UEFI boot modes.

3. Install the operating system.

a) Configure the server.

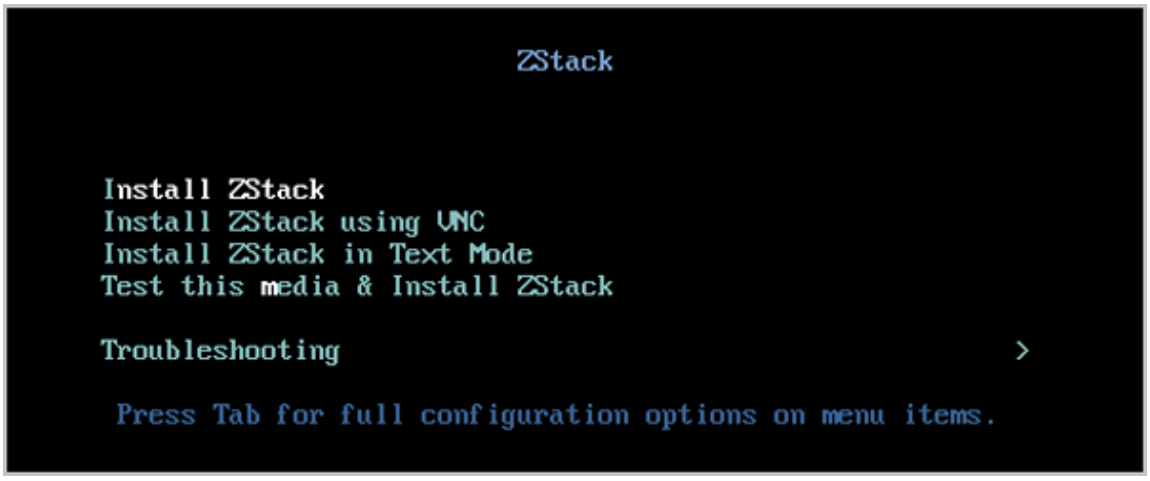
- Make sure that the data on the disks of the server is backed up. The data will be overwritten during installation.
- Enter BIOS and enable the virtualization technology and hyper-threading options for CPU .
- Enter the RAID configuration page and configure the RAID level to provide a data redundancy mechanism that suits your business needs.

- Place the system startup disk in the first boot order.

b) Select the boot item.

On the ISO system boot interface, select the default option and then install the operating system.

Figure 4-4: System Boot



Note:

- ZStack Cloud provides the following installation methods: (graphic user interface) GUI, virtual network computing (VNC), and character user interface (CUI). We recommend that you use GUI to install the operating system.
- If the server does not have a VGA connector and only supports serial communication, you can use the VNC or CUI method.

c) Installation configuration summary

The following figure displays system installation configurations. You can specify the configurations based on your needs. The default settings provided by ZStack Cloud are as follows:

- **DATE&TIME**: Asia/Shanghai timezone. We recommend that the admin checks the host time and sets to the current timezone and time.
- **LANGUAGE**: English(United States).
- **KEYBOARD**: English(US).

Figure 4-5: System Installation Interface

d) Select the installation mode.

On the **INSTALLATION SUMMARY** page, click **SOFTWARE SELECTION** to enter the **SOFTWARE SELECTION** page. Select an installation mode on the page.

ZStack Cloud provides the following installation modes:

- ZStack Enterprise Management Node

  Note:

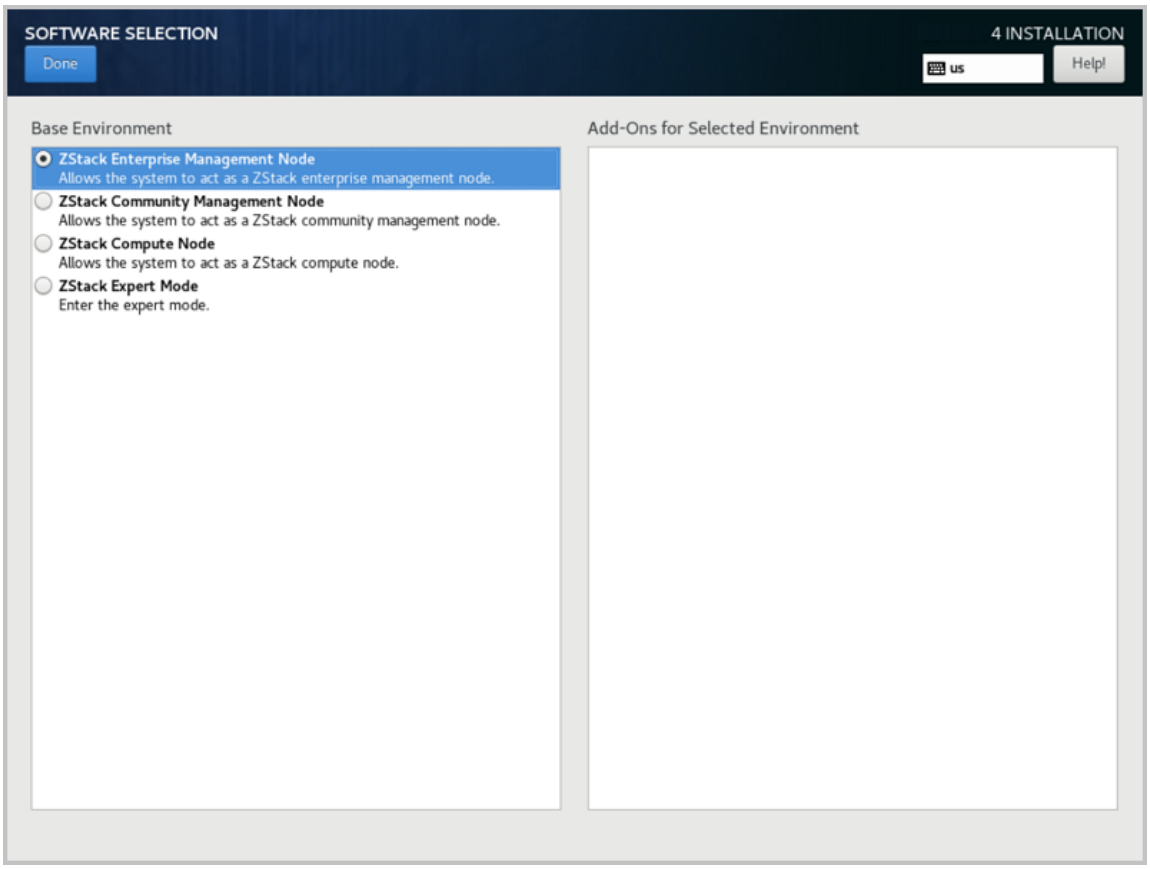
  We recommend that you select this mode in the initial installation.

- ZStack Community Management Node
- ZStack Compute Node
- ZStack Expert Mode

Note:

- If you select this mode, after the system is installed, you are redirected to the terminal where you can customize installation of the cloud platform. If you select other modes, after the system is installed, the system automatically installs the cloud platform in the selected mode.
- **No ZStack Local Repo**: simplified installation. If you select this item, the ISO image file is not copied during installation and internal repo is not generated.

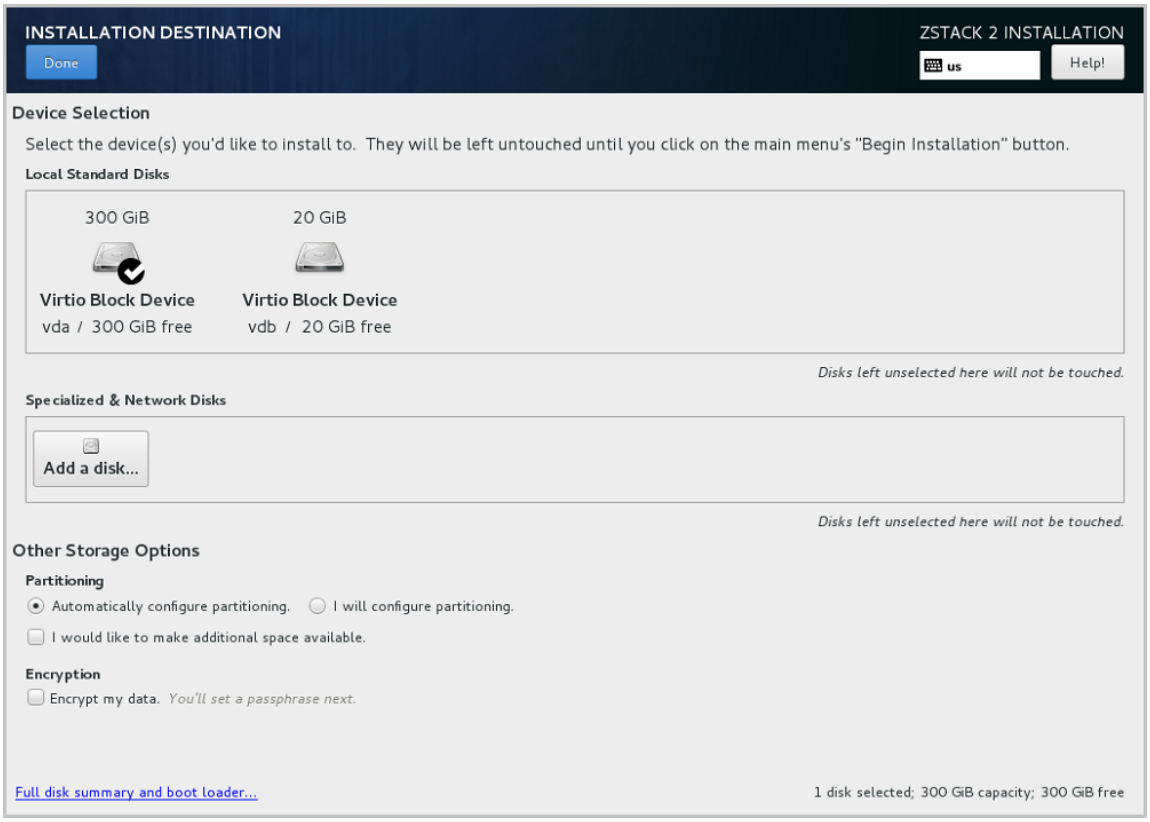
Figure 4-6: Select Installation Mode



e) Configure disk partitioning.

On the **INSTALLATION SUMMARY** page, click **INSTALLATION DESTINATION** to enter the **INSTALLATION DESTINATION** page.

Figure 4-7: Default Disk Partitioning



Note:

We recommend that you configure only the system disk on the page. After the system is installed, you can configure other disks.

ZStack Cloud sets partitioning to **Automatically configure partitioning** by default. If you want to customize partitioning, set the parameters based on the BIOS boot mode:

- UEFI mode
  - */boot*: stores the core files required for Linux startup. We recommend that you distribute 1 GB to the directory.
  - */boot/efi*: stores UEFI boot file. We recommend that you distribute 500 MB to the directory.
  - *swap*: swap. We recommend that you distribute 32 GB to the swap.
  - */*: Linux system root. We recommend that you distribute the rest of the space to the directory.
- Legacy mode

— */boot*: stores the core files required for Linux startup. We recommend that you distribute 1 GB to the directory.

— *swap*: swap. We recommend that you distribute 32 GB to the swap.

— */*: Linux system root. We recommend that you distribute the rest of the space to the directory.

Note:

- We recommend that the total disk capacity for ZStack Cloud be greater than 300 GB.
- In Legacy mode, if the capacity of the system disk is greater than 2 TB, you need to configure the BIOS boot partition for the support of the GPT partition. In UEFI mode, you do not need to configure this item and the GPT partition is supported.

f) Configure the network.

This step describes how to configure a static IP address for a NIC and enable auto-activation of NIC. This configuration is used only for proof of concept (POC). In the production environment, we recommend that you configure NIC bonding. For more information, see *Network Bonding (Optional)*.

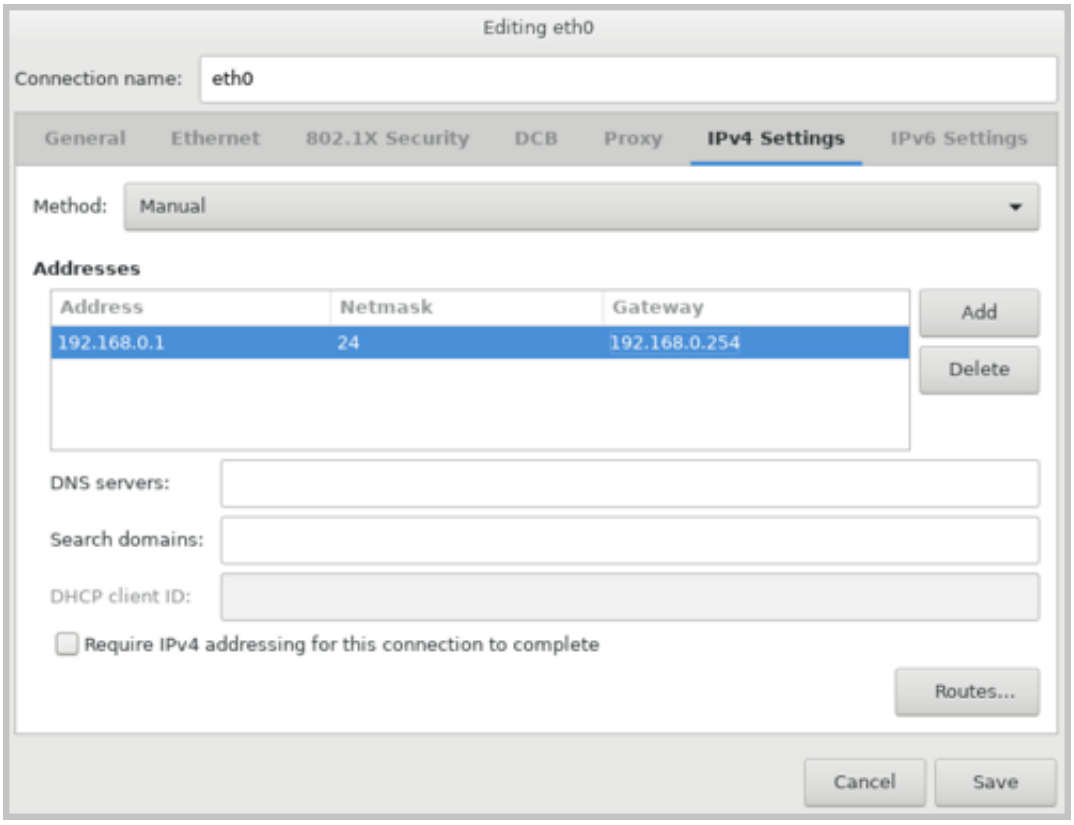
1. Configure a static IP address.

   a. On the **INSTALLATION SUMMARY** page, choose **NETWORK & HOST NAME** > **Ethernet (eth0)** > **Configure...**. Then the **Editing eth0** page is displayed. On the page, choose **IPv4 Settings** > **Method** > **Manual**. Then you can manually assign an IP address.

   Note:
   You can also use DHCP to automatically obtain an IP address.

   b. Click **Add** to add an IP entry, configure the IP address, subnet, and gateway, and then click **save** to save the configurations.

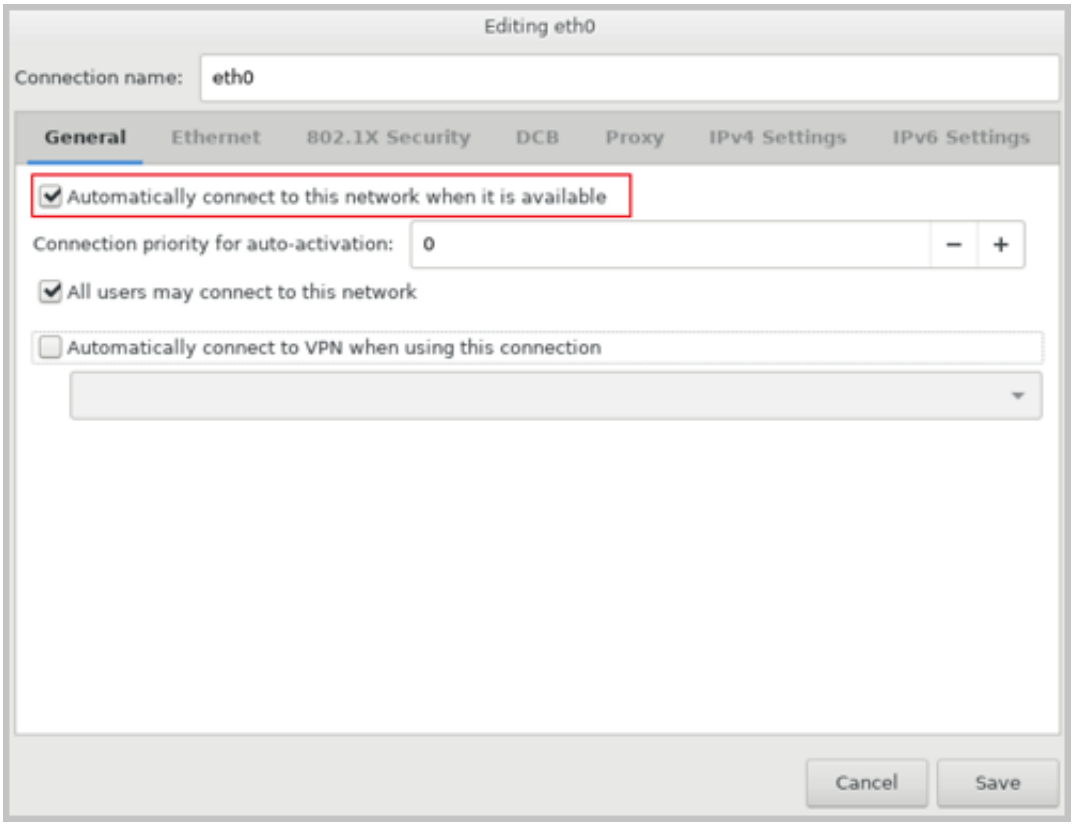
Figure 4-8: Configure Static Address



2. Configure NIC auto-activation.

   On the **Editing eth0** page, choose **General** > **Automatically connect to this network when it is available** > **Save**. Then the auto-activation is enabled.

Figure 4-9: Configure NIC Auto-Activation



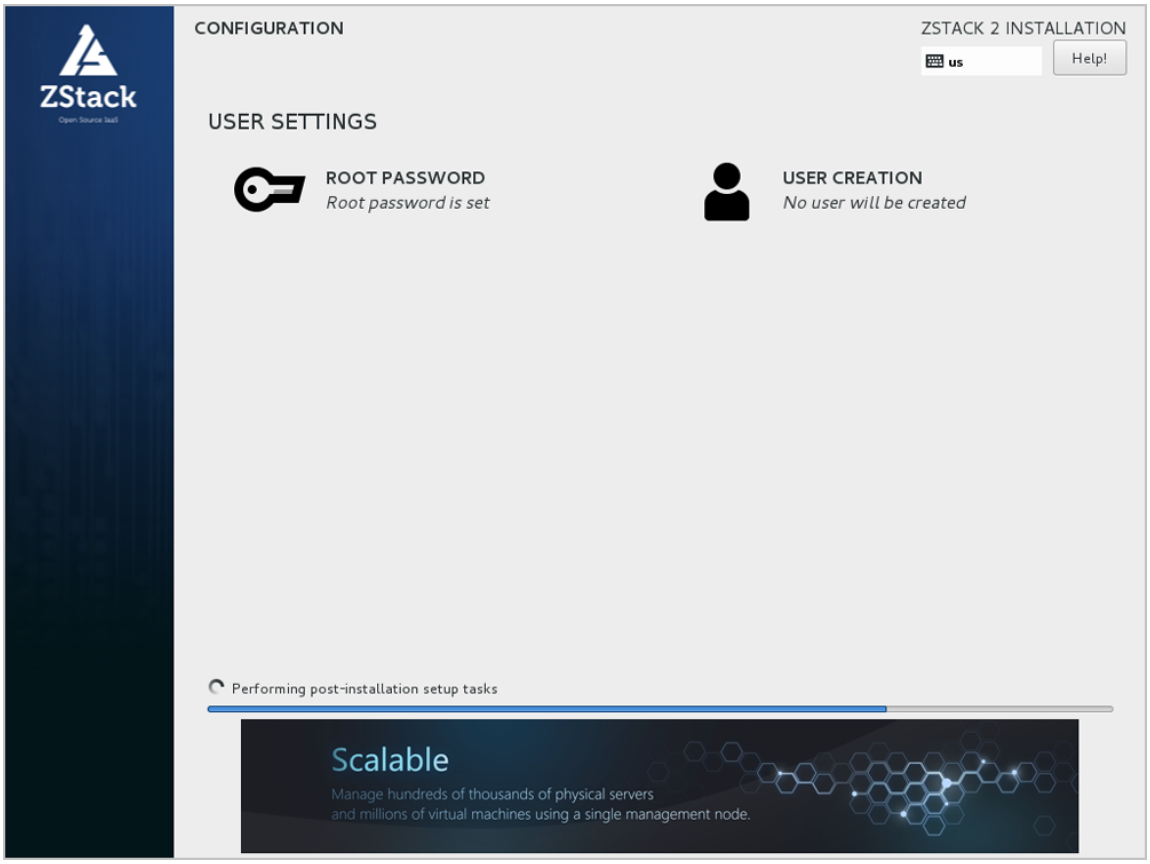
g) Start installation.

Go back to the **INSTALLATION SUMMARY** page, click **Begin Installation** to install the operating system.

h) Set a password.

When the installation is in progress, click **ROOT PASSWORD** to set a root password.

Figure 4-10: Set Password



i) Enter the system.

After the system is installed, click **Restart** and enter the custom system of ZStack Cloud.

4.1.1 Network Bonding (Optional)

This topic describes how to configure network bonding. You can use this method when you want to install and deploy ZStack Cloud in your production environments.

You can configure network bonding by using command line tool or GUI.

Command Line Tool

After you complete installing ZStack Cloud, you can configure network bonding by running the following commands according to your deployment requirements:

```
# Create a link aggregation virtual interface in LACP mode
zs-bond-lacp -c [bond-name]
zs-bond-lacp -c bond0

# Create another link aggregation virtual interface in active-backup
mode
zs-bond-ab -c [bond-name]
zs-bond-ab -c bond0
```

```
# Bind the physical interface to the link aggregation interface
zs-nic-to-bond -a [bond-name] [nic-name]
zs-nic-to-bond -a bond0 eth0

# Create a VLAN interface
zs-vlan -c [nic-name] [vlan]
zs-vlan -c bond0 10

# Create a network bridge, and configure the network IP address for
the network bridge
zs-network-setting -b [interface] [ipaddress] [netmask] [gateway]
zs-network-setting -b bond0.10 192.168.1.10 255.255.255.0 192.168.1.1
```

GUI

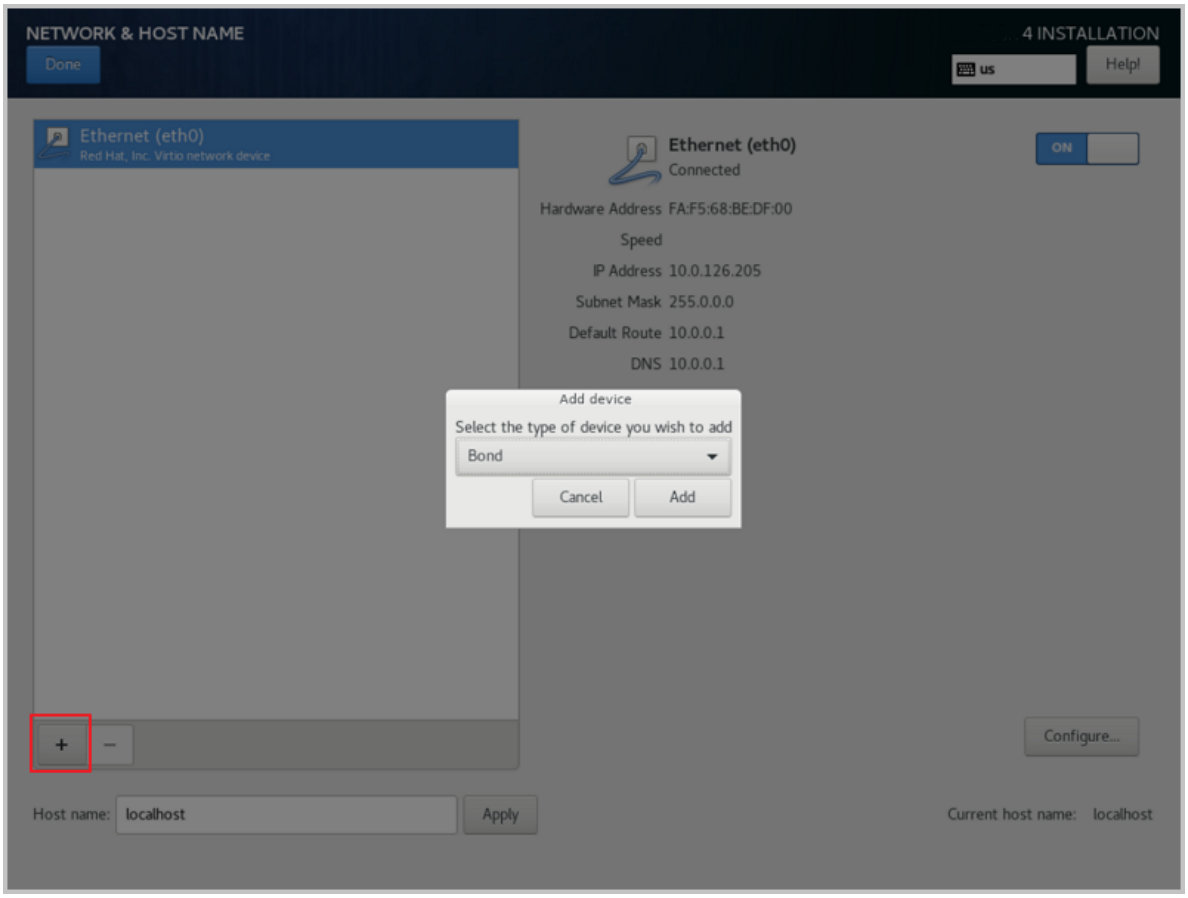
When you install the operating system, you can configure network bonding by using the GUI. The following lists the process of network bonding:

1. Add a bond device.
2. Add a bond slave.
3. Select a bond mode.
4. Disable IPv4 settings of original NIC.
5. Complete the NIC bonding configurations.
6. Configure static IP address for the bond.
7. Configure NIC auto-activation.

1. Add a bond device.

   On the **INSTALLATION SUMMARY** page, choose **NETWORK & HOST NAME** > **Ethernet (eth0)** > **Configure...**. Then the **eth0** configuration page is displayed. Click the plus sign (**+**) at the lower left, select **Bond** from the prompted **Add device** drop-down list, and click **Add**.

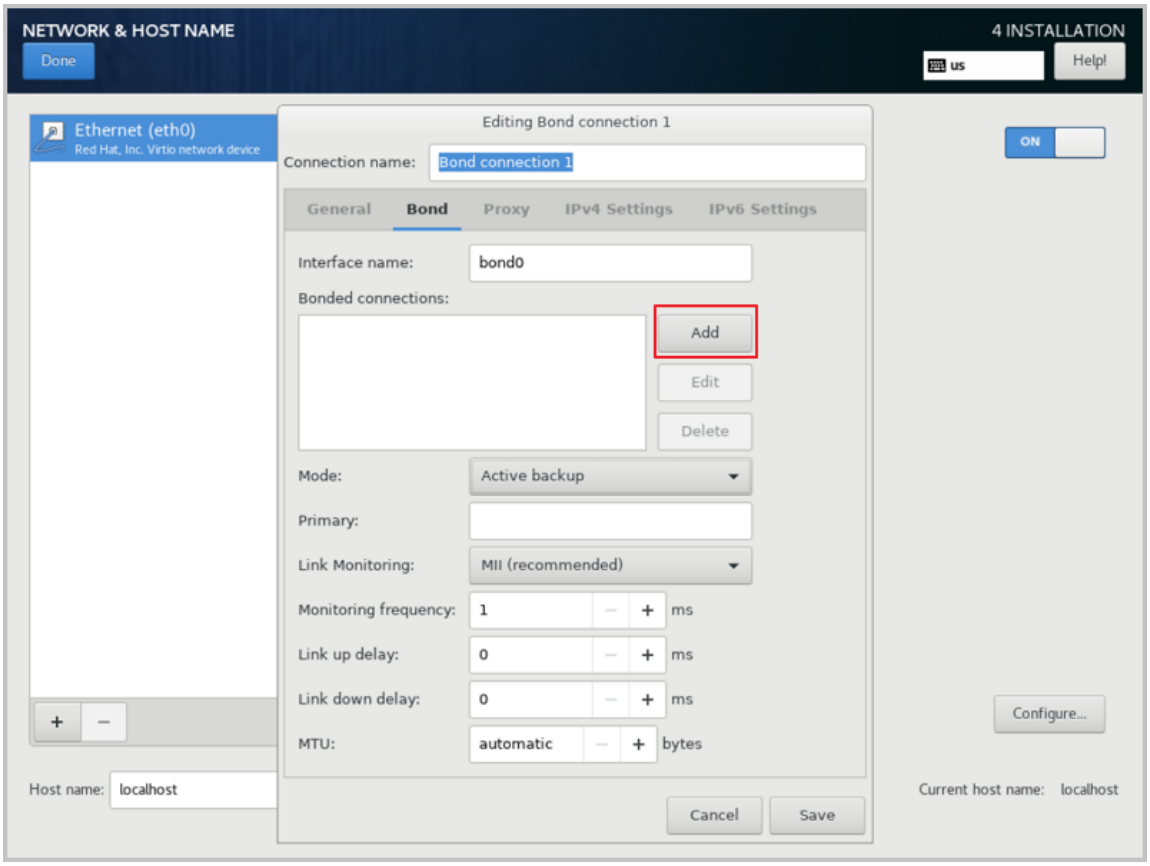
Figure 4-11: Add Bond Device



2. Add a bond slave.

   a. On the bond configuration page, click **Add** to add a bond slave.

Figure 4-12: Add Bond Slave

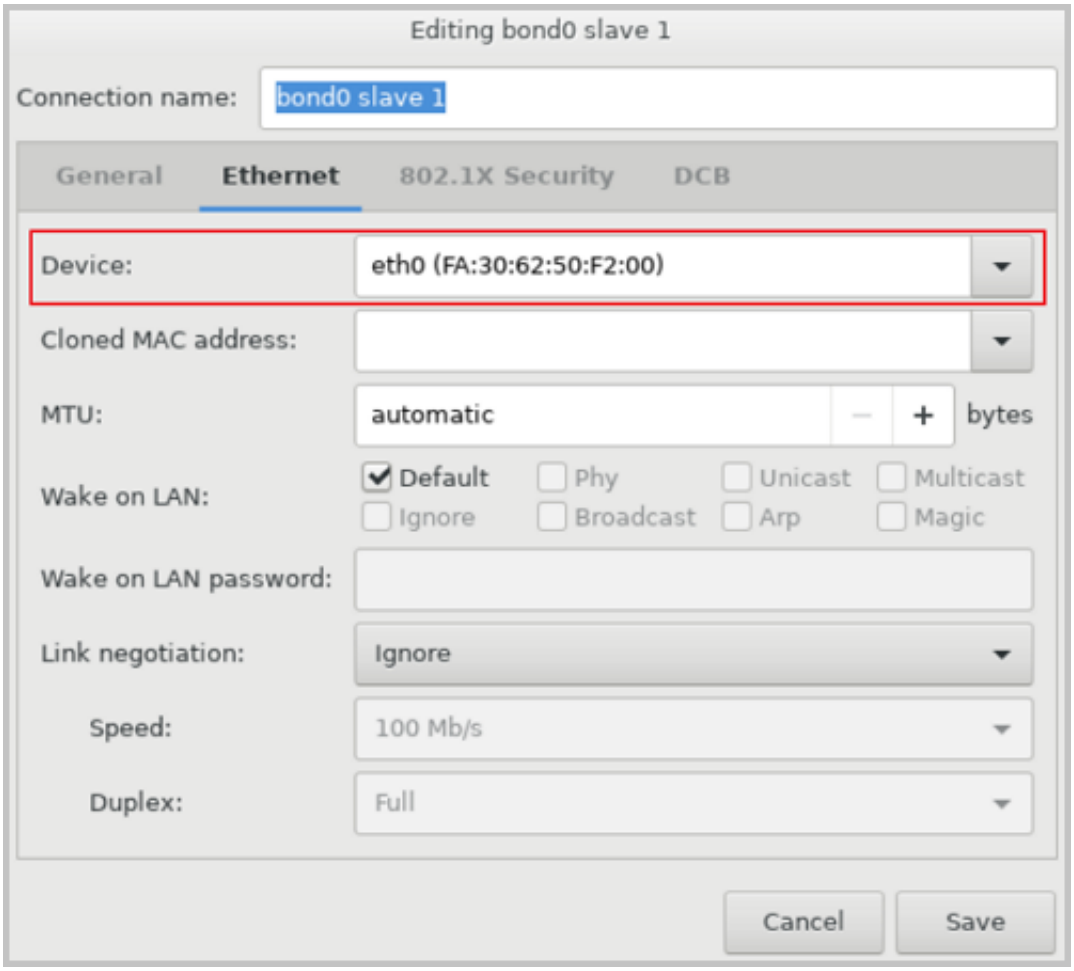


b. On the displayed **Choose a Connection Type** page, choose a bond slave connection type from the drop-down list, for example, **Ethernet** and then click **Create...**

Figure 4-13: Choose Bond Slave Connection Type

c. On the **Ethernet** tab of the **Editing bond0 slave1** page, select a bond slave device from the **`Device`** drop-down list, for example, **eth0 (MAC address)**. Then, configure settings or use the default settings for the other parameters. After you complete the settings, click **Save**.

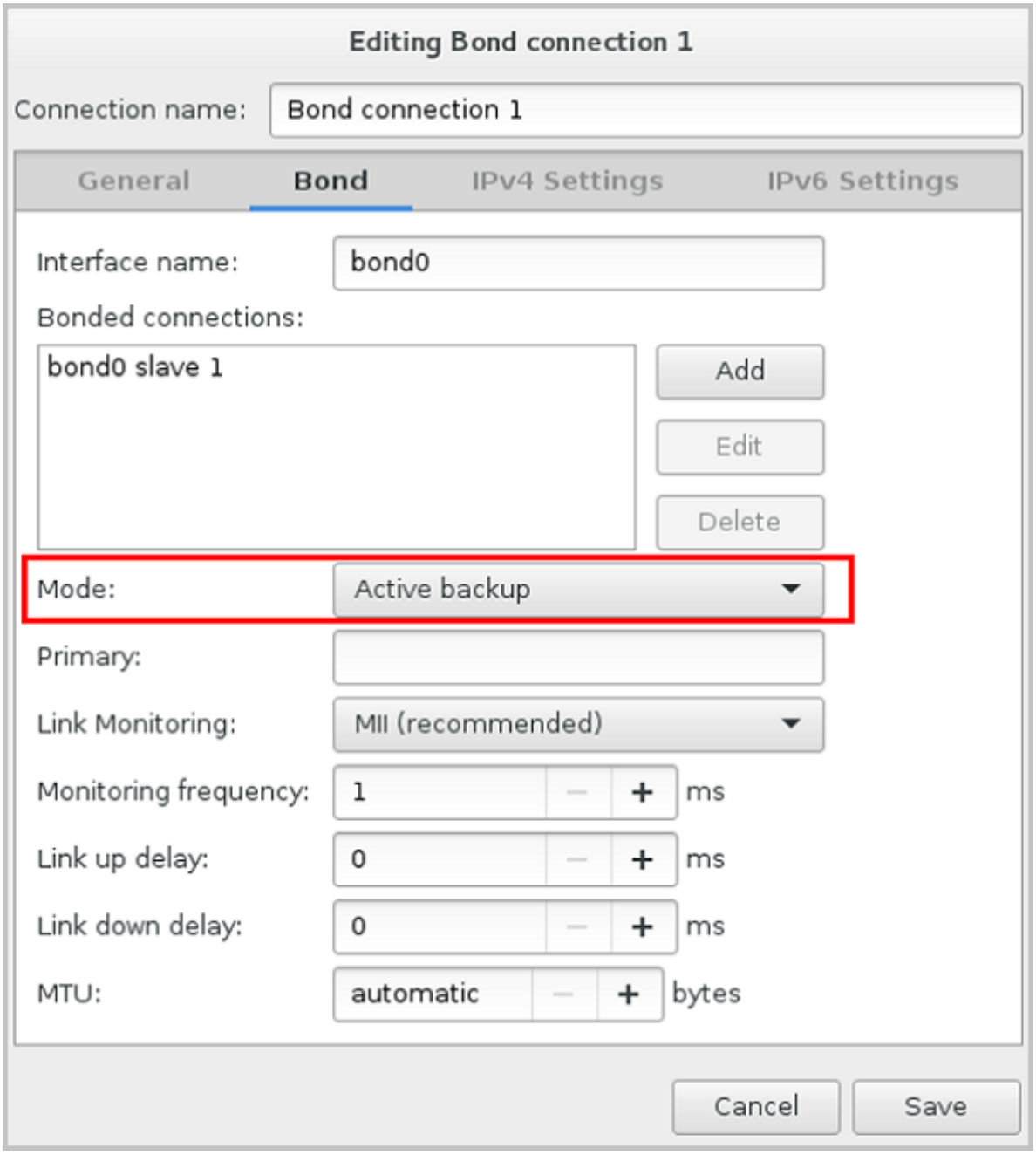
Figure 4-14: Select Bond Slave Device



3. Select a bond mode.

From the **`Mode`** drop-down list of the Bond tab, select the bond mode as need, such as **Active backup**. Then, configure settings or use the default settings for the other parameters. After you complete the settings, click **Save**.

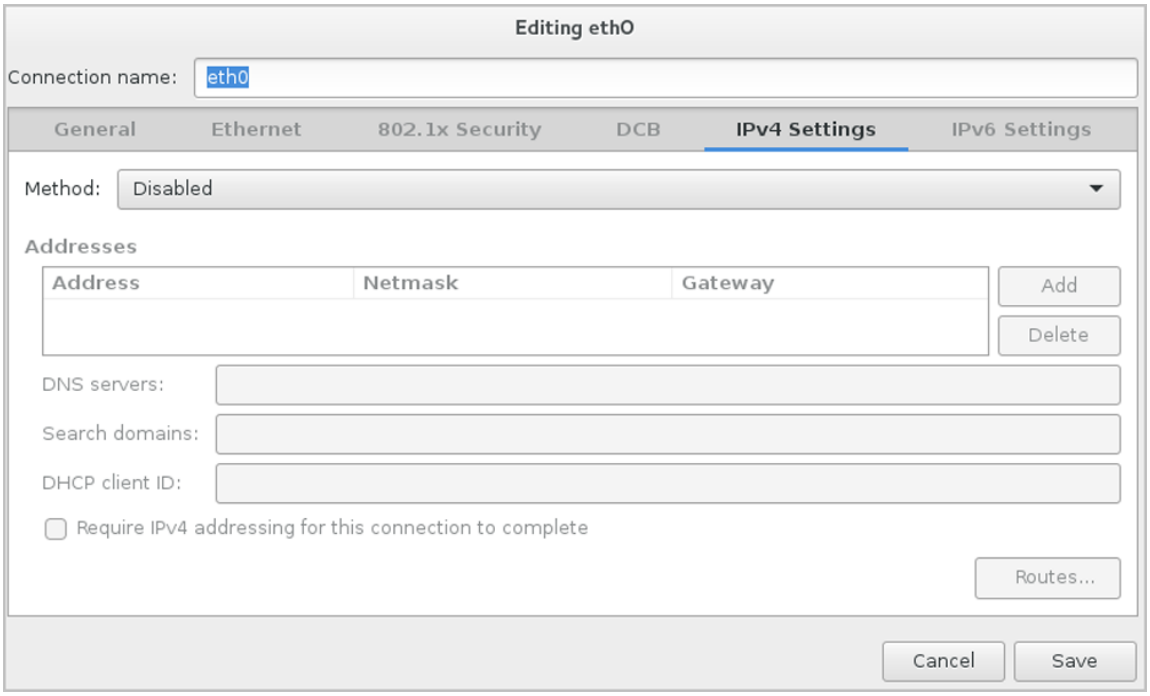
Figure 4-15: Select Bond Mode



4. Disable the IPv4 settings of the original NIC.

   - On the **Ethernet (eth0)** page, choose **Configure...** > **IPv4 Settings**. On the tab, set **Method** to **Disabled** and then click **Save**.

- **Figure 4-16: Disable IPv4**

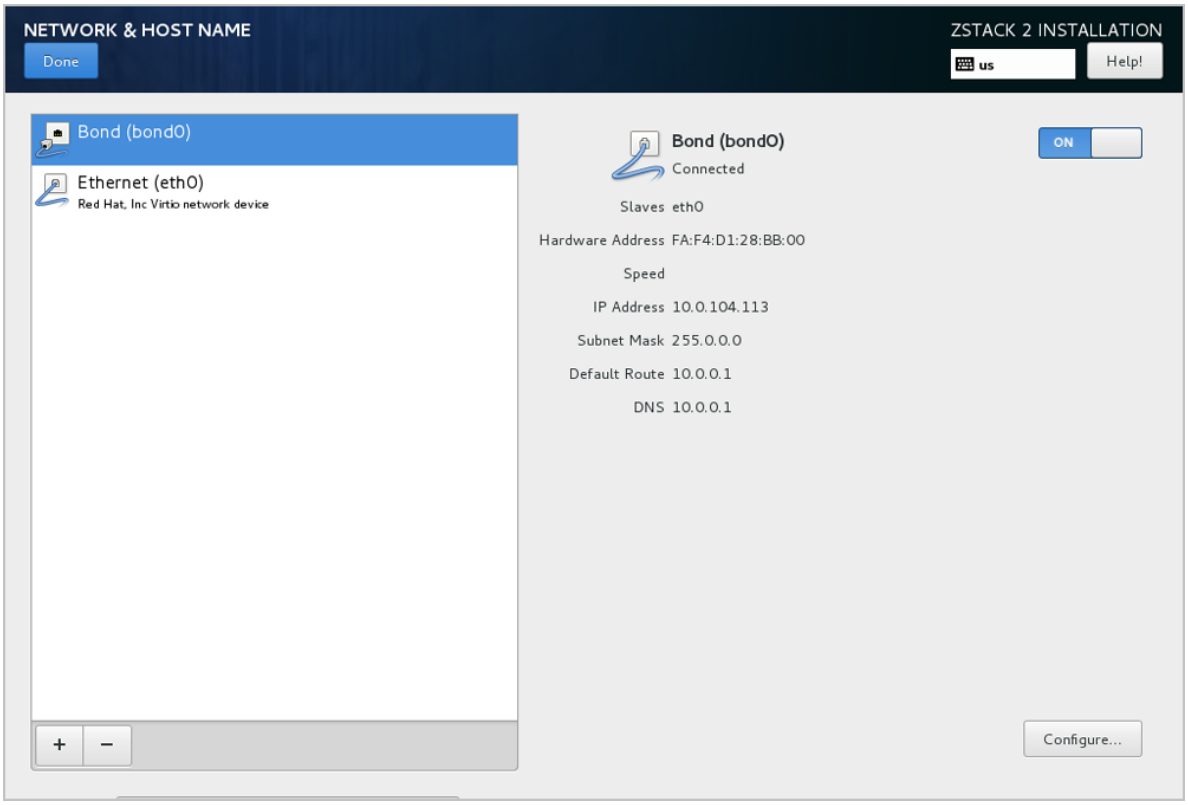


5. Complete the network bonding configurations.

Note:

Make sure that you turn on the **On** switch on the bond configuration tab and configure the IP address. In addition, make sure that you turn on the **On** switch for the bond slave, for example, eth0. Otherwise, you might fail to install ZStack Cloud properly.

Figure 4-17: Complete NIC Bonding



6. Configure a static IP address for bond device

   a. On the **INSTALLATION SUMMARY** page, choose **NETWORK & HOST NAME** > **Bond (bond0)** > **Configure...**. Then the **Bond (bond0)** page is displayed. On the page, choose **IPv4 Settings** > **Method** > **Manual**. Then you can manually assign an IP address.

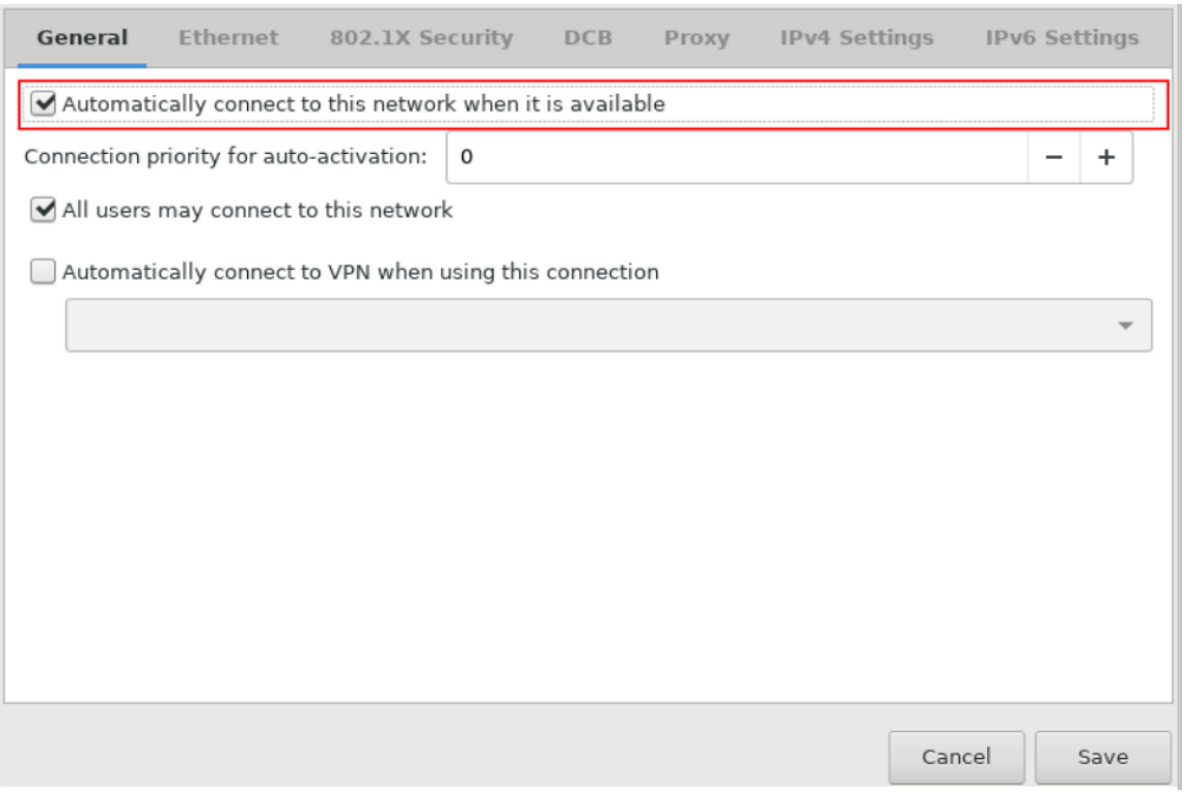
   > **Note:**
   > You can also use DHCP to automatically obtain an IP address.

   b. Click **Add** to add an IP entry, configure the IP address, subnet, and gateway, and then click **save** to save the configurations.

7. Configure NIC auto-activation.

   On the **Bond (bond0)** page, choose **General** > **Automatically connect to this network when it is available** > **Save**. Then the auto-activation is enabled.

Figure 4-18: Configure NIC Auto-Activation



4.2 Install ZStack Cloud

This topic describes the installation mode of ZStack Cloud 4.3.12.

ZStack Cloud Custom ISO Installation Mode

ZStack Cloud custom ISO provides the following installation modes:

- Enterprise Management Node Mode
- Community Management Node Mode
- Compute Node Mode
- Expert Mode

The following describes the installation process in different mode:

1. **Enterprise Management Node Mode**
   - Install the basic system.
   - Install dependencies such as MariaDB and CloudBus.
   - Auto-install and start ZStack Cloud
2. **Community Management Node Mode**

- Install the basic system.
- Install dependencies such as MariaDB and CloudBus.
- Auto-install and start ZStack Cloud

Note:

- The Enterprise Management Node Mode is different from the Community Management Node Mode in terms of **the license type, which decides the features available on the Cloud**.
- The Enterprise Management Node Mode is the same as the Community Management Node Mode in terms of the installation process.

3. **Compute Node Mode**

- Install the basic system.
- Install virtualization components such as Libvirt and QEMU.

4. **Expert Mode**

- Install the basic system.

Note:

- The expert mode is basically same as the minimum installation mode of CentOS 7 series.
- If the admin needs deep customization, the admin can select the Expert Mode and manually customize into one of the other three modes.

Different installation modes are applied to different installation scenarios.

Table 4-1: Installation Scenarios

Mode	Scenario
Enterprise Management Node Mode	Applicable only to the installation of management nodes of the Enterprise edition.
Community Management Node Mode	Applicable only to the installation of management nodes of the Community edition.
Compute Node Mode	Applicable to the installation of all nodes except the management nodes, such as • Compute node • ImageStore, Ceph backup storage node, and Ceph backup storage mount node
Expert Mode	

Mode	Scenario
	• Ceph primary storage node, and Ceph primary storage mount node • PXE deployment server node, local backup server node, and remote backup server node in another data center

4.2.1 ZStack Cloud Management Node Mode

As described in the previous topic,

- The Enterprise Management Node Mode is different from the Community Management Node Mode in terms of **the license type, which decides the features available on the Cloud**.
- The Enterprise Management Node Mode is the same as the Community Management Node Mode in terms of the installation process.

Auto-Install ZStack Cloud on Management Node

If you select Enterprise or Community Management Node Mode, the system automatically restarts and install the ZStack Cloud on the management node.

Figure 4-19: Auto-Installation on Management Node

4.2.2 ZStack Cloud Compute Node Mode

If you select Compute Node Mode, the system automatically restarts and install the ZStack Cloud on compute nodes.

> **Note:**
> In some scenarios, you may need to install ZStack Cloud in All-in-One mode. In this case, we recommend that you select ZStack Cloud Management Node Mode.

Considerations

Technically, a management node can manage unlimited compute nodes. Note that the number of compute nodes that you can use is limited by the quota authorized in the license.

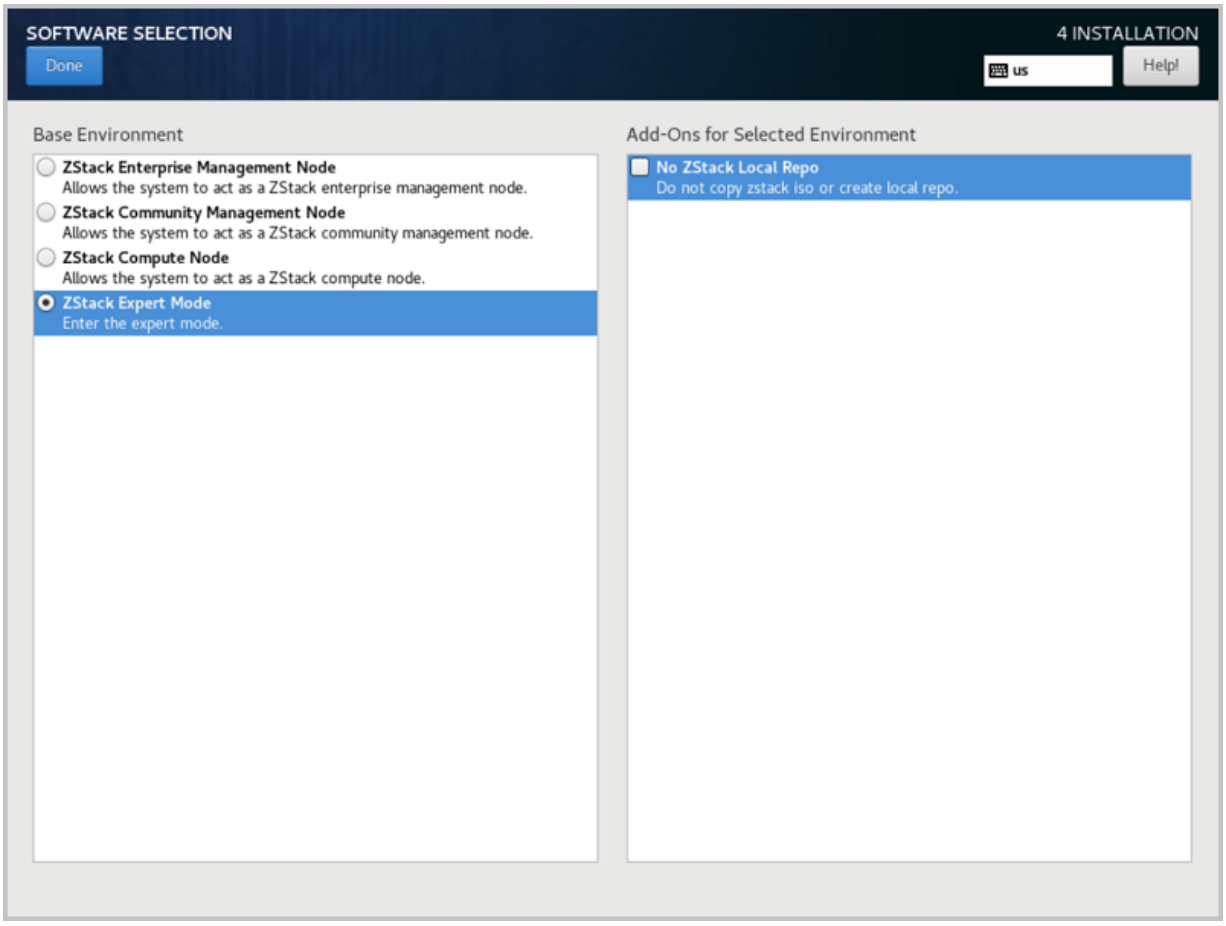
4.2.3 ZStack Cloud Expert Mode

If you select Expert Mode, after the system is installed and restarted, you are redirected to the terminal. Then you can customize installation of ZStack Cloud based on your needs.

Considerations

The expert mode supports simplified installation. After you select ZStack Expert Mode on the left pane, you can select **No ZStack Local Repo** on the right pane to implement simplified installation.

Figure 4-20: Simplified Expert Mode



Note:

In simplified expert mode, the ISO file in the `/opt/zstack-dvd/` directory is not copied and configuration files such as **zstack-local.repo** are not generated in the `/etc/yum.repos.d/` directory.

4.3 Manage ZStack Cloud

Procedure

1. After the initial installation, the system automatically starts ZStack Cloud service.
2. After the management node is restarted, ZStack Cloud service is started.
3. If the management node stops due to maintenance or other exceptions, you need to manually start the service.

You can use the following command to start ZStack Cloud service:

```
[root@localhost ~]#zstack-ctl start #Starts the management node and
 the UI service.
```

4. You can use the `zstack-ctl status` command to check the status of the management node services of ZStack Cloud:

```
[root@10-0-5-87 ~]# zstack-ctl status
ZSTACK_HOME: /usr/local/zstack/apache-tomcat/webapps/zstack
zstack.properties: /usr/local/zstack/apache-tomcat/webapps/zstack/
WEB-INF/classes/zstack.properties
log4j2.xml: /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/
classes/log4j2.xml
PID file: /usr/local/zstack/management-server.pid
log file: /usr/local/zstack/apache-tomcat/logs/management-server.log
version: 4.3.12 (ZStack-enterprise 4.3.12)
MN status: Running [PID:123135]
UI status: Running [PID:795] http://10.0.0.254:5000
```

5. You can use the `zstack-ctl ui_status` command to check the UI status:

```
[root@172-20-12-20 ~]# zstack-ctl ui_status
UI status: Running [PID:8459] http://10.0.0.254:5000
```

6. If you need to restart management node services but not the UI service, run the following command:

```
zstack-ctl restart_node
```

7. We recommend that you do not stop and then restart all services while using ZStack Cloud. If you do need to restart all services, run the following command:

```
zstack-ctl stop && zstack-ctl start
```

4.4 Upgrade ZStack Cloud

The upgrading process of ZStack Cloud ISO of the c74 edition is the same as the upgrading process of ISO of the c76 edition. This topic takes c76 ISO as an example to describe the upgrading process.

- Before you upgrade ZStack Cloud, make sure that the management node and compute nodes install an operating system (OS) of the c76 edition. Then you can upgrade the management node to c76 OS of the latest version.
- You only need to upgrade the management node. After you complete the management node upgrading, the upgrading of the compute nodes is automatically completed.
- Before you upgrade ZStack Cloud, you need to back up the database as the admin.

- During the upgrading, the UI platform and command line interface of the management node is inaccessible. However, the services of running VM instances are not affected.
- After the upgrading is completed, you need to clean up the browser cache or refresh the UI platform of the management node.

ZStack Cloud provides **incremental upgrading** and **offline upgrading** methods.

Incremental Upgrading

Incremental upgrading allows better user experience.

Offline upgrading requires you to download ISO of the version you need, upgrade the local repo, and then upgrade ZStack Cloud. Compared with **offline upgrading**, **incremental upgrading** only requires you to download the ZStack Cloud installation package of the latest version and then implement upgrading and installation. Then the installation package will automatically check the ISO version.

1. Before you implement ZStack Cloud online upgrading as the admin, you need to prepare the following installation package. We recommend that you save the installation package or script in the `/root/` directory.
   - ZStack Cloud installation package:
     - Software: ZStack-Cloud-installer-4.3.12.bin
     - Download address: *Click here*
2. Before you upgrade as the admin, you need to back up the database.
   - Run the following command to back up the database:

     ```
     [root@zstack-1 ~]# zstack-ctl dump_mysql --file-name zstack-mysql-before-upgrade
     ```

     Note:

     - After you run the command, a database backup is created in the `/var/lib/zstack/mysql-backup/` directory.
     - During the upgrading, ZStack Cloud proxy server is upgraded. Data stored on the primary storage and backup storage is not affected.
   - You can also use Backup Service of ZStack Cloud to implement scheduled backup of the database.

Note:

- Backup Service is provided in an independent module. You need to purchase the Backup Service Plus License, in addition to the Base License.

3. Run the following command as the admin to upgrade the management service of ZStack Cloud:

```
[root@zstack-1 opt]# bash ZStack-Cloud-installer-4.3.12.bin -u
```

Note:

- You can use the preceding command if the root password of the database is the default password **zstack.mysql.password**.
- If the root password of the database is a custom non-empty password, run the following command:

```
[root@zstack-1 opt]# bash ZStack-Cloud-installer-4.3.12.bin -u -P
 MYSQL_ROOT_PASSWORD
```

4. During the upgrading and installation, the installation package automatically checks the ISO version:
   - If the ISO version is detected too old, the local repo is automatically sync to the latest and then ZStack Cloud is to be installed.
   - If errors occur during local repo sync, you are prompted to use the offline upgrading method.

Note:

- Incremental upgrading must be implemented **online**.
- Incremental upgrading allows for seamless upgrading of ZStack Cloud to the latest version.

Offline Upgrading

1. Before you implement ZStack Cloud offline upgrading as the admin, you need to prepare the following installation package. We recommend that you save the installation package or script in the `/root/` directory.
   - ZStack Cloud custom ISO:
     - C76: ZStack-Cloud-x86_64-DVD-4.3.12-c76.iso
     - C74: ZStack-Cloud-x86_64-DVD-4.3.12-c74.iso

— Download address: *Click here*

- Upgrading Script

  — Software: ZStack-upgrade

  — Download address: *Click here*

> **Note:**
> The version of the upgrading version must be consistent with the ISO and bin version.

> **Note:**
> After the software packages are installed, you need to use a MD5 checker to check whether the MD5 hash of the packages is consistent with the officially released packages.

2. Before you upgrade as the admin, you need to back up the database.

   - Run the following command to back up the database:

```
[root@zstack-1 ~]# zstack-ctl dump_mysql --file-name zstack-mysql-
before-upgrade
```

> **Note:**
> - After you run the command, a database backup is created in the *`/var/lib/zstack/mysql-backup/`* directory.
> - During the upgrading, ZStack Cloud proxy server is upgraded. Data stored on the primary storage and backup storage is not affected.

   - You can also use Backup Service of ZStack Cloud to implement scheduled backup of the database.

> **Note:**
> - Backup Service is provided in an independent module. You need to purchase the Backup Service Plus License, in addition to the Base License.

3. Run the following command as the admin to upgrade the management service of ZStack Cloud:

```
#You can use the either of the following method to implement offline
 upgrading:
# 1. Upgrade the local repo and management service:
[root@zstack-1 opt]# bash zstack-upgrade ZStack-Cloud-x86_64-
DVD-4.3.12-c76.iso
# 2. Upgrade the local repo first and then the management service:
```

```
[root@zstack-1 opt]# bash zstack-upgrade -r ZStack-Cloud-x86_64-
DVD-4.3.12-c76.iso
[root@zstack-1 opt]# bash ZStack-Cloud-installer-4.3.12.bin -u
```

Note:

- You can use the preceding command if the root password of the database is the default password **zstack.mysql.password**.
- If the root password of the database is a custom non-empty password, run the following command:

```
#You can use the either of the following method to implement
 offline upgrading:
# 1. Upgrade the local repo and management service:
[root@zstack-1 opt]# bash zstack-upgrade ZStack-Cloud-x86_64-
DVD-4.3.12-c76.iso
# 2. Upgrade the local repo first and then the management
 service:
[root@zstack-1 opt]# bash zstack-upgrade -r ZStack-Cloud-x86_64-
DVD-4.3.12-c76.iso
[root@zstack-1 opt]# bash ZStack-Cloud-installer-4.3.12.bin -u -P
 MYSQL_ROOT_PASSWORD
```

- Before you run the zstack**-upgrade** command, make sure that you use ISO of the c76 edition instead of the c74 edition.

Considerations

The following lists the considerations that you need to take when you upgrade the Cloud to different versions. For any questions or assistance, contact our official technical support.

- Starting from ZStack Cloud 4.3.12, the QEMU version is automatically upgraded from 2.12 to 4.2.
  - If you deploy a new Cloud by using the ISO of 4.3.12 or a later version, QEMU 4.2 is installed by default. If you upgrade your Cloud to 4.3.12 or a later version, QEMU 2.12 is used by default.
  - To use the Cloud properly, make ensure that all hosts in the same cluster use the same QEMU version. Therefore, if you upgrade your Cloud to 4.3.12 or a later version, you could not expand the capacity by adding hosts (installed using the ISO of 4.3.12 or a later version) to the existing cluster. To expand the capacity, use a new cluster.
- Starting from ZStack Cloud 4.0.0, we bring you the following enhancements:
  - vRouter is upgraded to VPC vRouter.

Starting from 4.0.0, vRouter is upgraded to VPC vRouter and vRouter network is upgraded to VPC network. vRouter is no longer available on the UI. The seamless upgrade does not affect your business continuity.

- User Group and User are replaced by Enterprise Management Account System.

  Starting from 4.0.0, User Group and User are replaced by Enterprise Management Account System. User Group and User are no longer available on the UI. You cannot login to the Cloud by using a user or user group account. Before you implement upgrading, migrate the user and user group account data to Enterprise Management.

  Note:
  User accounts created by the admin and have the admin permissions are also cancelled. Platform admins in Enterprise Management have the equivalent permissions. You can use Enterprise Management to create platform managers based on your business needs.

- The integration of AD/LDAP and accounts is adjusted.

  Starting from 4.0.0, the integration of AD/LDAP and accounts is managed by Enterprise Management. Before you implement upgrading, migrate the AD/LDAP account data managed by the original account system to Enterprise Management.

- Starting from ZStack Cloud 3.9.0, if you use c74 ISO and QEMU 2.9, the libvirt version is automatically upgraded to 4.9.0.
  - If you use open-source Ceph distributed storage and enable the CEPHX (Ceph authentication) feature, when you hot-plug VM CD-ROM, an error may occur because libvirt of the new version does not support hot plugging. You can contact the official technical support when necessary.
  - Starting from 3.2.0, libvirt updates the format of shared volumes to raw. Therefore, when you create a shared volume, the format of the volume is raw. This type of volume does not allow you to create snapshots and resize capacities, or create images for powered-on VM instances to which this type of volume is attached. In later versions of ZStack Cloud, these limitations will be eliminated.
  - The libvirt auto-upgrading feature is enabled by default. You can disable the feature by using the following method:

Enter `/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/` and set the following parameter in the **zstack.properties** configuration file:

```
updatePkgWhenConnect = false
# Disable libvirt auto-upgrading.
```

Restart the management node to make the modification take effect.

- Starting from ZStack Cloud 3.7.1, ISO of the c76 and c74 editions are available and multiple repos are supported. When you upgrade the cloud platform, note that:
  - Starting from 3.7.1, ISO of the c72 edition is no longer used for installation and deployment of the new cloud platform. If you need to expand the capacity or upgrade the operating system, contact the official technical support for help.
  - Starting from 3.7.1, the local repo of ISO of the c72 edition is redirected to ISO of the c74 edition. If you use offline upgrading, you need to obtain ISO of the c74 edition to update the local repo.

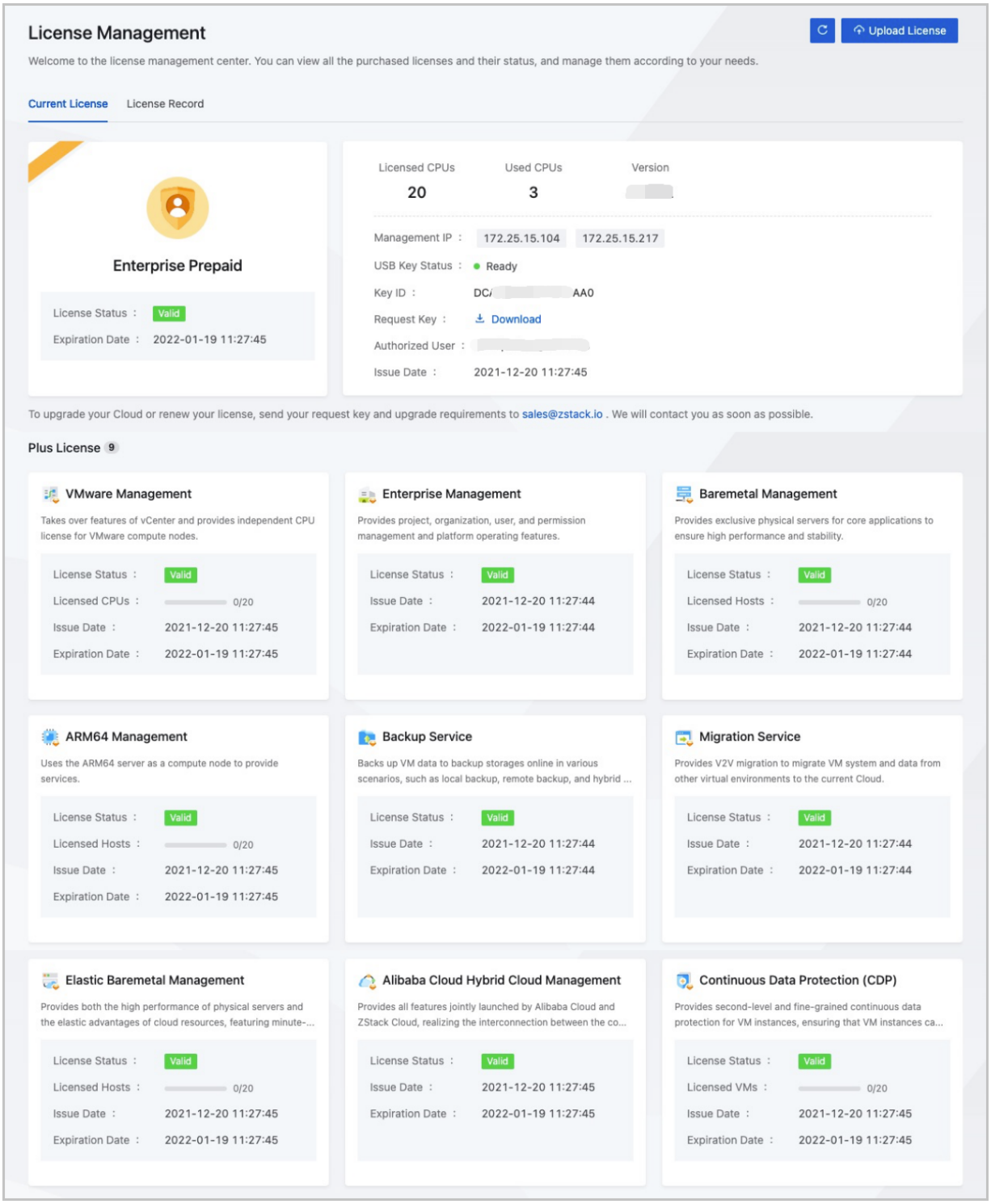
5 License Management

5.1 What is License?

The **License Management** page displays the licensing information such as the licensing mechanism, Cloud version, and license status.

On the ZStack Cloud main menu, click the profile icon and choose **License Management**. Then, the **License Management** page is displayed.

Figure 5-1: License Management



Licensing Mechanism

Licensing in ZStack Cloud is supplied in different functionality packages as Base and Plus.

- **Base License**

- Provides the basic and essential features of the Cloud, which can meet the mainstream business requirements.
- Covered functionalities: **Basic**, **Standard**, **Enterprise Trial**, and **Enterprise Prepaid**. For more detailed information about these editions, see *Edition Comparison*.

- **Plus License**
  - Provides add-on features or feature enhancements to meet the specific business requirements.
  - Covered functionalities: VMware Management, Enterprise Management, ARM64 Management, Backup Service, Continuous Data Protection (CDP) Service, Migration Service, Baremetal Management, Elastic Baremetal Management, Alibaba Cloud Hybrid Cloud Management, 5x8 (7x24) After-Sales Service, SR-IOV NIC Service, GPU Service, Billing Management, CloudFormation, Auto-Scaling Service, and Smart NIC Service.
  - A Base license is required to install the Plus license.

The licensing mechanism is detailed as follows.

Table 5-1: Licensing Mechanism

Licensing Mechanism	Functionality Covered	Description
/	Community	Provides a simple, ease-of-use, and productized private cloud platform with diversified features for community users. • Free of use. • Number of compute nodes: not limited. • Validity: perpetual. • Applicable features: part of the Cloud. • No after-sales technical support. • Not recommended in production environments.
Base License	Basic	Provides a lightweight, ease-of-use, and enterprise-level virtualization platform to meet customers' needs for unified management of virtualized resources. • Features are available after you purchase the Base license . • The number of compute nodes that you can manage is calculated by the number of physical CPUs you purchased. • Provides the basic and essential features of the Cloud within the licensed period.

Licensing Mechanism	Functionality Covered	Description
		• Add-on features are not available. • Provides official after-sales technical support within the specified period. • Applicable to product environments.
	Standard	Provides a full set of computing, storage, and network virtualization features. This helps to meet the various and flexible business requirements. • Features are available after you purchase the Base license . • The number of compute nodes that you can manage is calculated by the number of physical CPUs you purchased. • Provides a full set of computing virtualization, storage virtualization, and network virtualization features of the Cloud within the licensed period. • Allows you to purchase and use add-on features within the licensed period as needed. • Provides official after-sales technical support within the specified period. • Applicable to product environments.
	Enterprise Trial	Provides a full set of computing, storage, and network virtualization features, and enhanced features such as GPU, CloudFormation, and auto-scaling. This helps to meet the various and flexible business requirements. • 1-year free trial. • Provides one host for free. • Provides the basic and essential features of the Cloud within the licensed period. • Provides all add-on features within the licensed period. • No after-sales technical support. • Applicable to test environments.
	Enterprise Prepaid	Provides a full set of computing, storage, and network virtualization features, and enhanced features such GPU, CloudFormation, and as auto-scaling. This helps to meet the various and flexible business requirements. • Features are available after you purchase the Base license .

Licensing Mechanism	Functionality Covered	Description
		• The number of compute nodes that you can manage is calculated by the number of physical CPUs you purchased. • Provides the basic and essential features of the Cloud within the licensed period. • Allows you to purchase and use add-on features within the licensed period as needed. • Provides official after-sales technical support within the specified period. • Applicable to product environments.
Plus License	VMware Management	Manages all the features of vCenter and provides an independent CPU license for VMware compute nodes. • Features are available after you purchase the Plus license. • The Base license is required to install the Plus license. • If the independent license is not issued or the licensed quota exceeds, the KVM-licensed CPUs will be used. • Provides official after-sales technical support within the specified period.
	Enterprise Management	Provides the full functionalities of Enterprise Management, such as project management, organizational structure, users, permissions, and Cloud operations, during the licensed period . • Features are available after you purchase the Plus license. • The Base license is required to install the Plus license. • Provides official after-sales technical support within the specified period.
	ARM64 Management	Provides a specified number of ARM hosts within the licensed period, and provides stable support for ARM64 servers. • Features are available after you purchase the Plus license. • The Base license is required to install the Plus license. • Provides official after-sales technical support within the specified period.
	Backup Service	Backs up VM data to backup storages online in various scenarios, such as local backup, remote backup, and hybrid cloud backup. This enhances the data reliability. • Features are available after you purchase the Plus license. • The Base license is required to install the Plus license.

Licensing Mechanism	Functionality Covered	Description
		• Provides official after-sales technical support within the specified period.
	Continuous Data Protection (CDP) Service	Provides second-level and fine-grained continuous data protection for VM instances, ensuring that VM instances can quickly recover when a failure occurs. • Features are available after you purchase the Plus license. • The Base license is required to install the Plus license. • Provides official after-sales technical support within the specified period.
	Migration Service	Provides V2V migration to migrate VM system and data from other virtual environments to the current Cloud. • Features are available after you purchase the Plus license. • The Base license is required to install the Plus license. • Provides official after-sales technical support within the specified period.
	Baremetal Management	Provides a specified number of dedicated physical servers within the licensed period to ensure the high performance and stability of core applications. • Features are available after you purchase the Plus license. • The Base license is required to install the Plus license. • Provides official after-sales technical support within the specified period.
	Elastic Baremetal Management	Provides the license for managing specified number of flexible physical servers during the licensed period, improving the ease of use and flexibility in addition to ensuring the high performance and stability of physical servers. • Features are available after you purchase the Plus license. • The Base license is required to install the Plus license. • Provides official after-sales technical support within the specified period.
	Alibaba Cloud Hybrid Cloud Management	Provides all features of Alibaba Cloud Hybrid Cloud Management, realizing the interconnection between the control plane and the data plane. • Features are available after you purchase the Plus license. • The Base license is required to install the Plus license.

Licensing Mechanism	Functionality Covered	Description
		• Provides official after-sales technical support within the specified period.
	5x8 (7x24) After-Sales Service	Provides official 5x8 or 7x24 after-sales technical support within the specified period. • Features are available after you purchase the Plus license. • The Base license is required to install the Plus license.
	SR-IOV NIC Service	Allows you to generate VF NICs from physical NICs based on the SR-IOV specification and allocate these VF NICs to VM instances. This provides VM instances strong I/O performance comparable to that of physical NICs. • Features are available after you purchase the Plus license. • Provided in the Enterprise Base license by default. • A Standard Base license is required to install the Plus license. • Provides official after-sales technical support within the specified period.
	GPU Service	Allows you to passthrough a physical GPU (pGPU) to VM instances or divide a pGPU into multiple virtual GPUs (vGPUs) and distribute the vGPUs to VM instances. This empowers VM instances with strong computing capabilities of physical GPUs. • Features are available after you purchase the Plus license. • Provided in the Enterprise Base license by default. • A Standard Base license is required to install the Plus license. • Provides official after-sales technical support within the specified period.
	Billing Management	Provides billing methods like that of the public cloud, uses pricing lists to manage billing of resources of various unit prices, and offer bill services to the admin and tenants based on the pricing lists. • Features are available after you purchase the Plus license. • Provided in the Enterprise Base license by default. • A Standard Base license is required to install the Plus license.

Licensing Mechanism	Functionality Covered	Description
		• Provides official after-sales technical support within the specified period.
	CloudFormation	Uses stack templates to batch deploy and configure resources and manage the lifecycle of the resources. In addition, offers designers that allow efficient orchestration of cloud resources. • Features are available after you purchase the Plus license. • Provided in the Enterprise Base license by default. • A Standard Base license is required to install the Plus license. • Provides official after-sales technical support within the specified period.
	Auto-Scaling Service	Allows automatic scale-in or scale-out of VM instances based on the load balancing result of application workloads, thereby improving resource utilization, lowering maintenance costs, and securing stable business operations. • Features are available after you purchase the Plus license. • Provided in the Enterprise Base license by default. • A Standard Base license is required to install the Plus license. • Provides official after-sales technical support within the specified period.
	Smart NIC Service	Allows you to use smart NICs to free more computing powers of physical CPUs and improve network performance. In addition, allows you to divide a smart NIC into multiple vDPA NICs and distribute the vDPA NICs to VM instances, thereby empowering the VM instances with high I/O performance like that of smart NICs. • Features are available after you purchase the Plus license. • Provided in the Enterprise Base license by default. • A Standard Base license is required to install the Plus license. • Provides official after-sales technical support within the specified period.

Note:

- For more details, contact us by sending emails to **sales@zstack.io**.
- To obtain a trial, or to purchase or upgrade your ZStack Cloud license, send your key ID or request key with your requirements to **sales@zstack.io**. We will contact you as soon as possible.

Licensing Method

ZStack Cloud supports two licensing methods: USB key and request key.

- **Licensing by USB Key**
  - You can obtain the authorization by inserting only one USB key into the management node.
  - If you are using a dual-MN environment, insert only one USB key.
  - The Plus licenses authorized by an USB Key cannot be deleted.
- **Licensing by Request Key**
  - You can obtain the authorization by uploading the license file to the management node.
  - You can upload both the Base license and Plus license at the same time by using a tar.gz package.
  - If you are using a dual-MN environment, we recommend that you upload the license file on the management node where the virtual IP address is located.

5.2 Install a License

The admin can install a license by using an USB key or a request key. These two methods are detailed in the following topics.

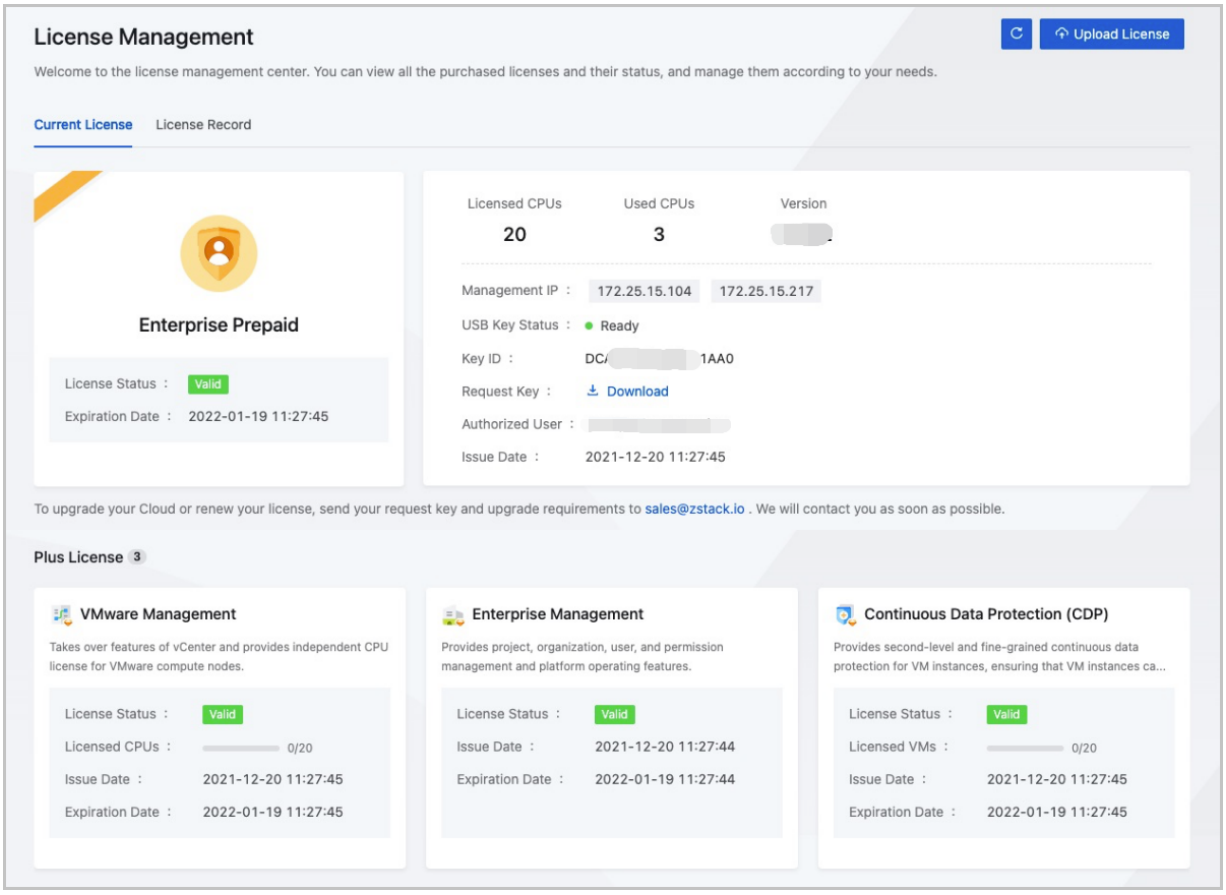
5.2.1 Install a License by Using an USB Key

To install a license by using an USB key, follow these steps:

1. Insert the USB key into the management node.
2. Refresh the UI.

   On the **License Management** page, click the **refresh** button on the left of **Upload License**.
3. Then, you can see the whole licensing information.

Figure 5-2: Licensing Information



Note:

- You can update your license by using the key ID or request ID.
- The Plus licenses authorized by an USB Key cannot be deleted.
- If you are using a dual-MN environment, note that:
  - You can obtain the authorization by inserting only one USB key into the management node.
  - If the node with the USB key inserted is faulty, we recommend that you remove the USB key and insert it into another healthy node to ensure the business continuity.

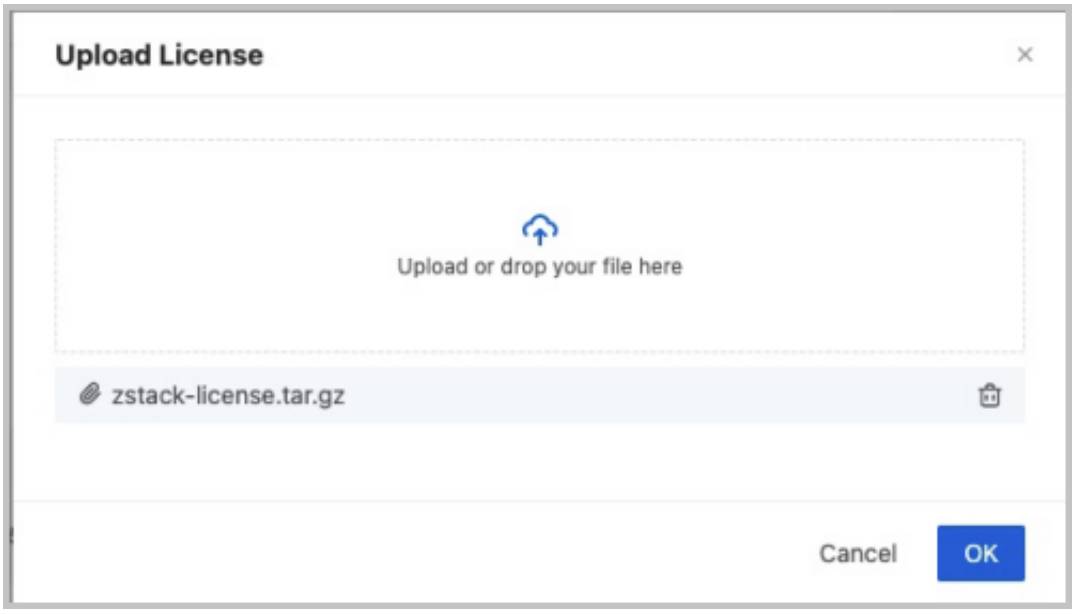
5.2.2 Install a License by Using a Request Key

To install a license by using a request key, follow one of the methods:

Install the License on the UI

On the **License Management** page, click **Upload License** in the upper right corner. On the displayed **Upload License** page, upload the obtained license.

Figure 5-3: Upload License



Note:

- You can update your license by using the key ID or request ID.
- You can upload both the Base license and Plus license at the same time by using a tar.gz package or a .txt file.
- If you are using a dual-MN environment, we recommend that you download the request key and upload the license file on the management node where the virtual IP address is located. Then, the licensing information on both nodes can be updated.
- You can re-load the license by clicking the **refresh** button on the **License Management** page.
- Only the admin has the permission to load or delete licenses. Note that the Base license cannot be deleted.

Install the License by Using Command Line Tool

1. Import the license by using a command line tool.

```
[root@localhost ~]# zstack-ctl install_license -f zstack-
license.tar.gz
```

2. Refresh the license.

   Re-load the license by using the following commands:

```
[root@localhost ~]# zstack-cli

  ZStack command line tool
  Type "help" for more information
```

```
  Type Tab key for auto-completion
  Type "quit" or "exit" or Ctrl-d to exit

>>>LogInByAccount accountName=admin password=password
{
    "inventory": {
        "accountUuid": "36c27e8ff05c4780bf6d2fa65700f22e",
        "createDate": "May 25, 2016 8:12:54 PM",
        "expiredDate": "May 25, 2016 10:12:54 PM",
        "userUuid": "36c27e8ff05c4780bf6d2fa65700f22e",
        "uuid": "d505bde1bcce46cb9c79774440654f42"
    },
    "success": true
}

>>>ReloadLicense
```

The method to install a license for a multi-node environment is the same as the method described above.

5.3 Manage a License

On the main menu of ZStack Cloud, choose **Personal Center** > **License Management**. Then, the **License Management** page is displayed.

The following table lists the actions that you can perform on a license.

Action	Description
Upload License	Upload a license. **Note:** • If you installed a license by using an USB key, you can upload both the Base license and Plus license at the same time by using a .txt file. • If you installed a license by using a request key, you can upload both the Base license and Plus license at the same time by using a tar.gz package. • If you are using a dual-MN environment, we recommend that you download the request key and upload the license on the management node where the virtual IP is located. Then, the licensing information on both nodes can be updated. • You can click the refresh button in the upper right corner of the **License Management** page to reload the license. • Only the admin has the permission to load or delete licenses. Note that the Base license cannot be deleted.
Copy Key ID	Copy the key ID required to generate a license. You can update the license by using a key ID.

Action	Description
Download Request Key	Download the request key required to generate a license. You can update the license by using a request ID.
Delete Plus License	Delete a Plus license you added to the Cloud. **Note:** The Plus licenses obtained by using an USB key cannot be deleted.

License Status

A license has the following statuses.

Status	Description
Valid	The Base License is in the valid status.
Expired	The Base License or a Plus License expired. If a Plus License expires, the corresponding features would be unavailable.

License Expiration Reminder

If an exception occurs to your license, the Cloud will remind you accordingly. The details are listed as follows.

Exception	Details
License to Expire	When the remaining license period is less than 15 days, a banner prompt will appear after you log in to the Cloud. **Note:** • You will receive a reminder when the remaining period of the 5x8 (7x24) after-sales service is less than 30 days. Please contact us for authorization update as soon as possible to obtain a complete official after-sales technical support service. • You can click **Check** in the banner prompt to go to the **License Management** page. In order not to affect your use of the Cloud, we recommend that you contact us as soon as possible for authorization update.
License Expired	When the Base License expired, you will be redirected to the **License Management** page after login. In order not to affect your use of the Cloud, we recommend that you contact us as soon as possible for authorization update.

Exception	Details
	Note: • If your Base License expired, the business on the Cloud can be still running properly. However, do not perform any operations, such as reconnecting your host, backup storage, or primary storage, so as not to affect the business continuity. • If your Plus License expired, all the features provided by the Plus License will be unavailable. For example, if your Enterprise Management Plus License expired, the project login page will be locked. • If your Base License expired, but the Plus License is still within the authorization period, you can view the relevant resources related to the Plus License, but do not operate on these resources. For example, if your **Enterprise Prepaid** Base License expired, but the Enterprise Management Plus License is still within the authorization period, you can log in to the Cloud from the project login portal, but you cannot operate on related resources.
Licensed Quota Exceeds	When you update your license, you may find that the used resources exceed the authorized quota. In this case, most features of the Cloud become unavailable. To ensure your business continuity, we recommend that you update your license to expand the capacity. The limitations and operations that you can perform are as follows: • You can log in to the Cloud and obtain, refresh, and view the status of resource. • You can reduce resource usage by for example, deleting a host, a vCenter, a cluster, or a VM instance, changing the state of a host, and expunging a VM instance. • You can manage your license, such as downloading the request key , uploading a license, and deleting a license. • You can perform no operations other than the preceding operations. **Note:** • Resource authorization by license can be delivered by using the following three methods: CPU sockets, hosts, and VM instances . If the resources usage exceeds the quota authorized by using either of the three methods, some features of the Cloud become unavailable. • If you power off the management node, the management node cannot be started. You can only login to the management node

Exception	Details
	console and update the license by using CLI. For more information, see *Install the Licensing by Using Command Line Tool*.

Figure 5-4: License to Expire

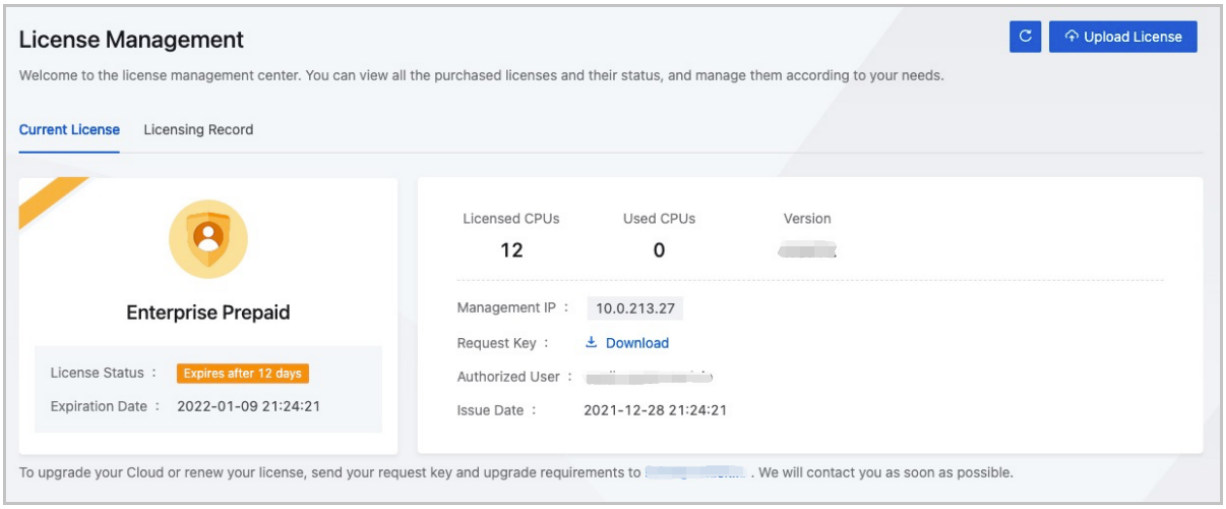
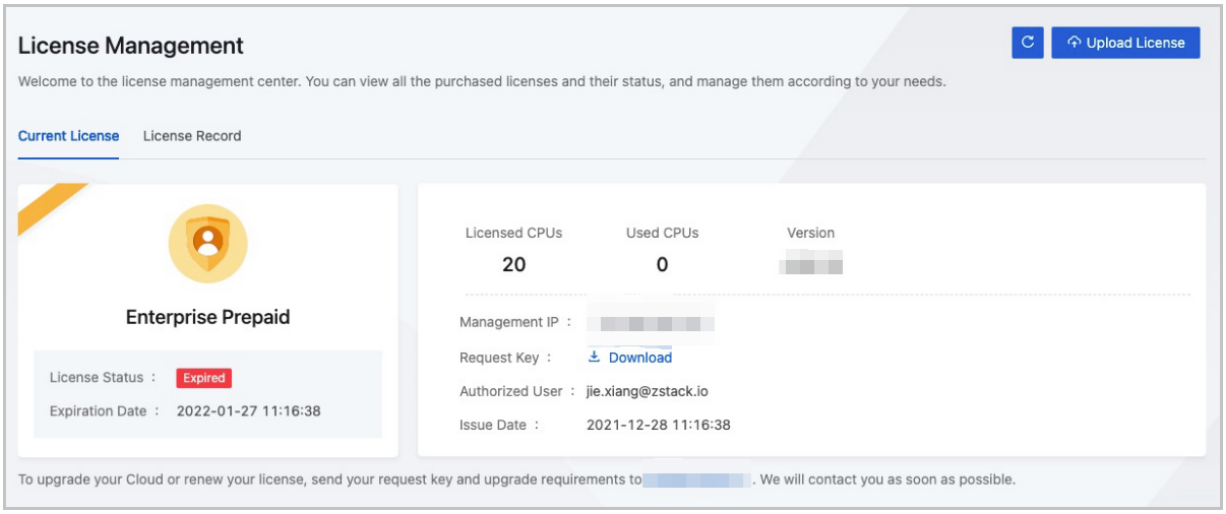


Figure 5-5: License Expired

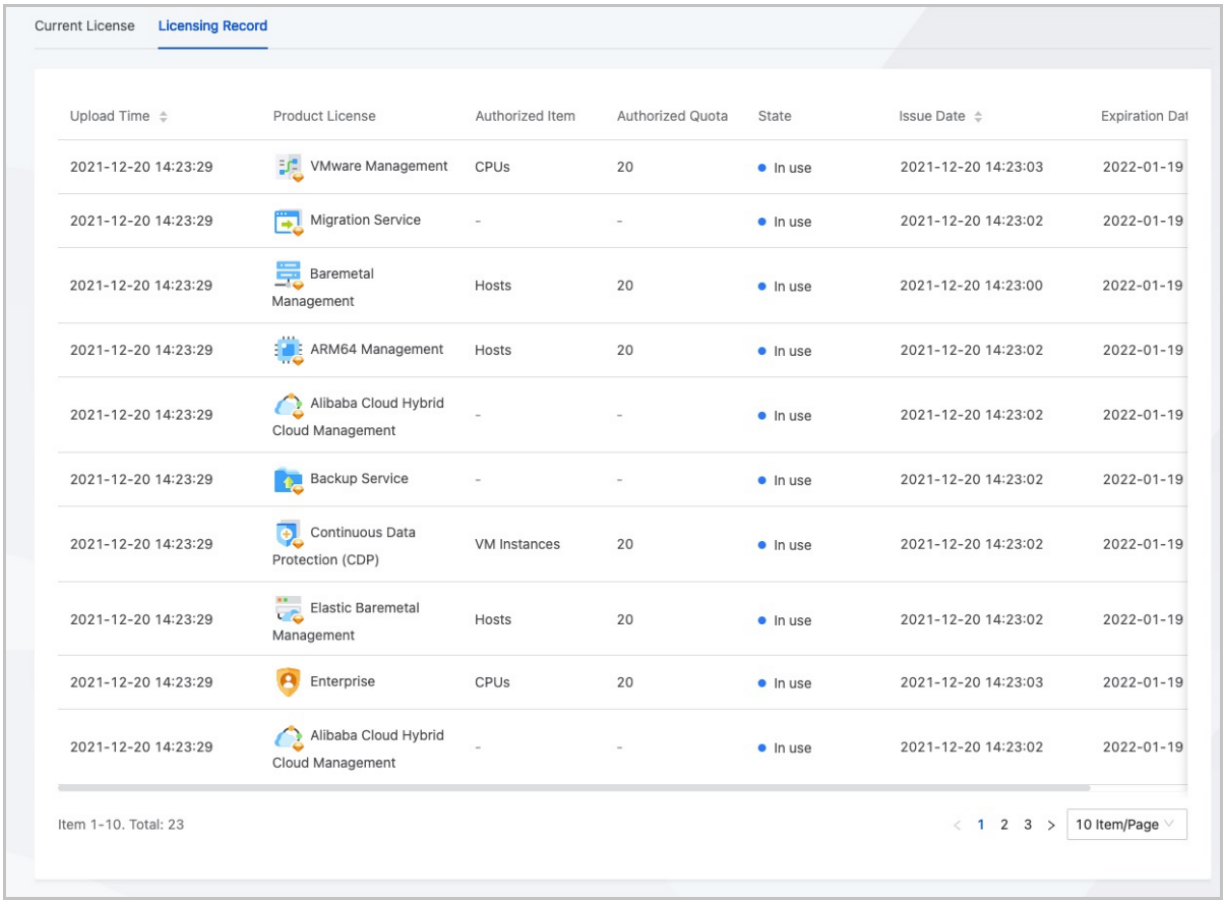


Licensing Record

On the main menu of ZStack Cloud, choose **Personal Center** > **License Management** > **Licensing Record**. Then, the **Licensing Record** page is displayed.

The admin can view the licensing records of the Cloud on the UI, including the upload time, license type, authorized items, authorized quota, state, time when the license was issued, and time when the license expires.

Figure 5-6: Licensing Record



Current License | Licensing Record

Upload Time	Product License	Authorized Item	Authorized Quota	State	Issue Date	Expiration Dat
2021-12-20 14:23:29	VMware Management	CPUs	20	In use	2021-12-20 14:23:03	2022-01-19
2021-12-20 14:23:29	Migration Service	-	-	In use	2021-12-20 14:23:02	2022-01-19
2021-12-20 14:23:29	Baremetal Management	Hosts	20	In use	2021-12-20 14:23:00	2022-01-19
2021-12-20 14:23:29	ARM64 Management	Hosts	20	In use	2021-12-20 14:23:02	2022-01-19
2021-12-20 14:23:29	Alibaba Cloud Hybrid Cloud Management	-	-	In use	2021-12-20 14:23:02	2022-01-19
2021-12-20 14:23:29	Backup Service	-	-	In use	2021-12-20 14:23:02	2022-01-19
2021-12-20 14:23:29	Continuous Data Protection (CDP)	VM Instances	20	In use	2021-12-20 14:23:02	2022-01-19
2021-12-20 14:23:29	Elastic Baremetal Management	Hosts	20	In use	2021-12-20 14:23:02	2022-01-19
2021-12-20 14:23:29	Enterprise	CPUs	20	In use	2021-12-20 14:23:03	2022-01-19
2021-12-20 14:23:29	Alibaba Cloud Hybrid Cloud Management	-	-	In use	2021-12-20 14:23:02	2022-01-19

Item 1-10. Total: 23

< 1 2 3 > 10 Item/Page

6 Initialization by Wizard

When you login to ZStack Cloud for the first time, you are directed to use the wizard provided by ZStack Cloud to setup an initialization environment.

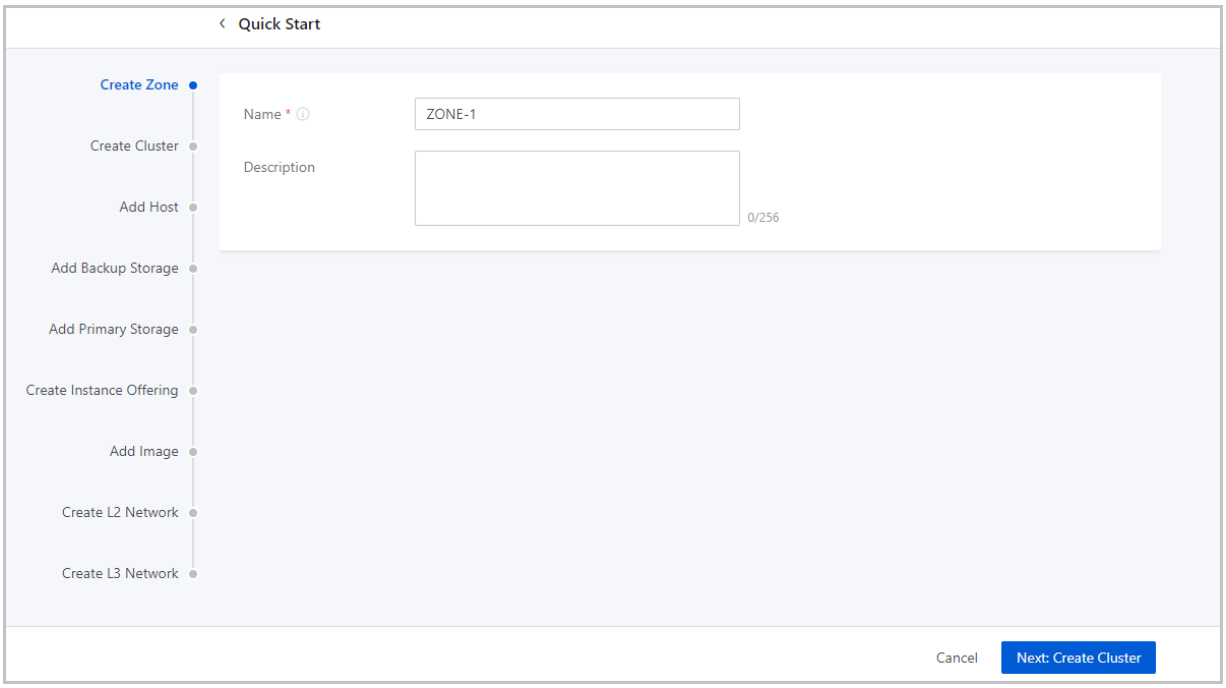
- If you stop using the wizard or delete key resources during initial setup, **you are not directed to use the wizard again**.
- We recommend that you use the wizard to complete the basic environment configurations of ZStack Cloud.

6.1 Create a Zone

Context

A zone is a logical group of resources such as clusters, L2 networks, and primary storages. Zone is the largest resource scope defined in the Cloud.

Figure 6-1: Create Zone



On the displayed page, set the following parameters:

- **Name**: Enter a name for the zone.
- **Description**: Optional. Enter a description for the zone.

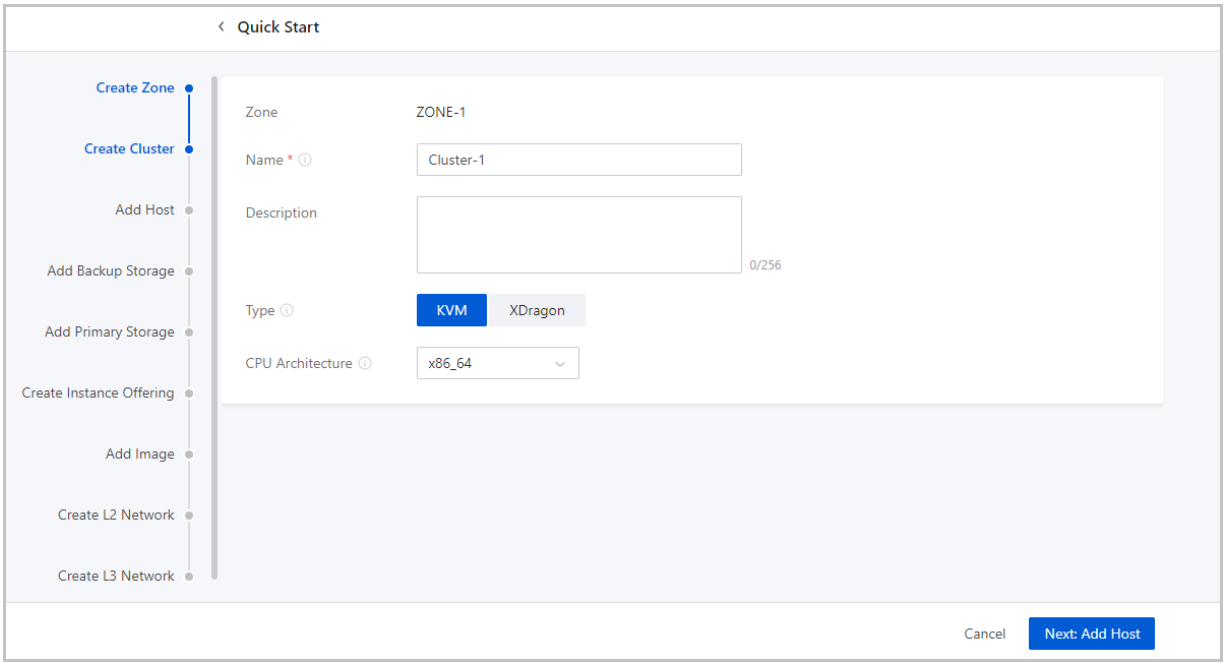
Click **Next** to complete the creation of the zone.

6.2 Create a Cluster

Context

A cluster is a logical group of hosts (compute nodes).

Figure 6-2: Create Cluster



On the displayed page, set the following parameters:

- **Name**: Enter a name for the cluster.
- **Description**: Optional. Enter a description for the cluster.
- **Type**: Optional. Select a hypervisor type for the server. Valid values: KVM and XDragon.
- **CPU Architecture**: Optional. Set the CPU architecture of the hosts in the cluster. If left blank, when you add the first host to the cluster, the CPU architecture of the hosts that you later add to the cluster must be the same as the architecture of this host. You cannot change the CPU architecture of the cluster any more.

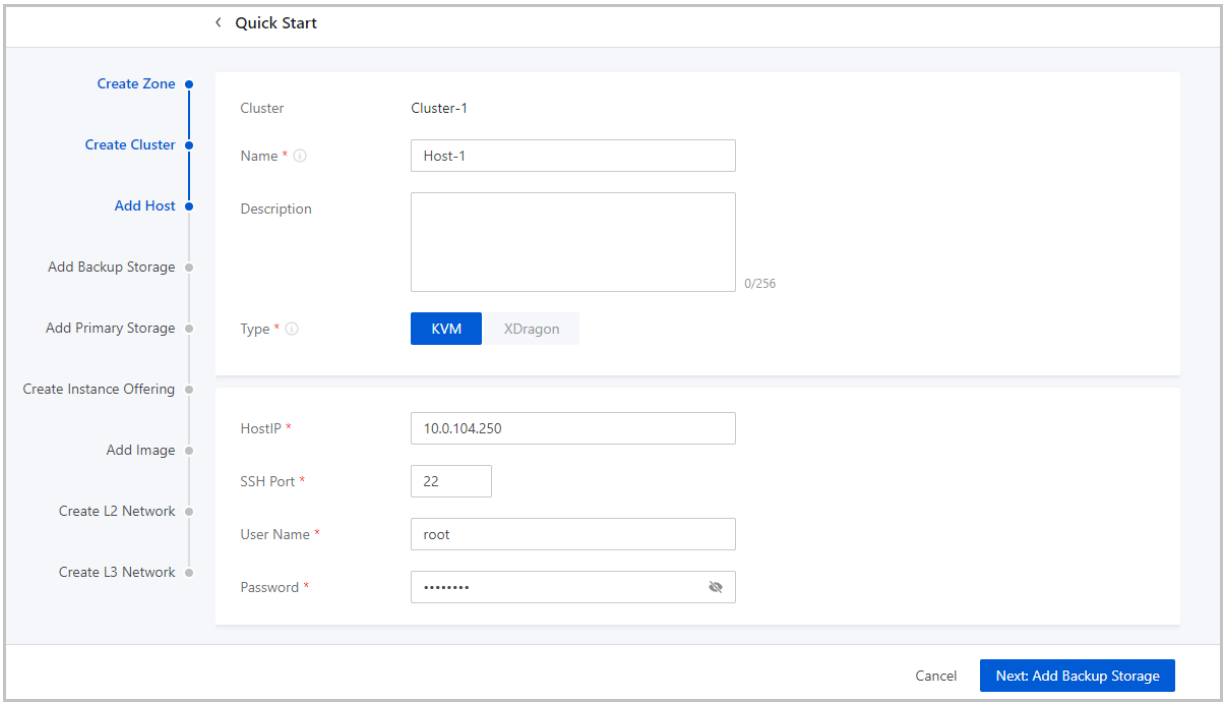
Click **Next** to complete the creation of the cluster.

6.3 Add a Host

Context

A host provides compute, network, and storage resources for VM instances.

Figure 6-3: Add Host



On the displayed page, set the following parameters:

- **Name**: Enter a name for the host.
- **Description**: Optional. Enter a description for the host.
- **Type**: Select a hypervisor type for the server. Valid values: KVM and XDragon.
- **Host IP**: Enter an IP address for the host, for example, *172.20.14.32*.

  — In the production environment, for stability and security concerns, we recommend that you separate the management network from the public network so that the management nodes and compute nodes reside in independent networks and have independent IP addresses.

  For example, if you use eth0 to connect a management network, ZStack Cloud uses the management network to communicate with compute nodes. If you use eth1 to connect to a public network, you can use the top aggregation switch to interconnect with the Internet.

  — The separation of the management network and public network can maximize system security and ensure sufficient bandwidth for the management network.
- **SSH Port**: Enter an SSH port for the host. Default: 22. If you do not specify an SSH port for the host, the system uses port 22 as the SSH port.
- **User Name**: Enter a username that has the sudo permission for the host.

  — If you specify a normal user, the user must have the sudo permission.

- We recommend that you use the **`adduser`** command to create a normal user.

  The following script shows how to create a normal user and grant the user the sudo permission.

  ```
  #Create a normal user named test
  [root@localhost ~]# adduser test
  #Grant the user the sudo permission
  [root@localhost ~]# echo "test    ALL=(ALL)    NOPASSWD: ALL" >>/
  etc/sudoers
  ```

- **Password**: Enter a password for the user. Note the password is case sensitive.

Click **Next** and ZStack Cloud will call the backend to configure the host.

- The configuration process may last several minutes.
- Error messages are prompted if errors occur.

What's next

After you complete the wizard, if you want to add more hosts to the same cluster as you set in the wizard, you must configure the same CentOS system, SSH port, username, and password for the hosts.

6.4 Add a Backup Storage

A backup storage is one or more servers that store VM image templates, including ISO image files .

You can add the following types of backup storages:

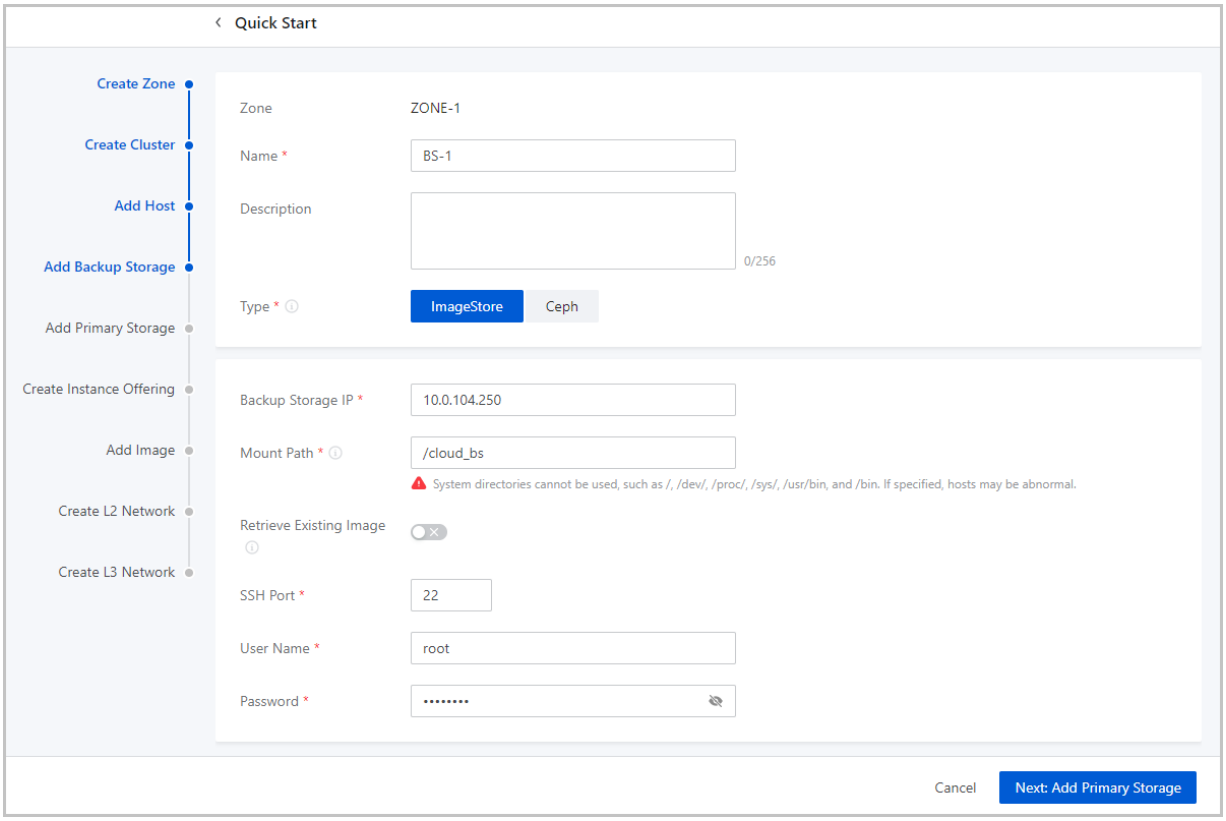
- **ImageStore**: stores images in the format of chips and supports incremental storage.
- **Sftp**: stores images in the format of files.
- **Ceph**: stores images in the format of distributed blocks.

Configure a backup storage based on your business needs.

6.4.1 ImageStore

Context

Figure 6-4: Add ImageStore Backup Storage



On the displayed page, set the following parameters:

- **Name**: Enter a name for the backup storage.
- **Description**: Optional. Enter a description for the backup storage.
- **Type**: Select ImageStore.
- **Backup Storage IP**: Enter a backup storage IP.
  - In the production environment, for the concerns of security and stability concerns, we recommend that you separate the management network from the public network.
  - You can assign a management network IP address to the backup storage and save public network bandwidth.
  - If the public network has ten-gigabits of bandwidth, you can assign a public network IP address to the backup storage. This increases the image transmission rate between the backup storage and compute nodes.

    In most cases, adding or saving an image consumes large amounts of bandwidth. If you assign a public network IP address to the backup storage, we recommend that you add or save an image during network idle time.

— You can set a dedicated storage network if necessary.

- **Mount Path**: Specify a path on the backup storage that corresponds to sufficient storage space, for example, `/ImageStore_bs`.
- **Retrieve Existing Image**: Choose whether to retrieve images stored in the specified path.
- **SSH Port**: Enter an SSH port for the backup storage. Default: 22. If you do not specify an SSH port for the backup storage, the system uses port 22 as the SSH port.
- **User Name**: Enter a username. By default, root user is used. You can also specify a normal user.

  — If you do not specify a normal user for the backup storage, the root user is used.

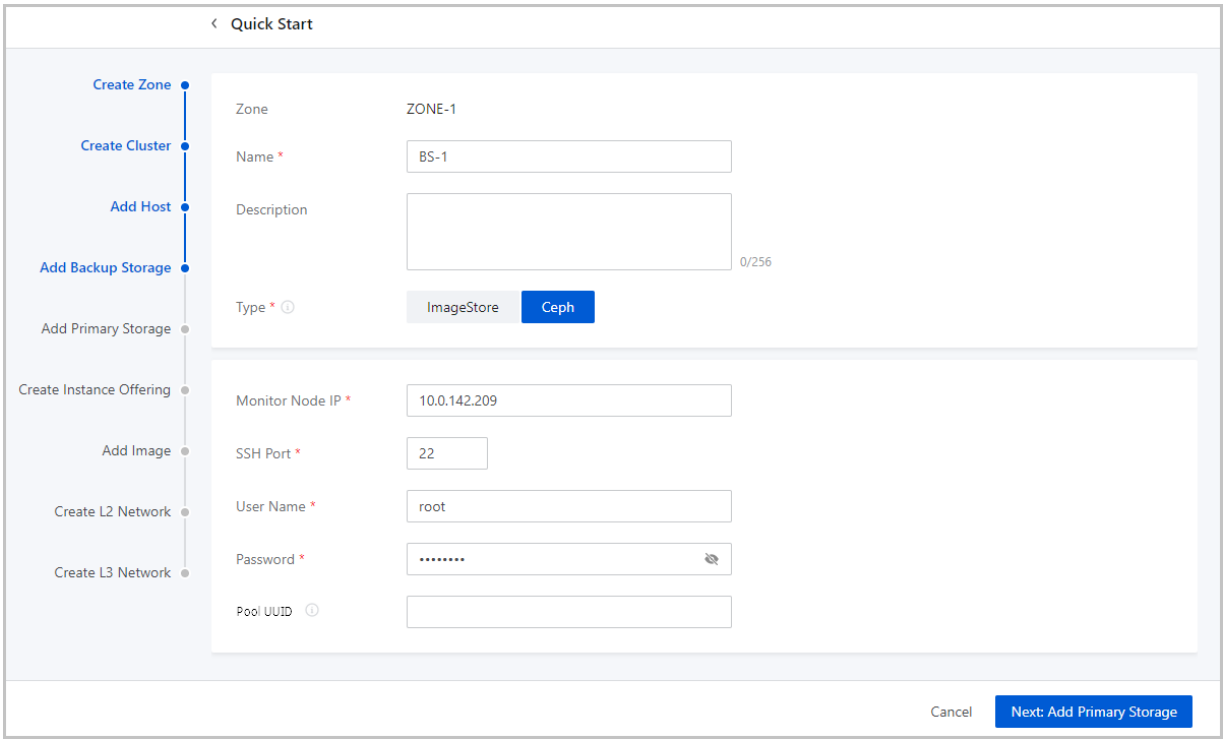
  — If you specify a normal user, the user must have the sudo permission.
- **Password**: Enter a password for the user. Note the password is case sensitive.

Click **Next** and ZStack Cloud will configure the ImageStore backup storage.

6.4.2 Ceph

Context

Figure 6-5: Add Ceph Backup Storage



On the displayed page, set the following parameters:

- **Name**: Enter a name for the backup storage.
- **Description**: Optional. Enter a description for the backup storage.
- **Type**: Select Ceph.
- **Monitor Node IP**: Enter the IP address of the Ceph monitor node.
- **SSH Port**: Enter an SSH port for the monitor node. Default: 22. If you do not specify an SSH port for the monitor node, the system uses port 22 as the SSH port.
- **User Name**: Enter a username. By default, root user is used. You can also specify a normal user.
  - If you do not specify a normal user for the backup storage, the root user is used.
  - If you specify a normal user, the user must have the sudo permission.
- **Password**: Enter a password for the user. Note the password is case sensitive.
- **Pool UUID**: Optional. Specify a storage pool for the Ceph backup storage.
  - Before you specify a pool, you need to create a pool in the Ceph storage cluster.
  - If left blank, a storage pool is created automatically.

Click **Next** and ZStack Cloud will configure the Ceph backup storage.

6.5 Add a Primary Storage

A primary storage is one or more servers that store volume files of VM instances. These files include root volume snapshots, data volume snapshots, image caches, root volumes, and data volumes.

In the wizard, you can add the following types of primary storage:

- **LocalStorage**: uses the disks of the host for storage.
- **Network Sharing Storage**: supports NFS, Shared Mount Point, and Ceph.
  - NFS allows you to store files by using the NFS protocol.
  - Shared Mount Point provides network sharing storage by using popular distributed file systems including MooseFS, GlusterFS, OCFS2, and GFS2.
  - Ceph stores files in the format of distributed blocks.

Note:

The type of primary storage is associated with the type of backup storage:

- If you use ImageStore backup storage, you can use a primary storage of the LocalStorage, NFS, Share Mount Point, or Ceph type.
- If you use a Ceph backup storage, you can use only Ceph primary storage.

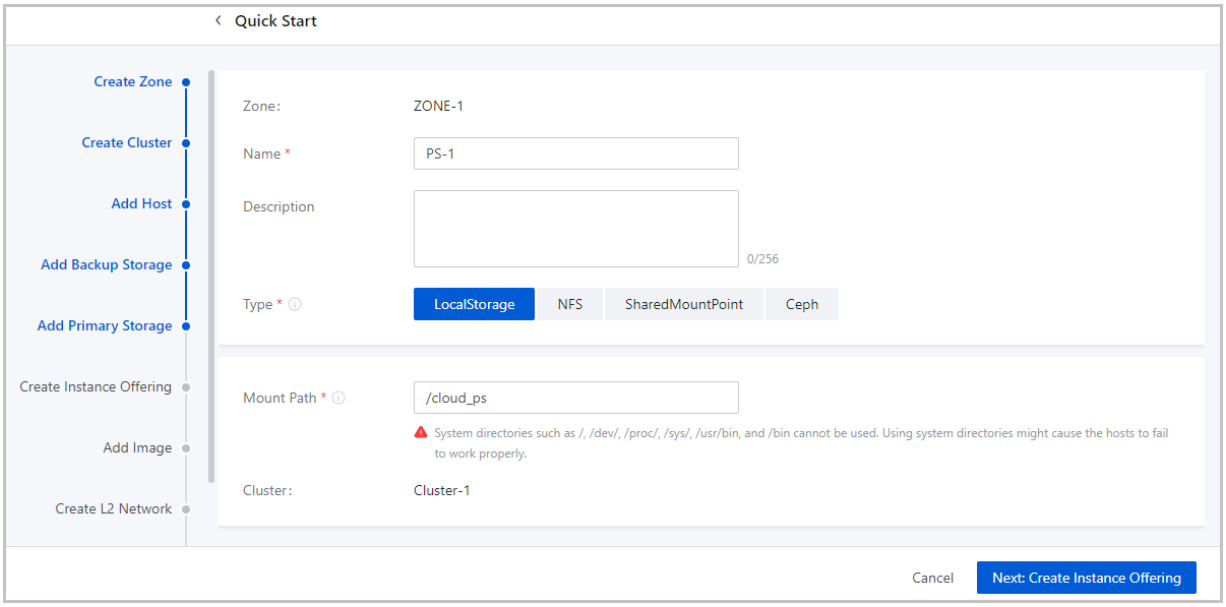
If you need to add a primary storage of the SharedBlock type, exit the wizard and add a primary storage on the primary storage management page.

6.5.1 LocalStorage

Context

If you add a LocalStorage primary storage, all hosts are configured with the same directory that you specify.

Figure 6-6: Add LocalStorage Primary Storage



On the displayed page, set the following parameters:

- **Name**: Enter a name for the primary storage.
- **Description**: Optional. Enter a description for the primary storage.
- **Type**: Select LocalStorage.
- **Mount Path**: Specify a path on the primary storage

Note:

- If the specified path does not exist on the primary storage, the system automatically creates the path.

- You cannot specify the following system paths. Otherwise, a host error may occur:
  - `/`
  - `/dev/`
  - `/proc/`
  - `/sys/`
  - `/usr/bin`
  - `/bin`

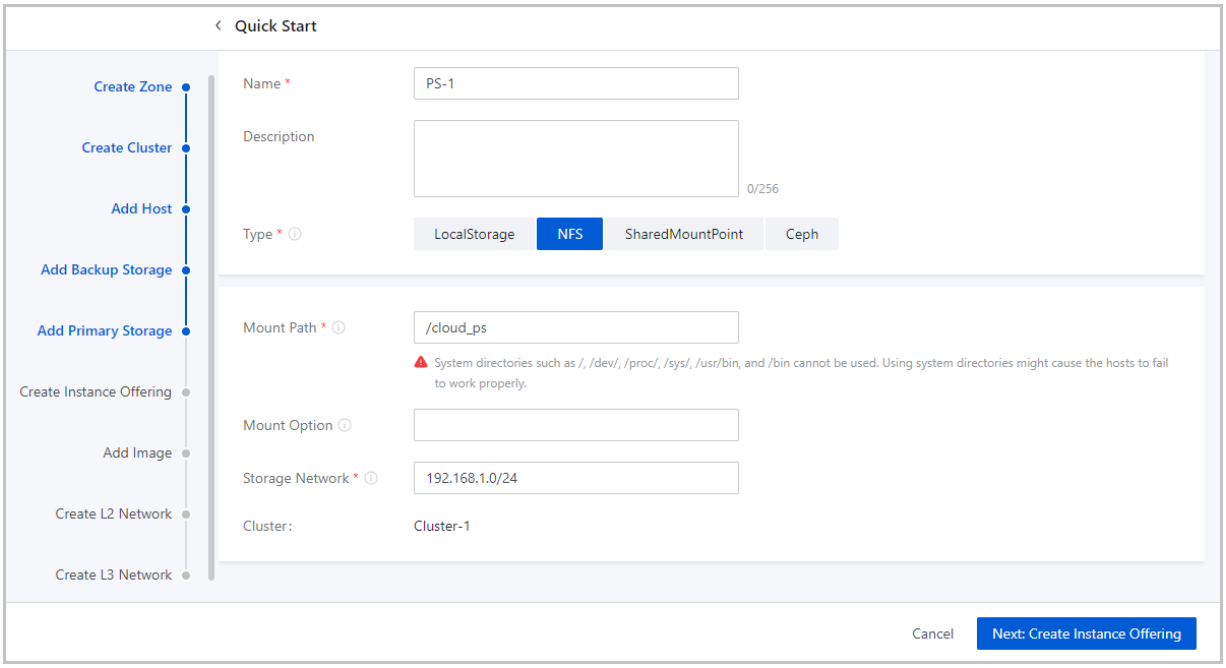
Click **Next** to complete the addition of the primary storage.

6.5.2 NFS

Context

If you use NFS primary storage, ZStack Cloud mounts the shared NFS directory to all the hosts. The hosts need to be granted read and write permissions on the mounted directory.

Figure 6-7: Add NFS Primary Storage



On the displayed page, set the following parameters:

- **Name**: Enter a name for the primary storage.
- **Description**: Optional. Enter a description for the primary storage.
- **Type**: Select NFS.

- **Mount Path**: Specify the URL of a shared directory on the NFS server a path on the primary storage. You can specify an IP address or domain name.

  Note:

  - The URL is in the format of *`NFS_Server_IP:/NFS_Share_folder`*, for example, *`192.168.0.1:/nfs_root`*.
  - You need to configure access permissions on the shared directory on the NFS server side in advance.
  - To ensure the security of the NFS server, we recommend that you configure security rules to implement access control.
  - You need to use the `showmount -e` command on the NFS server to check the shared directory.
  - You cannot specify the following system paths. Otherwise, a host error may occur:
    - *`/`*
    - *`/dev/`*
    - *`/proc/`*
    - *`/sys/`*
    - *`/usr/bin`*
    - *`/bin`*
- **Mount Option**: To add mount options, make sure that these options are supported by the NFS server.

  Note:

  - Separate each option with a comma (,), for example, nfsvers=3,sec=sys,tcp,intr,timeo=5 . This example means that NFS Version 3 is used on the NFS server, the standard UNIX authentication mechanism is used, TCP is used as the transmission protocol, an NFS call can be interrupted in case of an exception, and the timeout is 0.5 seconds (5/10).
  - To specify **`mount`** options, you can refer to the content in the **`-o`** option of **`mount`**.
  - You can set the options according to the commonly used **`mount`** options on clients. If the configured option conflict with the NFS server, the configuration on the server side shall prevail.
- **Storage Network**: Specify a network for the shared storage. You can use the management network.

Note:

- If you specify a dedicated storage network, you need to specify the CIDR of the network.
- You can use the storage network to check the health status of VM instances.

- Click **Next** to complete the addition of the NFS primary storage.

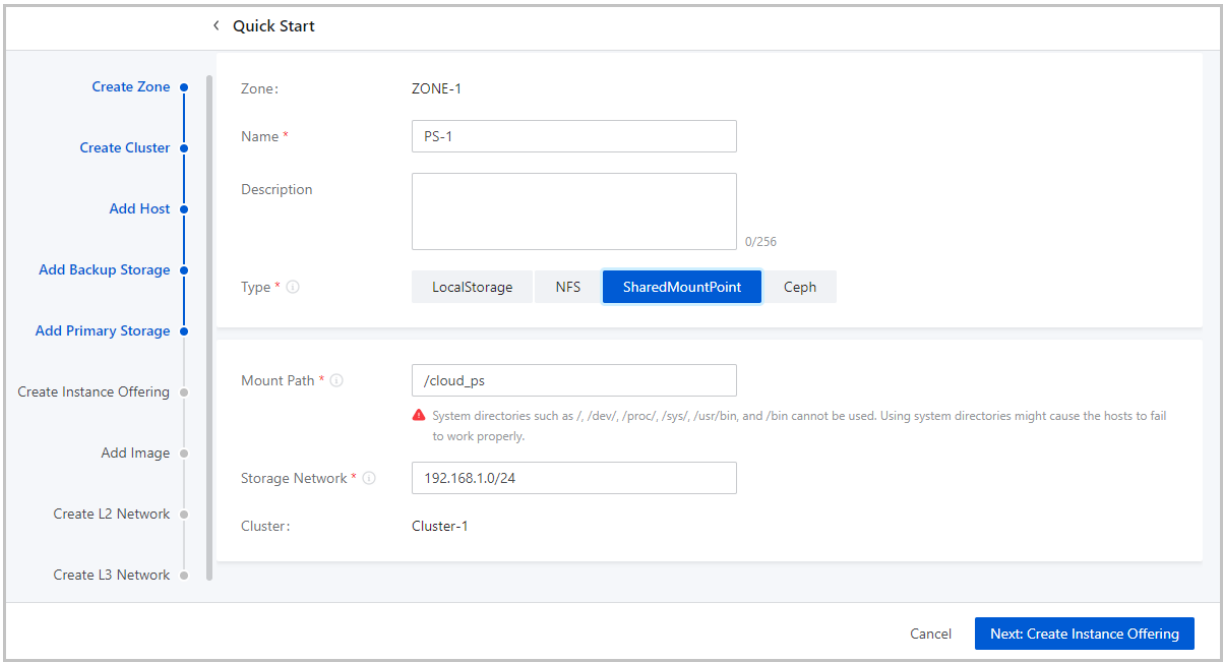
6.5.3 Shared Mount Point

Prerequisites

If you use Shared Mount Point (SMP) primary storage on ZStack Cloud, you can use distributed file systems such as MooseFS, GlusterFS, OCFS2, and GFS2 to provide network sharing storage.

Context

Figure 6-8: Add SMP Primary Storage



On the displayed page, set the following parameters:

- **Name**: Enter a name for the primary storage.
- **Description**: Optional. Enter a description for the primary storage.
- **Type**: Select SharedMountPoint.
- **Mount Path**: Specify the URL of the shared directory mounted on hosts.
- **Storage Network**: Specify a network for the shared storage. You can use the management network.

Note:

- If you specify a dedicated storage network, you need to specify the CIDR of the network.
- You can use the storage network to check the health status of VM instances.

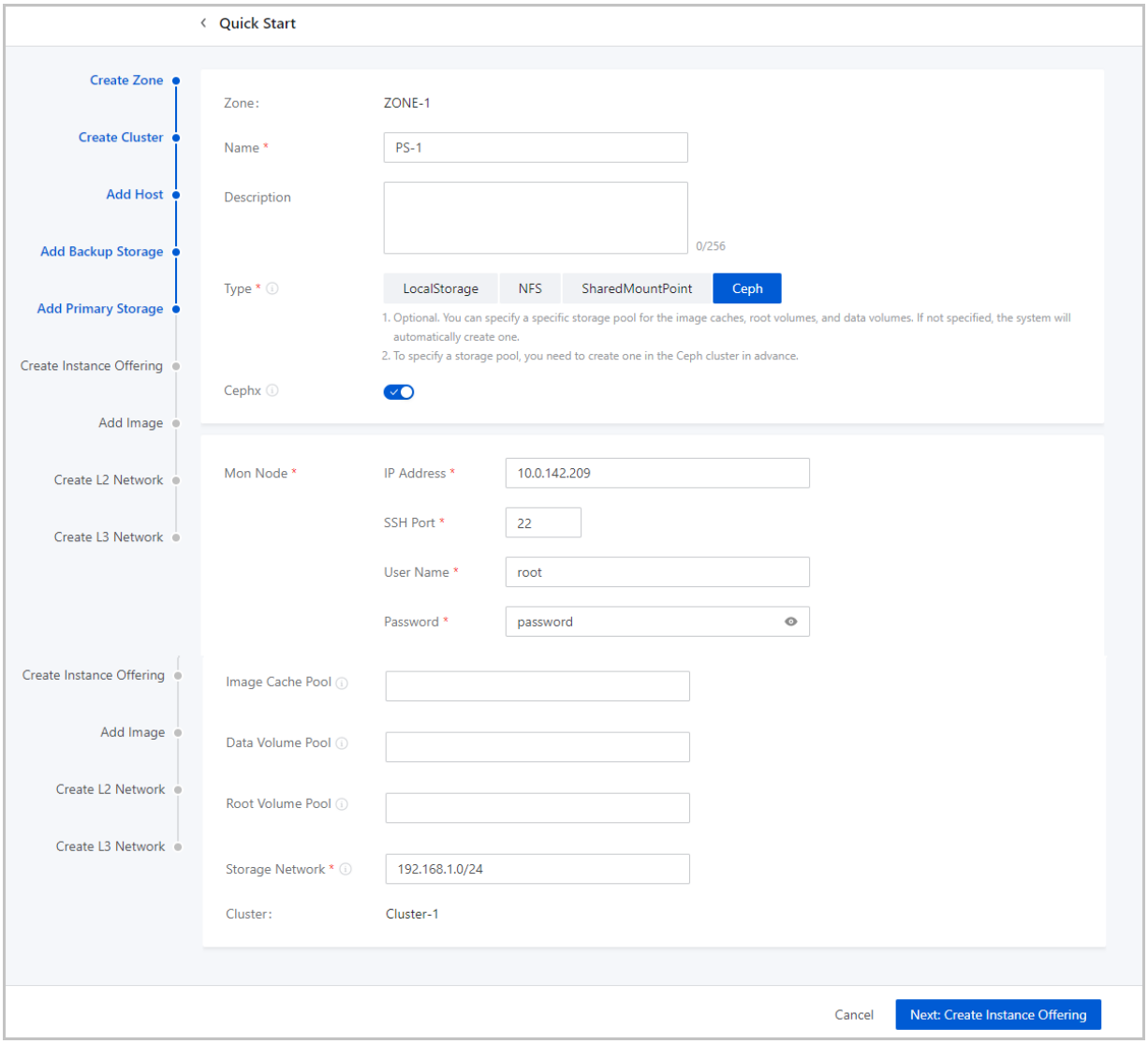
Click **Next** to complete the addition of the SMP primary storage.

6.5.4 Ceph

Context

ZStack Cloud allows you to store files in Ceph primary storage in the format of blocks. If you add a Ceph primary storage, you need to add a Ceph primary storage, you need to add a Ceph or ImageStore backup storage and configure Ceph distributed storage in advance.

Figure 6-9: Add Ceph Primary Storage



On the displayed page, set the following parameters:

- **Name**: Enter a name for the primary storage.
- **Description**: Optional. Enter a description for the primary storage.
- **Type**: Select Ceph.
- **Cephx**: Choose whether to use keys for authentication.

Note:

- By default, the Cephx authentication feature is enabled.
- If you disable Cephx, the authentication feature is disabled.

- If storage nodes and compute nodes reside in secure networks, you can disable Cephx to avoid authentication failures.
- Make sure that the Cephx configuration on Ceph storage is consistent with this configurat ion. If Cephx is enabled on Ceph storage but disabled on the cloud platform, VM instances may fail to be created.

- **IP Address**: Enter the IP address of the Ceph monitor node.
- **SSH Port**: Enter the SSH port of the Ceph monitor node. Default: 22.
- **User Name**: Enter the username of the Ceph monitor node.
- **Password**: Enter the password for the specified username.
- **Image Cache Pool**: Enter an image cache pool. If left blank, the system automatically creates a pool.
- **Data Volume Pool**: Enter a data volume pool. If left blank, the system automatically creates a pool.
- **Root Volume Pool**: Enter a root volume pool. If left blank, the system automatically creates a pool.
- **Storage Network**: Specify a network for the shared storage. You can use the management network.

Note:

- If you specify a dedicated storage network, you need to specify the CIDR of the network.
- You can use the storage network to check the health status of VM instances.

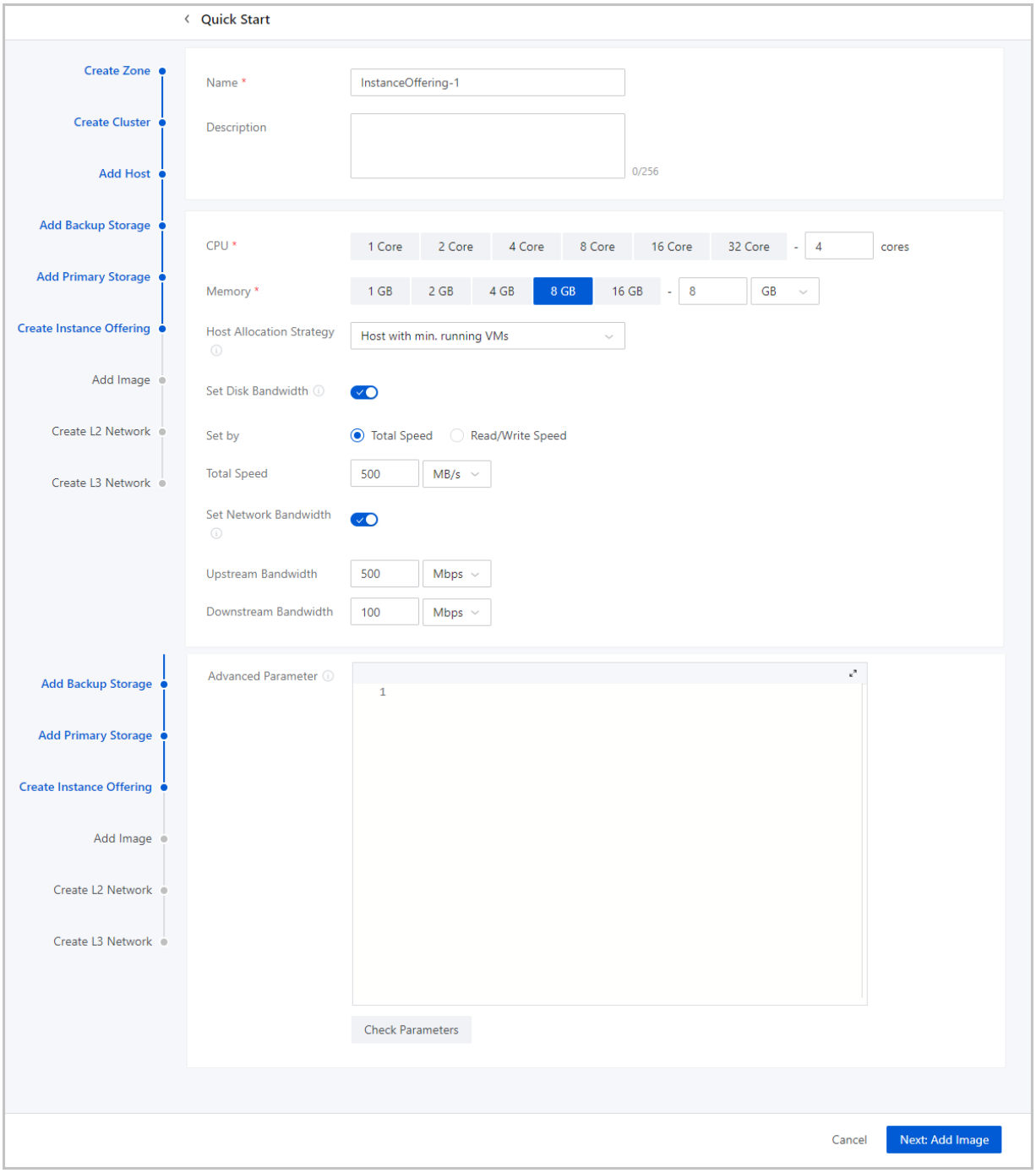
Click **Next** to complete the addition of the Ceph primary storage.

6.6 Create an Instance Offering

Context

An instance offering defines the number of vCPU cores, memory size, network bandwidth, and other configuration settings of VM instances.

Figure 6-10: Create Instance Offering



On the displayed page, set the following parameters:

- **Name**: Enter a name for the instance offering.
- **Description**: Optional. Enter a description for the instance offering.
- **CPU**: Enter the number of CPU cores of a VM instance.
- **Memory**: Set the size of the VM memory. Note that this value must be an integer. Unit: MB, GB, and TB.

- **Host Allocation Strategy**: Specify how the Cloud allocates hosts when you create VM instances. Default strategy: **Host with min. running VMs**.
  - **Host with min. running VMs**: Allocates the host with the minimum number of running VM instances to create VM instances.
  - **Host with min. CPU utilization**: Allocates the host with the minimum CPU utilization to create VM instances.

    Note:

    - The Cloud collects the host CPU loads over a period of time, calculates the CPU average utilization during this period, and then selects the host with the lowest CPU utilization to create VM instances.
    - By default, the Cloud collects data at an interval of 10 minutes. You can change the collection cycle by using the following method:

      Choose **Settings** > **Platform Setting** > **Global Setting** > **Advanced** > **Host** and set **Host CPU Utilization Collection Interval**
  - **Host with min. memory utilization**: Allocates the host with the minimum memory utilization to create VM instances.

    Note:

    - The Cloud collects the host memory loads over a period of time, calculates the memory average utilization during this period, and then selects the host with the lowest memory utilization to create VM instances.
    - By default, the Cloud collects data at an interval of 10 minutes. You can change the collection cycle by using the following method:

      Choose **Settings** > **Platform Setting** > **Global Setting** > **Advanced** > **Host** and set **Host Memory Utilization Collection Interval**.
  - **Host with max. running VMs**: Allocates the host with the maximum number of running VM instances to create VM instances. Before you can use this option, set the maximum number of VM instances that can run on a host. Then, the Cloud selects the host that meets the requirements to create VM instances. If no host is available, you will fail to create a VM instance.
  - **Host where the VM located last time**: When you restart a stopped VM instance, the system selects the host where the VM was running last time.

> **Note:**
> If you start a VM instance for the first time, the Cloud allocates a host randomly.

— **Random allocation**: Randomly allocates a host to create VM instances.

- **Set Disk Bandwidth**: Optional. Set an upper limit for the I/O bandwidth of the root volume.

  If not set, the I/O bandwidth of the root volume is not limited. Unit: MB/s, GB/s, and TB/s. You can set the I/O bandwidth by using either of the following methods:

  - **Total Speed**:

    Set an upper limit for the total read and write speed of the root volume. Value values: 1 MB/s to 100 GB/s, integer. Unit: MB/s and GB/s.

  - **Read/Write Speed**:

    Set an upper limit for the read or write speed of the root volume.

    - **Read Speed**: Optional. Set an upper limit for the read speed of the root volume. Value values: 1 MB/s to 100 GB/s, integer. Unit: MB/s and GB/s.
    - **Write Speed**: Optional. Set an upper limit for the write speed of the root volume. Value values: 1 MB/s to 100 GB/s, integer. Unit: MB/s and GB/s.

- **Set Network Bandwidth**: Optional. Set an upper limit for the network bandwidth of a VM instance.

  — **Upstream Bandwidth**: Optional. Set an upper limit of the network bandwidth for uploading data from a VM instance. If not set, the network bandwidth of a VM instance is not limited. Value values: 8 Kbps to 100 Gbps, integer. Unit: Kbps, Mbps, and Gbps.

  — **Downstream Bandwidth**: Optional. Set an upper limit of the network bandwidth for downloading data from a VM instance. If not set, the network bandwidth of a VM instance is not limited. Value values: 8 Kbps to 100 Gbps, integer. Unit: Kbps, Mbps, and Gbps.

  > **Note:**
  > Before you make any settings, make sure that you fully understand the configurations of the disk bandwidth and network bandwidth. Otherwise, you might fail to upload files to or download files from a VM instance.

- **Advanced Parameter**: Optional. Configure a JSON file to customize disk performance.

  Sample:

```
{
```

```
  "allocate": {
    "primaryStorage": {
      "type": "Enter a primary storage type. Valid values: Ceph,
LocalStorage, NFS, and SharedBlock.",
      "uuid": "Enter the UUID of a primary storage.",
      "poolNames": [
        "Enter the name of a Ceph pool. Delete this parameter if you
 do not specify a Ceph primary storage."
      ]
    }
  },
  "priceUserConfig": {
    "rootVolume": {
      "priceKeyName": "Set the billing name of a root volume.
Make sure that advanced parameter setting in the pricing list is
consistent with this setting. Otherwise, the corresponding bills
cannot be generated."
    }
  },
  "displayAttribute": {
    "rootVolume": {
      "diskType": "Set the display type of a root volume. You can
view this parameter setting on the VM details page."
    }
  }
}
```

The preceding configuration settings can be divided into the following three parts:

1. Set the primary storage for root volumes.

```
"allocate": {
    "primaryStorage": {
      "type": "Enter a primary storage type. Valid values: Ceph,
LocalStorage, NFS, and SharedBlock.",
      "uuid": "Enter the UUID of a primary storage.",
      "poolNames": [
        "Enter the name of a Ceph pool. Delete this parameter if
you do not specify a Ceph primary storage."
      ]
    }
  }
```

- **`type`**: Enter a primary storage type. Valid values: Ceph, LocalStorage, NFS, and SharedBlock. If you specify a Ceph primary storage, you can specify a Ceph pool.
- **`uuid`**: Enter the UUID of a primary storage.
- **`poolNames`**: Enter the name of a Ceph pool. Delete this parameter if you do not specify a Ceph primary storage.

Note:

If you do not specify a primary storage, delete the preceding parameter settings.

2. Set the billing type of a root volume.

```
"priceUserConfig": {
    "rootVolume": {
      "priceKeyName": "Set the billing name of a root volume.
Make sure that advanced parameter setting in the pricing list is
consistent with this setting. Otherwise, the corresponding bills
cannot be generated."
    }
  }
```

- **`priceKeyName`**: Set the billing name of a root volume. Make sure that advanced parameter setting in the pricing list is consistent with this setting. Otherwise, the corresponding bills cannot be generated.

Note:

If you do not need billing settings, delete the preceding parameter settings.

3. Set the display type of a root volume.

```
"displayAttribute": {
    "rootVolume": {
      "diskType": "Set the display type of a root volume. You can
view this parameter setting on the VM details page."
    }
  }
```

- **`rootVolume`**: Set the display type of a root volume. You can view this parameter setting on the VM details page. You can also set multiple attributes in key-value pair format.

Note:

If you do not need special display, delete the preceding parameter settings.

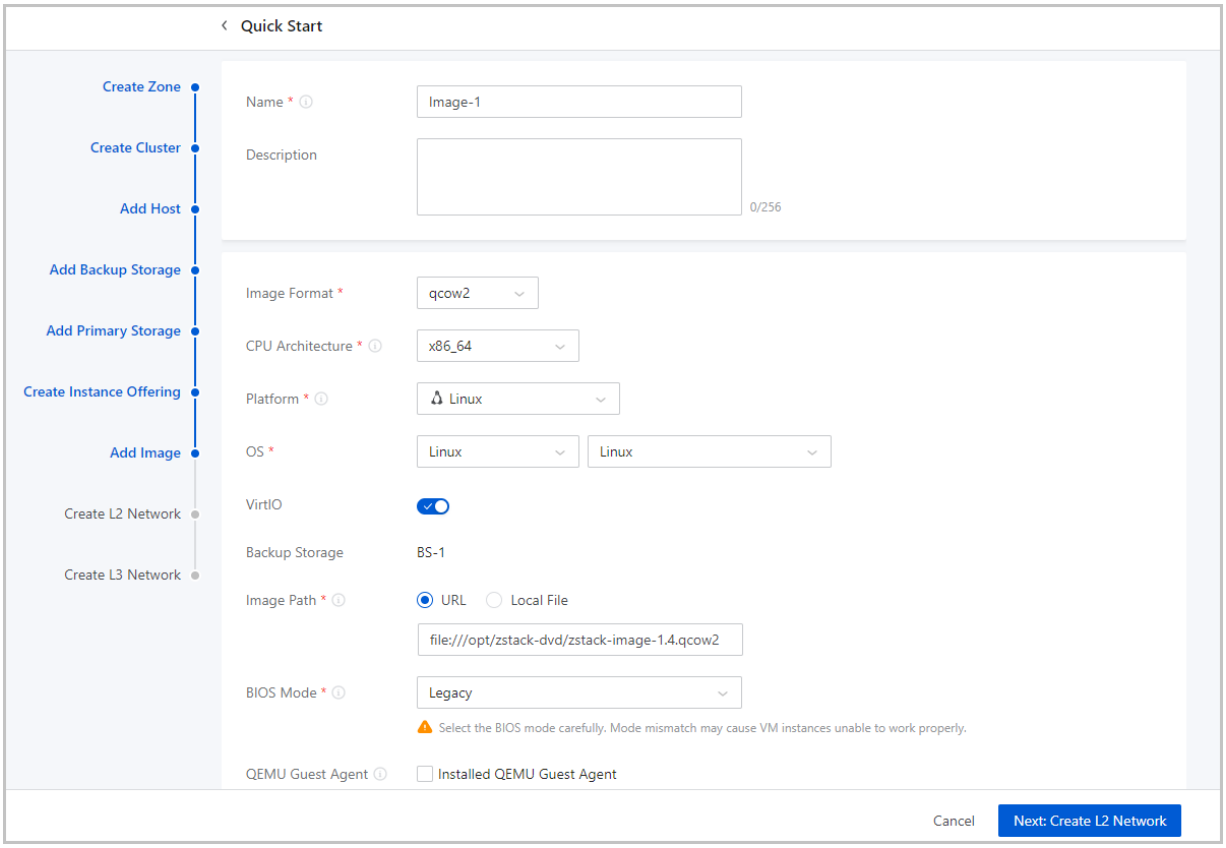
Click **Next** to complete the creation of the instance offering.

6.7 Add an Image

Context

An image is a template file used to create a VM instance or volume. Images are categorized into system images and volume images.

Figure 6-11: Add Image



On the displayed page, set the following parameters:

- **Name**: Enter a name for the image.
- **Description**: Optional. Enter a description for the image.
- **Image Format**: Select an image format. You can select qcow2, iso, or raw based on the image file property.
- **Platform**: Select an image platform type. Valid values: Linux, Windows, WindowsVirtio, Other, and Paravirtualization.

> **Note:**
> The Other platform type allows compatibility with earlier versions of an OS.

- **Image Path**: Specify an image URL or upload a local file:
  - **URL**: Enter a specified URL to add an image. You can enter a URL by using either of the following syntax:
    - A URL that starts with *http* or *https*:

  - Syntax: `http://host[:port]/path/file` or `https://host[:port]/path/file`.
  - Example: `http://cdn.zstack.io/product_downloads/images/zstack-image.qcow2`
- A URL that starts with *ftp*:
  - Syntax that does not specifies the user: `ftp://hostname[:port]/path/file`.

    Example: *ftp://172.20.0.10/pub/zstack-image.qcow2*.
  - Syntax that specifies the user: `ftp://user:password@hostname[:port]/path/file`.

    Example: *ftp://zstack:password@172.20.0.10/pub/zstack-image.qcow2*.
- A URL that starts with *sftp*:
  - Syntax that specifies the user identity: `sftp://user:password@hostname[:port]/path/file`.

    Example: *sftp://root:password@172.20.0.10/pub/zstack-image.qcow2*.
  - User-identity-free syntax: `sftp://user@hostname[:port]/path/file`.

    Example: *sftp://root@172.20.0.10/pub/zstack-image.qcow2*.
- The absolute path of an image file that is stored on a backup storage. The backup storage that stores the image file can be an ImageStore backup storage.

  Example: `file:///opt/zstack-dvd/zstack-image-1.4.qcow2`.

Note:

- The image file to be added to the destination backup storage must exist and the backup storage needs to have access to the URL of the image file.
- If you enter a URL that starts with *sftp* and does not specify user identity, make sure that you enable mutual password-free SSH login between the backup storage and SFTP server.
- For the progress bar and resumption from breakpoint features:
  - If you use an ImageStore backup storage, a progress bar will appear to display the upload progress. In addition, upload resumption from breakpoints is also supported.
  - If you use a Ceph backup storage, a progress bar will appear to display the upload progress. However, upload resumption from breakpoints is not supported.

- If you specify a URL with the `file:///` syntax to add an image:
  - Ceph backup storage does not support the *file:///* syntax.
  - The three forward slashes (/) in `file:///` represents the absolute path of a file on a backup storage. For example, if you specify the URL `file:///opt/zstack-dvd/image-1.4.qcow2`, you add the image file named *image-1.4.qcow2* in the `/opt/zstack-dvd` path of a backup storage to the Cloud.

— **Local File**: Select a local image file that the current browser can access and upload the image file to the specified backup storage. The backup storage that stores the image file can be an ImageStore or Ceph backup storage.

- **BIOS Mode**: Select a BIOS mode. You can select the Legacy or UEFI mode.

— Legacy: This mode supports all operating systems (OSs) and ensures stable operation. We recommend you select this mode.

— UEFI: This mode supports Windows and CentOS. Note that the Compatibility Support Module (CSM) must be enabled for Windows 7 and Windows Server 2008 R2.

Note:

Mode mismatch may cause VM instances unable to work as expected. Select a mode based on your business needs:

- If you add an image in qcow2 or raw format, select the mode consistent with the mode used when the image was created.
- If you add an image in iso format, you can select either of the two modes. OS will be boot based on the selected mode.
- If you want to boot the OS of a VM instance in UEFI mode, we recommend that you select a VM image that is created from one of the OS listed in the following table.

OS	BIOS Mode	Supported Versions
Windows	UEFI	• Windows 8 or later
	UEFI with CSM	• Windows 7 • Windows Server 2008 R2
Linux	UEFI	• CentOS 7.2 • CentOS 7.3 • CentOS 7.4 or later

- As mentioned in the preceding table, you can create a Linux-based VM instance by using an image that is created from CentOS 7.4 or later and that uses the UEFI mode. However, if the VM instance is restarted, the system may enter the UEFI Shell. To avoid this situation, you can use one of the following methods to boot the OS:

  — Use a script to skip the UEFI Shell and directly load the OS.

  In the installed OS, run the `vim /boot/efi/startup.nsh` command to create a file, enter the following content in the file, and save the file. Then when you restart the VM instance, the UEFI Shell is skipped and the OS is boot.

  ```
  FS0:
  CD EFI
  CD centos
  shimx64-centos.efi
  ```

  — Manually exit the UEFI Shell.

  If you have entered the UEFI Shell, run the following commands to exit the UEFI Shell:

  ```
  Shell> fs0:
  FS0:\> cd EFI
  FS0:\EFI\> cd centos
  FS0:\EFI\centos\> shimx64-centos.efi
  ```

- If you use a Window-based VM instance such as Windows Server 2012 R2, Windows Server 2016, or Windows 10 that has its OS boot in UEFI mode, the following figure will display after you start the VM instance. In this case, press any key to continue the installation of the OS. Otherwise, the system will enter the UEFI Shell.

  Figure 6-12: Press Any Key to Continue

  If you have entered the UEFI Shell, run the following commands to exit the UEFI Shell:

  ```
  Shell> fs0:
  FS0:\> dir
  FS0:\> cd EFI
  FS0:\EFI\> cd BOOT
  FS0:\EFI\BOOT\> BOOTX64.EFI
  ```

  Then press any key in a timely manner. Otherwise, the system will reenter the UEFI Shell.

- **QEMU Guest Agent**: Optional. Choose whether the current image has installed QEMU Guest Agent (QGA).

Note:

If the image has installed QGA and has set the agent as auto-start and you use the image to create a VM instance, you can modify the passwords of this VM instance, the clones of this VM instance, and the VM instances created from the image that is created from this VM instance when all these instances are in running state.

- **Support Elastic Baremetal Instance**: Optional. Choose whether the image can be used to create an elastic baremetal instance. If enabled, the image can be used to create an elastic baremetal instance.

Note:

When you add an image of an elastic baremetal instance, make sure:

- The image has installed the agent. Otherwise, after you use the image to create an elastic baremetal instance, you cannot open the console or modify the password of the elastic baremetal instance. In addition, you cannot attach a volume or network to the instance or detach a volume or network from the instance.
- The BIOS mode of the image is the same the system configuration. Default: UEFI. If you want to use Legacy, contact the technical support.

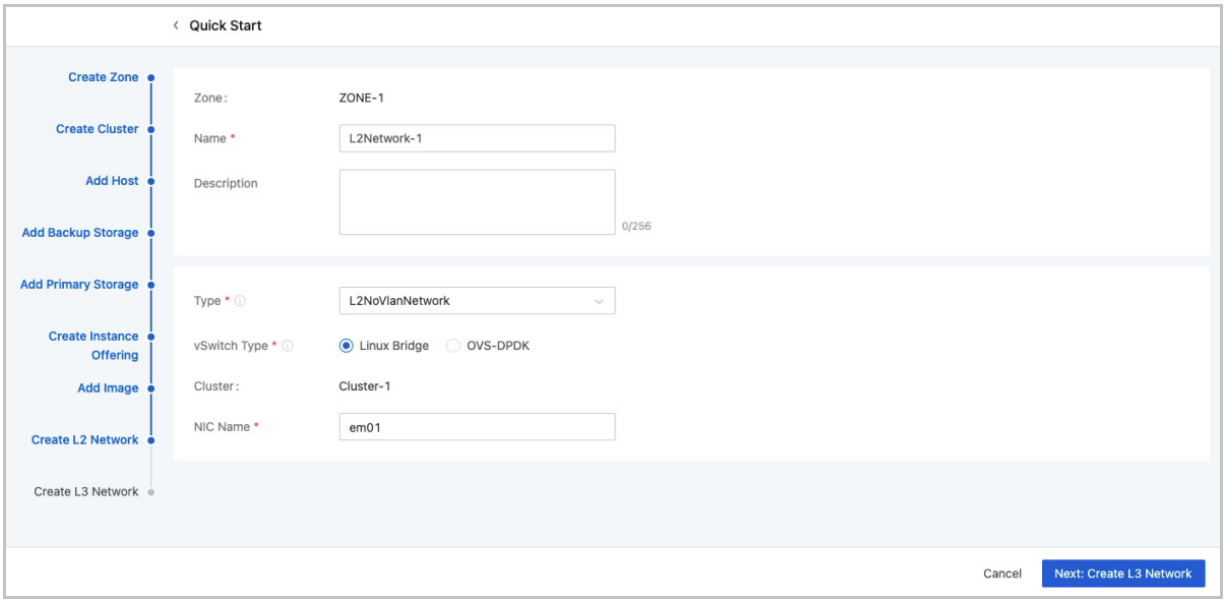
Click **Next** to complete the addition of the image.

6.8 Create an L2 Network

Context

An L2 network is a layer 2 broadcast domain used for layer 2 isolation. Generally, L2 networks are identified by names of devices on the physical network.

Figure 6-13: Create L2 Network



On the displayed page, set the following parameters:

- **Name**: Enter a name for the L2 network.
- **Description**: Optional. Enter a description for the L2 network.
- **Type**: Valid values: L2NoVlanNetwork and L2VlanNetwork.
  - L2NoVlanNetwork
    - If you do not need to use VLAN, select L2NoVlanNetwork.
    - If you specify L2NoVlanNetwork, the switch port connected by the specified NIC must be in Access mode.
    - **NIC Name**: Enter the NIC name of the corresponding host.
  - L2VlanNetwork
    - If you need to use VLAN on ZStack Cloud, select L2VlanNetwork.
    - If you specify L2NoVlanNetwork, the switch port connected by the specified NIC must be in Access mode.
    - **VLAN ID**: Specify a VLAN ID that matches the actual network configurations. Valid values: 1 to 4094.
    - **NIC Name**: Enter the NIC name of the corresponding host.
- **vSwitch Type**: The vSwitch type of the L2 network, including Linux Bridge and OVS-DPDK. Default: Linux Bridge.
- **NIC Name**: Enter a NIC name for the L2 network. For example, em01.

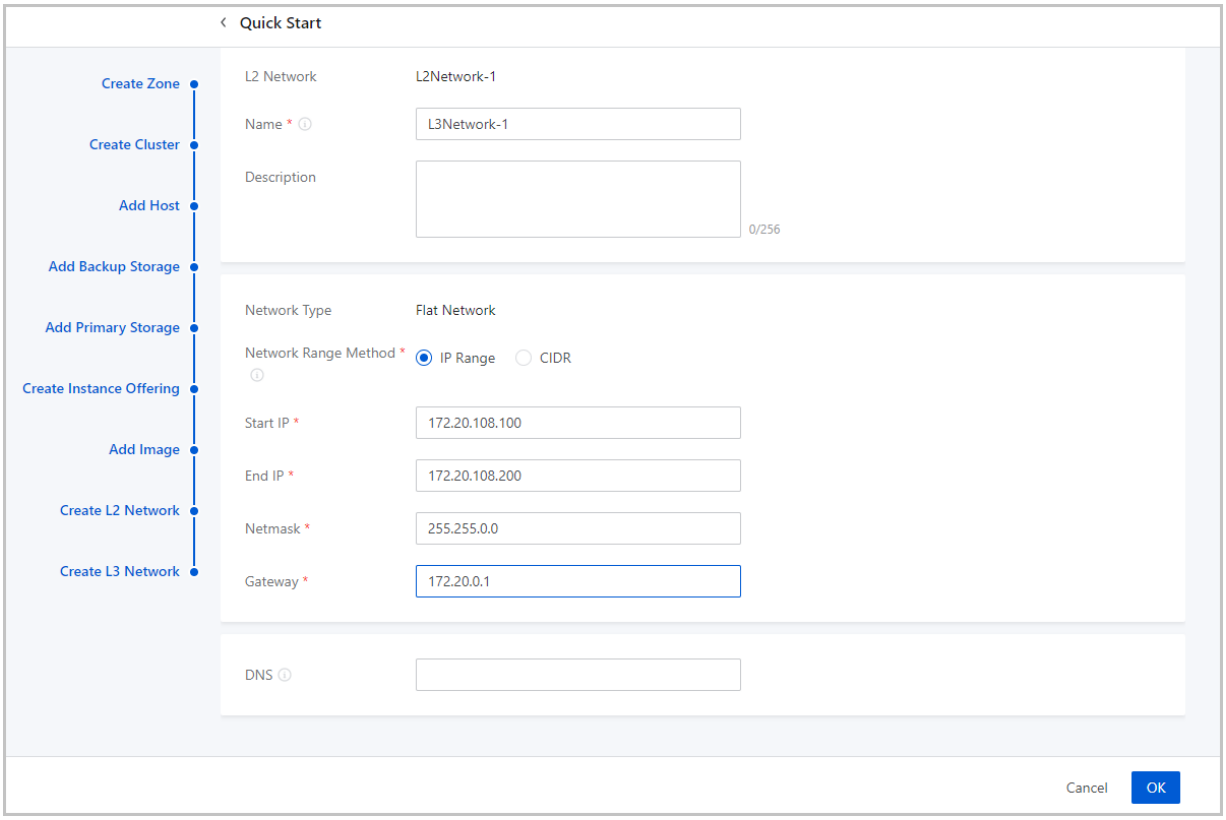
Click **Next** to complete the creation of the L2 network.

6.9 Create an L3 Network

Context

An L3 network includes IP ranges, gateway, DNS, and other network configurations that are used by VM instances.

Figure 6-14: Create L3 Network



On the displayed page, set the following parameters:

- **Name**: Enter a name for the L3 network.
- **Description**: Optional. Enter a description for the L3 network.
- **Network Type**: The wizard supports only flat network.
- **Network Range Method**: Select a method to add a network range for the L3 network. You can select IP Range or CIDR.

  If you select **IP Range**, you need to set the following parameters:

  - **Start IP**: Set a start IP address for the network range, for example, *172.20.108.100*.
  - **End IP**: Set an end IP address for the network range, for example, *172.20.108.200*.

- **Netmask**: Set a netmask for the network range, for example, *255.255.0.0*.
- **Gateway**: Set a gateway for the network range, for example, *172.20.0.1*.
- **DNS**: Add a DNS server to provide domain name resolution services for the L3 network. You can specify *223.5.5.5*, *8.8.8.8*, or *114.114.114.114*.

If you select **CIDR**, you need to set the following parameters:

- **CIDR**: Set a CIDR block for the L3 network, for example, *192.168.108.1/24*.
- **Gateway**: Set a gateway for the L3 network, for example, *192.168.108.1*.

  Note:

  - You can use the first or last IP address in the specified CIDR block as the gateway.
  - If left blank, the first IP address in the specified CIDR block is used as the gateway.
- **DNS**: Add a DNS server to provide domain name resolution services for the L3 network. You can specify *223.5.5.5*, *8.8.8.8*, or *114.114.114.114*.

Click **Next** to complete the creation of the L3 network.

What's next

The wizard is complete.

7 Resource Center

7.1 Resource Pool

7.1.1 VM Instance

7.1.1.1 What is VM Instance?

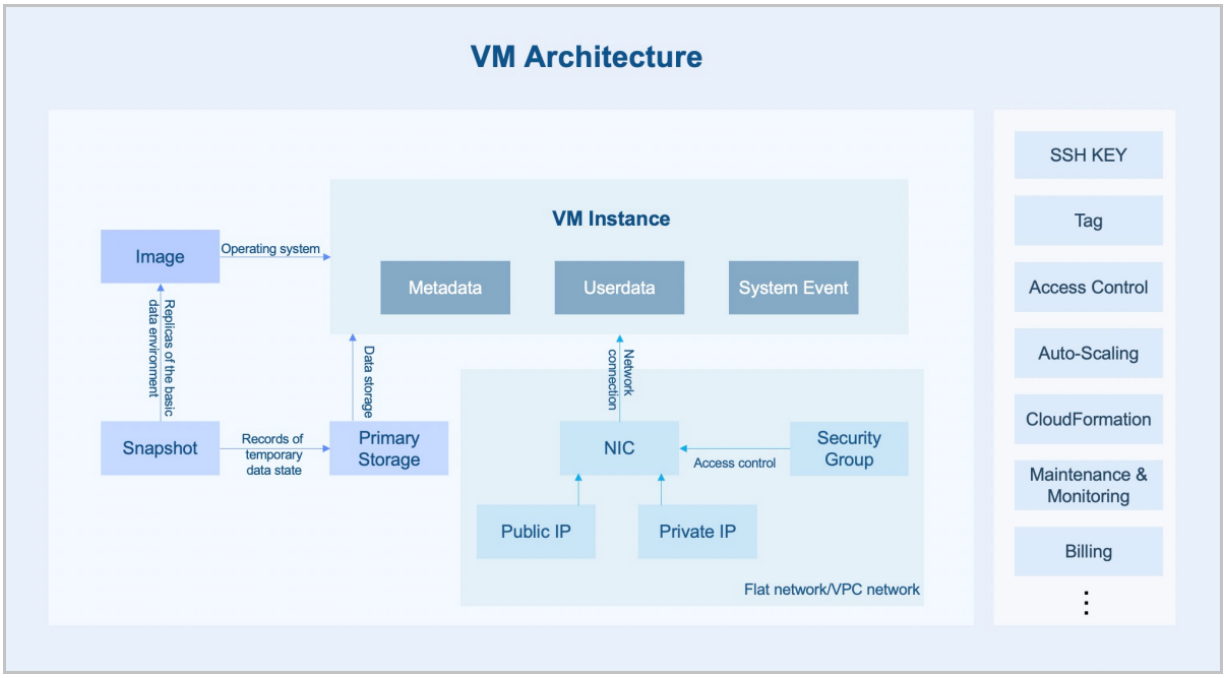
A VM instance is a virtual machine instance running on a host. A VM instance has its own IP address and can access public networks and run application services.

Architecture

A VM instance consists of the following core components:

- Instance: A virtual machine instance running on a host. An instance includes the basic resources such as CPU, memory, operating system, network configurations, and disks.
- Image: An image is a template file used to create a VM instance. Images provide the operating system required by a VM instance.
- Primary storage: A primary storage is one or more servers that store volume files of VM instances. These files include root volume snapshots, data volume snapshots, image caches, root volumes, and data volumes.
- Snapshot: A snapshot is a point-in-time capture of data status in a volume. Before you perform a business-sensitive operation on a VM instance, you can schedule snapshot creation at specified time points to record the state of the VM data. This allows rollback in case of breakdowns.
- Networks:
  - Flat network: A flat network is connected to the network where the host is located and has direct access to the Internet. VM instances in a flat network can access public networks by using elastic IP addresses.
  - VPC network: A VPC network is a private network where VM instances can be created. A VM instance in a VPC network can access the Internet through a VPC vRouter.
- Security group: A security group provides security control services for VM instances on the L3 network. It filters the ingress or egress TCP, UDP, and ICMP packets of specified VM instances in specified networks based on the specified security rules.

Figure 7-1: VM Architecture



Characteristics

VM instances have the following characteristics:

- High availability (HA): You can set an HA mode for a VM instance. When the VM instance is stopped due to daily maintenance or exceptions, the HA policy can trigger the automatic restart of the VM instance to improve the VM availability.
- Security:
  - The VM console allows you to conveniently monitor and manage VM instances. Note that you must have the corresponding permissions before you can log in to the VM console.
  - A VM instance supports IP/MAC/ARP anti-spoofing. Abnormal protocol access sent by the VM instance at the data link layer of a host is isolated to block MAC/ARP spoofing and achieve IP anti-spoofing at the network layer.
  - You can create an image for a VM instance. The image contains all of the information about the VM instance. You can quickly copy the corresponding resources through the image.
  - You can create a snapshot for a VM instance. Before you perform a business-sensitive operation on the VM instance, you can schedule snapshot creation at specified time points to record the state of the VM data. This allows rollback in case of breakdowns.
  - A VM instance supports encrypted storage of plain text passwords to protect sensitive data on the VM instance.

  - You can set a delete policy for a VM instance, including Direct, Delay, and Never. When you delete a VM instance in the UI, a dialog box is displayed to remind you of the consequences of deleting the VM instance. You must acknowledge the risks before you can delete it. This helps to reduce the risks caused by misoperations.
  - A VM instance supports role-based access control and permission management.
  - A VM instance supports operation logs and auditing, which can meet the needs of security analysis, intrusion detection, resource change tracking, and compliance auditing.
- Scalability:
  - A VM instance allows you to modify its CPU and memory online and expand the attached root volumes and data volumes online. You can modify the VM configurations as needed.
  - A VM instance supports auto-scaling. The Cloud can automatically trigger VM auto-scaling or self-healing according to business changes.

Scenarios

VM instances can be used in the following scenarios:

- Breaks down the traditional IT information silos.

  VM instances integrate the business of an enterprise on the cloud and migrate the information service system from traditional physical servers to VM instances. This helps to improve the resource utilization and reduce repeated investments. VM instances realize the rationalized scheduling of resources through intelligent load balancing services. In addition, the VM HA feature can deal with various exceptions to ensure business continuity of VM instances..
- Improves the development and testing efficiencies of enterprises.

  For modern IT enterprises, the deployment and approval of a development and testing environment is time-consuming, which severely restricts the business launch cycle. With VM instances, resources can be allocated online, which helps to establish or recover a development and testing environment in seconds. This accelerates the business launch. In the same resource pool, an enterprise can develop its environment by using the encapsulated environment of a VM instance and arrange the testing plan more reasonably. After an application development is completed, resources occupied by the corresponding VM instance can be quickly released and assigned to other projects. You can plan resource configuration in advance and apply for immediate distribution as needed.
- Deploys PaaS and SaaS services for enterprises.

For enterprises that cannot migrate PaaS or SaaS services to the public cloud, they can use ZStack Cloud to build a private cloud environment and deploy the PaaS or SaaS services on VM instances. The flexibility, stability, and high concurrency characteristics of the VM instances help to ensure the security, stability, and high-efficiency of the enterprises.

- Provides a safe rehearsal environment.

  In recent years, network attack defense is tilted towards attackers. Enterprises are facing severe cloud security challenges as various high-risk vulnerabilities, APT targeted attacks, and computer viruses emerged in an endless stream. By using VM instances, enterprises can build a completely isolated security rehearsal environment and ensure the business security with monitoring and alarming, log auditing, vulnerability management, anti-virus and other means.

- 3D rendering, artificial intelligence (AI), and cloud desktop

  VM instances with GPU passthrough have strong computing capabilities and can be used in thin terminal scenarios such as 3D rendering, AI, and cloud desktops.

  - 3D rendering

    3D rendering is commonly used in movie production or three-dimensional video games. Due to the extremely high computational intensity, GPU server clusters are often used to provide computing abilities. ZStack Cloud provides GPU passthrough features, which enables extremely low performance loss (within 5%) as well as centralized and efficient cluster management. Coupled with intelligent monitoring and billing, VM instances can form a complete set of convenient and efficient rendering farm solution.

  - Artificial intelligence

    Enterprises can build a TensorFlow-based AI application by using VM instances with GPU passthrough. The powerful computing capabilities of GPU devices can fully meet the infrastructure requirements for large-scale model training.

  - Cloud desktop

    GPU devices play a critical role in the field of cloud desktop applications. GPU devices not only upgrade the desktop visual experience, but also assume the main computing role in special applications. Replacing traditional PC graphics stations, GPU devices allow users to implement their 3D work in a safer environment. By using VM instances with GPU passthrough and protocols such as RDP and PCoIP, users can fully enjoy the capabilities of graphics cards and obtain a near-physical machine experience.

7.1.1.2 Create a VM Instance (Fast Creation)

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Virtual Resource** > **VM Instance**. You can create a VM instance quickly through one of the following fast creation entrances:

- Click the **Fast Creation** button on the right of **Create VM Instance**. Then, the **Fast Creation** page is displayed.
- Click **Create VM Instance**. On the displayed page, click on **Fast Creation**.

On the **Fast Creation** tab page, set the following parameters:

- **Name**: Enter a name for the VM instance. Note that the VM name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Quantity**: Enter the number of VM instances to be created. Valid values: 1 to 100. You can change the maximum number by modifying the value of **Maximum VM Creation in Batch on UI** in the global setting.

  Note:
  When you create VM instances in bulk, the names of these VM instances will be followed by -1, -2, -3 and so forth to distinguish these VM instances.
- **Tag**: Optional. Bind one or more tags to the VM instance as needed.
- Set the VM offering by using one of the following methods:

  Basic Offering: Set the VM offering by selecting an existing instance offering and disk offering.

  - **Instance Offering**: Select an existing instance offering. The instance offering defines the number of CPU cores, memory size, host allocation strategy, and other configurations of the VM instance.
  - **Image**: Select an existing image. The image is used to install an operating system for the VM instance.

    Note:
    If you select an Windows-based ISO image that has enabled Virtio, the Virtio drive is attached to the image by default. You need to manually install the drive when you install the operating system. If you restart the VM instance on the UI, the drive will be detached.

- **Root Disk Offering**: Select an existing disk offering for the root volume of the VM instance. The root disk offering defines the root volume information such as the size and disk bandwidth. This parameter appears only when the image type is ISO.
- **Data Volume**: Optional. Choose whether to create a data volume and attach it to the VM instance. By default, no data volumes will be created.

  If you choose to create a data volume, set the following parameters:

  - **Data Disk Offering**: Select an existing disk offering for the data volume of the VM instance. The data disk offering defines the data volume information such as the volume size and disk bandwidth.
  - **VirtIO SCSI**: Optional. Choose whether to use a VirtIO SCSI bus to create a SCSI data volume.

    Note:

    - By default, VirtioSCSI is enabled if a shared storage is used, indicating that you can create VirtIO SCSI volumes.
    - If a LocalStorage primary storage is used, you can enable VirtioSCSI on the volume details page.
    - VirtIO SCSI volumes support multiple I/O queues, which can be identified as IDs (WWN).

    By default, a VirtIO SCSI bus is used to create SCSI data volumes for shared storages. We recommend that you do not create SCSI data volumes for LocalStorage primary storages.

Custom Offering: Set the VM offering by customizing the following VM configurations:

- **CPU**: Set the number of CPU cores of the VM instance. Valid values: 1 to 1024, integer.
- **Memory**: Set the memory size of the VM instance. Valid values: 16 MB to 1000 TB, integer. Unit: MB, GB, and TB.
- **Image**: Select an existing image. This image is used to install an operating system for the VM instance.

  Note:

If you select an Windows-based ISO image that has enabled Virtio, the Virtio drive is attached to the image by default. You need to manually install the drive when you install the operating system. If you restart the VM instance on the UI, the drive will be detached.

- **Root Volume**: Set the size of the root volume. Valid values: 1 MB to 1024 TB, integer. Unit: MB, GB, and TB. This parameter appears only when the image type is ISO.
- **Data Volume**: Optional. Choose whether to create a data volume with the VM instance. By default, no data volumes will be created.

  If you choose to create a data volume, set the following parameters:

  - **Data Volume Size**: Set the size of the data volume. Valid values: 1 MB to 1024 TB, integer. Unit: MB, GB, and TB.
  - **VirtIO SCSI**: Optional. Choose whether to use a VirtIO SCSI bus to create a SCSI data volume.

    Note:

    - By default, VirtioSCSI is enabled if a shared storage is used, indicating that you can create VirtIO SCSI volumes.
    - If a LocalStorage primary storage is used, you can enable VirtioSCSI on the volume details page.
    - VirtIO SCSI volumes support multiple I/O queues, which can be identified as IDs (WWN).

    By default, a VirtIO SCSI bus is used to create SCSI data volumes for shared storages. We recommend that you do not create SCSI data volumes for LocalStorage primary storages.

- **Network Configurations**: Configure the networks used by the VM instance. You can add multiple networks as needed.

  — **Network**: Select an L3 network for the VM instance. Supported network types: VPC network, public network, and flat network.

  — **Make Default**: Set one of the networks as the default network of the VM instance.

  — **Enable SR-IOV**: Optional. Choose whether to use SR-IOV to generate a VF NIC and pass it through to the VM instance. By default, SR-IOV is disabled. You can enable it if you have qualified hardware resources.

Note:

To enable SR-IOV, note that:

- Make sure that SR-IOV is enabled for the L2 network corresponding to the L3 network of the VM instance. Otherwise, SR-IOV cannot be enabled.
- Enabling SR-IOV generates a VF NIC and passes it through to the VM instance. If not enabled, a vNIC will be assigned to the VM instance.
- Before you enable SR-IOV, make sure that the physical NIC corresponding to the L3 network has an available VF NIC. Otherwise, the VM instance might fail to be created.

— **Assign IP**: Optional. Choose whether to assign an IP address to the VM NIC. By default, the Cloud assigns an IP address to the VM instance through DHCP.

Note:

To assign an IP address, note that:

- The IP address must be unique within the network segment of the selected network.
- By default, the drop-down menu displays 5 recommended IP addresses. If the current network has less than 5 IP addresses, all available IP addresses will be displayed.
- If you create VM instances in bulk and assign an IP address here, the Cloud automatically assigns IP addresses to these VM instances with the first assigned IP address as the start IP. If an IP address is occupied or if IP addresses are insufficient within the continuously assigned IP range, the corresponding VM instance will fail to be created.
- If DHCP is not enabled for the L3 network, we recommend that you assign an IP address to the VM instance.

— **MAC Address**: Optional. Choose whether to customize a MAC address for the VM instance. By default, the Cloud assigns a MAC address to the VM instance.

— **Security Group**: Optional. Associate a security group with the VM instance.

— **EIP**: Optional. Associate an elastic IP address (EIP) with the VM instance.

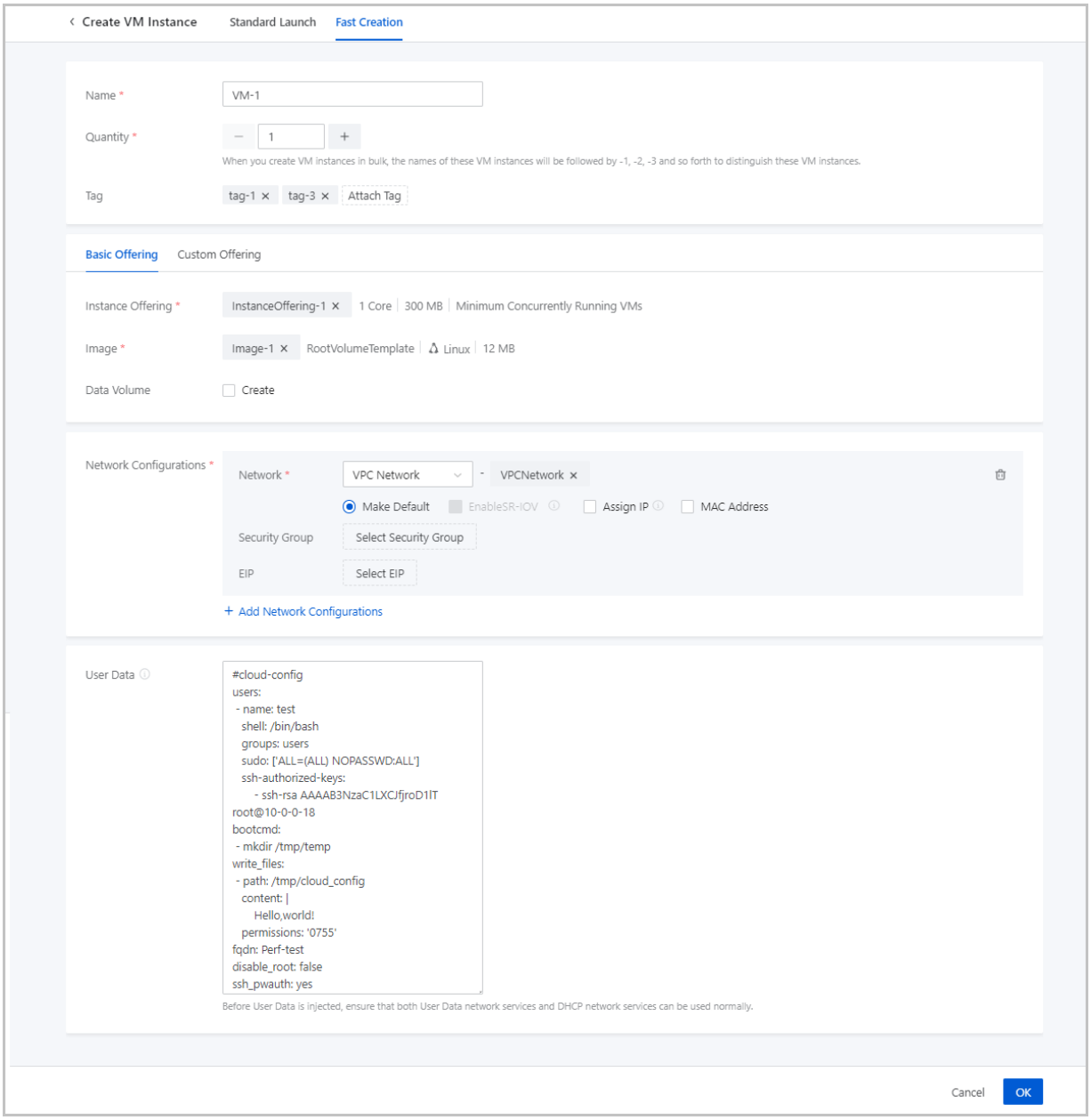
- **User Data**: Optional. Inject user-defined parameters or scripts to customize configurations for the VM instance or to accomplish specific tasks.

Note:

To use user data, note that:

- Before you import user data, make sure that both the user data network service and DHCP network service work as expected.
- Before you inject user data to Linux-based VM instances, make sure that cloud-init is installed on the images of the VM instances. We recommend that you install cloud-init 0.7.9 , 17.1, 19.4, 19.4, or later.
- Before you inject user data to Windows-based VM instances, make sure that Cloudbase-Init is installed on the images of the VM instances. You can install Cloudbase-Init of any version.
- If you set a root user password in user data for a VM instance, the password is displayed in the User Data option on the details page of the VM instance. Make sure that your password is well protected.

Figure 7-2: Create VM Instance (Fast Creation)



7.1.1.3 Create a VM Instance (Standard Creation)

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Virtual Resource** > **VM Instance**. Click **Create VM Instance**. On the displayed page, click on **Standard Creation**.

To create a VM instance through the standard creation entrance, follow these four steps:

1. Complete the basic configurations.

   Set the following parameters:

- **Name**: Enter a name for the VM instance.
- **Description**: Optional. Enter a description for the VM instance.
- **Quantity**: Enter the number of VM instances to be created. You can create VM instances in bulk.

  Note:

  - The quantity must be an integer ranging from 1 to 100.
  - You can change the maximum number of VM instances that you can create. Method:

    Go to **Settings** > **Platform Setting** > **Global Setting** > **Advanced** > **Resource Center** > **Resource Pool** > **VM instance**, locate **Maximum VM Creation in Batch on UI**, and change its value as needed. Default: 100.
- **Tag**: Optional. Bind one or more tags to the VM instance.

  Note:

  - The Cloud supports 50 tags per resource and an unlimited number of resources per tag.
  - Multiple tags can be bound to multiple resources.
  - An administrator can unbind or delete tags created by a tenant.
  - An administrator can set the number of tags can be created by a tenant by using the following method:

    Go to **Settings** > **Platform Setting** > **Global Setting** > **Advanced** > **Platform Policy** > **Quota Policy**, locate **Tag Default Quota for Tenant**, and change its value as needed. Default: 20.
- Set the VM offering by using one of the following methods:

  — **Basic Offering**: Set the VM offering by selecting an existing instance offering and disk offering.

    - **Instance Offering**: Select an existing instance offering.
    - **Image**: Select an existing image.
    - **Root Disk Offering**: Select an existing disk offering for the root volume of the VM instance. This parameter appears only when the image type is ISO.
    - **Data Volume**: Optional. Choose whether to create a data volume and attach it to the VM instance. By default, no data volumes will be created.

- **Data Disk Offering**: Select an existing disk offering for the data volume.
- **VirtIO SCSI**: Optional. Choose whether to create a SCSI data volume.

Note:

- By default, VirtioSCSI is enabled if a shared storage is used, indicating that you can create VirtIO SCSI volumes.
- If a LocalStorage primary storage is used, you can enable VirtioSCSI on the volume details page.
- VirtIO SCSI volumes support multiple I/O queues, which can be identified as IDs (WWN).

— **Custom Offering**: Set the VM offering by customizing the following VM configurations:

- **CPU**: Set the number of CPU cores of the VM instance. Valid values: 1 to 1024, integer.
- **Memory**: Set the memory size of the VM instance. Valid values: 16 MB to 1000 TB, integer. Unit: MB, GB, and TB.
- **Image**: Select an existing image.
- **Data Volume**: Choose whether to create a data volume and attach it to the VM instance.
  - **Data Volume Size**: Set the size of the data volume. Valid values: 1 MB to 1024 TB, integer. Unit: MB, GB, and TB.
  - **VirtIO SCSI**: Optional. Choose whether to create a SCSI data volume.

Note:

- By default, VirtioSCSI is enabled if a shared storage is used, indicating that you can create VirtIO SCSI volumes.
- If a LocalStorage primary storage is used, you can enable VirtioSCSI on the volume details page.
- VirtIO SCSI volumes support multiple I/O queues, which can be identified as IDs (WWN).

- **Advanced**:

— **HA Mode**: Optional. Choose a high availability (HA) mode for the VM instance.

Note:

- You can enable or disable the VM HA feature in the Cloud by using the following method:

  Go to **Settings** > **Platform Setting** > **Global Setting** > **Advanced** > **Platform Policy** > **HA Policy**, locate **Enable VM HA Globally**, and enable or disable the switch as needed. Default: true.
- The HA switch of a single VM instance is strictly controlled by that in the global setting.
- If you disable the switch in the global setting, you cannot set HA mode for a VM instance on the VM details page. In this case, the VM business may not be protected by HA. Please exercise caution.

— **Time Sync**: Optional. Choose whether to synchronize the VM base time with the host time. If yes, the base time of the VM instance is the same as that of the host. The time sync feature is enabled by default.

Note:

- If you enable time synchronization for a running Windows VM instance, the VM time is synchronized with the host time automatically on a regular basis.
- If you enable time synchronization for a stopped or paused Windows VM instance, the setting takes effect after the VM instance reboots.
- If you disable time synchronization for a Windows VM instance, the VM time is not synchronized with the host time.
- The time synchronization setting does not take effect on Linux VM instances.
- You can enable time sync in Global Setting for all Windows VM instances on the cloud. To enable time sync in Global Setting, set VM Time Sync to Sync. By default, the time sync global setting is disabled.
- If you specifically set time sync for the VM instance, the VM Time Sync global setting does not take effect on the VM instance.

— **Resource Priority**: Optional. Set a high resource priority for the VM instance so that VM instance can compete for more resources in case of resource contention.

Note:

- When resource contention occurs due to high host workloads, priority is given to allocating resources to VM instances with the high resource priority.
- We recommend that you set a high resource priority for vital VM instances.

— **Affinity Group**: Optional. Select an affinity group for the VM instance. You can set the affinity group policy for the VM instance as needed. Valid affinity group policies: anti-affinity group (soft) and anti-affinity group (hard).

■ Anti-affinity group (soft):

Allocates VM instances in the affinity group to different hosts as much as possible. If no more hosts are available, the VM instances will be allocated randomly.

■ Anti-affinity group (hard):

Strictly allocates VM instances in the affinity group to different hosts. If no more hosts are available, the allocation fails.

— **USB Redirection**: Optional. Set USB redirection for the VM instance.

Note:

- The Cloud currently supports redirection of multiple USB devices. If you want to use the VDI feature, you can redirect the USB device on the VDI client to the VDI VM instance.
- The setting takes effect after you restart the VM instance.

— **Anti-Spoofing Mode**: Optional. Enable the anti-spoofing mode for the VM instance.

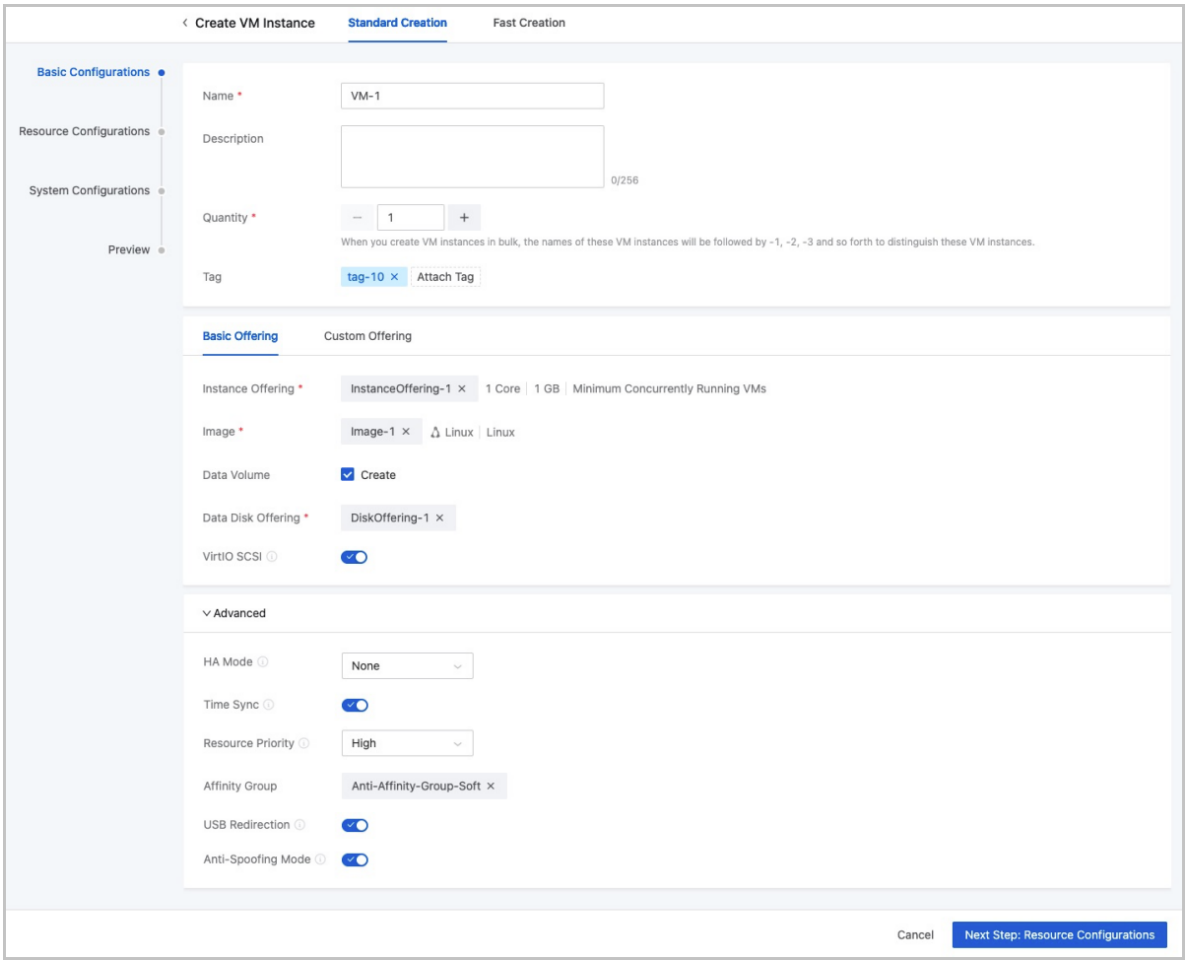
Note:

- This mode provides IP/MAC anti-spoofing and ARP anti-spoofing for the VM instance . If enabled, the VM instance can only communicate with outside networks by using the IP or MAC addresses allocated by the Cloud.
- You can set whether to enable the anti-spoofing mode globally by using the following method:

  Go to **Settings** > **Platform Setting** > **Global Setting** > **Basic** > **Resource Center** > **Resource Pool** > **VM Instance**, locate **IP/MAC Anti-Spoofing**, and enable or disable the switch as needed. Default: false.
- By default, the anti-spoofing mode of a single VM instance is strictly controlled by that in the global setting.

- If anti-spoofing is disabled in the global setting, you can enable it for a single VM instance on the VM details page.

Figure 7-3: Basic Configurations



2. Complete the resource configurations.

   Set the following parameters:

   - **Network Configurations**: Select an L3 network used by the VM instance and complete the network configurations.

     — **Network**: Select an L3 network used by the VM instance. Supported network types: public network, flat network, and VPC network.

     Note:

     When you select an L3 network, note that:

     - A VM instance can have multiple networks attached, and each L3 network corresponds to a NIC.

- If the selected L3 network has both an IPv4 and IPv6 address, the VM instance would have a dual-stack NIC. That is, the VM NIC has both an IPv4 and IPv6 address.
- Before you can create a VM instance by using an IPv6 or IPv4+IPv6 network, obtain the IP address by using **`dhclient -6 NIC_NAME`**.
- We recommended that you use only one IPv6 address for VM instances to avoid potential risks.

— **Make Default**: If you add multiple network configurations, set one of the networks as the default network.

— **Enable SR-IOV**: Optional. Choose whether to use SR-IOV to generate a VF NIC and pass it through to the VM instance.

- By default, SR-IOV is not enabled. In this case, the VM instance that you created will have a vNIC attached.
- If enabled, the VM instance that you created will have a VF NIC attached.

Note:

To enable SR-IOV, note that:

- Only IPv4 networks support SR-IOV, but IPv6 or IPv4+IPv6 networks do not.
- Make sure that SR-IOV is enabled for the L2 network corresponding to the L3 network of the VM instance. Otherwise, SR-IOV cannot be enabled.
- After SR-IOV is enabled, make sure that the physical NIC corresponded by the L3 network has an available VF NIC. Otherwise, the VM instance might fail to be created .
- If SR-IOV is enabled, NICs of the VM instances that were created by using a public network or a flat network do not support the network services such as security group and EIP. If the VM instances were created by using a VPC network, their NICs do not support the security group network services.

— **Assign IP**: Optional. Choose whether to assign an IP address to the VM NIC.

- The Cloud assigns an IP address to the VM instance by default.
- If you choose to assign an IP address to the VM instance, set the following parameters:
  - **Assign IPv4**: Assign an IPv4 address to the VM instance.

- **Assign IPv6**: Assign an IPv4 address to the VM instance.

Note:

- If you use the custom configuration, the Cloud assigns an IP address to the VM instance according to your configurations. In this case, pay attention to avoid IP address conflicts.
- If you create VM instances in bulk and choose to assign an IP address here, the Cloud automatically assigns IP addresses to these VM instances with the first assigned IP address as the start address. If an IP address is occupied or if IP addresses are insufficient within the continuously assigned IP range, the corresponding VM instance will fail to be created.

— **MAC Address**: Optional. Choose whether to configure a MAC address for the VM instance.

- By default, the Cloud assigns a MAC address to the VM instance.
- If you choose to configure a MAC address, set the following parameters:
  - **MAC Address**: Customize a MAC address for the VM instance.
-

Note:

- If you use the custom configuration, the Cloud assigns a MAC address to the VM instance according to your configurations. In this case, pay attention to avoid MAC address conflicts.
- If you create VM instances in bulk and choose to assign a MAC address here, the Cloud automatically assigns MAC addresses to these VM instances with the first assigned MAC address as the start address. If a MAC address is occupied within the continuously assigned MAC range, the corresponding VM instance will fail to be created.

— **Security Group**: Optional. Associate a security group with the VM instance.

The security group is used to better protect the VM instance by implementing access control in the group. You can customize access rules in the security group. These rules take effect immediately when the VM instance joins the security group. This protects the VM instance in real time.

— **EIP**: Optional. Associate an elastic IP address (EIP) with the VM instance.

Note:

This parameter does not appear if you selected a public network.

- **Cluster**: Optional. Specify a cluster for the host on which the VM instance is to be started.
- **Storage Allocation Policy**: Specify how the Cloud allocates a primary storage.

Note:

- System allocation: The Cloud allocates a primary storage according to the preconfigured policy.
- Manual allocation: You can select a primary storage as needed.

— If you select **System Allocation**, set the following parameters:

  - **Host**: Optional. Select the host on which the VM instance is to be started. If you specified a cluster, select a host from the cluster.
  - **vDrive**: Optional. Add a virtual drive (vDrive) for the VM instance.

    You can click **Add vDrives** to create more vDrives. Then, you can click **Select ISO** to attach an ISO to a vDrive.

    - — If you select a qcow2 image or raw image, the Cloud creates an empty vDrive by default. To delete a vDrive, click the delete icon next to the **vDrive** parameter.

      — If you select an ISO image, the Cloud creates a vDrive by default and attaches the ISO image to the vDrive. Note that this vDrive cannot be deleted here.
    - You can set the maximum number of vDrives for a VM instance after stopping the VM instance. The method is as follows:

      Go to **Settings** > **Platform Setting** > **Global Setting** > **Basic** > **Resource Center** > **Resource Pool** > **VM Instance**, locate **Maximum Virtual Drive**, and change its value as needed. Default: 3. Valid values: 1, 2, and 3.
  - **GPU**: Add a GPU device for the VM instance by specifying a GPU specification or device. The GPU device can be either a physical GPU (pGPU) or a virtual GPU (vGPU).

    - **Load GPU Specification**: Allocate a CPU device according to the selected specification when you create a VM instance.

- **Auto Detach GPU Device**: Choose whether to uninstall a GPU device automatically after the VM instance is stopped.
  - If a pGPU specification is used, this option is not selected by default. If a vGPU specification is used, this option is selected by default.
  - If selected, the GPU device will be automatically uninstalled after the VM instance is stopped. When the VM instance is restarted, a new GPU device will be allocated to the VM instance according to the GPU specification.
  - If not selected, the GPU device will be retained after the VM instance is stopped . When the VM instance is restarted, the existing GPU device will be used.
- **Load GPU Device**: Attach the GPU device you selected when you create a VM instance.

Note:

- You can attach multiple pGPU devices or only one vGPU device to a VM instance at a time.
- You cannot attach both pGPU and vGPU devices to a VM instance at the same time.
- You can attach GPU devices to a VM instance from the host where the VM instance is located. Currently, you cannot attach GPU devices to a VM instance across hosts.

- **CPU Pinning**: Specify the association between the pCPU of the host and the vCPU of the VM instance. Then, the Cloud allocates a pCPU to the VM instance accordingly. This helps to improve the VM performance.
  - You can click **Add CPU Pinning** to specify more CPU pinning policies.
  - Enter the vCPU range in the left text box and the pCPU range in the right. Note that the **-** symbol indicates the value range, while the **^** symbol indicates that a value is not included. If you specify multiple rules in a policy, separate each rule by using a comma (,). The following are some examples:
    - 0-2 indicates CPU 0, CPU 1, and CPU 2.
    - ^2 indicates that CPU 2 is not included.
    - 0-2,^2 indicates CPU 0 and CPU 1.
    - 1-7,^2,^3,^4,10 indicates CPU 1, CPU 5, CPU 6, CPU 7, and CPU 10.

Note:

- The vCPU range depends on the selected instance offering of the VM instance , while the pCPU range depends on the selected cluster or the number of pCPUs of the selected host.
- If a vCPU has multiple CPU pinning policies, the union of the policies is used.
- ZStack Cloud supports CPU overcommitment. Therefore, the number of vCPUs can be greater than that of pCPUs. However, if the number of vCPUs specified in the CPU pinning policy is greater than that of pCPUs, the VM performance will be affected. Therefore, CPU overcommitment is not recommended.
- You can modify the CPU pinning policy on the **Overview** tab page of a VM details page. The modification takes effect after you restart the VM instance.
- Cloning or migrating a VM instance also copies the CPU binding policy, while creating a VM image or performing VM backup does not.
- When you create a VM instance, the Cloud firstly checks the affinity group and host allocation strategies, and then checks the CPU pinning policy.
- When you power off a VM instance to modify its instance offering and reduce its CPU, the invalid CPU pinning policy will not take effect. In this case, we recommend that you modify or delete this policy.

— If you select **Manual Allocation**, set the following parameters:

- **Primary Storage**: Select a primary storage for the VM instance.
- - **Host**: Optional. Select the host on which the VM instance is to be started. If you specified a cluster, select a host from the cluster.
  - **vDrive**: Optional. Add a virtual drive (vDrive) for the VM instance.

    You can click **Add vDrives** to create more vDrives. Then, you can click **Select ISO** to attach an ISO to a vDrive.

    - — If you select a qcow2 image or raw image, the Cloud creates an empty vDrive by default. To delete a vDrive, click the delete icon next to the **vDrive** parameter.

— If you select an ISO image, the Cloud creates a vDrive by default and attaches the ISO image to the vDrive. Note that this vDrive cannot be deleted here.

- You can set the maximum number of vDrives for a VM instance after stopping the VM instance. The method is as follows:

  Go to **Settings** > **Platform Setting** > **Global Setting** > **Basic** > **Resource Center** > **Resource Pool** > **VM Instance**, locate **Maximum Virtual Drive**, and change its value as needed. Default: 3. Valid values: 1, 2, and 3.

- **GPU**: Add a GPU device for the VM instance by specifying a GPU specification or device. The GPU device can be either a physical GPU (pGPU) or a virtual GPU (vGPU).
  - **Load GPU Specification**: Allocate a CPU device according to the selected specification when you create a VM instance.
  - **Auto Detach GPU Device**: Choose whether to uninstall a GPU device automatically after the VM instance is stopped.
    - If a pGPU specification is used, this option is not selected by default. If a vGPU specification is used, this option is selected by default.
    - If selected, the GPU device will be automatically uninstalled after the VM instance is stopped. When the VM instance is restarted, a new GPU device will be allocated to the VM instance according to the GPU specification.
    - If not selected, the GPU device will be retained after the VM instance is stopped. When the VM instance is restarted, the existing GPU device will be used.
  - **Load GPU Device**: Attach the GPU device you selected when you create a VM instance.

Note:

- You can attach multiple pGPU devices or only one vGPU device to a VM instance at a time.
- You cannot attach both pGPU and vGPU devices to a VM instance at the same time.

- You can attach GPU devices to a VM instance from the host where the VM instance is located. Currently, you cannot attach GPU devices to a VM instance across hosts.

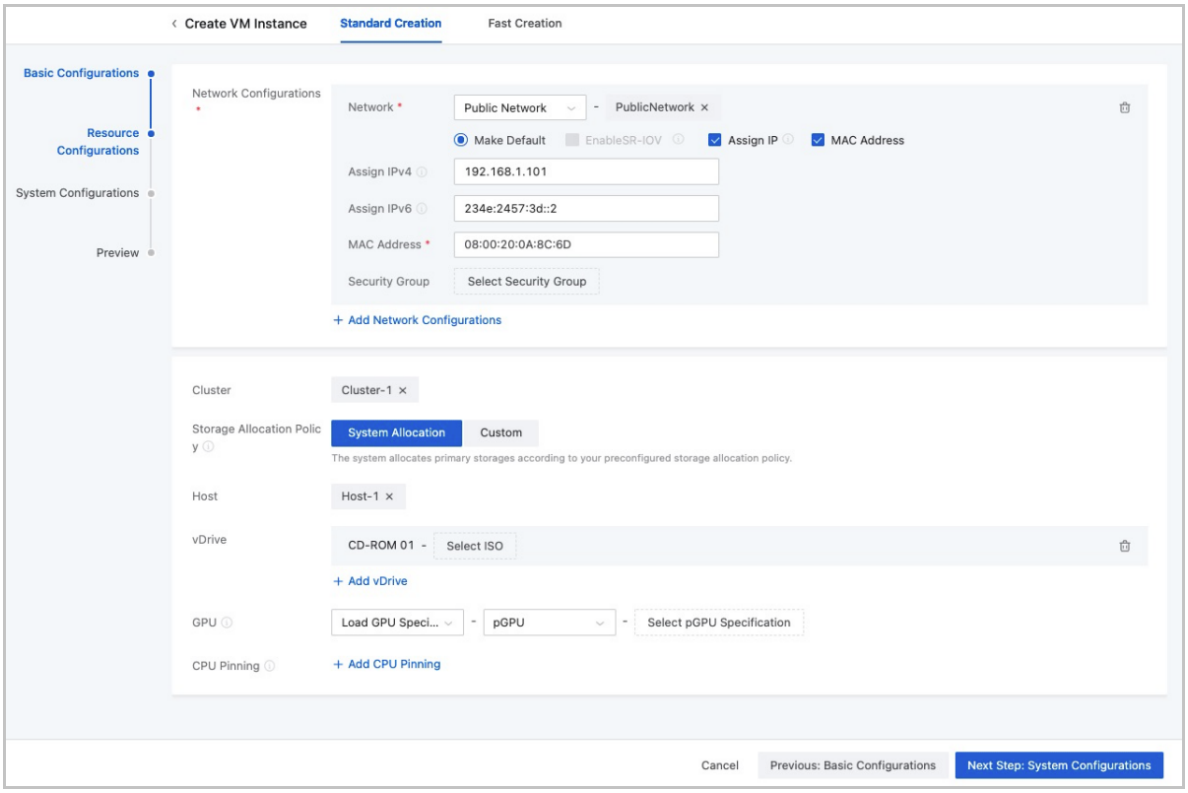
- **CPU Pinning**: Specify the association between the pCPU of the host and the vCPU of the VM instance. Then, the Cloud allocates a pCPU to the VM instance accordingly. This helps to improve the VM performance.
  - You can click **Add CPU Pinning** to specify more CPU pinning policies.
  - Enter the vCPU range in the left text box and the pCPU range in the right. Note that the **-** symbol indicates the value range, while the **^** symbol indicates that a value is not included. If you specify multiple rules in a policy, separate each rule by using a comma (,). The following are some examples:
    - 0-2 indicates CPU 0, CPU 1, and CPU 2.
    - ^2 indicates that CPU 2 is not included.
    - 0-2,^2 indicates CPU 0 and CPU 1.
    - 1-7,^2,^3,^4,10 indicates CPU 1, CPU 5, CPU 6, CPU 7, and CPU 10.

Note:

- The vCPU range depends on the selected instance offering of the VM instance, while the pCPU range depends on the selected cluster or the number of pCPUs of the selected host.
- If a vCPU has multiple CPU pinning policies, the union of the policies is used.
- ZStack Cloud supports CPU overcommitment. Therefore, the number of vCPUs can be greater than that of pCPUs. However, if the number of vCPUs specified in the CPU pinning policy is greater than that of pCPUs, the VM performance will be affected. Therefore, CPU overcommitment is not recommended.
- You can modify the CPU pinning policy on the **Overview** tab page of a VM details page. The modification takes effect after you restart the VM instance.
- Cloning or migrating a VM instance also copies the CPU binding policy, while creating a VM image or performing VM backup does not.
- When you create a VM instance, the Cloud firstly checks the affinity group and host allocation strategies, and then checks the CPU pinning policy.

- When you power off a VM instance to modify its instance offering and reduce its CPU, the invalid CPU pinning policy will not take effect. In this case, we recommend that you modify or delete this policy.

Figure 7-4: Resource Configurations



3. Complete the system configurations.

   Set the following parameters:

   - For Linux VM instances, you can log in to them by using an SSH key or a password.

     — **SH Public Key**: If you select this method, set the following parameters:

     - **SSH Public Key**: After an SSH key is injected to your VM instance, you can SSH in to the VM instance without entering a password when the VM instance is running.

     Note:

     - If cloud-init is installed in your VM image, you can log in to your VM instance by using an SSH public key or a password.
     - For more information, see *SSH Key Management*.

     — **Password**: If you select this method, set the following parameters:

- **Username**: The default username is root.
- **Password**: After a root password is injected to your VM instance, you can SSH in to the VM instance by entering a password when the VM instance is running.

Note:

- Before you set a password, make sure that Cloud-Init is installed for the VM image.
- If a VM instance runs CentOS, you can install Cloud-Init by running the `yum install cloud-init` command.
- After you set the password, do not set the it again via User Data to avoid conflicts of duplicate operations.
- After you set the password, a clear-text password is displayed on User Data of the VM details page. Remember to secure your password.

- For Windows VM instances, you can log in to them by using a password only when they are running.
  - **Username**: The default username is **administrator**.
  - **Password**: After a password is injected to your VM instance, you can log in to the VM instance by using the password when the VM instance is running.

Note:

- Before you set a login password, make sure that Cloudbase-Init is installed for the VM image. Recommended Cloudbase-Init version: 0.9.11.
- For more information about how to install Cloudbase-Init, see the *Cloudbase Documentation*.
- After you set the password, do not set the it again via User Data to avoid conflicts of duplicate operations.
- After you set the password, a clear-text password is displayed on User Data of the VM details page. Remember to secure your password.

- **Hostname**: Set a hostname for the VM instance.
  - The rules for setting Linux hostname and Windows hostname are different.
    - Linux hostname: The hostname must be 2 to 60 characters in length, and can be uppercase, lowercase, digits, and hyphens (-). Note that a hostname cannot contain consecutive hyphens (-) and cannot start or end with hyphens (-).

  - Windows hostname: The hostname must be 2 to 15 characters in length, and can be uppercase, lowercase, digits, and hyphens (-). Note that a hostname cannot contain consecutive hyphens (-), cannot start or end with hyphens (-), and cannot contain only digits.
- To set a hostname, make sure that the DHCP service of the corresponding L3 network is enabled.
- For Linux images, the hostname must be set to **localhost.localdomain**.
- After you set a hostname, do not set it again in User Data to avoid conflicts.

• **User Data**: Optional. Inject user-defined parameters or scripts to customize configurations for the VM instance or to accomplish specific tasks.

- Before you import user data, make sure that both the user data network service and DHCP network service work as expected.
- By default, the user data network service and DHCP network service in the flat network and VPC network environments are enabled.
- For Linux VM instances:
  - Before you inject user data, make sure that Cloud-Init is installed for the VM image. Recommended Cloud-Init versions: 0.7.9, 17.1, 19.4, 19.4, and later.
  - If you set a hostname and password by using the user data, do not set them again in **SSH Login Method** > **Password** to avoid conflicts.
  - If you create an Linux VM instance by using an image with Cloud-Init installed, you must import user data. Otherwise, the Cloud-Init task will wait until timeout.
- For Windows VM instances:
  - Before you import user data, make sure that Cloudbase-Init is installed for the VM image. Recommended Cloudbase-Init version: 0.9.11.
  - For more information about how to install Cloudbase-Init, see the *Cloudbase Documentation*.
  - If you set the login password/hostname in user data, do not set them again in the **Login Password** or **Hostname** input box. This helps avoid conflicts.
  - If you create a Windows VM instance by using an image with Cloudbase-Init installed, you must import user data. Otherwise, the Cloudbase-Init task will wait until timeout.
- After you set the login password in user data, a clear-text password is displayed on User Data of the VM details page. Remember to secure your password.

- If you use user data, note that you can configure only one L3 network for an L2 network.
- The following is an example of importing user data to a Linux VM instance.

```
#cloud-config
users:
 - name: test
   shell: /bin/bash
   groups: users
   sudo: ['ALL=(ALL) NOPASSWD:ALL']
   ssh-authorized-keys:
       - ssh-rsa AAAAB3NzaC1LXCJfjroD1lT root@10-0-0-18
bootcmd:
 - mkdir /tmp/temp
write_files:
 - path: /tmp/ZStack_config
   content: |
       Hello,world!
   permissions: '0755'
fqdn: Perf-test
disable_root: false
ssh_pwauth: yes
chpasswd:
  list: |
      root:word
  expire: False
runcmd:
 - echo ls -l / >/root/list.sh
```

The preceding script can do the following:

1. Create a user named test and use ssh-key when a VM instance is created.
2. Write the *`/etc/hosts`* file when the VM instance is started, create a directory named *`/tmp/temp`*, create a file, and write data to the file.
3. Set a hostname, enable the root user, enable SSH login with password, and change the root password.
4. Run the `echo ls -l /` command.

- The following is an example of importing user data to a Windows VM instance.

```
#cloud-config
write_files:
   -   encoding: b64
       content: NDI=
       path: C:\b64
       permissions: '0644'
   -   encoding: base64
       content: NDI=
       path: C:\b64_1
       permissions: '0644'
   -   encoding: gzip
       content: !!binary |
           H4sIAGUfoFQC/zMxAgCIsCQyAgAAAA==
       path: C:\gzip
```

```
        permissions: '0644'
```

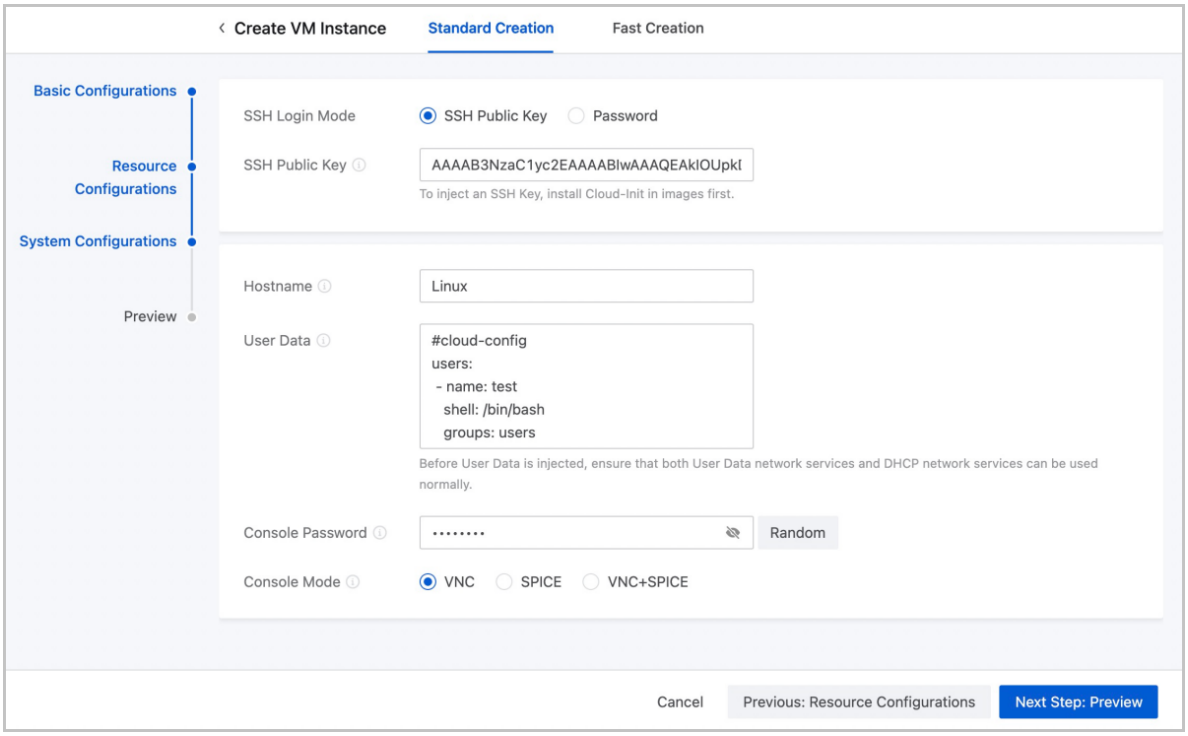
The preceding script can do the following:

- Create **b64**, **b64_1**, and **gzip** files under C drive when the VM instance is started.

- **Console Password**: Set a console password for the VM instance. The password must be 6 to 18 characters long.
- **Console Mode**: Set the console mode. Options: VNC, SPICE, and VNC+SPICE. Default: VNC.

> **Note:**
>
> - If not set, the console mode specified in the global setting will be used by default.
> - If you set one, the VM instance will use this mode by default.
> - If you change the console mode of a VM instance, reboot the VM instance to take effect.

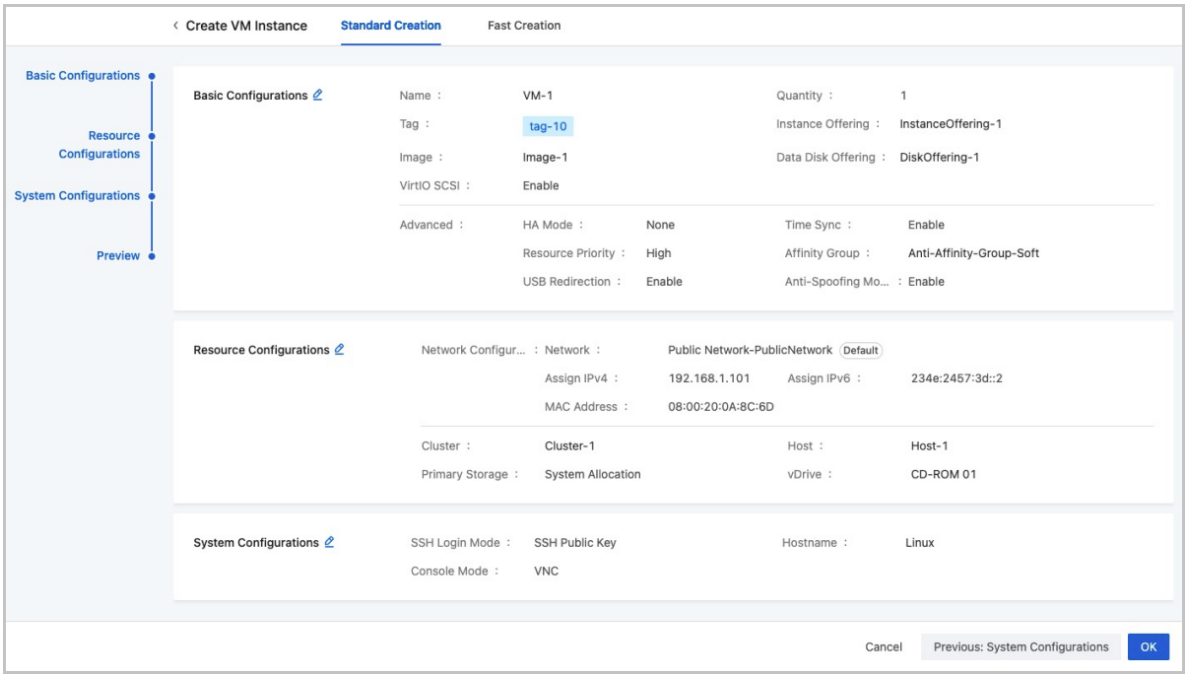
Figure 7-5: System Configurations



4. Confirm the information.

View the information about the VM instance. You can edit the information by clicking the **Edit** icon.

Figure 7-6: Confirm Information



Considerations

When you create a VM instance, note the following:

- — The image BIOS mode includes Legacy and UEFI. A VM instance inherits the BIOS mode of the image added to the VM instance.
  — You need to get the corresponding image ready, and select a proper BIOS mode.
  — You can change the BIOS mode on the VM details page. Exercise caution when you make any changes. The VM instance may fail to work properly if the BIOS mode does not match the VM instance. After you change the BIOS mode, restart the VM instance for the changes to take effect.
  — The Legacy mode is recommended when you create a VM instance. If you want to use the UEFI mode, we recommend that you select the corresponding image from the following list of operating system versions.

OS	BIOS Mode	Supported Versions
Windows	UEFI	• Windows 8 or later
	UEFI with CSM	• Windows 7 • Windows Server 2008 R2
Linux	UEFI	• CentOS 7.2

OS	BIOS Mode	Supported Versions
		• CentOS 7.3 • CentOS 7.4 or later

7.1.1.4 Manage a VM Instance

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Virtual Resource** > **VM Instance**. Then, the **VM Instance** page is displayed.

The following table lists the actions that you can perform on a VM instance.

Action	Description	VM State
Create VM Instance	Create one or more VM instances. The Cloud provides two creation methods: standard creation and fast creation .	/
Edit VM Instance	Edit the name and description of a VM instance.	Running/Stopped /Paused
Start VM Instance	Start a VM instance that is in the stopped state.	Stopped
Stop VM Instance	Stop a VM instance that is in the running state. **Note:** If the VM instance has HA enabled, you can make the VM instance not automatically reboot this time after being stopped.	Running
Reboot VM Instance	Reboot a VM instance that is in the running state.	Running
Restore VM Instance	Restore a VM instance that is in paused state.	Paused
Pause VM Instance	Pause a VM instance that is in running state. **Note:** Pausing a VM instance does not really stop the VM instance. However, stopping the host on which the paused VM instance is located will affect the business running.	Running
Force Stop VM Instance	Forcibly change the VM state from Unknown to Stopped. **Note:**	Unknown

Action	Description	VM State
	• Force stopping a VM instance might cause VM errors and crash. We recommend that you restore the host where the VM instance is located first. • Only admin and platform managers can force stop a VM instance.	
Power Off VM Instance	Power off a VM instance that is in the running state. **Note:** We recommend that you do not power off a VM instance in general scenarios.	Running
Launch Console	Launch the console of a VM instance. **Note:** • You can set the boot options for a newly-started VM instance by pressing **ESC** in the VM console. • If you could not launch the VM console, go to the **Console Proxy** page and change the IP address of the console proxy to the IP address of the current management node.	Running
Clone VM Instance	Clone a VM instance that has the same system as the current VM instance based on the VM instance offering. • If you clone the VM instance without attached volumes, note that: — Only the root volume of the VM instance will be cloned. — Supported backup storage types: ImageStore and Ceph. — ■ If the backup storage is ImageStore, the primary storage can be LocalStorage, NFS, SMP, Ceph , or SharedBlock. ■ If the backup storage is Ceph, the primary storage can be Ceph. ■ If the backup storage is Ceph+ImageStore, the primary storage can be Ceph+SharedBlock. — If you use any primary storages mentioned above, you can clone the VM instance when it is running, paused, or powered off.	Running/Stopped /Paused

Action	Description	VM State
	• If you clone the VM instance with attached volumes, note that: — Both the root volume and data volumes of the VM instance will be cloned. — Supported backup storage types: ImageStore and Ceph. — ■ If the backup storage is ImageStore, the primary storage can be LocalStorage, NFS, SMP, Ceph , or SharedBlock. ■ If the backup storage is Ceph, the primary storage can be Ceph. ■ If the backup storage is Ceph+ImageStore, the primary storage can be Ceph+SharedBlock. — If you use any primary storages mentioned above, you can clone the VM instance when it is running, paused, or powered off. — If the VM instance has a shared volume attached, the shared volume cannot be cloned. • When you clone a VM instance that uses a SharedBlock primary storage, select a provisioning method, including thick provisioning and thin provisioning. — Thick provisioning: Pre-allocates the required storage space and provides sufficient storage capacity to the VM instance to ensure the storage performance. — Thin provisioning: Allocates storage space to the VM instance according to the actual usage to achieve higher storage utilization. • When you clone a VM instance that uses a Ceph primary storage, you can specify a storage pool as needed. — When you clone a VM instance without the attached volumes, you can specify a Ceph pool (root volume pool). — For VM instances that use an ImageStore or a Ceph backup storage, when you clone a VM instance with attached volumes, you can specify a data volume pool and a root volume pool.	

Action	Description	VM State
	• You can specify whether to power off the newly cloned VM instances after cloning. • When you clone a VM instance, you can set a storage allocation policy, including system allocation and manual allocation. — System allocation: The system allocates a primary storage according to the preconfigured policy. — Manual allocation: You can manually select a primary storage. **Note:** • Cloning VM instances online clones only the data written to the disks at the beginning of the cloning jobs. The real-time cached data is not cloned. • To ensure data integrity, we recommend that you pause or power off high I/O VM instances before performing the cloning action. • The VM configuration, installation program, password, and other information, excluding the tags and scheduled jobs, will be copied to the newly cloned VM instance. • For the newly cloned VM instance, you need to reboot it to make the console password take effect. • If your environment has a LocalStorage and other types of primary storage, once the LocalStora ge primary storage is unavailable, you could not successfully create VM instances by using the system allocation policy. In this case, we recommend that you manually select an available primary storage for the root volume. • When you clone a VM instance, avoid setting a static IP address for the source VM instance. Otherwise , login errors might occur because multiple VM instances share the same IP address.	
Attach Tag to VM Instance	Attach tags to a VM instance. • The Cloud provides two types of tags: admin tag and tenant tag. — Admin tags are created and owned by admins (administrators and platform managers).	Running/Stopped /Paused

Action	Description	VM State
	— Tenant tags are created and owned by tenants (sub-accounts and projects). • Tag owners cannot be changed. • A tenant can attach tenant tags to resources belonging to the tenant. An admin can attach any tags to any resources. • Relationship between tenants and tags: — A sub-account can see and perform operations on tags belonging to the sub-account. — Tags in a project belong to the project, and everyone in the project (project admin/project manager/project member) can perform operations on these tags. — Tenants cannot perform operations on admin tags. • Relationship between admins and tags: — Admins can see and perform operations on both admin tags and tenant tags. — For example, an admin can detach or delete tenant tags. **Note:** • The Cloud now supports up to 50 tags per resource and an unlimited number of resources per tag. • You can attach multiple tags to multiple resources. • Tags can be sorted in order according to the creation time or tag name (priority: characters > numbers > Chinese characters > English characters). By default, tags are sorted in order by tag name. You can change the sort order in the global setting by changing the value of **Tag Sort Method**. • After the Cloud is seamlessly upgraded, existing tags are automatically updated and displayed in the latest way.	
Detach Tag from VM Instance	Detach tags from the VM instance. **Note:** • Changing a resource owner detaches the tenant tags on the resource. Admin tags are not affected.	Running/Stopped /Paused

Action	Description	VM State
	• You can detach tags from a resource in bulk or detach resources from a tag in bulk. • Tenants can only detach tags on the resources of these tenants, and administrators can detach tags on all resources.	
Migrate VM Instance	Migrate a VM instance to the other node. • Hot migration: — Migrate a VM instance that is in the running state. This action mainly copies the CPU register status and memory information. — Supported primary storage types: LocalStorage, NFS, SMP, Ceph, and SharedBlock. — If the VM instance uses a LocalStorage primary storage, you could not hot migrate the VM instance with data volumes. In this scenario, perform the hot migration by following these steps: **1.** In the Global Setting, enable **Live Migration in Local Storage**. **2.** Detach the data volumes attached to the VM instance. **3.** Migrate the VM instance and data volumes to other nodes, respectively. **4.** Attach the detached data volumes to the VM instance again. — Windows-based VM instances on LocalStorage primary storages cannot be hot migrated. — If a VF NIC is attached to a VM instance, before you hot migrate the VM instance, detach the VF NIC from the VM instance. — If a VM instance is on primary storage of the LocalStorage type or a shared storage type,you can hot migrate the VM instance. — If a VM instance is attached a block device and deployed as the master node of a Windows fail-over cluster, hot migrating the VM instance may	Running/Stopped

Action	Description	VM State
	make the fail-over cluster become unavailable. Proceed with caution. — If the migration is blocked because the VM instance has high I/O operations for a long time, you can enable auto converge to ensure the migration is successful. ■ You can enable auto converge for all VM instances in the Cloud. Method: In the Global Setting, enable **Auto Converge**. ■ You can also enable auto converge for a single VM instance. By default, this setting complies with that in the Global Setting. **Note:** If your applications are performance sensitive, we recommend that you do not enable auto converge. • Cold migration: — Migrate a VM instance that is in the stopped state. — Supported primary storage type: LocalStorage. — If the VM instance uses a LocalStorage primary storage, you could not cold migrate the VM instance with data volumes. — To perform a cold migration, follow these steps: **1.** Stop the VM instance. **2.** Detach the data volumes from the VM instance. **3.** Migrate the VM instance and data volumes to other nodes, respectively. **4.** Attach the detached data volumes to the VM instance again. — You can cold migrate VM instances that are on LocalStorage primary storage and are attached vDPA NICs. • You can migrate VM instances based on the workloads of the destination compute node. — In the list of recommended destination compute nodes, you can sort the destination compute nodes by the average CPU utilization or memory utilizatio	

Action	Description	VM State
	n. By default, the compute nodes are sorted by the average memory utilization in ascending order. — If the scale of compute nodes in the cluster is large , you can sort the top 20 or top 50 compute nodes. **Note:** • Before you hot or cold migrate a VM instance, detach the data volumes, ISOs, or peripheral devices (if any) from the VM instance first. • The migration speed is related to the network configuration of the source and destination compute nodes. Low network configuration might cause lower migration speed.	
Storage Migration	Cold or hot migrate a VM instance across primary storages or within the same primary storage. • **Cold/Hot Migration Across Primary Storages** **1.** Cold migration across primary storages of the same type: You can cold migrate a VM instance across primary storages of the same type, including Ceph↔Ceph, NFS↔NFS, and SharedBlock↔SharedBlock. **Note:** • Ceph↔Ceph: — Before you cold migrate a VM instance across Ceph primary storages, you must power off the VM instance and detach all data volumes from the VM instance. — Make sure that the monitor nodes of these two Ceph primary storages can communicate with each other. — You can specify a root volume pool for the destination primary storage. • NFS↔NFS: — Before you cold migrate a VM instance across NFS primary storages, you must	Running/Stopped

Action	Description	VM State
	power off the VM instance and detach all data volumes from the VM instance. — The destination NFS primary storage can be attached to the cluster where the VM instance to be migrated is located. • SharedBlock↔SharedBlock: — Before you cold migrate a VM instance across SharedBlock primary storages, you must power off the VM instance. — You can migrate the VM instance with all attached volumes. — If a shared volume is attached to the VM instance, the shared volume cannot be migrated. — The destination SharedBlock primary storage can be attached to the cluster where the VM instance to be migrated is located. • The network configurations of the cluster to which the destination primary storage is attached can satisfy the network requirements of the VM instance. **2.** Hot migration across primary storages of the same type: You can hot migrate a VM instance across primary storages of the same type, including Ceph↔Ceph, NFS↔NFS, and SharedBlock↔SharedBlock. **Note:** • You can only implement entire VM migration across primary storages. • If a shared volume is attached to the VM instance, the shared volume cannot be migrated. • Snapshots of the VM instance to be migrated will not be saved after the hot migration. • The network configurations of the cluster to which the destination primary storage is	

Action	Description	VM State
	attached can satisfy the network requirements of the VM instance. • Before you hot migrate a VM instance across Ceph primary storages, make sure that the monitor nodes of these two Ceph primary storages can communicate with each other. • If you hot migrate a VM instance across Ceph primary storages, you can specify a root volume pool and data volume pool for the destination primary storage. • Before you hot migrate a VM instance across primary storages, make sure that the VF NICs , if any, are detached from the VM instance. **3.** Hot migration across primary storages of different types: You can hot migrate a VM instance across primary storages of different types, including Ceph↔SharedBlock, LocalStorage↔SharedBlock, LocalStorage↔Ceph, LocalStorage↔NFS, SharedBlock↔NFS, and Ceph↔NFS. **Note:** • You can only implement entire VM migration across primary storages. • If a shared volume is attached to the VM instance, the shared volume cannot be migrated. • Snapshots of the VM instance to be migrated will not be saved after the hot migration. • The network configurations of the cluster to which the destination primary storage is attached can satisfy the network requirements of the VM instance. • If you hot migrate a VM instance from a SharedBlock, Localstorage, or an NFS primary storage to a Ceph primary storage, you can specify a root volume pool and data volume pool for the destination primary storage.	

Action	Description	VM State
	• Before you hot migrate a VM instance across primary storages, make sure that the VF NICs , if any, are detached from the VM instance. • **Cold/Hot Migration Within the Same Primary Storages** **1.** If a VM instance uses a Ceph primary storage, you can cold or hot migrate the VM instance across Ceph pools within the Ceph primary storage. **2.** Before you cold migrate a VM instance, note that: • You must power off the VM instance and detach all data volumes from the VM instance. • You can only implement entire VM migration across Ceph pools. • If a shared volume is attached to the VM instance, the shared volume cannot be migrated . **3.** Before you hot migrate a VM instance, note that: • You can migrate only the root volumes or implement entire VM migration. • If a shared volume is attached to the VM instance, the shared volume cannot be migrated . • Snapshots of the VM instance to be migrated will not be saved after the hot migration. **Note:** Before you migrate a VM instance, detach the ISOs, LUNs, or peripheral devices (if any) from the VM instance first.	
Modify Instance Offering	Modify the instance offering of a VM instance. **Note:** After the modification, only the CPU, memory, and host allocation policy in the new instance offering take effect for the VM instance. • You can modify the instance offering of Linux VM instances when they are running or powered off.	Running/Stopped

Action	Description	VM State
	— To modify the instance offering of a running VM instance, follow these steps: 1. Open **NUMA**. • You can enable NUMA for all VM instances in the Cloud. Method: In the Global Setting, enable **NUMA**. • You can also enable NUMA for a single VM instance. By default, this setting complies with that in the Global Setting. 2. Restart the VM instance. 3. Modify the instance offering of the VM instance. **Note:** When you modify the instance offering of a running VM instance, make sure that the new CPU core count and memory size are greater than the current one. • You can also modify the instance offering of Windows VM instances when they are running or powered off. The method is the same as that of Linux VM instances. **Note:** We recommend that you do not modify the number of CPU cores and memory size of a Windows VM instance in the production environment.	
Set GPU Specification	Set the GPU specification of a VM instance. • **Set pGPU specification**: Attach or modify the physical GPU (pGPU) specification of a VM instance. — You cannot set the pGPU specification for a running VM instance. — After you modify the pGPU specification of a VM instance, the next time the VM instance starts, the VM instance attaches pGPU devices by using the latest pGPU specification. Meanwhile, the pGPU devices related to the original pGPU specification will be detached.	Stopped

Action	Description	VM State
	— When you set the pGPU specification, you can enable or disable the **Auto Detach GPU Device** mechanism as needed. ■ By default, **Auto Detach GPU Device** is disabled. That is, the attached pGPU devices still exist after the VM instance is powered off. ■ If enabled, the VM instance automatically detaches the attached pGPU devices (if any) after the VM instance is powered off. • **Set vGPU specification**: Attach or modify the virtual GPU (vGPU) specification of a VM instance. — You cannot set the vGPU specification for a running VM instance. — After you modify the vGPU specification of a VM instance, the next time the VM instance starts, the VM instance attaches vGPU devices by using the latest vGPU specification. Meanwhile, the vGPU devices related to the original vGPU specification will be detached. — When you set the vGPU specification, you can enable or disable the **Auto Detach GPU Device** mechanism as needed. ■ By default, **Auto Detach GPU Device** is enabled. That is, the VM instance automatically detaches the attached vGPU devices (if any) after the VM instance is powered off. ■ If disabled, the attached vGPU devices still exist after the VM instance is powered off. • **No set**: The VM instance does not load GPU specifications. — In this case, VM instances without a GPU specification attached do not attach other GPU specifications, and VM instances with GPU specifications attached will detach these GPU specifications. — You cannot detach GPU specifications for a running VM instance.	
Resize Root Volume	Expand the root volume of a VM instance.	Running/Stopped

Action	Description	VM State
	• You can expand the root volume of a VM instance when the VM instance is running or stopped. The new size takes effect immediately. • The new size must be larger than the current size. The increment must be equal to or larger than 4 MB. Unit: MB, GB, and TB. • The new size must be a multiple of 4 MB. For example, if you enter a size of 37 MB, the actual size is 40 MB. • You can specify whether to automatically create a snapshot of the VM root volume upon resizing for all VM instances in the Cloud. Method, in the Global Setting, enable **Snapshot Auto-Creation upon Volume Resizing**. • The setting of a single VM instance complies with that in the Global Setting.	
Change Owner	Change the owner of a VM instance. **Note:** Changing a VM owner detaches all of the tenant tags on this VM instance. Admin tags are not affected.	Running/Stopped
Change System	Change the system of a VM instance. • Before you change the system, stop or power off the VM instance first. The new system takes effect after the VM instance reboots. • Make sure that the type of the destination image is Image. **Note:** • Changing the operating system expunges root volume. Please back up the root volume data to avoid data loss. • If the VM instance has a data volume attached, changing the operating system across platforms may cause the partition format of the data volume unable to be correctly identified.	Stopped
Reimage VM Instance	Restore a VM instance to the initial state of the VM image and overwrite all the data in the root volume.	Stopped

Action	Description	VM State
	• Before you reimage a VM instance, stop or power off the VM instance first. The action takes effect after the VM instance reboots. • VM instances created by using ISO cannot be reimaged. **Note:** Please back up the original root volume data in advance to avoid loss.	
Set Boot Order	Set the boot order for a VM instance. • This setting takes effect after the VM instance reboots . • If a VM instance is created from an ISO image, the VM instance boots from CD ROM after creation. • If you attach an ISO to an existing VM instance, the default boot order is as follows: **1.** First boot order: Hard disk **2.** Second boot order: CD ROM • If you want the VM instance boot from network, set the first boot order to Network. • If you set the first boot order of a running VM instance to CD ROM or Network, the setting takes effect only after you reboot the VM instance or start the VM instance after you stop it. If you reboot the VM instance by using the **`reboot`** command, the VM instance still boots from Hard Disk next time.	Running/Stopped
Boot from Host	Specify a host on which a VM instance boots. • After you stop a VM instance that uses a shared storage, you can specify a host on which the VM instance boots. • After you stop a VM instance that uses a LocalStora ge primary storage, the VM instance can boot only from the host where the VM root volume is located.	Stopped
Set VM HA	Set the high availability (HA) policy of a VM instance. • VM HA policies: — None: Disables VM HA. — NeverStop: Enables VM HA.	Running/Stopped

Action	Description	VM State
	• When a VM instance is shut down due to planned maintenance or exceptions, the VM HA policy can trigger automatic VM reboot to improve the VM availability. • If hosts are running properly, VM instances with HA enabled can reboot automatically in case of an abnormal shutdown. • If hosts are abnormal or enter the maintenance mode , VM instances using a LocalStorage primary storage and with HA enabled can reboot automatically in case of an abnormal shutdown. • If hosts are abnormal or enter the maintenance mode , VM instances using a shared storage and with HA enabled can reboot automatically in case of an abnormal shutdown. • You can set whether to enable HA for all VM instances in the Cloud. Method: In the Global Setting, enable **VM HA**. • If a VM instance has HA enabled, you can make the VM instance not automatically reboot this time after being stopped.	
Set Time Sync	Set whether the base time of a VM instance is the same as that of the host. By default, these two times are the same. **Note:** • If you enable time synchronization for a running Windows VM instance, the VM time is synchronized with the host time automatically on a regular basis. • If you enable time synchronization for a stopped or paused Windows VM instance, the setting takes effect after the VM instance reboots. • If you disable time synchronization for a Windows VM instance, the VM time is not synchronized with the host time. • The time synchronization setting does not take effect on Linux VM instances. • You can enable time sync in Global Setting for all Windows VM instances on the cloud. To enable time	Running/Stopped /Paused

Action	Description	VM State
	sync in Global Setting, set VM Time Sync to Sync. By default, the time sync global setting is disabled. • If you specifically set time sync for the VM instance, the VM Time Sync global setting does not take effect on the VM instance.	
Set Error Policy	Set the error policy for a VM instance, including error inspection and error handling. • Error inspection — You can enable error inspection for a running VM instance. ■ By default, error inspection is disabled. If enabled, reboot the VM instance to make the setting take effect. Note that you cannot reboot the VM instance through the VM console. ■ After you enable error inspection, if a VM instance crashes, the system automatically handles the error based on the specified error handling policy. In addition, the VM Crash alarm is triggered. ■ You can view the error alarms of the VM instance on the **Alarm Message** page. ■ You can also customize the **VM Crashed** alarm as needed. — You can enable error inspection for all VM instances in the Cloud. Method: In the Global Setting, enable **Error Inspection**. — You can also enable error inspection for a single VM instance. Then, the VM instance is not affected by the setting in the Global Setting. **Note:** • Before you enable error inspection for a VM instance, make sure that the VM instance has the latest version of GuestTools installed and the GuestTools is in the running state. • If you enable error inspection for a Linux-based VM instance, the kdump module is disabled after you reboot the instance. • Error handling	Running

Action	Description	VM State
	— After you enable error inspection, you can set an error handling policy for the VM instance. Supported policies: ■ Preserve: Errors occurred on a VM instance, such as blue screen of a Windows-based VM instance or Linux VM instance crash, are not handled. ■ Reboot: After a VM error occurs, such as blue screen of a Windows-based VM instance or Linux-based VM instance crash, the VM instance reboots automatically. ■ If the number of reboots reaches the threshold and the VM instance does not reboot successfully within the specified time, the VM instance does not reboot again. ■ You can set the **Restart Policy Upon Error** in the Global Setting. By default, the VM instance reboots up to five times within 30 minutes. If the VM instance is not rebooted after five attempts within 30 minutes, the VM instance remains crashed. ■ Shutdown: After a VM error occurs, such as blue screen of a Windows-based VM instance or Linux-based VM instance crash, the VM instance shuts down automatically. — The error handling policy takes effect immediately without the need of rebooting the VM instance. — You can set the error handling policy for all VM instances in the Cloud. Method: In the Global Setting, enable **Error Inspection** and set an error handling policy as needed. — You can also set the error handling policy for a single VM instance. This setting is not affected by that in the Global Setting. **Note:** • If you pause or stop a VM instance, the GuestTools on the VM instance will be stopped . In this case, you cannot set the error handling policy for the VM instance.	

Action	Description	VM State
	• If you restore a paused VM instance, start a stopped VM instance, or reboot a running VM instance, the GuestTools on the VM instance will be rebooted automatically. In this case, you can set the error handling policy for the VM instance . Note that some delays might occur during the starts or reboots.	
Set SSH Key	Set the SSH key for a VM instance, including injecting an SSH key, change an SSH key, or delete an SSH key. • After you inject an SSH key into a VM instance, you can SSH to the VM instance without a password when the VM instance is running. • Currently, SSH keys are injected by using cloud-init. Therefore, before you inject an SSH key, install cloud-init on the VM image first. • If you inject an SSH key when you create a VM instance, the SSH key takes effect after the VM instance starts for the first time. • If you inject an SSH key into an existing VM instance , reboot the VM instance to make the SSH key take effect. • If you inject an SSH key into a VM instance that already has an SSH key, run the `rm -rf /var/lib/cloud/instances` command to clear the previous configurations and inject the SSH key again. Then, reboot the VM instance to make the new SSH key take effect. • Deleting an SSH key only deletes the SSH key information recorded in the system. The SSH key information injected into the VM configuration is not deleted. If you need to completely delete the SSH key information, manually clean up the VM configuration file *`/root/.ssh/authorized_keys`*. • For more information about SSH key, see *SSH Key Management*.	Running/Stopped
Change VM Password	Change the username or password of a VM instance. • You can change the VM username or password when the VM instance is running. The change takes effect immediately.	Running

Action	Description	VM State
	• Before you change the password of a VM instance, make sure that: — The VM instance is running. — The VM instance has a QEMU guest agent (QGA) installed, and the QGA is running properly. In addition, make sure that the QGA is enabled on the VM details page. • You can change the password of VM instances that are created from the following images: — CentOS 7.x/6.x (32 bit/64 bit) — Ubuntu 16.x/15.x/14.x/13.x/12.x (64 bit) — Windows 2003/2008/7/10/2012/2016 (64 bit) **Note:** • If you fail to change the password of a VM instance, check whether the VM instance has a QGA installed , and then enter the terminal to manually check whether the QGA running status is normal. • If you can change the password of a VM instance, you can also change the password of the images of the VM instance or the cloned VM instances.	
Set VM Console Password	Set a console password or cancel the console password for a VM instance. • After you set or cancel a console password, reboot the VM instance to make the setting take effect. • The password is the VNC protocol password, not the password of the VM instance. • You can set the console password strength for all VM instances in the Cloud. Method: In the Global Setting, enable **VNC Console Password Strength Policy**, and set the password strength. — The default password length is 6 to 8 characters . A console password can contain at least 6 characters and at most 32 characters. — A console password can contain a combination of digits, letters, and special characters.	Running/Stopped

Action	Description	VM State
	• The console password strength policy of a single VM instance complies with that specified in the Global Setting.	
Toggle Console Mode	Toggle the console mode of a VM instance. The console mode includes VNC, SPICE, and VNC+SPICE. • The toggle action takes effect after the VM instance reboots. • You can set the console mode for all VM instances in the Cloud. Method: In the Global Setting, edit **Console Mode**. Default: VNC. • You can also set the console mode for a single VM instance. This setting is not affected by that specified in the Global Setting.	Running/Stopped /Paused
Set RDP Mode	Set the RDP mode for the VDI UI. Then, the VM console is opened in the RDP mode.	Running/Stopped /Paused
Resource Priority	Set the resource priority for a VM instance. • Options: Normal and High. Default: Normal. • When resource contention occurs due to high host workloads, VM instances with **High** resource priority can compete for more resources than those with **Normal** resource priority. **Note:** • We recommend that you set Resource Priority to High only for vital VM instances. • VPC vRouters have higher resource priority than VM instances. • When resource contention occurs, the resource priority is as follows: VM instances with **Normal** priority < VM instances with **High** priority < VPC vRouters. • For example, when resource contention occurs due to high host workloads, VPC vRouters can compete for more CPU resources than VM instances. • If you use the performance-dedicated load balancing service, the corresponding load balancer instances have the same resource priority as the VPC vRouters.	Running/Stopped /Paused

Action	Description	VM State
Cross-Cluster HA Policy	Set the cross-cluster HA policy for a VM instance. • By default, this policy is enabled, indicating that the VM instance can be automatically migrated across clusters. • If disabled, the VM instance can only operate in the cluster where the VM instance resides when this policy takes effect. • Background: — In versions earlier than 3.8.0, when the VM HA policy is triggered or the host enters maintenanc e mode, the system automatically restores or migrates the VM instance on/to the other host. The host might be selected from other clusters if these clusters attached the same L3 networks and storages. — From 3.8.0, you can set the cross-cluster HA policy for a VM instance. If the policy is disabled, the VM instance can only operate in the cluster where the VM instance resides when this policy takes effect. • Currently, this policy applies to host migration scenarios such as starting up a VM instance on another host to achieve HA or migrating a VM instance to another host if the source host enters the maintenance mode. • This policy takes effect only for VM auto-migrations . Other actions, such as manual hot migration, VM startups on specified hosts, and Dynamic Resource Scheduling (DRS) policy-based migrations are not affected. • If enabled, VM instances will not be stuck to a specified cluster.	Running/Stopped /Paused
USB Redirection	Set USB redirection for a VM instance. • If you need the VDI feature, you can redirect the USB device on the VDI client to a VDI VM instance. • The redirection action supports multiple USB devices. • To make the redirection take effect, reboot your VM instance.	Running/Stopped /Paused

Action	Description	VM State
Create Snapshot	Create a snapshot for a VM instance. • Before you perform a business-sensitive operation on a VM instance, you can schedule snapshot creation at specified time points to record the state of the root volume or data volume of the instance. This allows rollback in case of breakdowns. • You can create a single snapshot or snapshot group. — Single snapshot: Create a snapshot for the root volumes of the VM instance. — Snapshot Group: Create a snapshot for both the root volumes and data volumes of the VM instance. **Note:** • In the production environment, we recommend that you create no more than five snapshots for a volume. Too many snapshots will lower the VM performance, increase data security risks, and occupy storage space of the primary storage. To back up data for the long term, you can use a backup service. • In the production environment, to ensure data integrity, we recommend that you do not create snapshots for high I/O VM instances. If you create snapshots for a VM instance with I/O, some data in the memory might fail to be saved to the hard disk and thus cannot be saved in the snapshot.	Running/Stopped/Paused
Create Backup	Create a backup for a VM instance. • Before you create a backup for a VM instance, make sure that the VM instance is in the running state. • You can create a full backup or an incremental backup for a VM instance. • You can create a backup for a VM instance with its volumes. • You cannot create a backup for a VM instance with its shared volumes (if any). • Before you create a backup, add a local backup service to the Cloud in advance.	Running

Action	Description	VM State
	• You can synchronize the backup data to a remote backup server. Note that you need to add a remote backup server to the Cloud in advance.	
Attach Volume	Attach an available data volume to a VM instance. **Note:** • You can attach up to 24 data volumes to a VM instance. • In the LocalStorage scenarios, the VM instance and the volume to be attached must be on the same host . If not, migrate the volume to the host where the VM instance is located and then attach the volume to the VM instance. • To attach a VirtIO volume to a VM instance, make sure that the VM instance has the VirtIO driver installed. — Mainstream Linux distributions such as CentOS 6 and CentOS 7 are integrated with VirtIO drivers. Therefore, you do not need to install them again. — For Windows-based VM instances, you need to install VirtIO drivers manually. — If the owner of the volume is different from the owner of the instance and you attach the volume to the instance, the VM instance may become invisible to the tenant, which makes the tenant unable to manage the VM instance.	Running/Stopped
Detach Volume	Detach a volume from a VM instance. **Note:** Detaching a volume interrupts the data reads/writes of the volume and might affect the business continuity. Please exercise caution.	Running/Stopped
Create Image	Create a template image based on a VM instance so that you can create VM instances in bulk in a custom way. • To ensure application integrity, we recommend that you power off the VM instance before you create a VM image.	Running/Stopped

Action	Description	VM State
	• You can create either a system image or a volume image.	
Attach ISO	Attach an ISO for a VM instance. • The ISO will be attached in the sequence of the virtual drive name of the VM instance. • By default, a VM instance can attach up to three ISOs . Bulk attach is not supported. • You can set the maximum number of virtual drives that can be attached to all VM instances in the Cloud. Method: In the Global Setting, set the value of **Maximum Virtual Drive**. Valid values: 1, 2, and 3. • The maximum number of virtual drives that can be attached to a single VM instance is controlled by the setting in the Global Setting. **Note:** If the number of virtual drives attached by a VM instance exceeds the setting in the Global Setting, the Global Setting does take effect for this VM instance.	Running/Stopped
Detach ISO	Detach an ISO from a VM instance. **Note:** Detaching an ISO from a running VM instance might affect the business continuity. Please exercise caution.	Running/Stopped
Associate Affinity Group	Associate an affinity group with a VM instance. Then, the affinity policy takes effect for the VM instance immediatel y.	Running/Stopped
Disassociate Affinity Group	Disassociate an affinity group from a VM instance. Then, the affinity policy does not take effect for the VM instance any more.	Running/Stopped
Delete VM Instance	Deleting a VM instance releases the associated CPU, memory, and IP address. By default. the deleted VM instance is displayed on the Recycle Bin tab. • By default, a VM instance in the recycle bin is expunged 7 days after the deletion. • You can set a deletion for all VM instances in the Cloud. Method: In the Global Setting, set **Instance Deletion Policy**. Options:	Running/Stopped /Paused

Action	Description	VM State
	— Direct: If you delete a VM instance, the VM instance is deleted at once. — Delay: If you delete a VM instance, the VM instance is marked as deleted and listed on the Recycle Bin tab. The default retention period of deleted VM instances is 7 days. When the retention period expires or if you expunge a deleted VM instance, the VM instance is completely deleted. — Never: If you delete a VM instance, the system does not automatically expunge the deleted VM instance. **Note:** You can delete a VM instance with its all attached classic volumes except for shared volumes.	
Expunge/Recover VM Instance	You can completely delete or recover a VM instance in the recycle bin. • Expunging a VM instance also expunges resources associated with the VM instance. This operation is irreversible. Please exercise caution. • After a VM instance is expunged, its IP address will be returned to the IP address pool. • After a VM instance is recovered, the VM instance is displayed on the **Available** tab and is in the stopped state. You can choose whether to boot the VM instance after its recovery as needed. • After a VM instance is recovered, the Cloud allocates a new IP address to the VM instance again.	Deleted

7.1.1.5 VM Details

7.1.1.5.1 VM Configurations

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Virtual Resource** > **VM Instance**. On the **VM Instance** page, click on the name of a VM instance. Then, the details page of the VM instance is displayed. Click on the **Configuration Info** tab page. Then, the **Configuration Info** tab page is displayed.

The **Configuration Info** tab page displays the configuration information about the VM instance in the form of a list.

Volume

This section displays a list of root volumes and data volumes attached to the VM instance. You can perform operations on these volumes as needed.

NIC

This section displays a list of NICs attached to the VM instance. You can perform operations on these NICs as needed. The following table lists the actions that you can perform on a NIC.

Action	Description	VM State
Attach NIC	Attach a NIC to the VM instance. • You can set a default network for the VM instance. • You can enable SR-IOV for the VM instance. If enabled, the VM instance will have a VF NIC attached . If not enabled, the VM instance will have a vNIC attached. • You can attach a VDPA NIC to a VM instance. • You can set an IPv4 or an IPv6 address for the NIC. **Note:** • To enable SR-IOV, note the following: — Only IPv4 networks support SR-IOV. IPv6 and IPv4+IPv6 networks do not support SR-IOV. — Make sure that SR-IOV is enabled on the L2 network corresponding to the selected L3 network . Otherwise, you cannot enable SR-IOV here. — Make sure that the physical NICs on the corresponding L3 network have available VF NICs. Otherwise, you might fail to enable SR-IOV . — If the VM instance is using a public network or flat network, the VM NIC does not support security groups and elastic IP addresses after SR-IOV is enabled. — If the VM instance is using a VPC network, the VM NIC does not support security groups after SR-IOV is enabled. • If you attach vDPA NIC to a VM instance, note that:	Running/Stopped

Action	Description	VM State
	— Before you use vDPA NIC, make sure: ■ Network acceleration support is enabled for the associated cluster. ■ The L2 network attached to the cluster uses the OVS-DPDK vSwitch. ■ Hosts in the cluster have smart NICs of the specified model. Supported model includes Mellanox CX-5. ■ SR-IOV is enabled in the BIOS. — You can attach vDPA NICs only to VM instances that are in IPv4 VPC networks. — vDPA NICs support all VPC network services excluding security group and port forwarding. • If the DHCP service is not enabled on the selected network, stop the VM instance and assign an IP address. Otherwise, the IP address might loss after the VM instance reboots.	
Detach NIC	Detach a NIC from the VM instance. **Note:** • Detaching a NIC affects the network connectivity of the VM instance and disassociates other associated network services. Please exercise caution. • vDPA NICs that are attached to VM instances cannot be detached.	Running/Stopped
Set NIC Type	Change the NIC type from a VF NIC to a vNIC. **Note:** • Before you can set the NIC type, stop the VM instance. • Only VF NICs can be changed to vNICs.	Stopped
Set MAC	Set a MAC address the VM NIC. • Before you set a MAC address, stop the VM instance.	Stopped
Set the NIC Model	Set the NIC model for the VM instance. supported VM NIC models: virtio, rtl8139, and e1000.	Running/Stopped

Action	Description	VM State
	Note: • Before you set a NIC model, make sure that you installed a NIC driver that matches the NIC model. Otherwise, network exception may occur to the VM instance. • After you set the NIC model, reboot the VM instance to make the setting take effect. • Creating VM images and V2V migrations do not inherit configurations associated with the NIC model. • Only Linux and Paravirtualization operating systems are supported.	
Set NIC QoS	Set the upstream bandwidth and downstream bandwidth of the VM NIC. • To set the NIC QoS, either the upstream bandwidth or downstream bandwidth is required. Bandwidth range : 8 Kbps – 60 Gbps. Unit: Kbps, Mbps, and Gbps. • If not set, both the upstream and downstream bandwidth is not limited.	Running/Stopped
Set IP Address	Set an IP address for the VM NIC. • If you choose to assign an IP address, enter an IP address in the selected network range. • If you choose random allocation, the system will automatically allocate an IP address from the selected network range. **Note:** • Before you can set the IP address, stop the VM instance. • Make sure that the IP address does not conflict with other IP addresses.	Stopped
Set Default Network	Set a default network for the VM instance if the VM instance has multiple NICs. **Note:** Reboot the VM instance to take effect.	Running/Stopped

vDrive

This section displays a list of virtual drives (vDrives) attached to the VM instance. You can perform operations on these vDrives as needed. The following table lists the actions that you can perform on a vDrive.

Action	Description	VM State
Create vDrive	Create a vDrive for the VM instance. **Note:** • Before you create vDrive, stop the VM instance first. • A VM instance can have up to three vDrives. You can change the maximum of vDrives that can be created for a VM instance globally. Method: In the Global Setting, modify **Maximum Virtual Drive**. Valid values: 1, 2, and 3.	Stopped
Set as Default Drive	Set a vDrive for the VM instance if the VM instance has multiple vDrives. **Note:** • Reboot the VM instance to take effect. • If you change the default drive, note that: — The serial number of the vDrive will be changed , thus affecting the mapping between the device name and ISO. — For example, assume that you have three vDrives : CDROM-1, CDROM-2, and CDROM-3. If you make CDROM-2 default, CDROM-2 and the loaded ISO become CDROM-1, and the original CDROM-1 becomes CDROM-2.	Running/Stopped
Delete vDrive	Delete a vDrive. **Note:** • Before you can delete a vDrive, stop the VM instance. • After you delete a vDrive, the serial number of the remaining vDrives will be updated in order. — For example, assume that you have three vDrives : CDROM-1, CDROM-2, and CDROM-3. If you	Stopped

Action	Description	VM State
	delete CDROM-2, CDROM-3 and the loaded ISO becomes CDROM-2.	

LUN

This section displays a list of LUNs passed through from SAN storages to the VM instance. You can perform operations on these LUNs as needed. The following table lists the actions that you can perform on a LUN.

Action	Description	VM State
Attach LUN	Pass through a LUN to the VM instance directly as a storage medium. **Note:** • One VM instance can attach multiple LUNs. • One LUN can also be attached to multiple VM instances.	Running/Stopped
Detach LUN	Detach a LUN from the VM instance. **Note:** This operation interrupts the data reads/writes and may affect the business continuity. Please exercise caution.	Running/Stopped

pGPU Device

This section displays a list of physical GPU (pGPU) devices passed through from hosts to the VM instance. You can perform operations on these pGPU devices as needed. The following table lists the actions that you can perform on a pGPU device.

Action	Description	VM State
Attach pGPU Device	Pass through a pGPU device to a VM instance directly. **Note:** • One VM instance can attach multiple pGPU devices. • Currently, you cannot attach pGPU devices and vGPU devices to the same VM instance at the same time.	Running/Stopped

Action	Description	VM State
Detach pGPU Device	Detach a pGPU device from the VM instance. **Note:** This operation might affect the business continuity. Please exercise caution.	Running/Stopped

vGPU Device

This section displays a list of vGPU devices passed through from hosts to the VM instance. You can perform operations on these vGPU devices as needed. The following table lists the actions that you can perform on a vGPU device.

Action	Description	VM State
Attach vGPU Device	Pass through a vGPU device to a VM instance directly. **Note:** • Before you can attach a vGPU device to a VM instance, stop the VM instance first. • A VM instance can only attach one vGPU device at a time. • Currently, you cannot attach pGPU devices and vGPU devices to the same VM instance at the same time.	Stopped
Detach vGPU Device	Detach a vGPU device from the VM instance. **Note:** Before you detach a vGPU device from a VM instance, stop the VM instance first.	Stopped

USB Device

This section displays a list of USB devices passed through from hosts to the VM instance. You can perform operations on these USB devices as needed. The following table lists the actions that you can perform on a USB device.

Action	Description	VM State
Attach USB Device	Pass through a USB device to a VM instance directly. The following two attach modes are supported:	Running/Stopped

Action	Description	VM State
	• Passthrough: Attach a USB device from the host where the VM instance is located to the VM instance . If you want to migrate the VM instance, detach the USB device first. • Forward: Attach a USB device from the host that is in the same as the VM instance to the VM instance. If you want to migrate the VM instance, do not detach the USB device. **Note:** To attach a USB device to a VM instance, note the following: • You can attach a USB device to only one VM instance. • A VM instance can have a maximum of 1 USB 1.x device, 6 USB 2.x devices, and 4 USB 3.x devices attached. • For VM instances in the running state or VM instances using LocalStorages and are in the stopped state, you can attach only available USB devices on the hosts where these VM instances are located. In this case, you cannot attach USB devices across hosts. • For VM instances using shared storages and are in the stopped state, you can attach multiple USB devices on a host in the same cluster with the VM instance.	
Detach USB Device	Detach a USB device from the VM instance. **Note:** This operation interrupts the data reads/writes on the USB device. Please exercise caution.	Running/Stopped

Other Device

This section displays a list of other PCI devices, such as Ali-NPU cards, IB cards (PCI mode), and FPGA cards, passed through from hosts to the VM instance. You can perform operations on these PCI devices as needed. The following table lists the actions that you can perform on a PCI device.

Action	Description	VM State
Attach Other Device	Pass through a PCI device to the VM instance. **Note:** To attach a PCI device to a VM instance, note the following: • You need to edit the allowlist of PCI devices and then add the target device to the allowlist. • After you edit the allowlist, reconnect to the host to take effect. • For details about how to customize the allowlist for other devices and how to pass through them, consult the official technical support.	Running/Stopped
Detach Other Device	Detach a PCI device from the VM instance. **Note:** This operation might affect the business continuity. Please exercise caution.	Running/Stopped

7.1.1.5.2 Advanced Settings

ZStack Cloud allows you to set the advanced parameters of a VM instance. This setting takes effect only for the VM instance. If not set, the values set in the Global Setting will be used by default.

Currently, the following table lists the advanced parameters that you can set for a VM instance.

Parameter	Description
NUMA	• Specifies whether to enable NUMA. Enabling NUMA for a VM instance allows you to modify the CPU and memory of the VM instance online. By default, NUMA is disabled. • This setting is available for VM instances that run CentOS 7.2, CentOS 6.6, Ubuntu 14.04, and Ubuntu 16.04. • We do not recommend that you modify the CPU and memory of VM instances online in production environmen ts. • For Windows-based VM instances, we recommend that you stop these VM instance before you set the NUMA.

Parameter	Description
Hyper-V Virtualization	Specifies whether to enable Hyper-V of a VM instance. By default, Hyper-V is disabled. Note that you can set Hyper-V for Windows-based VM instances only.
NIC Queue Number	Set the number of queues when VirtIO NIC traffics are allocated to multiple CPUs. Default: 1. Valid values: 1 to 256, integer.

7.1.1.5.3 External Monitoring

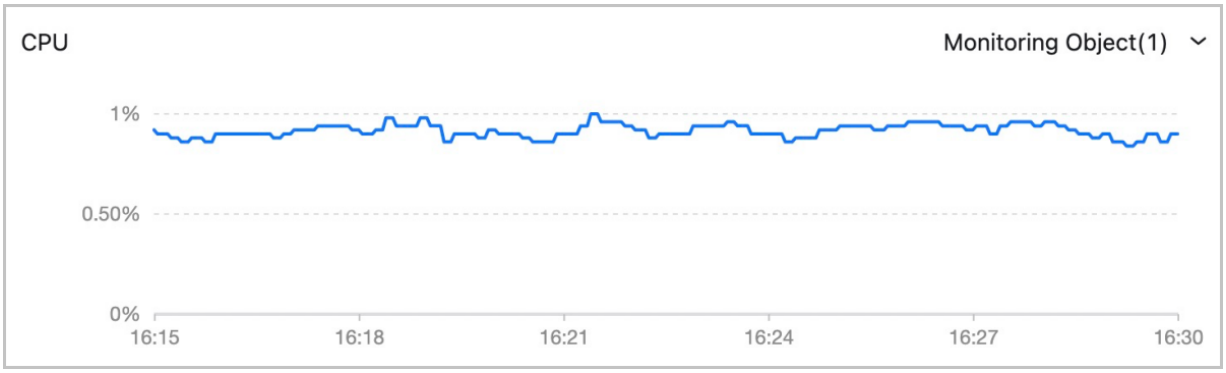
The External Monitoring tab displays the VM performance data, such as the CPU, memory, disk I/O, and NIC data, obtained from a host by using a libvirt. These data is displayed dynamically in real time through graphs.

CPU

You can select a time span to view the real-time CPU utilization of a VM instance.

- Available time spans: 15 minutes, 1 hour, 6 hours, 1 day, 1 week, 1 month, 1 year, and custom.
- Monitoring object:
  - Select All: Display the average, real-time utilization of all CPUs of a VM instance and the utilization of a single CPU.
  - Average: Display the average, real-time utilization of all CPUs of a VM instance.
  - Single CPU: Display the real-time utilization of a single CPU, such as CPU No. 1, No.2, and No. 3.

Figure 7-7: CPU Real-Time Monitoring

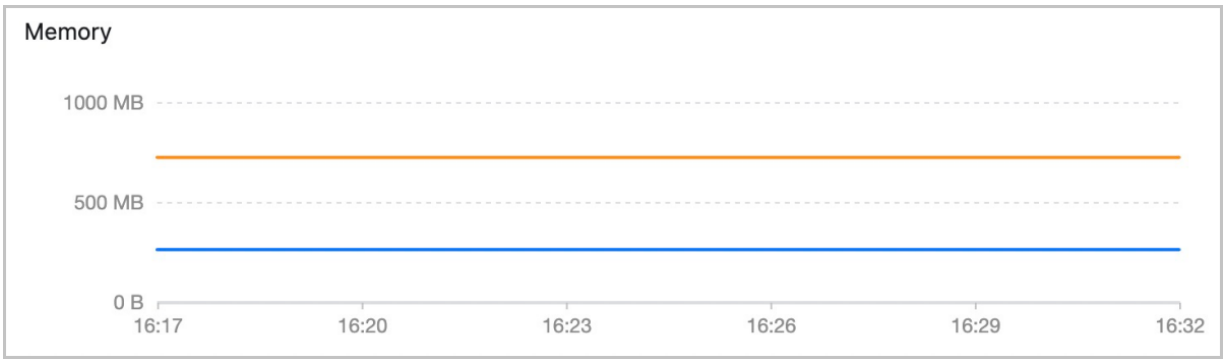


Memory

You can select a time span to view the real-time memory utilization of a VM instance.

- Available time spans: 15 minutes, 1 hour, 6 hours, 1 day, 1 week, 1 month, 1 year, and custom.
- Monitoring object:
  - By default, both the used memory and the free memory are displayed.
  - used: Display the used memory of the VM instance.
  - free: Display the free memory of the VM instance.

Figure 7-8: Memory Real-Time Monitoring



Note:

You can also monitor the real-time usage of the VM memory by using the `virsh dommemstat` command provided by libvirt.

```
# Obtain the ID of the VM instance.
[root@localhost ~]# virsh list
 Id    Name                           State
----------------------------------------------------
 1     fe3790c408204c9998ccd6b54272fab1 running

# Obtain the real-time memory utilization of the VM instance. Unit:
KB.
[root@localhost ~]# virsh dommemstat 1
actual 2097152
swap_in 0
swap_out 16
major_fault 698
minor_fault 686260
unused 23876
available 2048544
rss 2147224
```

Note:

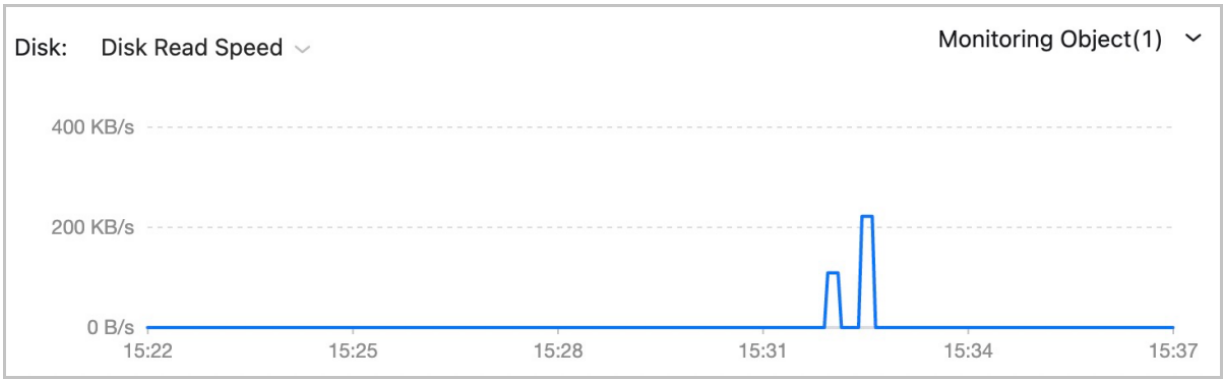
For memory data, internal monitoring is more accurate than external monitoring. We recommend that you use internal monitoring to monitor the memory data.

Disk I/O

You can select a time span to view the real-time disk I/O of a VM instance.

- Available time spans: 15 minutes, 1 hour, 6 hours, 1 day, 1 week, 1 month, 1 year, and custom.
- Monitoring metrics:
  - Disk Read Speed: The read speed of a disk.
  - Disk Read IOPS: The read I/O operations per second (IOPS) of a disk.
  - Disk Write Speed: The write speed of a disk.
  - Disk Write IOPS: The write I/O operations per second (IOPS) of a disk.
- Monitoring object:
  - Select All: Display the real-time status of all disk partitions.
  - Single disk partition: Display the real-time read/write status of a single disk partition, such as the vda partition.

Figure 7-9: Disk I/O Real-Time Monitoring



NIC

You can select a time span to view the real-time NIC status of a VM instance.

- Available time spans: 15 minutes, 1 hour, 6 hours, 1 day, 1 week, 1 month, 1 year, and custom.
- Monitoring metrics:
  - NIC Data Out Rate: The speed of sending NIC data.
  - NIC Data In Rate: The speed of receiving NIC data.
  - NIC Packets Out Rate: The speed of sending NIC packets.
  - NIC Packets In Rate: The speed of receiving NIC packets.
  - NIC Packets Out Discard Rate: The rate of outgoing packet errors.

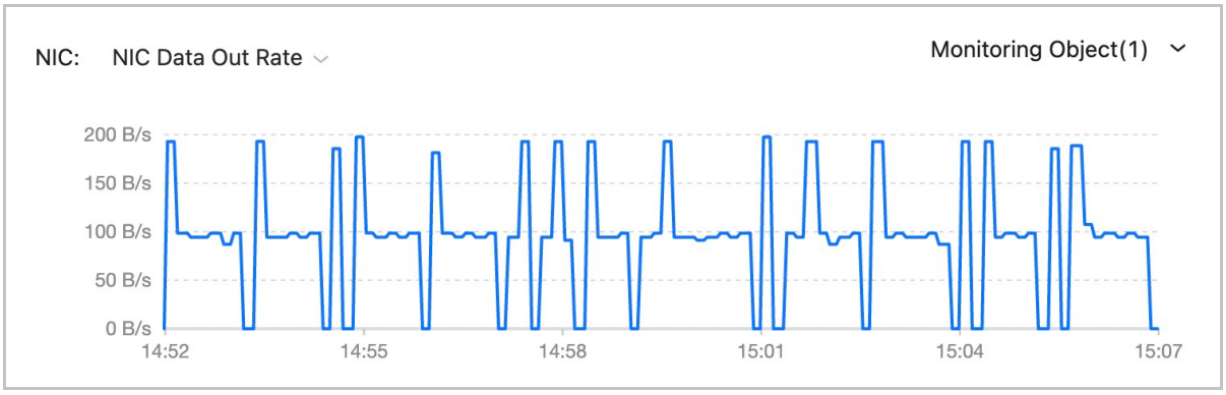
— NIC Packets In Discard Rate: The rate of incoming packet errors.

- Monitoring object:

  — Select All: Display the utilization of all VM NICs.

  — Single NIC: Display the real-time downstream and upstream rate of the single VM NIC, such as vnic7.0.

Figure 7-10: NIC Real-Time Monitoring



7.1.1.5.4 Internal Monitoring

The **Internal Monitoring** tab displays the VM performance data, such as the CPU, memory, and disk capacity, obtained by the agent from a host. These data is displayed dynamically in real time through graphs.

Note:

Before you can view the internal monitoring data, install an agent for the VM instance. For details about how to install the agent, see *Internal Monitoring Agent*.

CPU

You can select a time span to view the real-time CPU utilization of a VM instance.

- Available time spans: 15 minutes, 1 hour, 6 hours, 1 day, 1 week, 1 month, 1 year, and custom.
- Monitoring metrics:

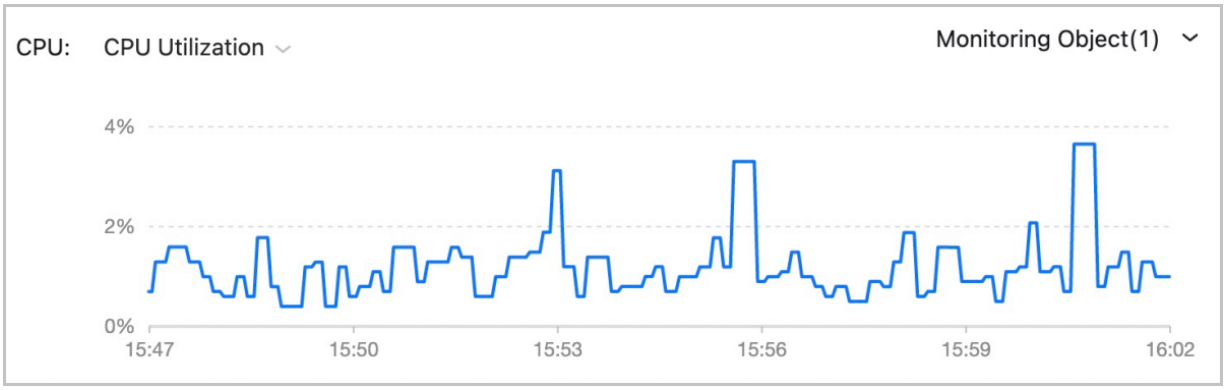
  — CPU Occupancy Rate (System Process): The percentage of CPUs occupied by the current kernel space of the VM instance.

  — CPU Occupancy Rate (User Process): The percentage of CPUs occupied by the current user process of the VM instance.

- CPU Occupancy Rate (Waiting): The percentage of CPUs used for waiting for the I/O operations of the VM instance.
- CPU Idle Rate: The percentage of idle CPUs of the VM instance.
- CPU Utilization: The percentage of used CPUs of the VM instance.

- Monitoring object:
  - Select All: Display the average, real-time utilization of all CPUs of a VM instance and the utilization of a single CPU.
  - Average: Display the average, real-time utilization of all CPUs of a VM instance.
  - Single CPU: Display the real-time utilization of a single CPU, such as CPU No. 1, No.2, and No. 3.

Figure 7-11: CPU Real-Time Monitoring

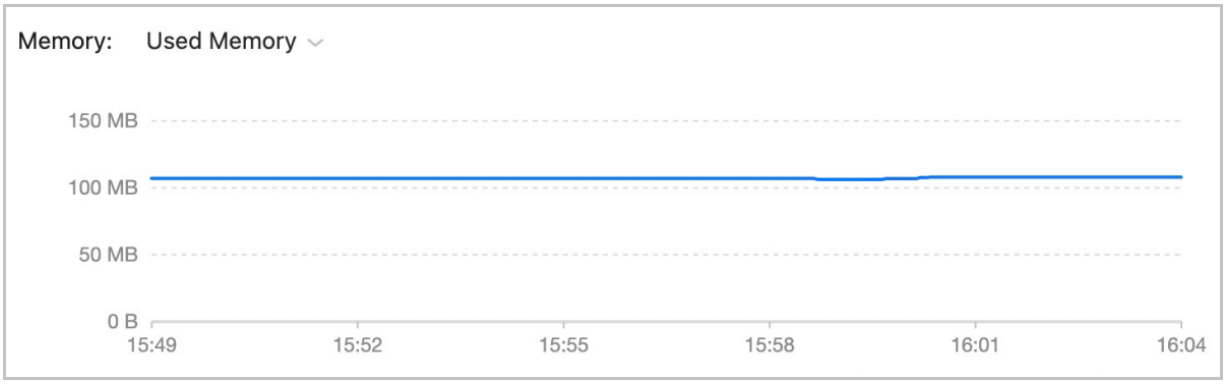


Memory

You can select a time span to view the real-time memory utilization of a VM instance.

- Available time spans: 15 minutes, 1 hour, 6 hours, 1 day, 1 week, 1 month, 1 year, and custom.
- Monitoring metrics:
  - used: The used memory of a VM instance.
  - available: The available memory of a VM instance.
  - free: The idle memory of a VM instance.
  - total: The total memory of a VM instance.
  - freeutilization: The percentage of idle memory of a VM instance.
  - usedutilization: The percentage of the used memory of a VM instance.

Figure 7-12: Memory Real-Time Monitoring



Note:

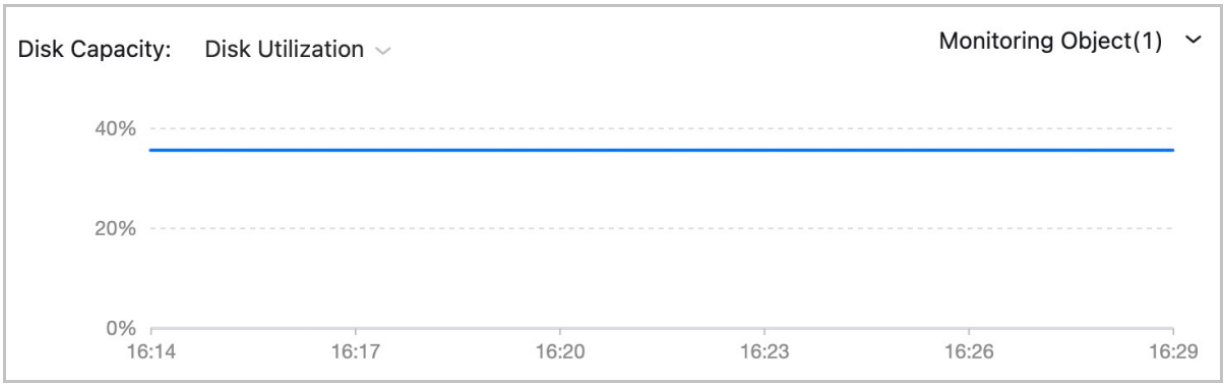
For memory data, internal monitoring is more accurate than external monitoring. We recommend that you use internal monitoring to monitor the memory data.

Disk Capacity

You can select a time span to view the real-time disk capacity of a VM instance.

- Available time spans: 15 minutes, 1 hour, 6 hours, 1 day, 1 week, 1 month, 1 year, and custom.
- Monitoring metrics:
  - Disk Utilization: The percentage of used disk of a VM instance.
  - Disk Used Capacity: The used capacity of the VM disk.
  - Disk Idle Rate: The percentage of idle disk capacity of a VM instance.
  - Disk Idle Capacity: The idle disk capacity of a VM instance.
- Monitoring object:
  - Select All: Display the real-time status of all disk partitions.
  - Single disk partition: Display the real-time read/write status of a single disk partition, such as the vda partition.

Figure 7-13: Disk Capacity Real-Time Monitoring



7.1.1.5.5 Internal Monitoring Agent

The agent is installed on a VM instance and regularly pushes the VM monitoring data to the specified host through the internal network.

Note:

- Before you can view the monitoring data of a VM instance, install the agent first.
- Internal monitoring relies on the DHCP and User Data services of the l3 network. To install and use the agent successfully, enable the DHCP and User Data services of the VM instance first.

Installation Method

The agent is included in the performance optimization tool (GuestTools). The installation method varies according to the operating systems installed by the VM instance.

- Linux VM instances

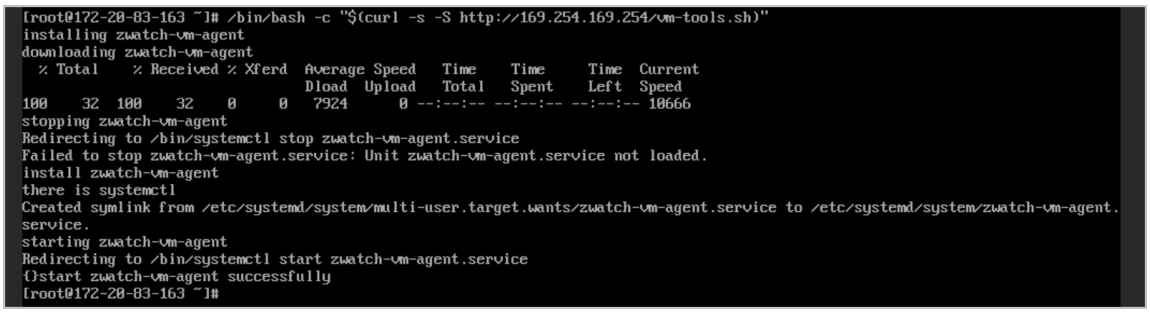
  UI-based installation

  1. Install GuestTools on the details page of the VM instance.

2. Launch the VM console and run the following command:

```
/bin/bash -c "$(curl -s -S http://169.254.169.254/vm-tools.sh)"
```

Figure 7-14: Install agent



Note:

- In the command above, *169.254.169.254* is the IP address of the User Data server.
- Before you install or upgrade an agent, make sure that you installed the corresponding Linux command tools, such as **`tar`**, **`wget`**, and **`curl`**.
- The agent can be upgraded automatically,

User Data-based installation

1. Perform **System Configurations** when you create a VM instance.
2. In the **User Data** input box, enter the following information:

```
#cloud-config
runcmd:
- /bin/bash -c "$(curl -s http://169.254.169.254/cloud-tools.sh)"
```

Note:

Before you inject User Data into Linux-based VM instances, install cloud-init on the VM image first.

- Windows/Windows VirtIO-bassed VM instances

  1. Install the GuestTools on the details page of the VM instance.
  2. Launch the VM console and install GuestTools as prompted.

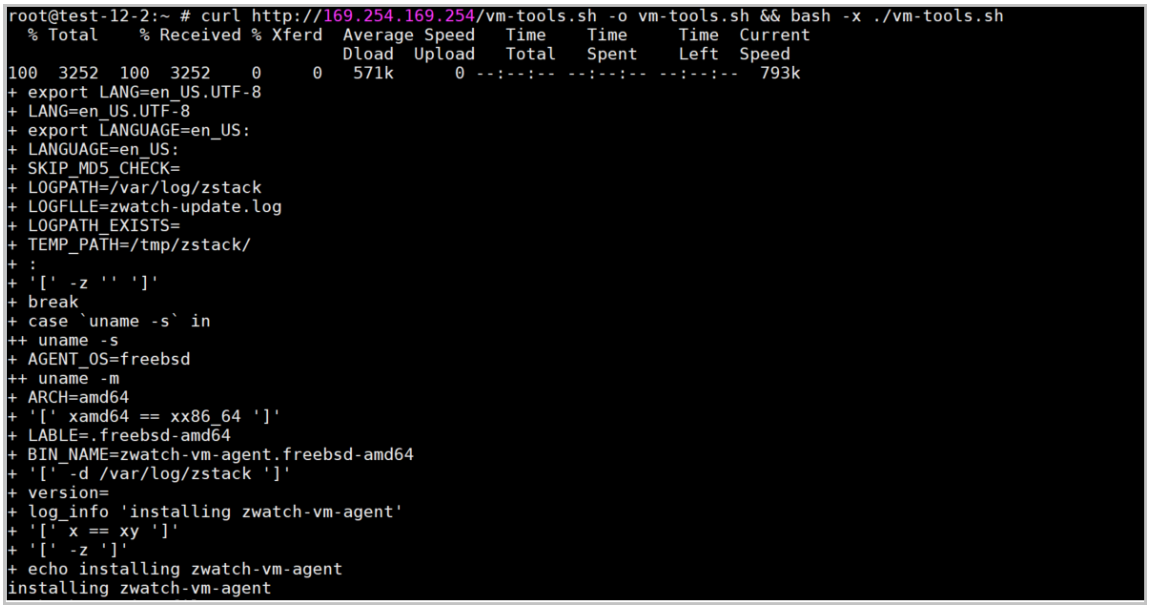
- FreeBSD VM instance

  1. Install GuestTools on the details page of the VM instance.

2. Launch the VM console and run the following command:

```
curl http://169.254.169.254/vm-tools.sh -o vm-tools.sh && bash -x
 ./vm-tools.sh
```

Figure 7-15: Install agent



```
root@test-12-2:~ # curl http://169.254.169.254/vm-tools.sh -o vm-tools.sh && bash -x ./vm-tools.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3252  100  3252    0     0   571k      0 --:--:-- --:--:-- --:--:--  793k
+ export LANG=en_US.UTF-8
+ LANG=en_US.UTF-8
+ export LANGUAGE=en_US:
+ LANGUAGE=en_US:
+ SKIP_MD5_CHECK=
+ LOGPATH=/var/log/zstack
+ LOGFLLE=zwatch-update.log
+ LOGPATH_EXISTS=
+ TEMP_PATH=/tmp/zstack/
+ :
+ '[' -z '' ']'
+ break
+ case `uname -s` in
++ uname -s
+ AGENT_OS=freebsd
++ uname -m
+ ARCH=amd64
+ '[' xamd64 == xx86_64 ']'
+ LABLE=.freebsd-amd64
+ BIN_NAME=zwatch-vm-agent.freebsd-amd64
+ '[' -d /var/log/zstack ']'
+ version=
+ log_info 'installing zwatch-vm-agent'
+ '[' x == xy ']'
+ '[' -z ']'
+ echo installing zwatch-vm-agent
installing zwatch-vm-agent
```

Note:

- In the command above, *169.254.169.254* is the IP address of the User Data server.
- Before you install the agent, make sure that you installed the **`bash`**, **`security/libgcrypt`**, and **`curl`** tools.

Installation Requirements

Table 7-1: Version Requirements

Supported Operating System	Supported Version
CentOS	• CentOS 6.8 64 bit • CentOS 6.9 64 bit • CentOS 6.10 64 bit • CentOS 7.2 64 bit • CentOS 7.3 64 bit • CentOS 7.4 64 bit • CentOS 7.5 64 bit • CentOS 7.6 64 bit

Supported Operating System	Supported Version
	• CentOS 8.0 64 bit
RHEL	• Red Hat Enterprise Linux Server 6.9 64 bit • Red Hat Enterprise Linux Server 7.4 64 bit • Red Hat Enterprise Linux Server 7.5 64 bit • Red Hat Enterprise Linux Server 7.6 64 bit
Fedora	• Fedora 30 64 bit **Note:** This version does not support the **`service`** command, which results in an execution error in line 54 of `systemctl start`. You can successfully start the agent by changing the command to `systemctl start`. • Fedora 31 64 bit
Debian	• Debian 9.9 64 bit • Debian 10.0 64 bit
Ubuntu	• Ubuntu 14.04 64 bit • Ubuntu 16.04 64 bit • Ubuntu 16.10 64 bit • Ubuntu 18.04 64 bit
Kylin	• Kylin 4.0.2 64 bit
openSUSE	• openSUSE 15.0 64 bit
SLES	• SUSE Linux Enterprise Server 15 64 bit • SUSE Linux Enterprise Server 12 64 bit
FreeBSD	• FreeBSD 11 64 bit • FreeBSD 12 64 bit • FreeBSD 13 64 bit
Windows	• Windows Server 2003 R2 64 bit • Windows Server 2008 R2 64 bit • Windows Server 2012 64 bit • Windows Server 2016 64 bit

Table 7-2: Other Requirements

Entry	Requirements
Environmental dependence	• rpm • systemd
Ports	• 9103 • 9100 • 25826

Note:

- The agent must be installed by the root account of the VM operating system.
- If the default port is occupied, the agent might fail to be started after installation. In this case, you can go the installation directory, find the `conf.yaml` file, and manually change the port.
- The agent pushes VM monitoring data to the host through the internal network at an interval of 10 seconds. Note that the data is not uploaded to the external network.

Manage the Agent

You can manage the agent by using the following commands:

- Stop the agent service: `service zwatch-vm-agent stop`.
- Start the agent service: `service zwatch-vm-agent start`.
- Restart the agent service: `service zwatch-vm-agent restart`.
- Query the agent service: `service zwatch-vm-agent status`.

Uninstallation Method

The uninstallation method varies according to the operating system of the VM instance.

- Linux-based VM instances
  1. Stop the agent by running the **`service zwatch-vm-agent stop`** command.
  2. Delete the service configuration file by running the **`rm -f /etc/systemd/system/zwatch-vm-agent.service`** command.
  3. Delete the agent installation directory by running the **`rm -rf /usr/local/zstack/zwatch-vm-agent`** command.
- Windows-based VM instances
  1. Delete registry related entries.

Run the Windows command prompt as an administrator and run the following command to delete the relevant keys in the system:

```
reg delete HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
MSDTC /f
reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDTC /f
reg delete HKEY_CLASSES_ROOT\CID /f
```

2. Stop and reinstall msdtc service.

   Run the Windows command prompt as an administrator and run the following commands to stop and reinstall the msdtc service:

```
net stop msdtc
msdtc -uninstall
msdtc -install
```

3. Reboot the VM instance.
4. Uninstall the agent.

   Run the Windows command prompt as an administrator and run the following command to delete the agent:

```
msiexec /a "c:\Program Files\GuestTools\qemu-ga.msi" targetdir="c:
\Program Files"
"c:\Program Files\QEMU Guest Agent\Qemu-ga\qemu-ga.exe" -s vss-
uninstall
```

7.1.1.5.6 SSH Key Management

After you inject an SSH key into a VM instance, you can SSH to the VM instance without entering a password.

Steps

1. Install cloud-init.

   Currently, you can inject an SSH key into a VM instance by using cloud-init. Before you can inject an SSH key, install cloud-init on the VM image first.

   1. Install cloud-init. Recommended versions: 0.7.9, 17.1, 19.4, and later.
   2. After you install cloud-init, the SSH password authentication is disabled by default. To enable the SSH password authentication, set the `ssh_pwauth` option under *`/etc/cloud/cloud.cfg`* to **1**.
2. Generate an SSH key.

a. The SSH key is generated by running the **ssh-keygen** command and is stored in *`/root/.ssh/id_rsa.pub`* by default.

b. Paste the file content into the SSH Key input box.

3. Inject the SSH key into the VM instance.

   You can inject the SSH key into the VM instance by the following two methods:

   - Method 1: When you create a VM instance, inject an SSH key.
   - Method 2: For existing VM instances, inject an SSH key by performing the **Set SSH KEY** action.

   After you inject the SSH key, you can check the basic information about the SSH key on the details page of the VM instance. The basic information includes the corresponding username and host information.

Note:

- If you inject an SSH key when you create a VM instance, the SSH key takes effect upon the first VM starts.
- If you inject an SSH key into an existing VM instance for the first time, reboot the VM instance to take effect.
- If you inject an SSH key into a VM instance that already has an SSH key, clean up the previous configurations by running the `rm -rf /var/lib/cloud/instances` command, inject the new SSH key, and reboot the VM instance to take effect.
- If you need to delete an SSH key, only the SSH key information recorded in the system is deleted. The SSH key information injected into the VM configurations is not deleted. To delete the SSH key information completely, manually clean up the VM configuration file *`/root/.ssh/authorized_keys`*.

Image Downloads

You can download the corresponding images for test use from the CentOS and Ubuntu official websites. The download links are as follows:

- CentOS 7: Click *here*.
- Ubuntu 14.04: Click *here*.

7.1.1.5.7 Resize the Root Volume

ZStack Cloud allows you to resize the root volume of a VM instance when the VM instance is in the running or stopped state. Note that only increasing volume size is supported.

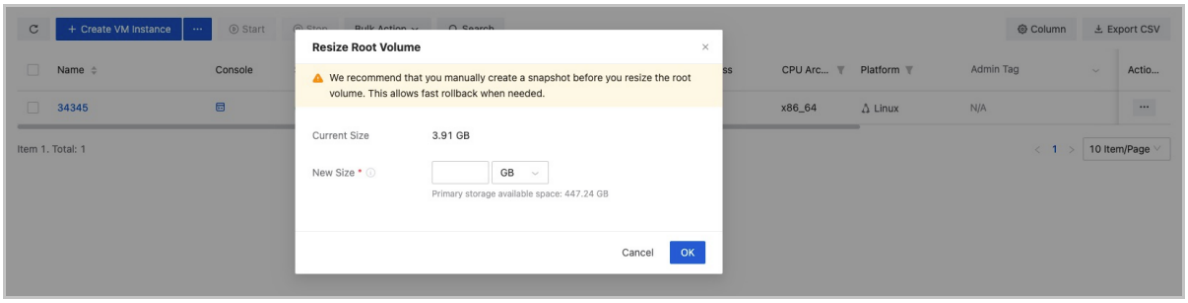
Resize the Root Volume

You can resize the root volume of a VM instance by using one of the following methods:

1. On the **VM Instance** management page, select a VM instance that is in the running or stopped state and choose **Actions** > **System Configurations** > **Resize Root Volume**. Then, the **Resize Root Volume** dialog box is displayed.

   You can set a new size as needed. The new size takes effect immediately.

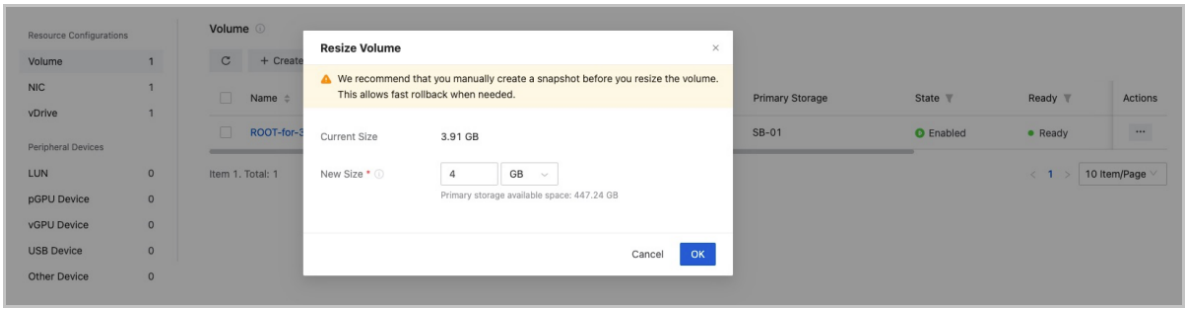
   Figure 7-16: Resize Root Volume



2. Select a VM instance that is in the running or stopped state and go to the details page of the VM instance. On the **Configuration Info** tab page, select the root volume to be resized and choose **Actions** > **Resize Volume**. Then, the **Resize Volume** dialog box is displayed.

   You can set a new size as needed. The new size takes effect immediately.

   Figure 7-17: Resize Volume



3. Select a VM instance that is in the running or stopped state and go to the details page of the VM instance. On the **Configuration Info** tab page, click on the name of the root volume to be resized and set a new size for the root volume. The new size takes effect immediately.

The steps above only increase the size of the root volume. To make the new size recognized by the VM instance, partition and resize the hard disk in the operating system of the VM instance.

Partition and Resize the Hard Disk

The resize method varies according to the VM type, partition, and file system.

Note:

- Before you resize a root volume, create a snapshot for the VM instance to enhance the data security.
- The resize operation has potential risks. For security reasons, we recommend that you plan a new partition for the new size.
- The resize operation only increases the size, not reduce the size.
- The increased size can be merged into the last partition for continuous use.
  - If the last partition is a system backup partition (Windows), you must plan a new partition for the increased size.
  - If the last partition is a swap partition, you can delete the swap partition first, add the increased size to the last partition, and then rebuild a swap partition.

The following are four different resize scenarios.

1. Use the GParted open source tool to resize the ext4 root partition for an instance that has both the ext4 and swap partitions.

   Note:

   - In this scenario, you need to re-plan the current partition by using Live CD.
   - To prevent data loss, exercise caution when you adjust a partition.

   Assume that VM instance uses an ext4 root partition of 35 GB and a swap partition of 5 GB. The total size is 40 GB. After you resize the root volume from 40 GB to 50 GB, you want to add the increased size to the ext4 root partition.

   Procedure:

   1. Add a GParted ISO. You can download the ISO from the GParted official website *https://gparted.org/download.php*. We recommend that you download the amd64 iso, indicating that 64-bit operating systems are supported.

2. After you add the ISO, set CD ROM as the first boot order and Hard Disk as the second. Then, the VM instance boots from CD ROM next time.
3. Use GParted Live CD to boot the system and launch the console of the VM instance. After the GParted boot finished, follow the instructions and long-press the **Enter** key until you enter the graphical interface.
4. In the GParted interface, right-click the original swap partition to delete it, resize ext4 from 35 GB to 46 GB, and create a new swap partition for the unallocated 4 GB.

Figure 7-18: Delete Original swap Partition

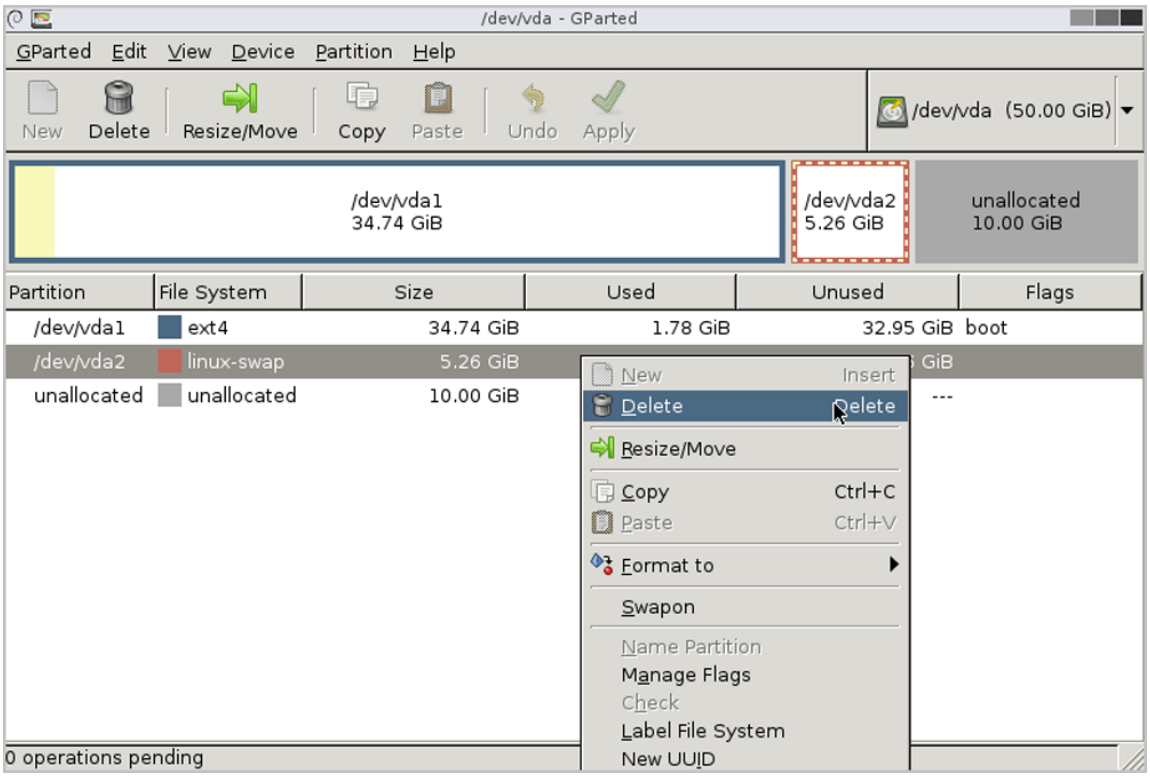
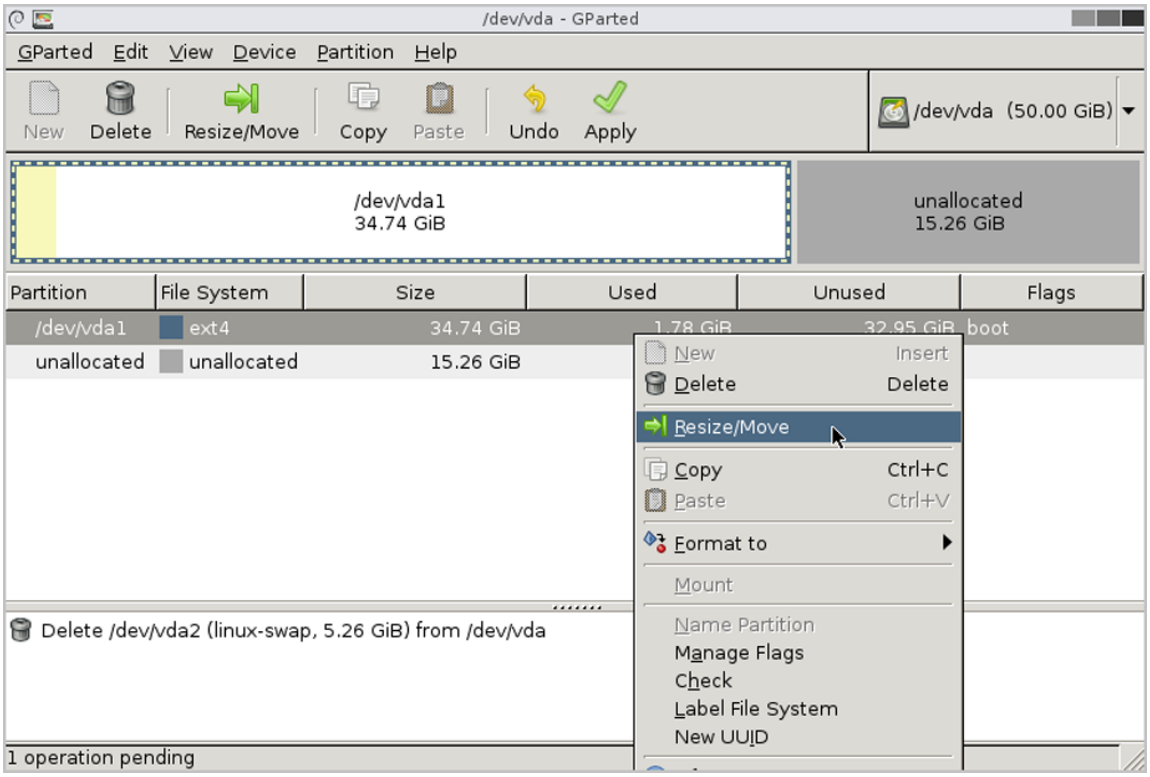


Figure 7-19: Resize ext4 from 35 GB 46 GB



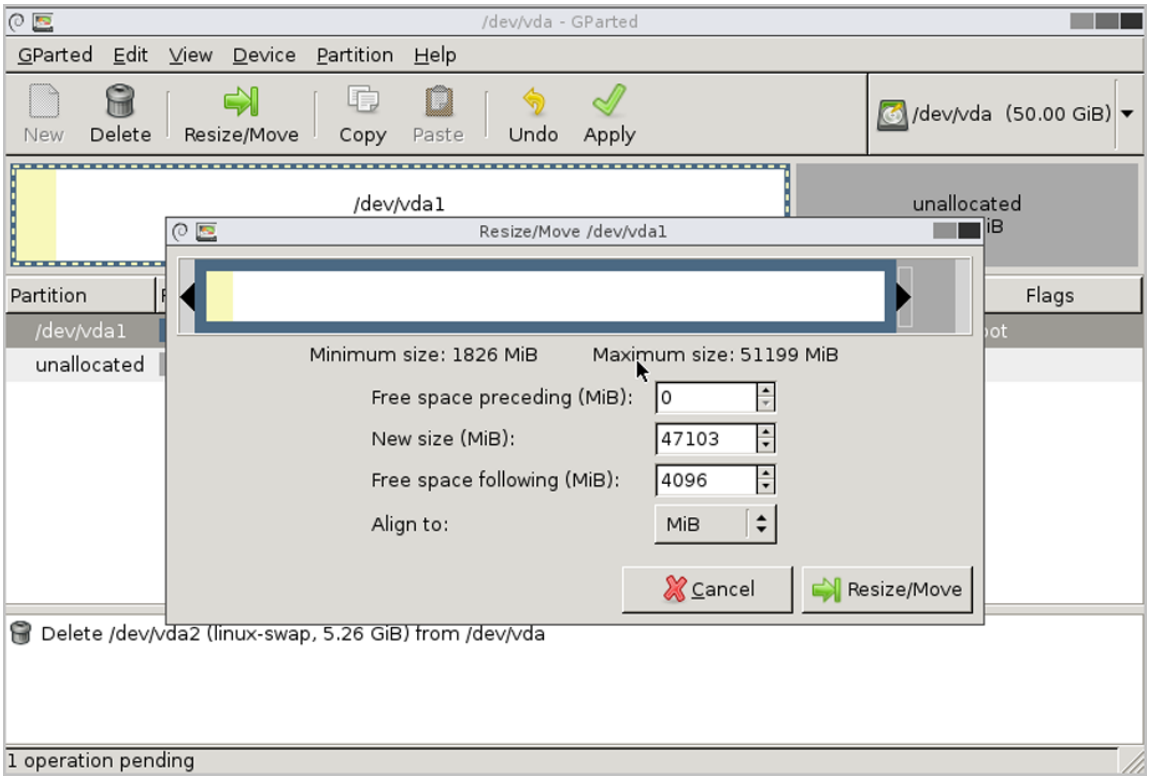
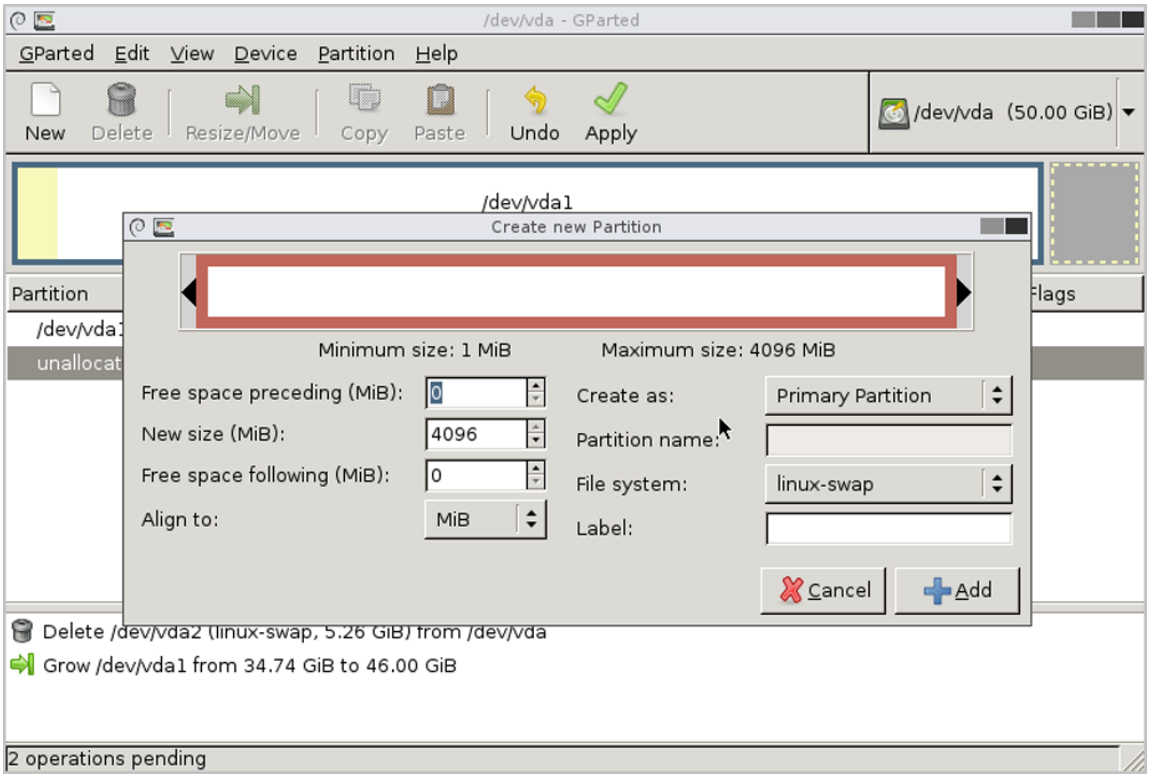
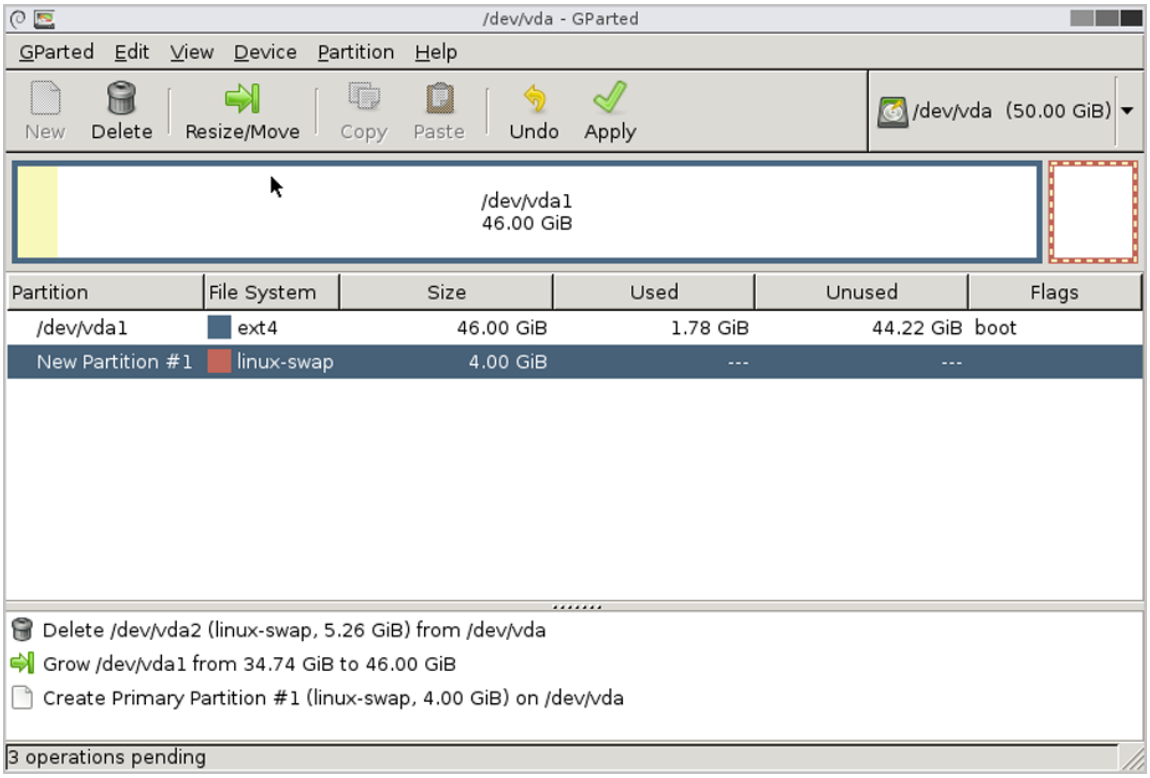


Figure 7-20: Create a 4 GB swap Partition





5. Power off the VM instance, detach the ISO, and start the VM instance again.

6. Launch the VM console and run the `df -h` command. Then, you can see that the size of the root partition is increased to 46 GB.

```
[root@10-58-21-213 ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/vda1 46G 1.2G 42G 3% /
```

7. Enable the swap partition and modify the *`/etc/fstab`* disk partition table.

```
[root@10-58-21-213 ~]# fdisk -l|grep vda
Disk /dev/vda: 53.7 GB, 53687091200 bytes, 104857600 sectors
/dev/vda1 * 2048 96468991 48233472 83 Linux
/dev/vda2 96468992 104857599 4194304 82 Linux swap / Solaris

[root@10-58-21-213 ~]# mkswap /dev/vda2
mkswap: /dev/vda2: warning: wiping old swap signature.
Setting up swapspace version 1, size = 4194300 KiB
no label, UUID=ed99f72b-aafb-43ad-be8f-fcd09794beb0
#You can see that the UUID of the swap partition is ed99f72b-aafb-
43ad-be8f-fcd09794beb0.

[root@10-58-21-213 ~]# swapon /dev/vda2
#Enable the swap partition.

[root@10-58-21-213 ~]# free -m
 total used free shared buff/cache available
Mem: 911 106 671 6 133 657
Swap: 4095 0 4095

[root@10-58-21-213 ~]# sed -i '/swap/d' /etc/fstab
echo "UUID=ed99f72b-aafb-43ad-be8f-fcd09794beb0 swap swap defaults
 0 0"
#Write the swap settings into the disk partition table so that it
can be started automatically upon the VM boots.
```

8. After you power off and reboot the VM instance, the ext4 partition of the root volume is resized successfully, and the swap partition reserves 4 GB.

2. Use the LVM partition tool to resize the LVM partition for an instance that has both the xfs and swap partitions.

> **Note:**
> This method applies to the dynamic resizing of LVM partitions without the need of using other tools.

Assume that the VM instance uses an LVM partition and formats the LVM partition as a boot partition, an xfs root partition, and a swap partition. In this scenario, the size of the xfs root partition and swap partition is 94 GB and 6 GB, respectively. Therefore, the total size is 100 GB . After you resize the root volume from 100 GB to 120 GB, you want to add the increased size to the xfs root partition.

Procedure:

1. View the current partition and the LVM partition. Here, the size of the boot partition, LVM partition, and swap partition is 500 MB, 94 GB, and 6 GB, respectively. The boot partition and LVM partition use *`/dev/vda1`* and *`/dev/vda2`*, respectively. The path of the LVM partition and swap partition is *`/dev/vg/root`* and *`/dev/vg/swap`*, respectively.

```
[root@10-0-44-221 ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/vg-root 94G 6.5G 88G 7% /
/dev/vda1 477M 104M 344M 24% /boot
#The boot partition is 500 MB and uses /dev/vda1.
#The LVM partition is 94 GB and uses /dev/vda2. Path: /dev/vg/root
.
#The swap partition is 6 GB. Path: /dev/vg/swap.

[root@10-0-44-221 ~]# fdisk -l |grep vda
Disk /dev/vda: 128.8 GB, 128849018880 bytes, 251658240 sectors
/dev/vda1 * 2048 1026047 512000 83 Linux
/dev/vda2 1026048 209715199 104344576 8e Linux LVM

[root@10-0-44-221 ~]# pvdisplay |egrep "Name|Size"
 PV Name /dev/vda2
 VG Name vg
 PV Size 99.51 GiB / not usable 3.00 MiB
 PE Size 4.00 MiB
#The physical volume uses /dev/vda2.

[root@10-0-44-221 ~]# vgdisplay |egrep "Name|Size"
 VG Name vg
 VG Size 99.51 GiB
 PE Size 4.00 MiB
 alloc PE / Size 25463 / 99.46 GiB
 Free PE / Size 11 / 44.00 MiB
#The volume group information. Name: vg. This volume group will be
 resized.

[root@10-0-44-221 ~]# lvdisplay |egrep "Name|Size"
 LV Name root
 VG Name vg
 LV Size 93.59 GiB
 LV Name swap
 VG Name vg
 LV Size 5.88 GiB
#The logical volume information.
```

2. After the resizing, run the `fdisk /dev/vda` command to partition the increased size, create a new partition by using `n`, set the new partition to LVM format by using `t`, and make the setting take effect by using `w`. To make the setting take effect immediately, run the `partprobe` command.

```
[root@10-0-44-221 ~]# fdisk /dev/vda
Welcome to fdisk (util-linux 2.23.2).
Changes will remain in memory only, until you decide to write them
.
```

```
Be careful before using the write command.
Command (m for help): p
Disk /dev/vda: 128.8 GB, 128849018880 bytes, 251658240 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x0008168e
 Device Boot Start End Blocks Id System
/dev/vda1 * 2048 1026047 512000 83 Linux
/dev/vda2 1026048 209715199 104344576 8e Linux LVM
Command (m for help): n
Partition type:
 p primary (2 primary, 0 extended, 2 free)
 e extended
Select (default p):
Using default response p
Partition number (3,4, default 3):
First sector (209715200-251658239, default 209715200):
Using default value 209715200
Last sector, +sectors or +size{K,M,G} (209715200-251658239,
default 251658239):
Using default value 251658239
Partition 3 of type Linux and of size 20 GiB is set
Command (m for help): t
Partition number (1-3, default 3):
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'
Command (m for help): p
Disk /dev/vda: 128.8 GB, 128849018880 bytes, 251658240 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x0008168e
 Device Boot Start End Blocks Id System
/dev/vda1 * 2048 1026047 512000 83 Linux
/dev/vda2 1026048 209715199 104344576 8e Linux LVM
/dev/vda3 209715200 251658239 20971520 83 Linux LVM
Command (m for help): w
The partition table has been altered!
Calling ioctl() to re-read partition table.
WARNING: Re-reading the partition table failed with error 16:
Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.

[root@10-0-44-221 ~]# partprobe
```

3. Create a physical volume for the newly formatted partition.

```
[root@10-0-44-221 ~]# pvcreate /dev/vda3
 Physical volume "/dev/vda3" successfully created
#Create a physical volume.
```

4. Extend the volume group.

```
[root@10-0-44-221 ~]# vgextend vg /dev/vda3
 Volume group "vg" successfully extended
```

```
#Name of the volume group: vg. The new partition will be added to
the volume group vg.
```

5. Disable the swap partition and delete the original swap logical volume.

```
[root@10-0-44-221 ~]# swapoff -a
[root@10-0-44-221 ~]# lvremove /dev/vg/swap
Do you really want to remove active logical volume swap? [y/n]:
yes
 Logical volume "swap" successfully removed
```

6. Add 20 GB to the logical volume *`/dev/vg/root`*.

```
[root@10-0-44-221 ~]# lvextend -L +20G /dev/vg/root
 Size of logical volume vg/root changed from 93.59 GiB (23959
extents) to 113.59 GiB (29079 extents).
 Logical volume root successfully resized.
#Add 20 GB to /dev/vg/root.

[root@10-0-44-221 ~]# lvdisplay
 --- Logical volume ---
 LV Path /dev/vg/root
 LV Name root
 VG Name vg
 LV UUID UkyCVW-gd5E-Z4Q2-bVHv-T84e-c3GH-ZMiUdF
 LV Write Access read/write
 LV Creation host, time localhost, 2017-07-26 13:18:40 +0800
 LV Status available
 # open 1
 LV Size 113.59 GiB
 Current LE 29079
 Segments 2
 allocation inherit
 Read ahead sectors auto
 - currently set to 8192
 Block device 253:0
```

7. Run the `xfs_growfs` command to resize the XFS file system, make the new size take effect, and check the new partition.

```
[root@10-0-44-221 ~]# xfs_growfs /dev/vg/root
meta-data=/dev/mapper/vg-root isize=256 agcount=4, agsize=6133504
blks
 = sectsz=512 attr=2, projid32bit=1
 = crc=0 finobt=0
data = bsize=4096 blocks=24534016, imaxpct=25
 = sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0 ftype=0
log =internal bsize=4096 blocks=11979, version=2
 = sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
data blocks changed from 24534016 to 29776896

[root@10-0-44-221 ~]# df -h|grep vg-root
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/vg-root 114G 6.5G 108G 6% /
```

```
#Resizing of the new partition takes effect.
```

8. Divide a new size from the logical volume group to the swap partition, enable the swap partition, and write the disk configuration.

```
[root@10-0-44-221 ~]# lvcreate -L 4G -n swap vg
 Logical volume "swap" created.
#Create a 4 GB partition named swap from the volume group vg.

[root@10-0-44-221 ~]# mkswap /dev/vg/swap
Setting up swapspace version 1, size = 4194300 KiB
no label, UUID=bfc8a843-c758-4665-adfe-e32752ceda44
#Create a swap partition. Here, you can see that the UUID of the
swap partition is bfc8a843-c758-4665-adfe-e32752ceda44.

[root@10-0-44-221 ~]# swapon /dev/mapper/vg-swap
#Enable the swap partition.

[root@10-58-21-213 ~]# sed -i '/swap/d' /etc/fstab
echo "UUID=bfc8a843-c758-4665-adfe-e32752ceda44 swap swap defaults
 0 0"
#Write the swap settings into the disk partition table so that the
 swap partition can be enabled automatically after the VM instance
 is started.
```

9. After you power off and reboot the VM instance, the XFS system of the VM LVM partition is resized successfully, and the swap partition reserves 4 GB.

3. Use the growpart tool to extend the xfs root partition instance.

Note:

This method applies to the dynamic resizing of xfs partitions without the need of attaching an ISO or using an LVM partition tool.

Assume that the size of the xfs root partition is 6 GB and the total root volume size is 8 GB. After you resize the root volume from 8 GB to 40 GB, you want to add the increased size to the xfs root partition.

Procedure:

1. View the current partition. You can see that the root volume is resized to 40 GB, of which the xfs root partition is 6 GB. The extra disk space is unallocated and is not added to the disk partition.

```
[root@10-0-44-210 ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0  400G  0 disk
└─sda1   8:1    0  400G  0 part /mnt/nfs-data
vda    253:0    0   40G  0 disk
├─vda1 253:1    0    2G  0 part [SWAP]
```

```
└─vda2 253:2    0    6G  0 part /
```

2. Install the growpart tool.

```
[root@10-0-44-210 ~]# yum install -y cloud-utils-growpart
```

3. Resize the xfs root partition by using the `growpart <DeviceName> <PartionNumber>` command. Here, the **`DeviceName`** of the xfs root partition is *`/dev/vda`* and **`PartionNumber`** is 2.

```
[root@10-0-44-210 ~]# growpart /dev/vda 2
CHANGED: partition=2 start=4196352 old: size=12580864 end=16777216
 new: size=79689695 end=83886047
```

4. View the partitions. Then, you can see that the xfs root partition is resized from 6 GB to 38 GB.

```
[root@10-0-44-210 ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0  400G  0 disk
└─sda1   8:1    0  400G  0 part /mnt/nfs-data
vda    253:0    0   40G  0 disk
├─vda1 253:1    0    2G  0 part [SWAP]
└─vda2 253:2    0   38G  0 part /
```

5. Extend the XFS file system.

   a. To extend the XFS file system, make sure that the xfsprogs tool is installed. The installation command is as follows:

   ```
   [root@10-0-44-210 ~]# yum install xfsprogs
   ```

   b. Extend the file system in *`/dev/vda2`* by running the `xfs_growfs` command. Here, *`/`* is the mount point.

   ```
   [root@10-0-44-210 ~]# xfs_growfs /
   meta-data=/dev/vda2              isize=256    agcount=26,
   agsize=393152 blks
            =                       sectsz=512   attr=2,
   projid32bit=1
            =                       crc=0        finobt=0 spinodes
   =0
   data     =                       bsize=4096   blocks=9961211,
   imaxpct=25
            =                       sunit=0      swidth=0 blks
   naming   =version 2              bsize=4096   ascii-ci=0 ftype=
   0
   log      =internal               bsize=4096   blocks=2560,
   version=2
            =                       sectsz=512   sunit=0 blks,
   lazy-count=1
   realtime =none                   extsz=4096   blocks=0,
   rtextents=0
   ```

```
data blocks changed from 1572608 to 9961211
```

c. Check whether the file system reflects the increased volume size.

```
[root@10-0-44-210 ~]# df -h /
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda2        38G  3.3G   35G   9% /
```

Note:

We recommend that you install the expansion and formatting tools according to the actual operating system. For example,

- For CentOS 7, install the following tool:

```
yum install cloud-utils-growpart
yum install xfsprogs
```

- For Ubuntu 14, Ubuntu 16, Ubuntu 18, and Debian 9, install the following tool:

```
apt install cloud-guest-utils
apt install xfsprogs
```

- For Debian 8, openSUSE 42.3, openSUSE 13.1, and SLES 12 SP2, use the growpart or xfsprogs tool of the upstream version.

4. Resize the Windows partitions.

   You can resize disks of Windows partitions on the disk management page.

Note:

After you resize the disk of a Windows partition, scan the disk to take effect.

7.1.2 Volume

7.1.2.1 What is Volume?

A volume provides storage space for a VM instance. Volumes are categorized into root volumes and data volumes.

Note:

Volume management mainly involves data volumes.

Concepts

- Root volume: A root volume provides support for the system operations of a VM instance.
- Data volume: A data volume provides extended storage space for a VM instance.

Considerations

- A volume attached to a VM instance cannot be attached to a VM instance of another hypervisor type. For example, a volume attached to a KVM VM instance cannot be attached to a VMware VM instance.
- The storage space that a volume takes up is calculated based on the virtual size of the volume. When a volume is created, the virtual size of the volume is deducted. The actual storage space that the volume takes up is small upon creation while increases along with growing data writes.
- A non-shared volume can be attached to only one VM instance. A shared volume can be created on a Ceph primary storage and Shared Block primary storage and allows simultaneous access from multiple VM instances.
- A root volume is an integral part of a VM instance. It cannot be detached from a VM instance.
- A data volume attached to a VM instance can be detached from the VM instance and then attached to another VM instance of the same hypervisor type.
- When multiple primary storages are available, you can specify a primary storage to create a volume. If you do not specify a primary storage when you create a volume:
  - For Local Storage primary storages, the volume is created on the primary storage with largest available space by default.
  - For NFS primary storages, the volume is created on a random primary storage by default.
  - For the combination of Local Storage and NFS primary storages or the combination of Local Storage and Shared Mount Point (SMP) primary storages, by default, the volume is created on the primary storage that the root volume of the VM instance to which the volume is attached does not reside.
- You can set QoS for a data volume to limit disk bandwidth. Note that an excessively low QoS may greatly lower I/O performance.

7.1.2.2 Create a Volume

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Virtual Resource** > **Volume**. On the **Volume** page, click **Create Volume**. The **Create Volume** page appears.

The following lists the four volume creation methods:

- Create a non-shared volume based on a disk offering
- Create a non-shared volume based on a volume image

- Create a shared volume based on a disk offering
- Create a shared volume based on a volume image

Create Non-Shared Volume Based on Disk Offering

On the displayed page, set the following parameters:

- **Name**: Enter a name for the volume.
- **Description**: Optional. Enter a description for the volume.
- **Volumes**: Enter the number of volumes that you want to create.

  Note:

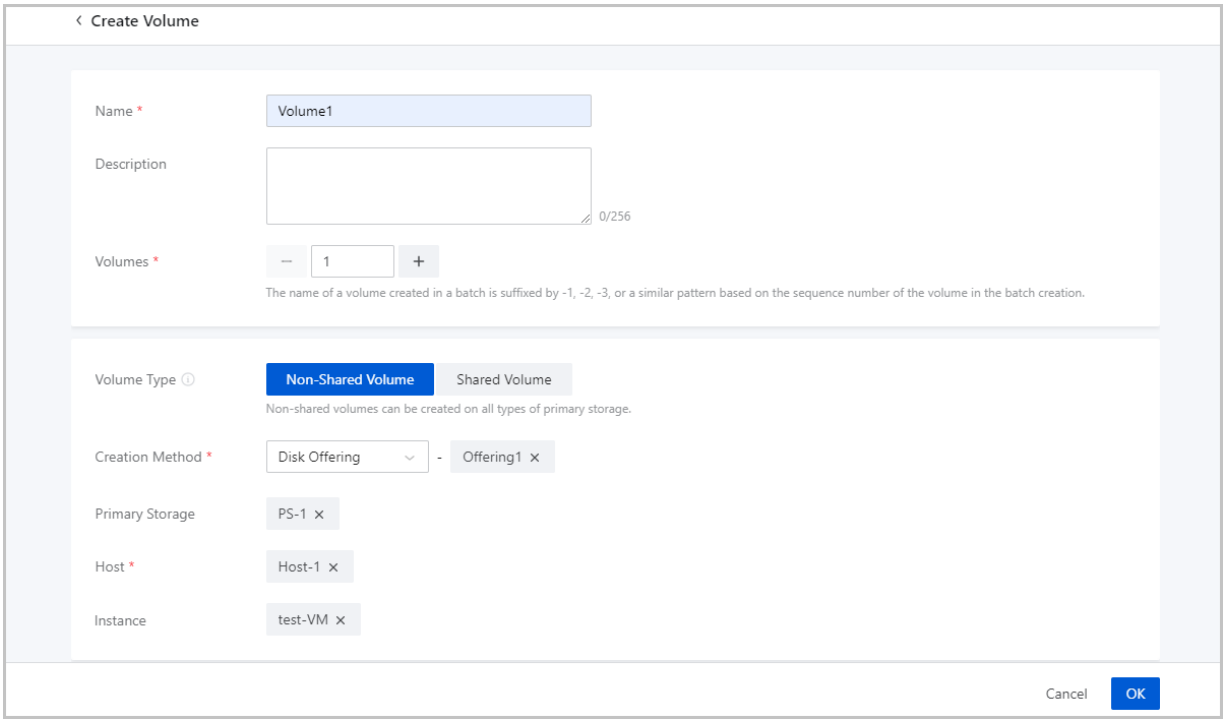
  Enter an integer that ranges from 1 to 24.

- **Volume Type**: Select Non-Shared Volume.
- **Creation Method**: Select a disk offering.
- **Primary Storage**: Optional. Select a primary storage.
- **Instance**: Optional. Select a VM instance or elastic baremetal instance to which the volume is attached.
- **VirtioSCSI**: This parameter indicates that the Virtio-SCSI bus is used to create an SCSI data volume.

  Note:

  - By default, VirtioSCSI is enabled if a shared storage is used, indicating that you can create VirtIO SCSI volumes.
  - If a LocalStorage primary storage is used, you can enable VirtioSCSI on the volume details page.
  - VirtIO SCSI volumes support multiple I/O queues, which can be identified as IDs (WWN).

Figure 7-21: Create Non-Shared Volume Based on Disk Offering



Create Non-Shared Volume Based on Volume Image

On the displayed page, set the following parameters:

- **Name**: Enter a name for the volume.
- **Description**: Optional. Enter a description for the volume.
- **Volumes**: Enter the number of volumes that you want to create.

> **Note:**
> You can only create one volume a time by using a volume image.

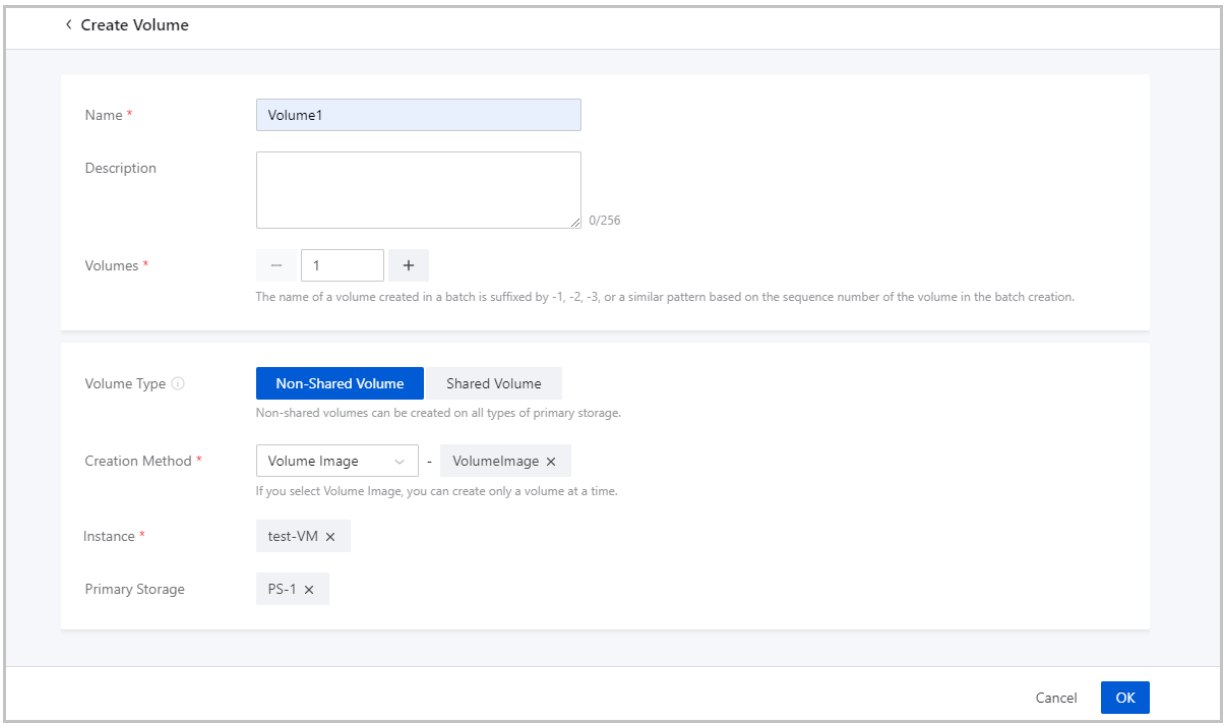
- **Volume Type**: Select Non-Shared Volume.
- **Creation Method**: Select a volume image.
- **Instance**: Optional. Select a VM instance or elastic baremetal instance to which the volume is attached.
- **Primary Storage**: Optional. Select a primary storage on which the volume is created.

> **Note:**
> You can use a volume image stored on an ImageStore backup storage to create a volume on a Ceph primary storage.

- **VirtioSCSI**: This parameter indicates that the Virtio-SCSI bus is used to create an SCSI data volume.

> **Note:**
>
> - By default, VirtioSCSI is enabled if a shared storage is used, indicating that you can create VirtIO SCSI volumes.
> - If a LocalStorage primary storage is used, you can enable VirtioSCSI on the volume details page.
> - VirtIO SCSI volumes support multiple I/O queues, which can be identified as IDs (WWN).

Figure 7-22: Create Non-Shared Volume Based on Volume Image



Create Shared Volume Based on Disk Offering

On the displayed page, set the following parameters:

- **Name**: Enter a name for the volume.
- **Description**: Optional. Enter a description for the volume.
- **Volumes**: Enter the number of volumes that you want to create.

> **Note:**
>
> Enter an integer that ranges from 1 to 24.

- **Volume Type**: Select Shared Volume.

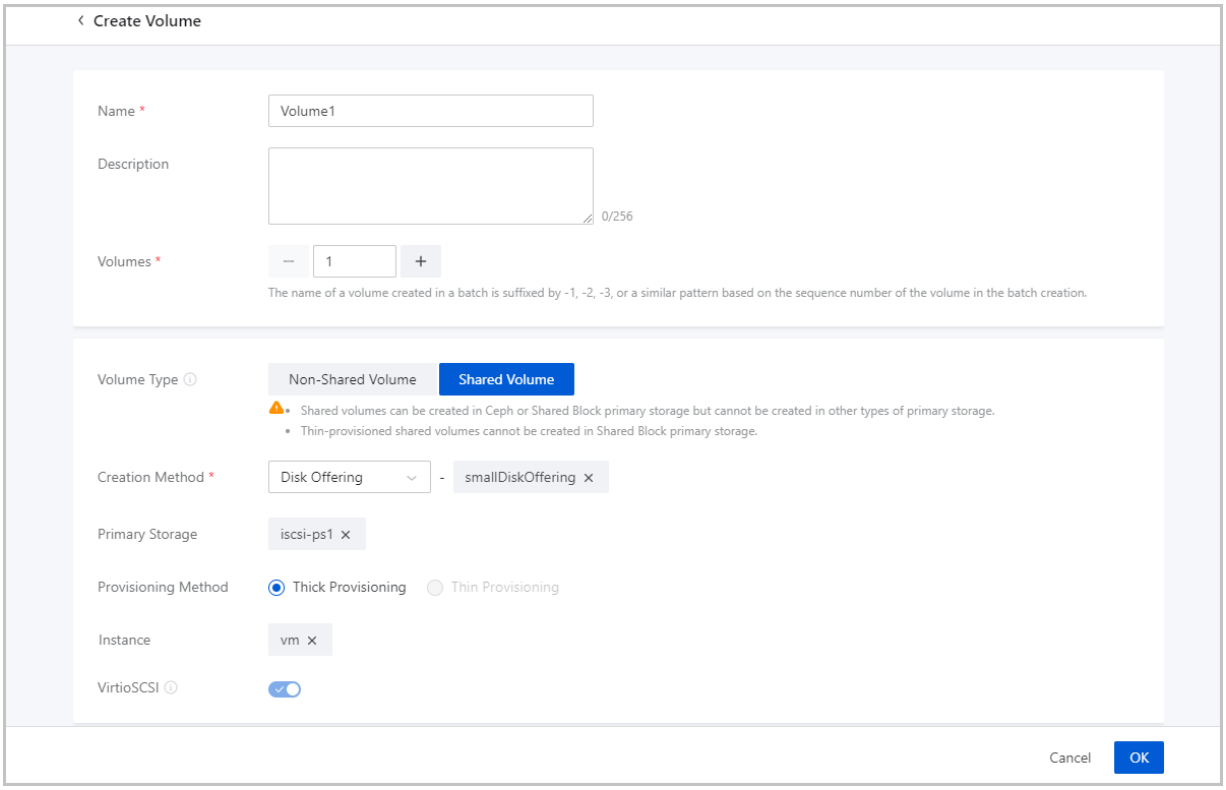
  Note:

  - You can create a shared volume on a Ceph primary storage or a Shared Block primary storage. Other types of primary storage do not support this operation.
  - You cannot create a thin-provisioned shared volume on a Shared Block primary storage.
- **Creation Method**: Select a disk offering.
- **Primary Storage**: Optional. Select a primary storage.
- **Instance**: Optional. Select a VM instance or elastic baremetal instance to which the volume is attached.
- **VirtioSCSI**: This parameter indicates that the Virtio-SCSI bus is used to create an SCSI data volume.

  Note:

  - By default, VirtioSCSI is enabled if a shared storage is used, indicating that you can create VirtIO SCSI volumes.
  - If a LocalStorage primary storage is used, you can enable VirtioSCSI on the volume details page.
  - VirtIO SCSI volumes support multiple I/O queues, which can be identified as IDs (WWN).

Figure 7-23: Create Shared Volume Based on Disk Offering



Create Shared Volume Based on Volume Image

On the displayed page, set the following parameters:

- **Name**: Enter a name for the volume.
- **Description**: Optional. Enter a description for the volume.
- **Volumes**: Enter the number of volumes that you want to create.

> **Note:**
> You can only create one volume a time by using a volume image.

- **Volume Type**: Select Shared Volume.

> **Note:**
>
> - You can create a shared volume on a Ceph primary storage or a Shared Block primary storage. Other types of primary storage do not support this operation.
> - You cannot create a thin-provisioned shared volume on a Shared Block primary storage.

- **Creation Method**: Select a volume image.

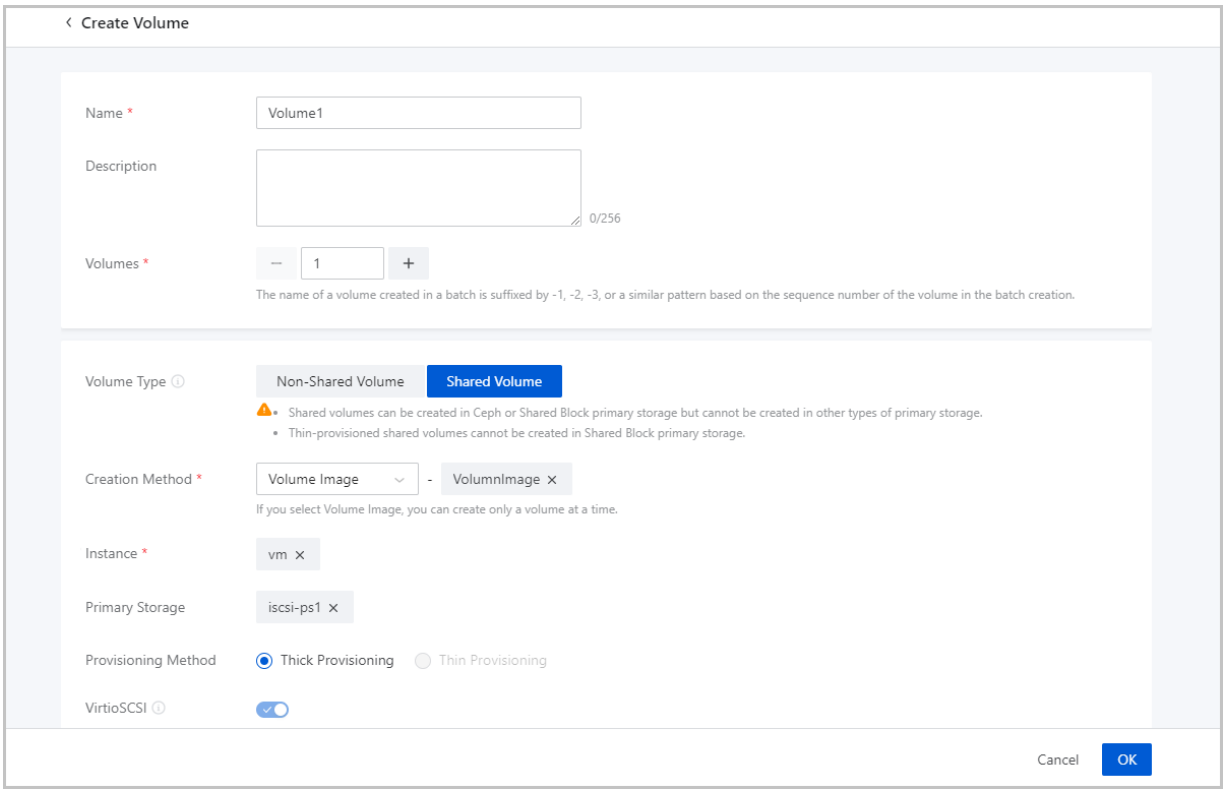
- **Instance**: Optional. Select a VM instance or elastic baremetal instance to which the volume is attached.
- **Primary Storage**: Optional. Select a primary storage on which the volume is created.

> **Note:**
> You can use a volume image stored on an ImageStore backup storage to create a volume on a Ceph primary storage.

- **VirtioSCSI**: This parameter indicates that the Virtio-SCSI bus is used to create an SCSI data volume.

> **Note:**
> - By default, VirtioSCSI is enabled if a shared storage is used, indicating that you can create VirtIO SCSI volumes.
> - If a LocalStorage primary storage is used, you can enable VirtioSCSI on the volume details page.
> - VirtIO SCSI volumes support multiple I/O queues, which can be identified as IDs (WWN).

Figure 7-24: Create Shared Volume Based on Volume Image



Notes

- You can batch create volumes only by using a disk offering.
- If you create a volume by using a disk offering, you can select a primary storage and VM instance based on your business requirements:
  - If you do not select a primary storage or VM instance, the created volume is in Uninstantiated state and is listed on the Uninstantiated tab.
  - If you select a VM instance but do not select a primary storage:
    - When only one primary storage is available, the volume is created on the primary storage.
    - When multiple primary storages are available:
      - If all these primary storages are of Local Storage type, the volume is created on the primary storage with largest available space by default.
      - If all these primary storages are of NFS or Shared Block type, the volume is created on a random primary storage by default.
      - If these primary storages are a combination of Local Storage and NFS primary storages, a combination of Local Storage and Shared Mount Point (SMP) primary storages, or a combination of Local Storage and Shared Block primary storages, by default, the volume is created on the primary storage that the root volume of the VM instance to which the volume is attached does not reside.
      - If these primary storages are a combination of Ceph and Shared Block primary storages, the volume is created on the primary storage with largest available space by default.
  - If you only select a primary storage and do not select a VM instance, the created volume is in Available state and takes up storage space of primary storage.

Note:

- If you select a primary storage of the **Local Storage** type, you must select a host.
- If you select a primary storage of the **Ceph** type, you can select a Ceph storage pool.
- If you select a primary storage of the **Shared Block** type, you must select a provisioning method, including thin provisioning and thick provisioning.
  - Thin provisioning: allocates storage space to a volume based on the data amount. This method improves usage efficiency of storage space.

— Thick provisioning: preallocates storage space that a volume needs. This method ensures sufficient storage space for a volume and thus ensures high storage performance.

- If you create a volume by using a volume image and do not select a primary storage:
  - — If the volume image is stored on a Ceph backup storage, the volume is created on a Ceph primary storage.
  - — If the volume image is not stored on a Ceph backup storage:
    - ■ When multiple primary storages are available:
      - ■ ■ If all these primary storages are of Local Storage type, the volume is created on the primary storage with largest available space by default.
      - ■ If all these primary storages are of NFS or Shared Block type, the volume is created on a random primary storage by default.
      - ■ If these primary storages are a combination of Local Storage and NFS primary storages, a combination of Local Storage and Shared Mount Point (SMP) primary storages, or a combination of Local Storage and Shared Block primary storages, by default, the volume is created on the primary storage that the root volume of the VM instance to which the volume is attached does not reside.
      - ■ If these primary storages are a combination of Ceph and Shared Block primary storages, the volume is created on the primary storage with largest available space by default.

7.1.3 Image

7.1.3.1 What is Image?

An image is a template file used to create a VM instance or volume. Images are categorized into system images and volume images.

- A system volume image can be of the ISO or Image type while a data volume image can only be of the Image type.
- Image-type images can be in raw or qcow2 format.
- Images are stored on backup storages. When an image is used to create a VM instance or volume, the image is downloaded to a primary storage and cached there.

The platform type of an image decides whether the VM instances that are created based on the image use KVM VirtIO drivers, including VirtIO disk drivers and VirtIO NIC drivers. The following lists the available platform types of an image:

- Linux: uses VirtIO drivers.
- Windows: does not use VirtIO drivers. QEMU is used to emulate devices. The operating system (OS) contained in the image is Windows that does not install VirtIO.
- WindowsVirtio: uses VirtIO drivers. The operating system (OS) contained in the image is Windows that has installed VirtIO drivers, including VirtIO disk drivers and VirtIO NIC drivers.
- Other: does not use VirtIO drivers. QEMU is used to emulate devices. The operating system (OS) contained in the image can be of any type and version. This platform type allows compatibility with earlier versions of an OS that does not support VirtIO drivers, such as RHEL 5.8.
- Paravirtualization: uses VirtIO drivers. The operating system (OS) contained in the image can be of any type and version that has installed VirtIO drivers.

You can add an image by specifying an image URL or uploading a local file:

- **URL**: Enter a specified URL to add an image. You can enter a URL by using either of the following syntax:
  - A URL that starts with http or https:
    - Syntax: *`http://host[:port]/path/file`* or *`https://host[:port]/path/file`*.
  - A URL that starts with ftp:
    - Syntax that does not specifies the user: *`ftp://hostname[:port]/path/file`*.
    - Syntax that specifies the user: *`ftp://user:password@hostname[:port]/path/file`*.
  - A URL that starts with sftp:
    - Syntax that specifies the user identity: *`sftp://user:password@hostname[:port]/path/file`*
    - User-identity-free syntax: *`sftp://user@hostname[:port]/path/file`*.
  - The absolute path of an image file that is stored on a backup storage. The backup storage that stores the image file can be an ImageStore backup storage.

    Syntax: *`file:///path/file`*

Note:

- The image file to be added to the destination backup storage must exist and the backup storage needs to have access to the URL of the image file.
- If you enter a URL that starts with sftp and does not specify user identity, make sure that you enable password-free SSH login to the server that stores the image file.
- For the progress bar and resumption from breakpoint features:
  - For both ImageStore and Ceph backup storage, a progress bar will appear to display the upload progress. In addition, upload resumption from breakpoints is also supported.
- If you specify a URL with the `file:///` syntax to add an image:
  - Ceph backup storage does not support the *file:///* syntax.
  - The three forward slashes (/) in `file:///` represents the an absolute path of a file on a backup storage. For example, if you specify the URL `file:///opt/dvd/image-1.4.qcow2`, you add the image file named *image-1.4.qcow2* in the `/opt/dvd` path of a backup storage to the Cloud.

- **Local File**: Select a local image file that the current browser can access and upload the image file to the specified backup storage. The backup storage that stores the image file can be an ImageStore or Ceph backup storage.

Note:

If you upload a local image file, the local browser serves as a transfer station. Do not refresh or close the browser or stop management node services. Otherwise, the image addition may fail.

7.1.3.2 Add an Image

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Compute Configuration** > **Image**. On the **Image** page, click **Add Image**. The **Add Image** page appears.

The following lists the two image addition scenarios:

- Add a system image
- Add a volume image

Add System Image

On the displayed page, set the following parameters:

- **Name**: Enter a name for the image.

  The name must be 1 to 128 characters in length and can contain Chinese characters, English letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the image.
- **Image Type**: System Image.
- **Image Format**: Select an image format. You can select qcow2, iso, or raw.
- **CPU Architecture**: Select a CPU architecture for the image. VM instances created from the image use this CPU architecture.

  Note:
  If you select aarch64 or mips64, set the BIOS mode to UEFI.
- **Platform**: Select an image platform type.

  The platform type of an image decides whether the VM instance created based on the image uses KVM VirtIO drivers, including VirtIO disk drivers and VirtIO NIC drivers. The following lists the available platform types of an image:

  - Linux: uses VirtIO drivers.
  - Windows: does not use VirtIO drivers. QEMU is used to emulate devices. The operating system (OS) contained in the image is Windows that does not install VirtIO.
  - WindowsVirtio: uses VirtIO drivers. The operating system (OS) contained in the image is Windows that has installed VirtIO drivers, including VirtIO disk drivers and VirtIO NIC drivers .
  - Other: does not use VirtIO drivers. QEMU is used to emulate devices. The operating system (OS) contained in the image can be of any type and version. This platform type allows compatibility with earlier versions of an OS that does not support VirtIO drivers, such as RHEL 5.8.
  - Paravirtualization: uses VirtIO drivers. The operating system (OS) contained in the image can be of any type and version that has installed VirtIO drivers.
- **OS**: Select an operating system that is consistent with the image.
- **VirtIO**: Choose whether to enable VirtIO according to your actual operating system and platform.
- **Backup Storage**: Select a backup storage.
- **Image Path**: Specify an image URL or upload a local file:

— **URL**: Enter a specified URL to add an image. You can enter a URL by using either of the following syntax:

- A URL that starts with http or https:
  - Syntax: `http://host[:port]/path/file` or `https://host[:port]/path/file`.
- A URL that starts with ftp:
  - Syntax that does not specifies the user: `ftp://hostname[:port]/path/file`.
  - Syntax that specifies the user: `ftp://user:password@hostname[:port]/path/file`.
- A URL that starts with sftp:
  - Syntax that specifies the user identity: `sftp://user:password@hostname[:port]/path/file`
  - User-identity-free syntax: `sftp://user@hostname[:port]/path/file`.
- The absolute path of an image file that is stored on a backup storage. The backup storage that stores the image file can be an ImageStore backup storage.

  Syntax: `file:///path/file`

Note:

- The image file to be added to the destination backup storage must exist and the backup storage needs to have access to the URL of the image file.
- If you enter a URL that starts with sftp and does not specify user identity, make sure that you enable password-free SSH login to the server that stores the image file.
- For the progress bar and resumption from breakpoint features:
  - If you use an ImageStore backup storage, a progress bar will appear to display the upload progress. In addition, upload resumption from breakpoints is also supported.
  - If you use a Ceph backup storage, a progress bar will appear to display the upload progress. However, upload resumption from breakpoints is not supported.
- If you specify a URL with the `file:///` syntax to add an image:
  - Ceph backup storage does not support the *file:///* syntax.
  - The three forward slashes (/) in `file:///` represents the absolute path of a file on a backup storage. For example, if you specify the URL `file:///opt/dvd/image-1`

`.4.qcow2`, you add the image file named *image-1.4.qcow2* in the `/opt/dvd` path of a backup storage to the Cloud.

— **Local File**: Select a local image file that the current browser can access and upload the image file to the specified backup storage. The backup storage that stores the image file can be an ImageStore or Ceph backup storage.

Note:

If you upload a local image file, the local browser serves as a transfer station. Do not refresh or close the browser or stop management node services. Otherwise, the image addition may fail.

- **BIOS Mode**: Select a BIOS mode. You can select the Legacy or UEFI mode.

— Legacy: This mode supports all operating systems (OSs) and ensures stable operation. We recommend you select this mode.

— UEFI: This mode supports Windows and CentOS. Note that the Compatibility Support Module (CSM) must be enabled for Windows 7 and Windows Server 2008 R2.

Note:

Mode mismatch may cause VM instances unable to work as expected. Select a mode based on your business needs:

- If you add an image in qcow2 or raw format, select the mode consistent with the mode used when the image was created.
- If you add an image in iso format, you can select either of the two modes. OS will be boot based on the selected mode.
- If you want to boot the OS of a VM instance in UEFI mode, we recommend that you select a VM image that is created from one of the OS listed in the following table.

OS	BIOS Mode	Supported Versions
Windows	UEFI	• Windows 8 or later
	UEFI with CSM	• Windows 7 • Windows Server 2008 R2
Linux	UEFI	• CentOS 7.2 • CentOS 7.3 • CentOS 7.4 or later

- As mentioned in the preceding table, you can create a Linux-based VM instance by using an image that is created from CentOS 7.4 or later and that uses the UEFI mode. However, if the VM instance is restarted, the system may enter the UEFI Shell. To avoid this situation, you can use one of the following methods to boot the OS:

  — Use a script to skip the UEFI Shell and directly load the OS.

  In the installed OS, run the `vim /boot/efi/startup.nsh` command to create a file, enter the following content in the file, and save the file. Then when you restart the VM instance, the UEFI Shell is skipped and the OS is boot.

  ```
  FS0:
  CD EFI
  CD centos
  shimx64-centos.efi
  ```

  — Manually exit the UEFI Shell.

  If you have entered the UEFI Shell, run the following commands to exit the UEFI Shell:

  ```
  Shell> fs0:
  FS0:\> cd EFI
  FS0:\EFI\> cd centos
  FS0:\EFI\centos\> shimx64-centos.efi
  ```

- If you use a Window-based VM instance such as Windows Server 2012 R2, Windows Server 2016, or Windows 10 that has its OS boot in UEFI mode, the following figure will display after you start the VM instance. In this case, press any key to continue the installation of the OS. Otherwise, the system will enter the UEFI Shell.

  Figure 7-25: Press Any Key to Continue

  If you have entered the UEFI Shell, run the following commands to exit the UEFI Shell:

  ```
  Shell> fs0:
  FS0:\> dir
  FS0:\> cd EFI
  FS0:\EFI\> cd BOOT
  FS0:\EFI\BOOT\> BOOTX64.EFI
  ```

  Then press any key in a timely manner. Otherwise, the system will reenter the UEFI Shell.

- **Enable CSM**: Optional. Choose whether to use the CSM.

The CSM can only be used for devices that can only work in Legacy mode and OSs that do not support or partially support the UEFI mode.

Note:

For Windows 7 and Windows Server 2008 R2, you must enable the CSM.

- **QEMU Guest Agent**: Optional. Choose whether the current image has installed QEMU Guest Agent (QGA).

  Note:

  If the image has installed QGA and has set the agent as auto-start and you use the image to create a VM instance, you can modify the passwords of this VM instance, the clones of this VM instance, and the VM instances created from the image that is created from this VM instance when all these instances are in running state.

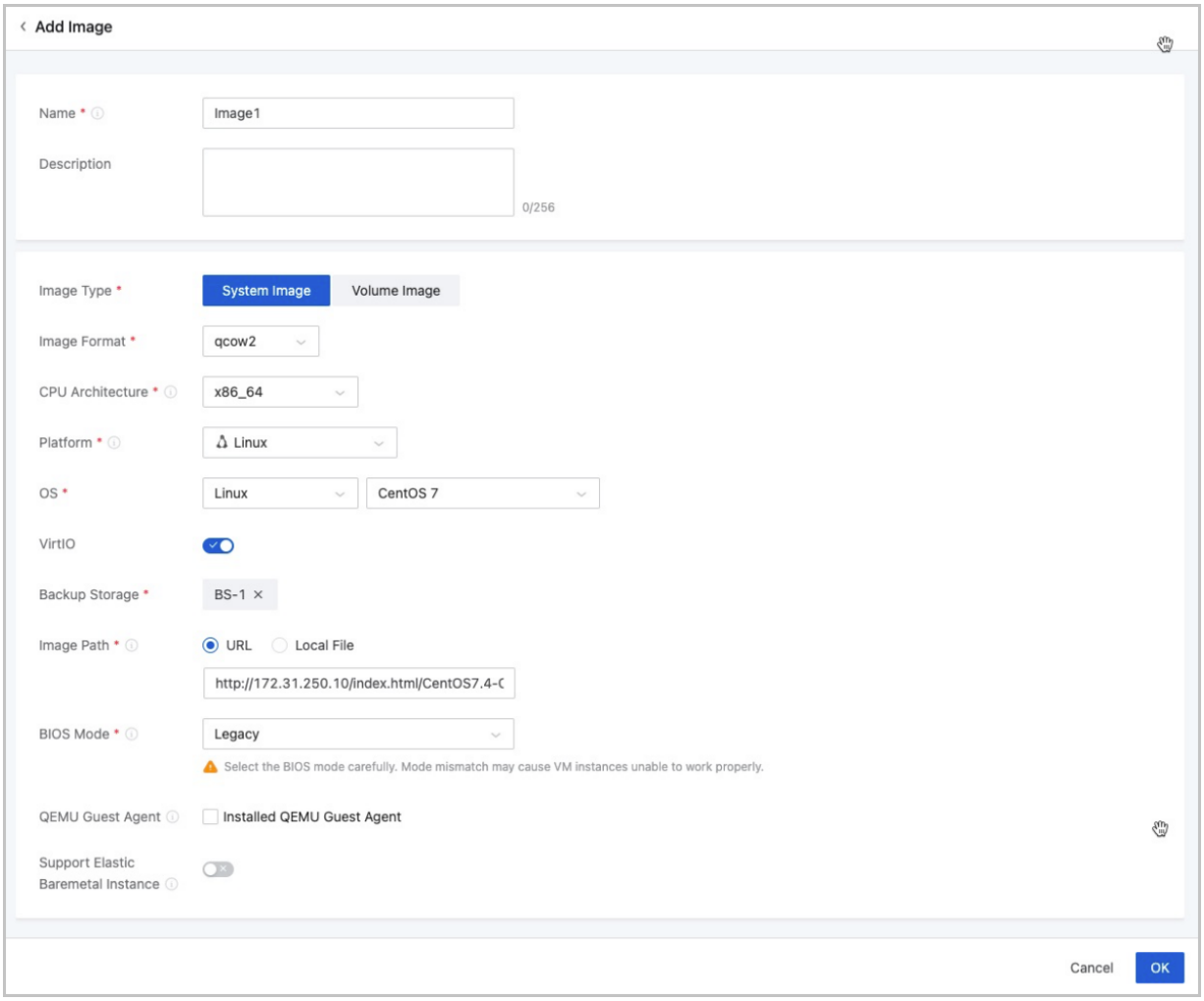
- **Support Elastic Baremetal Instance**: Optional. Choose whether the image can be used to create an elastic baremetal instance. If enabled, the image can be used to create an elastic baremetal instance.

  Note:

  When you add an image of an elastic baremetal instance, make sure:

  - The image has installed the agent. Otherwise, after you use the image to create an elastic baremetal instance, you cannot open the console or modify the password of the elastic baremetal instance. In addition, you cannot attach a volume or network to the instance or detach a volume or network from the instance.
  - The BIOS mode of the image is the same the system configuration. Default: UEFI. If you want to use Legacy, contact the technical support.

Figure 7-26: Add System Image

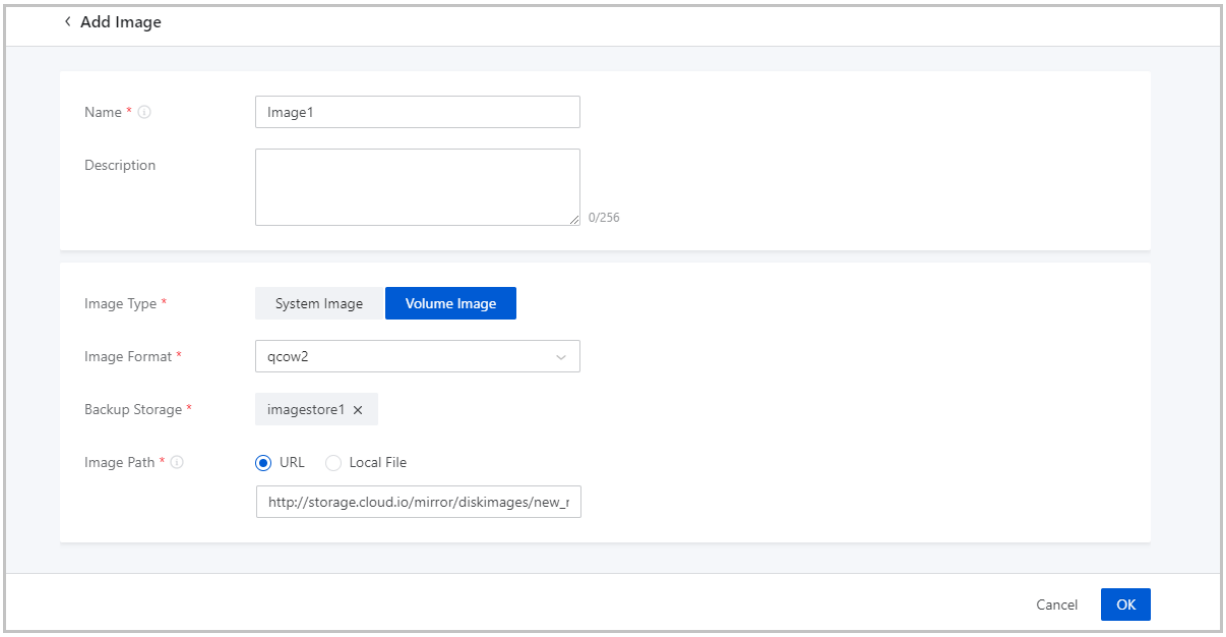


Add Volume Image

On the displayed page, set the following parameters:

- **Name**: Enter a name for the image.
- **Description**: Optional. Enter a description for the image.
- **Image Type**: Select System Image.
- **Image Format**: Select an image format. You can select qcow2, iso, or raw.
- **Backup Storage**: Select a backup storage.
- **Image Path**: Specify an image URL or upload a local file.

Figure 7-27: Add Volume Image



7.1.3.3 Manage an Image

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Compute Configuration** > **Image**. Then, the **Image** page appears.

The following table lists the actions that you can perform on an image.

Action	Description
Add Image	Add an image to a backup storage.
Edit Image	Edit the name and description of an image.
Enable Image	Enable an image that is in Disabled state.
Disable Image	Disable an image that is in Enabled state. If you disable an image, you cannot use the image to create a VM instance. VM instances created by using the image before the disablement are not affected.
Export Image	Export an image. ImageStore and Ceph backup storages support image export. Exported images are displayed on the **Exported** tab. **Note:** • Image exports from ImageStore backup storages may take a long time if the image size is great. • You can also run the rbd command on a Ceph backup storage to export an image from the Ceph backup storage. • An exported image cannot be exported again.

Action	Description
Storage Migration	Migrate an image across network shared storages. You can migrate an image across Ceph backup storages whose monitor nodes are connected with each. **Note:** • After the storage migration, the raw data is reserved in the source backup storage. You can go to the details page of the source Ceph backup storage and view the data on the Data Cleanup tab. • You can **Cleanup** the raw data. Before you perform this operation, make sure that the storage migrated data is intact. Cleaning up raw data will make the data unrecoverable. Proceed with caution.
Sync Image	Synchronize images that are stored in one or more backup storages to a specified backup storage that shares the same monitoring node with the source backup storages. Image synchronization is supported only by ImageStore backup storages. **Note:** To ease the pressure on the management network, you can set a network dedicated to image synchronizations by using either of the two methods: • Set an image synchronization network when you add a backup storage to the platform. • Set an image synchronization network on the details page of a backup storage. The setting takes effect immediately.
Set Sharing Mode	Set the sharing mode of the resource. The platform provides the following sharing modes: • Share Globally: shares the resource with all projects and accounts. • Share to Specified Projects/Accounts: shares the resource with specified projects and accounts. • Not Share: revokes the resource from projects and accounts to which the resource is shared. If you set Sharing Mode to Not Share for the resource, other projects and accounts cannot use the resource. **Note:** • If you modify the Sharing Mode setting of the resource from Share Globally to Share to Specified Projects/Accounts, the resource

Action	Description
	is visible only to the specified projects or accounts to which the resource is shared. • If the resource that you share with projects or accounts was used by the projects or accounts and then you modify the Sharing Mode setting of the resource, the resource is reserved for the projects or accounts until it is released.
Delete Image	Delete an image. A deleted image is displayed on the **Recycle Bin** tab.
Recover Image	Recover a deleted image. If you recover a deleted image, the image is displayed on the **Available** tab.
Expunge Image	Expunge a deleted image. You can only expunge an image that is in the recycle bin.
Download Exported Image	Download an exported image. ImageStore and Ceph backup storages support image export. If you download an exported image, the download is implemented by the browser. **Note:** ImageStore backup storages allow you to view the MD5 value of the downloaded image to check whether the downloaded image is the same as the exported image.
Delete Exported Image	Delete an exported image. **Note:** • In an ImageStore backup storage, image files are stored in the format of chips. Only when you export an image, or use an image, for example, to create a VM instance will a complete image file be produced. When you delete an exported image, only the complete image file is deleted. The image chips in the backup storage remain intact. • In a Ceph backup storage, image files are stored in the format of blocks. When you delete an exported image, only the exported image file is deleted. The image in the Ceph backup storage remain intact.

7.1.4 Instance Offering

7.1.4.1 What is Instance Offering?

An instance offering defines the number of vCPU cores, memory size, network bandwidth, and other configuration settings of VM instances.

7.1.4.2 Create an Instance Offering

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Compute Configuration** > **Instance Offering**. On the **Instance Offering** page, click **Create Instance Offering**. Then, the **Create Instance Offering** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the instance offering.

  The instance offering name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the instance offering.
- **CPU**: Enter the number of CPU cores of a VM instance. Note that this value must be an integer. Unit: core. Valid values: 1 to 1024.
- **Memory**: Set the size of the VM memory. Note that this value must be an integer. Unit: MB, GB, and TB. Valid values: 16 MB to 100 TB.
- **Host Allocation Strategy**: Specify how the Cloud allocates hosts when you create VM instances. Default strategy: **Host with min. running VMs**.
  - **Host with min. running VMs**: Allocates the host with the minimum number of running VM instances to create VM instances.
  - **Host with min. CPU utilization**: Allocates the host with the minimum CPU utilization to create VM instances.

  Note:

  - The Cloud collects the host CPU loads over a period of time, calculates the CPU average utilization during this period, and then selects the host with the lowest CPU utilization to create VM instances.
  - By default, the Cloud collects data at an interval of 10 minutes. You can change the collection cycle by using the following method:

Go to **Settings** > **Platform Setting** > **Global Setting** > **Advanced** > **Host**, locate **Host CPU Utilization Collection Interval**, and click the **Edit** icon.

— **Host with min. memory utilization**: Allocates the host with the minimum memory utilization to create VM instances.

Note:

- The Cloud collects the host memory loads over a period of time, calculates the memory average utilization during this period, and then selects the host with the lowest memory utilization to create VM instances.
- By default, the Cloud collects data at an interval of 10 minutes. You can change the collection cycle by using the following method:

  Go to **Settings** > **Platform Setting** > **Global Setting** > **Advanced** > **Host**, locate **Host Memory Utilization Collection Interval**, and click the **Edit** icon.

— **Host with max. running VMs**: Allocates the host with the maximum number of running VM instances to create VM instances. Before you can use this option, set the maximum number of VM instances that can run on a host. Then, the Cloud selects the host that meets the requirements to create VM instances. If no host is available, you will fail to create a VM instance.

— **Host where the VM located last time**: When you restart a stopped VM instance, the system selects the host where the VM was running last time.

Note:

If you start a VM instance for the first time, the Cloud allocates a host randomly.

— **Random allocation**: Randomly allocates a host to create VM instances.

- **Set Disk Bandwidth**: Optional. Set an upper limit for the I/O bandwidth of a volume.

  If not set, the I/O bandwidth of a volume is not limited. Unit: MB/s, GB/s, and TB/s. You can set the I/O bandwidth by using either of the following methods:

  - **Total Speed**: Set an upper limit for the total read and write speed of a volume.
  - **Read/Write Speed**: Set an upper limit for the read or write speed of a volume.

    — **Read Speed**: Optional. Set an upper limit for the read speed of a volume.

    — **Write Speed**: Optional. Set an upper limit for the write speed of a volume.

- **Set Network Bandwidth**: Optional. Set an upper limit for the network bandwidth of a VM instance.

  If not set, the network bandwidth of a VM instance is not limited. Unit: Kbps, Mbps, and Gbps. You can set the network bandwidth by using either of the following methods:

  - **Upstream Bandwidth**: Optional. Set an upper limit of the network bandwidth for uploading data from a VM instance.
  - **Downstream Bandwidth**: Optional. Set an upper limit of the network bandwidth for downloading data from a VM instance.

  Note:
  Before you make any settings, make sure that you fully understand the configurations of the disk bandwidth and network bandwidth. Otherwise, you might fail to upload files to or download files from a VM instance.

- **Advanced Parameter**: Optional. Configure a JSON file to customize disk performance.

  Sample:

```
{
  "allocate": {
    "primaryStorage": {
      "type": "Enter a primary storage type. Valid values: Ceph,
LocalStorage, NFS, and SharedBlock.",
      "uuid": "Enter the UUID of a primary storage.",
      "poolNames": [
        "Enter the name of a Ceph pool. Delete this parameter if you
 do not specify a Ceph primary storage."
      ]
    }
  },
  "priceUserConfig": {
    "rootVolume": {
      "priceKeyName": "Set the billing name of a root volume.
Make sure that advanced parameter setting in the pricing list is
consistent with this setting. Otherwise, the corresponding bills
cannot be generated."
    }
  },
  "displayAttribute": {
    "rootVolume": {
      "diskType": "Set the display type of a root volume. You can
view this parameter setting on the VM details page."
    }
  }
}
```

  The preceding configuration settings can be divided into the following three parts:

1. Set the primary storage for root volumes.

```
"allocate": {
    "primaryStorage": {
      "type": "Enter a primary storage type. Valid values: Ceph,
LocalStorage, NFS, and SharedBlock.",
      "uuid": "Enter the UUID of a primary storage.",
      "poolNames": [
        "Enter the name of a Ceph pool. Delete this parameter if
you do not specify a Ceph primary storage."
      ]
    }
  }
```

- **`type`**: Enter a primary storage type. Valid values: Ceph, LocalStorage, NFS, and SharedBlock. If you specify a Ceph primary storage, you can specify a Ceph pool.
- **`uuid`**: Enter the UUID of a primary storage.
- **`poolNames`**: Enter the name of a Ceph pool. Delete this parameter if you do not specify a Ceph primary storage.

Note:

If you do not specify a primary storage, delete the preceding parameter settings.

2. Set the billing type of a root volume.

```
"priceUserConfig": {
    "rootVolume": {
      "priceKeyName": "Set the billing name of a root volume.
Make sure that advanced parameter setting in the pricing list is
consistent with this setting. Otherwise, the corresponding bills
cannot be generated."
    }
  }
```

- **`priceKeyName`**: Set the billing name of a root volume. Make sure that advanced parameter setting in the pricing list is consistent with this setting. Otherwise, the corresponding bills cannot be generated.

Note:

If you do not need billing settings, delete the preceding parameter settings.

3. Set the display type of a root volume.

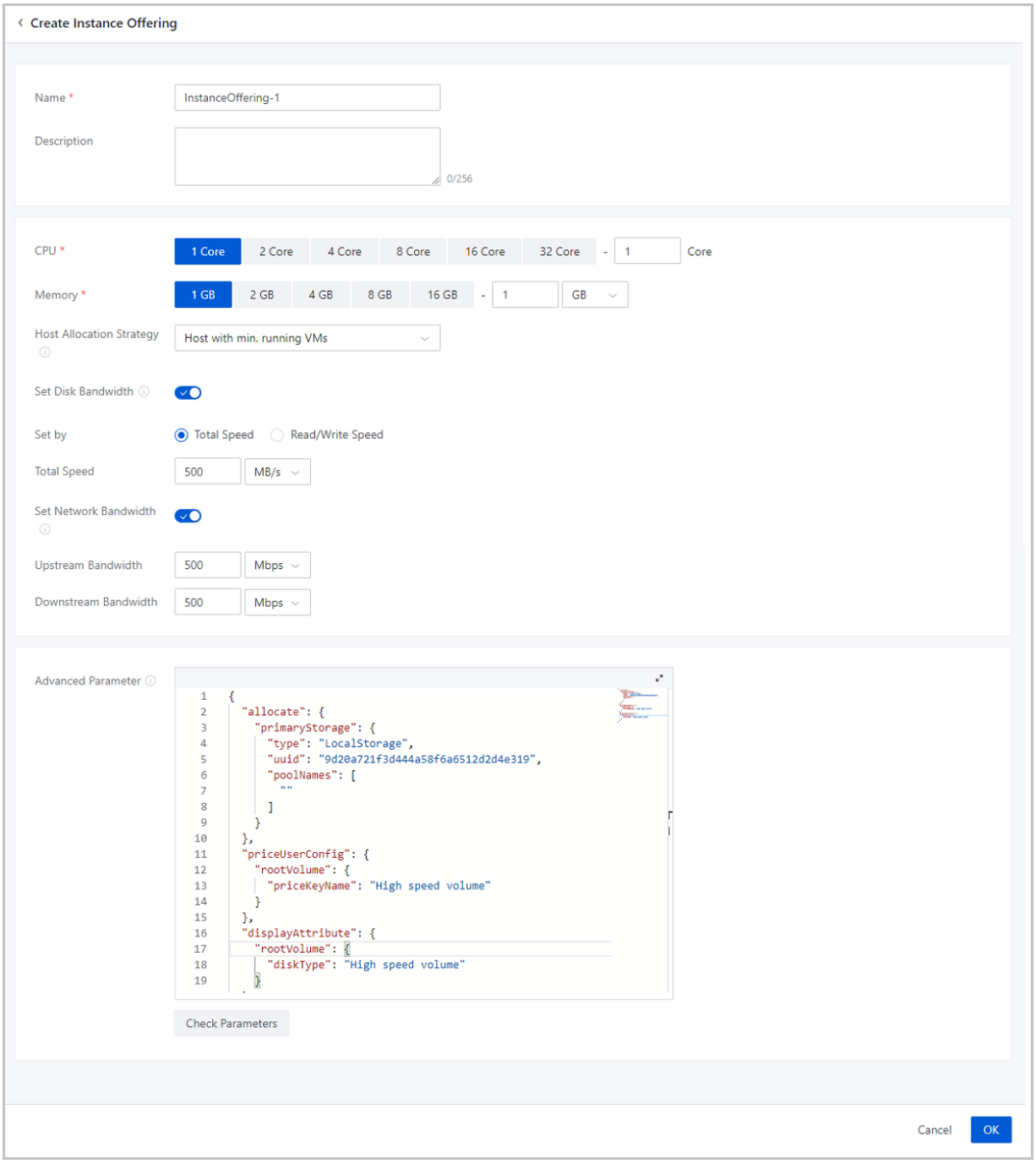
```
"displayAttribute": {
    "rootVolume": {
      "diskType": "Set the display type of a root volume. You can
view this parameter setting on the VM details page."
    }
```

```
}
```

- **`rootVolume`**: Set the display type of a root volume. You can view this parameter setting on the VM details page. You can also set multiple attributes in key-value pair format.

> **Note:**
> If you do not need special display, delete the preceding parameter settings.

Figure 7-28: Create Instance Offering



7.1.4.3 Manage an Instance Offering

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Compute Configuration** > **Instance Offering**. Then, the **Instance Offering** page is displayed.

The following table lists the actions that you can perform on an instance offering.

Action	Description
Create Instance Offering	Create an instance offering.
Edit Instance Offering	Edit the name and description of the instance offering.
Enable Instance Offering	Enable the instance offering when it is disabled.
Disable Instance Offering	Disable the instance offering when it is enabled.
Set Sharing Mode	Set the sharing mode of the resource. The platform provides the following sharing modes: • Share Globally: shares the resource with all projects and accounts. • Share to Specified Projects/Accounts: shares the resource with specified projects and accounts. • Not Share: revokes the resource from projects and accounts to which the resource is shared. If you set Sharing Mode to Not Share for the resource, other projects and accounts cannot use the resource. **Note:** • If you modify the Sharing Mode setting of the resource from Share Globally to Share to Specified Projects/Accounts, the resource is visible only to the specified projects or accounts to which the resource is shared. • If the resource that you share with projects or accounts was used by the projects or accounts and then you modify the Sharing Mode setting of the resource, the resource is reserved for the projects or accounts until it is released.
Delete Instance Offering	Delete the instance offering. In this case, a dialog box will be displayed, asking you to confirm the delete action.

7.1.5 Disk Offering

7.1.5.1 What is Disk Offering?

A disk offering defines the capacity and other configuration settings of volumes.

A disk offering can be used to create root volumes and data volumes.

7.1.5.2 Create a Disk Offering

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Virtual Resource** > **Disk Offering**. On the **Disk Offering** page, click **Create Disk Offering**. The **Create Disk Offering** page appears.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the disk offering.

  The name must be 1 to 128 characters in length and can contain Chinese characters, English letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the disk offering.
- **Disk Size**: Set the capacity of a volume.
- **Set Disk Bandwidth**: Optional. Set an upper limit for the I/O bandwidth of a volume.

  If you do not set this parameter, the I/O bandwidth of a volume is not limited. Unit: MB/s, GB/s, and TB/s. You can set the I/O bandwidth by using either of the following methods:

  - **Total Speed**: Set an upper limit for the total read and write speed of a volume.
  - **Read/Write Speed**: Set an upper limit for the read or write speed of a volume.
    - **Read Speed**: Optional. Set an upper limit for the read speed of a volume.
    - **Write Speed**: Optional. Set an upper limit for the write speed of a volume.
- **Advanced Parameter**: Optional. Configure a JSON file to customize disk performance.

  The following is a sample JSON configuration file:

```
{
  "allocate": {
    "primaryStorage": {
      "type": "Enter a primary storage type. Valid values: Ceph,
LocalStorage, NFS, and SharedBlock.",
      "uuid": "Enter the UUID of a primary storage.",
      "poolNames": [
        "Enter the name of a Ceph pool. Delete this parameter if you
 do not specify a Ceph primary storage."
      ]
```

```
    }
  },
  "priceUserConfig": {
    "volume": {
      "priceKeyName": "Set a display name of the billing type for
data volumes. The advanced parameter setting of the billing type in
 the pricing list must be consistent with this setting. Otherwise,
this billing type cannot be generated."
    }
  },
  "displayAttribute": {
    "volume": {
      "diskType": "Set the attribute display name of data volumes.
You can view this parameter setting on the volume details page."
    }
  }
}
```

The preceding configuration settings can be divided into the following three parts:

1. Configure the primary storage where a data volume is stored:

```
"allocate": {
    "primaryStorage": {
      "type": "Enter a primary storage type. Valid values: Ceph,
LocalStorage, NFS, and SharedBlock.",
      "uuid": "Enter the UUID of a primary storage.",
      "poolNames": [
        "Enter the name of a Ceph pool. Delete this parameter if
you do not specify a Ceph primary storage."
      ]
    }
  }
```

- `type`: Enter a primary storage type. Valid values: Ceph, LocalStorage, NFS, and SharedBlock. If you specify a Ceph primary storage, you can specify a Ceph pool.
- `uuid`: Enter the UUID of a primary storage.
- `poolNames`: Enter the name of a Ceph pool. Delete this parameter if you do not specify a Ceph primary storage.

Note:

If you do not specify a primary storage, delete the preceding parameter settings.

2. Configure the billing type of a data volume:

```
"priceUserConfig": {
    "volume": {
      "priceKeyName": "Set a display name of the billing type
for data volumes. The advanced parameter setting of the billing
 type in the pricing list must be consistent with this setting.
Otherwise, this billing type cannot be generated."
    }
```

```
  }
```

- `priceKeyName`: Set a billing item for data volumes. The advanced parameter setting of the billing item in the pricing list must be consistent with this setting. Otherwise, this billing item cannot be generated.

Note:

If you do not need billing settings, delete the preceding parameter settings.

3. Configure the display attributes of a data volume:

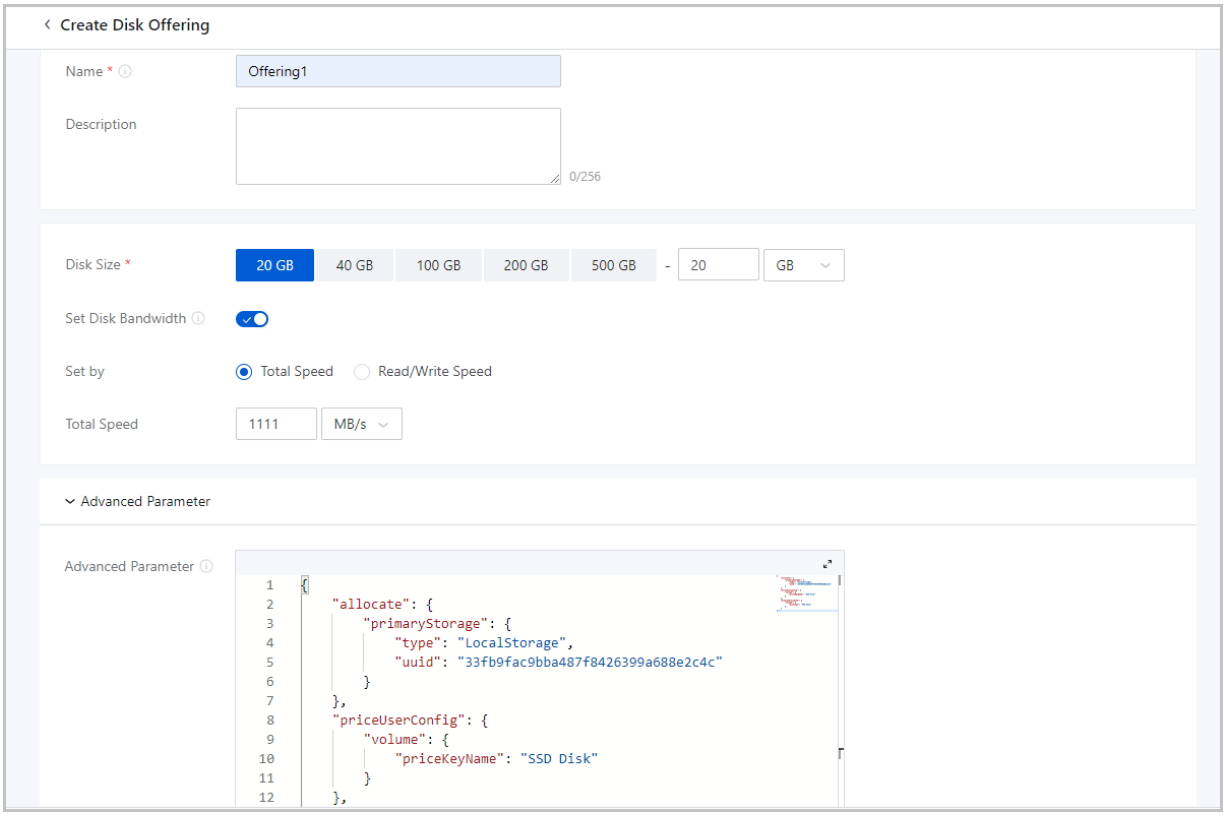
```
"displayAttribute": {
    "volume": {
      "diskType": "Set the attribute display name of data volumes
. You can view this parameter setting on the volume details page."
    }
  }
```

- `volume`: Set the attribute display name of data volumes. You can view this parameter setting on the volume details page. You can set multiple attributes in key-value pair format.

Note:

If you do not need special display, delete the preceding parameter settings.

Figure 7-29: Create Disk Offering



7.1.5.3 Manage a Disk Offering

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Compute Configuration** > **Disk Offering**. Then, the **Disk Offering** page appears.

The following table lists the actions that you can perform on a disk offering.

Action	Description
Create Disk Offering	Create a disk offering.
Edit Disk Offering	Modify the name and description of a disk offering.
Enable Disk Offering	Enable a disk offering.
Disable Disk Offering	Disable a disk offering. A disabled disk offering cannot be used to create a volume. However, the volumes created from the disk offering before the disablement are not affected.
Set Sharing Mode	Set the sharing mode of the resource. The platform provides the following sharing modes: • Share Globally: shares the resource with all projects and accounts. • Share to Specified Projects/Accounts: shares the resource with specified projects and accounts.

Action	Description
	• Not Share: revokes the resource from projects and accounts to which the resource is shared. If you set Sharing Mode to Not Share for the resource, other projects and accounts cannot use the resource. **Note:** • If you modify the Sharing Mode setting of the resource from Share Globally to Share to Specified Projects/Accounts, the resource is visible only to the specified projects or accounts to which the resource is shared. • If the resource that you share with projects or accounts was used by the projects or accounts and then you modify the Sharing Mode setting of the resource, the resource is reserved for the projects or accounts until it is released.
Delete Disk Offering	Delete a disk offering.

7.1.6 GPU Specification

7.1.6.1 What is GPU Specification?

A GPU specification defines the frame per second (FPS), video memory, resolution, and other configuration settings of a physical or virtual GPU. GPU specifications are categorized into physical GPU specifications and virtual GPU specifications.

- Physical GPU specification: defines the FPS, video memory, resolution, and other configuration settings of a physical GPU.
- vGPU specification: defines the FPS, video memory, resolution, and other configuration settings of a virtual GPU virtualized from a physical GPU.

7.1.7 Auto-Scaling Group

7.1.7.1 What is Auto-Scaling Group?

An auto-scaling group is a group of VM instances that are used for the same scenarios. An auto-scaling group can automatically scale out or in based on application workloads or health status of VM instances in the group.

7.1.7.2 Create an Auto-Scaling Group

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Resource Service** > **Auto-Scaling Group**. On the **Auto-Scaling Group** page, click **Create Auto-Scaling Group**. Then, the **Create Auto-Scaling Group** page is displayed.

To create an auto-scaling group, follow these steps:

1. Complete the basic configuration.

   To complete this step, set the following parameters:

   - **Zone**: By default, the current zone is displayed.
   - **Group Name**: Enter a name for the auto-scaling group.

     The name must be 1 to 128 characters in length and can contain Chinese characters, English letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
   - **Description**: Optional. Enter a description for the auto-scaling group.
   - **Initial VM Count**: Enter the initial number of VM instances in the group.
     - If you create an auto-scaling group for the first time, the number of VM instances in the group is equal to the initial VM count.
     - The initial VM count must be an integer ranging from 1 to 1000. Make sure that the initial VM count is between the minimum VM count and the maximum VM count. Make your configurations as needed.
   - **Minimum VM Count**: Enter the minimum number of VM instances in the auto-scaling group.
     - When a scale-in policy is configured, the number of VM instances in the auto-scaling group must not be smaller than that of the specified minimum VM count.
     - The minimum VM count must be an integer ranging from 1 to 1000. Make your configurat ions as needed.
   - **Maximum VM Count**: Enter the maximum number of VM instances in the auto-scaling group.
     - When a scale-out policy is configured, the number of VM instances in the group must not be greater than that of the specified maximum VM count.
     - The maximum VM count must be an integer ranging from 1 to 1000. Make your configurations as needed.

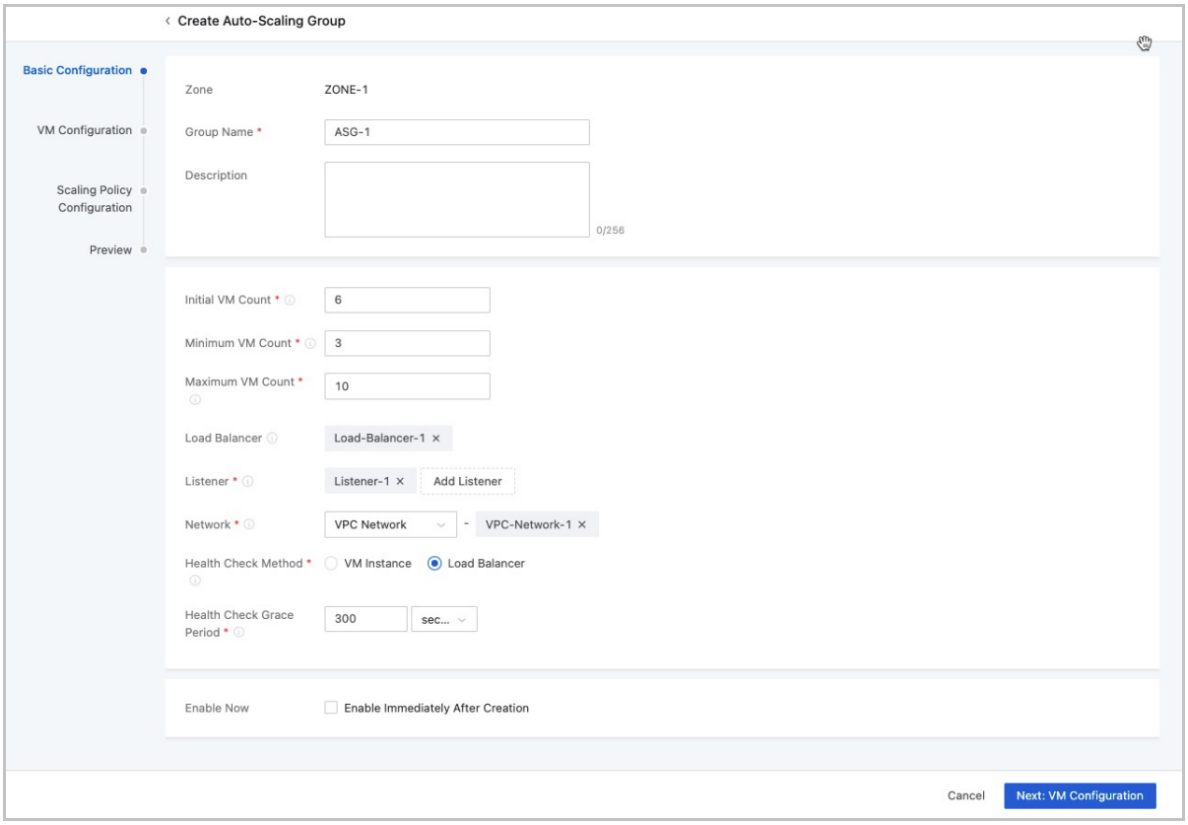
- If you choose to configure the load balancing service (recommended), set the following parameters:
  - **Load Balancer**: Select a load balancer.
    - Before you can select a load balancer, create it first and then associate one or more listeners with it.
  - **Listener**: Select a listener that is associated with the load balancer.
    - The listener list displays all listeners associated with the load balancer.
    - If you select multiple listeners, they listen on their respectively configured ports of VM instances in the auto-scaling group.
  - **Network**: Select an L3 network used for creating VM instances.
    - If you do not use the load balancing service, you can select a VPC network or flat network. Specifically, the VPC network must be attached to a VPC vRouter.
    - If you use the load balancing service, the network to be selected must be included in the backend network of the load balancer.
  - **Health Check Method**: Select a health check method. The load balancer-based health check method is recommended.
    - VM-based health check: This method checks the health status of VM instances in real time. If a VM instance is detected in stopped, unknown, or deleted state, the VM instance is considered to be unhealthy. Then, the VM instance is automatically removed from the auto-scaling group and a new one is created. This ensures the number of healthy VM instances in an auto-scaling group is not less than the specified minimum VM count.
    - Load balancer-based health check: This method is a built-in mechanism of load balancers.
  - **Health Check Grace Period**: Set the health check grace period after you select the load balancer-based health check method.
    - The health check grace period is a period of time after VM instances in the auto-scaling group are created and booted. During this period of time, application services related to these VM instances are probably still booting, and the auto-scaling group will not perform load balancer-based health checks. If this period of time is exceeded , the health status of the VM instances are monitored based on the health check mechanism of the load balancer.

- The grace period must be an integer greater than 10. Unit: second, minute, and hour.

- If you do not configure the load balancing service, set the following parameters:
  - **Load Balancer**: Leave this field blank.
  - **Network**: Select a private L3 network.

    Note:
    Currently, our auto-scaling service offers auto-scaling capabilities that let you automatically add or delete VM instances in the scenarios such as VPC networks and flat networks.
  - **Health Check Method**:
    - VM-based health check: This method checks the health status of VM instances in real time. If a VM instance is detected in stopped, unknown, or deleted state, the VM instance is considered to be unhealthy. Then, the VM instance is automatically removed from the auto-scaling group and a new one is created. This ensures the number of healthy VM instances in an auto-scaling group is not less than the specified minimum VM count.
- **Enable Immediately After Creation**: Choose whether to enable the auto-scaling group immediately after creation. By default, the group is not enabled immediately.

Figure 7-30: Basic Configuration



2. Complete the VM configuration.

   To complete this step, set the following parameters:

   - **VM Name**: Enter a name for the VM instance.
     - VM instances in an auto-scaling group are named in the format of **asg-Auto-Scaling Group Name-VM Name-First Five Digits of VM UUID**.
   - **Description**: Optional. Enter a description for the VM instance.
   - **Instance Offering** : Select an instance offering for the VM instance.
   - **Image**: Select an image for the VM instance.

   Note:

   - The image of a VM instance in an auto-scaling group can be in qcow2 or raw format.
   - If you want to use the internal monitoring metrics, select either an image with the agent installed, or install the agent manually by using the User Data script.

- If you modify the image after you create a VM instance, the new image will only be effective for the subsequently created VM instances, and the original image remains unchanged for the previously created VM instances.

- **L3 Network**: The L3 network you selected in the previous step is displayed.
- **Advanced**:
  - **Data Disk Offering**: Select a data disk offering. The data disk offering can be used to directly create data volumes and then attach them to the VM instance.
  - **Affinity Group**: Select an affinity group. Currently, only affinity groups with the anti-affinity group (soft) policy are supported.

    Note:

    - You can see only your own available resources from the tenant's perspective.
    - You can disassociate the affinity group from an auto-scaling group on the **Actions** column of the auto-scaling group.
  - **Security Group**: Select a security group. VM instances in the group share the same security group rules.
  - **Console Password**: Enter a password (VNC password) for the VM console. Password length: 6 to 18 characters.
  - **SSH Public Key**: Inject an SSH public key into the VM instance. By doing so, you can SSH in to the VM instance without a password.
    - Before you can inject an SSH public key into the VM instance, install cloud-init for the VM image first. Recommended cloud-init version: 0.7.9, 17.1, 19.4, 19.4, and later.
  - **User Data**: Import User Data. You can upload user-defined parameters or scripts to customize configurations for VM instances or to accomplish specific tasks.
    - Before you can import User Data to Linux-based VM instances, install cloud-init for the VM image first.

      The following is a sample script of importing User Data to a Linux-based VM instance.

```
#cloud-config
users:
 - name: test
   shell: /bin/bash
   groups: users
   sudo: ['ALL=(ALL) NOPASSWD:ALL']
   ssh-authorized-keys:
       - ssh-rsa AAAAB3NzaC1LXCJfjroD1lT root@10-0-0-18
bootcmd:
```

```
 - mkdir /tmp/temp
write_files:
 - path: /tmp/ZStack_config
   content: |
       Hello,world!
   permissions: '0755'
fqdn: Perf-test
disable_root: false
ssh_pwauth: yes
chpasswd:
  list: |
      root:word
  expire: False
runcmd:
 - echo ls -l / >/root/list.sh
```

The sample script above can achieve the following functionalities:

1. When you create a VM instance, create a user with the name test and inject an ssh -key into the VM instance.
2. Write the `/etc/hosts` file when the VM instance is started. Also, create the `/tmp/temp` directory, create a file under the directory, and write contents into the file.
3. Set a hostname, enable the user root, allow the root user SSH log in to the VM instance, and change the root password.
4. Run the `echo ls -l /` command.

- Before you can import User Data to Windows-based VM instances, install Cloudbase-Init for the VM image first. For more information about the installation method, see *Cloudbase-Init Documentation*.

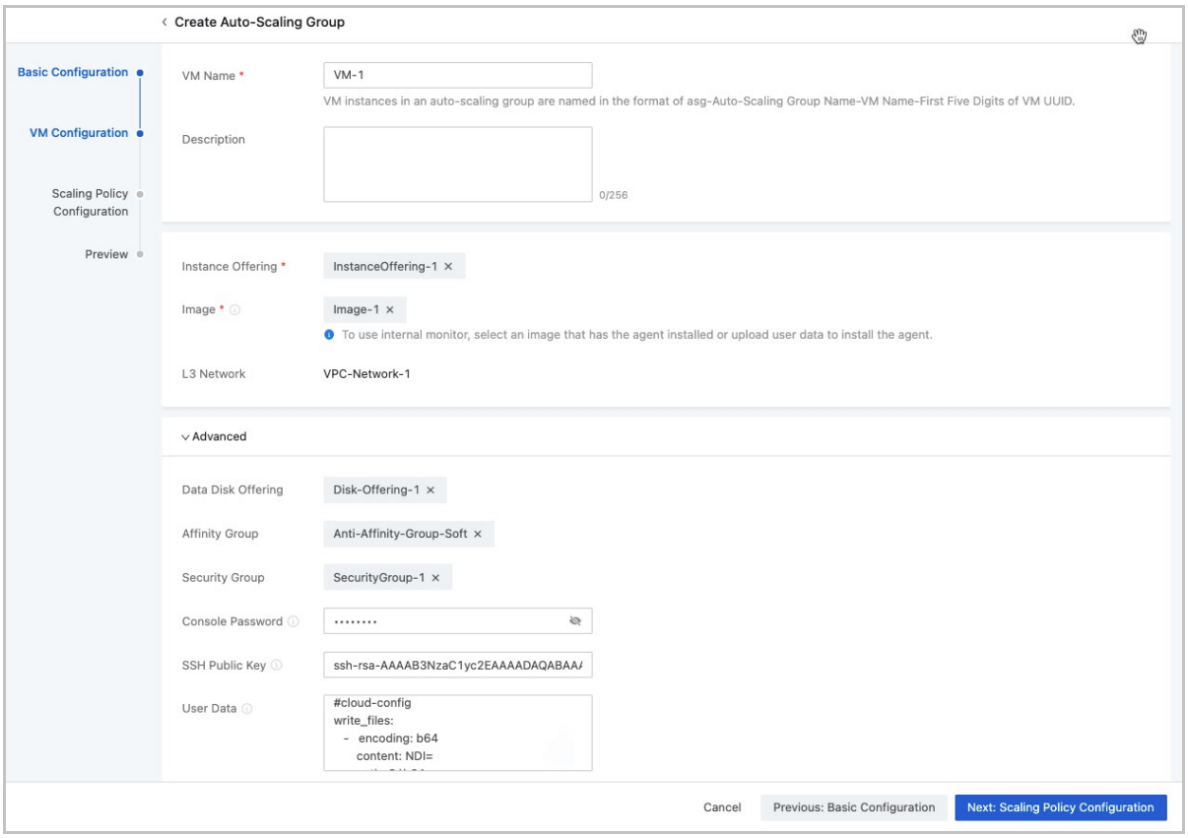
  The following is a sample script of importing User Data to a Windows-based VM instance.

```
#cloud-config
write_files:
   -   encoding: b64
       content: NDI=
       path: C:\b64
       permissions: '0644'
   -   encoding: base64
       content: NDI=
       path: C:\b64_1
       permissions: '0644'
   -   encoding: gzip
       content: !!binary |
           H4sIAGUfoFQC/zMxAgCIsCQyAgAAAA==
       path: C:\gzip
       permissions: '0644'
```

  The sample script above can achieve the following functionalities: When the VM instance is started, the **b64**, **b64_1**, and **gzip** files are created in the C drive.

> **Note:**
> When you use User Data, note that you can configure only one L3 network for an L2 network.

Figure 7-31: VM Configuration



> **Note:**
> Exercise caution. If you delete resources, such as instance offering, image, and network from the template configurations, you might fail to create the auto scaling group.

3. Complete the scaling policy configuration.

   The Cloud provides two types of scaling policy: resource-based policy and periodic policy.

   - **Resource-based Policy**: Configure the scale-out and scale-in policies based on the resource utilization. This policy type applies to unpredictable user business change scenarios to increase or decrease VM instances accordingly.

     — **Alarm Notification**: Choose whether to enable alarm notification. You can configure a monitoring and alarm mechanism to trigger auto scaling. By default, alarm notification is not enabled.

- If enabled, you must specify one or more endpoints.

  Endpoint: Specify one or more endpoints.

  - You can either select the system endpoint (default endpoint) or select a custom endpoint such as email, DingTalk, HTTP application, short message service, and Microsoft Teams.

— **Trigger Metric**: Select a trigger metric. Available trigger metrics are as follows:

- VM Memory Utilization Average: The sum of the memory utilization for a single VM instance in an auto-scaling group/The total number of VM instances in the auto-scaling group
- VM CPU Utilization Average: The sum of the CPU utilization for a single VM instance in an auto-scaling group/The total number of VM instances in the auto-scaling group
- VM Memory Utilization Average (Agent Required): The sum of the memory utilization for a single VM instance in an auto-scaling group/The total number of VM instances in the auto-scaling group
- VM CPU Utilization Average (Agent Required): The sum of the CPU utilization for a single VM instance in an auto scaling group/The total number of VM instances in the auto scaling group

Note:

- We recommend that you use an agent to monitor the average memory utilization of VM instances. By doing so, the monitoring data is more accurate.
- If you must select trigger metrics that require you to install an agent, make sure that you select an image with an installed agent when you create VM instances.
- You can install agents by using the User Data script for Linux-based VM instances. For more information, see the **User Data** part in this topic.
- If you did not install an agent for internal monitoring and still wanted to select trigger metrics that require you to install the agent, the auto scaling group would fail to take effect.

— Scale-out policy:

- **Trigger Rule**: Set a trigger condition and the threshold duration.

  — The utilization must be an integer ranging from 1 to 100. Unit: %.

  - The threshold duration must be an integer that is greater than 0. Unit: second, minute, and hour.
- **Cooldown Time**: Set the cooldown time.
  - Cooldown time refers to a period of time during which an auto-scaling group that is in the locked status rejects any new scaling activity after one scaling activity is launched successfully in the auto-scaling group.
  - The cooldown time must be an integer that is greater than 0. Unit: second and minute.
- **Addition Policy**: Enter the number of VM instances to be added each time when the auto-scaling group performs a scale-out activity.

  Note:
  A minimum number of 1 VM instance can be added each time during the scale-out activity. If the value is too large, the scale-out activity might fail.

- Scale-in policy:
  - When workloads decrease, auto-scaling groups automatically scale in to avoid resource waste.
  - Auto-scaling groups scale in based on the alarm rules that you set for the groups.

    For example, if the average memory utilization of all VM instances in an auto-scaling group keeps lower than 20% for a period of time, a reasonable number of VM instances are removed. This way, the workloads are well balanced at a reasonable level among the VM instances.

  To configure the scale-in policy, set the following parameters:

  - **Trigger Rule**: Set a trigger condition and the threshold duration.
    - The utilization must be an integer ranging from 1 to 100. Unit: %. Note that the trigger rule set for the scale-out policy cannot conflict with that for the scale-in policy.
    - The threshold duration must be an integer that is greater than 0. Unit: second, minute, and hour.
  - **Cooldown Time**: Set the cooldown time.

- Cooldown time refers to a period of time during which an auto scaling group that is in the locked status rejects any new scaling activity after one scaling activity is launched successfully in the auto scaling group.
- The cooldown time must be an integer that is greater than 0. Unit: second and minute.

- **Removal Policy**: Select a removal policy and enter the number of VM instances to be removed each time when the auto-scaling group performs a scale-in activity. Available removal policies are as follows:
  - Most Recent Created VM Instance (default): When the auto-scaling group starts performing scale-in activities, the latest created VM instances are removed successively at first.
  - Earliest Created VM Instance: When the auto-scaling group starts performing scale-in activities, the earliest created VM instances are removed successively at first.
  - VM with Minimum CPU Usage: When the auto-scaling group starts performing scale-in activities, VM instances with the minimum CPU usage are removed successively at first.
  - VM with Minimum Memory Usage: When the auto-scaling group starts performing scale-in activities, VM instances with the minimum memory usage are removed successively at first.

  Note:
  A minimum number of 1 VM instance can be removed each time during the scale-in activity. If the value is too large, the scale-in activity might fail.

- **Periodic Policy**: Perform scale-out or scale-in policies periodically. This policy type applies to predictable user business change scenarios to increase or decrease VM instances periodically.
  - Scale-out policy:
    - **Scale-out Period**: Select a scale-out period. Options: scale-out by month, scale-out by week, scale-out by day, scale-out by hour, and scale-out by minute.
    - **Execution Time**: Configure when the scale-out activity is to be performed.
    - **Cooldown Time**: Set the cooldown time.

- Cooldown time refers to a period of time during which an auto-scaling group that is in the locked status rejects any new scaling activity after one scaling activity is launched successfully in the auto-scaling group.
- The cooldown time must be an integer that is greater than 0. Unit: second and minute.

- **Schedule Effective Time**: Specify the time when the scale-out activity is to be performed. The auto-scaling group scales out according to the configured scale-out period.

> **Note:**
> You can set the schedule effective time when you choose to scale-out by month, scale-out by week, or scale-out by day.

- **Addition Policy**: Enter the number of VM instances to be added each time when the auto-scaling group performs a scale-out activity.

> **Note:**
> A minimum number of 1 VM instance can be added each time during the scale-out activity. If the value is too large, the scale-out activity might fail.

— Scale-in policy:

- **Scale-in Period**: Select a scale-in period. Options: scale-in by month, scale-in by week, scale-in by day, scale-in by hour, and scale-in by minute.
- **Execution Time**: Configure when the scale-in activity is to be performed.
- **Cooldown Time**: Set the cooldown time.
  - Cooldown time refers to a period of time during which an auto-scaling group that is in the locked status rejects any new scaling activity after one scaling activity is launched successfully in the auto-scaling group.
  - The cooldown time must be an integer that is greater than 0. Unit: second and minute.
- **Schedule Effective Time**: Specify the time when the scale-in activity is to be performed. The auto-scaling group scales in according to the configured scale-in period.

> **Note:**

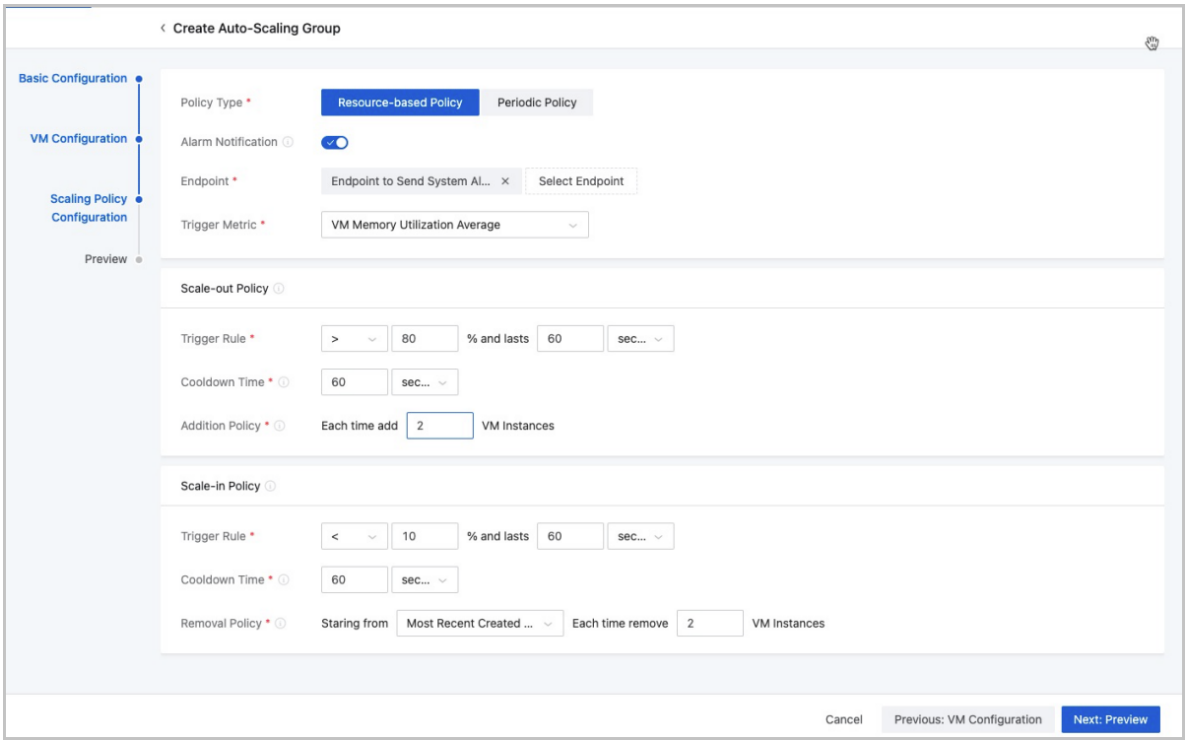
You can set the schedule effective time when you choose to scale-in by month, scale-in by week, or scale-in by day.

- **Removal Policy**: Select a removal policy and enter the number of VM instances to be removed each time when the auto-scaling group performs a scale-in activity. Available removal policies are as follows:
  - Most Recent Created VM Instance (default): When the auto-scaling group starts performing scale-in activities, the latest created VM instances are removed successively at first.
  - Earliest Created VM Instance: When the auto-scaling group starts performing scale-in activities, the earliest created VM instances are removed successively at first.
  - VM with Minimum CPU Usage: When the auto-scaling group starts performing scale-in activities, VM instances with the minimum CPU usage are removed successively at first.
  - VM with Minimum Memory Usage: When the auto-scaling group starts performing scale-in activities, VM instances with the minimum memory usage are removed successively at first.

Note:

A minimum number of 1 VM instance can be removed each time during the scale-in activity. If the value is too large, the scale-in activity might fail.

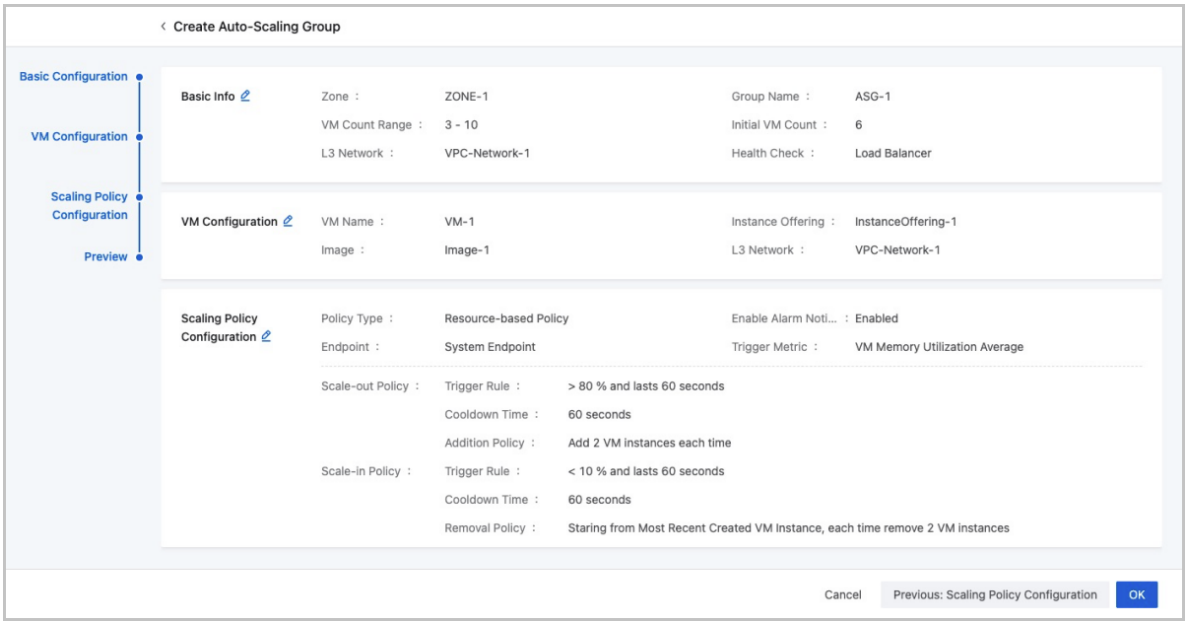
Figure 7-32: Scaling Policy Configuration



4. Preview the configurations.

   Preview the configured information about the auto-scaling group. You can modify the configurat ions by clicking the "Edit" icon.

Figure 7-33: Preview Configurations



7.1.8 Snapshot

7.1.8.1 What is Snapshot?

A snapshot is a point-in-time capture of data status in a volume. Before you perform a business-sensitive operation, you can schedule snapshot creation at specified time points to record the state of the system volume or data volume of a VM instance. This allows rollback in case of breakdowns. If you want to backup data for a long term, you can use Backup Service.

Snapshot Category

Snapshots can be classified into the following two categories:

- Manual snapshot: snapshots that are manually created for root volumes or data volumes.
- Auto snapshot: snapshots that are automatically created at a scheduled time interval or in specific scenarios.
  - To create auto snapshots for a resource at a scheduled time interval, you need to create a scheduled snapshotting policy for the resource. This way, the system creates snapshots at scheduled time points for the resource.
  - The system may create an auto snapshot in the following scenarios:
    - Root volume capacity expansion
    - Data volume capacity expansion
    - VM reset
    - Snapshot rollback

      Note:

      - By default, the system does not create a snapshot in case of snapshot rollback.
      - You can enable or disable one-time snapshot-creation in case of snapshot rollback on the Global Setting page.

        Choose **Setting** > **Platform Setting** > **Global Setting** > **Advanced** > **Resource Center** > **Resource Pool** > **Snapshot**. Turn on or off the **Auto Create Volume Snapshot** switch based on your business needs.
    - Image creation of root volume or data volume on Ceph primary storage

Snapshot View

ZStack Cloud provides the following two views of snapshots:

- List view: In this view, snapshots are displayed in a list, including the name, type, size, creation time, and supported operations.
- Topology view: In this view, snapshots are displayed in a hierarchical tree, including snapshot chain and snapshot node. You can locate the current snapshot, reset canvas, zoom in or out the canvas, and enter the full screen of the view.

Scenarios

Snapshots can be used for the following scenarios:

- Fast recovery from breakdowns: If the production environment breaks down, you can rollback snapshots to return to the normal state. Snapshot rollback is a temporary use for unexpected breakdowns. To backup data for a long term, we recommend that you use Backup Service.
- Data exploration: You can create snapshots for production data and use the snapshots to do data mining, query, and development and test.
- Fault tolerance improvement: Before you perform a business-sensitive operation such as upgrading your system or migrating data, we recommend that you create one or more snapshots. This allows fast recovery to the normal state in case of any errors or exceptions during the operation.

7.1.8.2 Snapshot Fundamentals

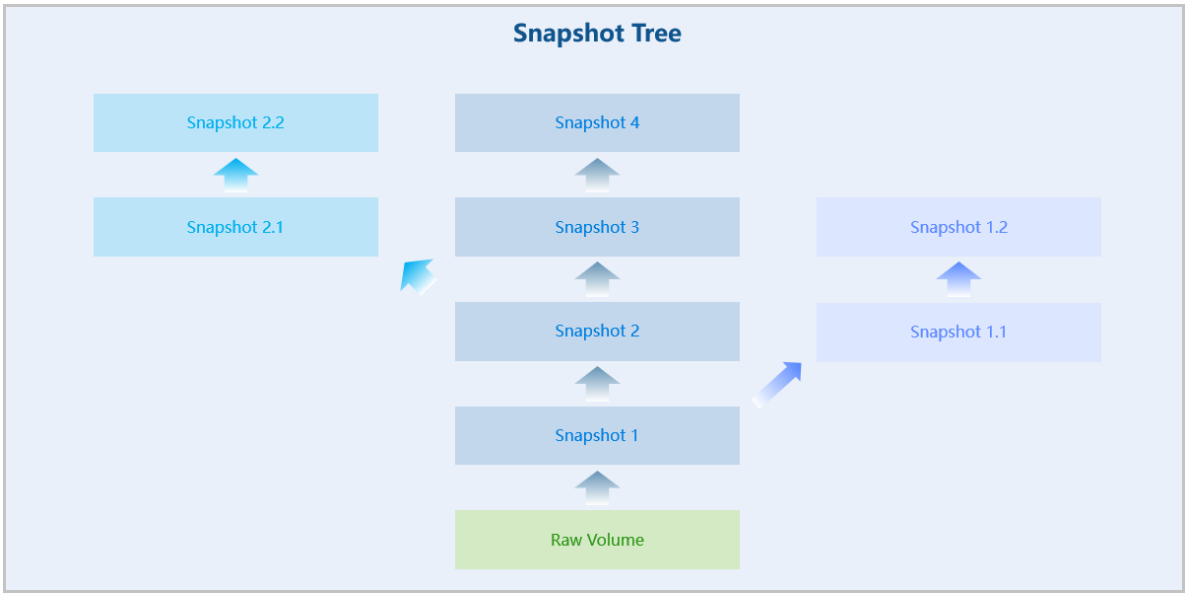
Non-Ceph Storage QCOW2 External Snapshot Mechanism

For non-Ceph storage including LocalStorage, NFS, Shared Mount Point, and Shared Block, ZStack Cloud uses QCOW2 (QEMU Copy On Write, Version 2) external snapshot mechanism.

1. **Snapshot Tree and Snapshot Chain**

   A volume corresponds to a snapshot chain. ZStack Cloud allows you to create a snapshot tree for a volume. Each branch of the snapshot tree is a snapshot chain.

Figure 7-34: Snapshot Tree



A snapshot tree includes the following information:

- Snapshot chain: a chain of snapshots of a volume that are associated with each other. Each branch of a snapshot tree is a snapshot chain.
- Snapshot node: a node in a snapshot chain that represents a snapshot of a volume.
- Snapshot size: the storage space that a snapshot occupies. You can view the total size of all snapshots in a snapshot tree and the size of an individual snapshot node.

Note:

- For non-Ceph storage, a snapshot node can have a maximum of 128 nodes by default. You can customize the maximum length of a snapshot chain Global Setting by setting **Maximum Incremental Volume Snapshot**. For Ceph storage, a snapshot node can have a maximum of 32 nodes, including the auto-created and manually-created nodes.
- If the length of a snapshot chain reaches the threshold:
  - If an auto-snapshot is created, the system automatically deletes the snapshot that was created at the earliest time.
  - If you manually create a snapshot, you need to manually delete the snapshot that you do not need.
- In the production environment, we recommend that you limit the number of snapshots created for a volume to 5. Too many snapshots will lower VM and volume performance,

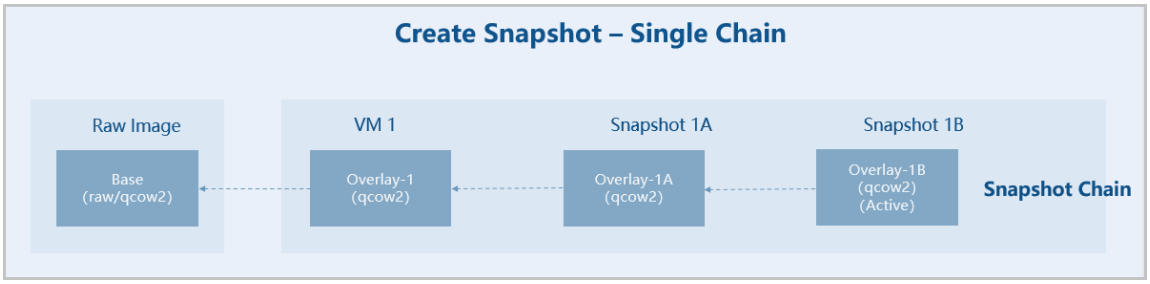
increase data security risks, and occupy storage space of primary storage. To back up data for the long term, you can use Backup Service.

2. **Create Snapshot**

When an external snapshot is created, an empty qcow2 file is created. The backing file of the empty file points to the previous qcow2 file. This qcow2 file is set to read-only and become a snapshot. Data is written to the empty qcow2 file.

- Create single-chain snapshots based on the backing file.

Figure 7-35: Create Single-Chain Snapshots

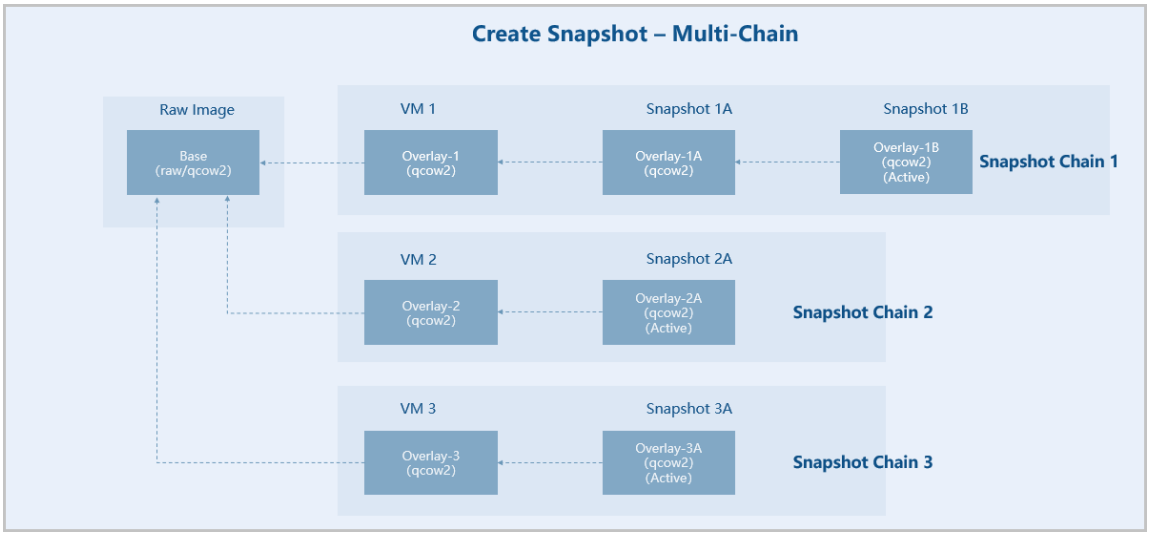


Suppose you have a raw image. You use the image to create a VM instance named VM 1 and then create snapshot 1A and 1B for VM 1.

- Raw image: a disk image file that includes a complete operating system and boot process. The image is a read-only file used as the base file.
- VM 1: creates an empty file named Overlay-1. The backing file of the empty file points to the base file. The base file is kept read-only and becomes a snapshot. Data is written to Overlay-1.
- Snapshot 1A: creates an empty file named Overlay-1A. The backing file of the empty file points to Overlay-1. Overlay-1 is set to read-only and becomes a snapshot. Data is written to Overlay-1A.
- Snapshot 1B: creates an empty file named Overlay-1B. The backing file of the empty file points to Overlay-1A. Overlay-1A is set to read-only and becomes a snapshot. Data is written to Overlay-1B. Overlay-1B is the last snapshot in the snapshot chain and is in Active state. VM 1 uses the disk file that corresponds to the snapshot Overlay-1B.

- Create a multi-chain snapshot chain based on the backing file.

Figure 7-36: Create Multi-Chain Snapshots



Suppose you have a raw image. You use the image to create VM instances named VM 1, VM 2, and VM 3 and then create snapshot 1A and 1B for VM 1, snapshot 2 for VM 2, and snapshot 3A for VM 3.

- Raw image: a disk image file that includes a complete operating system and boot process. The image is a read-only file used as the base file.
- Snapshot chain 1:
  - VM 1: creates an empty file named Overlay-1. The backing file of the empty file points to the base file. The base file is kept read-only and becomes a snapshot. Data is written to Overlay-1.
  - Snapshot 1A: creates an empty file named Overlay-1A. The backing file of the empty file points to Overlay-1. Overlay-1 is set to read-only and becomes a snapshot. Data is written to Overlay-1A.
  - Snapshot 1B: creates an empty file named Overlay-1B. The backing file of the empty file points to Overlay-1A. Overlay-1A is set to read-only and becomes a snapshot. Data is written to Overlay-1B. Overlay-1B is the last snapshot in the snapshot chain and is in Active state. VM 1 uses the disk file that corresponds to the snapshot Overlay-1B.
- Snapshot chain 2:

- VM 2: creates an empty file named Overlay-2. The backing file of the empty file points to the base file. The base file is kept read-only and becomes a snapshot. Data is written to Overlay-2.
- Snapshot 2A: creates an empty file named Overlay-2A. The backing file of the empty file points to Overlay-2. Overlay-2 is set to read-only and becomes a snapshot. Data is written to Overlay-2A. Overlay-2A is the last snapshot in the snapshot chain and is in Active state. VM 1 uses the disk file that corresponds to the snapshot Overlay-2A.

- Snapshot chain 3:
  - VM 2: creates an empty file named Overlay-3. The backing file of the empty file points to the base file. The base file is kept read-only and becomes a snapshot. Data is written to Overlay-3.
  - Snapshot 3A: creates an empty file named Overlay-3A. The backing file of the empty file points to Overlay-3. Overlay-3 is set to read-only and becomes a snapshot. Data is written to Overlay-3A. Overlay-3A is the last snapshot in the snapshot chain and is in Active state. VM 1 uses the disk file that corresponds to the snapshot Overlay-3A.

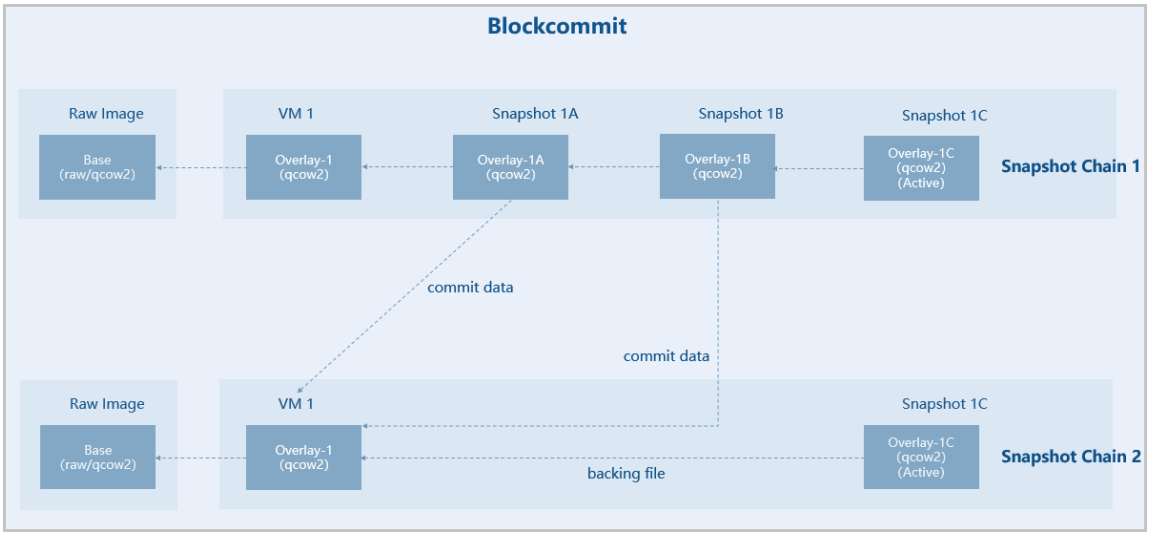
3. **Consolidate Snapshots**

External snapshots are interdependent with each overlay snapshot depending on its backing file. Each snapshot captures certain amounts of data. You cannot directly delete a snapshot to shorten a snapshot chain. To shorten a snapshot chain, you can blockcommit or blockpull external snapshots.

- Blockcommit

  Consolidate overlay snapshots of a snapshot chain into backing files.

Figure 7-37: Blockcommit

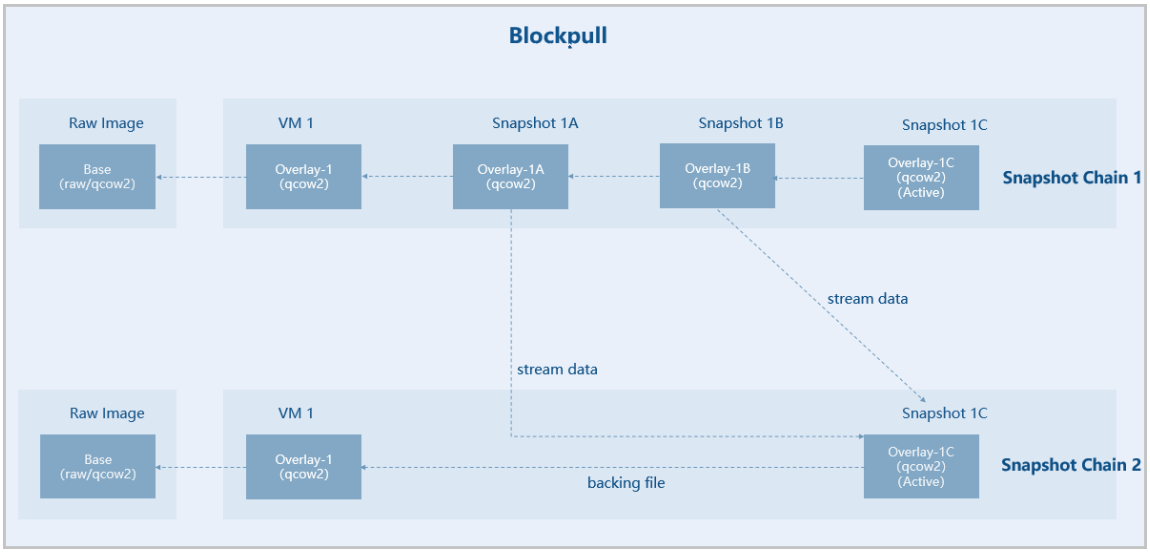


Suppose you have a raw image. You use the image to create VM instance named VM 1 then create three dependent snapshots named 1A, 1B, and 1C for VM 1. Then you blockcommit snapshot 1A and 1B to VM 1. This makes the backing file of snapshot 1C which is in Active state points to VM 1 and shortens the snapshot chain. Snapshot 1A and 1B are no longer useful and you can delete the two snapshots.

- Blockpull

  Consolidate backing files of a snapshot chain into overlay snapshots.

Figure 7-38: Blockpull



Suppose you have a raw image. You use the image to create VM instance named VM 1 then create three dependent snapshots named 1A, 1B, and 1C for VM 1. Then you blockpull snapshot 1A and 1B to snapshot 1C of VM 1. This makes the backing file of snapshot 1C which is in Active state points to VM 1 and shortens the snapshot chain. Snapshot 1A and 1B are no longer useful and you can delete the two snapshots.

Ceph Storage Snapshot Mechanism

For Ceph storage, ZStack Cloud uses the mainstream ROW (Redirect-On-Write) snapshot mechanism of Ceph.

7.1.8.3 Create a Snapshot

The following lists the two snapshot creation scenarios:

- Create VM snapshots:
  - Single volume snapshot: creates a snapshot for the root volume of a VM instance.
  - Snapshot group: creates snapshots for the root volume and data volumes of a VM instance.
- Create volume snapshots: creates snapshots for data volumes.

Create VM Snapshot

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Virtual Resource** > **VM Instance**. On the **VM Instance** page, select a running or stopped VM instance, and then choose **Actions** > **Snapshot and Backup** > **Create Snapshot**. Then, the **Create Snapshot for VM Instance** dialog box appears.

On the dialog box, set the following parameters:

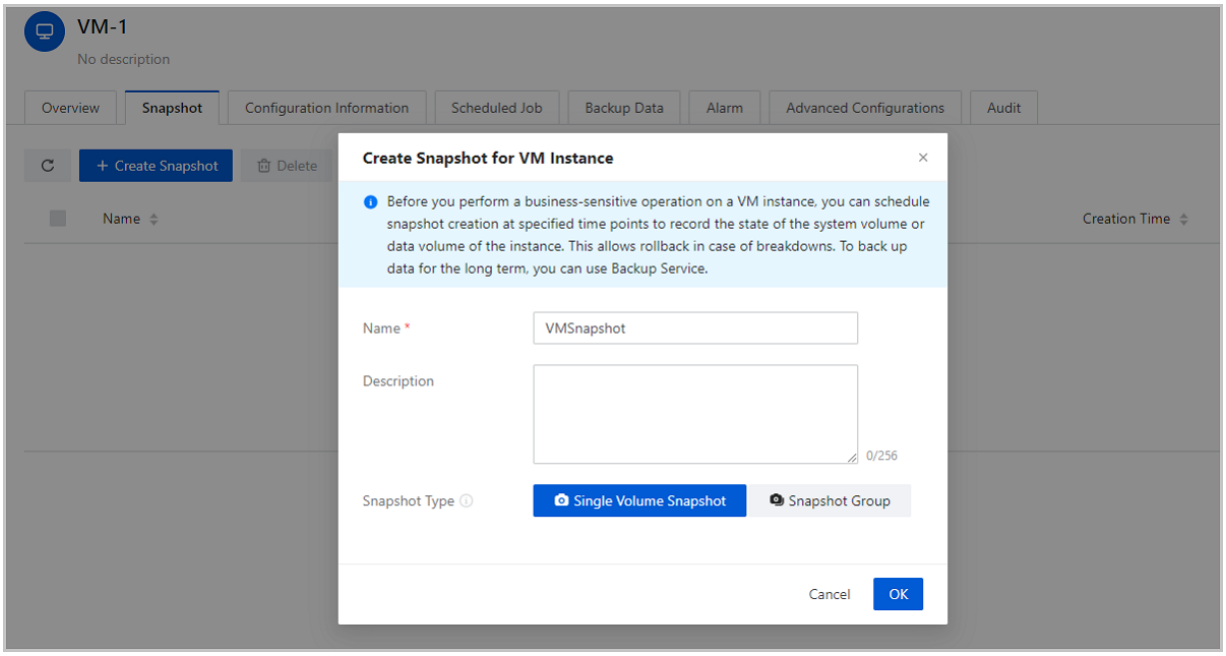
- **Name**: Enter a name for the volume.

  The name must be 1 to 128 characters in length and can contain Chinese characters, English letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the snapshot.
- **Snapshot Type**: Select either of the following type of snapshots that you want to create:
- — **Single Volume Snapshot**: creates a snapshot for the root volume of the VM instance.
  - **Snapshot Group**: creates a group of snapshots for the volumes of the VM instance, including the root volume and data volumes.

> **Note:**
> You cannot create snapshot groups for a VM instance to which shared volumes are attached.

You can also create snapshots for a VM instance on its details page. On the details page, click the **Snapshot** tab. On the tab, click **Create Snapshot**. Then, the **Create Snapshot for VM Instance** dialog box appears. On the dialog box, set the required parameters and create a snapshot for the VM instance.

Figure 7-39: Create VM Snapshot



Create Volume Snapshot

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Virtual Resource** > **Volume**. On the **Volume** page, select a volume, and then choose **Actions** > **Create Volume Snapshot**. Then, the **Create Volume Snapshot** dialog box appears.

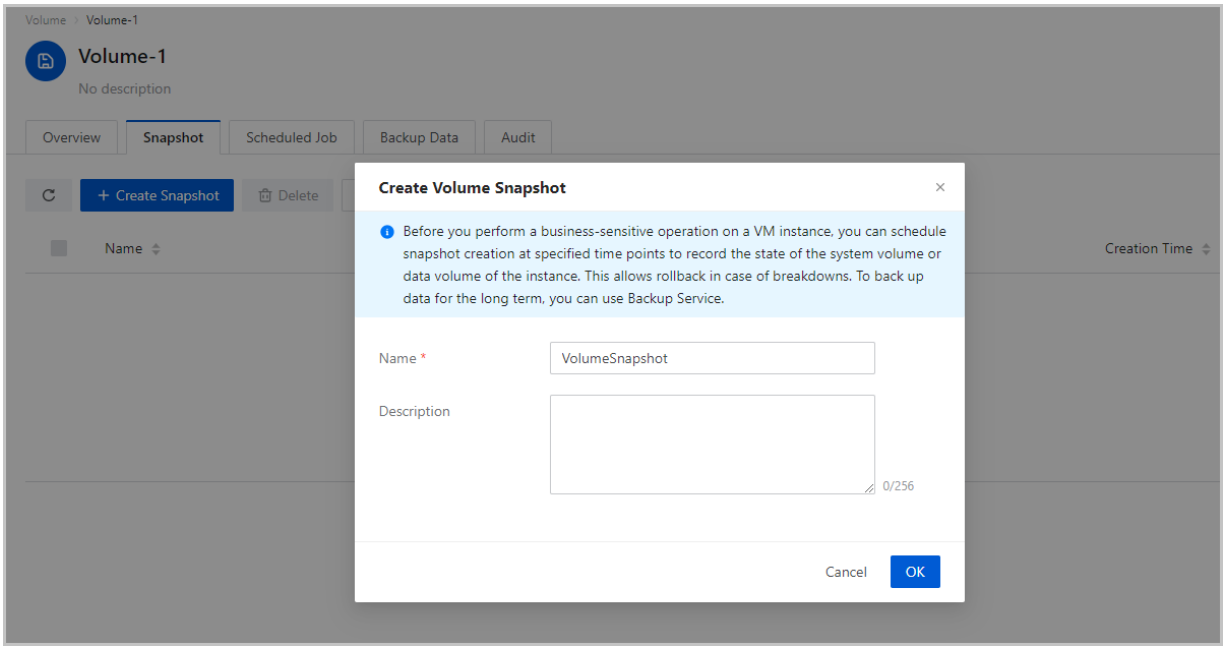
On the dialog box, set the following parameters:

- **Name**: Enter a name for the volume.

  The name must be 1 to 128 characters in length and can contain Chinese characters, English letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the snapshot.

You can also create snapshots for a volume on its details page. On the details page, click the **Snapshot** tab. On the tab, click **Create Snapshot**. Then, the **Create Volume Snapshot** dialog box appears. On the dialog box, set the required parameters and create a snapshot for the volume.

Figure 7-40: Create Volume Snapshot



Notes

- You can create a snapshot for a running or stopped VM instance.
- In the production environment, we recommend that you create a maximum of five snapshots for a volume. Excessive number of snapshots lowers I/O performance of volumes or VM instances, increases data security risks, and occupies storage space of primary storage. To back up data for the long term, you can use Backup Service.
- In the production environment, we do not recommend that you create snapshots for VM instances with high I/O operations. This is because if a VM instance has high I/O operations , some data may be still in the memory and is not stored on the volume when you create a snapshot for the VM instance. This part of data is not reserved in the snapshot, thus affecting data integrity.
- VM or volume snapshots do not occupy the storage space of Ceph primary storage. The displayed snapshot size indicates the actual size of the VM or volume at the creation time of the snapshot.
- More information about various editions of Ceph primary storage:

— The sizes of volume snapshots in Open-source Ceph Hammer series and Ceph Enterprise 3.2.0 or earlier are inaccessible.

— The sizes of volume snapshots in Ceph Enterprise 3.2.0 or later may be inaccessible due to the format of RBD images.

- You cannot create a snapshot for a shared volume that is created on a Shared Block or Ceph primary storage.

7.1.9 Affinity Group

7.1.9.1 What is Affinity Group?

An affinity group is an orchestration policy for IaaS resources to ensure the high performance and high availability of businesses...

Affinity Group Policy

ZStack Cloud provides two affinity group policies to better manage VM instances and hosts:

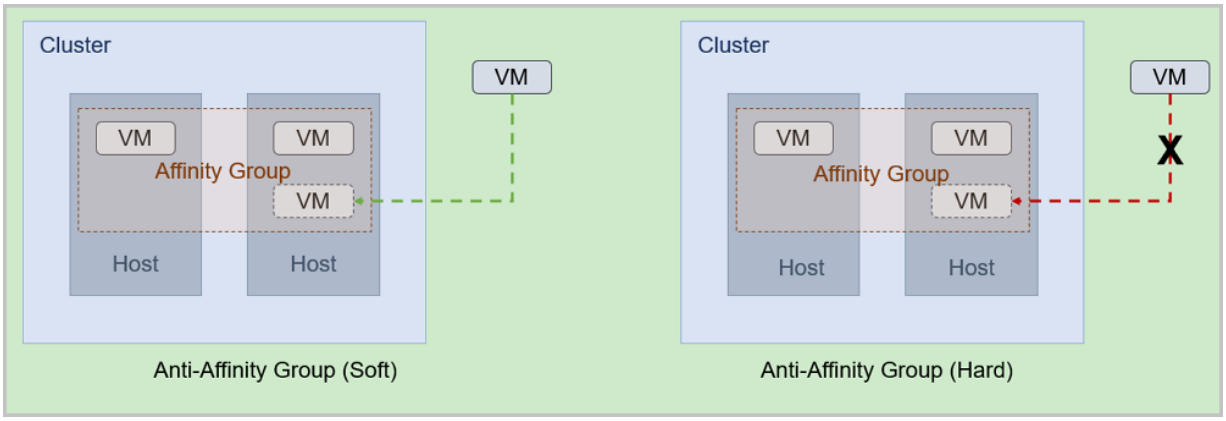
- Anti-affinity group (soft):

  Allocates VM instances in the affinity group to different hosts as much as possible. If no more hosts are available, the VM instances will be allocated randomly.

- Anti-affinity group (hard):

  Strictly allocates VM instances in the affinity group to different hosts. If no more hosts are available, the allocation fails.

Figure 7-41: Anti-Affinity Group (Soft) and Anti-Affinity Group (Hard)



Scenarios

This section provides some usage examples of anti-affinity group (soft) and anti-affinity group (hard) policies.

- Anti-affinity group (soft):

  You might want to deploy Hadoop nodes with different roles on different hosts to improve the overall system performance.

  - For example, when you deploy a Hadoop system, you might find it difficult to calculate the exact number of nodes of different roles such as NameNode, DataNode, JobTracker, and TaskTracker. However, deploying nodes on different hosts is more effective. With the anti -affinity group (soft) policy, you can deploy Hadoop clusters on different hosts as much as possible. This relieves the I/O pressure and improves the overall performance of the system .

- Anti-affinity group (hard):

  You might want to deploy two VM instances that run an active and a standby database on different hosts to ensure high availability.

  - For example, you deploy two VM instances to run an active and a standby MySQL database respectively, which cannot be down at the same time. In this case, you must deploy these two VM instances on different hosts. Due to deployment automation, you might not predict which hosts have sufficient resources. With the anti-affinity group (hard) policy, you can choose two different hosts to run these two VM instances respectively, which ensures the high availability.

7.1.9.2 Create an Affinity Group

On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Resource Service** > **Affinity Group**. On the **Affinity Group** page, click **Create Affinity Group**. Then, the **Create Affinity Group** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the affinity group.
- **Description**: Optional. Enter a description for the affinity group.
- **Policy**: Select an affinity group policy.

  ZStack Cloud provides two affinity group policies to better manage VM instances and hosts:

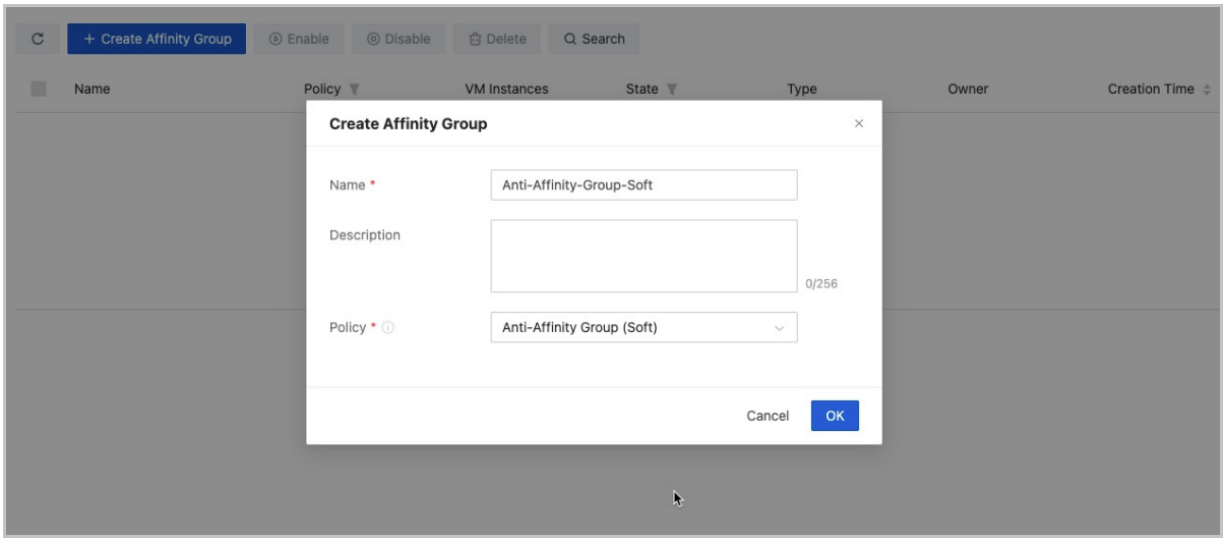
- Anti-affinity group (soft):

  Allocates VM instances in the affinity group to different hosts as much as possible. If no more hosts are available, the VM instances will be allocated randomly.

- Anti-affinity group (hard):

  Strictly allocates VM instances in the affinity group to different hosts. If no more hosts are available, the allocation fails.

Figure 7-42: Create Affinity Group



7.2 Hardware

7.2.1 Zone

7.2.1.1 What is Zone?

A zone is a logical group of resources such as clusters, L2 networks, and primary storages. Zone is the largest resource scope defined in the Cloud.

Basics

- In a data center, a zone corresponds to an equipment room.
- A zone defines a visible boundary. Sub-resources within the same zone can be visible mutually and can form a certain relationship. However, sub-resources within different zones are invisible mutually and cannot form mutual relationships.

Characteristics

- Zone isolation:

Isolates physical sub-resources such as primary storages and hosts in different zones, ensuring stability and fault tolerance to the maximum extent.

Reduces network delay and allows for faster access.

- Resource management:

  You can set a platform administrator for each zone. A platform administrator can manage one or more zones.

  The resources of each project can belong to only one area.

- Global view:

  After you plan a zone, you can view all the resources in the zone on a dedicated dashboard. You can view the resource usage by KVM or vCenter.

Considerations

When you plan a zone, note that:

1. Hosts in the same physical layer 2 broadcast domain must be in the same zone. These hosts can be grouped as one or more clusters.
2. A physical layer 2 broadcast domain cannot span multiple zones. Instead, it must be mapped as an L2 network in a single zone.
3. A primary storage cannot span multiple zones. Instead, it must be mapped as a primary storage in a single zone.
4. A data center can have multiple zones.
5. A zone can have one or more backup storages attached.
   - Resources in a zone, such as a primary storage, can only access the backup storages attached to the zone.
   - A backup storage can be deleted from a zone. After the backup storage is deleted, resources in the zone will not see the backup storage any more.
   - If a backup storage is no longer accessible to resources of a zone due to network typology changes in a data center, you can detach the backup storage from this zone.
   - To better manage the relationship between backup storages and zones, the UI specifies that a backup storage can only be attached to one zone at a time. That is, a backup storage that has been attached to a zone cannot be reattached to the other zone. When you add a backup storage in the UI, the backup storage will be automatically attached to the current

zone. When you delete a zone, you will directly delete the backup storage attached to the zone.

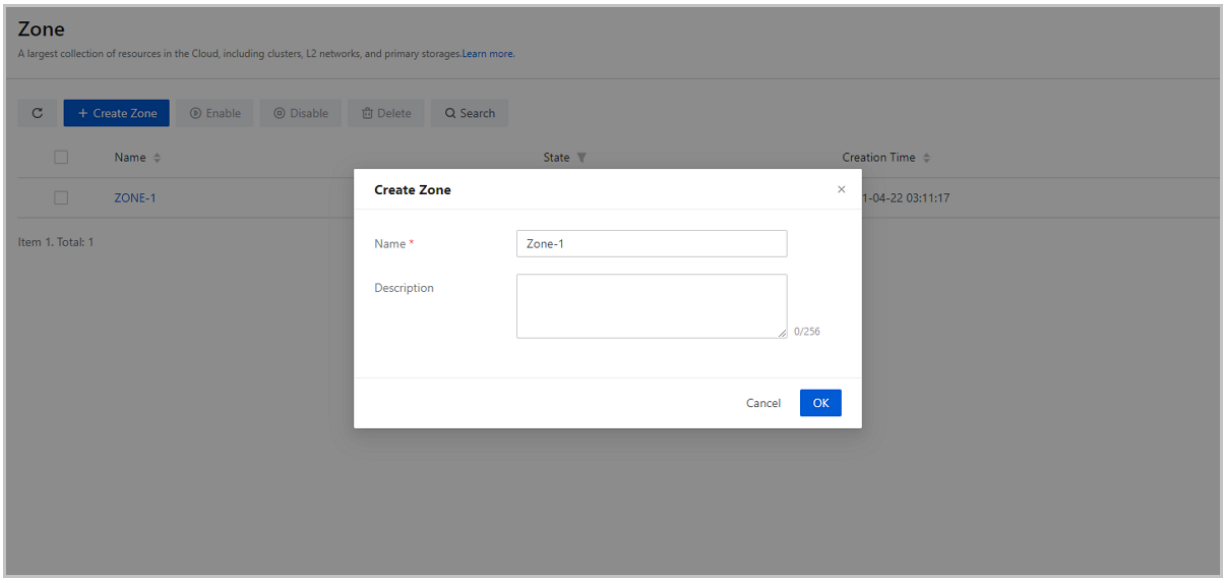
7.2.1.2 Create a Zone

On the main menu of ZStack Cloud, choose **Resource Center** > **Hardware** > **Computing Facility** > **Zone**. On the **Zone** page, click **Create Zone**. Then, the **Create Zone** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the zone.
- **Description**: Optional. Enter a description for the zone.

Figure 7-43: Create Zone



7.2.1.3 Manage a Zone

On the main menu of ZStack Cloud, choose **Resource Center** > **Hardware** > **Computing Facility** > **Zone**. Then, the **Zone** page is displayed.

The following table lists the actions that you can perform on a zone.

Action	Description
Create Zone	Create a zone.
Edit Zone	Edit the name and description of the zone.
Enable Zone	Enable the zone when it is disabled.
Disable Zone	Disable the zone when it is enabled.

Action	Description
	Note: • Disabling a zone also disables all the resources in the zone. Please exercise caution. • Disabling a zone also disables the clusters to which the L2 network in the zone is attached. In this case, the L2 and L3 networks in the zone are unavailable and cannot be used to create VM instances. However, existing businesses are not affected. • After a zone is disabled, you can manually enable some clusters in the zone, or create new clusters in the zone without enabling the zone again.
Delete Zone	Delete the zone. **Note:** Deleting a zone also deletes the clusters, hosts, networks, primary storages, and managed vCenters, and other resources in the zone. Please exercise caution.

7.2.2 Cluster

7.2.2.1 What is Cluster?

A cluster is a logical group of hosts (compute nodes). In a real data center, a cluster usually maps to a rack.

When you plan a cluster, note that:

- All hosts in the same cluster must be installed with the same operating system.
- All hosts in the same cluster must have the same network configuration.
- All hosts in the same cluster must be able to access the same primary storage.
- Before a cluster can provide VM services, the cluster must have a primary storage and an L2 network attached.
- The scale of a cluster, which is the maximum number of hosts that the cluster can contain, is not enforced.

The relationship between a typical cluster and its associated resources is as follows.

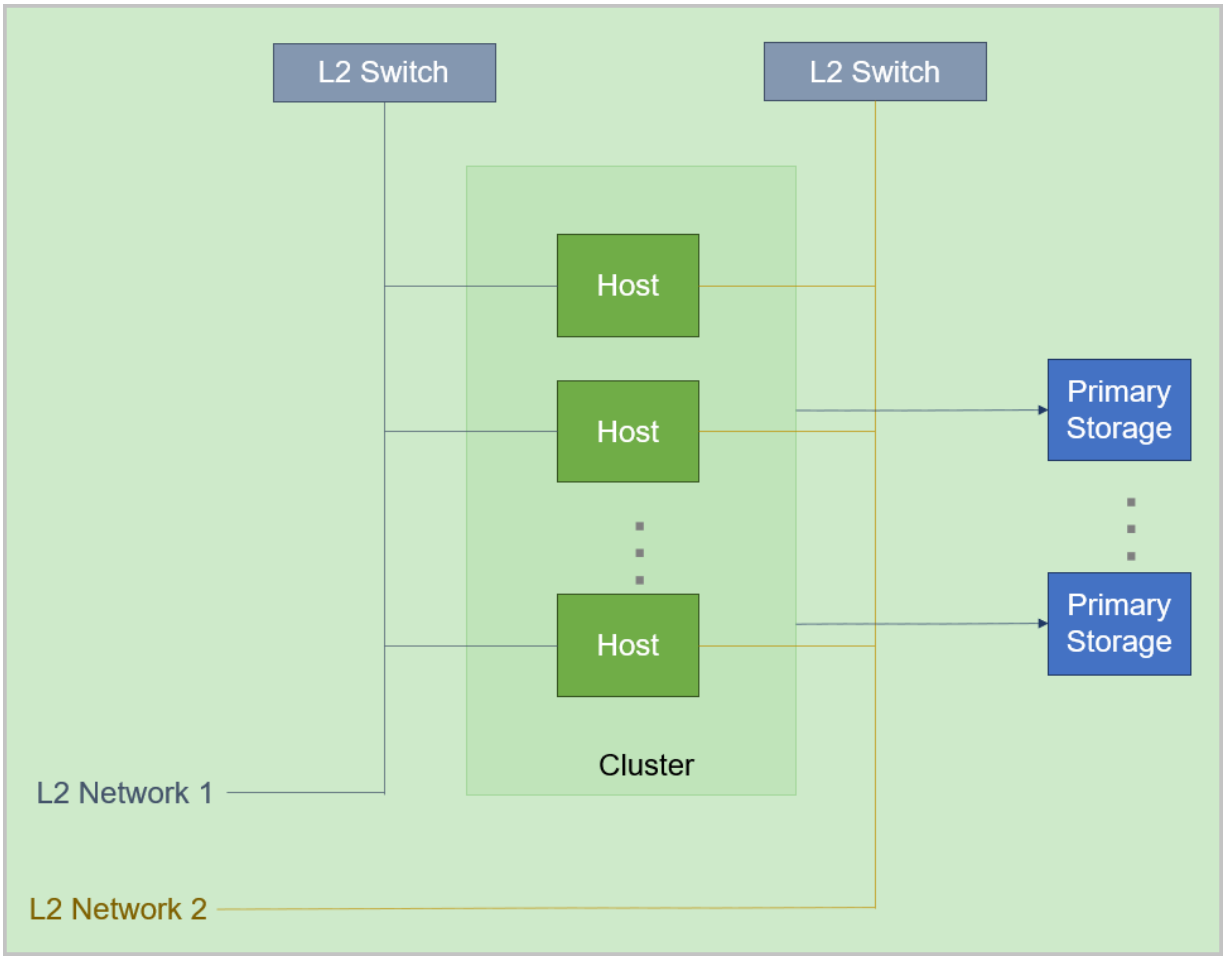
Cluster | Zone

You can create more than one cluster in a zone, and allocate newly created hosts to different clusters as needed.

Cluster | Primary Storage and L2 Network

You can attach primary storages and L2 networks to or detach them from a cluster. The following diagram shows the relationship between cluster and primary storage, L2 network.

Figure 7-44: Relationship Between Cluster and Primary Storage, L2 Network



Note:

When you attach a primary storage and an L2 network to a cluster, note that:

1. Cluster | Primary Storage
   - A primary storage can be attached to one or more clusters.
   - A cluster can have one or more primary storages attached.

The following are primary storages of the same type that a cluster can have:

- A cluster can have one or more LocalStorage primary storages attached.
- A cluster can have one or more NFS primary storages attached.
- A cluster can have one or more SharedBlock primary storages attached.
- A cluster can have one SharedMountPoint (SMP) primary storages attached.
- A cluster can have only one Ceph primary storage attached.
- A cluster can have only one AliyunNAS primary storage attached.
- A cluster can have only one AliyunEBS primary storage attached.

The following are combinations of primary storages that a cluster can have:

- A cluster can have both a LocalStorage and an NFS primary storage attached.
- A cluster can have both a LocalStorage and an SMP primary storage attached.
- A cluster can have both a LocalStorage and a SharedBlock primary storage attached.
- A cluster can have both a Ceph and a SharedBlock primary storage attached.
- A cluster can have both a Ceph and more than one SharedBlock primary storage attached.

The following table lists the relationship between primary storages and a cluster.

Table 7-3: Relationship Between Primary Storage and Cluster

Primary Storage	Cluster
LocalStorage	A cluster can have one or more LocalStorage primary storages attached.
NFS	A cluster can have one or more NFS primary storages attached.
SharedBlock	A cluster can have one or more SharedBlock primary storages attached.
SMP	A cluster can have one SMP primary storage attached.
Ceph	A cluster can have only one Ceph primary storage attached.
AliyunNAS	A cluster can have only one AliyunNAS primary storage attached.

Primary Storage	Cluster
AliyunEBS	A cluster can have only one AliyunEBS primary storage attached.
LocalStorage + NFS	A cluster can have one LocalStorage and one NFS primary storage attached.
LocalStorage + SMP	A cluster can have one LocalStorage and one SMP primary storage attached.
LocalStorage + SharedBlock	A cluster can have one LocalStorage and one SharedBlock primary storage attached.
Ceph + SharedBlock	• A cluster can have one Ceph and one SharedBlock primary storage attached. • A cluster can have one Ceph and multiple SharedBlock primary storages attached.

- When you attach multiple LocalStorage primary storages to a cluster, partition the corresponding URLs on the hosts before you add hosts and primary storages, and make sure that each LocalStorage is deployed on an exclusive logical volume or physical disk.
- A primary storage can be accessed by all hosts in the cluster to which the primary storage belongs.
- If a primary storage cannot be accessed by hosts in the cluster due to network typology changes in the data center, you can detach the primary storage from the cluster.

2. Cluster | L2 Network

- A cluster can have one or more L2 networks attached. Also, an L2 network can be attached to one or more clusters.
- A cluster can have a VXLAN pool attached. The VNIs in the VXLAN pool can be used to create different VXLAN networks.
- One NIC can be used to create only one NoVlan network.
- For VLAN networks, different VLAN IDs represent different L2 networks.
- If hosts in a cluster no longer exist in the layer 2 broadcast domain of an L2 network due to network typology changes in the data center, you can detach the L2 network from the cluster.

Cluster | Backup Storage

No direct dependency exists between a cluster and a backup storage. A backup storage can provide services for multiple clusters.

The following table lists the relationship between primary storages (PS) and backup storages (BS).

Table 7-4: Relationship Between PS and BS

PS/BS	ImageStore	SFTP	Ceph
LocalStorage	○	○	×
NFS	○	○	×
SMP	○	○	×
Ceph	○	×	○
SharedBlock	○	×	×

- When primary storages are LocalStorage, NFS, or SMP, the default type for backup storages is ImageStore.
- When primary storages are NFS or SMP, you can manually mount the corresponding shared directories to the local directories of the corresponding backup storages. In this regard, both primary storages and backup storages can use the network shared storage.
- When primary storages are Ceph, you can use the primary storages in the same Ceph cluster as backup storages. You can also use the ImageStore primary storages as backup storages.
- When primary storages are SharedBlock, the default type for backup storages is ImageStore.
- When primary storages are AliyunNAS, the default type for backup storages is ImageStore.
- When primary storages are AliyunEBS, the default type for backup storages is AliyunEBS.

7.2.2.2 Create a Cluster

On the main menu of ZStack Cloud, choose **Resource Center** > **Hardware** > **Computing Facility** > **Cluster**. On the **Cluster** page, click **Create Cluster**. Then, the **Create Cluster** page is displayed.

On the displayed page, set the following parameters:

- **Zone**: By default, the current zone is selected.
- **Name**: Enter a name for the cluster.

The cluster name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).

- **Description**: Optional. Enter a description for the cluster.
- **Virtualization Technology**: Select the hypervisor type of the cluster. You can select KVM or XDragon.
  - If you select KVM, make sure that the hosts to be added to the cluster apply the KVM virtualization technology.
  - If you select XDragon, make sure that the hosts to be added to the cluster apply the X-Dragon architecture.
- **CPU Architecture**: Select a CPU architecture for hosts to be added to the cluster. You can select x86_64, aarch64, and mips64el.

  Note:

  - If left blank, the system will specify the CPU architecture of the fist host you add to the cluster.
  - The CPU architecture cannot be changed after being set. Please select a proper one according to your cloud environment.
- **Network Acceleration Support**: Choose whether to enable network acceleration for a cluster. By default, network acceleration support is disabled.

  Note:

  - If you enable network acceleration support for a cluster, make sure that the L2 network associated with the cluster uses an OVS-DPDK vSwitch and the hosts in the cluster must be attached with smart NICs of the specified model. Otherwise, network acceleration does not work as expected.
  - Once you enable network acceleration support, the feature cannot be disabled.
  - You can enable network acceleration support only when you create a cluster.
  - The network acceleration support feature is supported by KVM clusters but not by XDragon clusters.
- **Network Configuration**: Configure a dedicated VDI network or migration network for the cluster.

— **VDI Network**: Optional. Enter the CIDR of the VDI network.

- If you deployed a dedicated network for VDI, add the network directly to the Cloud.
- Using a dedicated VDI network can avoid network congestions and improve transmission efficiencies.
- If not set, the VDI will use a management network by default.

— **Migration Network**: Optional. Enter the CIDR of the migration network.

- If you deployed a dedicated network for VM migration, add the network directly to the Cloud.
- Using a dedicated migration network can avoid network congestions and improve transmission efficiencies.
- If not set, VM migrations will use a management network by default.

- **Advanced**: Make advanced configurations if you selected the KVM type in the previous steps.

— **VM CPU Model**: Optional. Specify a CPU model for VM instances in the cluster.

Cluster CPU Architecture	VM CPU Model in Cluster	VM CPU Mode in Global Setting	Note
x86_64	By default, **none** is selected. • If you select **none**, the VM CPU model in the cluster is decided by the **CPU Mode** you specified in the global setting.	none (default)	If you select none, the CPU model of VM instances on the Cloud is inconsistent with the host CPU model.
		host-model	If you select host-model, the CPU model of the VM instance is the same as that of the host, such as Intel Haswell CPU. **Note:** If you select host-model, the CPU of the VM instance may not support the extended page table extension, huge page, and virtualization features.
		host-passthrough	If you select host-passthrough, the CPU features of VM instances on the Cloud are the same as the CPU features of the host, such as

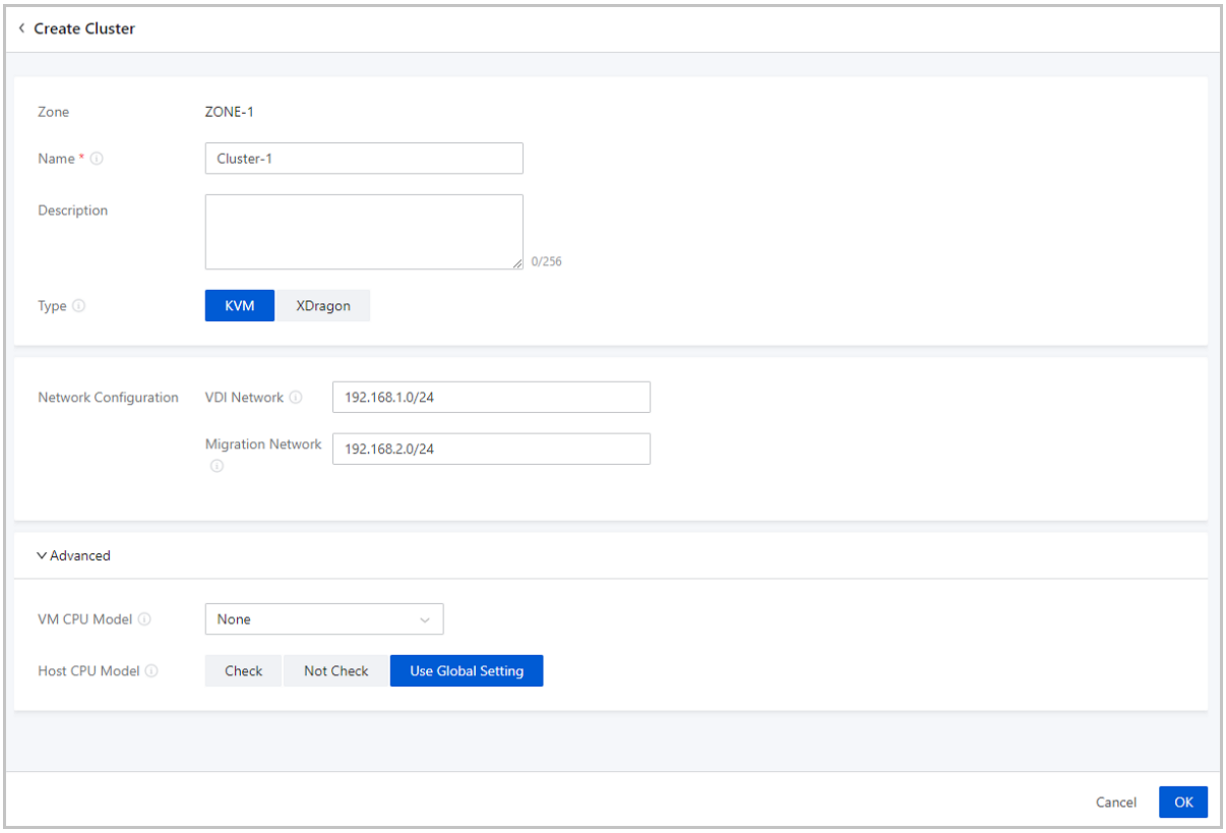
Cluster CPU Architecture	VM CPU Model in Cluster	VM CPU Mode in Global Setting	Note
			the page table extension, huge page, and virtualization features. **Note:** • If you select host-passthroug h, VM instances allow for virtualization. • However, if you migrate a VM instance to a host whose CPU model is different from the current host, the migration may fail. • In addition, the CPU utilizatio n of a VM instance measured within the instance may differ from the CPU utilization measured from the host.
	host-model	N/A	If you select host-model, the CPU model of the VM instances in the cluster is the same as that of the host.
	host-passthroug h	N/A	If you select host-passthrough, the CPU model and features of the VM instance in the cluster are the same as the CPU model and features of the hosts in the cluster.
	A custom CPU model	N/A	If you specify a custom CPU model , the VM instances in the cluster share the specified CPU model.
aarch64	host-passthroug h	N/A	The CPU model and features of the VM instance in the cluster are the same as the CPU model and features of the hosts in the cluster.
mips64el	A custom CPU model	N/A	If you specify a custom CPU model , VM instances in the cluster share the specified CPU model.

— **Host CPU Model**: Select a checking mechanism for the host CPU model in the current cluster.

Host CPU Model Checking Mechanism in Cluster	Host CPU Model Check Global Setting	Note 1	Note 2
By default, **Use Global Setting** is selected. • The host CPU model is decided based on the **Host CPU Model Check** you specified in the global setting.	false (default)	If you turn off **Host CPU Model Check**, when you hot migrate a VM instance or add a host, the Cloud does not check the consistency of the CPU models between the source host and the destination host.	The CPU model consistency of hosts in a cluster ensures that VM migration across hosts can succeed.
	true	If you turn on **Host CPU Model Check**, when you hot migrate a VM instance or add a host, the Cloud checks whether the CPU models of the source and destination hosts are consistent. **Note:** If not, the Cloud does not allow you to hot migrate the VM instance or add the host.	
Check	N/A	If you select **Check**, when you hot migrate a VM instance or add a host, the Cloud checks whether the CPU models of the source and destination hosts are consistent. **Note:** If not, the Cloud does not allow you to hot migrate the VM instance or add the host.	
Not Check	N/A	If you select **Not Check**, when you hot migrate a VM instance or add a host, the Cloud does not check the consistency of the CPU	

Host CPU Model Checking Mechanism in Cluster	Host CPU Model Check Global Setting	Note 1	Note 2
		models between the source and destination hosts.	

Figure 7-45: Create Cluster



7.2.2.3 Manage a Cluster

On the main menu of ZStack Cloud, choose **Resource Center** > **Hardware** > **Computing Facility** > **Cluster**. Then, the **Cluster** page is displayed.

The following table lists the actions that you can perform on a cluster.

Action	Description
Create Cluster	Create a cluster in the current zone.
Edit Cluster	Edit the name and description of the cluster.

Action	Description
Enable Cluster	Enable the cluster when it is disabled.
Disable Cluster	Disable the cluster when it is enabled. **Note:** • Disabling a cluster also disables all the hosts in the cluster. • After a cluster is disabled, you can manually re-enable some hosts in the cluster, or add new hosts to the cluster without enabling the cluster again.
Attach L2 Network	Attach an L2 network to the cluster.
Detach L2 Network	Detach an L2 network from the cluster. **Note:** Detaching an L2 network also detaches the corresponding VM NIC. Please exercise caution.
Attach Primary Storage	Attach a primary storage to the cluster.
Detach Primary Storage	Detach a primary storage from the cluster. **Note:** When you detach a primary storage from a cluster, note the following: • This operation might shut down VM instances on the primary storage and associated with the selected cluster, thus affecting the service running. Please exercise caution. • This operation might delete VPC vRouters on the primary storage and associated with the selected cluster, thus affecting the corresponding network service. Please exercise caution. • This operation might cause the volumes on the primary storage and associated with the selected cluster to fail to work properly. Please exercise caution.
Delete Cluster	Delete the cluster. **Note:** • Deleting a cluster also deletes all the hosts in the cluster. • If the cluster has a LocalStorage primary storage attached, you will also delete the VM instances, volumes, and snapshots on the hosts of the cluster. Please exercise caution.

7.2.3 Host

7.2.3.1 What is Host?

A host provides compute, network, and storage resources for VM instances. Hosts are core resources on the Cloud. VM instances are running on hosts.

7.2.3.2 Add a Host

On the main menu of ZStack Cloud, choose **Resource Center** > **Hardware** > **Computing Facility** > **Host**. On the **Host** page, click **Add Host**. Then, the **Add Host** page is displayed.

ZStack Cloud allows you to add a host by one of the following methods:

- Manual addition
- Import template

Manual Addition

With this method, you can specify an IP address or an IP range to add hosts. You can add up to 500 hosts at a time. To use this method, set the following parameters:

- **Name**: Enter a name for the host. The name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the host.
- **Virtualization Technology**: Select the hypervisor type of the server. You can select KVM or XDragon.
  - If the server applies the KVM virtualization technology, select KVM.
  - If the server applies the X-Dragon architecture, select XDragon.
- **Tag**: Optional. Attach one or more tags to the host.
- **Cluster**: Select the cluster where the host is located.

Note:

- Hosts that apply the KVM virtualization technology can be added only to KVM-based clusters.
- You can enable network acceleration for a KVM-based cluster. If you add a host to a cluster for which network acceleration is enabled, note that:

— If the L2 network associated with the cluster uses an OVS-DPDK vSwitch, the host must be attached with a smart NIC of the specified model and be in maintenance mode.

- Hosts of the X-Dragon architecture can be added only to X-Dragon-based clusters.
- XDragon-based clusters do not support network acceleration.

- **Host Info**: Configure the host information such as the host IP and SSH port according to your actual needs. You can configure the host information by entering an IP address or an IP range.

  — If you select the **IP Address** method, set the following parameters:

  - **IP Address**: Enter the IP address of the host.
  - **SSH Port**: Enter the SSH port of the host. Default: 22.
  - **User Name**: Enter the user name of the host. Default: root. You can enter a user name according to your actual needs.
  - **Password**: Enter a password for the user name.

  — If you select the **IP Range** method, set the following parameters:

  - **Start IP**: Enter the start IP address for the IP range.
  - **End IP**: Enter the end IP address for the IP range.
  - **SSH Port**: Enter the SSH port for the host. Default: 22.

    Note:
    Make sure that all hosts in the specified IP range share the same SSH port.

  - **User Name**: Enter the user name of the host. Default: root. You can enter a user name according to your actual needs.

    Note:
    Make sure that all hosts in the specified IP range share the same user name.

  - **Password**: Enter a password for the user name.

    Note:
    Make sure that all user name in the specified IP range share the same password.

  — **Scan Host IOMMU Setting**: Optional. Choose whether to scan the IOMMU setting of the host. The IOMMU setting is used in scenarios such as peripheral device passthrough and virtualization. By default, the host IOMMU setting is not scanned.

Note:

If you choose to scan the host IOMMU setting, note the following:

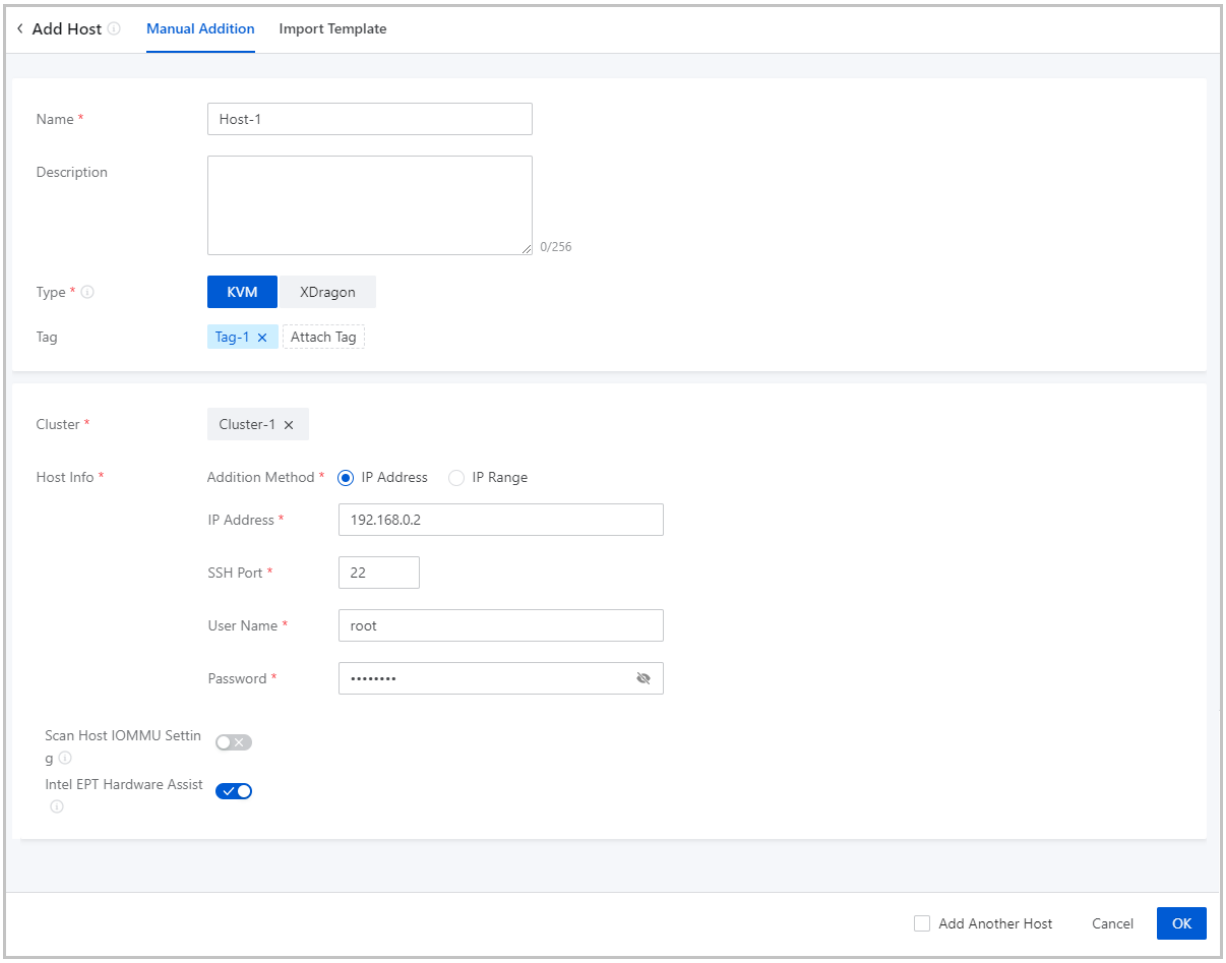
- Scanning the host IOMMU setting will traverse available GPU devices on the host and physical NICs that can be virtualized. Before you scan the setting, make sure that Intel VT-d or AMD IOMMU is enabled in the host BIOS.
- Before you can use GPU passthrough, vGPU virtualization, and SR-IOV, scan the host IOMMU setting.
- If you are scanning the host IOMMU setting for the first time, restart the host to make the setting take effect.

— **Intel EPT Hardware Assist**: Optional. Choose whether to enable Intel EPT hardware assist for Intel CPUs to improve the CPU performance. By default, Intel EPT hardware assist is enabled.

Note:

If the CPU model of your Intel server is too old, you might fail to create VM instances or cannot open the console properly of the newly created VM instances. In this case, disable the Intel EPT hardware assist.

Figure 7-46: Manual Addition



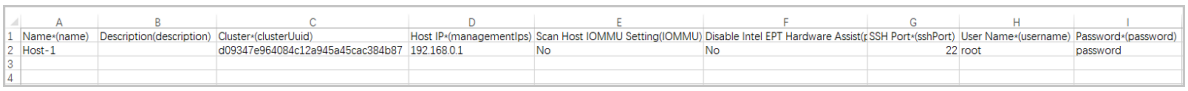
Import Template

With this method, download the CSV template file provided by the Cloud, fill in the host information according to the specified format, and upload the file. You can add hosts in bulk with this method. The procedure is detailed as follows.

1. Download the configuration template.

   Click **Download Template** to download the configuration template file in CSV format.

   Figure 7-47: Configuration Template File



	A	B	C	D	E	F	G	H	I
1	Name*(name)	Description(description)	Cluster*(clusterUuid)	Host IP*(managementIps)	Scan Host IOMMU Setting(IOMMU)	Disable Intel EPT Hardware Assist(g	SSH Port*(sshPort)	User Name*(username)	Password*(password)
2	Host-1		d09347e964084c12a945a45cac384b87	192.168.0.1	No	No	22	root	password
3									
4									

2. Fill in the host information according to the specified format.

   The configuration template contains a header a row of sample. You can delete or overwrite the sample as needed.

Set the following parameters in the template:

- **Name**: Enter a name for the host. If null, the Cloud allocates a name (HOST-host IP address) to the host by default.
- **Description**: Optional. Enter a description for the host.
- **Cluster**: Enter the UUID of the cluster where the host is located.

  Note:
  You can add only KVM-based hosts in the template.

- **Host IP**: Enter an IP address or an IP range for the host.

  If you enter multiple IP ranges for the host, use commas (,) to separate the ranges. **^** means that the IP range is not included. For example,

  ```
  192.168.0.1-192.168.0.100,^192.168.0.3-192.168.0.5
  ```

- **Scan Host IOMMU Setting**: Optional. Choose whether to scan the IOMMU setting of the host. The IOMMU setting is used in scenarios such as peripheral device passthrough and virtualization. By default, the host IOMMU setting is not scanned.

  Note:
  If you choose to scan the host IOMMU setting, note the following:

  - To enable this feature, enter YES, Yes, yes, Y, or y. To disable this feature, enter NO, No, no, N, or n. If null, this feature is disabled.
  - Before you can use GPU passthrough, vGPU virtualization, and SR-IOV, scan the host IOMMU setting.
  - Scanning the host IOMMU setting will traverse available GPU devices on the host and physical NICs that can be virtualized. Before you scan the setting, make sure that Intel VT-d or AMD IOMMU is enabled in the host BIOS.
  - If you are scanning the host IOMMU setting for the first time, restart the host to make the setting take effect.

- **Intel EPT Hardware Assist**: Optional. Specify whether to enable Intel EPT hardware assist for Intel CPUs to improve the CPU performance.

  Note:
  When you set this parameter, note the following:

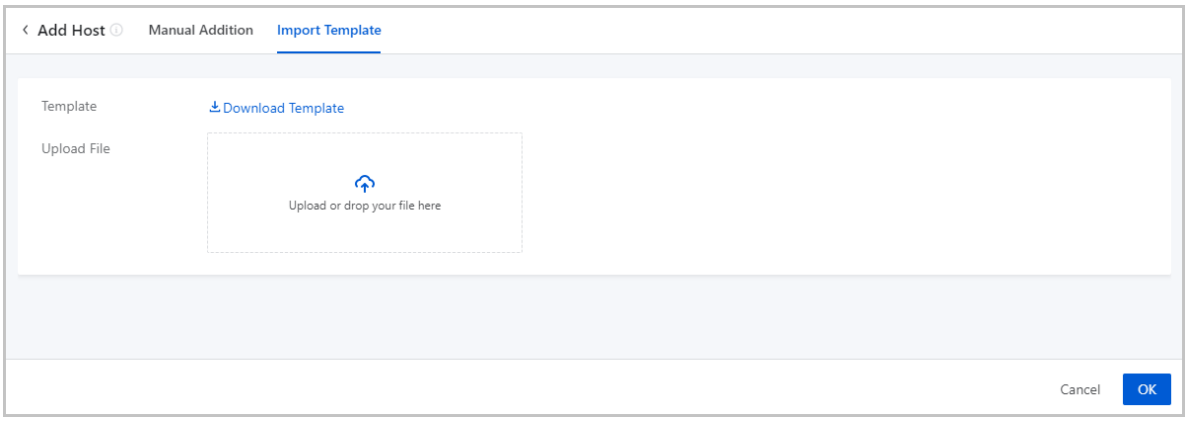
- If you enter NO, No, no, N, or n, the Intel EPT hardware assist will be enabled. If you enter YES, Yes, yes, Y, or y, the Intel EPT hardware assist will be disabled.
- If the CPU model of your Intel server is too old, you might fail to create VM instances or cannot open the console properly of the newly created VM instances. In this case, disable the Intel EPT hardware assist.

- **SSH Port**: Enter the SSH port for the host. If null, the Cloud will use port 22.
- **User Name**: Enter the user name of the host.
- **Password**: Enter a password for the user name.

3. Upload the configuration file.

   After you fill in the host information, verify that the grammar is correct, and then upload the file to the Cloud.

   Figure 7-48: Import Template



4. Add hosts by using the template.

   Click **OK**. Then, the Cloud add hosts according to the configuration file.

7.2.3.3 Manage a Host

On the main menu of ZStack Cloud, choose **Resource Center** > **Hardware** > **Computing Facility** > **Host**. Then, the **Host** page appears.

The following table lists the actions that you can perform on a host.

Action	Description	Preconditioned Host Status
Add Host	Add one or more hosts.	/
Edit Host	Edit the name and description of a host.	/

Action	Description	Preconditioned Host Status
Enable Host	Enable a host.	Disabled
Disable Host	Disable a host. **Note:** Disabling a host does not affect the resources already running on the host. However, the host is no longer available as a candidate when you apply for new resources.	Enabled
Reconnect Host	Reconnect a host. **Note:** In most cases, host reconnection can be implemented when the host configurations are updated. For example, if the memory or volume capacity of a hots is updated, you can reconnect the host to update the database.	ALL
Enter Maintenance Mode	Enter the maintenance mode. If a host is in maintenance mode, you can power off the host or troubleshoot failures. • If the primary storage is of the LocalStorage type, VM instances on a host are stopped when the host enters maintenance mode. • If the primary storage is of a shared storage type, VM instances on a host are automatically migrated when the host enters maintenance mode. **Note:** If the primary storage is of a shared storage type, you can configure the policy on failures of VM migration triggered when the host enters maintenance mode. On the main menu of ZStack Cloud, choose **Settings** > **Platform Setting** > **Global Setting** > **Advanced** > **Host**, and configure the **Policy for VM Migration Failure in Entering Host Maintenance Mode** setting: • **StopVmOnMigrationFailure**: When the host enters maintenance mode, VM instances are automatically	Connected

Action	Description	Preconditioned Host Status
	migrated to another host. If a VM instance fails to be migrated, the VM instance is forcibly stopped. • **JustMigrate**: When the host enters maintenance mode, VM instances are automatically migrated to another host. If a VM instance still runs on the host, the host fails to enter the maintenance mode.	
Attach Tag	Attach a tag to one or more hosts. **Note:** • You can attach a maximum of 50 tags to a resource . The number of resources to which a tag can be attached is not limited. • You can attach one or more tags to one or more resources. • A tag created by a tenant can be attached only to the resources owned by the tenant. The admin can attach a tag to all resources. • The admin can detach or delete tags created by a tenant. • You can sort tags attached to resources by attachment time or tag name. Tag names are sorted based on symbols, digits, Chinese letters, and English letters in descending order. To configure the sorting method, go to the main menu of ZStack Cloud, choose **Settings** > **Platform Setting** > **Global Setting** > **Basic**, and then configure the **Tag Sort Method** setting. By default, resources are sorted by tag name.	ALL
Detach Tag	Detach a tag from a host. **Note:** • The admin tags are created and owned by the admin . The tenant tags are created and owned by tenants. • A tag created by a tenant can be attached only to the resourced owned by the tenant. The admin can attach a tag to all resources.	ALL

Action	Description	Preconditioned Host Status
	• The admin can detach or delete tags created by a tenant. • Tags created in a project belongs to the project. All project members, including the project admin, project managers, and normal project members, can perform actions on the tags. • You cannot change the owner of a tag. • If you change the owner of a resource, all tenant tags attached to the resource are detached. The admin tags are not affected. • After a seamless migration of the cloud platform, tags that were created are automatically updated and displayed in the latest format. If an error or exception occurs, refresh the browser or create a new tag. • You can detach a batch of tags from a resource or detach a tag from a batch of resources. • A tenant can only detach tags from resources owned by the tenant. The admin can detach tags from all resources.	
Update Password	Update the password of a host. After the password is updated, the host is automatically reconnected.	/
Delete Host	Delete a host. **Note:** If you delete a host, note that: • Deleting a host stops all VM instances running on the host. • If a LocalStorage primary storage is attached to the cluster to which the host belongs: — Deleting a host deletes all VM instances and volumes on the host. — If you add the deleted host to the cloud platform , the system redeploys the host. If you did not backup the database, the related business data cannot be recovered. • If a shared primary storage is attached to the cluster to which the host belongs:	/

Action	Description	Preconditioned Host Status
	— If you disable HA for VM instances: Deleting a host stops the VM instances running on the host. — If you enable HA for VM instances: Deleting a host stops the VM instances for which HA is enabled and then migrates the VM instances to other hosts where resources are available. Then the VM instances are automatically started. During the process, data security is not affected. If host resources are insufficient, the VM instances are stopped upon the host deletion. — Deleting a host does not affect data volumes stored on shared storages. • If a host is designated as the migration server, deleting a host also deletes the migration server and the migration task on the migration server will be cancelled. Proceed with caution.	

7.2.4 Primary Storage

7.2.4.1 What is Primary Storage?

A primary storage is one or more servers that store volume files of VM instances. These files include root volume snapshots, data volume snapshots, image caches, root volumes, and data volumes.

The Cloud supports the following types of primary storage:

- **Local Storage:** This type of primary storage uses the hard disks to store disk files.
- **Network Shared Storage:** This type of primary storage supports NFS, Shared Mount Point (SMP), Ceph, SharedBlock, AliyunNAS, and AliyunEBS.
  - NFS primary storages use the network file system (NFS) to store files.
  - SMP primary storages support network shared storages provided by commonly used distributed file systems, such as MooseFS, GlusterFS, OCFS2, and GFS2.

- Ceph primary storages use distributed block storages to store files.
- SharedBlock primary storages use shared block storages to store files.
- AliyunNAS primary storages use distributed files to store files.
- AliyunEBS primary storages use distributed block storages to store files.

The following table lists the relationship between primary storages and a cluster.

Table 7-5: Relationship Between Primary Storage and Cluster

Primary Storage	Cluster
LocalStorage	A cluster can have one or more LocalStorage primary storages attached.
NFS	A cluster can have one or more NFS primary storages attached.
SharedBlock	A cluster can have one or more SharedBlock primary storages attached.
SMP	A cluster can have one SMP primary storage attached.
Ceph	A cluster can have only one Ceph primary storage attached.
AliyunNAS	A cluster can have only one AliyunNAS primary storage attached.
AliyunEBS	A cluster can have only one AliyunEBS primary storage attached.
LocalStorage + NFS	A cluster can have one LocalStorage and one NFS primary storage attached.
LocalStorage + SMP	A cluster can have one LocalStorage and one SMP primary storage attached.
LocalStorage + Shared Block	A cluster can have one LocalStorage and one SharedBlock primary storage attached.
Ceph + SharedBlock	• A cluster can have one Ceph and one SharedBlock primary storage attached. • A cluster can have one Ceph and multiple SharedBlock primary storages attached.

7.2.4.2 Add a Primary Storage

On the main menu of ZStack Cloud, choose **Resource Center** > **Hardware** > **Storage Facility** > **Primary Storage**. On the **Primary Storage** page, click **Add Primary Storage**. Then, the **Add Primary Storage** page is displayed.

The following lists the primary storages that you can add:

- Add a LocalStorage primary storage.
- Add an NFS primary storage.
- Add a SharedMountPoint (SMP) primary storage.
- Add a Ceph primary storage.
- Add a SharedBlock primary storage.

Add a LocalStorage Primary Storage

Set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the primary storage.

  The primary storage name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the primary storage.
- **Type**: Select LocalStorage.

  Note:

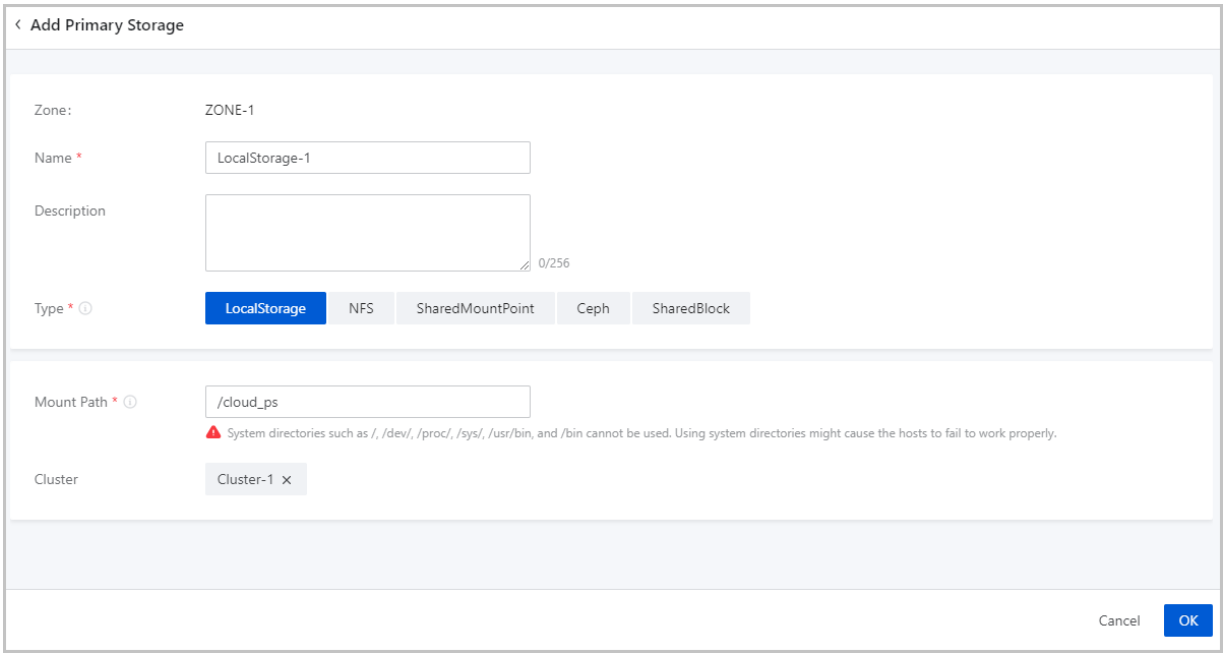
  - If you select LocalStorage, the Cloud uses the hard disks of each host as a primary storage. LocalStorage primary storages can work with ImageStore and SFTP backup storages. The total capacity of a LocalStorage primary storage is the sum of each host directory capacity.
  - If you attach multiple LocalStorage primary storages, make sure that each LocalStorage primary storage is deployed on an exclusive logical volume or physical disk.
- **Mount Path**: Enter the directory for mounting the LocalStorage primary storage.

  Note:

  - If the directory you entered does not exist, the Cloud automatically creates one.

- The following system directories cannot be used. Otherwise, the hosts might fail to work properly.
  - `/`
  - `/dev`
  - `/proc`
  - `/sys`
  - `/usr/bin`
  - `/bin`
- **Cluster**: Select a cluster to which the LocalStorage primary storage is attached.

Figure 7-49: Add LocalStorage Primary Storage



Add an NFS Primary Storage

Set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the primary storage.

  The primary storage name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the primary storage.

- **Type**: Select NFS.

  Note:

  If you select NFS, ZStack Cloud automatically mounts the same NFS shared directory on all the hosts as a primary storage. NFS primary storages can work with ImageStore and SFTP backup storages, and can automatically mount the directory on all hosts.

- **Mount Path**: Enter the shared directory of the NFS server. Either an IP address or a domain is supported.

  Note:

  - Format: *`NFS_Server_IP:/NFS_Share_folder`*. For example, *`192.168.0.1:/nfs_root`*.
  - You need to set the access permissions of the corresponding directories on the NFS server in advance.
  - To ensure security control on the NFS server, we recommend that you configure corresponding security rules for access control.
  - You can check the shared directory of the NFS server by using the `showmount -e` command on NFS server in advance.
  - The following system directories cannot be used. Otherwise, the hosts might fail to work properly.
    - *`/`*
    - *`/dev`*
    - *`/proc`*
    - *`/sys`*
    - *`/usr/bin`*
    - *`/bin`*

- **Mount Parameter**: Optional. Before you specify mount parameters, make sure that these parameters are supported by the NFS server.

  Note:

  - The parameters are separated by commas (,). For example, nfsvers=3,sec=sys,tcp,intr, timeo=5. The preceding example means that the NFS server version is 3, the standard

UNIX authentication mechanism is used, TCP is used as the transmission protocol, an NFS call can be interrupted in case of an exception, and the timeout is 0.5 seconds (5/10).

- To specify the **mount** parameters, you can refer to the content in the **-o** option of **mount**.
- You can set the parameters according to the **mount** command on commonly used clients. If the parameters conflict with the NFS server side, the server side shall prevail.

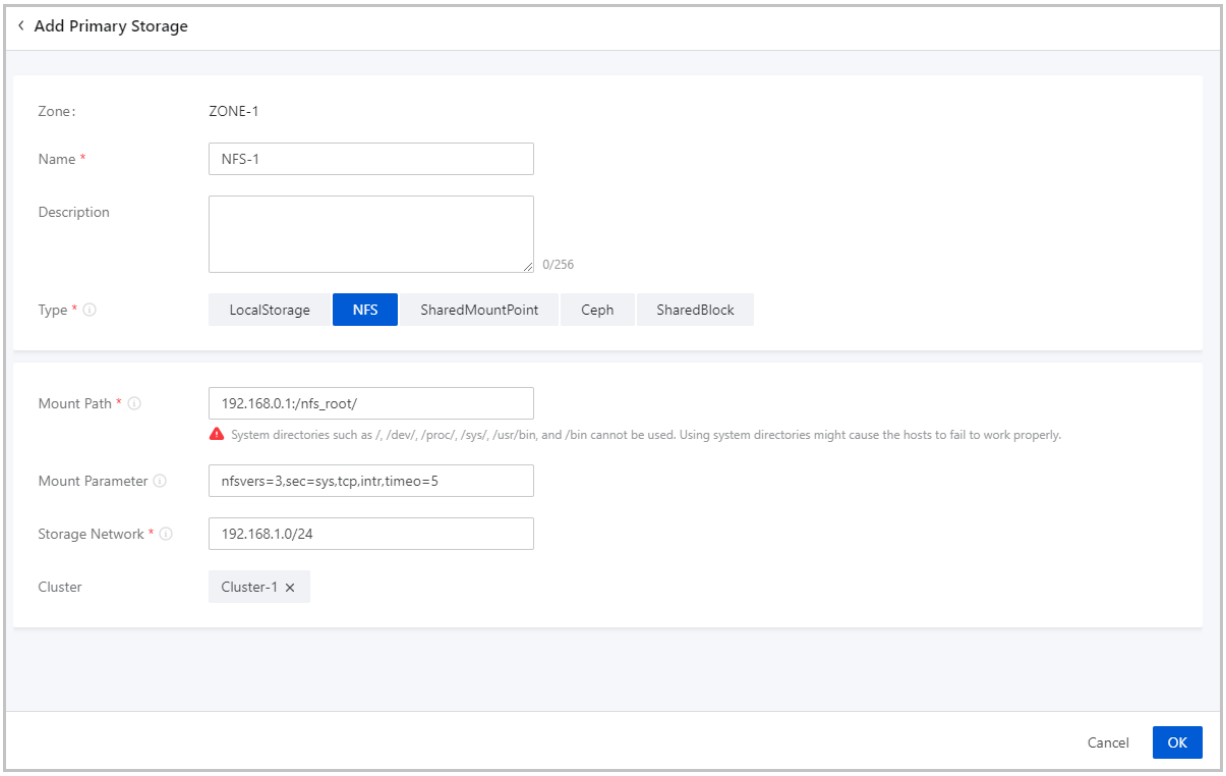
- **Storage Network**: Enter the storage network specified for the shared storage. The storage network can be the management network of the management node.

Note:

- If you have a dedicated storage network, enter its CIDR.
- We recommend that you plan an independent storage network in advance to avoid potential risks. If you do not have an independent storage network, enter the network address according to your actual needs.
- The Cloud uses the storage network to check the health status of VM instances.

- **Cluster**: Select a cluster to which the NFS primary storage is attached.

Figure 7-50: Add NFS Primary Storage



Add a SMP Primary Storage

Before you add a SMP primary storage, configure the corresponding distributed file system in advance, and mount the shared file system to the same file path on each host according to the client configuration of different storage systems.

The following example uses MooseFS as an example.

- Download and install the client tool **mfsmount** of MooseFS, and create a directory as the mount node.
- Assuming that the IP address of the MooseFS master server is *172.20.12.19*, create `/mnt/mfs` as the mount point, and use the `mfsmount` command to mount the MooseFS system.
- You can also use the `mfssetgoal` command to set the number of file copies to be saved as needed.

```
[root@localhost ~]#mkdir /mnt/mfs
[root@localhost ~]#mfsmount /mnt/mfs -H 172.20.12.19
[root@localhost ~]#mkdir /mnt/mfs/zstack
[root@localhost ~]#mfssetgoal -r 2 /mnt/mfs/zstack/
#The preceding commands mount the files in the /mnt/mfs/zstack/
 directory to 172.20.12.19, and save two copies to the MooseFS storage
 server.
```

To add a SMP primary storage, set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the primary storage.

  The primary storage name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the primary storage.
- **Type**: Select SharedMountPoint.

  Note:

  - For SMP primary storages, ZStack Cloud supports network shared storage provided by commonly used distributed file systems such as MooseFS, GlusterFS, OCFS2, and GFS2.
  - SMP primary storages can work with ImageStore and SFTP backup storages.
- **Mount Path**: Enter the directory of the shared storage mounted by the host.

  Note:

- The following system directories cannot be used. Otherwise, the hosts might fail to work properly.
  - `/`
  - `/dev`
  - `/proc`
  - `/sys`
  - `/usr/bin`
  - `/bin`

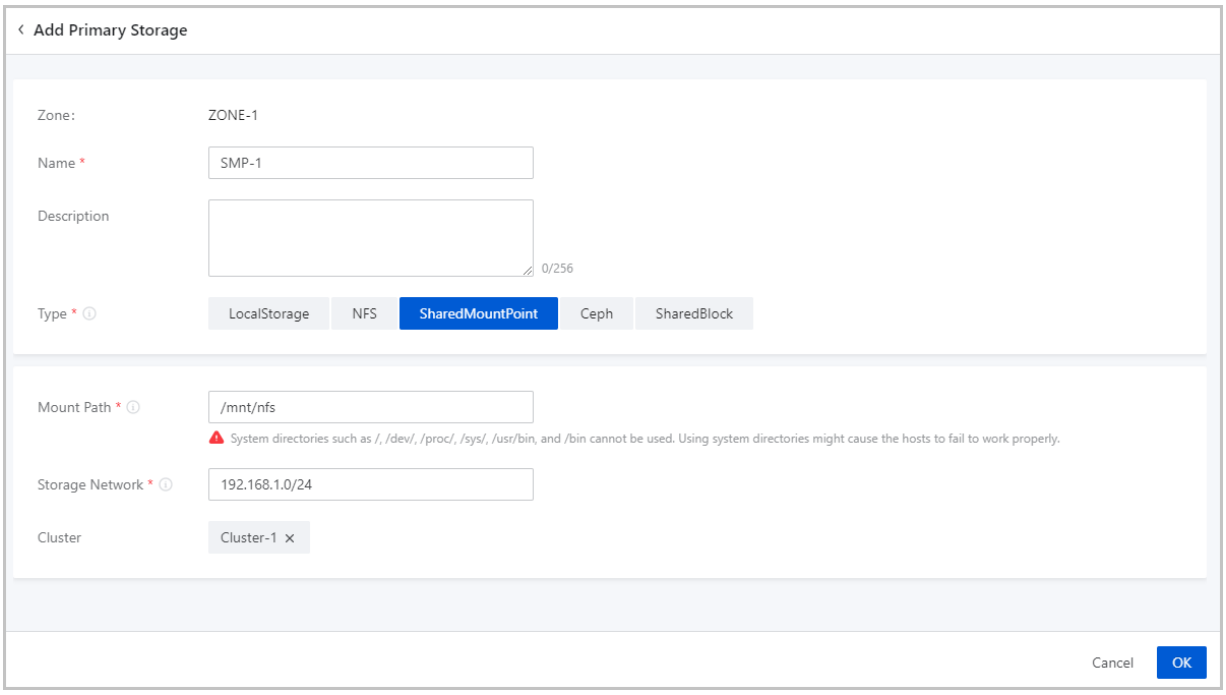
- **Storage Network**: Enter the storage network specified for the shared storage. The storage network can be the management network of the management node.

  Note:

  - If you have a dedicated storage network, enter its CIDR.
  - We recommend that you plan an independent storage network in advance to avoid potential risks. If you do not have an independent storage network, enter the network address according to your actual needs.
  - The Cloud uses the storage network to check the health status of VM instances.

- **Cluster**: Select a cluster to which the SMP primary storage is attached.

Figure 7-51: Add SMP Primary Storage



Add a Ceph Primary Storage

ZStack Cloud supports Ceph block storages. Before you can add a Ceph primary storage, add a Ceph or an ImageStore backup storage, and configure the Ceph distributed storage in advance.

To add a Ceph primary storage, set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the primary storage.

  The primary storage name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the primary storage.
- **Type**: Select Ceph.

  Note:

  ZStack Cloud primary storages can work with the following Ceph editions:

  - Ceph open-source edition: Jewel series, Luminous series, and Nautilus series.
  - Ceph Enterprise: All released Ceph Enterprise. If you are concerned more about data security and I/O performance, Ceph Enterprise is recommended. For more information, contact our official technical support.
- **Cephx**: Optional. Determine whether to enable Ceph authentication.

  Note:

  - By default, Ceph authentication is enabled.
  - If the network of the storage node and the compute node is relatively safe, you can disable Cephx to avoid Ceph authentication failure.
  - Make sure that the key authentication of the Ceph storage is consistent with this option. If Cephx is not disabled for the Ceph storage, enabling Ceph authentication here may cause VM creation failure.
- **Mon Node**: Enter the IP address, SSH port, user name, and password of the Ceph monitor.

  — **Management IP**: Enter the IP address of the Ceph monitor.

  — **SSH Port**: Enter the SSH port of the Ceph monitor. Default: 22.

  — **User Name**: Enter the user name of the Ceph monitor.

  — **Password**: Enter the password of the Ceph monitor.

You can click **Add Mon Node** to add more Ceph monitors.

- **Image Cache Pool**: Optional. Enter the name of an image cache storage pool.

  Note:

  - You can specify a storage pool for image caches. If you do not specify a storage pool, the Cloud creates one automatically.
  - If you specify a storage pool, make sure that a storage pool is already available in the Ceph cluster. Then you can specify the UUID of a storage pool.

- **Data Volume Pool**: Optional. Enter the name of a data volume storage pool.

  Note:

  - You can specify a storage pool for data volumes. If you do not specify a storage pool, the Cloud creates one automatically.
  - If you specify a storage pool, make sure that a storage pool is already available in the Ceph cluster. Then you can specify the UUID of a storage pool.

- **Root Volume Pool**: Optional. Enter the name of a root volume storage pool.

  Note:

  - You can specify a storage pool for root volumes. If you do not specify a storage pool, the Cloud creates one automatically.
  - If you specify a storage pool, make sure that a storage pool is already available in the Ceph cluster. Then you can specify the UUID of a storage pool.

- **Storage Network**: Enter the storage network specified for the shared storage. The storage network can be the management network of the management node.

  Note:

  - If you have a dedicated storage network, enter its CIDR.
  - We recommend that you plan an independent storage network in advance to avoid potential risks. If you do not have an independent storage network, enter the network address according to your actual needs.
  - The Cloud uses the storage network to check the health status of VM instances.

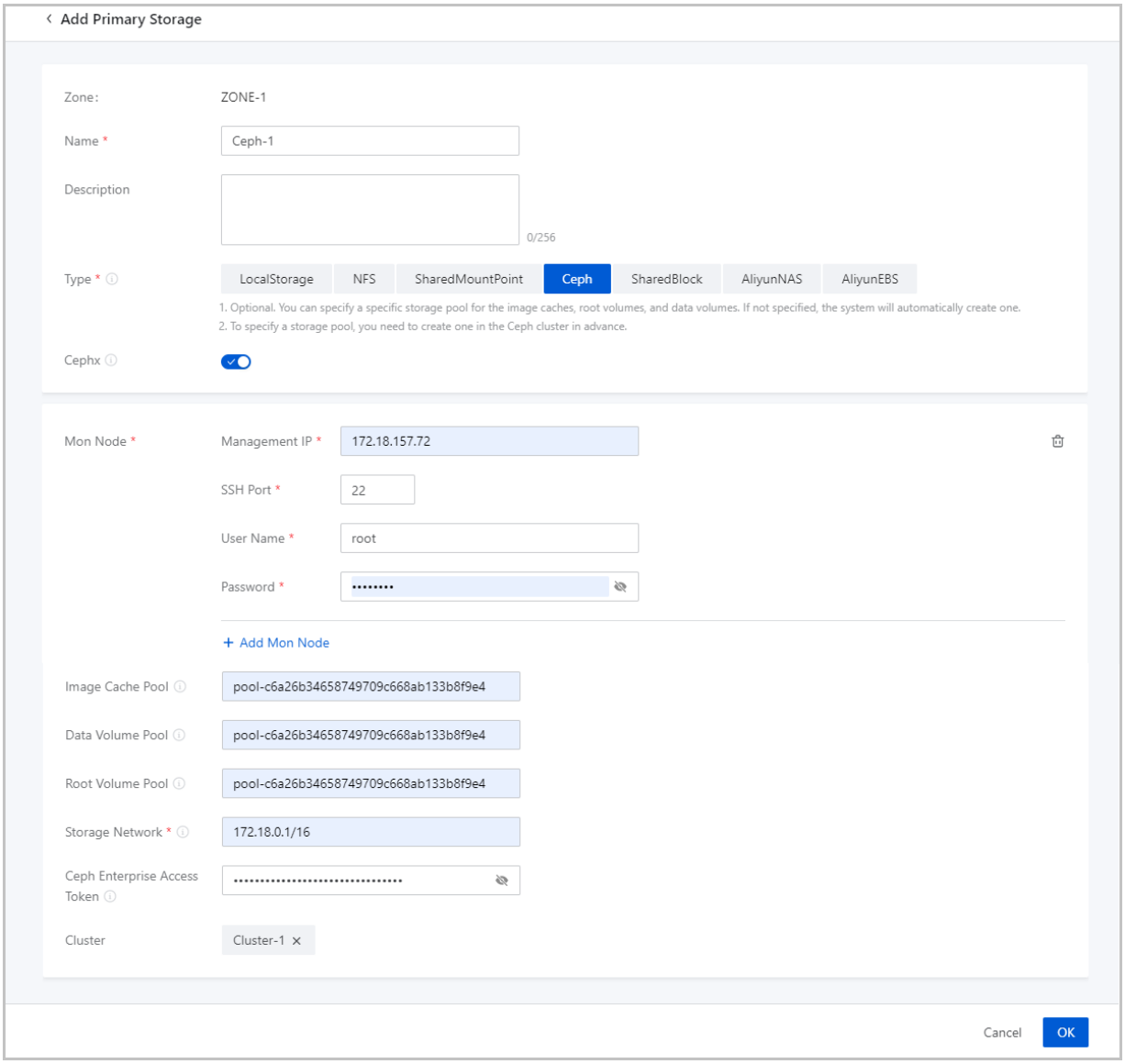
- **Ceph Enterprise Access Token**: Optional. If you add the access token, the Ceph Enterprise storage is managed by using the token.

Note:

- We recommend that you add the access token when you need to use Ceph Enterprise storage for elastic baremetal clusters.
- Make sure that your Ceph Enterprise license is valid.

- **Cluster**: Select a cluster to which the Ceph primary storage is attached.

Figure 7-52: Add Ceph Primary Storage



Add a SharedBlock Primary Storage

Set the following parameters:

- **Zone**: By default, the current zone is displayed.

- **Name**: Enter a name for the primary storage.

  The primary storage name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the primary storage.
- **Type**: Select SharedBlock.

  Note:

  - SharedBlock primary storages use LUN devices for storage and can work with ImageStore backup storages.
  - You can add LUN devices online.
  - Currently, SharedBlock primary storages support two shared access protocols: iSCSI and FC.
- **Default Storage Space Allocation Strategy**: Select a storage space allocation strategy, including thick provisioning and thin provisioning.

  — **Thick Provisioning**: Allocates the required storage space in advance to provide sufficient storage capacities and to ensure storage performances.

  — **Thin Provisioning**: Thin provision: Allocates storage spaces as needed to achieve a higher storage utilization.
- **Storage Network**: Enter the storage network specified for the shared storage. The storage network can be the management network of the management node.

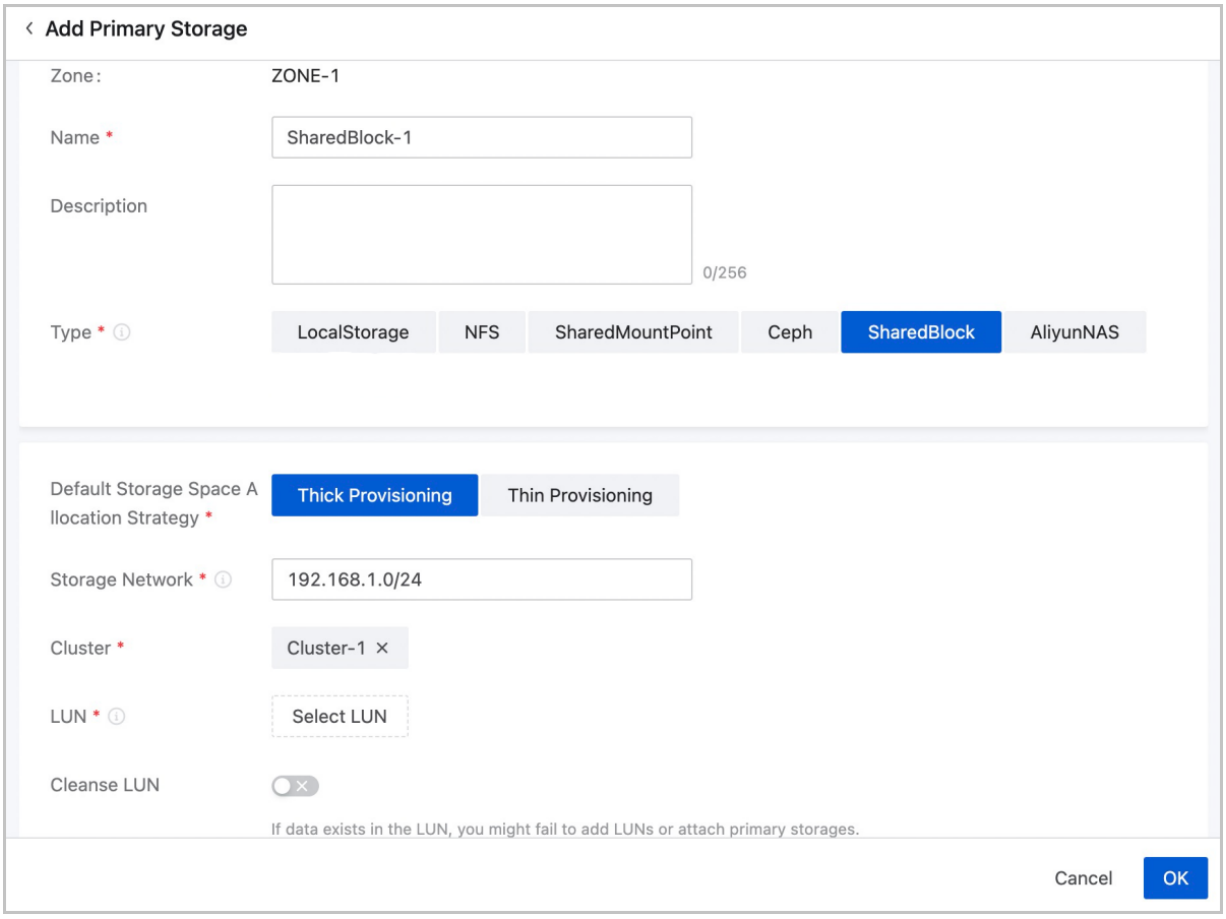
  Note:

  - If you have a dedicated storage network, enter its CIDR.
  - We recommend that you plan an independent storage network in advance to avoid potential risks. If you do not have an independent storage network, enter the network address according to your actual needs.
  - The Cloud uses the storage network to check the health status of VM instances.
- **Cluster**: Select a cluster to which the SharedBlock primary storage is attached.
- **LUN**: Select one or more LUN devices as needed. Here you need to enter the disk unique identifier.

> **Note:**
> Make sure that the compute node is properly connected to the storage device, and is added to the Cloud.

- **Cleanse LUN**: Optional. Determine whether to cleanse LUN devices. By default, LUN devices are not cleansed.
  - If you choose to cleanse LUN devices, the residual data, such as file systems, RAID, or signatures of partition tables in the LUN devices will be forced to clean up.
  - If data exists in your LUN devices, and you do not cleanse the devices, you will fail to add LUN devices or attach primary storages.
  - The LUN devices to be added cannot have partitions. Otherwise, you will fail to add the devices.

Figure 7-53: Add SharedBlock Primary Storage



7.2.4.3 Manage a Primary Storage

On the main menu of ZStack Cloud, choose **Resource Center** > **Hardware** > **Storage Facility** > **Primary Storage**. Then, the **Primary Storage** page is displayed.

The following table lists the actions that you can perform on a primary storage.

Action	Description
Add Primary Storage	Add a primary storage to the Cloud.
Edit Primary Storage	Edit the name and description of the primary storage.
Enable Primary Storage	Enable the primary storage when it is disabled.
Disable Primary Storage	Disable the primary storage. After the primary storage is disabled, you cannot use it to create VM instances, volumes, or snapshots. However, existing resources are not affected.
Reconnect Primary Storage	Reconnect the primary storage. This action will update the storage information about the primary storage. **Note:** If any host can connect properly to the primary storage, the status of the primary storage will be **Connected**.
Enter Maintenance Mode	Place the primary storage in maintenance mode. **Note:** • Placing a primary storage in maintenance mode stops resources such as VM instances on the primary storage. • After a primary storage enters into maintenance mode, volumes on the primary storage cannot be used.
Create Volume	Create a volume on the primary storage. Then, this volume will be an instantiated volume. **Note:** Shared volumes now support only Ceph and SharedBlock primary storages.
Attach Cluster	Attach the primary storage to a cluster. Note that one cluster can have multiple primary storages attached. The following are primary storages of the same type that a cluster can have:

Action	Description
	• A cluster can have one or more LocalStorage primary storages attached. • A cluster can have one or more NFS primary storages attached. • A cluster can have one or more SharedBlock primary storages attached. • A cluster can have one SharedMountPoint (SMP) primary storages attached. • A cluster can have only one Ceph primary storage attached. • A cluster can have only one AliyunNAS primary storage attached. • A cluster can have only one AliyunEBS primary storage attached. The following are combinations of primary storages that a cluster can have: • A cluster can have both a LocalStorage and an NFS primary storage attached. • A cluster can have both a LocalStorage and an SMP primary storage attached. • A cluster can have both a LocalStorage and a SharedBlock primary storage attached. • A cluster can have both a Ceph and a SharedBlock primary storage attached. • A cluster can have both a Ceph and more than one SharedBlock primary storage attached.
Detach Cluster	Detach the primary storage from a cluster. **Note:** If you detach a primary storage from a cluster, note the following: • This operation might shut down VM instances on the primary storage and associated with the selected cluster, thus affecting the service running. Please exercise caution. • This operation might delete VPC vRouters on the primary storage and associated with the selected cluster, thus affecting the corresponding network service. Please exercise caution. • This operation might cause the volumes on the primary storage and associated with the selected cluster to fail to work properly. Please exercise caution.

Action	Description
	If you detach a primary storage from an elastic baremetal cluster, note the following: • This operation might shut down VM instances on the primary storage and associated with the selected elastic baremetal cluster, thus affecting the service running. Please exercise caution. • This operation might cause the volumes on the primary storage and associated with the selected elastic baremetal cluster to fail to work properly. Please exercise caution.
Delete Primary Storage	Delete the primary storage. **Note:** When you delete a primary storage, note the following: • Before you can delete the primary storage, detach it from all clusters. • Deleting a primary storage also deletes all the resources on the primary storage, such as VM instances, elastic baremetal instances , volumes, and snapshots. Even if you add this primary storage again, the original files cannot be automatically detected.
Clean up Data	Clean up original data reserved during the migrations across Ceph primary storages, the migrations across NFS primary storages, and the migrations across SharedBlock primary storages. To perform this action, go to the **Data Cleanup** tab of the primary storage details page, and click **Cleanup**. These data cannot be recovered after cleanup. Please exercise caution.

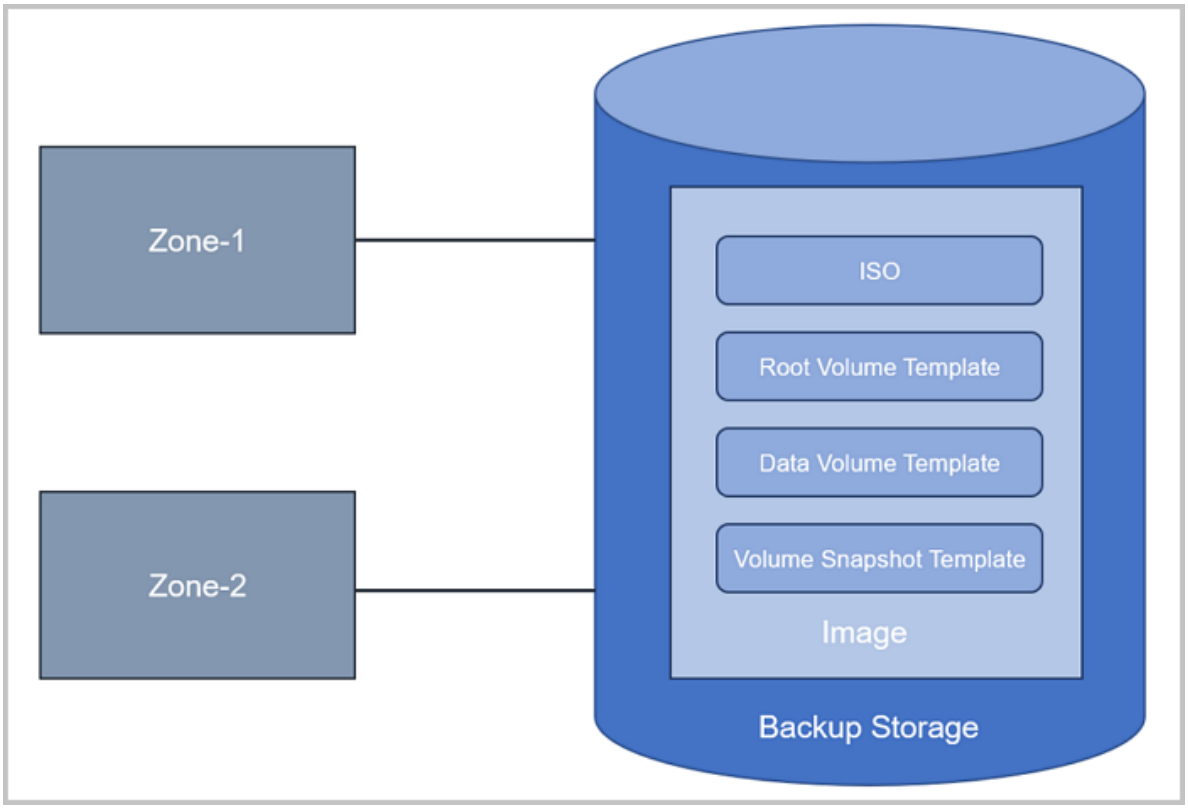
7.2.5 Backup Storage

7.2.5.1 What is Backup Storage?

A backup storage is one or more servers that store VM image templates, including ISO image files .

- A backup storage must be attached to a zone before the resources in the zone can access it. Note that you can share images across multiple zones by using the backup storage.

Figure 7-54: Backup Storage



- To better manage backup storages and zones, the UI specifies that one backup storage can only correspond to one zone. In the UI, when you add a backup storage, the backup storage will be attached to the current zone by default. When you delete a zone, the backup storage attached to the zone will also be deleted.

Backup Storage Type

The Cloud supports the following types of backup storage:

1. **ImageStore**

   - Stores image files by means of image slices and supports incremental storage.
   - Allows you to create snapshots and images when VM instances are running or stopped.
   - Allows you to clone VM instances without data volumes when these VM instances are running, paused, or stopped.
   - Allows you to clone VM instances with data volumes when these VM instances are running, paused, or stopped, and with storage types of LocalStorage, NFS, SharedMountPoint (SMP), Ceph, or SharedBlock.

- Supports image synchronization across ImageStore backup storages on the same management node.
- Allows you to obtain the existing image files under the URL path in the backup storage.

2. **Ceph**

- Stores image files by means of Ceph distributed block storages.
- Allows you to create snapshots and images when VM instances are running or stopped.
- Allows you to clone VM instances without data volumes when these VM instances are running, paused, or stopped.
- Allows you to clone VM instances with data volumes when these VM instances are running, paused, or stopped, and with the storage type of Ceph.
- Allows you to export images on the UI or backup storages.
  - You can export images, copy exported image URLs, and download exported images on the UI.
  - You can also export images on a backup storage.

    For example, assume that the image path you use is *ceph://bak-t-c9923f9821bf45498fdf9cdfa1749943/61ece0adc7244b0cbd12dafbc5494f0c*.

    Then, run the following command on the backup storage:

```
rbd export -p bak-t-c9923f9821bf45498fdf9cdfa1749943 --image
61ece0adc7244b0cbd12dafbc5494f0c --path /root/export-test.image

# bak-t-c9923f9821bf45498fdf9cdfa1749943 is the name of the
pool where the image resides.
# 61ece0adc7244b0cbd12dafbc5494f0c is the name of the image.
# /root/export-test.image is the name of the exported file.
```

3. **AliyunEBS**

- Stores image by means of object storages.
- Allows you to create snapshots and images when VM instances are running or stopped.
- Allows you to clone VM instances without data volumes when these VM instances are running, paused, or stopped.
- Does not allow you to clone VM instances with data volumes.
- Allows you to export images on backup storages. For more information, contact the official technical support.

Backup Storage | Primary Storage

The following table lists the relationship between primary storages (PS) and backup storages (BS).

Table 7-6: Relationship Between PS and BS

PS/BS	ImageStore	SFTP	Ceph
LocalStorage	○	○	×
NFS	○	○	×
SMP	○	○	×
Ceph	○	×	○
SharedBlock	○	×	×

- When primary storages are LocalStorage, NFS, or SMP, the default type for backup storages is ImageStore.
- When primary storages are NFS or SMP, you can manually mount the corresponding shared directories to the local directories of the corresponding backup storages. In this regard, both primary storages and backup storages can use the network shared storage.
- When primary storages are Ceph, you can use the primary storages in the same Ceph cluster as backup storages. You can also use the ImageStore primary storages as backup storages.
- When primary storages are SharedBlock, the default type for backup storages is ImageStore.
- When primary storages are AliyunNAS, the default type for backup storages is ImageStore.
- When primary storages are AliyunEBS, the default type for backup storages is AliyunEBS.

7.2.5.2 Add a Backup Storage

On the main menu of ZStack Cloud, choose **Resource Center** > **Hardware** > **Storage Facility** > **Backup Storage**. On the **Backup Storage** page, click **Add Backup Storage**. Then, the **Add Backup Storage** page is displayed.

The following lists the backup storages that you can add:

- Add an ImageStore backup storage.
- Add a Ceph backup storage.
- Add an AliyunEBS backup storage.

Add an ImageStore Backup Storage

Set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the backup storage.
- **Description**: Optional. Enter a description for the backup storage.
- **Type**: Select ImageStore.
- **Backup Storage IP**: Enter an IP address for the ImageStore backup storage.
- **Mount Path**: Enter the mount path the ImageStore backup storage. For example, `/cloud_bs`

  Note:

  - We recommend that you mount a large-capacity storage for the directory, and enter the absolute path of the directory.
  - The following system directories cannot be used. Otherwise, the hosts might fail to work properly.
    - `/`
    - `/dev/`
    - `/proc/`
    - `/sys/`
    - `/usr/bin`
    - `/bin`
- **Retrieve Existing Image**: Optional. Choose whether to obtain existing images for the ImageStore backup storage.

  Note:

  - You can obtain existing images from the mount path of the backup storage.
  - Only ImageStore backup storages allow you obtain their existing images.
- **SSH Port**: Set an SSH port for the backup storage.

  Note:

  The port must be an integer. Default: 22.
- **User Name**: Use either the default user name (root) or enter a user name for the backup storage.

- **Password**: Enter the password for the user name.
- **Data Network**: Optional. If you planned a dedicated network for data communication between the compute node and the backup storage, enter its CIDR.

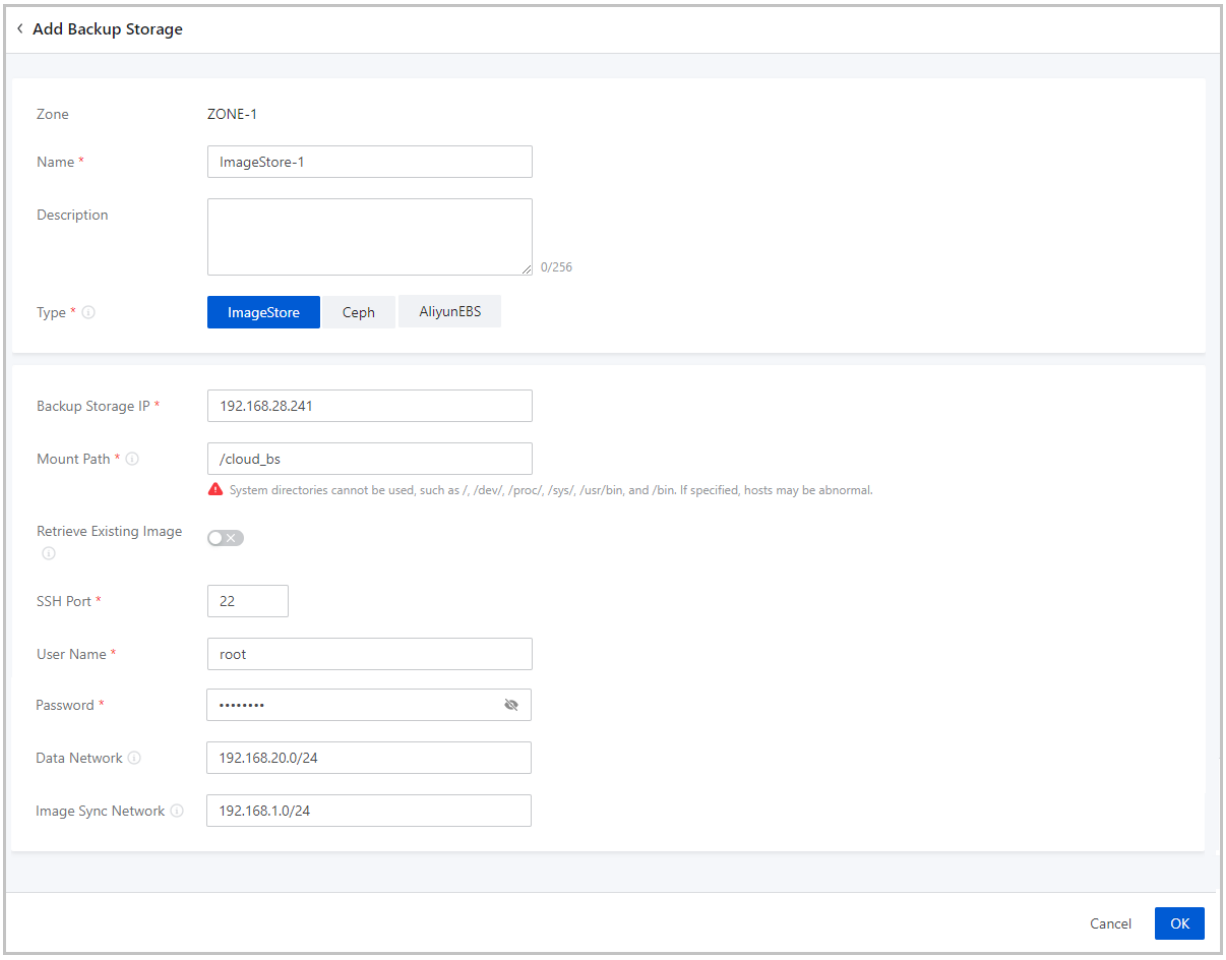
  Note:

  - If not set, the Cloud uses the management network by default.
  - If you planned a dedicated network for data communication between the compute node and the backup storage, add it directly to the Cloud.
- **Image Sync Network**: Optional. Enter the CIDR of the image synchronization network.

  Note:

  - If not set, a management network will be used by default for image synchronization.
  - You can synchronize images between ImageStore backup storages within the same management node.
  - If you deployed a dedicated network for image synchronization, add it directly to the Cloud.
  - Using a dedicated image synchronization network can avoid network congestion and improve transmission efficiencies.
  - If you set an image synchronization network for both a source ImageStore and a destinatio n ImageStore backup storage, only the image synchronization network of the destination ImageStore backup storage works.

Figure 7-55: Add ImageStore Backup Storage



Add a Ceph Backup Storage

Set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the backup storage.
- **Description**: Optional. Enter a description for the backup storage.
- **Type**: Select Ceph.
- **Mon Node**: Select the Ceph monitor for creating the Ceph backup storage and complete the following configurations:
  - **Mon Management IP**: Enter the IP address of the Ceph monitor.
  - **SSH Port**: Enter the SSH port of the Ceph monitor. Default: 22.
  - **User Name**: Enter the user name of the Ceph monitor.
  - **Password**: Enter the password of the Ceph monitor.

Note:

- You can set the interval that the management node reconnects the mon node of the Ceph backup storage if the mon IP fails to be detected. Method:

  Go to **Settings** > **Platform Setting** > **Global Setting** > **Advanced** > **Resource Center** > **Hardware** > **Backup Storage**, locate **Interval of Auto-Reconnection to Mon Node of Backup Storage**, and change its values as needed. Default: 30 seconds.
- You can specify whether to enable automatic reconnection to the mon node of the Ceph backup storage if the mon IP fails to be detected. Method:

  Go to **Settings** > **Platform Setting** > **Global Setting** > **Advanced** > **Resource Center** > **Hardware** > **Backup Storage**, locate **Enable Auto-Reconnection to Mon Node of Backup Storage**, and change its value as needed. By default, the auto reconnection is disabled.

You can click **Add Mon Node** to add more Ceph monitors.

- **Image Storage Pool**: Optional. Enter an image storage pool UUID.

Note:

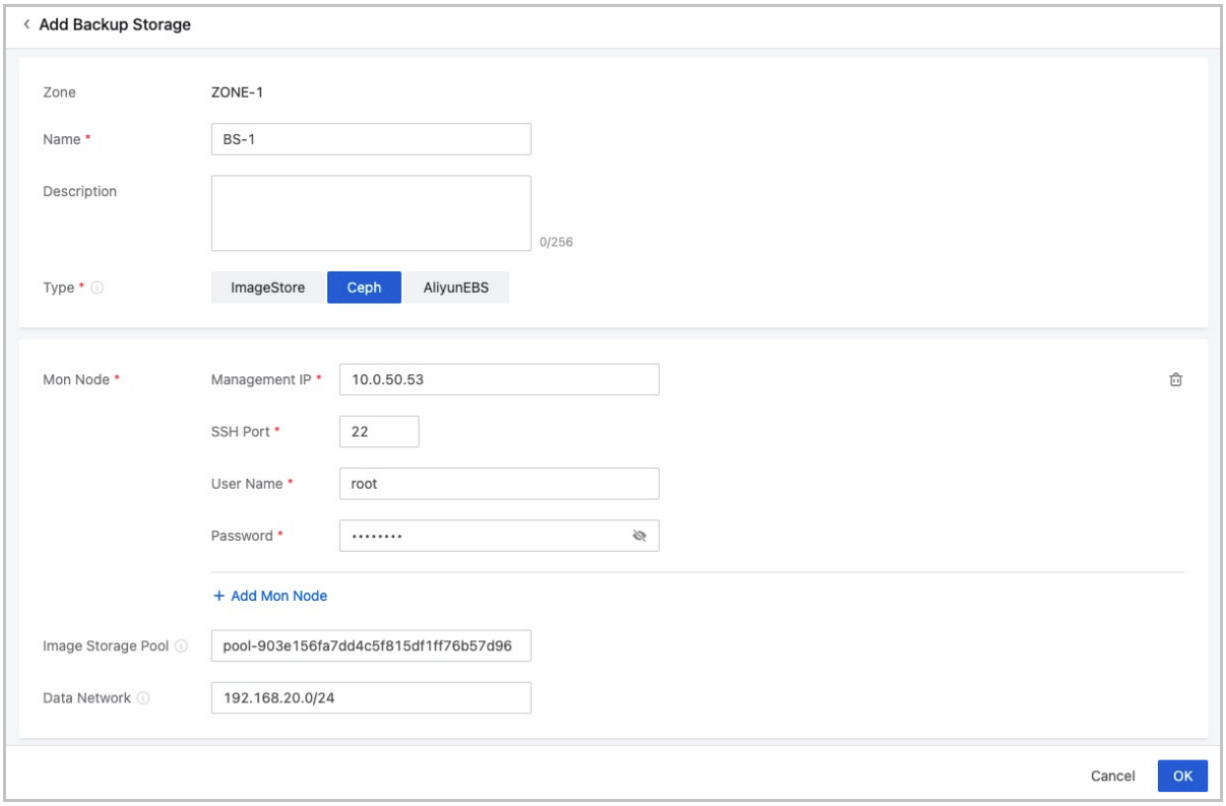
- You can specify a storage pool for the Ceph backup storage to store images. If you do not specify a storage pool, the Cloud creates one automatically.
- If you specify a storage pool, make sure that a storage pool is already available in the Ceph cluster. Then you can specify the UUID of a storage pool.

- **Data Network**: Optional. Enter the CIDR of a data network.

Note:

- If not set, the Cloud uses the management network by default.
- If you planned a dedicated network for data communication between the compute node and the backup storage, add it directly to the Cloud.

Figure 7-56: Add Ceph Backup Storage



Add an AliyunEBS Backup Storage

Set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the backup storage.
- **Description**: Optional. Enter a description for the backup storage.
- **Type**: Select AliyunEBS.
- **Mount Path**: Enter an Ocean API endpoint.

> **Note:**
>
> - **AliyunEBS** backup storages send requests to an Ocean server through this mount path.
> - Format: `http://Ocean_Server_Domain:Port/ocean/api`.

- **Bucket**: Select an OSS bucket you added to ZStack Cloud.

> **Note:**
>
> You can specify whether to roll back objects in OSS buckets if an error occurs when you upload custom images to Alibaba Cloud EBS backup storage. Method:

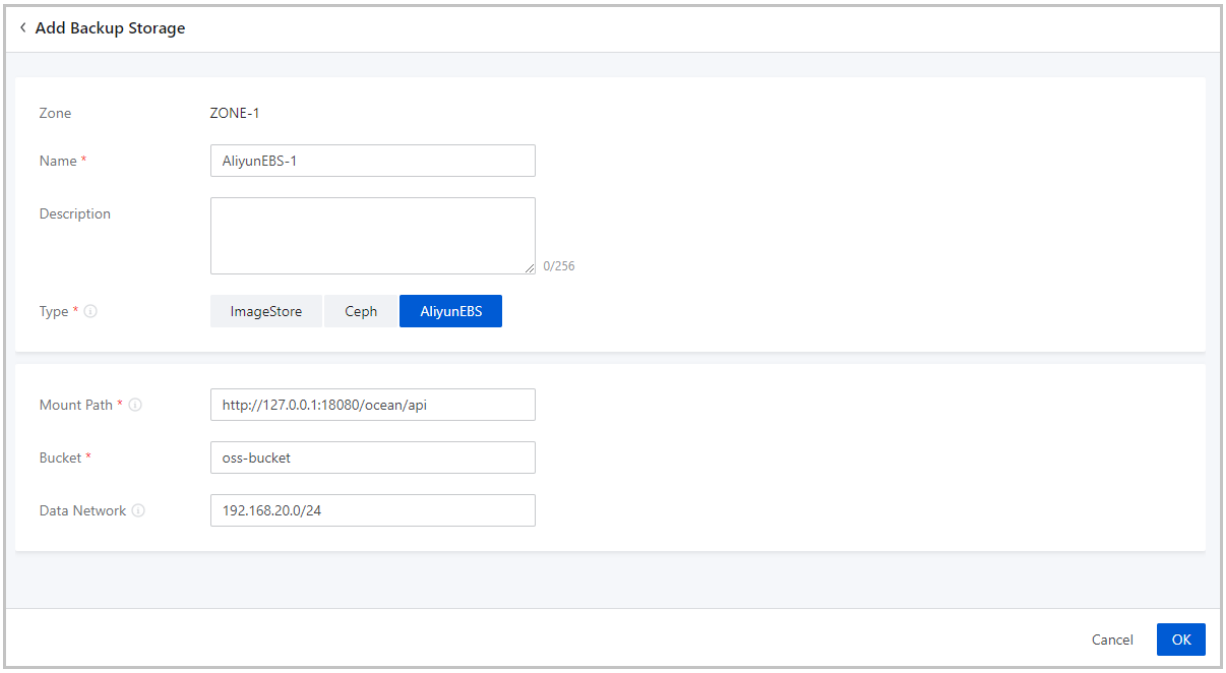
Go to **Settings** > **Hybrid Cloud Settings** > **Hybrid Cloud** > **Alibaba Cloud NAS**, locate **Rollback Imported Image**, and change its value as needed. Default: True.

- **Data Network**: Optional. If you planned a dedicated network for data communication between the compute node and the backup storage, enter its CIDR.

Note:

If not set, the Cloud uses the management network by default.

Figure 7-57: Add AliyunEBS Backup Storage



7.2.5.3 Manage a Backup Storage

On the main menu of ZStack Cloud, choose **Resource Center** > **Hardware** > **Storage Facility** > **Backup Storage**. Then, the **Backup Storage** page is displayed.

The following table lists the actions that you can perform on a backup storage.

Action	Description
Add Backup Storage	Add a backup storage to the Cloud.
Edit Backup Storage	Edit the name and description of the backup storage.
Enable Backup Storage	Enable the backup storage when it is disabled.

Action	Description
Disable Backup Storage	Disable the backup storage. **Note:** After a backup storage is disabled, you cannot add images to this backup storage. However, you can still use existing images to create VM instances.
Reconnect Backup Storage	Reconnect the backup storage. This action will update the storage information about the backup storage. **Note:** • You cannot perform any operations on resources of the backup storage during the reconnection. • If any host can connect properly to the backup storage, the status of the backup storage will be **Connected**.
Clean up Data	Clear both the invalid data that have been completely deleted and the temporary data that were expired on the backup storage to release storage spaces. **Note:** • For example, assume that you have deleted an image file (either an ordinary image or a vRouter image) totally, and have deleted the VM instances created from this image file. If you clean up data , storage spaces of the backup storage will be released. After you clean up the data successfully, the UI will display the released space size and the available space. • Only data stored on ImageStore backup storages can be cleaned up. • Avoid operations such as writing data during data cleanup.
Update Password	Update the password of the backup storage. You need to reconnect the backup storage after the updates.
Delete Backup Storage	Delete the backup storage. **Note:** • Deleting a backup storage also deletes all image files,including ordinary images and vRouter images on the backup storage. Please exercise caution.

Action	Description
	• The preceding deleting operation can only remove the records of the backup storage and the image on the ZStack Cloud. Real data will not be deleted. Deleting a backup storage only deletes the backup storage and image records on the ZStack Cloud but not the actual data.

7.2.6 SAN Storage

7.2.6.1 What is SAN Storage?

Storage Area Network (SAN) storage can be categorized into iSCSI storage and FC storage:

- iSCSI storage is an SAN storage that uses the iSCSI protocol for data transmission. You can add an iSCSI SAN block as a Shared Block primary storage or pass through the block to a VM instance.
- FC storage is an SAN storage that uses the FC technology for data transmission. You can add an FC SAN block as a Shared Block primary storage or pass through the block to a VM instance.

Scenarios

- Passes through an iSCSI or FC disk to a VM instance.
- Adds an iSCSI or FC disk as a shared block and takes the shared block as a Shared Block primary storage.

Considerations

iSCSI storage:

- You can add a disk that is not attached to a VM instance as a Shared Block primary storage.
- A logical unit number (LUN) that is added as a primary storage cannot be used for other purposes.
- You can attach a disk that is not added as a primary storage to a VM instance.
- You can attach a disk to multiple VM instances or attach multiple disks to one VM instance.

FC storage:

- If a block device is not attached to a VM instance and the cluster where the block device resides is in normal state, you can add the block device as a Shared Block primary storage.
- A logical unit number (LUN) that is added as a primary storage cannot be used for other purposes.

- You can attach a block device that is not added as a primary storage to a VM instance.
- You can attach a block device to multiple VM instances or attach multiple block devices to one VM instance.

7.2.6.2 Add an iSCSI Storage

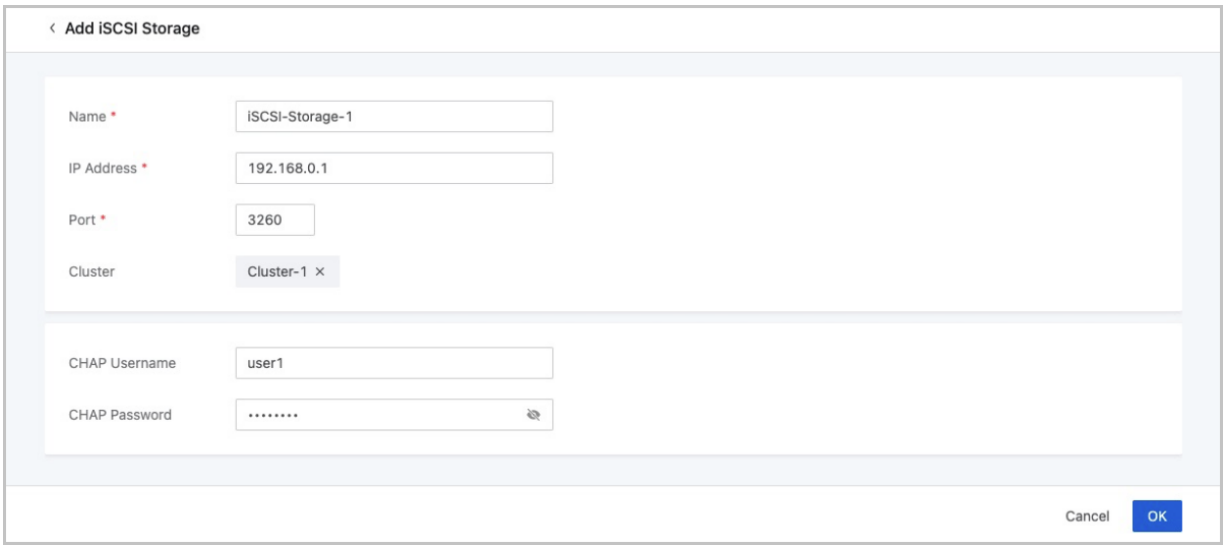
On the main menu of ZStack Cloud, choose **Resource Center** > **Hardware** > **Storage Facility** > **iSCSI Storage**. On the **iSCSI Storage** page, click **Add iSCSI Storage**. Then, the **Add iSCSI Storage** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter the name of the iSCSI storage.

  The name must be 1 to 128 characters in length and can contain Chinese characters, English letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **IP Address**: Set the IP address of the iSCSI storage.
- **Port**: Set the port of the iSCSI storage. Default port: *3260*.
- **Cluster**: Optional. Select a cluster. You can also attach a cluster after you add the iSCSI storage.
- **CHAP Username**: Optional. Enter the CHAP username if the iSCSI storage has CHAP authentication configured.
- **CHAP Password**: Optional. Enter the CHAP password if the iSCSI storage has CHAP authentication configured.

Figure 7-58: Add iSCSI Storage



7.3 Network Resource

This topic falls into the following parts:

- L2 network resources
- L3 network resources
- L3 network architecture model
- Dedicated networks
- Route resources
- SDN controller
- Network usage procedure
- Network protocol

L2 Network Resources

L2 network resources include L2 networks and VXLAN pools.

- An L2 network corresponds to a layer 2 broadcast domain. This L2 network supports multiple network types, such as L2NoVlanNetwork, L2VlanNetwork, VxlanNetwork, and HardwareVxlanNetwork.
- L2NoVlanNetwork and L2VlanNetwork is a group that must be identical to the configurations of compute node ports on the switch sides.
- Both VXLAN Pool and VxlanNetwork with the software SDN type provide the VxlanNetwork configurations. Before you use VxlanNetwork, create a VXLAN pool first. Then, create VxlanNetwork by specifying or randomly choosing VNIs.
- Both VXLAN Pool and HardwareVxlanNetwork with the hardware SDN type provide the HardwareVxlanNetwork configurations. Before you use HardwareVxlanNetwork, create a VXLAN pool first. Then, create HardwareVxlanNetwork by specifying or randomly choosing VNIs.

L3 Network Resources

An L3 network can serve as a sub-resource of the L2 network. Mainly based on the L2 network, the L3 network provides the network configurations for VM instances, including the IP range, gateway, DNS, and network service.

L3 Network Architecture Model

The Cloud supports two L3 network architecture models: flat network and VPC network.

Dedicated Networks

Dedicated networks include management networks and flow networks. Note that you cannot create VM instances by using dedicated networks.

Route Resources

ZStack Cloud provides network services for VM instances by using custom Linux VM instances to serve as routing devices. Related route resources mainly include VPC vRouters, VPC HA groups, vRouter images, and vRouter offerings.

SDN Controller

By adding SDN controllers, you can take over the SDN networks of hardware switches on the Cloud to lower the network latency and improve the VXLAN network performance.

Network Usage Procedure

You need to first create an L2 network, use the L2 network to create an L3 network, and then use these networks to provide multiple network services.

Network Protocol

ZStack Cloud public network, flat network, and VPC network support two network protocols: IPv4 and IPv6. You can create an IPv4 network, an IPv6 network, or an IPv4+IPv6 network as needed.

7.3.1 L2 Network

7.3.1.1 What is L2 Network?

An L2 network is a layer 2 broadcast domain used for layer 2 isolation. Generally, L2 networks are identified by names of devices on the physical network.

- VLAN, VXLAN, and SDN can be used as an L2 network.
- An L2 network is used to provide layer 2 isolation for an L3 network.

L2 Network Types

The following four types of L2 networks are supported:

1. **L2NoVlanNetwork**
   - You must specify the NIC name of the host.
   - The hosts in the cluster to which the L2 network is attached must have NICs that share the same name.

- When the data packets of VM instances flow out of the host NIC and reach the physical switch, the data packets are not flagged with VLAN tags. Note that the physical switch must be in VLAN Access mode.
- If you create an L2 network of the L2NoVlanNetwork type, a network bridge is created based on the specified host NIC.

2. **L2VlanNetwork**

- You must specify the host NIC name and VLAN ID.
- The hosts in the cluster to which the L2 network is attached must have NICs that share the same name.
- When the data packets of VM instances flow out of the host NIC and reach the physical switch, the data packets are tagged with the specified VLAN ID.
- If you create an L2 network of the L2VlanNetwork type, a VLAN device is created based on the specified VLAN ID and then a network bridge is created based on the VLAN device.
- If you attach an L2 network of the L2NoVlanNetwork type and an L2 network of the L2VlanNetwork type or attach multiple L2 networks of the L2VlanNetwork type to a cluster , the physical switch NIC must be in Trunk mode. Besides, the VLAN ID in use must be contained in the Trunk VLAN configurations.

3. **VxlanNetwork**

- Virtual Extensible LAN (VXLAN) is an overlay technology that allows for the creation of overlaying L2 networks. This technology can support a maximum of 16 million logical networks.
- VxlanNetwork is an implementation of the software-based VXLAN technology.
- If you create an L2 network of the VxlanNetwork type, you must specify a software SDN-based VXLAN pool. The L2 network must correspond to a VNI in the pool.
- The VTEP IPs of the hosts in the cluster to which the L2 network of the VxlanNetwork type is attached must belong to the specified VXLAN pool.
- When the data packets of VM instances flow out of the host, the host encapsulates VXLAN messages to the data packets and then sends the encapsulated data to the physical switch.

4. **HardwareVxlanNetwork**

- Virtual Extensible LAN (VXLAN) is an overlay technology that allows for the creation of overlaying L2 networks. This technology can support a maximum of 16 million logical networks.
- HardwareVxlanNetwork is a solution to the integration with third-party hardware SDN.

- If you create an L2 network of the HardwareVxlanNetwork type, you must specify a hardware SDN-based VXLAN pool. The L2 network must correspond to a VNI in the pool.
- When the data packets of VM instances flow out of the host NICs and reach the distributed virtual switches, the data packets are flagged with the specified VLAN ID. The VLAN ID is mapped with VXLAN ID based on the SDN controlled that you add to the Cloud.

Note:

- In CentOS 7, the NIC name in the ethX format will be changed after the system reboots. In addition, the NIC sequence will also be randomly changed. We recommend that you change the NIC name of each compute node (especially for VM instances with multiple NICs) to a non-ethX format, such as em01.

L2 Network | Cluster | L3 Network | VM Instance

The relationship between an L2 network and a cluster, an L3 network, a VM instance is as follows:

- If you attached an L2 network to a cluster whereas the L2 network was not attached to a host, you could not add the host to the cluster.
- If you did not attach an L2 network to a cluster and the L2 network was not attached to a host, you could not attach the L2 network to the cluster.
- If you attached an L2 network to a host whereas the corresponding L2 network devices were inconsistently connected to other hosts in a cluster, note that the VM IP that you created would not work properly.
- If you delete an L2 network, the corresponding L3 networks and VM NICs that are using these networks will also be deleted.
- If you delete an L2 network, the VPC vRouter and vRouter offering that use the L2 network will also be deleted.
- If you delete an L2 public network, all network services that are using the network, such as VPC vRouter, vRouter offering, VIP, EIP, port forwarding, load balancing, IPsec tunnel, and Netflow will also be deleted.
- You can create multiple L2 networks of the VxlanNetworks type by using a VXLAN Pool of the Software SDN type. These L2 networks can be applied to flat networks and VPC networks, respectively.
- VM instances in an L2 network of the VxlanNetwork type cannot be accessed through the Internet. To access these VM instances through the Internet, use an EIP or port forwarding.

- You can also create multiple L2 networks of the HardwareVxlanNetworks type by using a VXLAN Pool of the Hardware SDN type. These L2 networks can currently be applied to flat networks.
- If you use a vSwitch of the OVS-DPDK type for an L2 network, you can use the L2 network to create only IPv4 VPC networks and provide corresponding network services.

7.3.1.2 Create an L2 Network

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **L2 Network Resources** > **L2 Network**. On the **L2 Network** page, click **Create L2 Network**. Then, the **Create L2 Network** page is displayed.

The following lists the L2 networks that you can create:

- Create an L2NoVlanNetwork.
- Create a VxlanNetwork.
- Create an L2VlanNetwork.
- Create a HardwareVxlanNetwork.

Create an L2NoVlanNetwork

Set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the L2 network.

  The L2 network name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the L2 network.
- **Type**: Select L2NoVlanNetwork.
- **vSwitch Type**: The vSwitch type of the L2 network, including Linux Bridge and OVS-DPDK.
  - If you select **Linux Bridge**, you can choose whether to enable SR-IOV.
    - By default, SR-IOV is disabled. If you disable SR-IOV for an L2 network, this feature is disabled for the L3 network created from this L2 network.
    - If you enable SR-IOV for an L2 network, this feature is enabled for the L3 network created from this L2 network.

- Before you enable SR-IOV, make sure that VF NICs are generated from the physical NICs used by the L2 network.

— If you select **OVS-DPDK**, the SR-IOV option is not displayed.

Note:

- Linux Bridge vSwitches support all types of L2 networks and SR-IOV.
- OVS-DPDK vSwitches support only L2 networks of the L2VlanNetwork and L2NOVlanNetwork types and do not support SR-IOV.
- OVS-DPDK vSwitches occupy 4 GB huge pages of each host in a cluster. If you create a vSwitch of the OVS-DPDK type and attach the vSwitch to a cluster, make sure that the memory of the hosts in the cluster is sufficient.

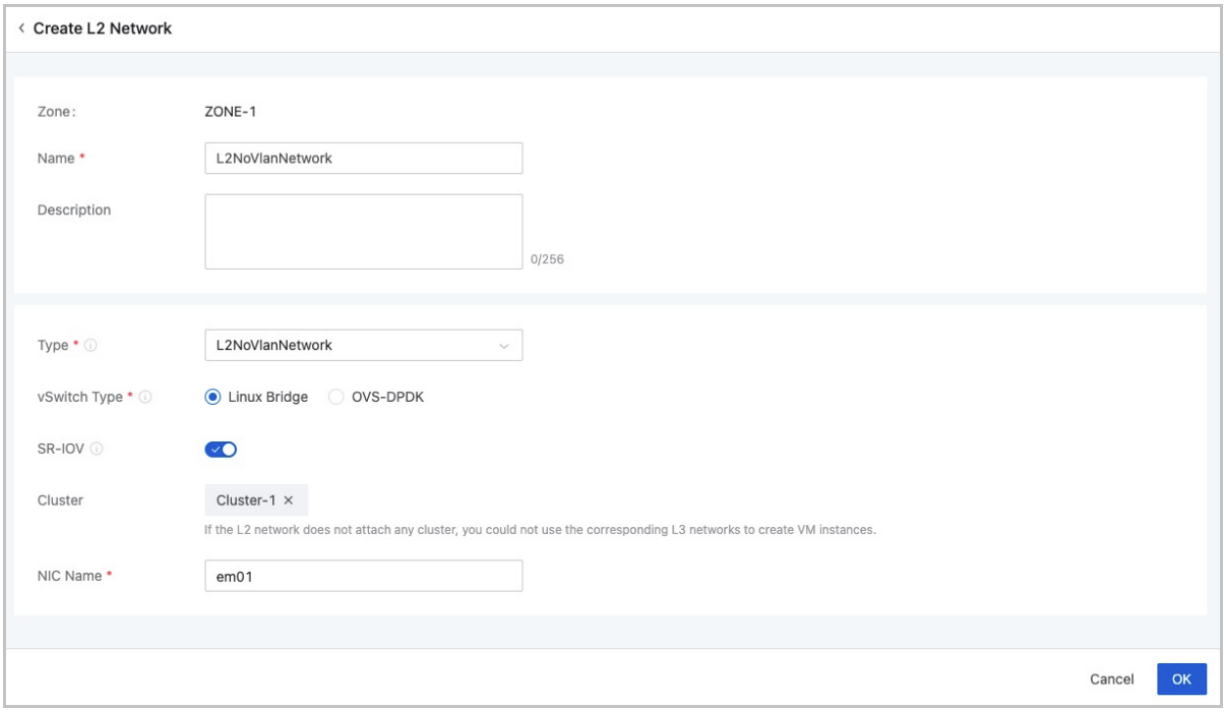
- **Cluster**: Optional. Select the cluster to be attached.

Note:

- You can attach a cluster when you create an L2NoVlanNetwork or after you create the L2 network.
- If an L2 network is not attached to a cluster, you cannot use the L2 network to create VM instances.

- **NIC Name**: Enter a NIC name for the L2 network. For example, em01.

Figure 7-59: Create L2NoVlanNetwork



Create an L2VlanNetwork

Set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the L2 network.

  The L2 network name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the L2 network.
- **Type**: Select L2VlanNetwork.
- **vSwitch Type**: The vSwitch type of the L2 network, including Linux Bridge and OVS-DPDK.

  — If you select **Linux Bridge**, set the following parameters:

  - **VLAN ID**: Specify a VLAN ID that matches the actual network configurations. Valid values: 1 to 4094.
  - **SR-IOV**: Optional. Choose whether to enable SR-IOV.
    - By default, SR-IOV is disabled. If you disable SR-IOV for an L2 network, this feature is disabled for the L3 network created from this L2 network.

- If you enable SR-IOV for an L2 network, this feature is enabled for the L3 network created from this L2 network.
- Before you enable SR-IOV, make sure that VF NICs are generated from the physical NICs used by the L2 network.

— If you select **OVS-DPDK**, set the following parameters:

- **VLAN ID**: Specify a VLAN ID that matches the actual network configurations. Valid values: 1 to 4094.

Note:

- Linux Bridge vSwitches support all types of L2 networks and SR-IOV.
- OVS-DPDK vSwitches support only L2 networks of the L2VlanNetwork and L2NOVlanNetwork types and do not support SR-IOV.
- OVS-DPDK vSwitches occupy 4 GB huge pages of each host in a cluster. If you create a vSwitch of the OVS-DPDK type and attach the vSwitch to a cluster, make sure that the memory of the hosts in the cluster is sufficient.

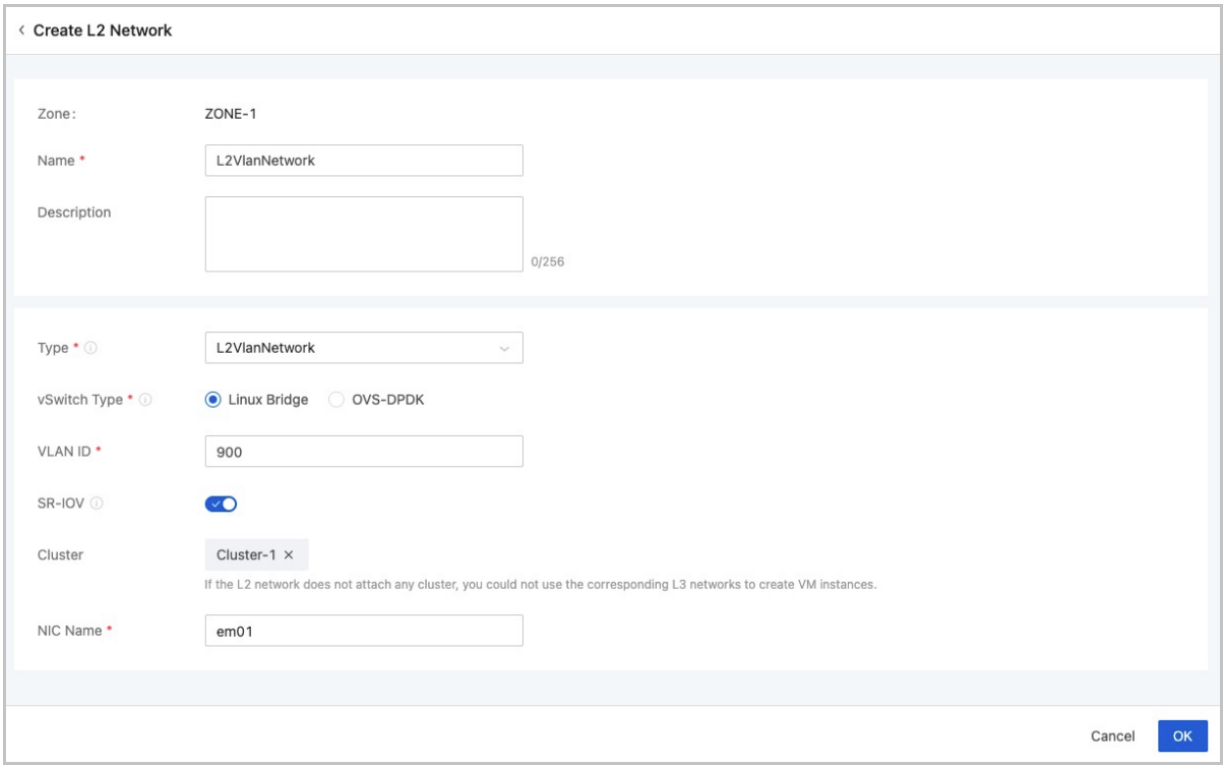
- **Cluster**: Optional. Select the cluster to be attached.

Note:

- You can attach a cluster when you create an L2NoVlanNetwork or after you create the L2 network.
- If an L2 network is not attached to a cluster, you cannot use the L2 network to create VM instances.

- **NIC Name**: Enter a NIC name for the L2 network. For example, em01.

Figure 7-60: Create L2VlanNetwork



Create a VxlanNetwork

Set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the L2 network.

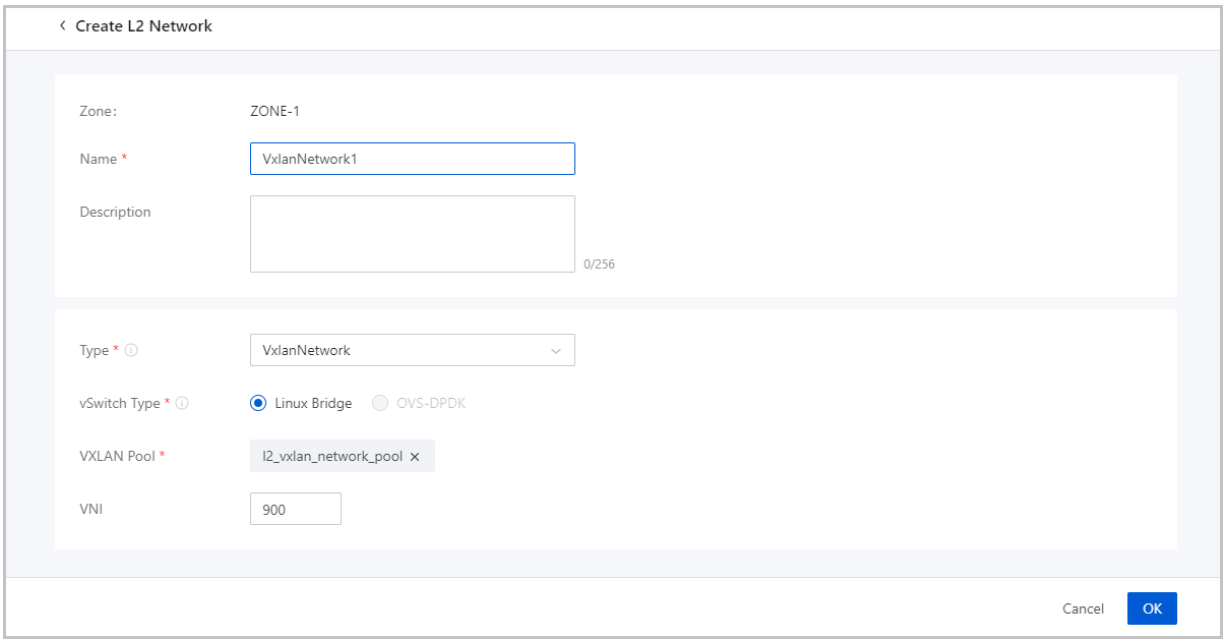
  The L2 network name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the L2 network.
- **Type**: Select VxlanNetwork.
- **vSwitch Type**: The vSwitch type of the L2 network. Only Linux Bridge is supported.
- **VXLAN Pool**: Select a VXLAN pool of the software SDN type.

  Note:

  - Before you can create a VxlanNetwork, create a VXLAN pool of the software SDN type.
  - For more information, see *Create Software-SDN VXLAN Pool*.
- **VNI**: Optional. Select a specified VNI in the VXLAN pool.

If not specified, the Cloud allocates a VNI randomly.

Figure 7-61: Create VxlanNetwork



Create a HardwareVxlanNetwork

Set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the L2 network.

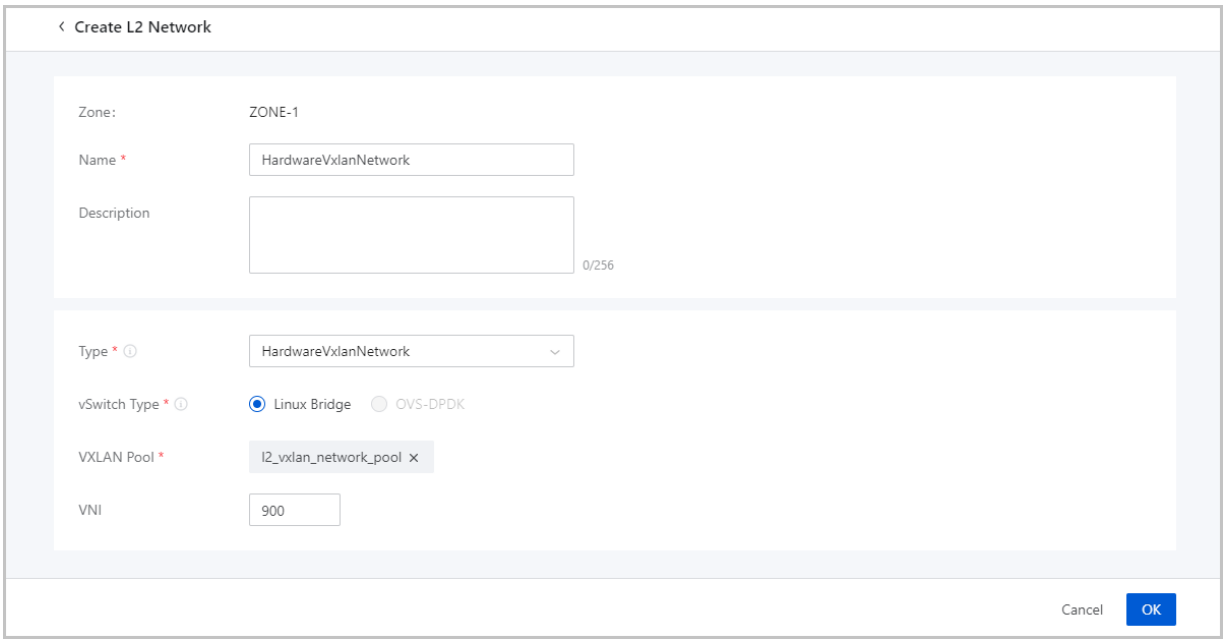
  The L2 network name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the L2 network.
- **Type**: Select HardwareVxlanNetwork.
- **vSwitch Type**: The vSwitch type of the L2 network. Only Linux Bridge is supported.
- **VXLAN Pool**: Select a VXLAN pool of the hardware SDN type.

  Note:

  - Before you can create a HardwareVxlanNetwork, create a VXLAN pool of the hardware SDN type.
  - For more information, see *Create Hardware-SDN VXLAN Pool*.
- **VNI**: Optional. Select a specified VNI in the VXLAN pool.

If not specified, the Cloud allocates a VNI randomly.

Figure 7-62: Create HardwareVxlanNetwork



7.3.1.3 Manage an L2 Network

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **L2 Network Resources** > **L2 Network**. Then, the **L2 Network** page is displayed. The following tables list the actions that you can perform on an L2 network.

Table 7-7: L2NoVlanNetwork/L2VlanNetwork Actions

Action	Description
Create L2 Network	Create an L2NoVlanNetwork or L2VlanNetwork network.
Edit L2 Network	Edit the name and description of the L2 network.
Attach Cluster	Attach the L2 network to a cluster.
Detach Cluster	Detach the L2 network from a cluster. **Note:** Detaching an L2 network from a cluster also detaches the corresponding VM NIC. Please exercise caution.
Set Sharing Mode	Set the sharing mode of the resource. The platform provides the following sharing modes: • Share Globally: shares the resource with all projects and accounts.

Action	Description
	• Share to Specified Projects/Accounts: shares the resource with specified projects and accounts. • Not Share: revokes the resource from projects and accounts to which the resource is shared. If you set Sharing Mode to Not Share for the resource, other projects and accounts cannot use the resource. **Note:** • If you modify the Sharing Mode setting of the resource from Share Globally to Share to Specified Projects/Accounts, the resource is visible only to the specified projects or accounts to which the resource is shared. • If the resource that you share with projects or accounts was used by the projects or accounts and then you modify the Sharing Mode setting of the resource, the resource is reserved for the projects or accounts until it is released.
Delete L2 Network	Delete the L2 network. **Note:** Deleting an L2 network also deletes its L3 networks and associated VPC vRouters, and detaches the corresponding VM NIC. Please exercise caution.

Table 7-8: VxlanNetwork Actions

Action	Description
Create L2 Network	Create a VxlanNetwork network.
Edit L2 Network	Edit the name and description of the L2 network.
Set Sharing Mode	Set the sharing mode of the resource. The platform provides the following sharing modes: • Share Globally: shares the resource with all projects and accounts. • Share to Specified Projects/Accounts: shares the resource with specified projects and accounts. • Not Share: revokes the resource from projects and accounts to which the resource is shared. If you set Sharing Mode to Not Share for the resource, other projects and accounts cannot use the resource.

Action	Description
	Note: • If you modify the Sharing Mode setting of the resource from Share Globally to Share to Specified Projects/Accounts, the resource is visible only to the specified projects or accounts to which the resource is shared. • If the resource that you share with projects or accounts was used by the projects or accounts and then you modify the Sharing Mode setting of the resource, the resource is reserved for the projects or accounts until it is released.
Delete L2 Network	Delete the L2 network. **Note:** Deleting an L2 network also deletes its L3 networks and associated VPC vRouters, and detaches the corresponding VM NIC. Please exercise caution.

Table 7-9: HardwareVxlanNetwork Actions

Action	Description
Create L2 Network	Create HardwareVxlanNetwork network.
Edit L2 Network	Edit the name and description of the L2 network.
Delete L2 Network	Delete the L2 network. **Note:** Deleting an L2 network also deletes its L3 networks and associated VPC vRouters, and detaches the corresponding VM NIC. Please exercise caution.

7.3.2 VXLAN Pool

7.3.2.1 What is VXLAN Pool?

VXLAN Pool: A VXLAN pool is a collection of VXLAN networks established based on VXLAN Tunnel Endpoints (VTEPs). The VNI of each VXLAN network in a VXLAN pool must be unique.

- Before you can use a VXLAN network, create a VXLAN pool in advance.
- A VXLAN pool is only a collection of VXLAN networks and cannot be used to create L3 networks.

- VXLAN pool supports two types of SDN: software SDN and hardware SDN.
  - Software SDN:
    - The VNI range of a software-SDN VXLAN pool can be 1-16777214.
    - Hosts in the cluster to which the software-SDN VXLAN pool is attached must have an IP address as a VXLAN tunnel endpoint (VTEP) in the specified CIDR.
      - Generally, a VTEP corresponds to a NIC IP of a compute node within a cluster. On the Cloud, you can configure a VTEP according to its CIDR. For example,
        - Assume that the NIC IP of a compute node is *10.12.0.8*, the netmask is *255.0.0.0*, and the gateway is *10.0.0.1*. Then, the CIDR of the VTEP is *10.0.0.1/8*.
        - Assume that the NIC IP of the compute node is *172.20.12.13*, the netmask is *255.255.0.0*, and the gateway is *172.20.0.1*. Then, the CIDR of the VTEP is *172.20.0.1/16*.
      - When a VXLAN pool is attached to a cluster, the IP address that is associated to the VTEP will be checked without checking physical L2 devices.
  - Hardware SDN:
    - Before you can create a hardware-SDN VXLAN pool, add an SDN controller to the Cloud in advance.
    - The VNI range of a hardware-SDN VXLAN pool depends on the distributed vSwitch to which an SDN controller corresponds.
    - The host NIC in the cluster to which the hardware-SDN VXLAN pool is attached must connect to a switch managed by the SDN controller.
    - If you use VCFC to configure hardware SDN, configure the mapping between VLAN and VXLAN on VCFC in advance.

7.3.2.2 Create a VXLAN Pool

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **L2 Network Resources** > **VXLAN Pool**. On the **VXLAN Pool** page, click **Create VXLAN Pool**. Then, the **Create VXLAN Pool** page is displayed.

The following lists two types of VXLAN pools that you can create:

- Create a software-SDN VXLAN pool
- Create a hardware-SDN VXLAN pool

Create Software-SDN VXLAN Pool

On the displayed page, set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the VXLAN pool.

  The name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the VXLAN pool.
- **SDN Type**: Select Software.
- **VNI Range**: Enter the start ID and end ID of VXLAN networks.

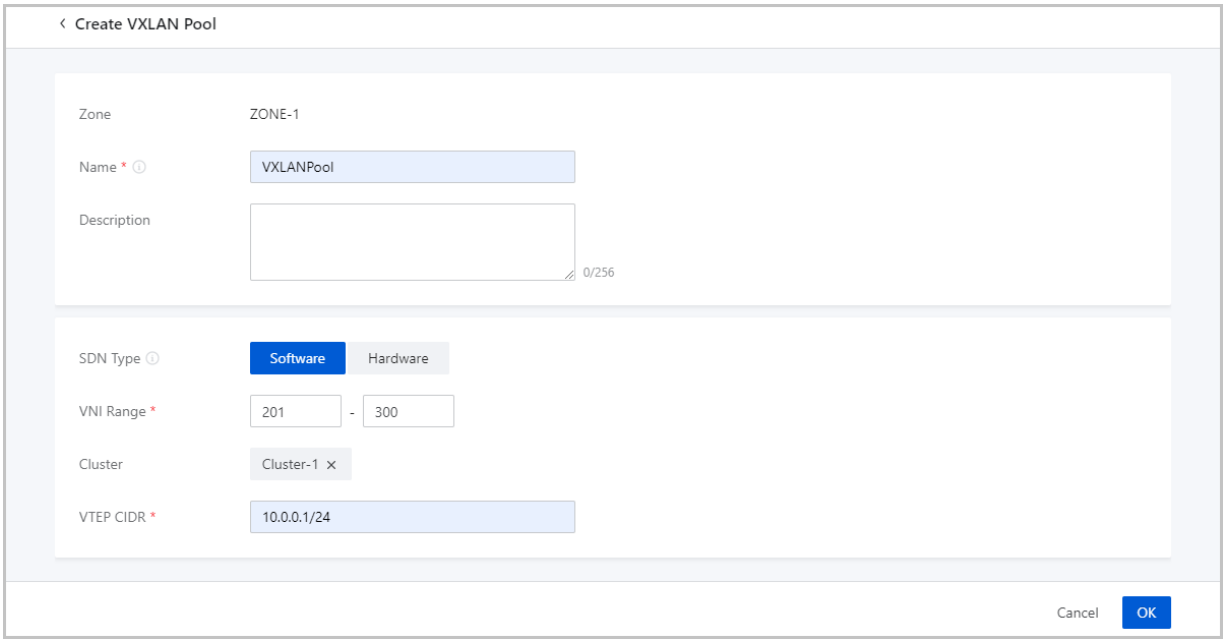
  Note:

  - You can enter an ID that ranges from 1 to 16777214.
  - The end ID must be equal to or greater than the start ID.
  - The two VNI IDs 16777215 and 16777216 are reserved by the system of this cloud platform.
- **Cluster**: Optional. Attach the VXLAN pool to a cluster.

  Note:

  - You can attach a VXLAN pool to a cluster when you create the VXLAN pool or after the VXLAN pool is created.
  - When you attach the VXLAN pool to a cluster, IP addresses of the compute nodes must be available in the cluster that correspond to the VTEP CIDR block.
- **VTEP CIDR**: Enter the corresponding VTEP CIDR block.

Figure 7-63: Create Software-SDN VXLAN Pool



Create Hardware-SDN VXLAN Pool

On the displayed page, set the following parameters:

- **Zone**: By default, the current zone is displayed.
- **Name**: Enter a name for the VXLAN pool.

  The name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the VXLAN pool.
- **SDN Type**: Select Hardware.
- **SDN Controller**: Select an SDN controller.

  Note:

  You need add an SDN controller to the cloud platform in advance.
- **VNI Range**: Enter the start ID and end ID of hardware-based VXLAN networks.

  Note:

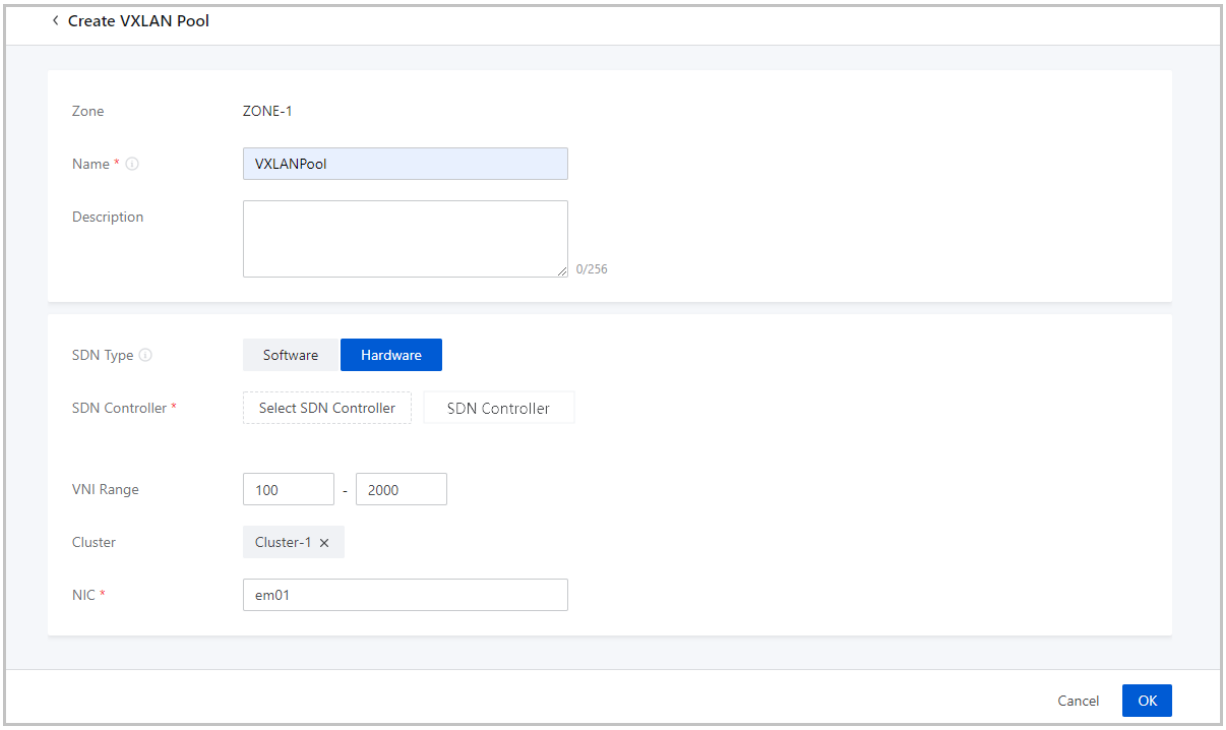
  - The end ID must be equal to or greater than the start ID.
  - The VNI range of a hardware-SDN VXLAN pool varies depending on the virtual distributed switches associated with the SDN controller.
- **Cluster**: Optional. Attach the VXLAN pool to a cluster.

> **Note:**
> You can attach a cluster to a VXLAN pool when you create the VXLAN pool or after the VXLAN pool is created.

- **NIC**: Enter a host NIC.

> **Note:**
> The host NICs in the cluster attached to the VXLAN pool must be connected with the switches managed by the SDN controller.

Figure 7-64: Create Hardware-SDN VXLAN Pool



7.3.2.3 Manage a VXLAN Pool

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **L2 Network Resources** > **VXLAN Pool**. Then, the **VXLAN Pool** page is displayed.

The following table lists the actions that you can perform on a VXLAN pool.

Action	Description
Create VXLAN Pool	Create a VXLAN pool.
Edit VXLAN Pool	Edit the name and description of the VXLAN pool.

Action	Description
Attach Cluster	Attach the VXLAN pool to a cluster. • Software-SDN VXLAN Pool: You need to specify a VTEP CIDR. Make sure that the hosts in the cluster attached to the software-SDN VXLAN pool have an IP address as the VTEP in the specified CIDR. • Hardware-SDN VXLAN Pool: The host NICs in the cluster attached to the VXLAN pool must be connected with the switches managed by the SDN controller.
Detach Cluster	Detach the VXLAN pool from a cluster.
Set Sharing Mode	Set the sharing mode of the resource. The platform provides the following sharing modes: • Share Globally: shares the resource with all projects and accounts. • Share to Specified Projects/Accounts: shares the resource with specified projects and accounts. • Not Share: revokes the resource from projects and accounts to which the resource is shared. If you set Sharing Mode to Not Share for the resource, other projects and accounts cannot use the resource. **Note:** • If you modify the Sharing Mode setting of the resource from Share Globally to Share to Specified Projects/Accounts, the resource is visible only to the specified projects or accounts to which the resource is shared. • If the resource that you share with projects or accounts was used by the projects or accounts and then you modify the Sharing Mode setting of the resource, the resource is reserved for the projects or accounts until it is released. VXLAN pools created by using hardware SDNs cannot be shared.
Delete VXLAN Pool	Deleting a VXLAN pool also deletes the VXLAN networks in the pool and the associated L3 networks and VM NICs. Proceed with caution.

7.3.3 L3 Network

An L3 network is a collection of network configurations for VM instances, including the network range, gateway, DNS, and network services.

- A network range includes an IP range (start IP and end IP), netmask, and gateway. For example, you can specify the IP range from *172.20.12.2* to *172.20.12.255*, set the netmask to

255.255.0.0, and set the gateway to *172.20.0.1*. In addition, you can use a CIDR to specify a network range, such as *192.168.1.0/24*.

- DNS provides DNS resolution services used for configuring VM networks.

Concepts

- Public network: Generally, a public network is a logical network that is connected to the Internet . However, in an environment that has no access to the Internet, you can also create a public network.
  - A public network can be used in the flat network environment to create VM instances.
  - A public network can be used in the VPC network environment to create VM instances that work with public networks.
- Flat network: A flat network is connected to the network where the host is located and has direct access to the Internet. VM instances in a flat network can access public networks by using elastic IP addresses.
  - A flat network supports multiple network services, including DHCP, User Data, EIP, security group, and port mirroring.
  - The network services provided by a flat network use the distributed DHCP and the distribute d EIP structure.
  - The DHCP service provided by a flat network also includes the DNS feature.
  - The network model used in the wizard is a flat network.
  - The flat network architecture based on VxlanNetwork or HardwareVxlanNetwork is supported.
- VPC network: A VPC network is a private network where VM instances can be created. A VM instance in a VPC network can access the Internet through a VPC vRouter.
  - A VPC network provides the following network services: DHCP, User Data, DNS, SNAT , route table, EIP, port forwarding, load balancing, IPsec tunnel, security group, dynamic routing, multicast routing, VPC firewall, port mirroring, and netflow.
  - The DHCP service of the VPC network uses DHCP by default.
  - VPC networks mainly use custom Linux VM instances as VPC vRouters to provide network services.
  - Network services can act on multiple subnets of a VPC at the same time, further improving network efficiencies.
  - Supports VxlanNetwork-based VPC network architecture.

- Supports distributed routing, optimizing east-west network traffic and effectively reducing network latency.

- Dedicated network:
  - Management network: A management network is used to manage physical resources in the Cloud. For example, you can create a management network to manage access to hosts, primary storages, backup storages, and VPC vRouters.

    Note:
    When you create a VPC vRouter, you need an IP address that can be interconnected between the management nodes of the VPC vRouter. With this IP address, you can deploy an agent and obtain messages returned by the agent.
  - Flow network: A flow network is a dedicated network for port mirror transmission. You can use a flow network to transmit the mirrors of data packets of NIC ports to the target ports. A flow network cannot be used for other purposes, such as creating VM instances.
- Specific network scenarios:
  - Storage network: A storage network is the network specified by the shared storage. You can use a storage network to check the health state of a VM instance. We recommend that you plan for an independent storage network in advance to avoid potential risks.
  - VDI network: When you create a cluster, you can specify CIDR for the VDI network in the cluster. In the VDI scenario, the network traffics generated by the protocol communicat ion between the server side and client side use the VDI network. If you do not make any configuration to the VDI network, notice that the management network will be used by default.
  - Migration network: When you create a cluster, you can specify CIDR for the migration network in the cluster. The migration network is used to migrate VM instances in the Cloud. If you do not make any configuration to the migration network, notice that the management network will be used for VM migrations.
  - Image synchronization network: An image synchronization network is used to synchronize images among ImageStore backup storages in the same management node.
    - If you deployed an independent network for synchronizing images, you can specify CIDR for the image synchronization network when you add an ImageStore backup storage.
    - If you do not make any configuration to the image synchronization network, notice that the management network will be used by default.

  - If you set an image synchronization network for both the source ImageStore backup storage and target one, only the image synchronization network in the target ImageStore backup storage takes effect.
- Data network: A data network is the network where data can transfer between a compute node and a backup storage.
  - Using an independent data network can avoid network congestion and improve the data transfer rate.
  - If you do not make any configuration to the data network, notice that the management network will be used by default.
- Backup network: If you are using the Backup Service or the Continuous Data Protection (CDP) service, in the local backup scenario,both the data backup and recovery are implemented by using the backup network.
  - If you deploy an independent network for local backups, you can specify CIDR for the backup network when you add a local backup server.
  - Using an independent backup network can avoid network congestion and improve the data transfer rate.
  - If you do not make any configuration to the backup network, notice that the management network will be used for local backup by default.

Note:

The Backup Service and the CDP Service are separately provided in a separate module . To use this feature, purchase both the Base License and the Plus License. Note that a Base License is required before you can install a Plus License.

Considerations

- When you create a VM instance, you can specify multiple L3 networks, including flat networks, VPC networks, or a combination of flat networks and VPC networks.
- The Cloud supports multi-layer networks. In addition, the L2 networks of multi-layer networks can intercommunicate. Therefore, you need to pay a special attention to avoid the conflict of IP address spaces.
- You can create multiple L3 networks by using an L2 network, which is not recommended.
- The network services and features supported by an L3 network are related to the network architecture model (flat network, VPC network) and the configured network protocol version

(IPv4, IPv6). If a network is configured with both IPv4 and IPv6 protocols, servers of these two protocol types are loaded at the same time to provide corresponding services.

	IPv4	IPv6
Flat network	Supported network services: DHCP , User Data, EIP, security group, and port mirroring	Supported network services: DHCP , DNS, EIP, and security group
VPC network	Supported network services: DHCP , User Data, DNS, SNAT, route table, EIP, port forwarding, load balancing, IPsec tunnel, security group, dynamic routing, multicast routing, VPC firewall, port mirroring, and Netflow	Supported network services: DHCP , DNS, and security group
	Supported network service: VPC vRouter HA group	Supported network service: VPC vRouter HA group

- If you use an L2 network of the HardwareVxlanNetwork type, the L3 network created from the L2 network supports only flat network and corresponding network services.
- If you use a vSwitch of the OVS-DPDK type for an L2 network, you can use the L2 network to create only IPv4 VPC networks and provide corresponding network services (excluding security group and port mirroring services).

7.3.3.1 Public Network

7.3.3.1.1 Create a Public Network

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **L3 Network Resources** > **Public Network**. On the **Public Network** page, click **Create Public Network**. The **Create Public Network** page appears.

The following lists the two public network creation scenarios:

- Create an IPv4 public network
- Create an IPv6 public network

Create IPv4 Public Network

On the displayed page, set the following parameters:

- **Name**: Enter a name for the public network.
- **Description**: Optional. Enter a description for the public network.

- **L2 Network**: Select an L2 network for the public network.

  Note:
  ZStack Cloud allows you to use an L2 network to create multiple L3 networks. However, we recommend that you do not use an L2 network to create multiple L3 networks if not for specific business needs.

  On the **Select L2 Network** pane, two tabs are displayed:

  - **Recommended**: lists L2 networks in the current zone that are not attached to an L3 network.
  - **All**: lists all L2 networks in the current zone.
- **Network Address Type**: Select IPv4.
- **Network Range Method**: Select a method to add a network range for the public network. You can select IP Range or CIDR.

  If you select **IP Range**, you need to set the following parameters:

  - **Start IP**: Set a start IP address for the network range, for example, *172.20.108.100*.
  - **End IP**: Set an end IP address for the network range, for example, *172.20.108.200*.
  - **Netmask**: Set a netmask for the network range, for example, *255.255.0.0*.
  - **Gateway**: Set a gateway for the network range, for example, *172.20.0.1*.
  - **DHCP Service**: Choose whether to enable the DHCP service.

    Note:
    - The DHCP service is enabled by default. This service automatically assigns an IP address to a VM instance. You can specify an IP address for the DHCP server. If you do not specify, the system assigns a random IP address for the DHCP server.
    - If you disable the DHCP service, no IP address is automatically assigned to VM instances in the public network. You need to manually configure IP addresses for the VM instances.

    — **DHCP IP**: Optional. Set an IP address for the DHCP server, for example, *172.20.108.10*.

    Note:

- When you create an L3 network and enable the DHCP service for the first time, or when you add the first network range for an L3 network that has the DHCP service enabled, you can specify an IP address for the DHCP server.
- If a DHCP IP is specified for an L3 network, you cannot specify another DHCP IP when you add a network range for the network.
- The DHCP IP can be within or out of the added IP range. However, the IP address must be within the CIDR block to which the added IP range belongs and must not be in use.
- The IP range determined by the start IP and end IP cannot contain the link-local address 169.254.0.0/16.
- If left blank, the system assigns a random IP address for the DHCP server.

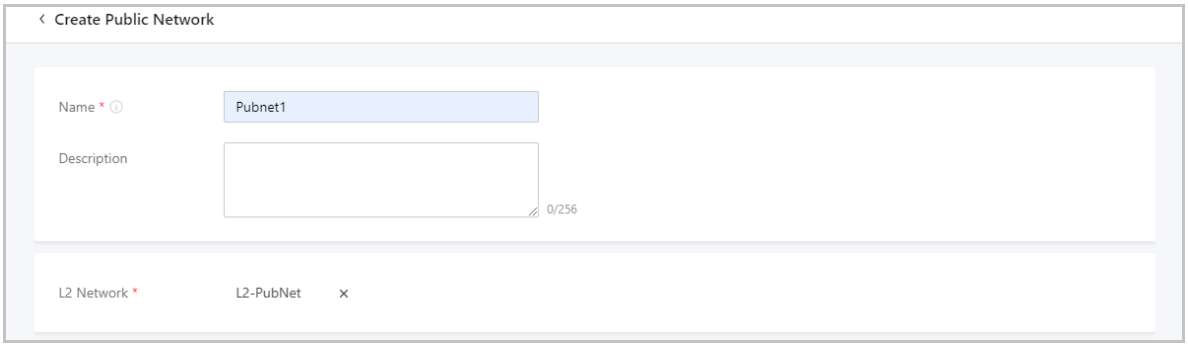
- **DNS**: Add a DNS server to provide domain name resolution services for the public network. You can specify *223.5.5.5*, *8.8.8.8*, or *114.114.114.114*.

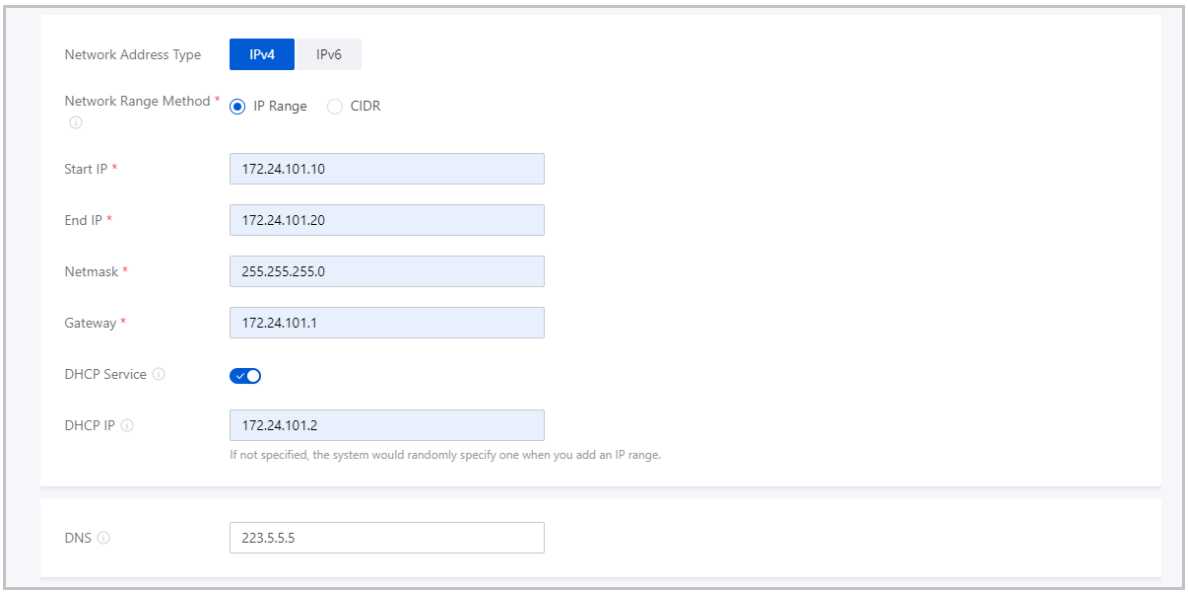
Note:

When you add an IP range for an IPv4 L3 network, note that:

- The IP range cannot contain gateway IP addresses in the format of *xxx.xxx.xxx.1*, broadcast addresses in the format of *xxx.xxx.xxx.255*, or network addresses in the format of *xxx.xxx.xxx.0*.
- The IP range of a private network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-65: Create IPv4 Public Network Using IP Range





If you select **CIDR**, you need to set the following parameters:

- **CIDR**: Set a CIDR block for the public network, for example, *192.168.108.1/24*.
- **Gateway**: Set a gateway for the public network, for example, *192.168.108.1*.

Note:

- You can use the first or last IP address in the specified CIDR block as the gateway.
- If left blank, the first IP address in the specified CIDR block is used as the gateway.

- **DHCP Service**: Choose whether to enable the DHCP service.

Note:

- The DHCP service is enabled by default. This service automatically assigns an IP address to a VM instance. You can specify an IP address for the DHCP server. If you do not specify, the system assigns a random IP address for the DHCP server.
- If you disable the DHCP service, no IP address is automatically assigned to VM instances in the public network. You need to manually configure IP addresses for the VM instances.

— **DHCP IP**: Optional. Set an IP address for the DHCP server, for example, *192.168.108.10*.

Note:

- When you create an L3 network and enable the DHCP service for the first time, or when you add the first network range for an L3 network that has the DHCP service enabled, you can specify an IP address for the DHCP server.
- If a DHCP IP is specified for an L3 network, you cannot specify another DHCP IP when you add a network range for the network.
- The DHCP IP must be within the CIDR block and must not be in use.
- If left blank, the system assigns a random IP address for the DHCP server.
- The first IP address in the CIDR block is predefined as the default gateway and cannot be used as a DHCP server IP.

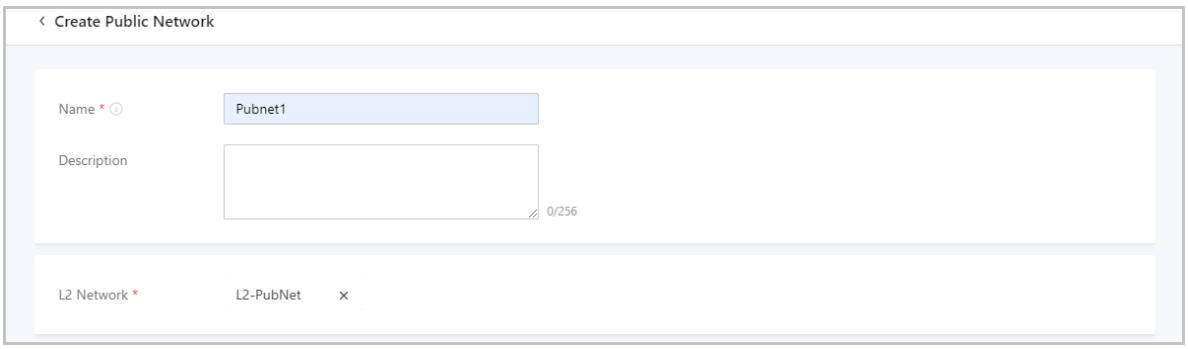
- **DNS**: Add a DNS server to provide domain name resolution services for the public network. You can specify *223.5.5.5*, *8.8.8.8*, or *114.114.114.114*.

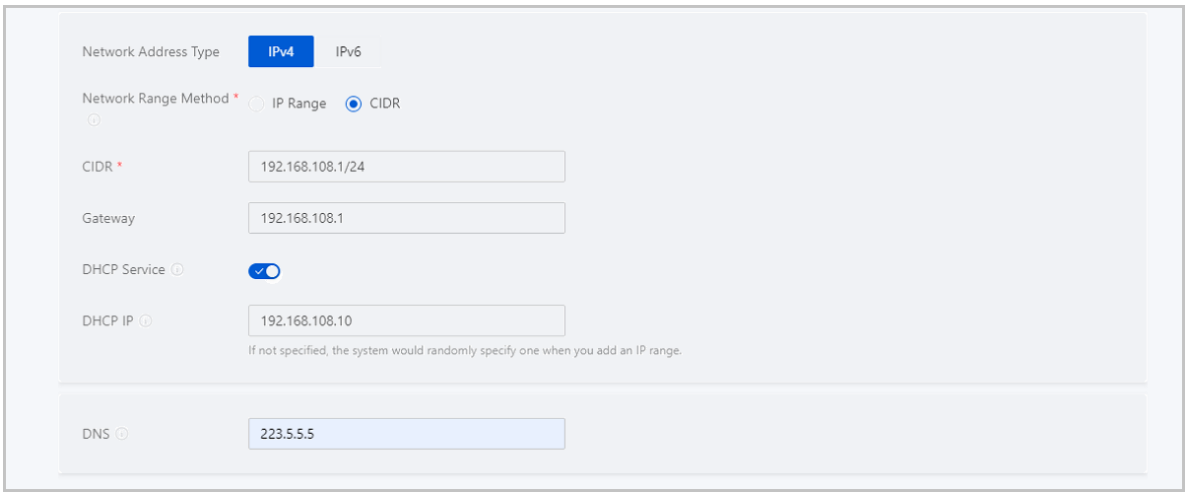
Note:

When you add a CIDR block for an IPv4 L3 network, note that:

- The CIDR block cannot contain the link-local address 169.254.0.0/16.
- The CIDR block of a private network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-66: Create IPv4 Public Network Using CIDR Block





Create IPv6 Public Network

On the displayed page, set the following parameters:

- **Name**: Enter a name for the public network.
- **Description**: Optional. Enter a description for the public network.
- **L2 Network**: Select an L2 network for the public network.

  > **Note:**
  > ZStack Cloud allows you to use an L2 network to create multiple L3 networks. However, we recommend that you do not use an L2 network to create multiple L3 networks if not for specific business needs.

  On the **Select L2 Network** pane, two tabs are displayed:

  - **Recommended**: lists L2 networks in the current zone that are not attached to an L3 network.
  - **All**: lists all L2 networks in the current zone.
- **Network Address Type**: Select IPv6.
- **Network Range Method**: Select a method to add a network range for the public network. You can select IP Range or CIDR.

  If you select **IP Range**, you need to set the following parameters:

  - **IP Configuration Mode**: Select the IP distribution mode:
    - Stateful-DHCP: The interface address and other parameters are all configured through DHCP. The IP range method supports stateful DHCP.

- **Start IP**: Set a start IP address for the network range, for example, *2000:910A:2222:5498:8475:1111:3900:2002*.
- **End IP**: Set an end IP address for the network range, for example, *2000:910A:2222:5498:8475:1111:3900:2009*.
- **Prefix Length**: Set a prefix length for the network range, for example, 64.

  Note:

  The prefix length ranges from 64 to 126. If you set a length smaller than 64, VM creation may fail.

- **Gateway**: Set a gateway for the network range, for example, *2000:910A:2222:5498:8475:1111:3900:2001*.
- **DHCP Service**: Choose whether to enable the DHCP service.

  Note:

  - The DHCP service is enabled by default. This service automatically assigns an IP address to a VM instance. You can specify an IP address for the DHCP server. If you do not specify, the system assigns a random IP address for the DHCP server.
  - If you disable the DHCP service, no IP address is automatically assigned to VM instances in the public network. You need to manually configure IP addresses for the VM instances.

  — **DHCP IP**: Optional. Set an IP address for the DHCP server, for example, *2000:910A:2222:5498:8475:1111:3900:2006*.

  Note:

  - When you create an L3 network and enable the DHCP service for the first time, or when you add the first network range for an L3 network that has the DHCP service enabled, you can specify an IP address for the DHCP server.
  - If a DHCP IP is specified for an L3 network, you cannot specify another DHCP IP when you add a network range for the network.
  - The DHCP IP can be within or out of the added IP range. However, the IP address must be within the CIDR block to which the added IP range belongs and must not be in use.

- The IP range determined by the start IP and end IP cannot contain the link-local address fe80::/10.
- If left blank, the system assigns a random IP address for the DHCP server.

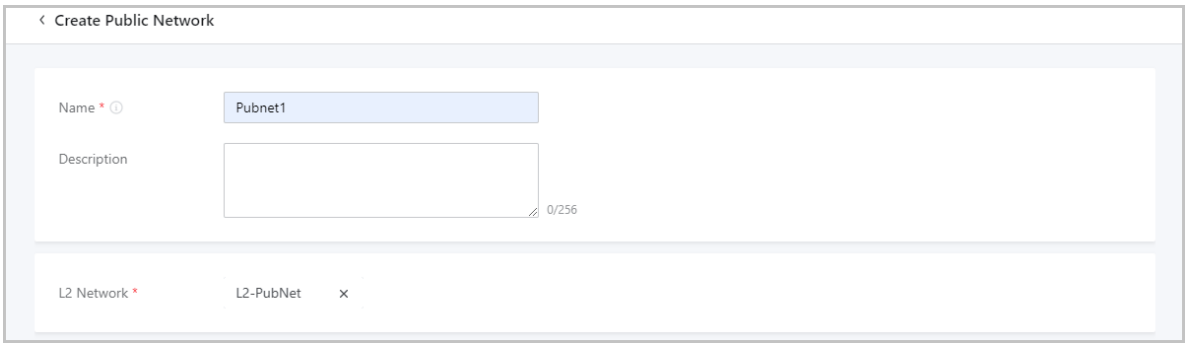
- **DNS**: Add a DNS server to provide domain name resolution services for the public network. You can specify *240C::6644* or *240C::6666*.

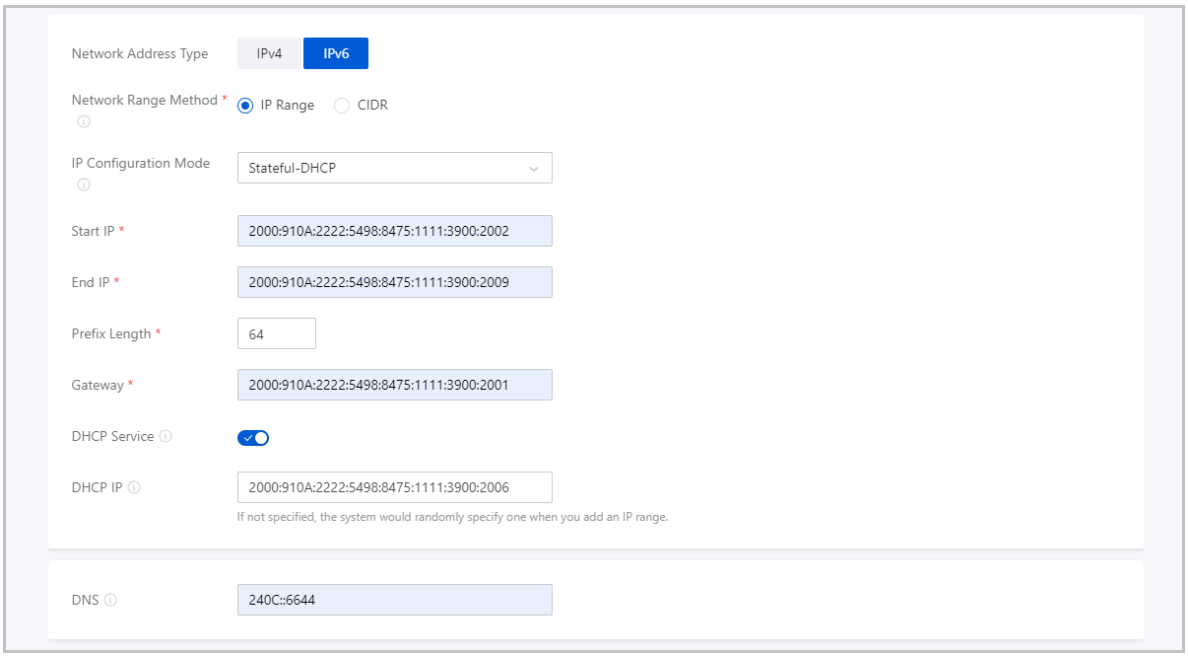
Note:

When you add an IP range for an IPv6 L3 network, note that:

- The IP range cannot contain gateway IP addresses *xxxx::1*.
- The IP range determined by the start IP and end IP cannot contain the link-local address fe80::/10.
- The IP range of a private network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-67: Create IPv6 Public Network Using IP Range





If you select **CIDR**, you need to set the following parameters:

- **IP Configuration Mode**: Select the IP distribution mode:
  - Stateful-DHCP: The interface address and other parameters are all configured through DHCP. The IP range method supports stateful DHCP.
  - Stateless-DHCP: The interface address is automatically derived from the route advertisement prefix and the interface Mac address. Other parameters are configured through DHCP.
  - SLAAC: The interface address is automatically derived from the prefix of the route advertisement that also contains other parameters.
- **CIDR**: Set a CIDR block for the public network, for example, *234E:2457:3D::/64*.
- **DHCP Service**: Choose whether to enable the DHCP service.

Note:

- The DHCP service is enabled by default. This service automatically assigns an IP address to a VM instance. You can specify an IP address for the DHCP server. If you do not specify, the system assigns a random IP address for the DHCP server.
- If you disable the DHCP service, no IP address is automatically assigned to VM instances in the public network. You need to manually configure IP addresses for the VM instances.

— **DHCP IP**: Optional. Set an IP address for the DHCP server, for example, *234E:2457:3D::F*.

Note:

- When you create an L3 network and enable the DHCP service for the first time, or when you add the first network range for an L3 network that has the DHCP service enabled, you can specify an IP address for the DHCP server.
- If a DHCP IP is specified for an L3 network, you cannot specify another DHCP IP when you add a network range for the network.
- The DHCP IP must be within the CIDR block and must not be in use.
- If left blank, the system assigns a random IP address for the DHCP server.
- The first IP address in the CIDR block is predefined as the default gateway and cannot be used as a DHCP server IP.

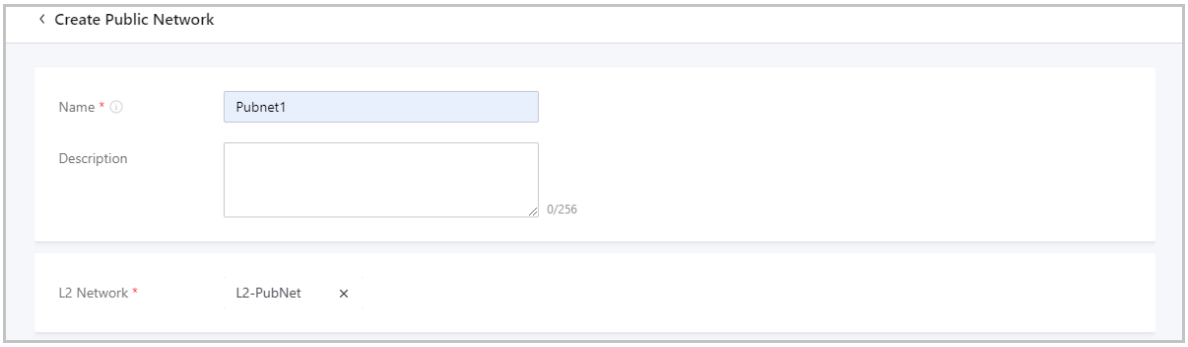
— **DNS**: Add a DNS server to provide domain name resolution services for the public network. You can specify *240C::6644* or *240C::6666*.

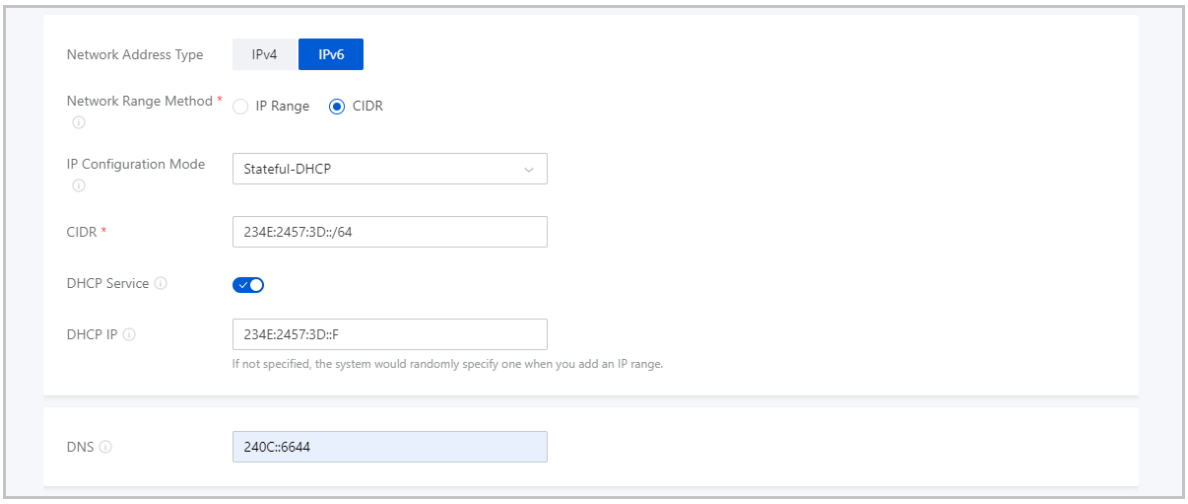
Note:

When you add a CIDR block for an IPv6 L3 network, note that:

- The first IP address in the CIDR block is used as the default gateway.
- The CIDR block cannot contain the link-local address fe80::/10.
- The IP range of a private network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-68: Create IPv6 Public Network Using CIDR Block





Considerations

Make sure that the network range of the public network is connected to the external networks. Otherwise, VPC vRouters may not work as expected.

7.3.3.1.2 Manage a Public Network

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **L3 Network Resources** > **Public Network**. The **Public Network** page appears.

The following table lists the actions that you can perform on a public network.

Action	Description
Create Public Network	Create a public network.
Add DNS	Add an IPv4 or IPv6 DNS server address: • IPv4 address: *223.5.5.5*, *8.8.8.8*, or *114.114.114.114*. • IPv6 address: *240C::6644* or *240C::6666*.
Set Sharing Mode	Set the sharing mode of a public network. The platform provides the following sharing modes: • Share Globally: shares a public network with all projects and normal accounts that have the Enterprise Management license. • Share to Specified Projects/Accounts: shares a public network with specified projects and normal accounts that have the Enterprise Management license. • Not Share: The public network is not shared with projects or normal accounts and can be used only by the admin.

Action	Description
	Note: • Modifying the sharing mode will also modify the permissions on shared public networks. • Public networks that are used by projects or accounts before a modification are not affected until the public networks are released.
Delete Public Network	Delete a public network. **Note:** Deleting a public network also detaches the VM NICs that are using this network, and removes the corresponding vRouters, network services, and vRouter offerings. Proceed with caution.

7.3.3.2 Flat Network

7.3.3.2.1 Create a Flat Network

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **L3 Network Resources** > **Flat Network**. On the **Flat Network** page, click **Create Flat Network**. The **Create Flat Network** page appears.

The following lists the two flat network creation scenarios:

- Create an IPv4 flat network
- Create an IPv6 flat network

Create IPv4 Flat Network

On the displayed page, set the following parameters:

- **Name**: Enter a name for the flat network.
- **Description**: Optional. Enter a description for the flat network.
- **L2 Network**: Select an L2 network for the flat network.

Note:
ZStack Cloud allows you to use an L2 network to create multiple L3 networks. However, we recommend that you do not use an L2 network to create multiple L3 networks if not for specific business needs.

On the **Select L2 Network** pane, two tabs are displayed:

- **Recommended**: lists L2 networks in the current zone that are not attached to an L3 network.
- **All**: lists all L2 networks in the current zone.

- **Network Address Type**: Select IPv4.
- **Network Range Method**: Select a method to add a network range for the flat network. You can select IP Range or CIDR.

  If you select **IP Range**, you need to set the following parameters:

  - **Start IP**: Set a start IP address for the network range, for example, *172.20.108.100*.
  - **End IP**: Set an end IP address for the network range, for example, *172.20.108.200*.
  - **Netmask**: Set a netmask for the network range, for example, *255.255.0.0*.
  - **Gateway**: Set a gateway for the network range, for example, *172.20.0.1*.
  - **DHCP Service**: Choose whether to enable the DHCP service.

    Note:

    - The DHCP service is enabled by default. This service automatically assigns an IP address to a VM instance. You can specify an IP address for the DHCP server. If you do not specify, the system assigns a random IP address for the DHCP server.
    - If you disable the DHCP service, no IP address is automatically assigned to VM instances in the flat network. You need to manually configure IP addresses for the VM instances.

  — **DHCP IP**: Optional. Set an IP address for the DHCP server, for example, *172.20.108.10*.

    Note:

    - When you create an L3 network and enable the DHCP service for the first time, or when you add the first network range for an L3 network that has the DHCP service enabled, you can specify an IP address for the DHCP server.
    - If a DHCP IP is specified for an L3 network, you cannot specify another DHCP IP when you add a network range for the network.
    - The DHCP IP can be within or out of the added IP range. However, the IP address must be within the CIDR block to which the added IP range belongs and must not be in use.

- The IP range determined by the start IP and end IP cannot contain the link-local address 169.254.0.0/16.
- If left blank, the system assigns a random IP address for the DHCP server.

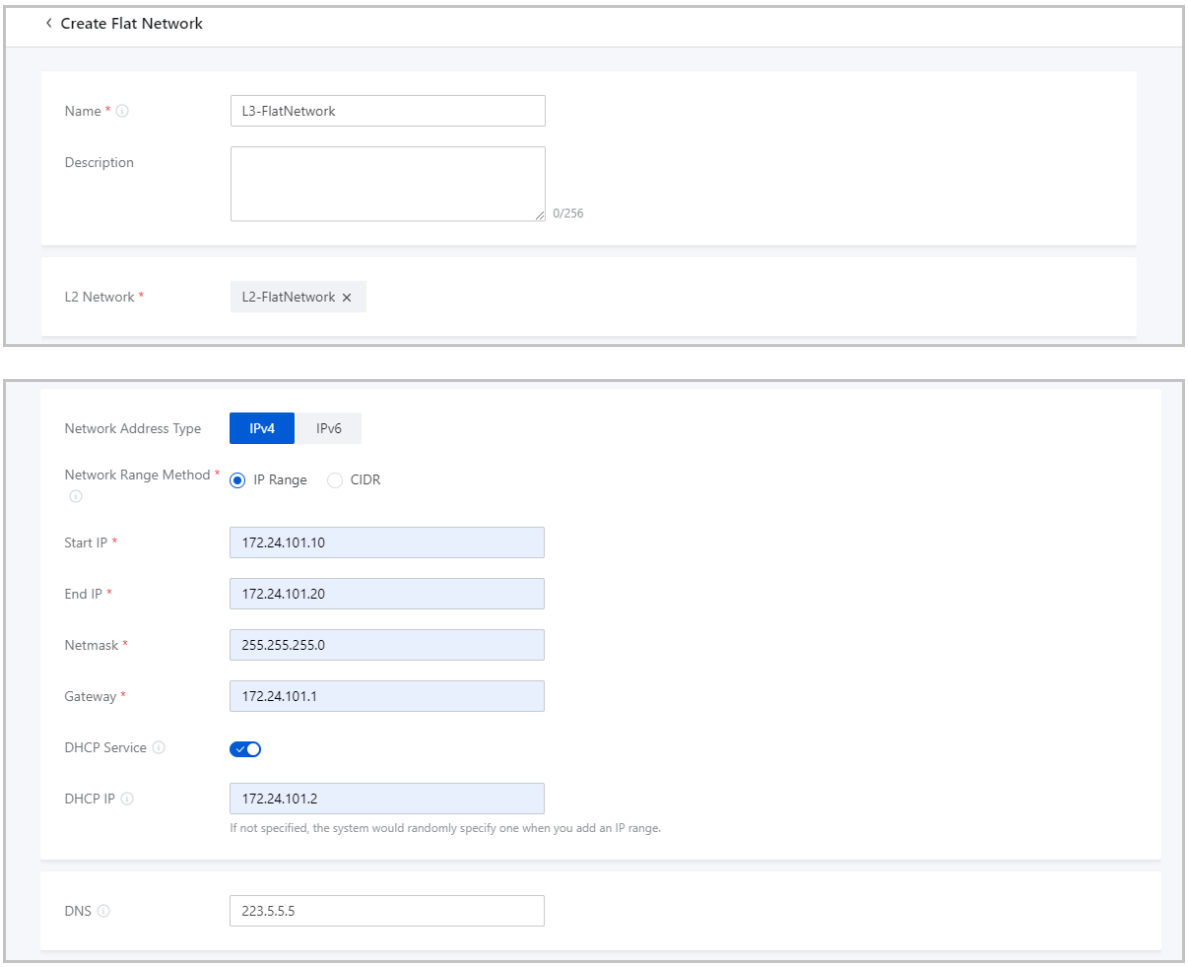
- **DNS**: Add a DNS server to provide domain name resolution services for the flat network. You can specify *223.5.5.5*, *8.8.8.8*, or *114.114.114.114*.

Note:

When you add an IP range for an IPv4 L3 network, note that:

- The IP range cannot contain gateway IP addresses *xxx.xxx.xxx.1*, broadcast addresses *xxx.xxx.xxx.255*, or network addresses in the format of *xxx.xxx.xxx.0*.
- The IP range of a flat network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-69: Create IPv4 Flat Network Using IP Range



If you select **CIDR**, you need to set the following parameters:

- **CIDR**: Set a CIDR block for the flat network, for example, *192.168.108.1/24*.
- **Gateway**: Set a gateway for the flat network, for example, *192.168.108.1*.

Note:

- You can use the first or last IP address in the specified CIDR block as the gateway.
- If left blank, the first IP address in the specified CIDR block is used as the gateway.

- **DHCP Service**: Choose whether to enable the DHCP service.

Note:

- The DHCP service is enabled by default. This service automatically assigns an IP address to a VM instance. You can specify an IP address for the DHCP server. If you do not specify, the system assigns a random IP address for the DHCP server.
- If you disable the DHCP service, no IP address is automatically assigned to VM instances in the flat network. You need to manually configure IP addresses for the VM instances.

— **DHCP IP**: Optional. Set an IP address for the DHCP server, for example, *192.168.108.10*.

Note:

- When you create an L3 network and enable the DHCP service for the first time, or when you add the first network range for an L3 network that has the DHCP service enabled, you can specify an IP address for the DHCP server.
- If a DHCP IP is specified for an L3 network, you cannot specify another DHCP IP when you add a network range for the network.
- The DHCP IP must be within the CIDR block and must not be in use.
- If left blank, the system assigns a random IP address for the DHCP server.
- The first IP address in the CIDR block is predefined as the default gateway and cannot be used as a DHCP server IP.

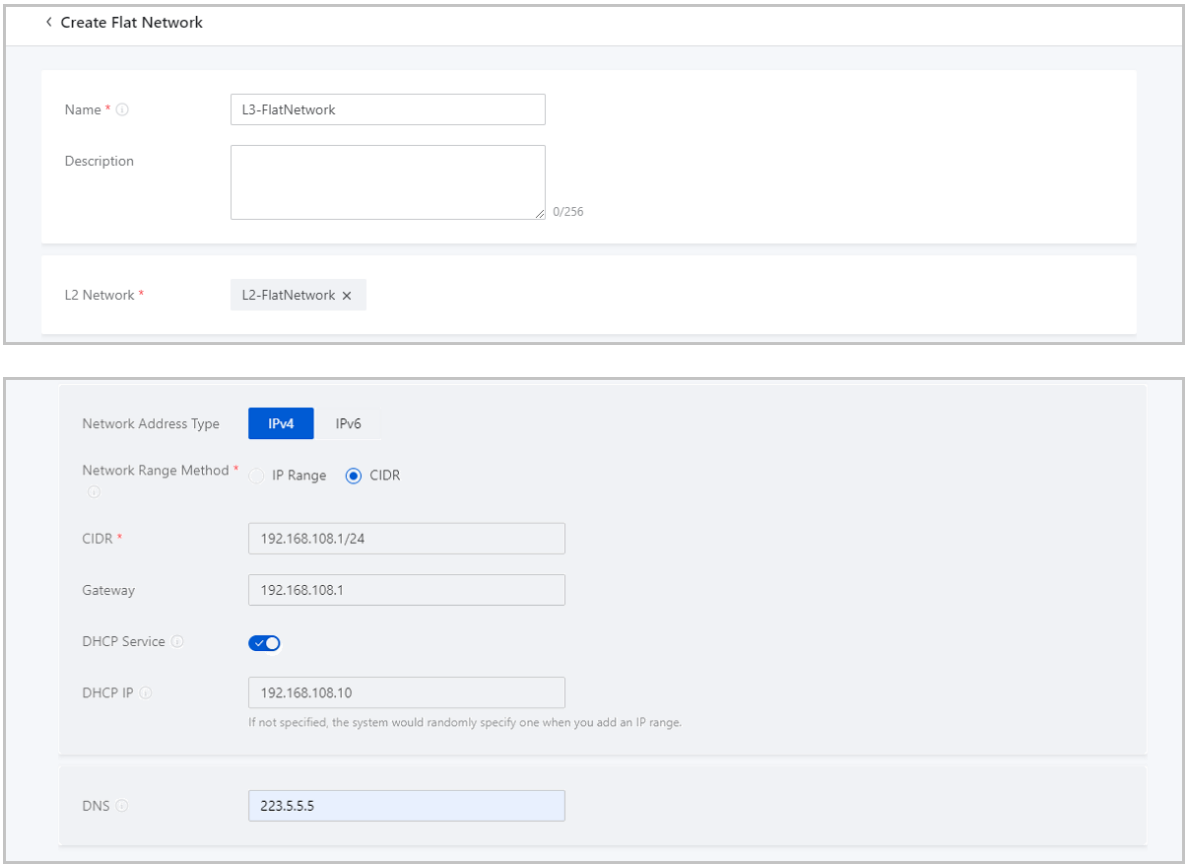
- **DNS**: Add a DNS server to provide domain name resolution services for the flat network. You can specify *223.5.5.5*, *8.8.8.8*, or *114.114.114.114*.

Note:

When you add a CIDR block for an IPv4 L3 network, note that:

- The CIDR block cannot contain the link-local address 169.254.0.0/16.
- The CIDR block of a flat network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-70: Create IPv4 Flat Network Using CIDR Block



Create IPv6 Flat Network

On the displayed page, set the following parameters:

- **Name**: Enter a name for the flat network.
- **Description**: Optional. Enter a description for the flat network.
- **L2 Network**: Select an L2 network for the flat network.

> **Note:**
> ZStack Cloud allows you to use an L2 network to create multiple L3 networks. However, we recommend that you do not use an L2 network to create multiple L3 networks if not for specific business needs.

On the **Select L2 Network** pane, two tabs are displayed:

- **Recommended**: lists L2 networks in the current zone that are not attached to an L3 network.
- **All**: lists all L2 networks in the current zone.

- **Network Address Type**: Select IPv6.
- **Network Range Method**: Select a method to add a network range for the flat network. You can select IP Range or CIDR.

  If you select **IP Range**, you need to set the following parameters:

  - **IP Configuration Mode**: Select the IP distribution mode:
    - Stateful-DHCP: The interface address and other parameters are all configured through DHCP. The IP range method supports stateful DHCP.
  - **Start IP**: Set a start IP address for the network range, for example, *2000:910A:2222:5498:8475:1111:3900:2002*.
  - **End IP**: Set an end IP address for the network range, for example, *2000:910A:2222:5498:8475:1111:3900:2009*.
  - **Prefix Length**: Set a prefix length for the network range, for example, 64.

    Note:
    The prefix length ranges from 64 to 126. If you set a length smaller than 64, VM creation may fail.
  - **Gateway**: Set a gateway for the network range, for example, *2000:910A:2222:5498:8475:1111:3900:2001*.
  - **DHCP Service**: Choose whether to enable the DHCP service.

    Note:
    - The DHCP service is enabled by default. This service automatically assigns an IP address to a VM instance. You can specify an IP address for the DHCP server. If you do not specify, the system assigns a random IP address for the DHCP server.
    - If you disable the DHCP service, no IP address is automatically assigned to VM instances in the flat network. You need to manually configure IP addresses for the VM instances.
    - **DHCP IP**: Optional. Set an IP address for the DHCP server, for example, *2000:910A:2222:5498:8475:1111:3900:2006*.

Note:

- When you create an L3 network and enable the DHCP service for the first time, or when you add the first network range for an L3 network that has the DHCP service enabled, you can specify an IP address for the DHCP server.
- If a DHCP IP is specified for an L3 network, you cannot specify another DHCP IP when you add a network range for the network.
- The DHCP IP can be within or out of the added IP range. However, the IP address must be within the CIDR block to which the added IP range belongs and must not be in use.
- The IP range determined by the start IP and end IP cannot contain the link-local address fe80::/10.
- If left blank, the system assigns a random IP address for the DHCP server.

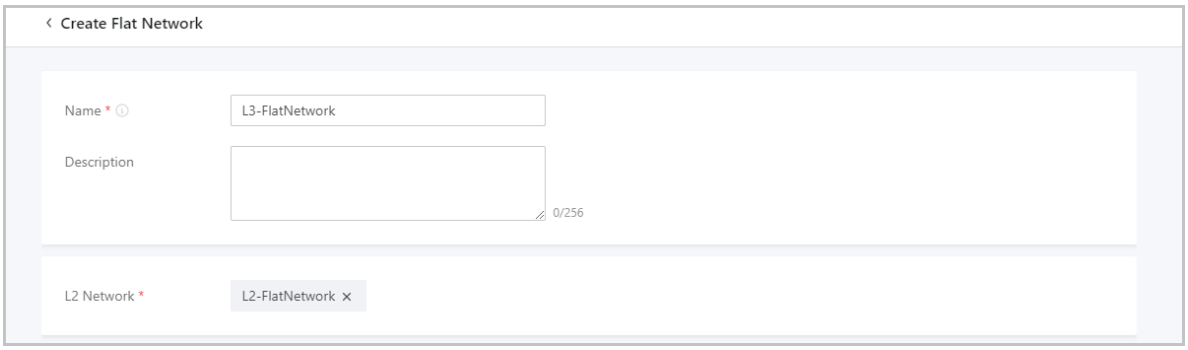
- **DNS**: Add a DNS server to provide domain name resolution services for the public network. You can specify *240C::6644* or *240C::6666*.

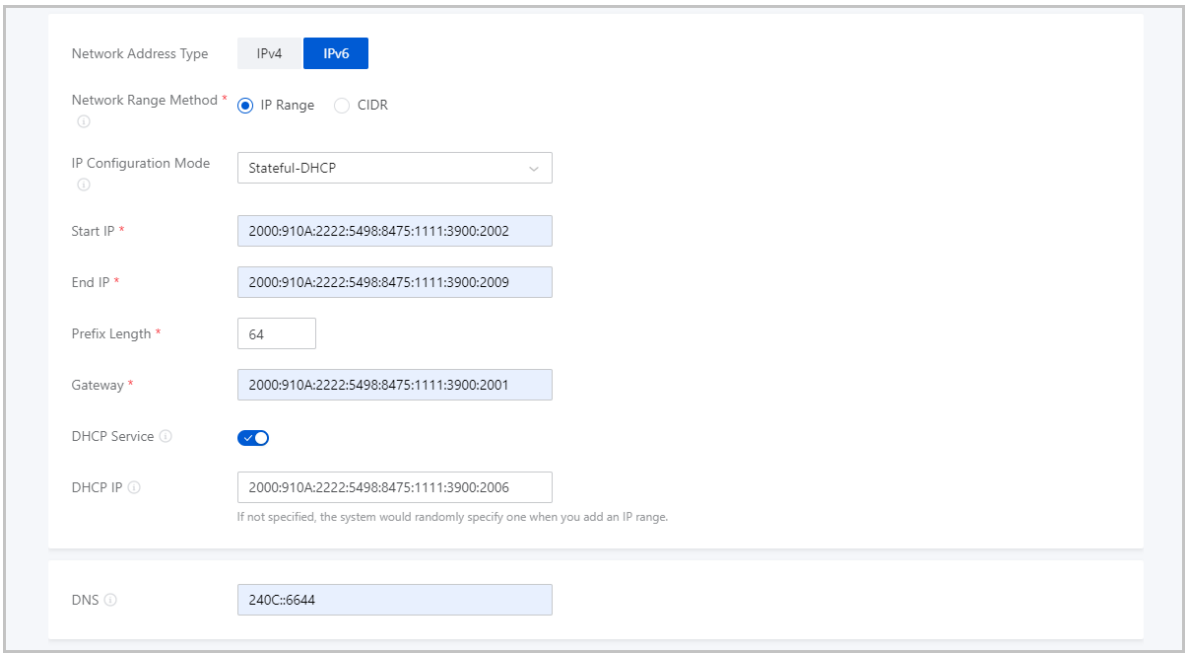
Note:

When you add an IP range for an IPv6 L3 network, note that:

- The IP range cannot contain gateway IP addresses *xxxx::1*.
- The IP range determined by the start IP and end IP cannot contain the link-local address fe80::/10.
- The IP range of a flat network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-71: Create IPv6 Flat Network Using IP Range





If you select **CIDR**, you need to set the following parameters:

- **IP Configuration Mode**: Select the IP distribution mode:
  - Stateful-DHCP: The interface address and other parameters are all configured through DHCP. The IP range method supports stateful DHCP.
  - Stateless-DHCP: The interface address is automatically derived from the route advertisement prefix and the interface Mac address. Other parameters are configured through DHCP.
  - SLAAC: The interface address is automatically derived from the prefix of the route advertisement that also contains other parameters.
- **CIDR**: Set a CIDR block for the flat network, for example, *234E:2457:3D::/64*.
- **DHCP Service**: Choose whether to enable the DHCP service.

Note:

- The DHCP service is enabled by default. This service automatically assigns an IP address to a VM instance. You can specify an IP address for the DHCP server. If you do not specify, the system assigns a random IP address for the DHCP server.
- If you disable the DHCP service, no IP address is automatically assigned to VM instances in the public network. You need to manually configure IP addresses for the VM instances.

— **DHCP IP**: Optional. Set an IP address for the DHCP server, for example, *234E:2457:3D::F*.

Note:

- When you create an L3 network and enable the DHCP service for the first time, or when you add the first network range for an L3 network that has the DHCP service enabled, you can specify an IP address for the DHCP server.
- If a DHCP IP is specified for an L3 network, you cannot specify another DHCP IP when you add a network range for the network.
- The DHCP IP must be within the CIDR block and must not be in use.
- If left blank, the system assigns a random IP address for the DHCP server.
- The first IP address in the CIDR block is predefined as the default gateway and cannot be used as a DHCP server IP.

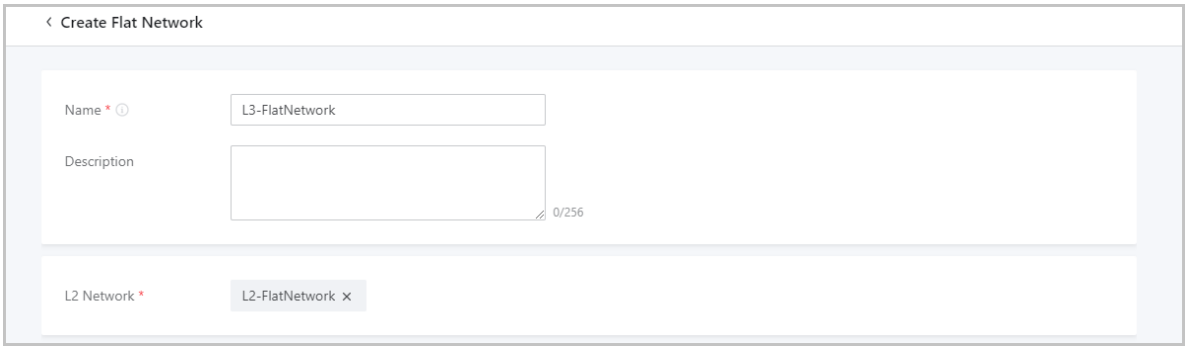
— **DNS**: Add a DNS server to provide domain name resolution services for the public network. You can specify *240C::6644* or *240C::6666*.

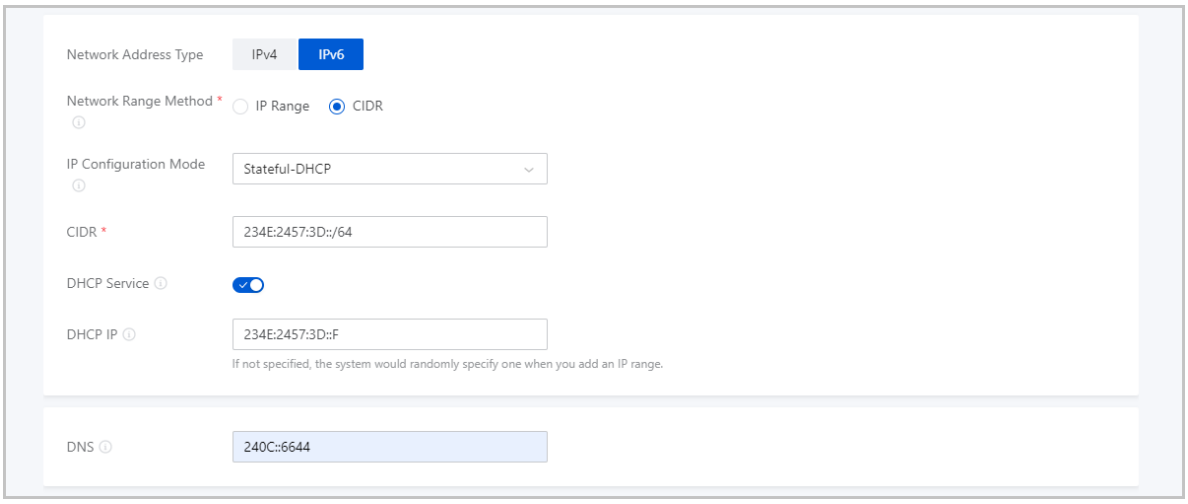
Note:

When you add a CIDR block for an IPv6 L3 network, note that:

- The first IP address in the CIDR block is used as the default gateway.
- The CIDR block cannot contain the link-local address fe80::/10.
- The IP range of a flat network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-72: Create IPv6 Flat Network Using CIDR Block





7.3.3.2.2 Manage a Flat Network

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **L3 Network Resources** > **Flat Network**. The **Flat Network** page appears.

The following table lists the actions that you can perform on a flat network.

Action	Description
Create Flat Network	Create a flat network.
Add DNS	Add an IPv4 or IPv6 DNS server address: • IPv4 address: *223.5.5.5*, *8.8.8.8*, or *114.114.114.114*. • IPv6 address: *240C::6644* or *240C::6666*.
Set Sharing Mode	Set the sharing mode of a flat network. The platform provides the following sharing modes: • Share Globally: shares a flat network with all projects and normal accounts that have the Enterprise Management license. • Share to Specified Projects/Accounts: shares a flat network with specified projects and normal accounts that have the Enterprise Management license. • Not Share: The flat network is not shared with projects or normal accounts and can be used only by the admin. **Note:** • Modifying the sharing mode will also modify the permissions on shared flat networks.

Action	Description
	• Flat networks that are used by projects or accounts before a modification are not affected until the flat networks are released.
Delete Flat Network	Delete a flat network. **Note:** Deleting a flat network also detaches the VM NICs that are using this network, and removes the corresponding vRouters, network services, and vRouter offerings. Proceed with caution.

7.3.3.3 VPC Network

7.3.3.3.1 Create a VPC Network

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **L3 Network Resources** > **VPC Network**. On the **VPC Network** page, click **Create VPC Network**. The **Create VPC Network** page appears.

The following lists the two VPC network creation scenarios:

- Create an IPv4 VPC network
- Create an IPv6 VPC network

Create IPv4 VPC Network

On the displayed page, set the following parameters:

- **Name**: Enter a name for the VPC network.
- **Description**: Optional. Enter a description for the VPC network.
- **L2 Network**: Select an L2 network for the VPC network.

  Note:
  ZStack Cloud allows you to use an L2 network to create multiple L3 networks. However, we recommend that you do not use an L2 network to create multiple L3 networks if not for specific business needs.

  On the **Select L2 Network** pane, two tabs are displayed:

  - **Recommended**: lists L2 networks in the current zone that are not attached to an L3 network.

  - **All**: lists all L2 networks in the current zone.
- **VPC vRouter**: Optional. You can specify a VPC vRouter when you create a VPC network or attach a VPC vRouter to a created VPC network.
- **Network Address Type**: Select IPv4.
- **Network Range Method**: Select a method to add a network range for the VPC network. You can select IP Range or CIDR.

  If you select **IP Range**, you need to set the following parameters:

  - **Start IP**: Set a start IP address for the network range, for example, *172.20.108.100*.
  - **End IP**: Set an end IP address for the network range, for example, *172.20.108.200*.
  - **Netmask**: Set a netmask for the network range, for example, *255.255.0.0*.
  - **Gateway**: Set a gateway for the network range, for example, *172.20.0.1*.
  - **DHCP Service**: Choose whether to enable the DHCP service.

    Note:

    - The DHCP service is enabled by default. This service automatically assigns an IP address to a VM instance. You can specify an IP address for the DHCP server. If you do not specify, the system assigns a random IP address for the DHCP server.
    - If you disable the DHCP service, no IP address is automatically assigned to VM instances in the VPC network. You need to manually configure IP addresses for the VM instances.

  — **DHCP IP**: Optional. Set an IP address for the DHCP server, for example, *172.20.108.10*.

    Note:

    - When you create an L3 network and enable the DHCP service for the first time, or when you add the first network range for an L3 network that has the DHCP service enabled, you can specify an IP address for the DHCP server.
    - If a DHCP IP is specified for an L3 network, you cannot specify another DHCP IP when you add a network range for the network.
    - The DHCP IP can be within or out of the added IP range. However, the IP address must be within the CIDR block to which the added IP range belongs and must not be in use.

- The IP range determined by the start IP and end IP cannot contain the link-local address 169.254.0.0/16.
- If left blank, the system assigns a random IP address for the DHCP server.

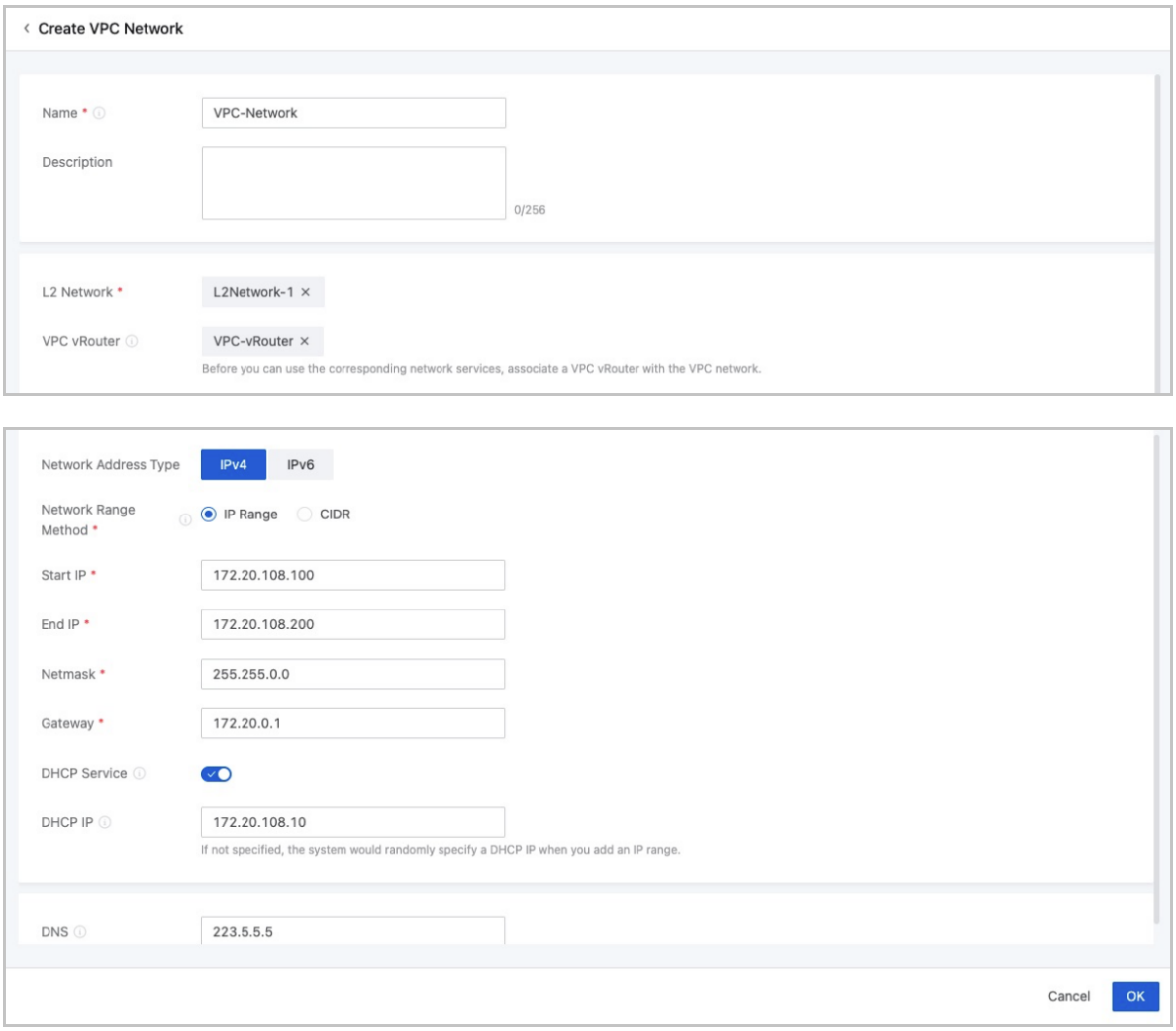
- **DNS**: Provide DNS services for an L3 network. Here, you can specify a DNS address such as 223.5.5.5.

Note:

When you add an IP range for an IPv4 L3 network, note that:

- The IP range cannot contain gateway IP addresses *xxx.xxx.xxx.1*, broadcast addresses *xxx.xxx.xxx.255*, or network addresses in the format of *xxx.xxx.xxx.0*.
- The IP range of a VPC network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-73: Create IPv4 VPC Network Using IP Range



If you select **CIDR**, you need to set the following parameters:

- **CIDR**: Set a CIDR block for the VPC network, for example, *192.168.108.1/24*.
- **Gateway**: Set a gateway for the VPC network, for example, *192.168.108.1*.

> **Note:**
>
> - You can use the first or last IP address in the specified CIDR block as the gateway.
> - If left blank, the first IP address in the specified CIDR block is used as the gateway.

- **DHCP Service**: Choose whether to enable the DHCP service.

> **Note:**
>
> - The DHCP service is enabled by default. This service automatically assigns an IP address to a VM instance. You can specify an IP address for the DHCP server. If you do not specify, the system assigns a random IP address for the DHCP server.
> - If you disable the DHCP service, no IP address is automatically assigned to VM instances in the VPC network. You need to manually configure IP addresses for the VM instances.

— **DHCP IP**: Optional. Set an IP address for the DHCP server, for example, *192.168.108.10*.

> **Note:**
>
> - When you create an L3 network and enable the DHCP service for the first time, or when you add the first network range for an L3 network that has the DHCP service enabled, you can specify an IP address for the DHCP server.
> - If a DHCP IP is specified for an L3 network, you cannot specify another DHCP IP when you add a network range for the network.
> - The DHCP IP must be within the CIDR block and must not be in use.
> - If left blank, the system assigns a random IP address for the DHCP server.
> - The first IP address in the CIDR block is predefined as the default gateway and cannot be used as a DHCP server IP.

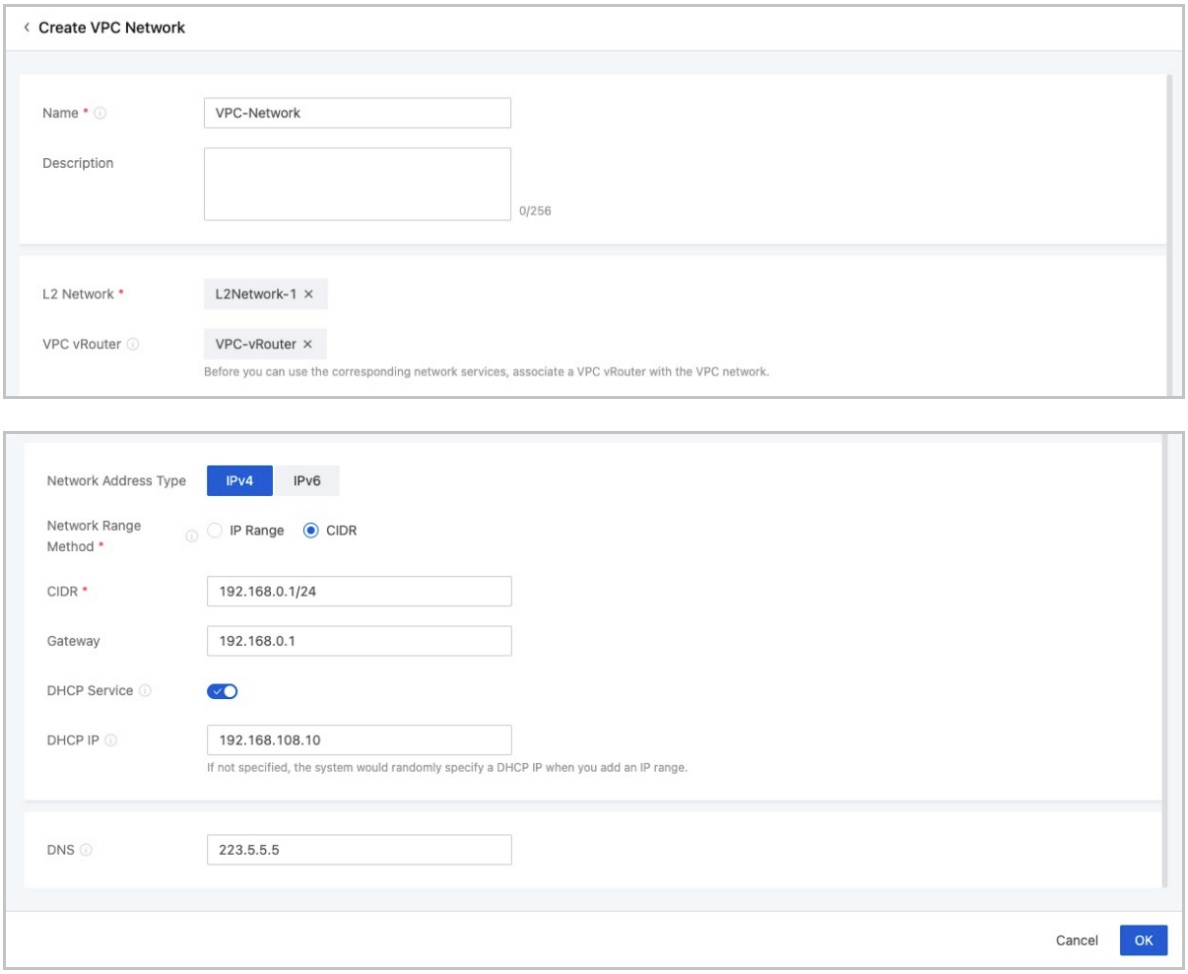
- **DNS**: Provide DNS services for an L3 network. Here, you can specify a DNS address such as 223.5.5.5.

Note:

When you add a CIDR block for an IPv4 L3 network, note that:

- The CIDR block cannot contain the link-local address 169.254.0.0/16.
- The CIDR block of a VPC network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-74: Create IPv4 VPC Network Using CIDR Block



Create IPv6 VPC Network

On the displayed page, set the following parameters:

- **Name**: Enter a name for the VPC network.
- **Description**: Optional. Enter a description for the VPC network.
- **L2 Network**: Select an L2 network for the VPC network.

> **Note:**
> ZStack Cloud allows you to use an L2 network to create multiple L3 networks. However, we recommend that you do not use an L2 network to create multiple L3 networks if not for specific business needs.

On the **Select L2 Network** pane, two tabs are displayed:

- **Recommended**: lists L2 networks in the current zone that are not attached to an L3 network.
- **All**: lists all L2 networks in the current zone.

- **VPC vRouter**: Optional. You can specify a VPC vRouter when you create a VPC network or attach a VPC vRouter to a created VPC network.
- **Network Address Type**: Select IPv6.
- **Network Range Method**: Select a method to add a network range for the VPC network. You can select IP Range or CIDR.

  If you select **IP Range**, you need to set the following parameters:

  - **IP Configuration Mode**: Select the IP distribution mode:
    - Stateful-DHCP: The interface address and other parameters are all configured through DHCP. The IP range method supports stateful DHCP.
  - **Start IP**: Set a start IP address for the network range, for example, *2000:910A:2222:5498:8475:1111:3900:2002*.
  - **End IP**: Set an end IP address for the network range, for example, *2000:910A:2222:5498:8475:1111:3900:2009*.
  - **Prefix Length**: Set a prefix length for the network range, for example, 64.

    > **Note:**
    > The prefix length ranges from 64 to 126. If you set a length smaller than 64, VM creation may fail.

  - **Gateway**: Set a gateway for the network range, for example, *2000:910A:2222:5498:8475:1111:3900:2001*.
  - **DHCP Service**: Choose whether to enable the DHCP service.

    > **Note:**

- The DHCP service is enabled by default. This service automatically assigns an IP address to a VM instance. You can specify an IP address for the DHCP server. If you do not specify, the system assigns a random IP address for the DHCP server.
- If you disable the DHCP service, no IP address is automatically assigned to VM instances in the VPC network. You need to manually configure IP addresses for the VM instances.

— **DHCP IP**: Optional. Set an IP address for the DHCP server, for example, *2000:910A:2222:5498:8475:1111:3900:2006*.

Note:

- When you create an L3 network and enable the DHCP service for the first time, or when you add the first network range for an L3 network that has the DHCP service enabled, you can specify an IP address for the DHCP server.
- If a DHCP IP is specified for an L3 network, you cannot specify another DHCP IP when you add a network range for the network.
- The DHCP IP can be within or out of the added IP range. However, the IP address must be within the CIDR block to which the added IP range belongs and must not be in use.
- The IP range determined by the start IP and end IP cannot contain the link-local address fe80::/10.
- If left blank, the system assigns a random IP address for the DHCP server.

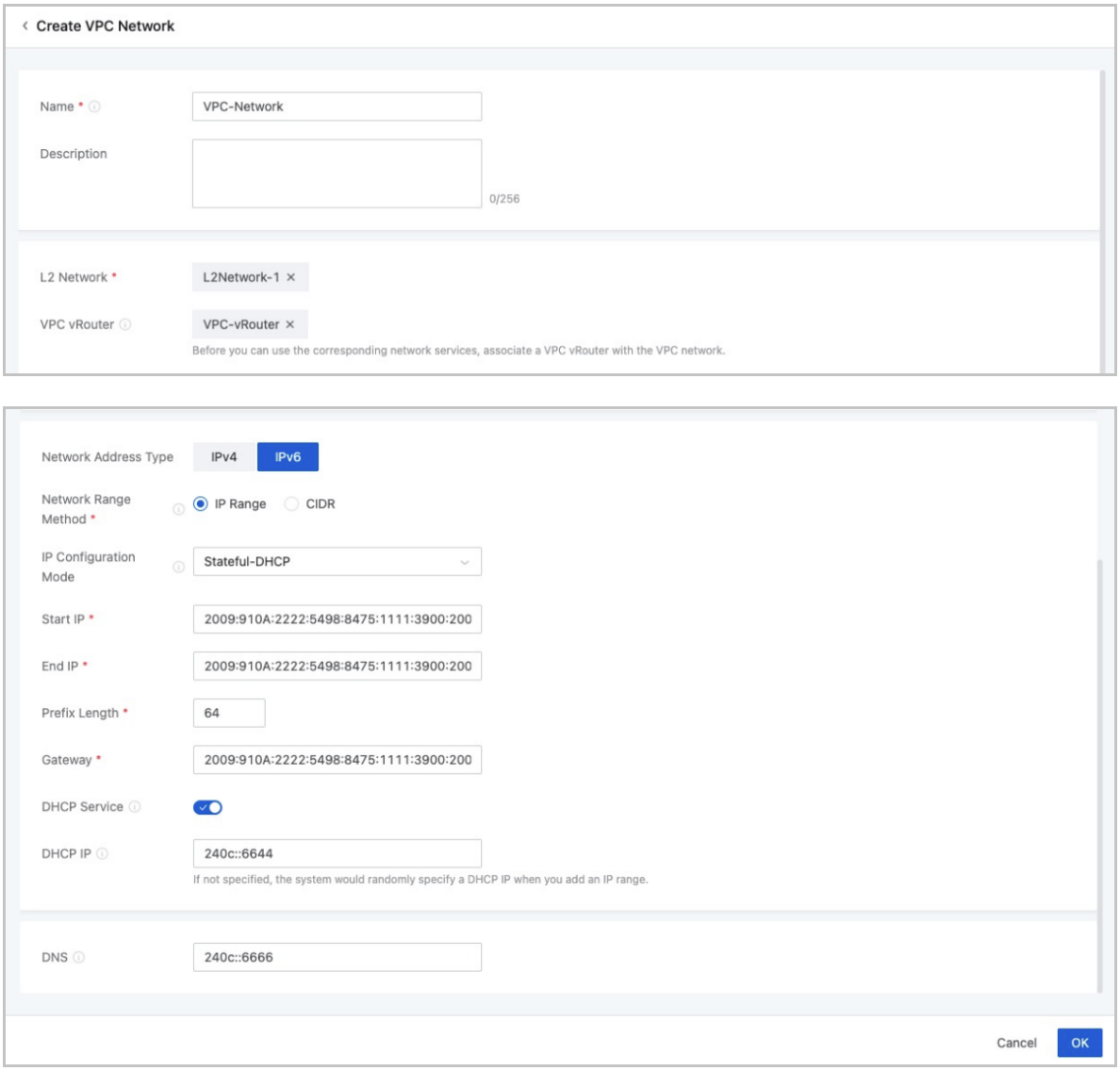
- **DNS**: Provide DNS services for an L3 network. Here, you can specify a DNS address such as 240C::6666.

Note:

When you add an IP range for an IPv6 L3 network, note that:

- The IP range cannot contain gateway IP addresses *xxxx::1*.
- The IP range determined by the start IP and end IP cannot contain the link-local address fe80::/10.
- The IP range of a VPC network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-75: Create IPv6 VPC Network Using IP Range



If you select **CIDR**, you need to set the following parameters:

- **IP Configuration Mode**: Select the IP distribution mode:
  - Stateful-DHCP: The interface address and other parameters are all configured through DHCP. The IP range method supports stateful DHCP.
  - Stateless-DHCP: The interface address is automatically derived from the route advertisement prefix and the interface Mac address. Other parameters are configured through DHCP.
  - SLAAC: The interface address is automatically derived from the prefix of the route advertisement that also contains other parameters.
- **CIDR**: Set a CIDR block for the VPC network, for example, *234E:2457:3D::/64*.

- **DHCP Service**: Choose whether to enable the DHCP service.

  Note:

  - The DHCP service is enabled by default. This service automatically assigns an IP address to a VM instance. You can specify an IP address for the DHCP server. If you do not specify, the system assigns a random IP address for the DHCP server.
  - If you disable the DHCP service, no IP address is automatically assigned to VM instances in the public network. You need to manually configure IP addresses for the VM instances.

  — **DHCP IP**: Optional. Set an IP address for the DHCP server, for example, *234E:2457:3D::F*.

  Note:

  - When you create an L3 network and enable the DHCP service for the first time, or when you add the first network range for an L3 network that has the DHCP service enabled, you can specify an IP address for the DHCP server.
  - If a DHCP IP is specified for an L3 network, you cannot specify another DHCP IP when you add a network range for the network.
  - The DHCP IP must be within the CIDR block and must not be in use.
  - If left blank, the system assigns a random IP address for the DHCP server.
  - The first IP address in the CIDR block is predefined as the default gateway and cannot be used as a DHCP server IP.

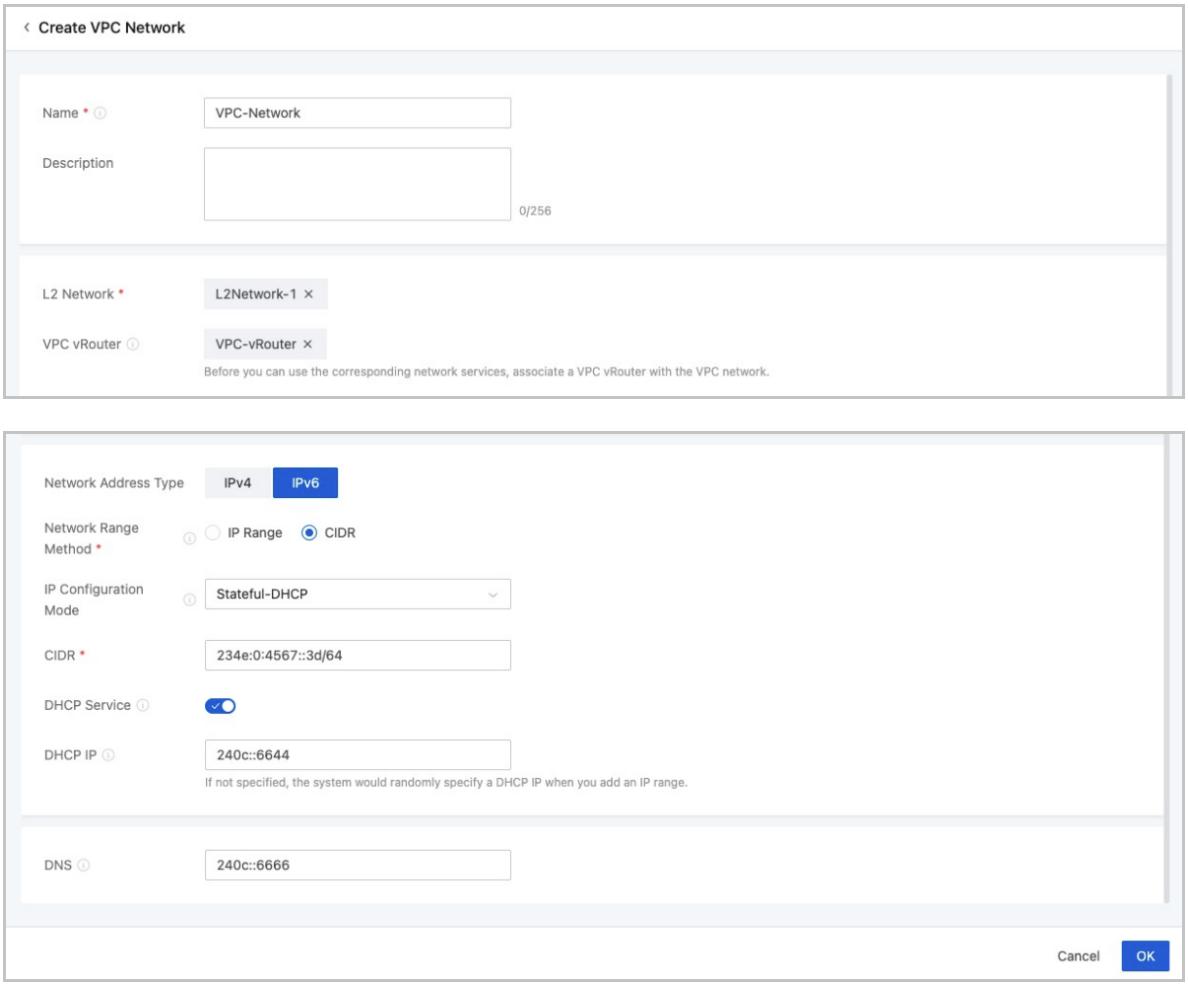
- **DNS**: Provide DNS services for an L3 network. Here, you can specify a DNS address such as 240C::6666.

Note:

When you add a CIDR block for an IPv6 L3 network, note that:

- The first IP address in the CIDR block is used as the default gateway.
- The CIDR block cannot contain the link-local address fe80::/10.
- The IP range of a VPC network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-76: Create IPv6 VPC Network Using CIDR Block



7.3.3.3.2 Manage a VPC Network

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **L3 Network Resources** > **VPC Network**. The **VPC Network** page appears.

The following table lists the actions that you can perform on a VPC network.

Action	Description
Create VPC Network	Create a VPC network.
Set Sharing Mode	Set the sharing mode of a VPC network. The platform provides the following sharing modes: • Share Globally: shares a VPC network with all projects and normal accounts that have the Enterprise Management license.

Action	Description
	• Share to Specified Projects/Accounts: shares a VPC network with specified projects and normal accounts that have the Enterprise Management license. • Not Share: The VPC network is not shared with projects or normal accounts and can be used only by the admin. **Note:** • Modifying the sharing mode will also modify the permissions on shared VPC networks. • VPC networks that are used by projects or accounts before a modification are not affected until the VPC networks are released.
Attach VPC vRouter	Attach a VPC vRouter to the VPC network.
Detach VPC vRouter	Detach a VPC vRouter from the VPC network.
Delete VPC Network	Delete a VPC network. **Note:** Deleting a VPC network also detaches the VM NICs that are using this network.

7.3.3.4 Management Network

7.3.3.4.1 Create a Management Network

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **Dedicated Network** > **Management Network**. On the **Management Network** page, click **Create Management Network**. Then, the **Create Management Network** page is displayed.

Create a Management Network

On the displayed page, set the following parameters:

- **Name**: Enter a name for the management network.
- **Description**: Optional. Enter a description for the management network.
- **L2 Network**: Select an L2 network for the management network.

Note:

ZStack Cloud allows you to use an L2 network to create multiple L3 networks. However, we recommend that you do not use an L2 network to create multiple L3 networks if not for specific business needs.

On the **Select L2 Network** pane, two tabs are displayed:

- **Recommended**: lists L2 networks in the current zone that are not attached to an L3 network.
- **All**: lists all L2 networks in the current zone.

- **Network Range Method**: Select a method to add a network range for the management network. You can select IP Range or CIDR.

  If you select **IP Range**, you need to set the following parameters:

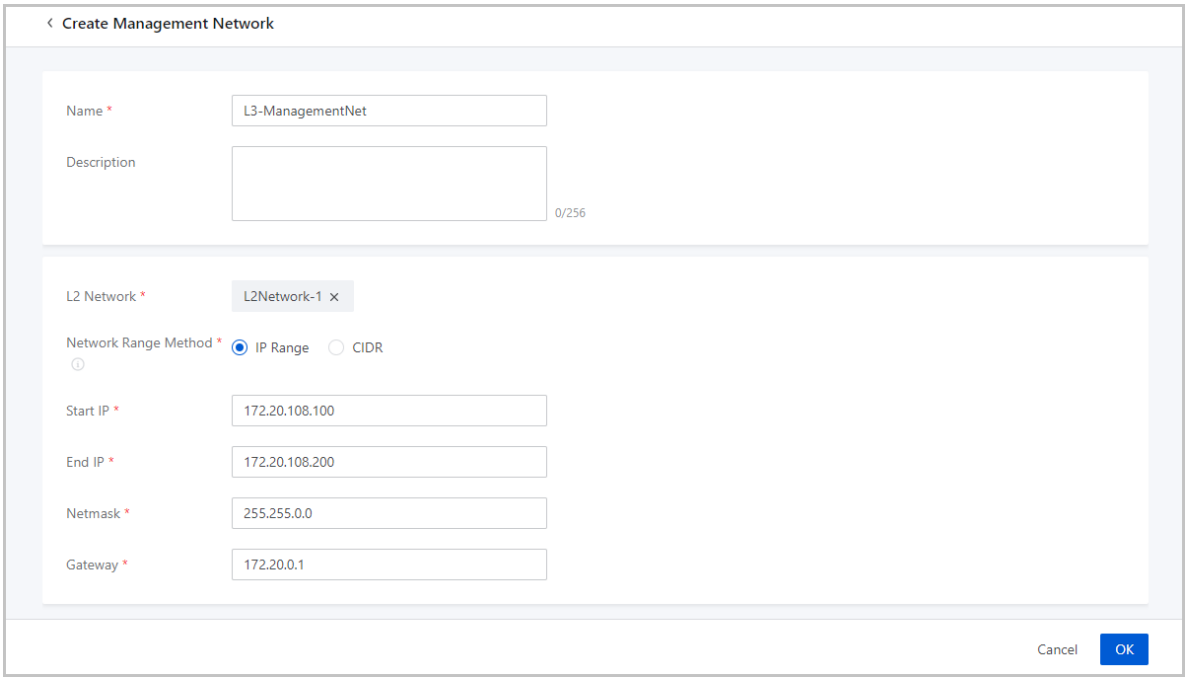
  - **Start IP**: Set a start IP address for the network range, for example, *172.20.108.100*.
  - **End IP**: Set an end IP address for the network range, for example, *172.20.108.200*.
  - **Netmask**: Set a netmask for the network range, for example, *255.255.0.0*.
  - **Gateway**: Set a gateway for the network range, for example, *172.20.0.1*.

  Note:

  When you add an IP range for an L3 network, note that:

  - The IP range cannot contain gateway IP addresses in the format of *xxx.xxx.xxx.1*, broadcast addresses in the format of *xxx.xxx.xxx.255*, or network addresses in the format of *xxx.xxx.xxx.0*.
  - The IP range of a private network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-77: Create Management Network Using IP Range



If you select **CIDR**, you need to set the following parameters:

- **CIDR**: Set a CIDR block for the management network, for example, *192.168.1.1/24*.
- **Gateway**: Set a gateway for the management network, for example, *192.168.1.1*.

Note:

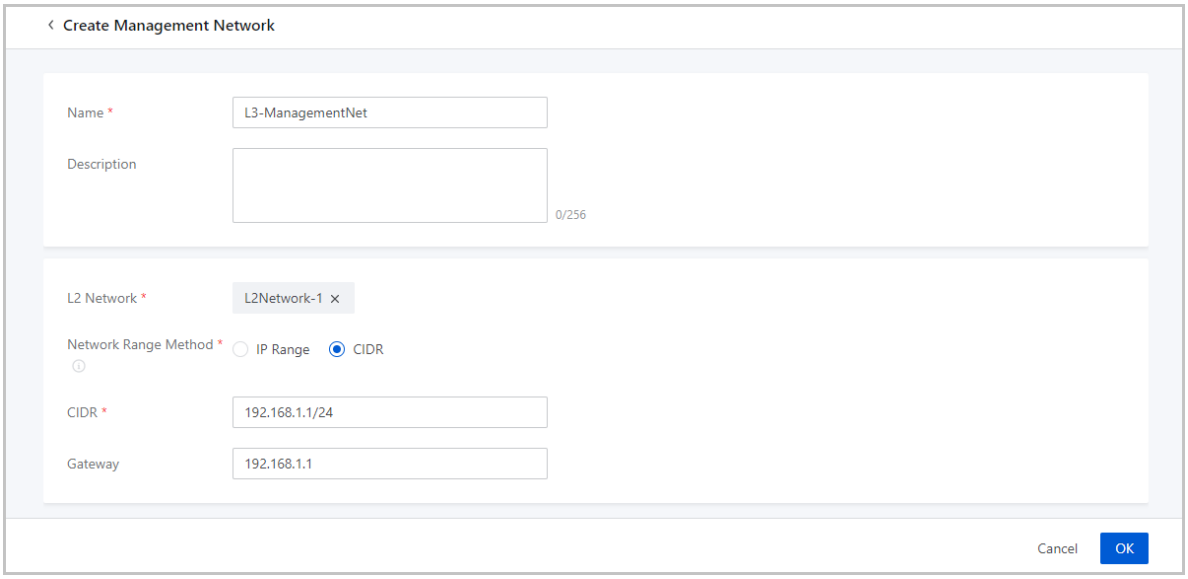
- You can use the first or last IP address in the specified CIDR block as the gateway.
- If left blank, the first IP address in the specified CIDR block is used as the gateway.

Note:

When you add a CIDR block for an L3 network, note that:

- The CIDR block cannot contain the link-local address 169.254.0.0/16.
- The CIDR block of a private network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-78: Create Management Network Using CIDR Block



Considerations

Make sure that the network range of the public network is different from the network range of the management network when you create a vRouter offering.

7.3.3.4.2 Manage a Management Network

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **L2 Network Resources** > **Dedicated Network** > **Management Network**. Then, the **Management Network** page is displayed.

The following table lists the actions that you can perform on a management network.

Action	Description
Create Management Network	Create a management network.
Delete Management Network	Delete a management network. **Note:** Deleting a management network also deletes the associated VPC vRouter.

7.3.3.5 Flow Network

7.3.3.5.1 Create a Flow Network

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **Dedicated Network** > **Flow Network**. On the **Flow Network** page, click **Create Flow Network**. Then, the **Create Flow Network** page is displayed.

Create a Flow Network

On the displayed page, set the following parameters:

- **Name**: Enter a name for the flow network.
- **Description**: Optional. Enter a description for the flow network.
- **L2 Network**: Select an L2 network for the flow network.

  Note:
  ZStack Cloud allows you to use an L2 network to create multiple L3 networks. However, we recommend that you do not use an L2 network to create multiple L3 networks if not for specific business needs.

  On the **Select L2 Network** pane, two tabs are displayed:

  - **Recommended**: lists L2 networks in the current zone that are not attached to an L3 network.
  - **All**: lists all L2 networks in the current zone.
- **Network Range Method**: Select a method to add a network range for the flow network. You can select IP Range or CIDR.

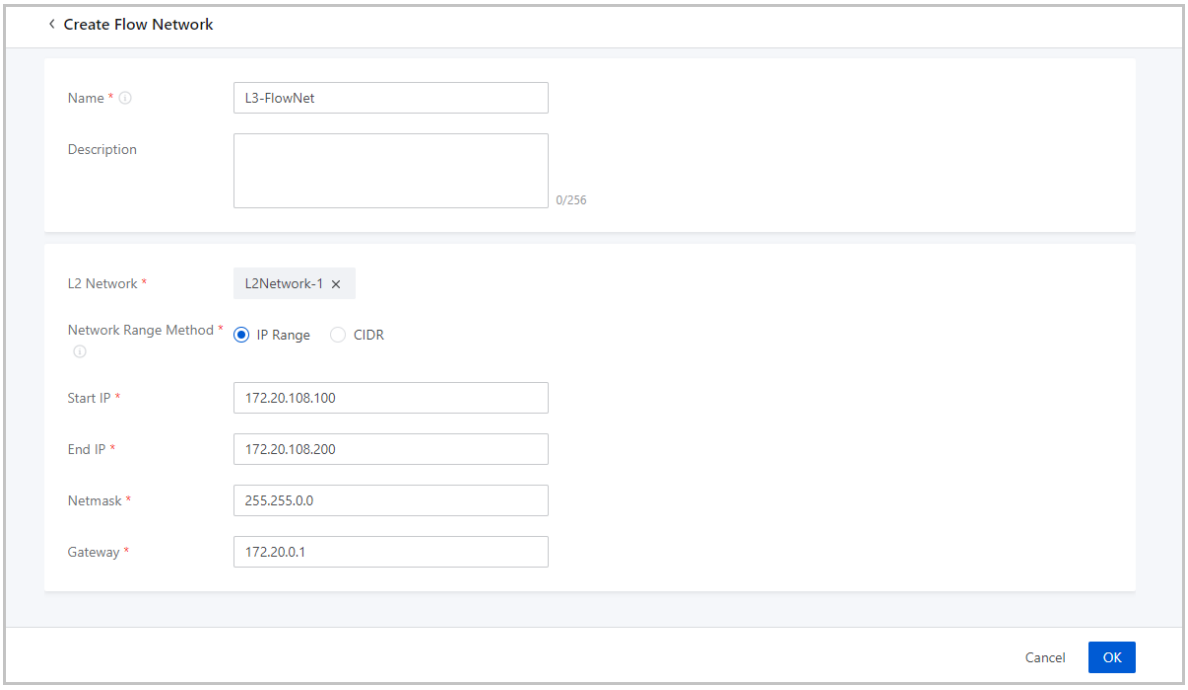
  If you select **IP Range**, you need to set the following parameters:

  - **Start IP**: Set a start IP address for the network range, for example, *172.20.108.100*.
  - **End IP**: Set an end IP address for the network range, for example, *172.20.108.200*.
  - **Netmask**: Set a netmask for the network range, for example, *255.255.0.0*.
  - **Gateway**: Set a gateway for the network range, for example, *172.20.0.1*.

  Note:
  When you add an IP range for an L3 network, note that:

- The IP range cannot contain gateway IP addresses in the format of *xxx.xxx.xxx.1*, broadcast addresses in the format of *xxx.xxx.xxx.255*, or network addresses in the format of *xxx.xxx.xxx.0*.
- The IP range of a private network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-79: Create Flow Network Using IP Range



If you select **CIDR**, you need to set the following parameters:

- **CIDR**: Set a CIDR block for the flow network, for example, *192.168.1.1/24*.
- **Gateway**: Set a gateway for the flow network, for example, *192.168.1.1*.

Note:

- You can use the first or last IP address in the specified CIDR block as the gateway.
- If left blank, the first IP address in the specified CIDR block is used as the gateway.

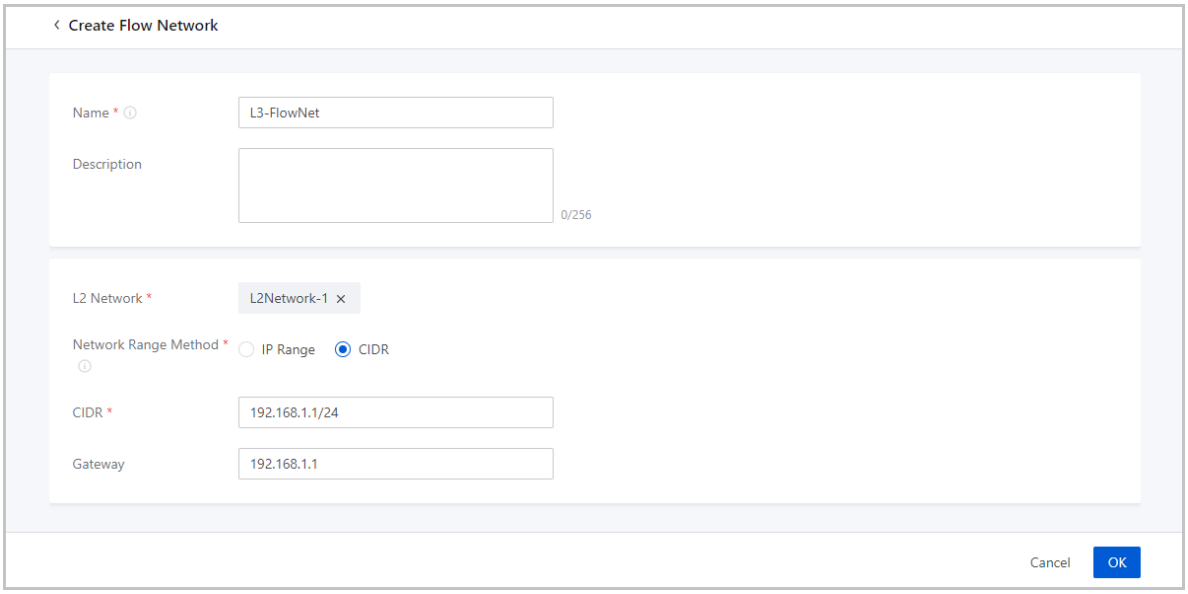
Note:

When you add a CIDR block for an L3 network, note that:

- The CIDR block cannot contain the link-local address 169.254.0.0/16.

- The CIDR block of a private network cannot overlap with the IP range of a public network used to create a vRouter offering or of a management network.

Figure 7-80: Create Flow Network Using CIDR Block



7.3.3.5.2 Manage a Flow Network

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **L2 Network Resources** > **Dedicated Network** > **Flow Network**. Then, the **Flow Network** page is displayed.

The following table lists the actions that you can perform on a flow network.

Action	Description
Create Flow Network	Create a flow network.
Delete Flow Network	Delete a flow network. **Note:** Deleting a flow network also deletes the associated VPC vRouter.

7.3.4 VPC vRouter

7.3.4.1 What is VPC vRouter?

A VPC vRouter is a dedicated VM instance that provides multiple network services.

Characteristics

A VPC vRouter is created from a vRouter offering with a public network and a management network.

- A VPC vRouter is essential to a VPC network. You can create a VPC vRouter by using a vRouter offering.
- Before you create a VPC vRouter, you need to create a public network, management network, and VPC vRouter image required for a vRouter offering.
- You can attach or detach a VPC network or public network to or from a VPC vRouter as needed.
- The public network and management network defined in a vRouter offering cannot be detached .
- You can use a vRouter offering to create multiple VPC cRouters. These VPC vRouters share the same public network and management network defined in the vRouter offering.
- The public network defined in the vRouter offering is used as the default network to provide multiple network services.
- VPC vRouters have higher priorities to use resources than VM instances. If the resource utilization of the host is so high that the resource distribution must be prioritized, the resources are distributed first to VPC vRouters, then to VM instances with **High** priorities, and then to VM instances with **Normal** priorities. For example, if VPC vRouters and VM instances are competing for CPU resources, the CPU resources are distributed first to VPC vRouters.

Notice

- We recommend that a VPC vRouter has no more than 23 VPC networks and public networks in total associated. Too many networks might lower the VPC vRouter performance and affect the quality of related network services.
- All network services in this Cloud share the bandwidth of the physical NIC. Therefore, too many VIPs on a VPC vRouter might cause network performance bottlenecks. We recommend that you reasonably plan the number of VIPs based on actual bandwidth requirements.

7.3.4.2 Create a VPC vRouter

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **vRouter** > **VPC vRouter**. On the **VPC vRouter** page, click **Create VPC vRouter**. Then, the **Create VPC vRouter** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the VPC vRouter.
- **Description**: Optional. Enter a description for the VPC vRouter.
- **Host**: Optional. Select a host on which the VPC vRouter is started.
- **vRouter Offering**: Select a vRouter offering you created before.
- **Default IPv4/IPv6 Address**: Optional. Specify a default IP address for the VPC vRouter. If not specified, the Cloud allocates one automatically.
- **DNS**: Optional. Set the DNS service for the VPC vRouter. If not specified, 223.5.5.5 will be used.

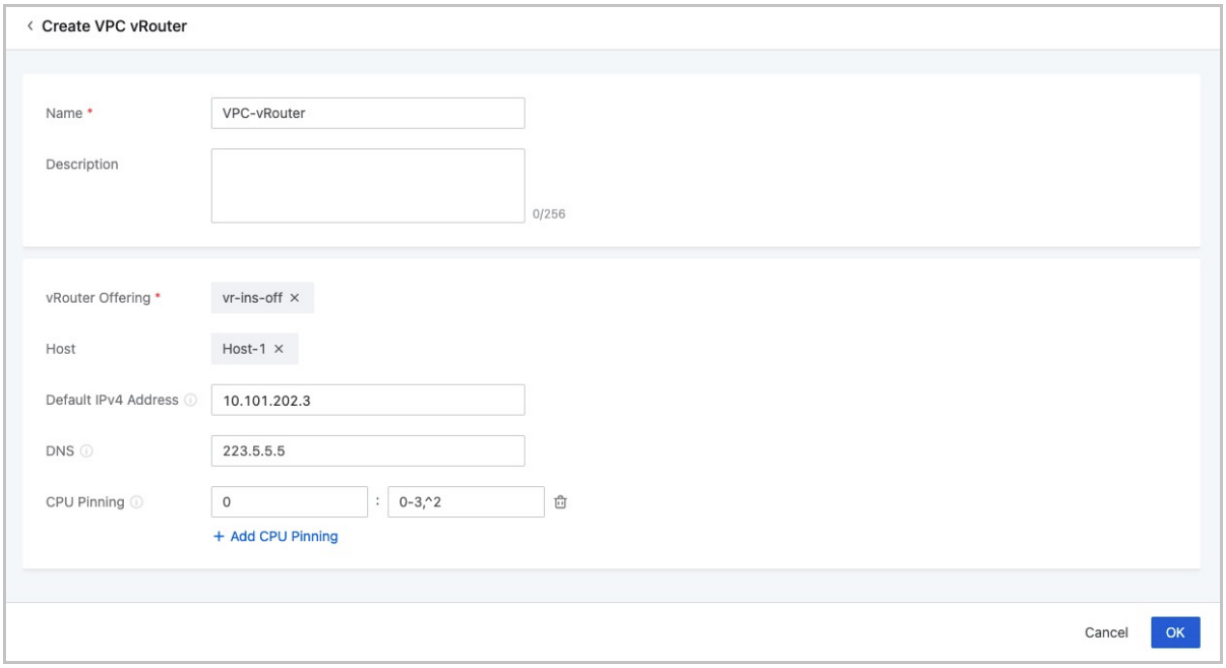
  Note:

  - You can set an IPv4 DNS or IPv6 DNS as needed. For example, you can set the IPv4 DNS to 223.5.5.5 or IPv6 DNS to 240C::6644.
  - Services in the VPC vRouter can access the public network services via DNS. You can also specify the other DNS address if necessary.
  - For VM instances created by using a VPC network, the DNS is the gateway of the VPC network. The VM traffics are forwarded by a VPC vRouter.
- **CPU Pinning**: Associate the virtual CPUs (vCPUs) of the VPC vRouter with host pCPUs stringently so that you can allocate specific pCPUs for the VPC vRouter, thus improving VPC vRouter performances.

  Note:

  - Pinning Format
    - In the left input box, set a vCPU range. In the right input box, set a pCPU range. Range format: integer, hyphen(-), and caret (^). Use commas to separate them.
    - The vCPU range depends on the vRouter offering attached to the VPC vRouter.
    - The pCPU range depends on the pCPU quantity of the selected cluster or host.
  - Example: In the left input box, enter 1. In the right input box, enter 0-3,^2. This example indicates that vCPU 1 is stringently associated with pCPU 0, pCPU 1, and pCPU 3, while ^ represents that vCPU 2 is excluded.

Figure 7-81: Create VPC vRouter



Considerations

When you use a VPC vRouter, note the following:

- VPC networks under different VPC vRouters are isolated from each other by default at Layer 2.
- The IP address segments of different VPC networks under the same VPC vRouter cannot overlap. In addition, the gateways of any two VPC networks cannot be the same.
- Before an ordinary account can create a VPC vRouter, the admin needs to share the vRouter offering. Otherwise, the ordinary account could not create a VPC vRouter or VPC network.
- Before you use a VPC vRouter to provide network services, make sure that the VPC vRouter is in the running or connected state. If the VPC vRouter is in other states, check whether exceptions occur on the related resources.
- If a VM instance is using a VPC network, the VPC network could not be detached from the VPC vRouter.
- You can login to a VPC vRouter by using a password or SSH key:
  - SSH login using password: By default, SSH login by using a password is disabled. To enable the login method, you can go to Global Setting to modify the related setting.

> **Note:**
> If you modify the setting, reconnect the VPC vRouter to make the modification take effect.

- SSH login using key: The SSH key is stored in the path: *$ZSTACK_HOME/WEB-INF/classes/ansible/rsaKeys/id_rsa*.

7.3.5 VPC HA Group

7.3.5.1 What is VPC HA Group?

A VPC vRouter HA group consists of two VPC vRouters. Either VPC vRouter can be a primary or secondary VPC vRouter for the group. If the primary VPC vRouter does not work as expected, the VPC vRouter becomes the secondary VPC vRouter in the group to ensure high availability of business.

Considerations

- Modifying the following configurations of a VPC vRouter also modifies the configurations of its partner VPC vRouter:
  - Attach or detach a network to or from a VPC vRouter.
  - Configure EIP, port forwarding, load balancing, IPsec, virtual IP QoS, DNS, SNAT, OSPF, dynamic routing, multicast routing, and distributed routing for a VPC vRouter.
- The restart, reconnect, delete, and open console actions only take effect on the target VPC vRouter.
- When you can add a VPC vRouter to a VPC vRouter HA group, note that:
  - The management network and the public network attached to this VPC vRouter must be deployed independently.
  - Before you add the VPC vRouter to a VPC vRouter HA group, stop the VPC vRouter first.
- VPC vRouters in a VPC vRouter HA group are displayed in the HA group details page. They are not displayed in the VPC vRouter management page.

7.3.5.2 Create a VPC vRouter HA Group

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **vRouter** > **VPC vRouter HA Group**. On the **VPC vRouter HA Group** page, click **Create VPC vRouter HA Group**. Then, the **Create VPC vRouter HA Group** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the VPC vRouter HA group.
- **Description**: Optional. Enter a description for the VPC vRouter HA group.

- **Monitor IP**: Set an IP address as the monitor IP address. The monitor IP address determines the primary-secondary relationship between two VPC vRouters in the HA group.

  Note:

  - The monitor IP address must be a public IP address that can be accessed by the primary and the secondary VPC vRouters in the HA group.
  - The monitor IP address must be a steady, secure IP address.

- **VPC vRouter**: Add a VPC vRouter by creating a new one or importing an existing one. After you add a VPC vRouter to the HA group, the Cloud automatically configures the peer vRouters with the same configurations.

  If you choose to create a new one, set the following parameters:

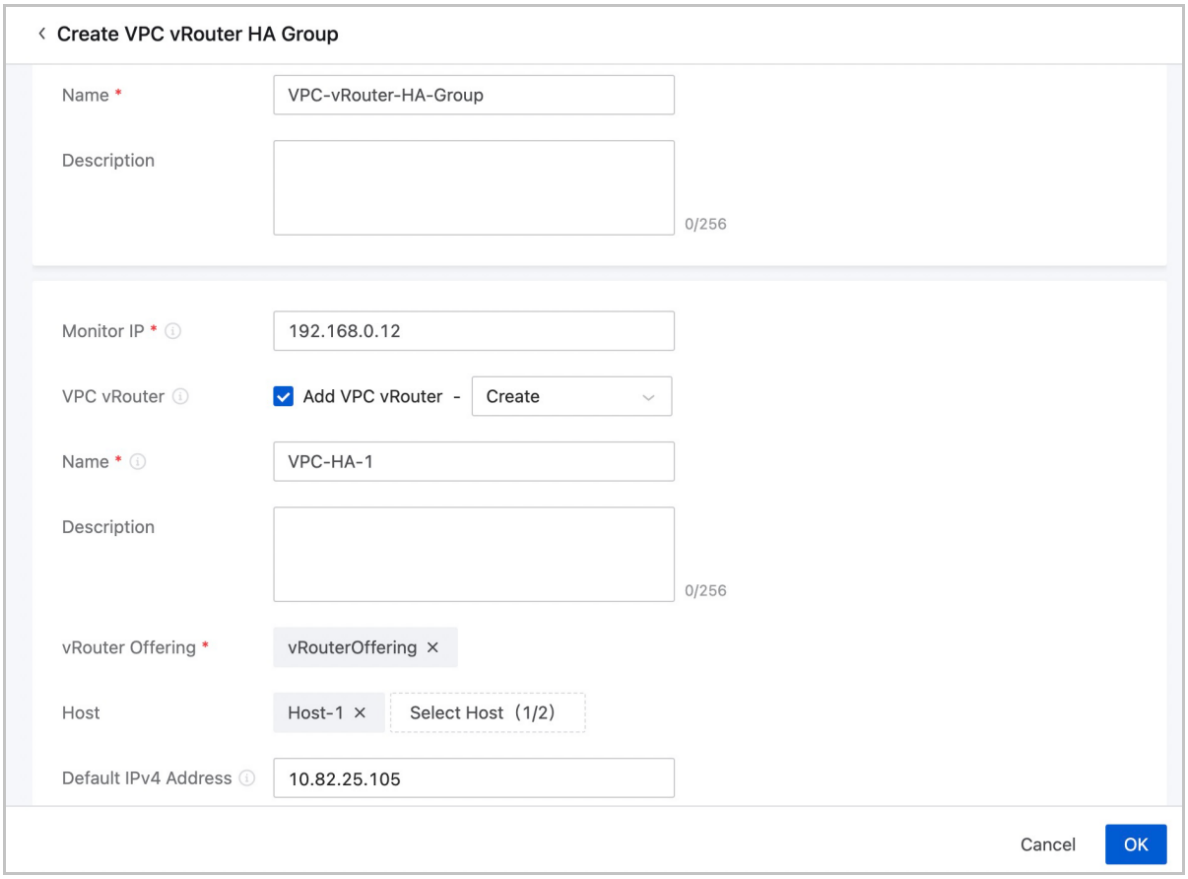
  - **Name**: Enter a name for the VPC vRouter.
  - **Description**: Optional. Enter a description for the VPC vRouter.
  - **Host**: Optional. Select a host where the VPC vRouter is located. You can select up to two hosts.
  - **vRouter Offering**: Select a vRouter offering you created before.

    Note:

    - Make sure that a vRouter offering is available before you can create a VPC vRouter.
    - After you create a VPC vRouter successfully and the primary-secondary relationship is determined, set the DNS on the VPC vRouter HA group details page to ensure that the VPC vRouters work properly.

  - **Default IPv4/IPv6 Address**: Optional. Specify a public IP address as the virtual IP address (VIP) for the HA group. If not specified, the Cloud allocates one automatically.

Figure 7-82: Create VPC vRouter HA Group by Creating New VPC vRouter

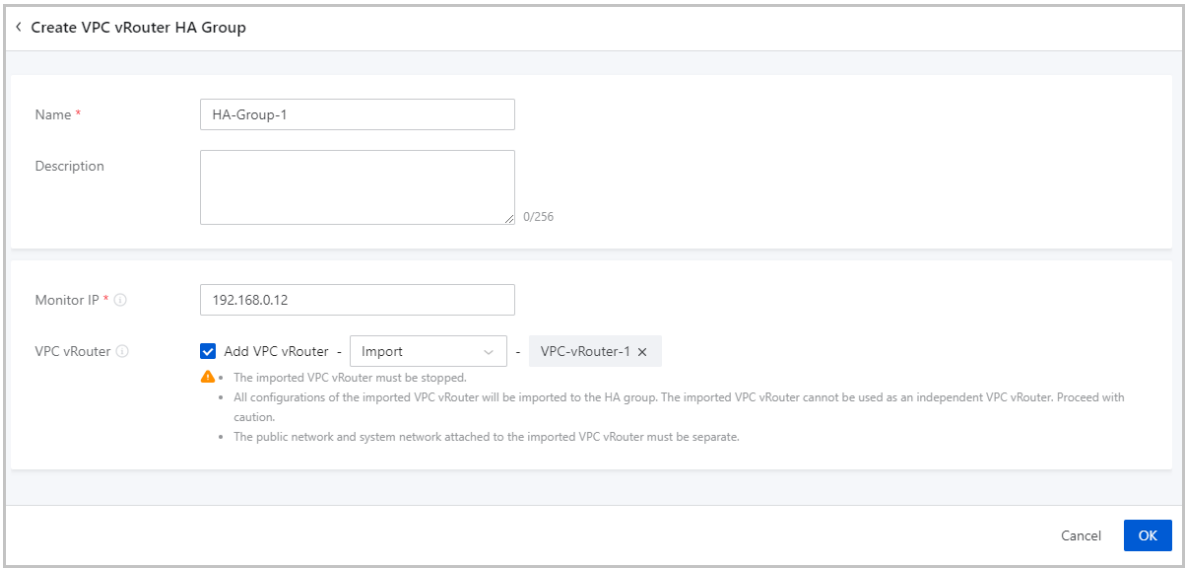


If you choose to import an existing one, set the following parameters:

- **Select VPC vRouter**: Select an existing VPC vRouter.

> **Note:**
>
> - The VPC vRouter to be imported must be stopped.
> - Importing an existing VPC vRouter also imports all configurations of the VPC vRouter. In this case, the VPC vRouter cannot be used independently. Please exercise caution.
> - Only VPC vRouters with isolated public network and system network can be added an HA group.

Figure 7-83: Create VPC vRouter HA Group by Adding Existing VPC vRouter



7.3.6 vRouter Image

7.3.6.1 What is vRouter Image?

A vRouter image encapsulates network services and can be used to create VPC vRouters and load balancers. vRouter images can be categorized into VPC vRouter images and load balancer (LB) images.

Characteristics

A VPC vRouter image encapsulates network services and can be used to create VPC vRouters. However, a VPC vRouter image cannot be used to create VM instances.

An LB image encapsulates dedicated-performance load-balancing services and can be used to create load balancer instances. However, an LB image cannot be used to create VM instances. A load balancer instance is a custom VM instance dedicated to providing load balancing services.

7.3.6.2 Add a vRouter Image

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **vRouter** > **vRouter Image**. On the **vRouter Image** page, click **Add vRouter Image**. Then, the **Add vRouter Image** page is displayed.

The Cloud allows you to add two types of vRouter images: VPC vRouter images (KVM) and load balancer (LB) KVM images (KVM).

Add a VPC vRouter Image (KVM)

Set the following parameters:

- **Name**: Enter a name for the vRouter image.
- **Description**: Optional. Enter a description for the vRouter image.
- **Image Usage**: Specify what the vRouter image is used for. Here, select **VPC vRouter**.
- **Backup Storage**: Select a backup storage to store the vRouter image.
- **Image Path**: Enter a URL or upload a local file.
  - **URL**: Enter the download URL of the vRouter image.

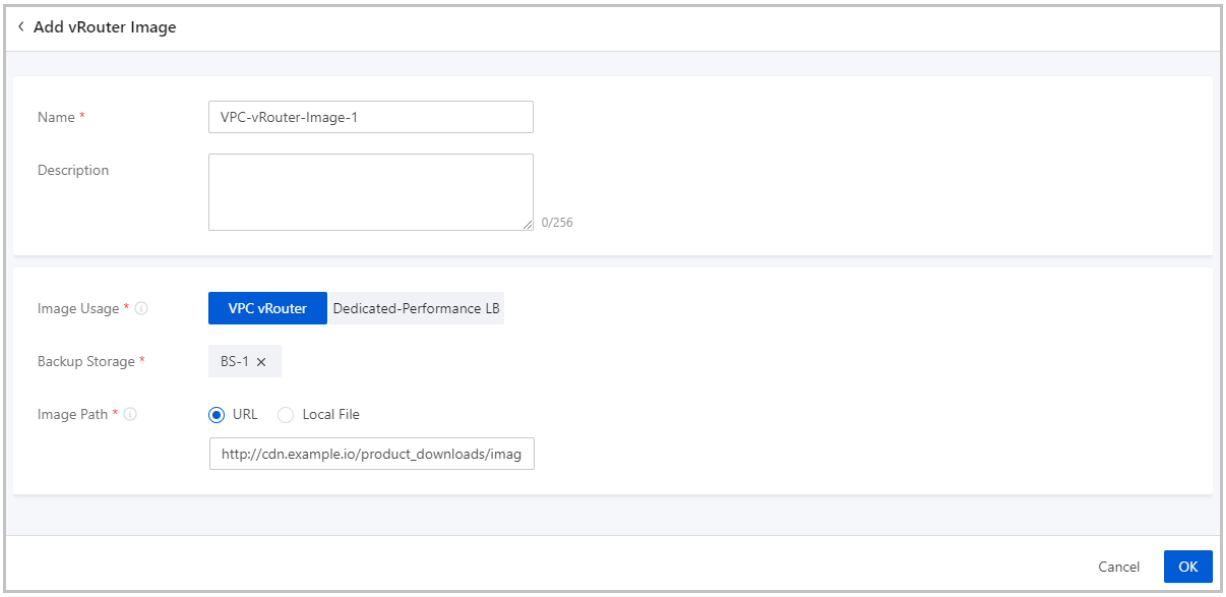
    ZStack Cloud provides you with dedicated VPC vRouter images (KVM). You can download the latest vRouter images from the official website.

    - Software: ZStack-vRouter-4.3.12.qcow2
    - Download address: *Click here*
  - **Local File**: Upload a vRouter image file that can directly be accessed by the current browser.

    Note:

    - You can upload the vRouter image to an ImageStore or Ceph backup storage.
    - A local browser will serve as a transmission relay used for uploading the vRouter image . Do not refresh or stop the current browser, and do not stop your management node. Or otherwise, you will fail to add the vRouter image.

Figure 7-84: Add VPC vRouter Image



Add an LB Image (KVM)

Set the following parameters:

- **Name**: Enter a name for the vRouter image.
- **Description**: Optional. Enter a description for the vRouter image.
- **Image Usage**: Specify what the vRouter image is used for. Here, select **Dedicated-Performance LB**.
- **Backup Storage**: Select a backup storage to store the vRouter image.
- **Image Path**: Enter a URL or upload a local file.

  — **URL**: Enter the download URL of the vRouter image.

  ZStack Cloud provides you with LB images (KVM). You can download the latest vRouter images from the official website.

  - Software: ZStack-SLB-4.3.12.qcow2
  - Download address: *Click here*

  Note:

  - ImageStore backup storages support breakpoint resume. If the connection is interrupted due to network fluctuations and other reasons, the upload task will be automatically suspended.

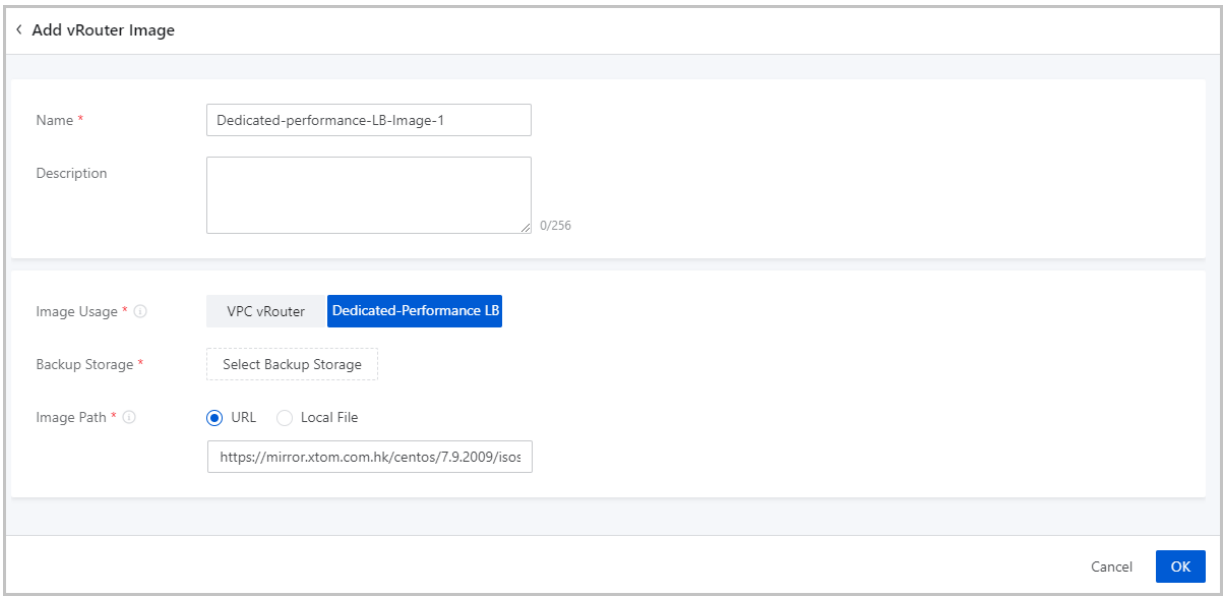
- You can cancel, suspend, or continue the task by going to **Platform O&M** > **Message Log** > **Event Center** > **Operation Log** > **Current Task** > **Add Image** > **Actions**.

— **Local File**: Upload a vRouter image file that can directly be accessed by the current browser.

Note:

- You can upload the vRouter image to an ImageStore or Ceph backup storage.
- ImageStore backup storages support breakpoint resume. If you refresh the browser, close the browser, or stop the management node service, the task will be automatically suspended. Otherwise, the upload task will fail.
- You can cancel, suspend, or continue the task by going to **Platform O&M** > **Message Log** > **Event Center** > **Operation Log** > **Current Task** > **Add Image** > **Actions**.

Figure 7-85: Add LB Image



7.3.7 vRouter Offering

7.3.7.1 What is vRouter Offering?

A vRouter offering defines the number of vCPU cores, memory size, image, management network , and public network configuration settings of VPC vRouters. You can use a vRouter offering to create VPC vRouters that can provide network services for public networks and VPC networks . You can use a vRouter offering to create multiple VPC vRouters. These VPC vRouters share the same public network and management network defined in the vRouter offering. The public

network and management network defined in the vRouter offering cannot be detached from the VPC vRouters.

7.3.7.2 Create a vRouter Offering

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **vRouter** > **vRouter Offering**. On the **vRouter Offering** page, click **Create vRouter Offering**. Then, the **Create vRouter Offering** page is displayed.

On the displayed page, set the following parameters:

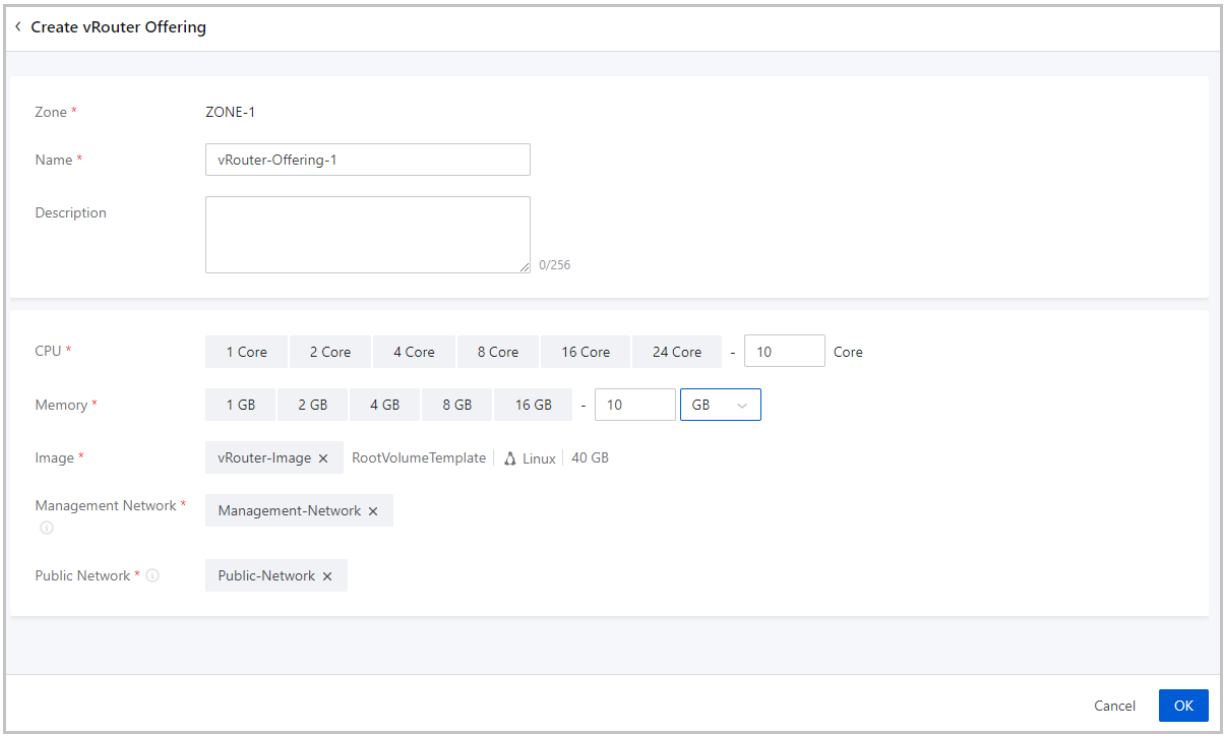
- **Name**: Enter a name for the vRouter offering.
- **Description**: Optional. Enter a description for the vRouter offering.
- **CPU**: Set the number of CPU cores for a vRouter.

  Note:
  Currently, a vRouter can have up to 240 CPU cores. In an actual production environment, we recommend that you set more than 8 CPU cores for a vRouter.
- **Memory**: Set the memory size for a vRouter. Unit: MB, GB, and TB. In an actual production environment, we recommend that the memory size greater than 8 GB.
- **Image**: Select a vRouter image you added before.

  Note:
  If the L3 public network in the vRouter offering has a network range of the IPv6 type, when you create a VPC vRouter, you must use the vRouter image of version 3.10.0 or later.
- **Management Network**: Select an L3 management network you created before.
- **Public Network**: Select a public network you created before.

  — vRouters created from this vRouter offering can provide VPC network services.

Figure 7-86: Create vRouter Offering



7.3.8 SDN Controller

7.3.8.1 What is SDN Controller?

An SDN controller is used to control network devices such as switches. You can add an external SDN controller to the Cloud and use the controller to control external switches and other network devices. By adding an SDN controller, you can take over SDN networks of hardware switches to reduce network latencies and improve VXLAN network performances.

- Before you can add an SDN controller to the Cloud, plan for management networks in advance , and complete the basic configurations of the SDN controller.
- Currently, the Cloud supports only H3C VCFC SDN controllers.

Note:

If you use VCFC to configure hardware SDN, configure the mapping between VLAN and VXLAN on VCFC in advance.

7.3.8.2 Add an SDN Controller

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Resource** > **SDN Device** > **SDN Controller**. On the **SDN Controller** page, click **Add SDN Controller**. Then, the **Add SDN Controller** page is displayed.

On the displayed page, set the following parameters:

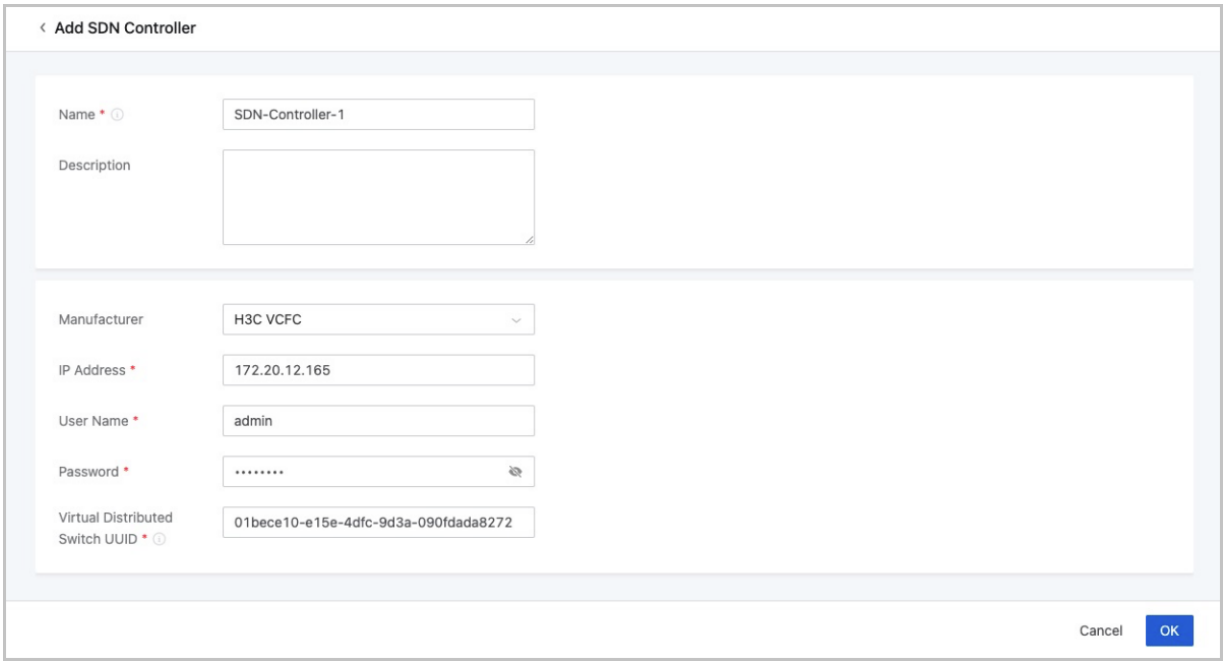
- **Name**: Enter the name of the SDN controller.

  The name must be 1 to 128 characters in length and can contain Chinese characters, English letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the SDN controller.
- **Manufacturer**: Select the SDN controller manufacturer. Currently, only H3C VCFC is supported.
- **IP Address**: Enter the IP address of the SDN controller.
- **User Name**: Enter the user name of the SDN controller.
- **Password**: Enter the password of the SDN controller.
- **Virtual Distributed Switch UUID**: Enter the UUID of the virtual distributed switch.

  Note:

  - You need to configure a virtual distributed switch on the SDN controller in advance.
  - With this virtual distributed switch, an available VNI range of the hardware SDN VXLAN Pool can be determined.

Figure 7-87: Add SDN Controller



7.4 Network Service

ZStack Cloud provides VM instances with multiple network services, including VPC firewall, security group, virtual IP address (VIP), elastic IP address (EIP), port forwarding, IPsec tunnel, load balancing, OSPF area, Netflow, port mirror, and route table.

ZStack Cloud supports the following two network models:

- Flat network
- VPC network

Network Service Module

Network Service Module provides a group of network services. Note that this module has been hidden on the UI.

Network Service Module has the following four types:

1. Virtual Router Network Service Module (Not recommended)

   Provides various network services: DNS, SNAT, load balancing, port forwarding, EIP, and DHCP.

2. Flat Network Service Module (Flat Network Service Provider)

   Provides the following network services:

- User Data: Injects user data, such as `ssh-key`. By running `cloud-init`, user data will be loaded into your VM instance and executed when the VM instance is started.
- EIP: Is realized by distributed EIP to access private networks through public networks.
- DHCP: Is realized by distributed DHCP to dynamically obtain an IP address.

> **Note:**
> The DHCP service includes the DNS feature.

- VIP QoS: Adjusts the upstream bandwidth and downstream bandwidth, and can only be applied to EIPs.

3. VPC vRouter Network Service Module

   Provides the following network services:

   - IPsec: Achieves VPN connections.
   - vRouter route table: Manages custom routes.
   - Centralized DNS: Is provided when the distributed DHCP service is enabled.
   - VIP QoS: Adjusts the upstream bandwidth and downstream bandwidth.
   - DNS: Uses VPC vRouters to provide the DNS service.
   - SNAT: Enables VM instances to access the Internet directly.
   - Load balancing: Distributes inbound traffics from a VIP to a group of backend VM instances . Then, unavailable VM instances will be detected and isolated automatically.
   - Port forwarding: Forwards port traffics of specified public IP addresses to the ports of corresponding VM instances according to specified protocols.
   - EIP: Uses VPC vRouters to access private networks of VM instances through public networks.
   - DHCP: Provides the centralized DHCP service.

4. Security Group Network Service Module

   Provides the following network service:

   - Security group: Manipulates securities of VM instance firewalls by using iptables.

Flat Network Practice

In your production environments, we recommend that you use the following combination of network services:

- Flat Network Service Module

- User Data: Injects user data, such as `ssh-key`. By running `cloud-init`, user data will be loaded into your VM instance and executed when the VM instance is started.
- EIP: Is realized by distributed EIP can access private networks through public networks.
- DHCP: Is realized by distributed DHCP to dynamically obtain an IP address.

> **Note:**
> The DHCP service includes the DNS feature.

- Security Group Network Service Module
  - Security group: Manipulates securities of VM instance firewalls by using iptables.

VPC Network Practice

In your production environments, we recommend that you use the following combination of network services:

- Flat Network Service Module
  - User Data: Injects user data, such as `ssh-key`. By running `cloud-init`, user data will be loaded into your VM instance and executed when the VM instance is started.
  - DHCP: DHCP allows you to dynamically obtain an IP address.
- vRouter Network Service Module
  - DNS: Uses vRouters to provide the DNS service.
  - SNAT: Allows VM instances to access directly the Internet.
  - vRouter route table: Manages custom routes.
  - EIP: Uses vRouters to access private networks of VM instances through public networks.
  - Port forwarding: Forwards port traffics of specified public IP addresses to the ports of corresponding VM instances according to specified protocols.
  - Load balancing: Distributes inbound traffics from a VIP to a set of backend VM instances. Then, unavailable VM instances will be detected and isolated automatically.
  - IPsec: Achieves VPN connections.
- Security Group Network Service Module
  - Security group: Manipulates securities of VM instance firewalls by using iptables.

VPC Network Practice

In your production environments, we recommend that you use the following combination of network services:

- Flat Network Service Module
  - User Data: Customizes some parameters, such as `ssh-key` injection. By running `cloud-init`, these parameters will be loaded and injected into your VM instance when the VM instance is started.
  - DHCP: Is realized by distributed DHCP to dynamically obtain an IP address.
- VPC vRouter Network Service Module
  - DNS: Uses VPC vRouters to provide DNS services.
  - SNAT: Allows VM instances to access directly the Internet.
  - vRouter route table: Manages custom routes.
  - EIP: Uses VPC vRouters to access private networks of VM instances through public networks.
  - Port forwarding: Forwards port traffics of specified public IP addresses to the ports of corresponding VM instances according to specified protocols.
  - Load balancing: Distributes inbound traffics from a VIP to a set of backend VM instances, and unavailable VM instances will be detected and isolated automatically.
  - IPsec: Achieves VPN connections.
- Security Group Network Service Module
  - Security group: Manipulates securities of VM instance firewalls by using iptables.

Advanced Network Services

- Dynamic routing: Uses the Open Shortest Path First (OSPF) routing protocol to distribute routing information within a single autonomous system. This service applies to VPC network scenarios.
- Multicast routing: Forwards the multicast information sent by the multicast source to VM instances, achieving one-to-multi-point communication in the transmission side and receiving side. This service applies to VPC network scenarios.
- VPC firewall: Filters the south-north traffic on the VPC vRouter ports, effectively protecting the VPC communication security and VPC vRouter security. This service applies to VPC network scenarios.
- Port mirroring: Copies and sends network traffics of VM NICs from a port to another port, and analyzes the business packets on the ports, better monitoring and managing the network data. This service applies to flat network, vRouter network, and VPC network scenarios.

- Netflow: Monitors and analyzes the inbound and outbound traffics of the VPC vRouter NICs. Currently, the following two types of data-flow output formats are supported: Netflow V5 and Netflow V9. This service applies to VPC network scenarios.

7.4.1 Security Group

7.4.1.1 What is Security Group?

A security group provides security control services for VM instances on the L3 network. It filters the ingress or egress TCP, UDP, and ICMP packets of specified VM instances in specified networks based on the specified security rules.

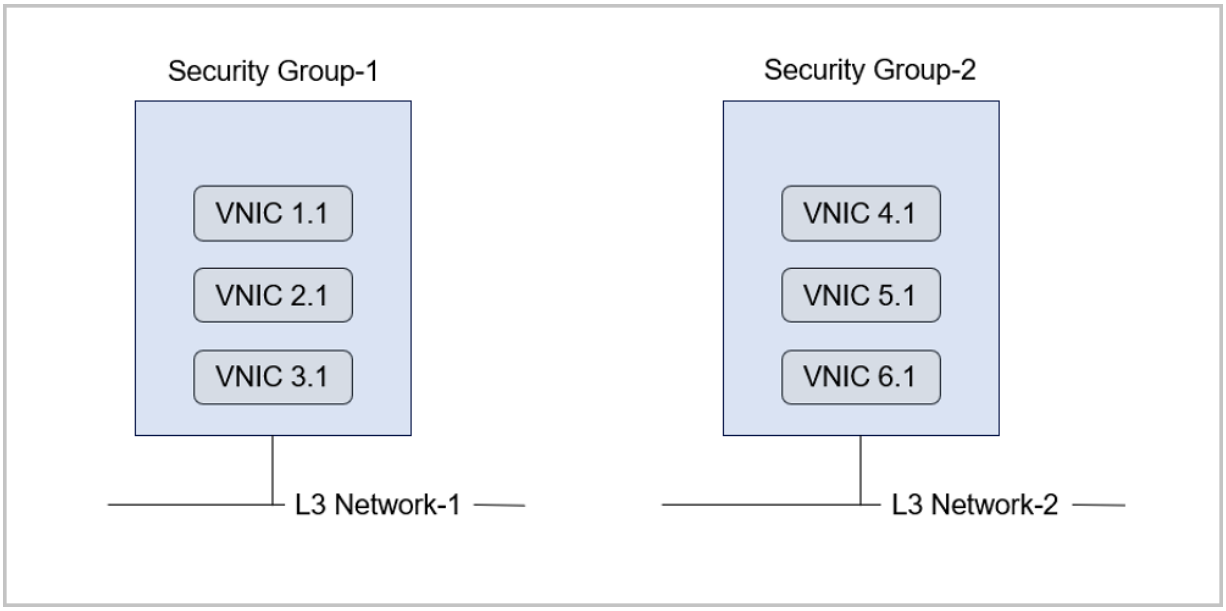
Characteristics

- A security group rule can be categorized into the following two types based on the packet flow direction:
  - Ingress: indicates data packets that flow into a VM instance.
  - Egress: indicates data packets that are sent from a VM instance.
- Security group rules support the following communication protocols:
  - ALL: indicates all types of protocols. If you select ALL, you cannot specify a port.
  - TCP: allows you to specify a port that ranges from 1 to 65535.
  - UDP: allows you to specify a port that ranges from 1 to 65535.
  - ICMP: start port and end port defaulted to -1. This protocol indicates all ICMP messages are supported.
- You can specify data sources in a security group rule to limit data access:
  - If you specify a CIDR block, only the ingress data from the CIDR block or egress data to the CIDR block is allowed.
  - If you specify a security group, only the ingress data from the security group or egress data to the security group is allowed.

Note:

If you specify both a CIDR block and a security group, only the ingress data from the intersection of the security group and CIDR block or egress data to the intersection of the security group and CIDR block is allowed.

Figure 7-88: Security Group



Considerations

- You can assign a security group to one or more VM instances. These VM instances share the same security group rules.
- You can associate a security group with one or more L3 networks. These L3 networks share the same security group rules.
- Security groups apply the whitelist mechanism. Only the traffic that follows the created rules is allowed to reach the specified ports.
- When you create a security group, the system automatically configures two rules (an ingress rule and an egress rule whose protocol types are both ALL) for communications of VM instances in the security group. You can delete these two default rules to cancel the intra-group communication.
- When you create a security group, if you do not set a rule, ingress traffic is not allowed to access VM instances in the security group. However, egress traffic from VM instances in the security group is allowed.
- If you use a security group along with other network services, such as load balancing and vRouter table, make sure that the security group rules required by these network services are added to the security group.
- Public networks, flat networks, and VPC networks support the security group service. It is provided by the security group network service module, which uses iptables to implement security control.

- A security group is a distributed firewall. Each security rule change, NIC association or disassociation will cause the security group rule to be updated on all associated VM instances.

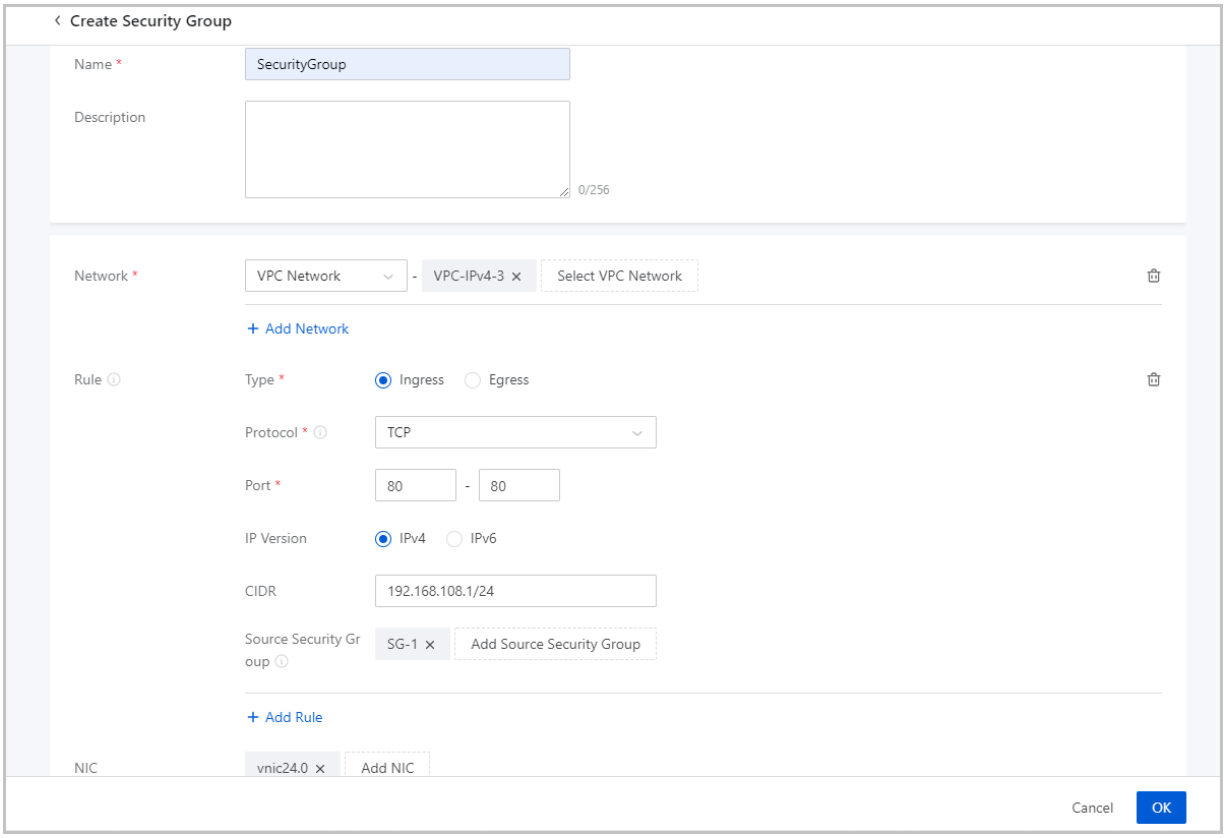
7.4.1.2 Create a Security Group

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Basic Network Service** > **Security Group**. On the **Security Group** page, click **Create Security Group**. Then, the **Create Security Group** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the security group.
- **Description**: Optional. Enter a description for the security group.
- **Network**: Select an L3 network you created. The L3 network can be a public network, flat network, or a VPC network.
- **Rule**: Optional. Add an ingress rule or egress rule for the security group. You can also add a rule after you create the security group.
- **NIC**: Optional. Add a NIC to the security group. You can also add a NIC after you create the security group.

Figure 7-89: Create Security Group



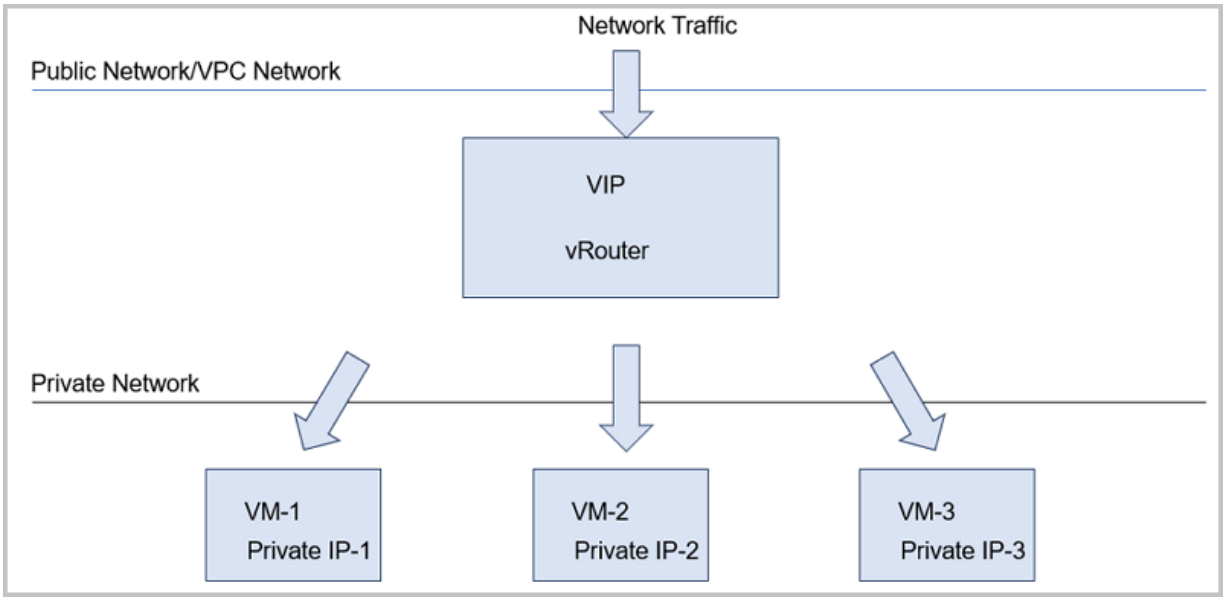
7.4.2 Virtual IP

7.4.2.1 What is Virtual IP?

In bridged network environments, a virtual IP address (VIP) provides network services such as serving as an elastic IP address (EIP), port forwarding, load balancing, IPsec tunneling. When a VIP provides the preceding network services, packets are sent to the VIP and then routed to the destination network where VM instances are located.

- VIPs created from a public network can provide network services such as EIP and load balancing for flat networks.
- VIPs created from a public network can provide network services, such as EIP, port forwarding , load balancing, and IPsec tunnel, for VPC networks.
- VIPs created from a VPC network can provide load balancing services for VPC networks.
- VIPs created from a flat network can provide network services, such as EIP and load balancing , for flat networks.

You can use a VIP to provide performance-shared load balancing services. A performance-shared load balancer uses a VPC vRouter to provide load balancing services. Traffic is distributed to backend servers by the VPC vRouter. If the VPC vRouter is providing multiple services, the load balancing service shares the performance of the VPC vRouter along with other services.



Concepts

- Public VIP: VIPs created from a public network. You can manually create a public VIP or use a public VIP automatically created after a VPC vRouter creation.

- A public VIP can provide network services, such as EIP and load balancing, for flat networks . A public VIP can also provide network services, such as EIP, port forwarding, load balancing, and IPsec tunnel, for VPC networks.
- You can use a public VIP to simultaneously provide port forwarding, load balancing, and IPsec tunnel services. However, you cannot specify the same port number for different services. You can also use a public VIP to provide one service for multiple VM instances.
- A public VIP supports QoS, monitoring data, performance TOP 5, performance analysis, alarm, and other features.

• VPC VIP: VIPs created from a VPC network. A VPC VIP can only be manually created.

- A VPC VIP can provide load balancing services for VPC networks.
- VPC VIPs do not support QoS, monitoring data, performance TOP 5, performance analysis, and alarm features.

• Flat network VIP: VIPs created from a flat network. You can manually create a flat network VIP or use a flat network VIP automatically created after a VPC vRouter creation.

- A flat network VIP provides network services, such as EIP and load balancing, for flat networks.
- A flat network VIP supports QoS, monitoring data, performance TOP 5, performance analysis, alarm, and other features.

• Custom VIP: manually created VIPs. You can customize a public VIP, VPC VIP, and flat network VIP based on your needs.

- One custom public VIP can only be applied to one EIP instance.
- Custom VIPs cannot be used across VPC vRouters.
- When you use the EIP, port forwarding, load balancing, or IPsec tunnel services, you can select **Create VIP** to create a new VIP, or you can select **Use Existing VIP** to provide the services.

• System VIP: VIPs automatically created by using the L3 network attached to VPC vRouters after the VPC vRouter creation. System VIPS can be categorized into public VIPs and flat network VIPs.

- A system VIP belongs to only one VPC vRouter. When you attach a public network to a VPC vRouter, the Cloud will automatically create a system VIP. This VIP is the default IP address of the vRouter in the network.

- By default, the system VIPs created from public networks are used to provide the source network address translation (SNAT) service.
- When you use the EIP, port forwarding, load balancing, or IPsec tunnel service, you can select **Use Existing IP** to provide the services.

7.4.2.2 Create a Virtual IP

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Basic Network Service** > **VIP**. On the **VIP** page, click **Create VIP**. Then, the **Create VIP** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the virtual IP address (VIP).
- **Description**: Optional. Enter a description for the VIP.
- **Network**: Select an L3 network you created. The L3 network can be a public network, flat network, or a VPC network.
  - VIPs created in a public network can provide EIP and load balancing services for flat networks.
  - VIPs created in a public network can provide EIP, port forwarding, load balancing, and IPsec tunnel network services for VPC networks.
  - VIPs created in a VPC network can provide load balancing services for VPC networks.
  - VIPs created in a flat network can provide EIP and load balancing services for flat networks.
- **Network Range**: Optional. Select a network range.

  Note:

  - If you selected an IPv4 public network, you can select a normal network range or an address pool. If you selected an IPv6 public network, you can only select a normal network range.
  - If you selected an IPv4 or IPv6 public network, you can only select a normal network range.
  - If you selected an IPv4 VPC network, you can only select a normal network range.
- **Assign IP**: Optional. You can assign a virtual IP address.

  Note:

  If left blank, the system automatically assigns a VIP.

- **VIP QoS**: You can limit the network bandwidth of public VIPs and flat network VIPs. You can set the QoS for a custom VIP when you create the VIP or after the VIP is created.

  Note:

  - You can set multiple QoS rules for a public VIP and flat network VIP. The QoS rule in which the port is unspecified has the lowest priority.
  - You cannot set QoS rules for a VPC VIP.

  — **Add VIP QoS**: Optional. You can set multiple QoS rules for a VIP.

  — **Port**: Optional. Specify a port to set QoS rule for the port.

  Note:

  - Enter an integer that ranges from 1 to 65535.
  - If left blank, the QoS rule takes effect on ports from 1 to 65535.

  — **Upstream Bandwidth**: Optional. Set the upstream bandwidth for a VIP.

  Note:

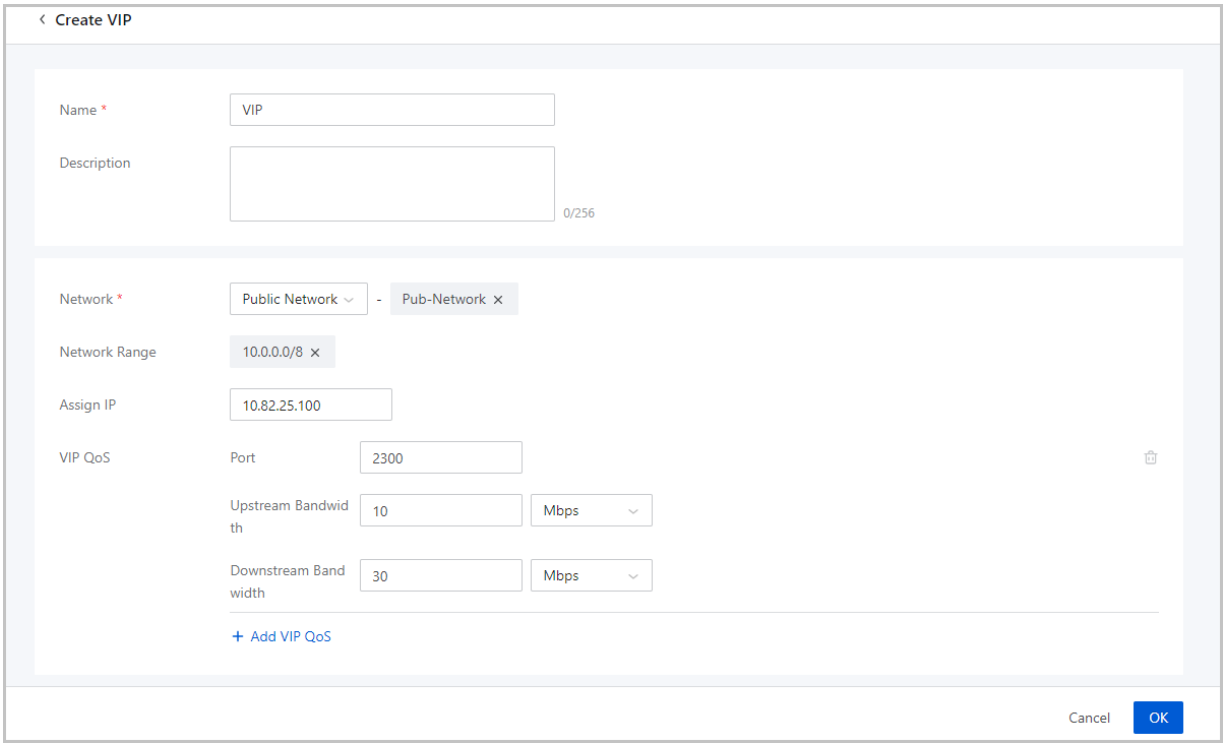
  - Enter an integer. Unit: Kbps, Mbps, and Gbps.
  - If left blank, the upstream bandwidth is not limited.

  — **Downstream Bandwidth**: Optional. Set the downstream bandwidth for a VIP.

  Note:

  - Enter an integer. Unit: Kbps, Mbps, and Gbps.
  - If left blank, the downstream bandwidth is not limited.

Figure 7-90: Create VIP



7.4.3 Elastic IP

7.4.3.1 What is Elastic IP?

An elastic IP address (EIP) functions based on the NAT technology. IP addresses in a private network are translated into an EIP that is in another network. This way, private networks can be accessed from other networks by using EIPs.

Concepts

- Public EIP: The EIP service provided by a virtual IP address (VIP) created from a public network.
  - The private network is an isolated network that cannot be directly accessed from other networks or the Internet. A public EIP can directly associate the access to a public network with the VM IP of the private network.
  - A public EIP can be associated with or disassociated from a VM instance dynamically.
  - A public EIP can be associated with VM instances created from private networks, such as flat networks and VPC networks.
    - The public EIP realized by a distributed EIP can access flat networks through public networks.

- A VPC vRouter can be used to access VPC networks through public networks.

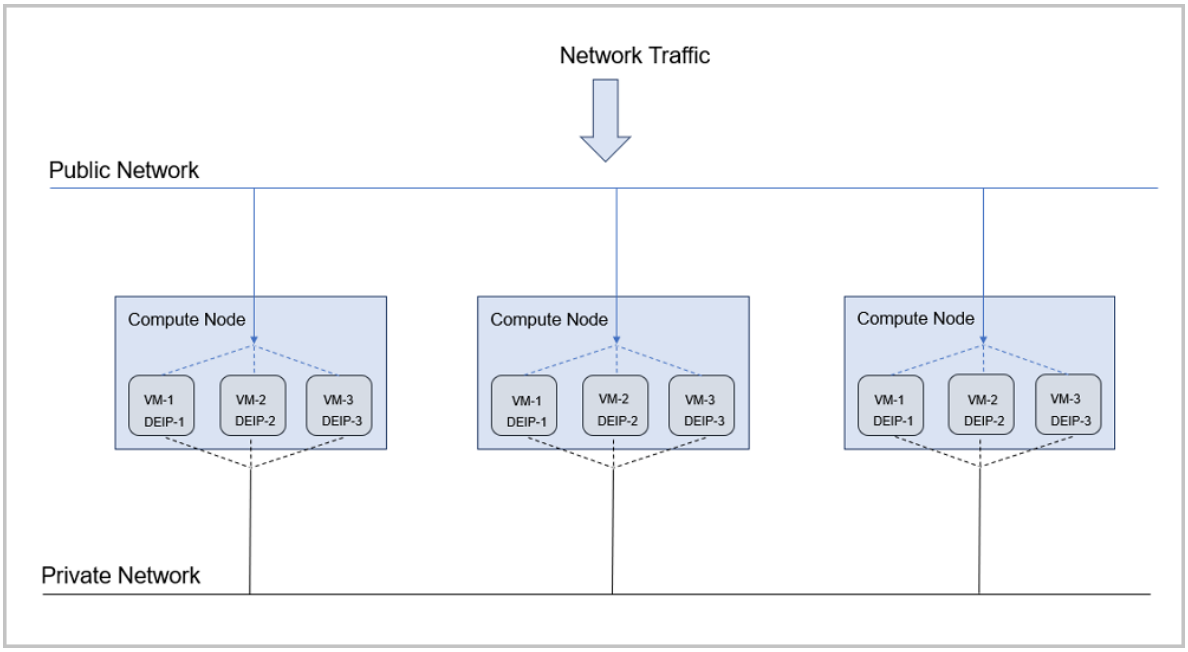
- Flat EIP: The EIP service provided by a VIP created from a flat network.
  - L3 isolations exist between flat networks of different network ranges. Therefore, these flat networks cannot be accessed directly. A flat EIP can be used to associate the access to one flat network with the VM IP created from another flat network.
  - A flat EIP can be associated with or disassociated from a VM instance dynamically.
  - A flat EIP can be associated with VM instances created from other flat networks.

Scenarios

- EIP usage in a flat network scenario:

  The following diagram shows how an EIP is used in a flat network scenario.

  Figure 7-91: EIP Usage in Flat Network Scenario

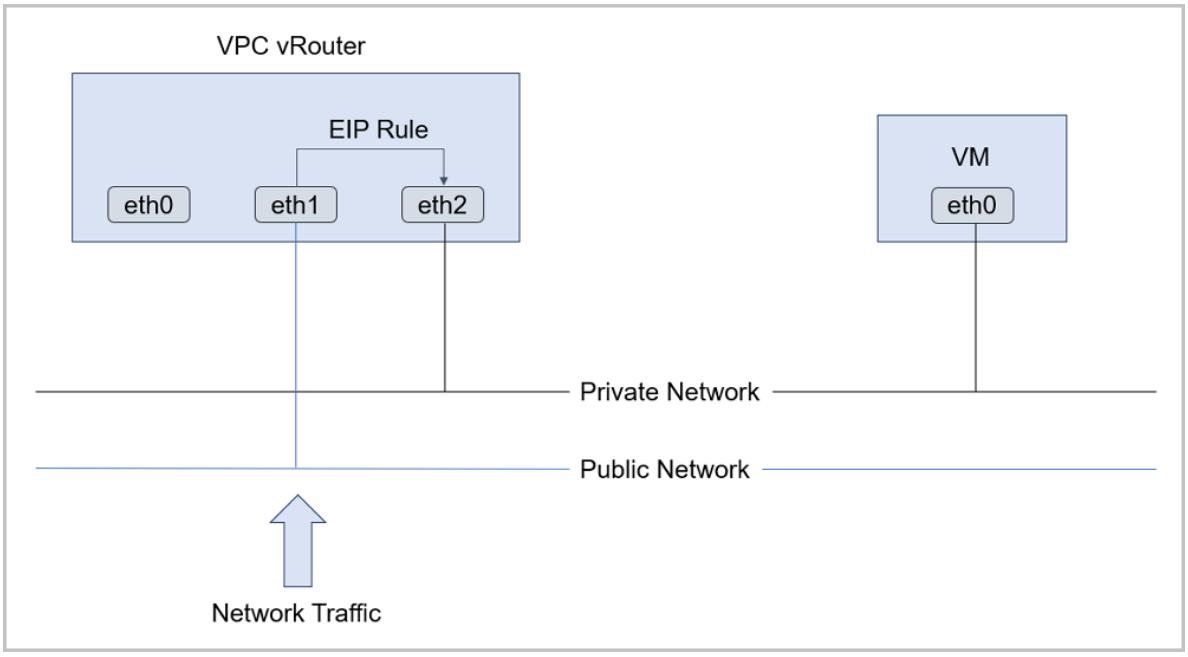


  - Public networks can connect to the Internet through firewalls.
  - Flat networks provide IP addresses for VM instances in each compute node. Notice that these IP addresses cannot connect to the Internet by default.
  - A distributed EIP is deployed on each compute node, and can be associated with public networks or private networks separately.

- EIP usage in a VPC network scenario:

  The following diagram shows how an EIP is used in a VPC network scenario.

Figure 7-92: EIP Usage in VPC Network Scenario



Considerations

When you use an EIP, note that:

- An instance can have only one EIP associated at a time.
- The EIP association and disassociation operations take effect in real time.
- Associating or Disassociating an EIP does not affect the running of an instance.

7.4.3.2 Create an Elastic IP

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Basic Network Service** > **EIP**. On the **EIP** page, click **Create EIP**. Then, the **Create EIP** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the EIP.
- **Description**: Optional. Enter a description for the EIP.
- You can use a virtual IP address by using either of the following methods:
  - **VIP**: Select **Create VIP**.
    - **Network**: Select an L3 network to create a VIP. The network can be a public network or flat network.

- **Network Range**: Optional. Select a network range.

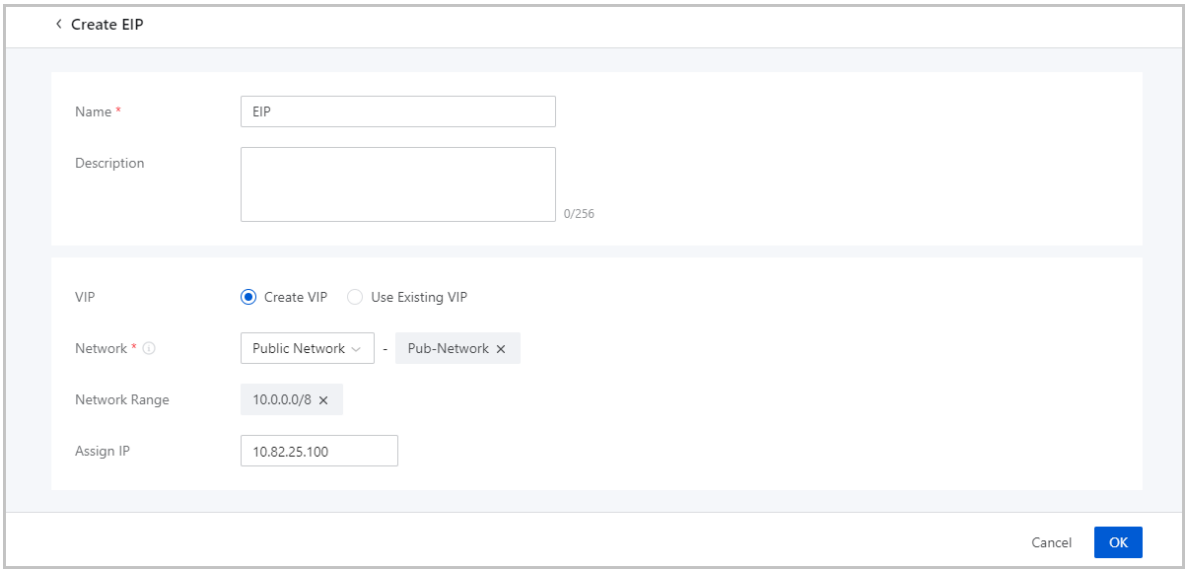
> **Note:**
>
> - If you selected an IPv4 public network, you can select a normal network range or an address pool. If you selected an IPv6 public network, you can only select a normal network range.
> - If you selected an IPv4 or IPv6 public network, you can only select a normal network range.
> - If you selected an IPv4 VPC network, you can only select a normal network range.

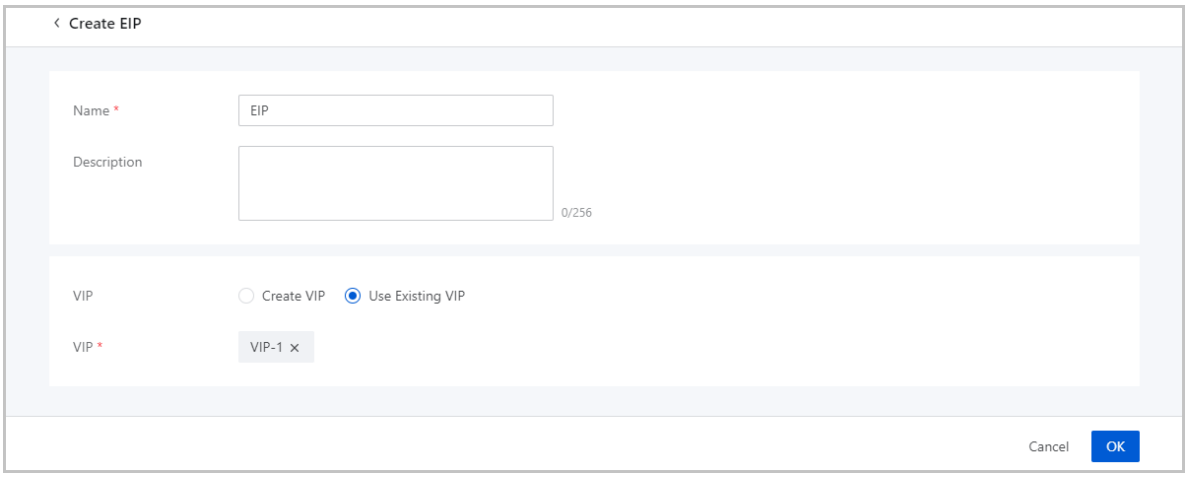
— **VIP**: Select **Use Existing VIP**.

Set the following parameter:

- **VIP**: Select an existing VIP.

Figure 7-93: Create EIP





7.4.4 Port Forwarding

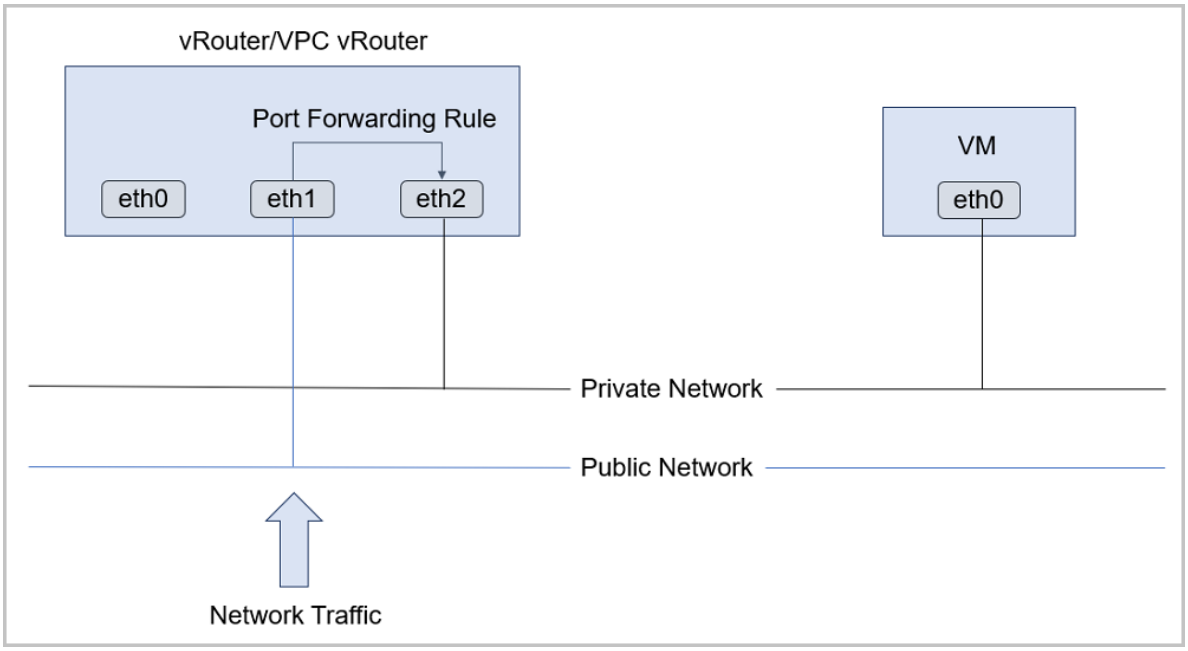
7.4.4.1 What is Port Forwarding?

Port forwarding functions based on the layer-3 forwarding service of VPC vRouters. This service forwards traffic flows of the specified IP addresses and ports in a public network to specified ports of VM instances by using the specified protocol. If your public IP addresses are insufficient, you can configure port forwarding for multiple VM instances by using one public IP address and port.

- VM instances in a private network for which SNAT is enabled can access external networks. However, the VM instances in the private network are inaccessible to external networks. You can use a port forwarding rule to allow access to specified ports of the VM instances from external networks.
- You can associate a port forwarding rule with a VM NIC and disassociate a port forwarding rule from a VM NIC based on your business needs.
- Port forwarding services are provided only by VPC vRouters.

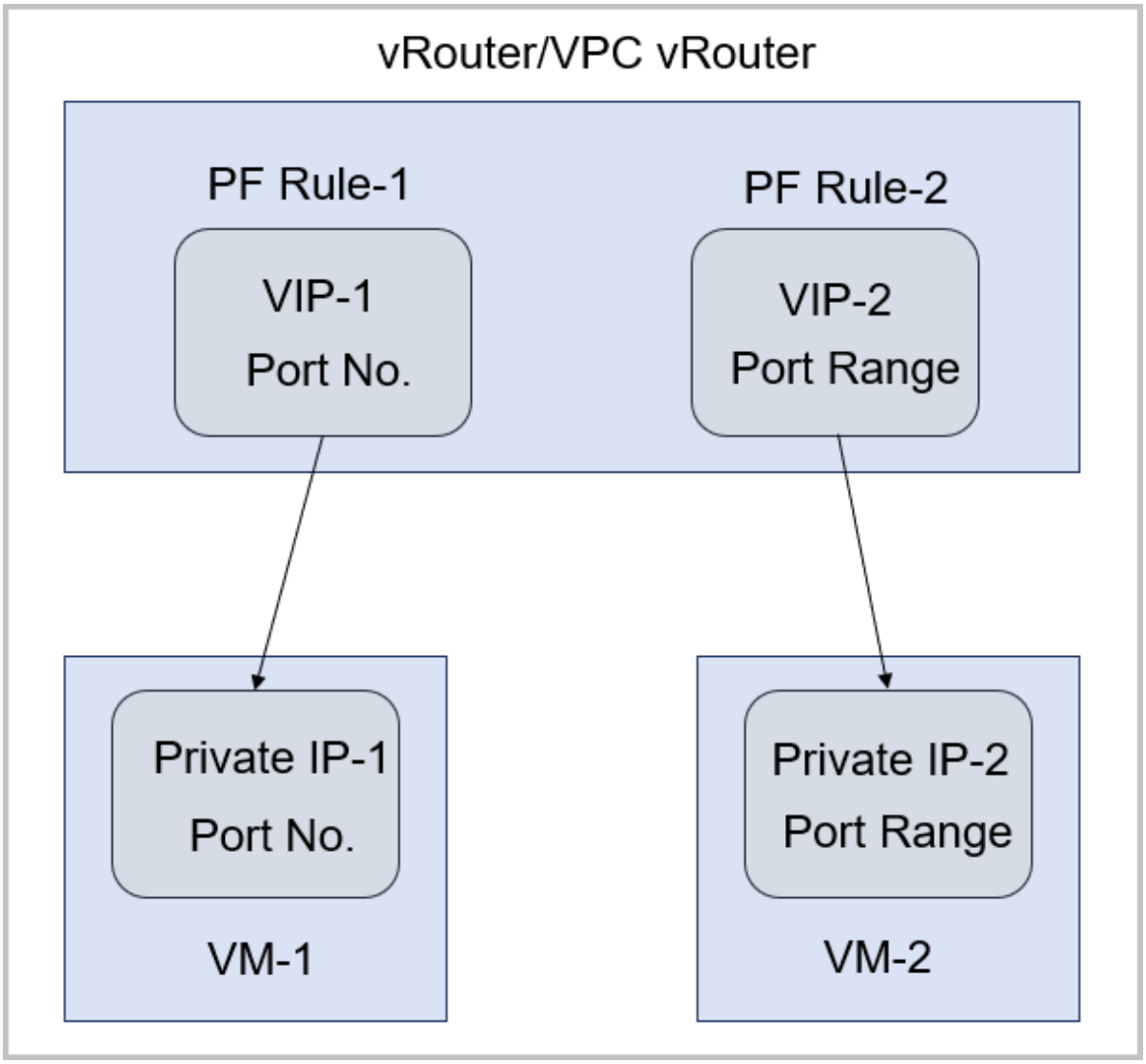
  Port forwarding rules are applied to a public network associated with a VPC vRouter and a private network where VM instances reside, as shown in the following figure.

Figure 7-94: Port Forwarding



- Port forwarding is achieved by using a virtual IP address (VIP).
  - A VIP is an available IP address in a public network.
  - You can use an existing VIP or create a VIP to provide port forwarding services.
  - Two port forwarding methods are supported: port-to-port mapping and port range-based mapping.

Figure 7-95: VIP-Port Forwarding



Limits

The port forwarding service has the following limits:

- The firewall policy of a VM instance must open the port specified for port forwarding.
- The ports used for port forwarding by the same VIP must be unique.
- You can use a VIP to provide port forwarding services for different ports of multiple VM NICs in the same L3 network.
- You can use only one VIP to provide port forwarding services for a VM instance.
- If you disassociate a VIP from a VM instance and then associate the VIP with a VM instance, you can select VM NICs that reside in the same L3 network as the previously disassociated VM instance.

- The source port range and target port range used for port forwarding must be consistent. For example, if you set the source port range to 22-80, the target port range must also be 22-80.

7.4.4.2 Create a Port Forwarding Rule

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Basic Network Service** > **Port Forwarding**. On the **Port Forwarding** page, click **Create Port Forwarding**. Then, the **Create Port Forwarding** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the port forwarding rule.

  The name must be 1 to 128 characters in length and can contain letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the port forwarding rule.
- **VIP**: You can create a VIP or use an existing VIP to provide port forwarding services.

  — **Create VIP**: Create a VIP. If you select to create a VIP, set the following parameters:

    - **Network**: Select a public network to create a VIP.
    - **Network Range**: Optional. Select a network range. If you selected an IPv4 public network, you can select a normal network range or an address pool.
    - **Assign IP**: Optional. You can assign a virtual IP address. If left blank, the system automatically assigns a VIP.

  — **Use Existing VIP**: Use an existing VIP. If you select to use an existing VIP, set the following parameters:

    - **VIP**: Select an existing VIP.

  Note:
  The system VIP of a VPC vRouter can be used to provide port forwarding services.
- **Protocol**: Select a protocol, Valid values: TCP and UDP.

  — TCP: supports ports 0-65535.

  — UDP: supports ports 0-65535.
- **Port**: Select a port mapping method.

  Two port mapping methods are supported: port-to-port mapping and port range-based mapping .

— **Specified Port**: If you specify ports, set the following parameters:

- **Source Port**: Select a port from ports 0-65535 as the source port.
- **VM Port**: Select a port from ports 0-65535 as the VM port.

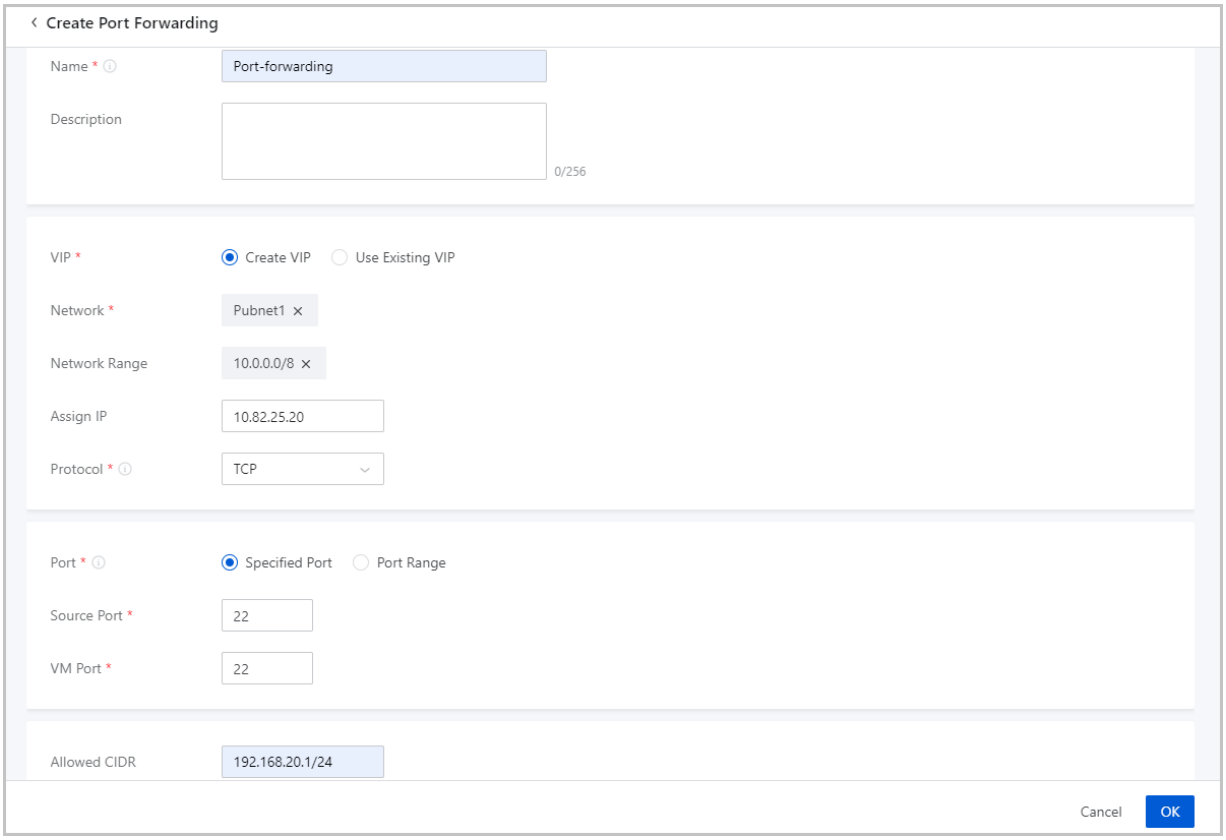
For example, if you set 24 as the source port and 22 as the VM port, the traffic to port 24 of the public IP will be forwarded to port 22 of the VM instance.

— **Port Range**: Select two ports from ports 1-65535 as the start port and end port, respectively.

For example, if the port range is 22-80, traffic to ports 22-80 of the public IP will be forwarded to ports 22-80 of the VM instance.

- **Allowed CIDR**: Optional. You can specify a CIDR block to allow access to only this CIDR block.

Figure 7-96: Create Port Forwarding Rule



7.4.5 Load Balancing

7.4.5.1 What is Load Balancer?

A load balancer distributes traffic flows of a virtual IP address to backend servers. It automatically inspects the availability of backend servers and isolates unavailable servers during traffic distributi on. This way, the load balancer improves the availability and service capability of your business.

The Cloud provides the following two types of load balancing services:

- Shared-performance load balancing: uses a VPC vRouter to provide load balancing services. Traffic is distributed to backend servers by the VPC vRouter. If the VPC vRouter is providing multiple services, the load balancing service shares the performance of the VPC vRouter with other services.
- Dedicated-performance load balancing: uses a load balancer instance to provide load balancing services. Traffic is distributed to backend servers by the load balancer instance. A load balancer instance is a custom VM instance dedicated to providing load balancing services.

Concepts

- Frontend network: A frontend network is a type of network that is associated with a load balancer. Requests from the network are distributed by the load balancer to backend servers based on a specified policy.
  - Shared-performance load balancer: You can specify a public network or VPC network as a frontend network.
  - Dedicated-performance load balancer: You can specify a public network, flat network, or VPC network as a frontend network.
- Backend network:A backend network is a type of network that is associated with a load balancer. Requests from frontend networks are distributed by the load balancer to servers in the backend network.
  - Shared-Performance Load Balancer:
    - If you specify a public network as the frontend network, you can specify any one of the VPC networks of the VPC vRouter to which the public network is attached as the backend network.
    - If you specify a VPC network as the frontend network, you can specify any one of the VPC networks of the VPC vRouter to which the VPC network is attached as the backend network.

- Dedicated-Performance Load Balancer:
  - If you specify a public network as the frontend network, you can specify a flat network or any one of the VPC networks of the VPC vRouter to which the public network is attached as the backend network.
  - If you specify a flat network as the frontend network, you must specify the same network as the backend network.
  - If you specify a VPC network of a VPC vRouter as the frontend network, you must specify the same network as the backend network. If you need to associate the load balancer with more backend networks, you can attach more NICs to the load balancer instance. Note that the backend networks that you associate are among the other VPC networks of the VPC vRouter.

- Load balancer instance: A load balancer instance is a custom VM instance used to provide load balancing services.
  - The network where the default NIC of a load balancer instance resides is the frontend network of the load balancer instance. The default NIC cannot be detached from a load balancer instance.
  - The networks of the NICs of a load balancer instance, except the default NIC, are the backend networks of the load balancer.
  - The management NIC (if any) cannot be detached.
- LB image: A dedicated-performance load balancer (LB) image encapsulates dedicated-performance load-balancing services and can be used to create load balancer instances . However, a dedicated-performance load balancer image cannot be used to create VM instances.
  - An LB image is a custom image. You can download the image from the Cloud official website and add the image to the platform.
- Load balancer instance: A load balancer (LB) instance offering defines the CPU, memory , image, and management network configuration settings used to create LB instances. LB instances provide load balancing services for the public network, flat network, and VPC network.
- Listener: A listener monitors the frontend requests of a load balancer and distributes the requests to a backend server based on the specified policy. In addition, the listener performs health checks on backend servers.
  - Listeners support the TCP, HTTP, HTTPS, and UDP protocols.

  - A load balancer can be associated with multiple listeners while a listener can be associated with only one load balancer.
  - If the listener uses the weighted round-robin load-balancing algorithm, you can set the weight value for each individual backend server on the backend server group details page.
- Forwarding rule: A forwarding rule forwards the requests from different domain names or URLs to different backend server groups.
  - A forwarding rule is composed of a domain name and URL.
  - A listener can have up to 40 forwarding rules.
  - You can configure a domain-based or URL-based forwarding rule for a load balancer. You can add multiple forwarding rules to a listener and associate these rules with different backend server groups.
  - A forwarding rule is matched by using the exact match and fuzzy match mechanisms. If multiple forwarding rules are matched, the forwarding rule matched through the exact match mechanism is used.
- Certificate: If you select HTTPS for a listener, associate it with a certificate to make the listener take effect. You can upload either a certificate or certificate chain.
- Backend server group: A backend server group is a group of backend servers that handles requests distributed by load balancers. It is the basic unit for traffic distribution by load balancer instances.
  - A load balancer can be associated with multiple backend server groups, while a backend server group can be associated with only one load balancer.
  - A backend server group can be associated with multiple listeners in the same load balancer.
  - Creating a load balancer will automatically create an empty backend server group.
- Backend server: A backend server handles requests distributed by a load balancer. You can add a VM instance on the Cloud or a server on a third-party cloud as a backend server.

7.4.5.2 Load Balancer

7.4.5.2.1 Create a Load Balancer

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Basic Network Service** > **Load Balancing**. On the **Load Balancer** page, click **Create Load Balancer**. The **Create Load Balancer** page appears.

The following lists the two load balancer (LB) creation scenarios:

- Create a shared-performance LB
- Create a dedicated-performance LB

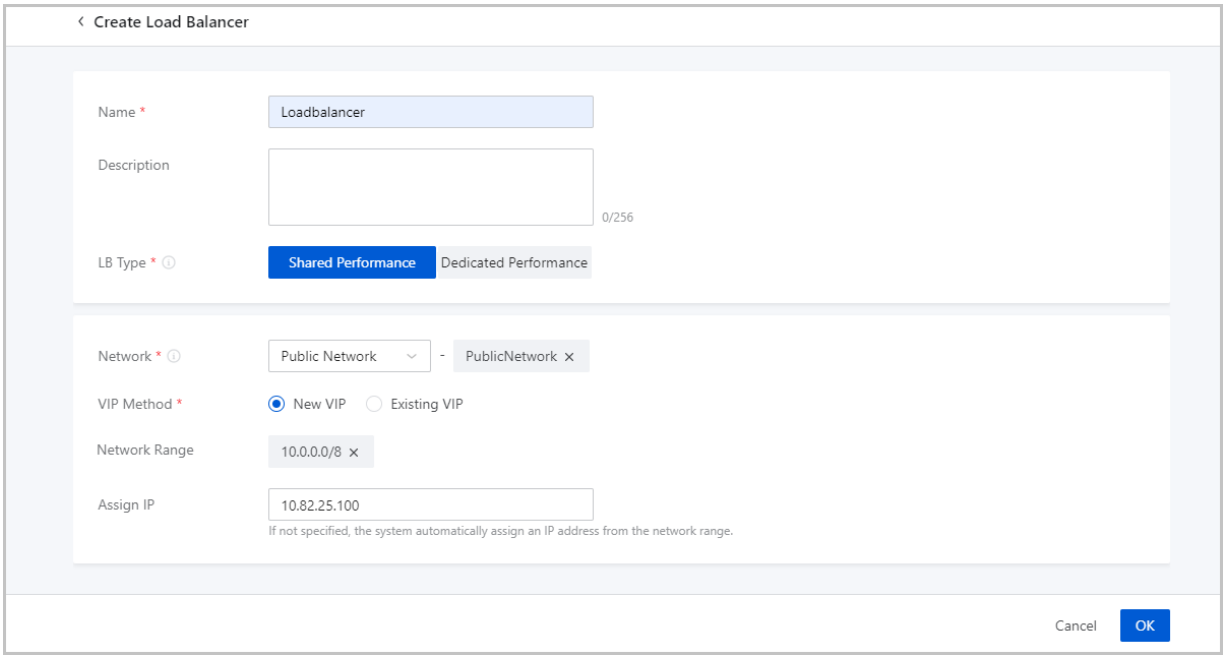
Create Shared-Performance LB

On the displayed page, set the following parameters:

- **Name**: Enter a name for the LB.
- **Description**: Optional. Enter a description for the LB.
- **LB Type**: Select Shared Performance.
  - A shared-performance LB distributes traffics to backend servers by using a VPC vRouter.
  - If the VPC vRouter are providing multiple services, the load balancing service needs to share the performance of the VPC vRouter with other services.
- **Network**: Select a network as the frontend network of the LB. You can select a public network or VPC network.

  Requests from the frontend network are distributed by the load balancer to backend servers based on a specified policy.
- **VIP Method**: You can create a virtual IP address (VIP) or use an existing VIP to provide load balancing services.
  - **New VIP**: If you create a VIP, you can set the following parameters:
    - **Network Range**: Optional. Select an IP range.
    - **Assign IP**: Optional. Specify a VIP. This parameter is available only after you select an IP range. If left blank, the system automatically assigns a VIP.
  - **Existing VIP**: If you use an existing VIP, you can set the following parameters:
    - **VIP**: Select an existing VIP. You can select a custom VIP or a system VIP:
      - **Custom**: Select a VIP that you create. You can select a VIP in a public network, VPC network, or flat network.
      - **System**: Select a system VIP. After a VPC vRouter is created, the system creates a VIP in the L3 network that is associated with the VPC vRouter. The automatically created VIP can be a public network VIP or a flat network VIP.

Figure 7-97: Create Shared-Performance LB



Create Dedicated-Performance LB

On the displayed page, set the following parameters:

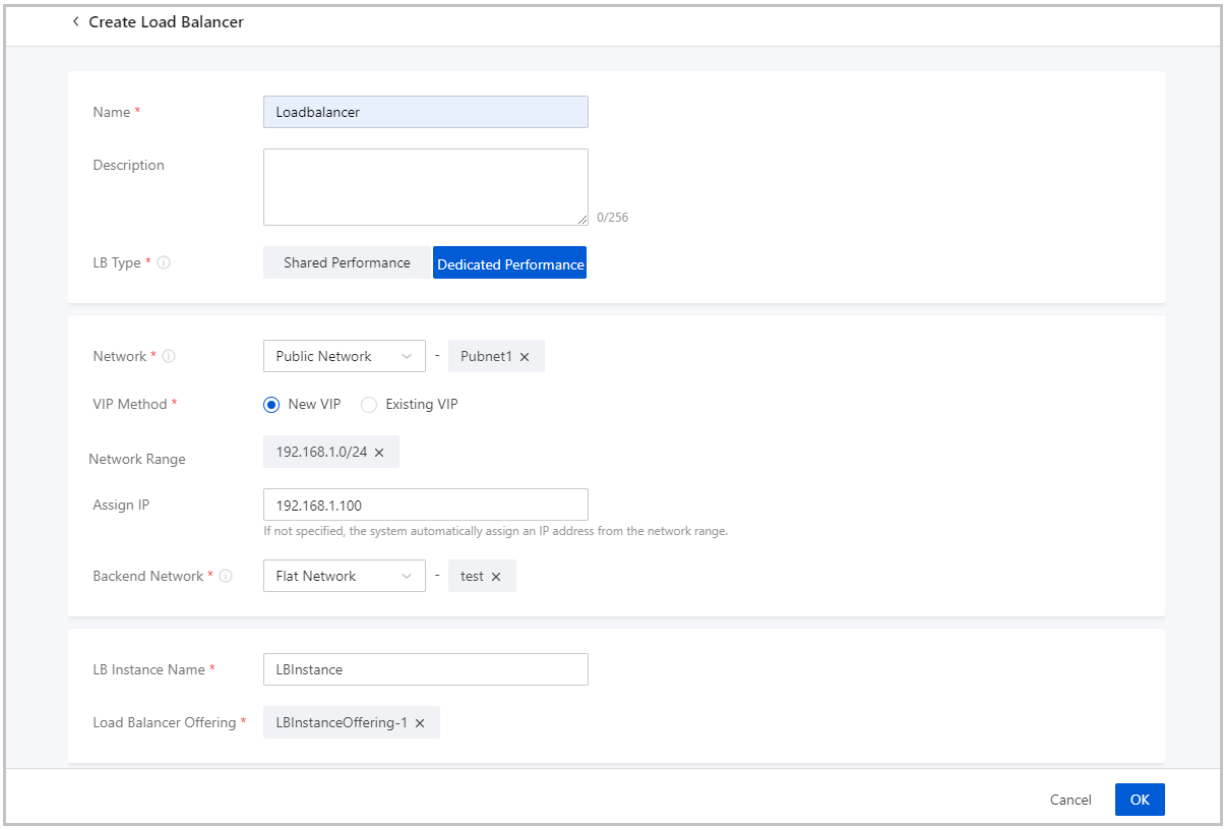
- **Name**: Enter a name for the LB.
- **Description**: Optional. Enter a description for the LB.
- **LB Type**: Select High Performance.
  - A dedicated-performance LB distributes traffics to backend servers by using LB instances.
  - A load balancer instance is a custom VM instance dedicated to providing load balancing services.
- **Network**: Select a network as the frontend network of the LB. You can select a public network, flat network, or VPC network.

  Requests from the frontend network are distributed by the load balancer to backend servers based on a specified policy.
- **VIP Method**: You can create a VIP or use an existing VIP to provide load balancing services.
  - **New VIP**: If you create a VIP, you can set the following parameters:
    - **Network Range**: Optional. Select an IP range.
    - **Assign IP**: Optional. Specify a VIP. This parameter is available only after you select an IP range. If left blank, the system automatically assigns a VIP.

- **Existing VIP**: If you use an existing VIP, you can set the following parameters:
  - **VIP**: Select an existing VIP. You can select a custom VIP or a system VIP:
    - **Custom**: Select a VIP that you create. You can select a VIP in a public network, VPC network, or flat network.
    - **System**: Select a system VIP. After a VPC vRouter is created, the system creates a VIP in the L3 network that is associated with the VPC vRouter. The automatically created VIP can be a public network VIP or a flat network VIP.

- **Backend Network**: Select a network as the backend network.
  - If you specify a public network as the frontend network, you can specify a flat network or any one of the VPC networks of the VPC vRouter to which the public network is attached as the backend network.
  - If you specify a flat network as the frontend network, you must specify the same network as the backend network.
  - If you specify a VPC network of a VPC vRouter as the frontend network, you must specify the same network as the backend network.
- **LB Instance Name**: Enter a name for the LB instance.
- **Load Balancer Offering**: Select a LB offering.

Figure 7-98: Create Dedicated-Performance LB



After you create a LB, you can add a listener and associate VM NICs with the listener to make the LB take effect.

7.4.5.3 Listener

7.4.5.3.1 Create a Listener

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Basic Network Service** > **Load Balancing**. On the load balancer management page, click the target load balancer. On the details page of the load balancer, click the **Listener** tab. On the tab, click **Create Listener**. The **Create Listener** page appears.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the listener.
- **Description**: Optional. Enter a description for the listener.
- **Protocol**: Select a listening protocol. Valid values: TCP, HTTP, HTTPS, and UDP.
  - If you select TCP, HTTP, or UDP, you can select a port that ranges from 1 to 65535.
  - If you select HTTPS:

- You can select a port that ranges from 1 to 65535.
- You need to associate the listener with a certificate. You can upload a certificate or certificate chain. For more information, see *Create a Certificate*.
- **Certificate**: Associate a certificate with the listener.

- **Load Balancer Algorithm**: Set a routing rule for data packets. Default: Round Robin.

  The following lists the supported load balancing algorithms:

  - Round Robin:

    The Round Robin algorithm evenly distributes external requests to each VM instance in sequence that is specified by the load balancing rule regardless of the established connections or system loads of a VM instance.
  - Min Connections:

    The Min Connections algorithm dynamically distributes external requests to VM instances that have established least connections. If VM instances in the cluster have similar system performance, you can use this algorithm to achieve even distribution of workloads.
  - Source IP Hash:

    The Source IP Hash algorithm uses a source IP address as a hash key and maps the hash key to a VM instance based on the mapping in the static hash table. If the VM instance is available and is not overloaded, requests are sent to the instance. Otherwise, no VM instance is returned to handle the requests.
  - Weighted Round Robin:

    The Weighted Round Robin algorithm is generated by combining the Round Robin algorithm with the Weighted algorithm. It assigns a weight to each VM instance and distributes more requests to VM instances with a higher weight. Requests are more likely to be distributed to VM instances with a higher weight.
- **Load Balancer Port**: Specify a port for load balancing. Valid values: 1 to 65535.
- **Backend Server Port**: Specify a backend server port. Valid values: 1 to 65535.

  For example, if you specify port 80 as the load balancing port and port 5000 as the backend server port, requests sent to port 80 of the load balancer (LB) virtual IP address are distributed to the port 8000 of backend servers.
- **Backend Server Group**: Optional. Select a backend server group.

Note:

- A backend server group is a group of backend servers that share the same configurat ions. You can associate one or more listeners with a backend server group. The listeners distribute traffic based on the weight that you assign to each backend server.
- You can associate a listener with one or more backend server groups that are attached to the same LB.
- If a backend server is added to multiple backend server groups, you cannot associate the same listener with these backend server groups.
- After you associate a listener with a backend server group, you can view the health status of the backend server group on the details page of the listener. A backend server group may be in Healthy or Unhealthy status.

- **Advanced**: Configure advanced settings for the listener.
  - **Health Check Protocol**: Set the health check protocol. Valid values: TCP, HTTP, and UDP. You can select a protocol different from the listening protocol.
    - If you select TCP, HTTP, or HTTPS as the listening protocol, you can select TCP or HTTP as the health check protocol.
    - If you select UDP as the listening protocol, you can select UDP as the health check protocol.
    - If you select HTTP as health check protocol, you can configure normal status code, health check URI, and HTTP health check method:
      - **Normal Status Code**: The HTTP status code returned when the health check passes. You can select one or more status codes. Valid values: http_2xx, http_3xx, http_4xx, and http_5xx.
      - **Health Check URI**: The URI of the page on which health checks are performed, for example, `/healthcheck.html`.

        A health check on static pages is recommended. When you set a health check URI, make sure that:

        - The URI must be 2 to 80 characters long.
        - The URI can contain only letters, digits, hyphens (-), forward slashes (/), periods (.), percentage signs (%), question marks (?), number signs (#), ampersands (&),or a combination of these characters.

- The URI must start with a forward slash (/) but it cannot contain only forward slashes.
- **HTTP Health Check Method**: The method used to perform HTTP health checks on server applications. Valid values: HEAD and GET. Default: HEAD. The health check requests simulate the access requests of a browser.

— **Idle Connection Timeout**: The amount of time that the load balancer terminates the connection between the server and the client when no data is transmitted. Default value: 60 seconds.

— **Healthy Threshold**: The maximum number of consecutive successful health checks required for a unhealthy backend server to be considered healthy. Default value: 2.

— **Health Check Port**: The health check port. Default: default. This value indicates that the health check port is the same as the specified backend server port. You can also specify another port.

— **Unhealthy Threshold**: The maximum number of consecutive failed health checks required for a healthy backend server to be considered unhealthy. Default value: 2.

— **Health Check Interval**: The time interval between each health checks of an individual backend server. Default value: 5 seconds.

— **Maximum Concurrent Requests**: The maximum number of concurrent connection requests of the listener. Valid values: 1 to 2000000. Default: 2000000.

> **Note:**
> The memory usage of a running load balancer is associated with the maximum concurrent requests. Excessively high memory usage may cause the out of memory (OOM) error. Set the parameter based on the actual memory size. For example, if you set the maximum concurrent requests of a listener to 2,000,000, the memory usage of the load balancer listener is around 200 MB.

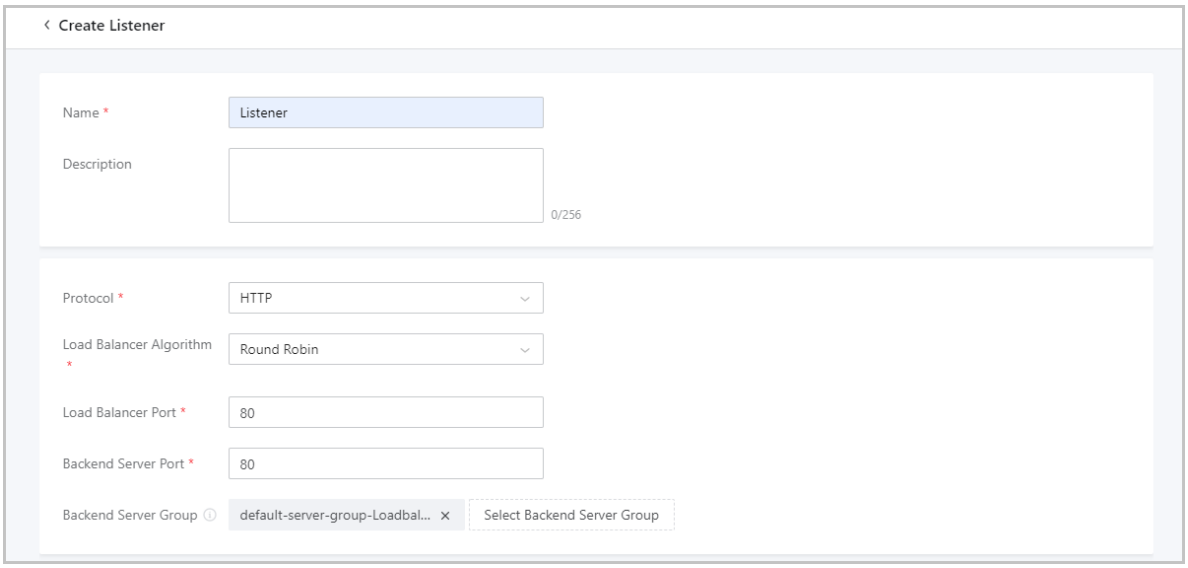
— **Processes**: The number of HAProxy processes. Default: 1.

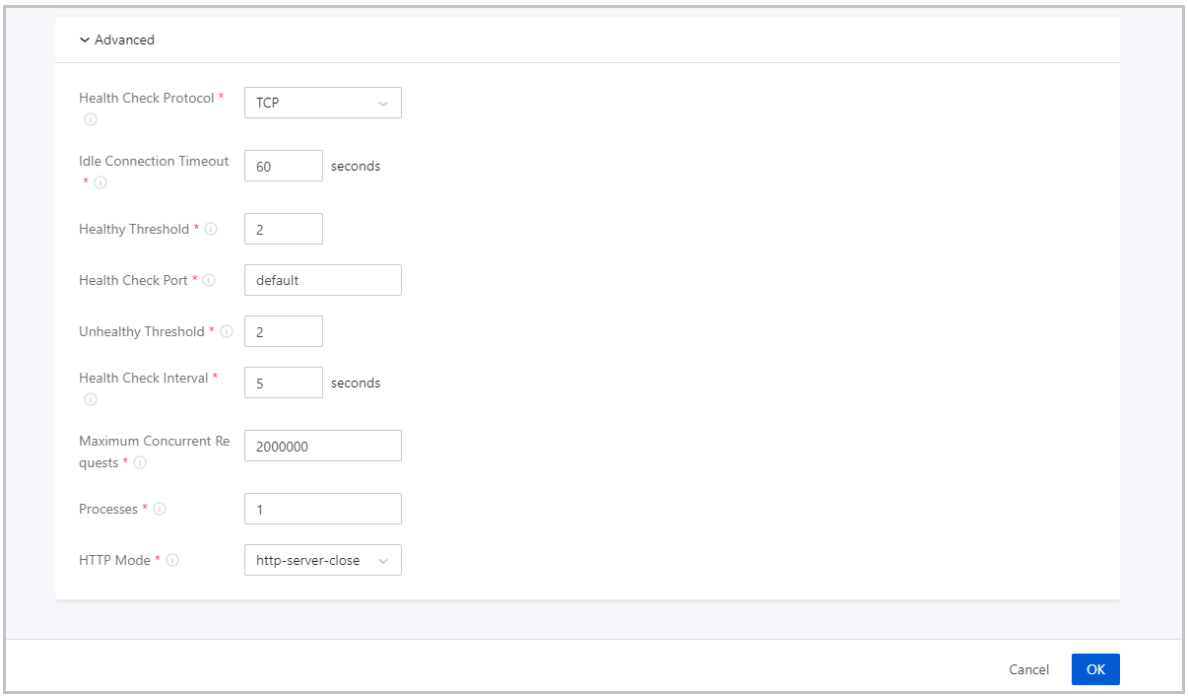
Using multiple processes can improve the listener performance and increase listening concurrency. However, multiple processes might occupy more memory and affect the listening accuracy.

— **HTTP Mode**: The HTTP connection mode of the load balancer. This option is available only when the listening protocol is HTTP.

- http-server-close: The server-facing connection is closed after the end of the response is received, and the client-facing connection remains open.
- http-keep-alive: All requests and responses are processed, and connections remain open but idle between responses and new requests.
- http-tunnel: Only the first request and response are processed and a tunnel is establishe d between the client and the server, so that they can talk without further analysis of HTTP protocol. This mode is not recommended.
- httpclose: The same as tunnel mode, but with a `Connection: close` header field appended in both the client and server directions. This mode is not recommended.
- forceclose: Both the client and the server connections are actively closed by the load balancer after the end of a response.

Figure 7-99: Create a Listener





7.4.5.3.2 Create a Forwarding Rule

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Basic Network Service** > **Load Balancing**. On the load balancer management page, click the target load balancer. On the details page of the load balancer, click the **Listener** tab. On the tab, click the target listener to go to the details page. On the page, click the **Forwarding Rule** tab. On the tab, click **Add Forwarding Rule**. Then, the **Add Forwarding Rule** page appears.

On the displayed page, set the following parameters:

- **Domain Name**: Optional. Enter the domain name that you need to forward. The domain name must be 0-125 characters in length and can contain letters, digits, hyphens (-), periods (.), and asterisks (*).

  Note:

  Consider the following when you use an asterisk (*) in a generic domain name:

  - Put the asterisk (*) in the first place of the domain name.
  - Do not fill in only asterisks (*) for the domain name.
  - Supported formats: *.example.com and *example.com.

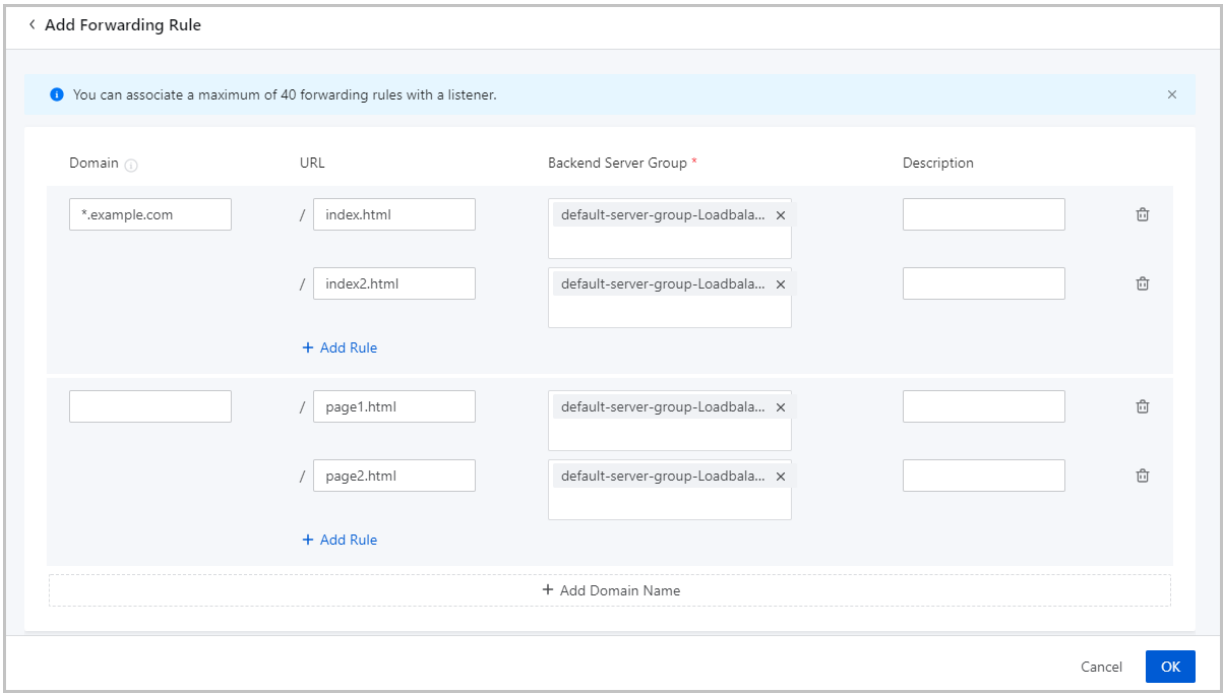
- **URL**: Optional. Enter a request URL. The URL must be 0-80 characters in length and can contain letters, digits, hyphens (-), forward slashes (/), periods (.), percent signs (%), question marks (?) number signs (#), and ampersands (&).

- **Backend Server Group**: Select a backend server group that you want to associate the rule with.
- **Description**: Optional. Enter a description for the forwarding rule.

Note:

- You must enter a domain name, URL, or both.
- You can add a forwarding rule by clicking **Add Rule** or **Add Domain Name**. A listener can be associated a maximum of 40 forwarding rules.

Figure 7-100: Forwarding Rule



Forwarding Rule Matching Algorithm

Forwarding rules are matched based on the following algorithm:

- — If the domain name is specified, the system attempts to match URLs:
  - If a URL is matched, the request is forwarded to the associated backend server group . If multiple URLs are matched based on the exact match mechanism, the request is forwarded to the backend server group associated with the URL that is matched most accurately.
  - If the specified URLs of the domain name are not matched, the request is forwarded to the backend server group associated with the root URL.

- If the root URL is not configured, errors are returned.

— If the domain name is not specified in the frontend request or no domain name is matched, the system attempts to match forwarding rules that have their domain names unspecified:

- If a forwarding rule is matched, the request is forwarded to the associated backend server group.
- If no forwarding rule is matched, the request is forwarded to the backend server group that is not associated with any rule.
- If all backend server groups associated with the listener have associated forwarding rules , errors are returned.

7.4.5.4 Backend Server Group

7.4.5.4.1 Create a Backend Server Group

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Basic Network Service** > **Load Balancing**. On the load balancer management page, click the target load balancer. On the details page of the load balancer, click the **Backend Server Group** tab. On the tab, click **Create Backend Server Group**. The **Create Backend Server Group** page appears.

The following lists the two backend server group creation methods:

- Create a backend server group by instance NIC
- Create a backend server group by IP address

Create Backend Server Group by Instance NIC

On the displayed page, set the following parameters:

- **Name**: Enter a name for the backend server group.
- **Description**: Optional. Enter a description for the backend server group.
- **Listener**: Select an existing listener.

Note:

- A listener monitors the frontend requests of a load balancer and distributes the requests to a backend server based on the specified policy. In addition, the listener performs health checks on backend servers.
- A backend server group can be associated with multiple listeners in the same load balancer.

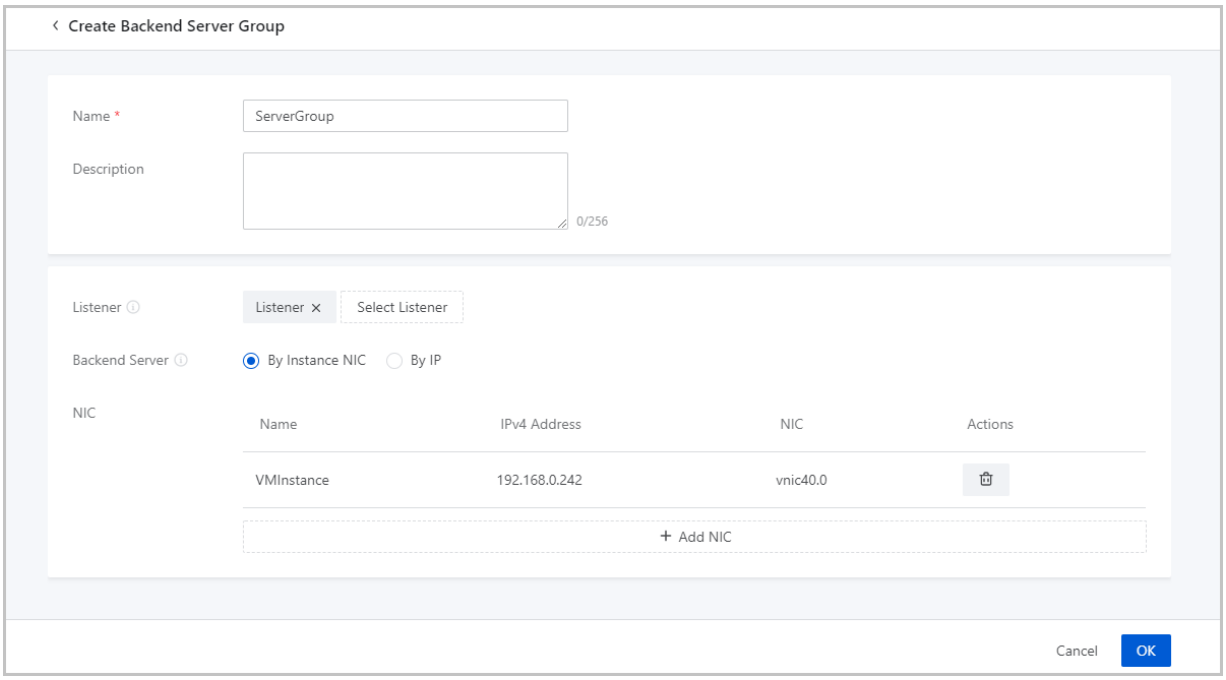
- If the listener uses the weighted round-robin load-balancing algorithm, you can set the weight value for each individual backend server on the backend server group details page.

- **Backend Server**: Select By Instance NIC.

> **Note:**
> You can filter instance NICs by the backend network of the load balancer and add instances as backend servers to the backend server group.

- **NIC**: Add instance NICs to the backend server group.

Figure 7-101: Create Backend Server Group by Instance NIC



Create Backend Server Group by IP Address

On the displayed page, set the following parameters:

- **Name**: Enter a name for the backend server group.
- **Description**: Optional. Enter a description for the backend server group.
- **Listener**: Select an existing listener.

> **Note:**
>
> - A listener monitors the frontend requests of a load balancer and distributes the requests to a backend server based on the specified policy. In addition, the listener performs health checks on backend servers.

- A backend server group can be associated with multiple listeners in the same load balancer.
- If the listener uses the weighted round-robin load-balancing algorithm, you can set the weight value for each individual backend server on the backend server group details page.

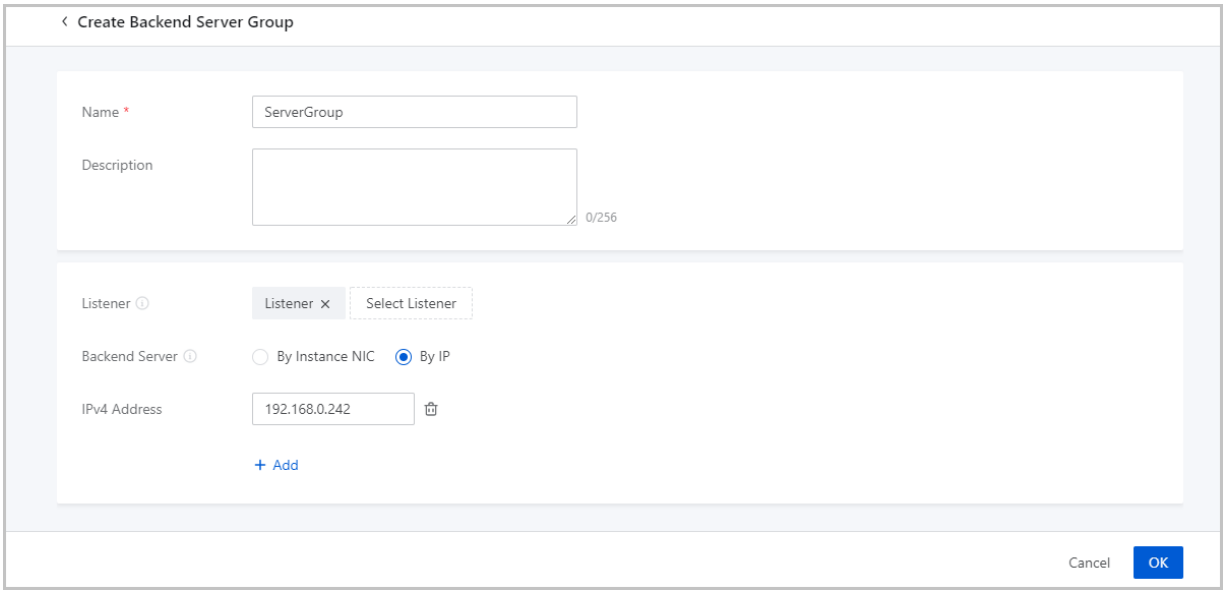
- **Backend Server**: Select By IP.

Note:

- You can add servers on third-party platforms to the Cloud as backend servers. The IP addresses of the servers that you add to the Cloud must be connected to the virtual IP address of the load balancer.
- This method applies to only dedicated-performance load balancers.

- **IPv4 Address**: Enter the IP address of the server that you want to add to the backend server group.
- **Add**: You can add one or more servers as backend servers.

Figure 7-102: Create Backend Server Group by IP Address



Considerations

- A backend server group is a group of backend servers that share the same configurations. You can associate one or more listeners with a backend server group. The listeners distribute traffic based on the weight that you assign to each backend server.
- A load balancer can be associated with multiple backend server groups, while a backend server group can be associated with only one load balancer.

- An empty backend server group is automatically created when you create a load balancer.

7.4.5.5 Certificate

7.4.5.5.1 Create a Certificate

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Basic Network Service** > **Load Balancing** > **Certificate Management**. On the **Certificate Management** tab, click **Create Certificate**. The **Create Certificate** page appears.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the certificate.
- **Description**: Optional. Enter a description for the certificate.
- **Certificate Text**: Enter the certificate content.

  Sample:

  ```
  -----BEGIN CERTIFICATE-----
  #end-usercertiicate#
  -----END CERTIFICATE-----
  ```

  Note:

  - The certificate content starts with `-----BEGIN CERTIFICATE-----` and ends with `-----END CERTIFICATE-----`.
  - The certificate content cannot contain spaces.

- **Private Key**: Enter the private key.

  Sample:

  ```
  -----BEGIN PRIVATE KEY-----
  #privatekey#
  -----END PRIVATE KEY-----
  ```

  Note:

  - The private key starts with `-----BEGIN CERTIFICATE-----` and ends with `-----END CERTIFICATE-----`.
  - The private key cannot contain spaces.

- **Certificate Chain**: Optional. If you need to upload multiple certificates, you need to combine the root and intermediates certificates and then upload the certificates.

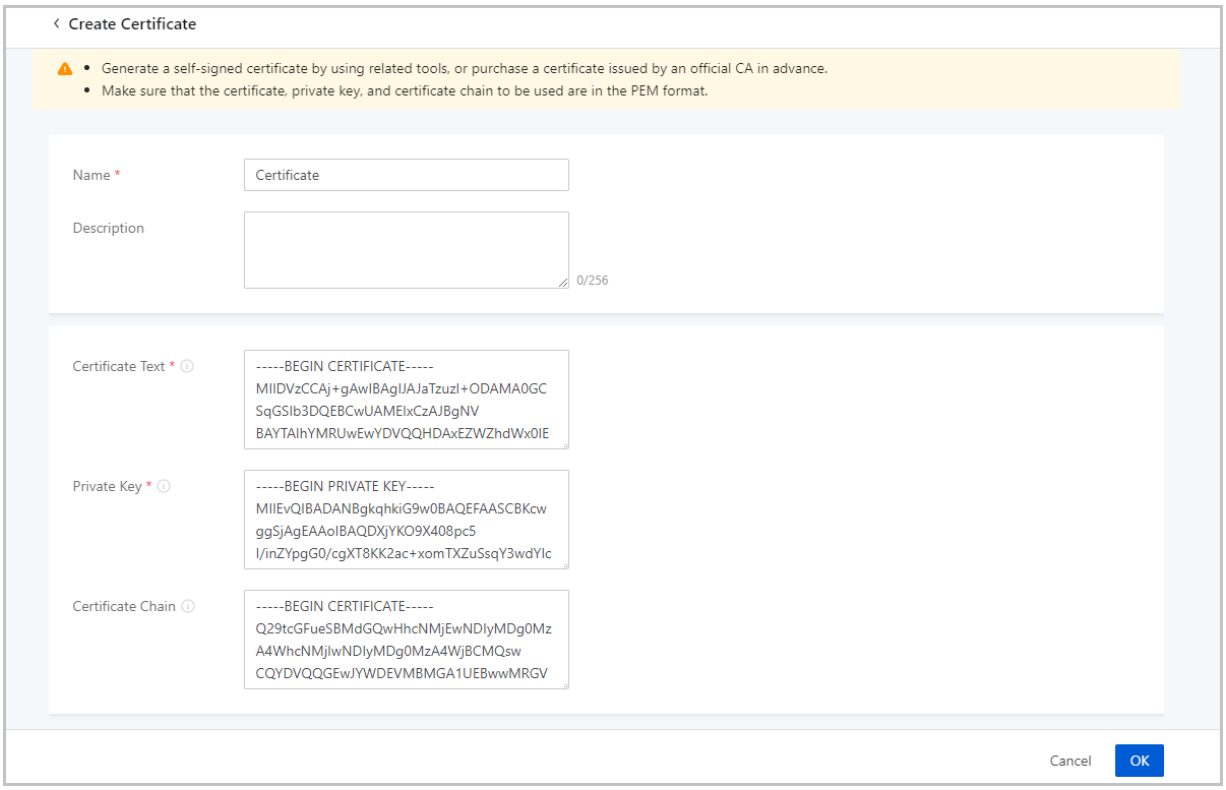
Sample:

```
-----BEGIN CERTIFICATE-----
#rootcertificate#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#intermediatescertiicate#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#intermediatescertificate#
-----END CERTIFICATE-----
```

Note:

- Put the root certificate in the first place and arrange the intermediate certificates in order from the second place. Do not leave blank lines between the certificates.
- The certificate content cannot contain spaces.

Figure 7-103: Create Certificate



Considerations

If an LB listener uses the HTTPS protocol, you must associate certificates with the listener. You can upload individual certificates or a certificate chain.

7.4.5.6 Load Balancing Configurations

7.4.5.6.1 Create a Load Balancer Instance Offering

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Basic Network Service** > **Load Balancing** > **Configuration**. On the **Configuration** tab, click **Create Load Balancer Instance Offering**. The **Create Load Balancer Instance Offering** page appears.

On the displayed page, set the following parameters:

- **Zone**: The current zone that you selected.
- **Name**: Enter a name for the load balancer (LB) instance offering.
- **Description**: Optional. Enter a description for the LB instance offering.
- **CPU**: Specify the number of CPU cores for the LB instance offering.

  Note:

  Enter an integer that ranges from 1 to 1,024.

- **CPU**: Specify the memory size for the LB instance offering.

  Note:

  Enter an integer. Unit: MB, GB, and TB. Valid values: 16MB to 100TB.

- **Image**: Select an LB image that you added to the platform.

  Note:

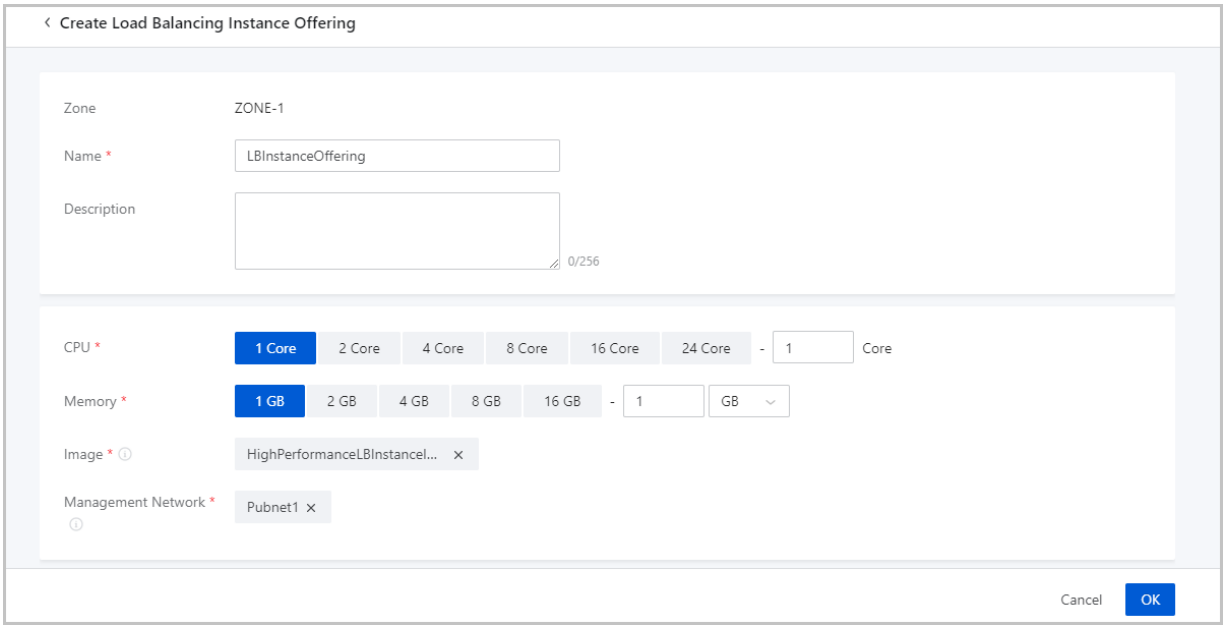
  If the public network defined in a vRouter offering has an IPv6 network range and you use the vRouter offering to create a VPC vRouter, you must use a VPC vRouter image with a version 3.10.0 or later.

- **Management Network**: Select a management network that you created.

  Note:

  - A management network is a network that the management node uses to deploy and configure resources such as hosts, VPC vRouters, and LB instances.
  - If you use a public network to manage physical resources, the public network shall be selected as the management network.

Figure 7-104: Create Load Balancer Instance Offering



7.4.6 Firewall

7.4.6.1 What is Firewall?

A firewall is an access control policy that monitors ingress and egress traffic of VPC vRouters and decides whether to allow or block specific traffic based on a defined set of security rules.

You can associate rules and rule sets with the egress or ingress flow direction of VPC vRouter NICs:

- Ingress: applies to the traffic that flows in the specified VPC vRouter via a network.
- Egress: applies to the traffic that flows out of the specified VPC vRouter via a network.

A rule set is a set of rules that a firewall uses to defend against network attacks. You need to associate a rule set with the egress or ingress flow direction of VPC vRouter NICs to make the rule set take effect.

Firewall rule:

- You can set a priority for a firewall rule. A small number indicates a higher priority. Valid values : 1001 to 2999.
- You can specify the source or destination of data packets to control traffic flows:
  - You can specify one or more source and destination IP addresses. These IP addresses can be static IP addresses, IP ranges, CIDR block, or a mix of the three.

- If you specify multiple entries, which include one or more CIDR blocks, the netmask of the CIDR block must be 24. If you specify only one CIDR block, the netmask of the CIDR block is not limited.
- You can enter a maximum of ten entries, with each entry separated by a comma (,).

A rule template is a template that you can select when you add rules to a rule set or a firewall.

An IP or port set is a set of IP addresses or ports that you can select when you add rules to a rule set or a firewall.

Firewall vs Security Group: A firewall manages the south-north traffic of VPC networks. A security group manages the east-west traffic of VPC networks and is applied to VM NICs. These services complement with each other. The following table compares the two services from three aspects.

Item	Security Group	Firewall
Application scope	VM NIC	The entire VPC network
Deployment mode	Distributed	Centralized
Deployment location	VM instance	VPC vRouter
Configuration policy	Supports only Allow policies	Allows you to customize Accept, Drop, or Reject policies as needed
Priority	Takes effect based on the predefined sequence	Allows you to customize priorities
Matching rules	Source IP address, source port , and protocol	Source IP address, source port, destination IP address, destination port, protocol, and packet status

7.4.6.2 Create a Firewall

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Advanced Network Service** > **Firewall**. On the **Firewall** page, click **Create Firewall**. Then, the **Create Firewall** page is displayed.

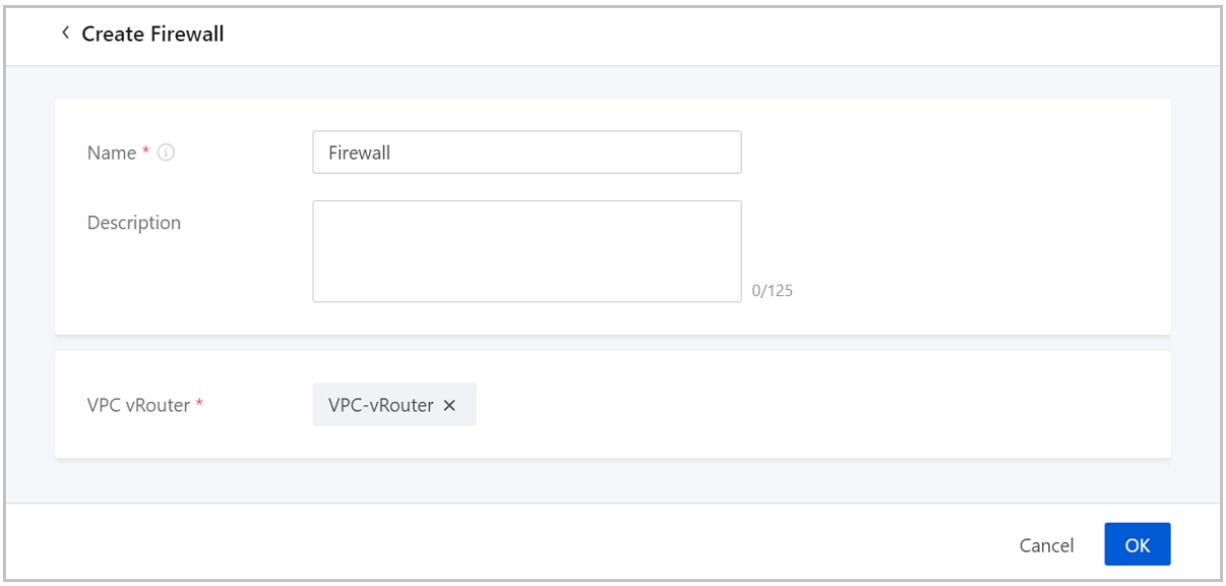
On the displayed page, set the following parameters:

- **Name**: Enter a name for the firewall.
- **Description**: Optional. Enter a description for the firewall.
- **VPC vRouter**: Select a VPC vRouter that you want to defend against attacks .

Note:

The VPC vRouter that you select must be in running state and is not associated with a firewall.

Figure 7-105: Create Firewall



After you create a firewall, you can add firewall rules on the details page to defend the VPC vRouter against attacks.

7.4.6.3 Rule Set

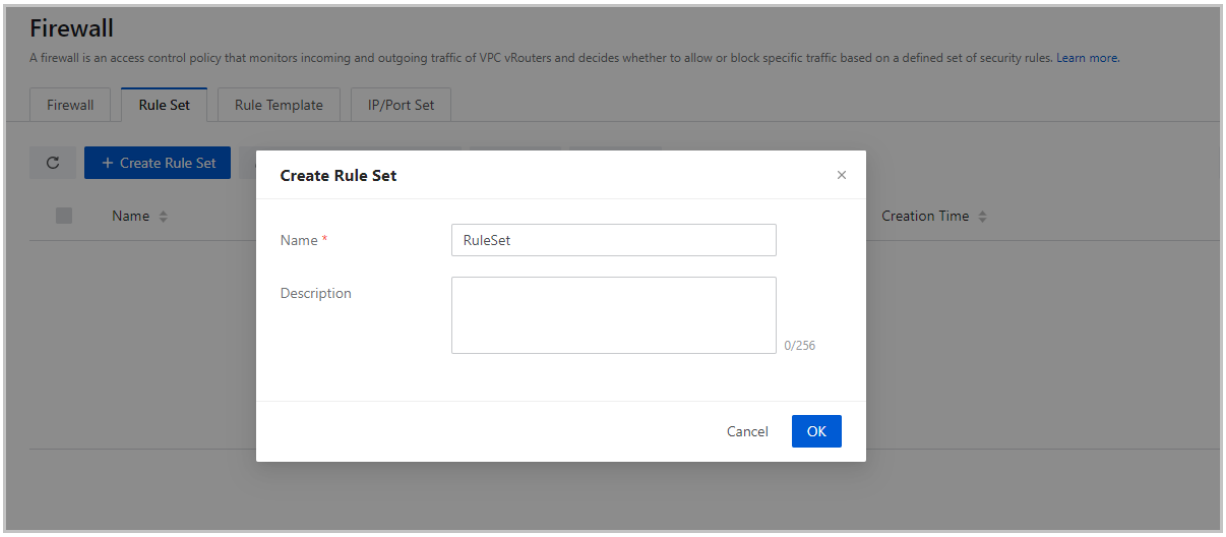
7.4.6.3.1 Create a Rule Set

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Advanced Network Service** > **Firewall**. On the **Firewall** page, click the **Rule Set** tab. On the tab, click **Create Rule Set**. Then, the **Create Rule Set** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the rule set.
- **Description**: Optional. Enter a description for the rule set.

Figure 7-106: Create Rule Set



After you create a rule set, you can add rules on the details page and associate the rules on the egress or ingress direction of a VPC vRouter NIC to defend the VPC vRouter against attacks.

7.4.7 IPsec Tunnel

7.4.7.1 What is IPsec Tunnel?

An IPSec tunnel encrypts and verifies IP packets that transmit over a virtual private network (VPN) from one site to another.

7.4.7.2 Create an IPsec Tunnel

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Advanced Network Service** > **IPsec Tunnel**. On the **IPsec Tunnel** page, click **Create IPsec Tunnel**. Then, the **Create IPsec Tunnel** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the IPsec tunnel.
- **Description**: Optional. Enter a description for the IPsec tunnel.
- **VIP**: You can create a VIP or use an existing VIP to provide IPsec tunnel services.

  Create VIP: Create a VIP. If you select to create a VIP, set the following parameters:

  - **Public Network**: Select a public network to create a VIP.
  - **IP Range**: Optional. Select an IP range. If you selected an IPv4 public network, you can select a normal IP range or an address pool.

- **Assign IP**: Optional. You can assign a virtual IP address. If left blank, the system automatically assigns a VIP.

Use Existing VIP: Use an existing VIP. If you select to use an existing VIP, set the following parameters:

- **VIP**: Select an existing VIP.

> **Note:**
> The system VIP of a VPC vRouter can be used to provide IPsec tunnel services.

- **Local Subnet**: Select a VPC network attached to the VPC vRouter that is associated with the selected public network. If only one VPC network is attached to the VPC vRouter, the VPC network is selected by default.
- **Peer Public IP**: Enter the peer public IP address that provides IPsec tunnel services.
- **Peer CIDR**: Specify a specified peer network CIDR.

> **Note:**
> The CIDR block cannot be overlapped with the network range of the management network and public network attached to the VPC vRouter.

- **Authentication Key**: Set a relatively strong authentication key.
- **Advanced**: You can configure advanced parameter settings for the IPsec tunnel. The Cloud automatically configures default settings for the parameters, as shown in the following list:

  — **Authentication Mode**: psk

  — **IPsec Mode**: tunnel

  — **IKE Authentication Algorithm**: sha1

  — **IKE Encryption Algorithm**: aes128

  — **IKE DH Group**: 2

  — **IPsec Security Protocol**: esp

  — **ESP Authentication Algorithm**: sha1

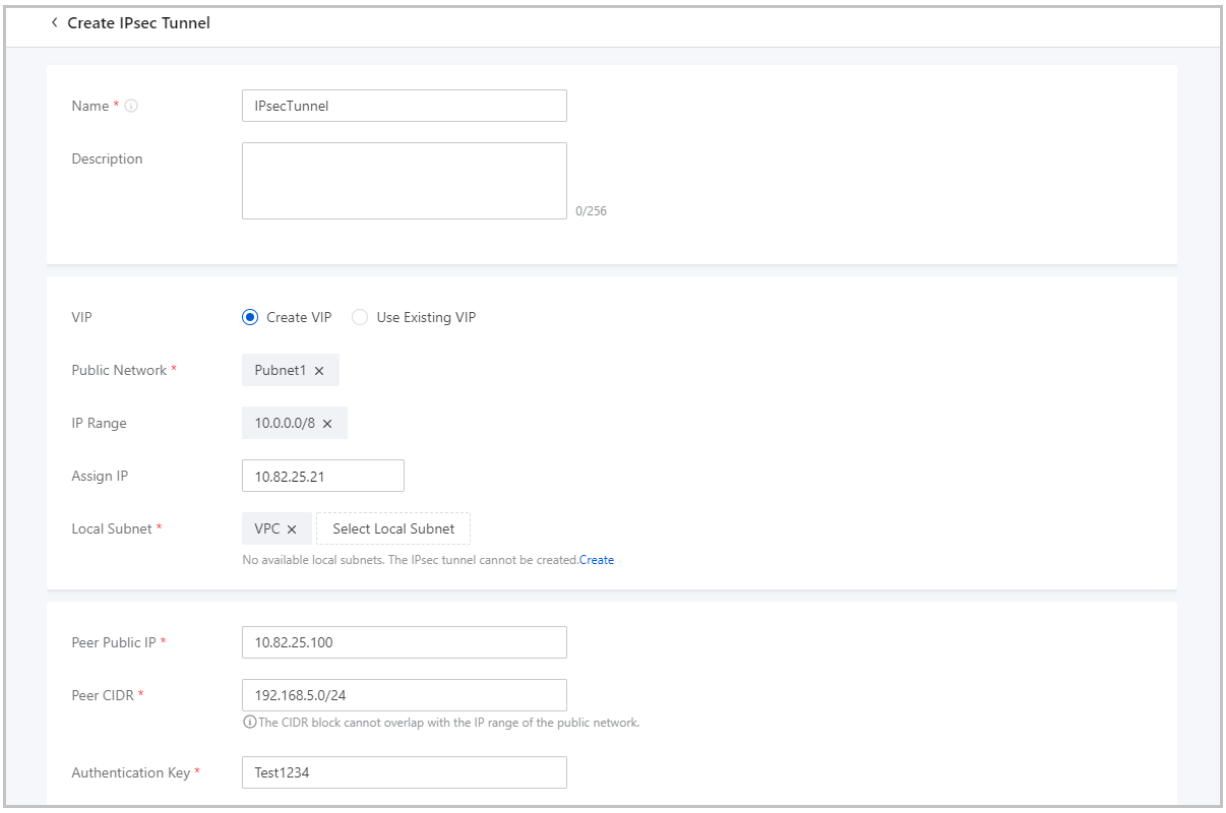
  — **ESP Encryption Algorithm**: aes128

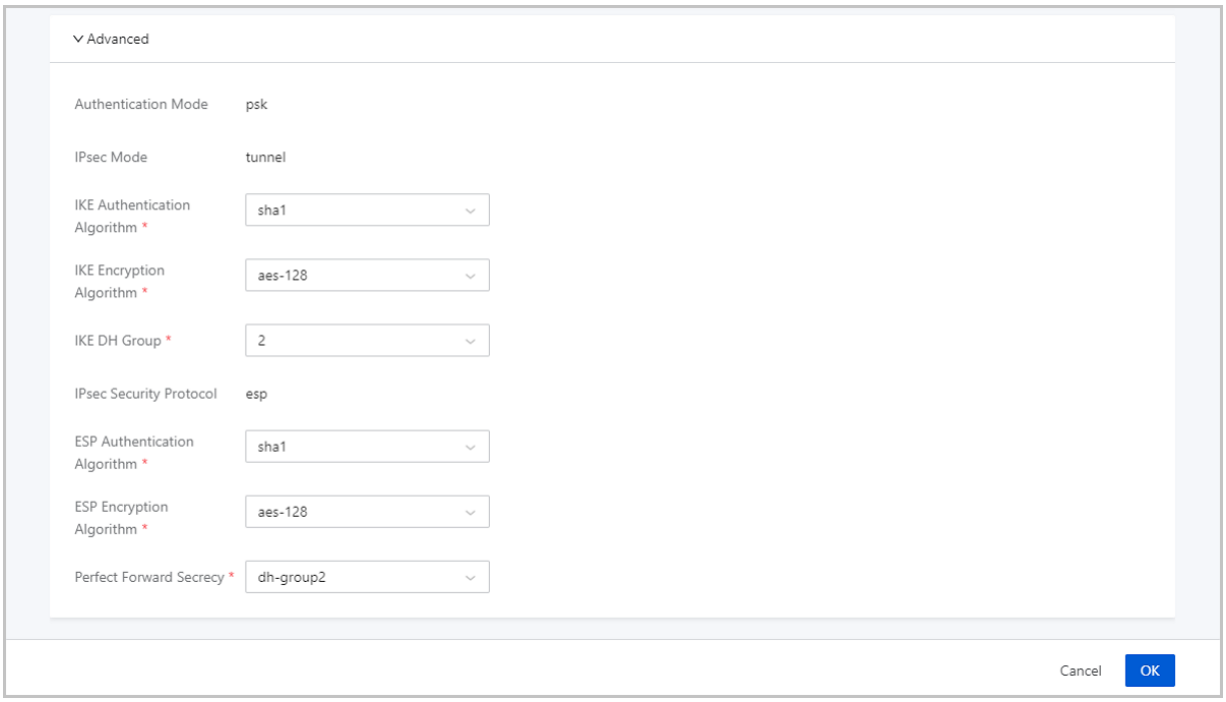
  — **Perfect Forward Secrecy**: dh-group2

> **Note:**

- If you configure an IPsec tunnel by using a VPC vRouter of ZStack Cloud and a third-party device, you need to negotiate the advanced settings of the two devices.
- When you create an IPsec tunnel, you need to adjust local advanced settings based on the IPsec configurations of the peer network device.

Figure 7-107: Create IPsec Tunnel





7.4.8 OSPF Area

7.4.8.1 What is OSPF Area?

An OSPF area is split from an autonomous system based on the OSPF protocol. This splitting simplifies the management of vRouters.

7.4.8.2 Create an OSPF Area

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Advanced Network Service** > **OSPF Area**. On the **OSPF Area** page, click **Create OSPF Area**. Then, the **Create OSPF Area** page is displayed.

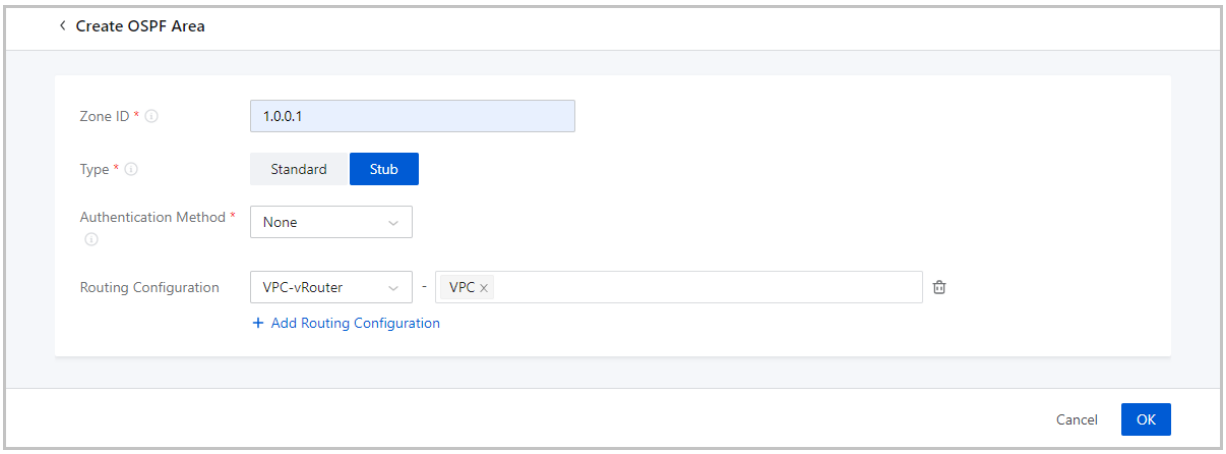
On the displayed page, set the following parameters:

- **Zone ID**: Set an area ID in dotted decimal notation that identifies an OSPF area. The area ID is in similar format as that of IPv4 address.
- **Type**: Select an OSPF area type. Valid values: Standard and Stub.
  - Standard: Standard areas support all types of LSAs.
  - Stub: Stub areas do not support Type 4 and Type 5 LSAs.
- **Authentication Method**: The authentication method used when you select VPC vRouters in an OSPF area to establish neighbors. Valid values: None, Plaintext, and MD5.
  - None: Packets are received without identity authentication.

  - Plaintext: Identity authentication is implemented by using the password contained in the received packets.
  - MD5: Identity authentication is implemented by using the **key ID** and **password** MD5 hash that are contained in the received packets.
- **Routing Configuration**: Optional. Set routing configurations. If you set this parameter, you need to:
  - Select a VPC vRouter to add to the OSPF area.
  - Select a network associated with the VPC vRouter to add to the OSPF area.

> **Note:**
> You can add a VPC vRouter to multiple OSPF areas, but you can add a VPC network or public network associated with the VPC vRouter to only one OSPF area.

Figure 7-108: Create OSPF Area



7.4.9 NetFlow

7.4.9.1 What is NetFlow?

An NetFlow monitors the ingress and egress traffic of the NICs of VPC vRouters. The supported versions of data flows are V5 and V9.

7.4.9.2 Create a Netflow

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Advanced Network Service** > **Netflow**. On the **Netflow** page, click **Create Netflow**. Then, the **Create Netflow** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the Netflow.
- **Description**: Optional. Enter a description for the Netflow.
- **IP**: Specify the IP address of a receiver.
- **Port**: Specify the port of a receiver.

> **Note:**
> Make sure that the configured IP and port suite of the receiver is correct. Otherwise, the Netflow service may not work as expected.

- **Version**: Select a Netflow version.

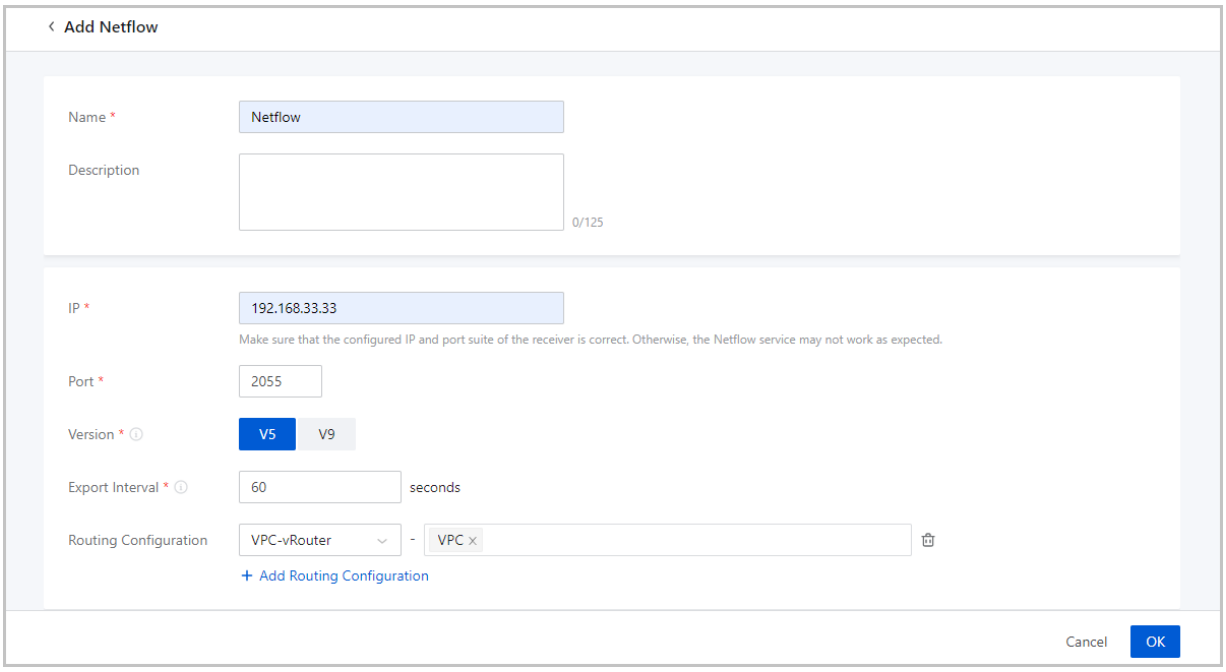
> **Note:**
> The output data format varies depending on the NetFlow version. Select a Netflow version based on your business requirements.

- **Export Interval**: Set the interval that a Netflow sends data monitor information to the receiver.
- **Routing Configuration**: Optional. Set the VPC vRouters and networks that you want to monitor. You can also set the routing configurations after the Netflow is created.

  If you set this parameter, you need to:

  - Select one or more VPC vRouters that you want to monitor.
  - Select one or more networks that you want to monitor.

Figure 7-109: Create Netflow



Considerations

- You can use a Netflow to monitor traffic flows of multiple networks associated with multiple VPC vRouters. However, traffic flows of all networks associated with a VPC vRouter can be monitored by using only one Netflow.
- Make sure the IP address and port suite of the receiver you configure is correct. Otherwise, packets may be lost during data collection.
- You can use a Netflow to collect east-west and north-south traffic of a VPC vRouter. However, if you enable distributed routing for a VPC vRouter, east-west traffic may be optimized and thus cause data loss during collection.
- If you use a Netflow to monitor VPC vRouters in a VPC HA group, the Netflow continually monitors the network traffic of the primary VPC vRouter to ensure data integrity.
- If you use a Netflow to monitor network traffic of a VPC vRouter, the performance of the VPC vRouter is compromised. You can customize a monitor plan best suited your business to lower the impact on VPC vRouter performance.
  - The more VPC networks that a Netflow monitors, the greater the impact on VPC vRouter performance.
  - The shorter the export interval, the greater the impact on VPC vRouter performance and the higher the pressure on business network bandwidth.
  - A stable network is required for accessing the receiver through the public network of a VPC vRouter, thus ensuring that the Netflow service works as expected.

7.4.10 Port Mirroring

7.4.10.1 What is Port Mirroring?

Port mirroring mirrors the traffic data of VM NICs and sends the traffic data to the target ports. This allows for the analysis of data packets of ports and simplifies the monitoring and management of data traffic and makes it easier to locate network errors and exceptions.

7.4.10.2 Create a Port Mirroring

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Advanced Network Service** > **Port Mirroring**. On the **Port Mirroring** page, click **Create Port Mirroring**. Then, the **Create Port Mirroring** page is displayed.

On the displayed page, set the following parameters:

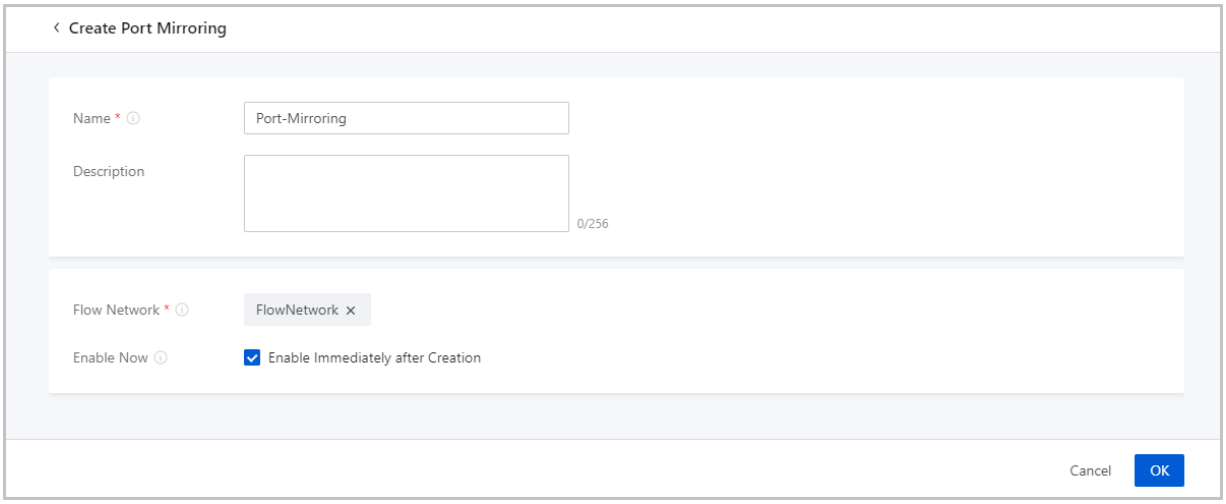
- **Name**: Enter a name for the port mirroring.

- **Description**: Optional. Enter a description for the port mirroring.
- **Flow Network**: Select a flow network for port mirroring.

> **Note:**
>
> - A flow network is a dedicated network for port mirroring. You can use a flow network to transmit the mirrors of data packets of NIC ports to the target ports.
> - You cannot use a flow network for other purposes except for port mirroring.
> - A port mirroring occupies a flow network.
> - The VM instances for which port mirroring is configured must reside in the cluster where the associated flow networks are located.

- **Enable Immediately after Creation**: Optional. Choose whether to enable port mirroring immediately after the port mirroring is created. Enabling port mirroring immediately after the creation may occupy physical network bandwidth. Make sure that your business is not affected and then select the checkbox.

Figure 7-110: Create Port Mirroring



7.4.11 Route Table

7.4.11.1 What is Route Table?

A route table contains information about various routes that you configure. Route entries in a route table must include the destination network, next hop, and route priority.

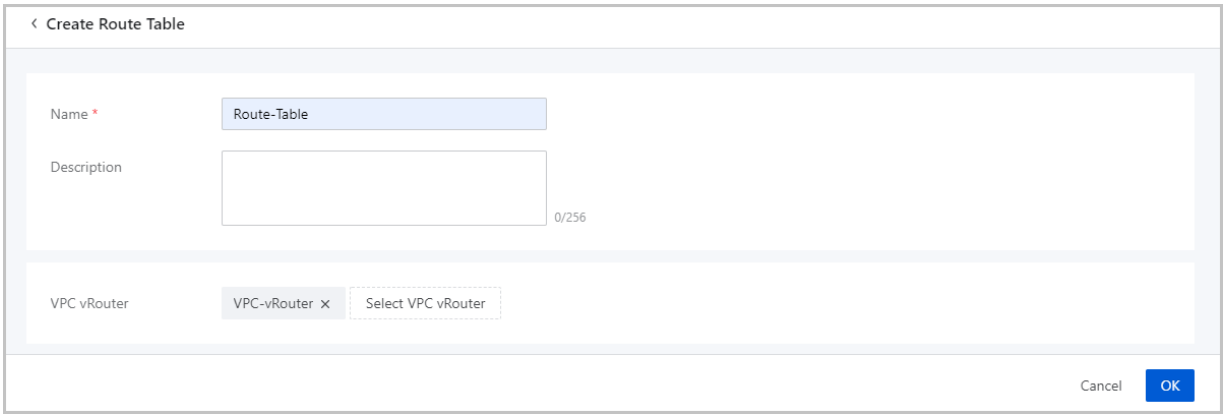
7.4.11.2 Create a Route Table

On the main menu of ZStack Cloud, choose **Resource Center** > **Network Service** > **Advanced Network Service** > **Route Table**. On the **Route Table** page, click **Create Route Table**. Then, the **Create Route Table** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the route table.
- **Description**: Optional. Enter a description for the route table.
- **VPC vRouter**: Optional. Select a VPC vRouter to which the route table is attached.

Figure 7-111: Create Route Table



7.5 CloudFormation

7.5.1 What is CloudFormation?

CloudFormation is a service that simplifies the management of cloud resources and automates deployment and O&S. You can create a stack template to configure cloud resources and their dependencies. This way, resources can be automatically configured and deployed in batches. CloudFormation provides easy management of the lifecycle of cloud resources and integrates automatic O&S into API and SDK.

Characteristics

- You can create a stack template or modify an existing one to define what cloud resources you need, the dependency between the resources, and the resource configurations. Then CloudFormation automatically uses the orchestration engine to create and configure the resources.

- You can use sample templates and a designer provided by the Cloud to create stack templates . This greatly promotes efficiency.
- You can update a stack template as needed. Then you can use the updated template to adjust your resource stacks to accommodate the dynamic changes of your business needs.
- If you no longer need a resource stack, you can delete the stack with one click. This deletes all resources in the stack.
- You can use an existing stack template to quickly duplicate all stack resources and their configuration settings.
- You can flexibly combine cloud services based on different scenarios to meet the needs of automatic maintenance.

7.6 Baremetal Management

7.6.1 What is Baremetal Management?

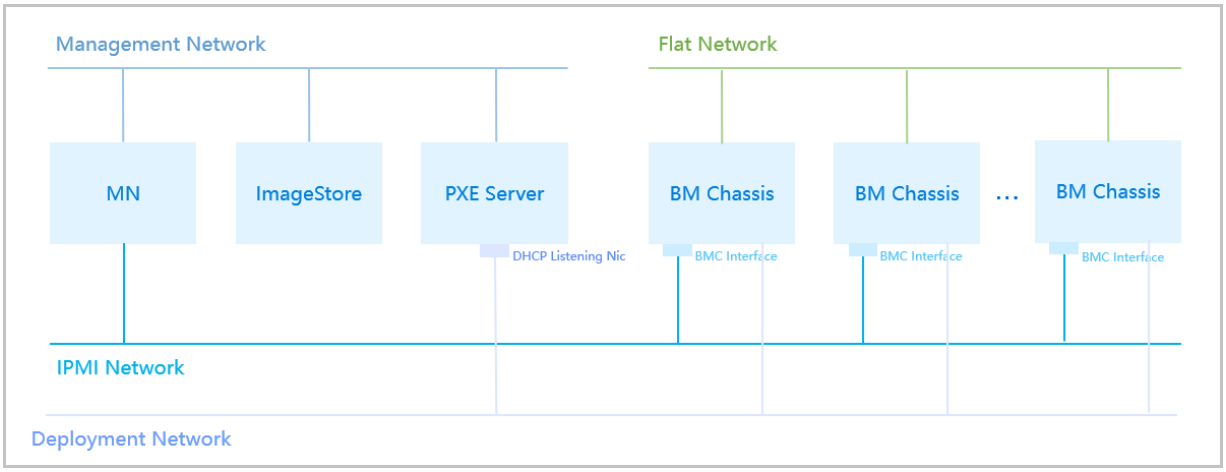
Baremetal Management provided by ZStack Cloud offers dedicated physical servers for your applications to ensure high performance and stability of your applications. After you complete the configurations of your servers and other preparations, you can deploy baremetal (BM) chassis in bulk on the UI. Then you can use these BM chassis to create BM instances. Afterwards, you can use preconfigured templates to implement unattended batch installation of operating systems on these BM instances. In addition, you can configure business networks for BM instances and implement lifecycle management of these BM instances.

Note:
The Baremetal Management feature is provided in a separate module. Before you can use this feature, you need to purchase the Plus License of Baremetal Management, in addition to the Base License.

Basics

In Baremetal Management, the deployment server provides DHCP and FTP services, instructs PEX boot of multiple baremetal chassis, and assigns dynamic IP addresses to the baremetal chassis. These baremetal chassis then download software packages from the deployment server for the system installation of baremetal instances.

Figure 7-112: Network Topology



Concepts

- Baremetal cluster: A baremetal cluster consists of baremetal chassis. You can manage baremetal chassis by managing a baremetal cluster where the chassis reside.
  - You must attach a deployment server to a baremetal cluster to provide PXE services for baremetal instances in the cluster.
  - You can attach only one deployment server to a baremetal cluster. However, you can attach a deployment server to multiple baremetal clusters.
  - You can attach an L2 network to a baremetal cluster to provide network services for baremetal instances in the cluster.
  - Baremetal Management supports flat networks. Baremetal instances and VM instances that share the same L2 network with the baremetal instances can access each other without using the gateway.
- Deployment server: A deployment server is a server that provides PXE services and console proxy services for baremetal chassis. You can specify a server as the deployment server.
  - We recommend that you deploy a dedicated server as the deployment server. This avoids mutual conflicts with other services and improves deployment efficiency.
  - You must attach a deployment server to a baremetal cluster.
  - You can attach only one deployment server to a baremetal cluster. However, you can attach a deployment server to multiple baremetal clusters.
  - The deployment server must have sufficient storage space to store the image for PXE deployment.

- The deployment server must be connected to the management network so as to connect the management node.
- The deployment server must be connected to the deployment network so as to connect baremetal chassis.
- The DHCP listening NIC of the deployment server must be connected to the deployment network. Note that you cannot configure other DHCP services for the deployment network. Otherwise, conflicts may occur.
- The deployment server must be installed the latest version of ZStack Cloud custom ISO (recommended c76). Otherwise, the deployment server cannot provide software packages for baremetal chassis by using the FTP service.

- Baremetal chassis: A baremetal chassis is used to create a baremetal instance and is identified based on the BMC interface and IPMI configuration setting. The management node can remotely manage the power-on, power-off, network boot, disk boot, and other behaviors of baremetal chassis by using the IPMI network. You can use the admin account to complete batch deployment of all baremetal chassis on the UI.
  - The management node must be connected with the IPMI network to remotely manage baremetal chassis.
  - The baremetal chassis must be configured with the BMC interface, IPMI address, port, username, and password, and be connected to the IPMI network.
  - The PXE-capable NIC of the baremetal chassis must be connected to the deployment network.
  - Other NICs of baremetal chassis must be connected to corresponding L2 networks.
- Preconfigured template: A preconfigured template is used to create a preconfigured file that allows for unattended batch installation of an operating system (OS) on baremetal instances.
  - You must have a well-prepared preconfigured template in the Cloud.
  - Preconfigured templates can be classified into the following types:
    - System template: A system template is provided by the Cloud and includes basic system variables. You can use a system template for simple unattended deployment scenarios.
    - Custom template: You can upload a UTF-8-encoded custom template file that includes custom variables, in addition to the basic system variables. You can use a custom template for complex unattended deployment scenarios.

- Baremetal instance: A baremetal instance is an instantiated baremetal chassis. You need to add a baremetal chassis to a baremetal cluster before you can use the baremetal chassis to create a baremetal instance.
  - You can use a preconfigured template to create a preconfigured file and achieve unattended batch installation of an operating system on baremetal instances.
  - You can install an operating system that suits your business needs. The supported OSs include the custom OS of the Cloud and mainstream Linux distributions such as Red Hat Enterprise Linux (RHEL), CentOS, Debian, Ubuntu, SUSE, and openSUSE. Note that the Linux distributions must be in ISO format and are not live CDs.
  - You can configure a flat network as a business network for baremetal instances. By using a flat network, baremetal instances and VM instances that share the same L2 network with the baremetal instances can access each other without using the gateway. Note that you need to attach the baremetal cluster where the baremetal chassis reside to the related L2 network.

Characteristics

- Baremetal Management provides dedicated physical servers for your applications to ensure high performance and stability of your key applications.
- We recommend that you deploy a dedicated server as the deployment server. Then you can use the Baremetal Management feature for multi-MN host HA scenarios. The network environments are simpler and DHCP conflicts are avoided. In addition, a dedicated deployment server is attached to a baremetal cluster. This avoid single point of failures and improves deployment efficiency.
- You can batch add baremetal chassis on the UI through manual addition or template import. You can batch add IPMI addresses and deploy baremetal clusters to improve O&M efficiencies.
- You can use a preconfigured template to create a preconfigured file and achieve unattended batch installation of an operating system on baremetal instances.
- You can install an operating system that suits your business needs. The supported OSs include the custom OS of the Cloud and mainstream Linux distributions such as Red Hat Enterprise Linux (RHEL), CentOS, Debian, Ubuntu, SUSE, and openSUSE.
- You can configure a flat network for baremetal instances. By using a flat network, baremetal instances and VM instances that share the same L2 network with the baremetal instances can access each other without using the gateway.

Scenarios

- Scenarios that require high security and strict monitoring:

  The financial and insurance industries have high requirements over business deployment compliance and data security. In these scenarios, you can use Baremetal Management to secure dedicated resources, data isolation, easy management, and operation-tracking. This way, you can ensure the reliability and security compliance of your key business system and data.

- High-performance computing scenarios:

  In supercomputing, genome sequencing, and other high-performance computing scenarios, the requirements over the computing performance, stability, and timeliness of the server are very high. The Baremetal Management feature is fitting for these scenarios. In addition, the feature can be used for scenarios that require high throughput or high computing performance that can accommodate changing access requests and scenarios. Virtualization and hyperthreading may compromise some performance. Deploying a reasonable number of baremetal clusters can meet the high-performance computing requirements.

- Key database scenarios:

  To meet business requirements, you may not want to deploy some key databases on VM instances while want to deploy the databases on physical servers that feature dedicated resources, network isolation, and guaranteed performance. In these scenarios, you can use Baremetal Management to provide dedicated high-performance physical servers for your applications.

7.7 Elastic Baremetal Management

7.7.1 What is Elastic Baremetal Management?

Elastic Baremetal Management provides dedicated physical servers for your applications to ensure high performance and stability. In addition, this feature allows elastic scaling. You can apply for and scale resources based on your needs. Elastic Baremetal Management integrates the benefits of hosts and VM instances. It delivers powerful and stable computing capacities of hosts and allows you to use primary storages, L3 networks, and other resources on the Cloud for your applications. This way, it avoids virtualization overheads and allows flexible use of cloud resources and physical resources, thus promoting the availability of cloud resources. You can use this feature to deploy applications for traditional non-virtualization scenarios.

- The Elastic Baremetal Management feature is provided in a separate module. Before you can use this feature, you need to purchase the Plus License of Elastic Baremetal Management, in addition to the Base License.
- A tenant can use an elastic baremetal offering shared by the admin to create an elastic baremetal instance.

Concepts

- Provision network: A provision network is a dedicated network for PXE boot and image downloads while creating elastic baremetal instances.
  - Before you can use Elastic Baremetal Management, you need to deploy an IPv4 provision network.
  - Provision networks require high network performance. We recommend that you use at least 10 Gigabit NICs for your provision network.
  - You can configure a gateway for your provision network. This way, the provision network can be connected to other networks. If you do not need to connect your provision network with other networks, you do not need to configure a gateway for your provision network.
- Elastic baremetal cluster: An elastic baremetal cluster consists of elastic baremetal instances. You can manage elastic baremetal instances by managing an elastic baremetal cluster where the instances reside.
  - You must attach a provision network to an elastic baremetal cluster to provide PXE services for baremetal nodes in the cluster.
  - You can attach only one provision network to an elastic baremetal cluster. However, you can attach a provision network to multiple elastic baremetal clusters.
  - You can attach an L2 network to an elastic baremetal cluster to provide an extended L2 business network for elastic baremetal instances in the cluster. Elastic baremetal instances and VM instances that share the same L2 network with the elastic baremetal instances can access each other without using the gateway. The L2 network that you can attach to an elastic baremetal cluster can be of the VLAN or NoVLAN type.
- Gateway node: A gateway node is a node where the ingress and egress traffic of the Cloud and elastic baremetal instances is forwarded.
  - You can attach multiple gateway nodes to an elastic baremetal cluster. However, you can attach only one gateway node to an elastic baremetal cluster.

- A gateway node is used to take over primary storages and assign storage space for elastic baremetal instances.
- A gateway node provides iPXE, DHCP, and other services. It is used to deliver configuration settings to elastic baremetal instances.

- Baremetal node: A baremetal node is used to create a baremetal instance and is identified based on the BMC interface and IPMI configuration setting.
  - The management node must be connected to the IPMI network to remotely manage baremetal nodes.
  - Baremetal nodes must be configured with the BMC interface, IPMI address, port, username , and password, and be connected to the IPMI network.
  - A baremetal node can be distributed to only one elastic baremetal instance and an elastic baremetal instance can only be assigned one baremetal node.
  - You can provide compute resources for elastic baremetal instances based on the baremetal node or baremetal offering.
- Elastic baremetal instance offering: An elastic baremetal offering defines the number of vCPU cores, memory size, CPU architecture, CPU model, and other configuration settings of elastic baremetal instances.
  - After you obtain the hardware information of a baremetal node on the UI, you can obtain the corresponding elastic baremetal offering. The Cloud allows you to manage baremetal nodes of the same elastic baremetal offering in a unified way.
  - You can use an elastic baremetal offering to create an elastic baremetal instance. You can also release the advanced settings of baremetal nodes to avoid resource idling.
  - You can create a pricing list for elastic baremetal instances based on elastic baremetal offerings. Then bills are generated for the elastic baremetal instances based on their usage.
- Elastic baremetal instance: An elastic baremetal instance has the same performance as physical servers and allows elastic scaling. You can apply for and scale resources based on your needs.
  - The following two startup methods are supported for elastic baremetal instances:
    - Volume: Uses a volume as the system volume of the elastic baremetal instance to install and deploy the operating system.
    - Local Disk: Uses a local disk as the system disk of the elastic baremetal instance to install and deploy the operating system.

- The Local Disk (Non Take-Over) and Local Disk (Take-Over) methods are supported:
  - Local Disk (Non Take-Over): When you use a baremetal node to create the elastic baremetal instance, the operating system is downloaded from the Cloud and installed on the elastic baremetal instance. This method will format the local system disk.
  - Local Disk (Take-Over): When you use a baremetal node to create the elastic baremetal instance, the original operating system on the local system disk is used as the operating system of the elastic baremetal instance.

— The following describes the resources supplied to elastic baremetal instances of different startup methods:

- For elastic baremetal instances of both the volume startup method and local disk startup method, baremetal nodes provide compute resources and L3 networks on the Cloud are used as the business networks.
- For elastic baremetal instances of the volume startup method, SharedBlock or Ceph primary storages on the Cloud provide storage resources and the provision network provides support for PXE boot.
- For elastic baremetal instances of local disk startup method, the local disks of the instances provide storage resoures. If you attach data volumes to the instances, SharedBlock or Ceph primary storages on the Cloud also provides storage resources

— We recommend that you create an elastic baremetal instance by using an image that has installed the agent. Otherwise, you cannot open the console of the elastic baremetal instance, modify the password of the instance, attach a volume to or detach a volume from the instance, or attach a network to or detach a network from the instance.

— By default, the supported BIOS mode of the image used to create an elastic baremetal instance is UEFI. To use an image whose BIOS mode is Legacy, contact the official technical support.

— You can configure business networks for elastic baremetal instances. If you attach an L2 network to the cluster where your baremetal nodes reside, elastic baremetal instances and VM instances that share the same L2 network with the elastic baremetal instances can access each other without using the gateway.

— Elastic baremetal instances of the volume startup method allow you to release the associated baremetal node upon instance power-off. If you enable this feature, when an elastic baremetal instance of the volume startup method is powered off, the associated

baremetal node is automatically released and can be used by another elastic baremetal instance. This mechanism avoids resource idling.

Scenarios

- Scenarios that require high security and strict monitoring:

  The financial and insurance industries have high requirements over business deployment compliance and data security. In these scenarios, you can use Baremetal Management to secure dedicated resources, data isolation, easy management, and operation-tracking. This way, you can ensure the reliability and security compliance of your key business system and data.

- High-performance computing scenarios:

  In supercomputing, genome sequencing, and other high-performance computing scenarios, the requirements over the computing performance, stability, and timeliness of the server are very high. The Baremetal Management feature is fitting for these scenarios. In addition, the feature can be used for scenarios that require high throughput or high computing performance that can accommodate changing access requests and scenarios. Virtualization and hyperthreading may compromise some performance. Deploying a reasonable number of baremetal clusters can meet the high-performance computing requirements.

- Key database scenarios:

  To meet business requirements, you may not want to deploy some key databases on VM instances while want to deploy the databases on physical servers that feature dedicated resources, network isolation, and guaranteed performance. In these scenarios, you can use Baremetal Management to provide dedicated high-performance physical servers for your applications.

Considerations

When you use the Elastic Baremetal Management feature, note that:

- The server that you use as a baremetal node must have at least one PXE boot NIC used for network management. Make sure the first port of the first NIC of the server is used as the provision NIC.
- You can use x86 servers and Kunpeng and other China localized mainstream ARM servers as baremetal nodes.
- You can use x86 servers as gateway nodes. If you use an ARM server as a baremetal node, you need to add ARM repos for gateway nodes.

- Physical network environments include management network, storage network, provision network, IPMI network, and business network. The provision network requires high performanc e. We recommend that you configure a 10-Gigabit network.
- To avoid DHCP conflict, make sure that you do not configure an additional DHCP service.
- You can use a flat network, public network, and VPC network as a business network.
- Windows-based elastic baremetal instances only support L2 networks of the NoVLAN type.
- You need to install the agent or relevant dependency packages on the elastic baremetal image . Otherwise, some features of elastic baremetal instances cannot work as expected.
- You can use a Shared Block primary storage and Ceph Enterprise primary storage for elastic baremetal instances. Note that the version of Ceph Enterprise must be later than 4.2.0.300.
- If you use a Ceph Enterprise primary storage, you need to login to the Ceph Enterprise management node, choose **Setting** > **Access Token**, and obtain an access token generated by using the admin account. Then you need to add the access token when you add a Ceph primary storage.

Note:

Make sure that the license of the Ceph Enterprise storage is valid.

Figure 7-113: Obtain Access Token

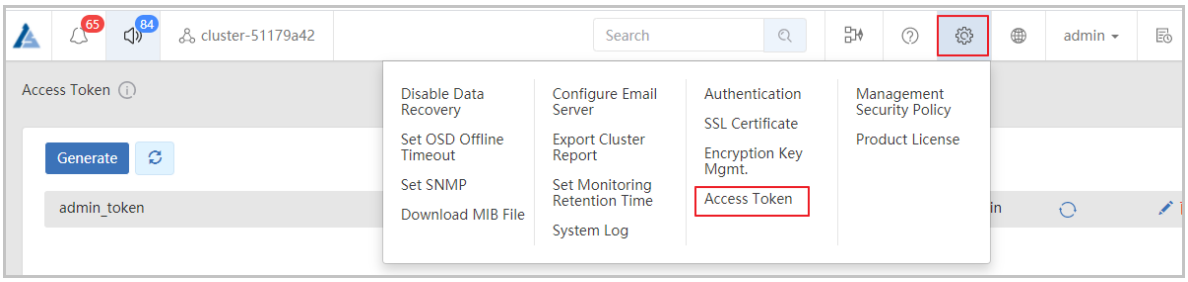
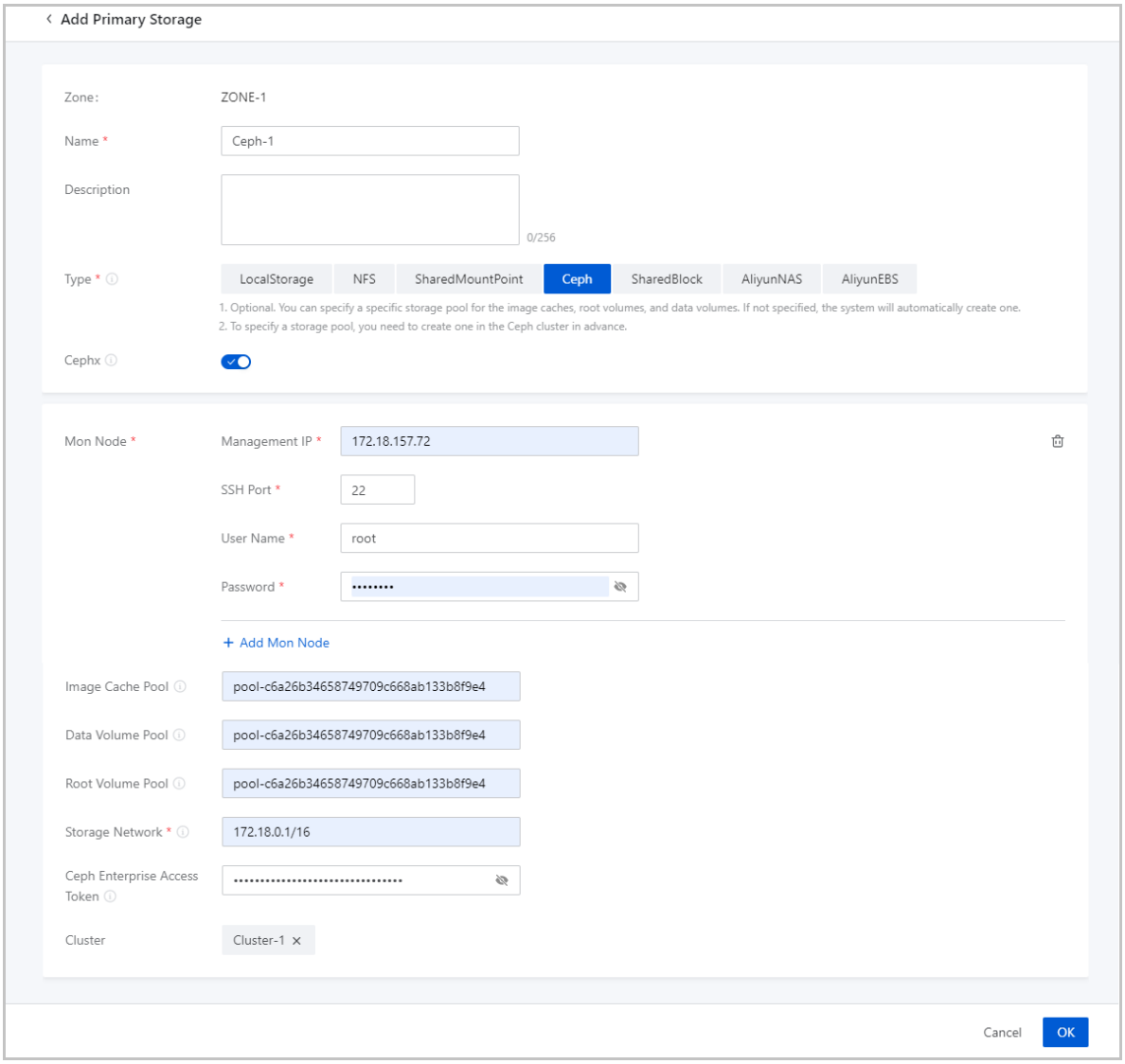


Figure 7-114: Add Ceph Enterprise Primary Storage



- The following table describes the limits on the primary storage that you can attach to an elastic baremetal cluster.

Table 7-10: Relationship of Elastic Baremetal Cluster and Primary Storage

Primary Storage	Elastic Baremetal Cluster
Ceph	You can attach only one Ceph primary storage to an elastic baremetal cluster.
Shared Block	You can attach one or more Shared Block primary storage to an elastic baremetal cluster.

Primary Storage	Elastic Baremetal Cluster
Ceph + Shared Block	You can attach one Ceph primary storage (excluding Ceph Enterprise) and one or more Shared Block primary storage to an elastic baremetal cluster.

- You can install mainstream x86 operating systems (OSs) and some ARM OSs on elastic baremetal instances.

Table 7-11: Operating Systems

CPU Architecture	OS Type	OS
x86	Windows	• Windows 2012 • Windows 2016 • Windows 2019
	Linux	• CentOS 7 • CentOS 8 • Ubuntu 18LTS • Ubuntu 20LTS
ARM	Linux	• CentOS 7 • Kylin V10

7.7.2 Quick Start

Context

On the main menu of ZStack Cloud, choose **Resource Center** > **Elastic Baremetal Management** > **Guide Center** > **Quick Start Wizard**. Then, you are redirected to the **Quick Start Wizard** page.

You can follow the following steps to quick start Elastic Baremetal Management.

Procedure

1. Preparation

   Elastic Baremetal Management provides dedicated physical servers for your applications to ensure high performance and stability. In addition, this feature allows elastic scaling. You can apply for and scale resources based on your needs.

Before you can use Elastic Baremetal Management, you need to complete the following preparations:

- Understand Basics

  You can refer to the working principal diagram in Introduction and understand what resources are needed and the relationship between the resources.

- Deploy Physical Network:

  Make sure that you have deployed IPv4 physical networks, including management networks , storage networks, provision networks, business networks, IPMI networks. We recommend that you use at least 10 Gigabit NICs for your provision network.

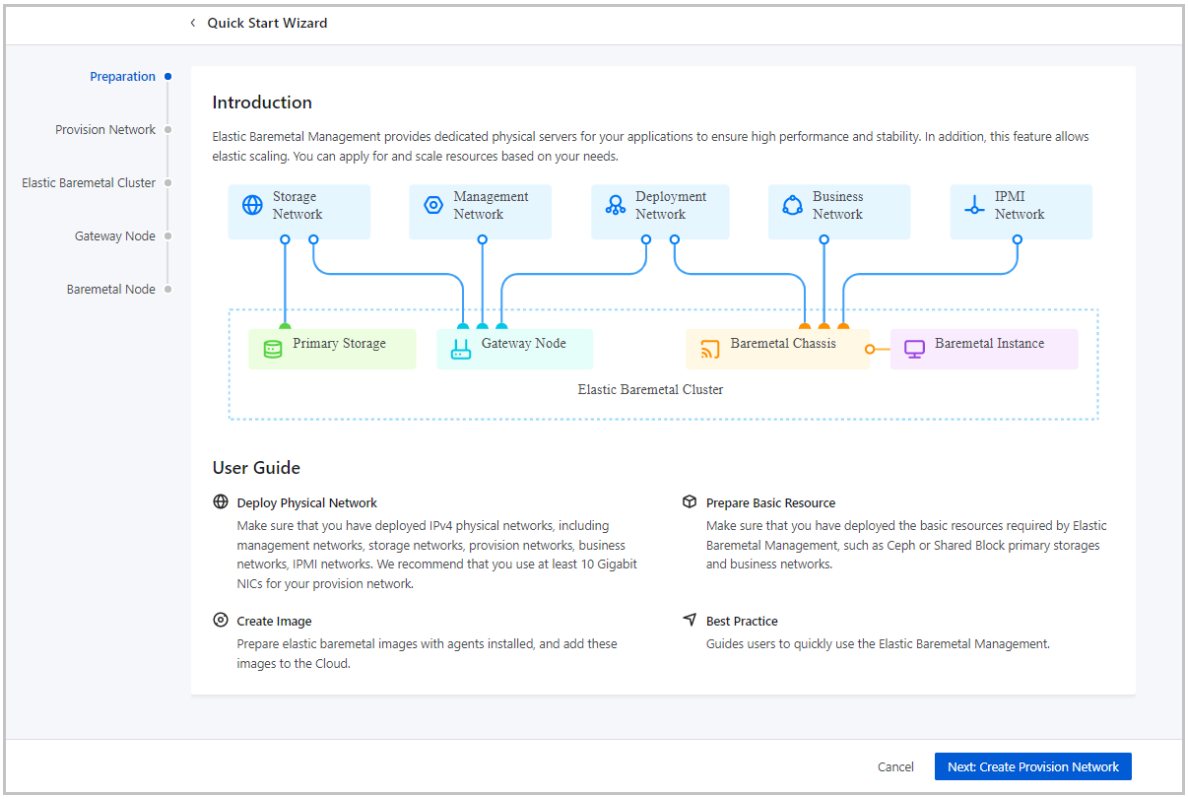
- Prepare Basic Resource:

  Make sure that you have deployed the basic resources required by Elastic Baremetal Management, such as Ceph or Shared Block primary storages and business networks.

- Create Image:

  Prepare elastic baremetal images with the agent installed, and add these images to the Cloud. Otherwise, you cannot open the console, change the password of the elastic baremetal instance, attach/detach volumes or networks, or view monitoring data.

Figure 7-115: Preparation



2. Provision Network

Provision Network：A provision network is a dedicated network for PXE boot and image downloads while creating elastic baremetal instances.

- Before you can use Elastic Baremetal Management, you need to deploy an IPv4 provision network.
- Provision networks require high network performance. We recommend that you use at least 10 Gigabit NICs for your provision network.
- You can configure a gateway for your provision network. This way, the provision network can be connected to other networks. If you do not need to connect your provision network with other networks, you do not need to configure a gateway for your provision network.

On the displayed page, set the following parameters:

- **Name**: Set a name for the provision network. A name can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the provision network.

- **NIC**: Enter the name of the NIC in the provision network. The NIC name must be consistent with the NIC name in the actual deployment environment.

  Note:

  - Make sure that the first NIC of the server is connected to the provision network. Otherwise, baremetal nodes cannot be started.
  - Make sure that no other DHCP service is deployed in the provision network. This avoids DHCP conflicts.

- **Network Range Method**: Select a method to add a network range for the provision network. You can select IP Range or CIDR.

  If you select **IP Range**, you need to set the following parameters:

  - **Start IP**: Set a start IP address for the network range, for example, *192.168.0.2*.
  - **End IP**: Set an end IP address for the network range, for example, *192.168.0.254*.
  - **Netmask**: Set a netmask for the network range, for example, *255.255.0.0*.
  - **Gateway**: Set a gateway for the provision network, for example, *192.168.0.1*.

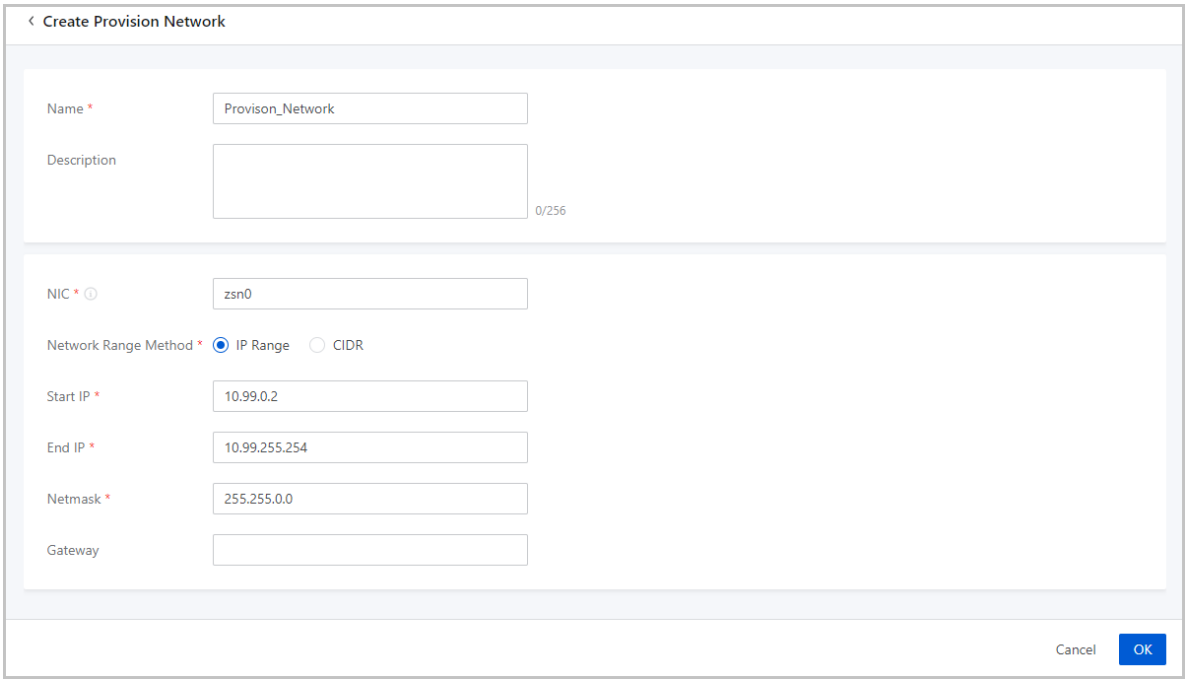
    Note:
    If you do not need to connect to other networks, you do not need to configure a gateway.

  If you select **CIDR**, you need to set the following parameters:

  - **CIDR**: Set a CIDR block for the provision network, for example, *192.168.0.0/24*.
  - **Gateway**; Optional. Set a gateway for the provision network, for example, *192.168.108.1*.

    Note:
    If you do not need to connect to other networks, you do not need to configure a gateway.

Figure 7-116: Create Provision Network



3. Elastic Baremetal Cluster

Elastic Baremetal Cluster: An elastic baremetal cluster consists of elastic baremetal instances. You can manage elastic baremetal instances by managing an elastic baremetal cluster where the instances reside.

- You must attach a provision network to an elastic baremetal cluster to provide PXE services for baremetal nodes in the cluster.
- You can attach only one provision network to an elastic baremetal cluster. However, you can attach a provision network to multiple elastic baremetal clusters.
- You can attach an L2 network to an elastic baremetal cluster to provide an extended L2 business network for elastic baremetal instances in the cluster. Elastic baremetal instances and VM instances that share the same L2 network with the elastic baremetal instances can access each other without using the gateway. The L2 network that you can attach to an elastic baremetal cluster can be of the VLAN or NoVLAN type.

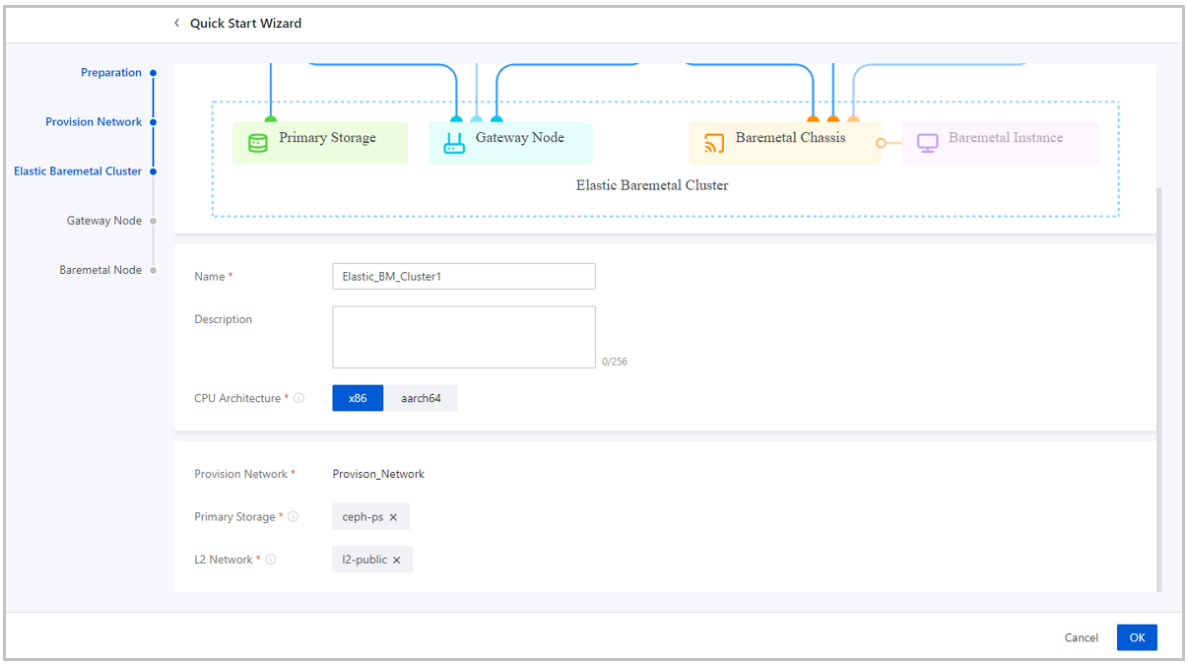
On the displayed page, set the following parameters:

- **Name**: Set a name for the elastic baremetal cluster. A name can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the elastic baremetal cluster.

- **CPU Architecture**: The CPU architecture of the elastic baremetal cluster. The available architectures include x86_64 and aarch64.
  - If you need to add only baremetal nodes with the x86_64 architecture to the elastic baremetal cluster, select x86_64.
  - If you need to add only baremetal nodes with the aarch64 architecture to the elastic baremetal cluster, select aarch64.

  Note:
  Make sure that the CPU architecture of the elastic baremetal cluster is consistent with that of baremetal nodes and gateway node.
- **Provision Network**: Select a provision network that you need to attach to the cluster.
- **Primary Storage**: Select a primary storage that you need to attach to the cluster. You can select a primary storage of the SharedBlock or Ceph type.
- **iSCSI Storage**: If you select a primary storage of the SharedBlock type, you need to attach the iSCSI storage to the cluster.
- **L2 Network**: Select an L2 network that you need to attach to the cluster.

Figure 7-117: Create Elastic Baremetal Cluster



4. Gateway Node

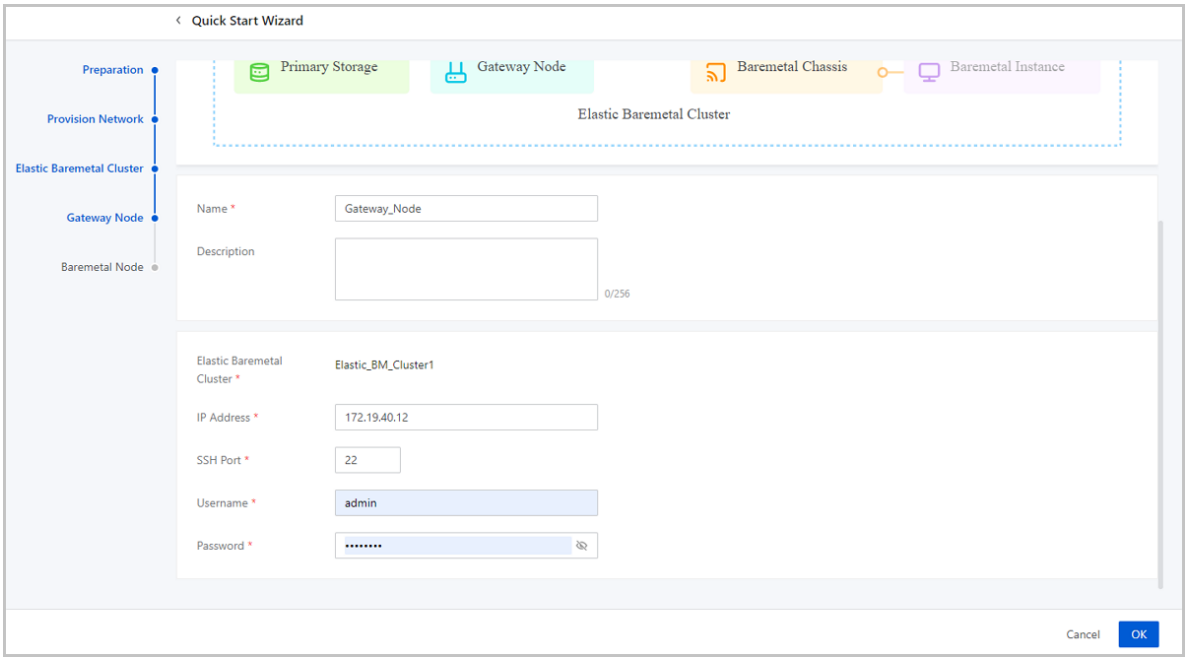
Gateway Node: A gateway node is a node where the ingress and egress traffic of the Cloud and elastic baremetal instances is forwarded.

- You can attach multiple gateway nodes to an elastic baremetal cluster. However, you can attach only one gateway node to an elastic baremetal cluster.
- A gateway node is used to take over primary storages and assign storage space for elastic baremetal instances.
- A gateway node provides iPXE, DHCP, and other services. It is used to deliver configuration settings to elastic baremetal instances.

On the displayed page, set the following parameters:

- **Name**: Set a name for the gateway node. A name can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the gateway node.
- **Elastic Baremetal Cluster**: Select an elastic baremetal cluster to which you need to attach the gateway node.
- **IP Address**: Enter an IP address for the gateway node based on your actual scenario.
- **SSH Port**: Enter an SSH port for the gateway node based on your actual scenario. Default: 22
- **Username**: Enter the username of the gateway node.
- **Password**: Enter the password of the username.

Figure 7-118: Add Gateway Node



5. Baremetal Node

Baremetal Node: A baremetal node is used to create a baremetal instance and is identified based on the BMC interface and IPMI configuration setting.

- The management node must be connected to the IPMI network to remotely manage baremetal nodes.
- Baremetal nodes must be configured with the BMC interface, IPMI address, port, username , and password, and be connected to the IPMI network.
- A baremetal node can be distributed to only one elastic baremetal instance and an elastic baremetal instance can only be assigned one baremetal node.
- You can provide compute resources for elastic baremetal instances based on the baremetal node or baremetal offering.

On the displayed page, set the following parameters:

- **Name**: Set a name for the baremetal node. A name can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the baremetal node.
- **CPU Architecture**: The CPU architecture of the elastic baremetal cluster. The available architectures include x86_64 and aarch64.

> **Note:**
> Make sure that the CPU architecture of the elastic baremetal cluster is consistent with that of baremetal nodes and gateway node.

- **Elastic Baremetal Cluster**: Select an elastic baremetal cluster where the baremetal node resides.
- **Startup Method**: The startup method of the elastic baremetal instance. The following two startup methods are supported:
  - **Volume**: Uses a volume as the system volume of the elastic baremetal instance to install and deploy the operating system.
  - **Local Disk**: Uses a local disk as the system disk of the elastic baremetal instance to install and deploy the operating system.
    - **Take Over Original System**: The Local Disk (Non Take-Over) and Local Disk (Take-Over) methods are supported.
      - **Non Take-Over** : When you create an elastic baremetal instance, the operating system is downloaded from the Cloud and installed on the elastic baremetal instance. This method will format the local system disk.
      - **Take-Over**: When you create an elastic baremetal instance, the original operating system on the local system disk is used as the operating system of the elastic baremetal instance.
        - **Platform**: Select the platform type based on the operating system that you take over. Supported types of platform: Linux and Windows.

> **Note:**
> If you take over the original system, note that:
>
> - We recommend that you take over a system that has installed the agent. If the took-over system does not have the agent installed, install the agent after the elastic baremetal instance is created. Otherwise, you cannot open the console of the elastic baremetal instance, modify the password of the instance, attach a volume to or detach a volume from the instance, or attach a network to or detach a network from the instance.

- By default, the supported BIOS mode of the image used to create an elastic baremetal instance is UEFI. To use an image whose BIOS mode is Legacy, contact the official technical support.
- Make sure that the operating system you take over is officially supported by Elastic Baremetal Management. Otherwise, you can perform very limited operations on the elastic baremetal instance created from the baremetal node. For more information, see *Operating Systems*.

- **IPMI Information**: Enter the IPMI information by using the IPMI address method or IPMI range method.

  If you use the IPMI address method, set the following parameters:

  - **IPMI Address**: Enter an IPMI address.
  - **Port**: Enter an IPMI port.
  - **User Name**: Enter an IPMI username.
  - **Password**: Enter the password of the IPMI username.

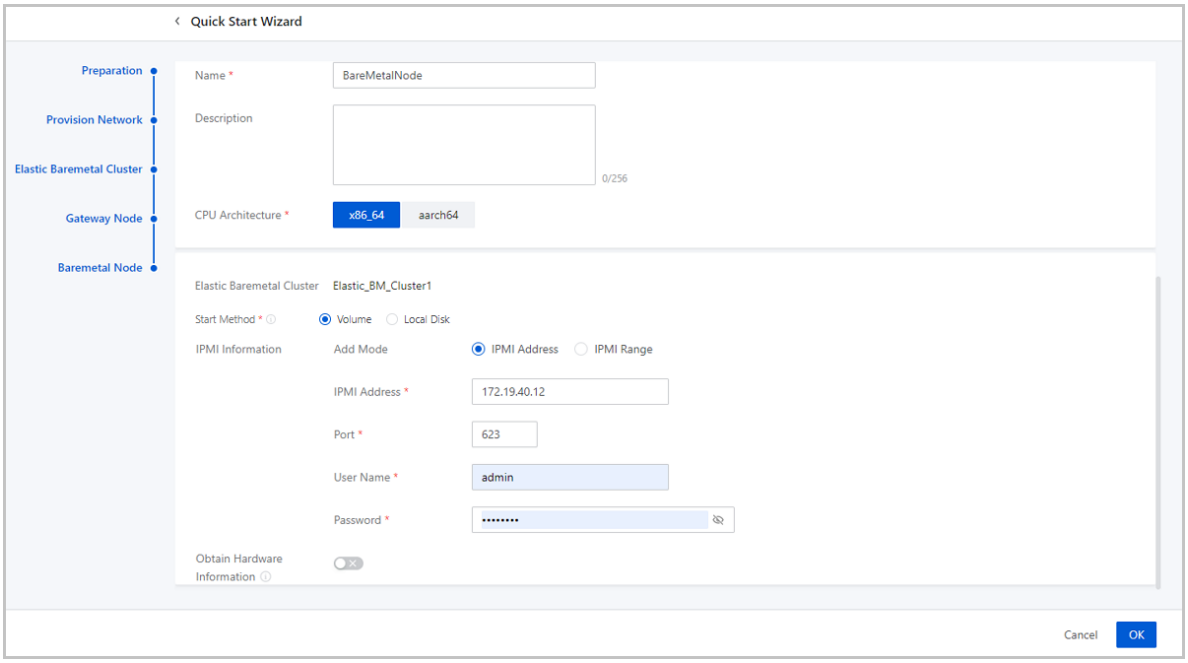
  If you use the IPMI range method, set the following parameters:

  - **IPMI Range**: Enter an IPMI range.
  - **Port**: Enter an IPMI port. Make sure that the ports of the IPMI range are consistent with each other.
  - **User Name**: Enter an IPMI username. Make sure that the usernames of the IPMI range are consistent with each other.
  - **Password**: Enter the password of the IPMI username. Make sure that the passwords of the IPMI range are consistent with each other.
- **Obtain Hardware Information**: Reboot the baremetal node and obtain hardware information. By default, the switch is turned off.

  Note:

  If you add a new baremetal node, you must turn on the switch to obtain hardware information. However, rebooting a baremetal node may affect business operations. Before you reboot baremetal nodes, make sure that this operation does not affect your business.

Figure 7-119: Add Baremetal Node



6. Check Configurations

After you complete the Quick Start Wizard, you can create an elastic baremetal instance. However, you need to check the following configurations due to deployment concerns before you create an instance:

- If you use ZStack Ceph Enterprise storage and want to add an access token for the ZStack Ceph Enterprise storage, you need to login to the management node of the ZStack Ceph Enterprise storage as the admin in advance, choose **Setting (icon)** > **Access Token**, and obtain an access token of th admin permission. Then you need to enter the acess token when you add Ceph primary storage on the Cloud.

> **Note:**
> Make sure that the license of the ZStack Ceph Enterprise storage is valid.

Figure 7-120: Obtain Access Token

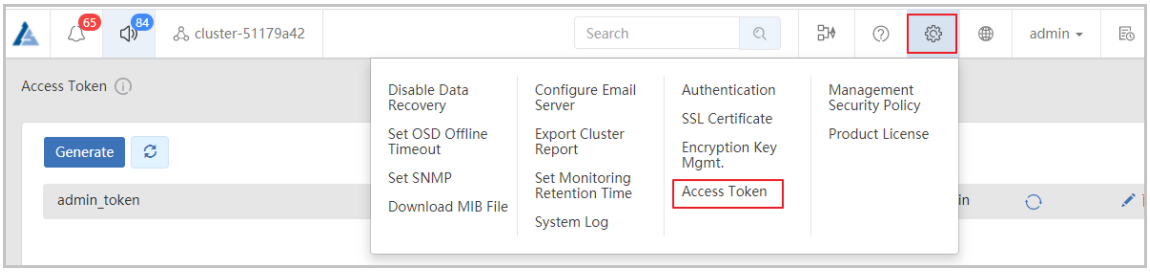
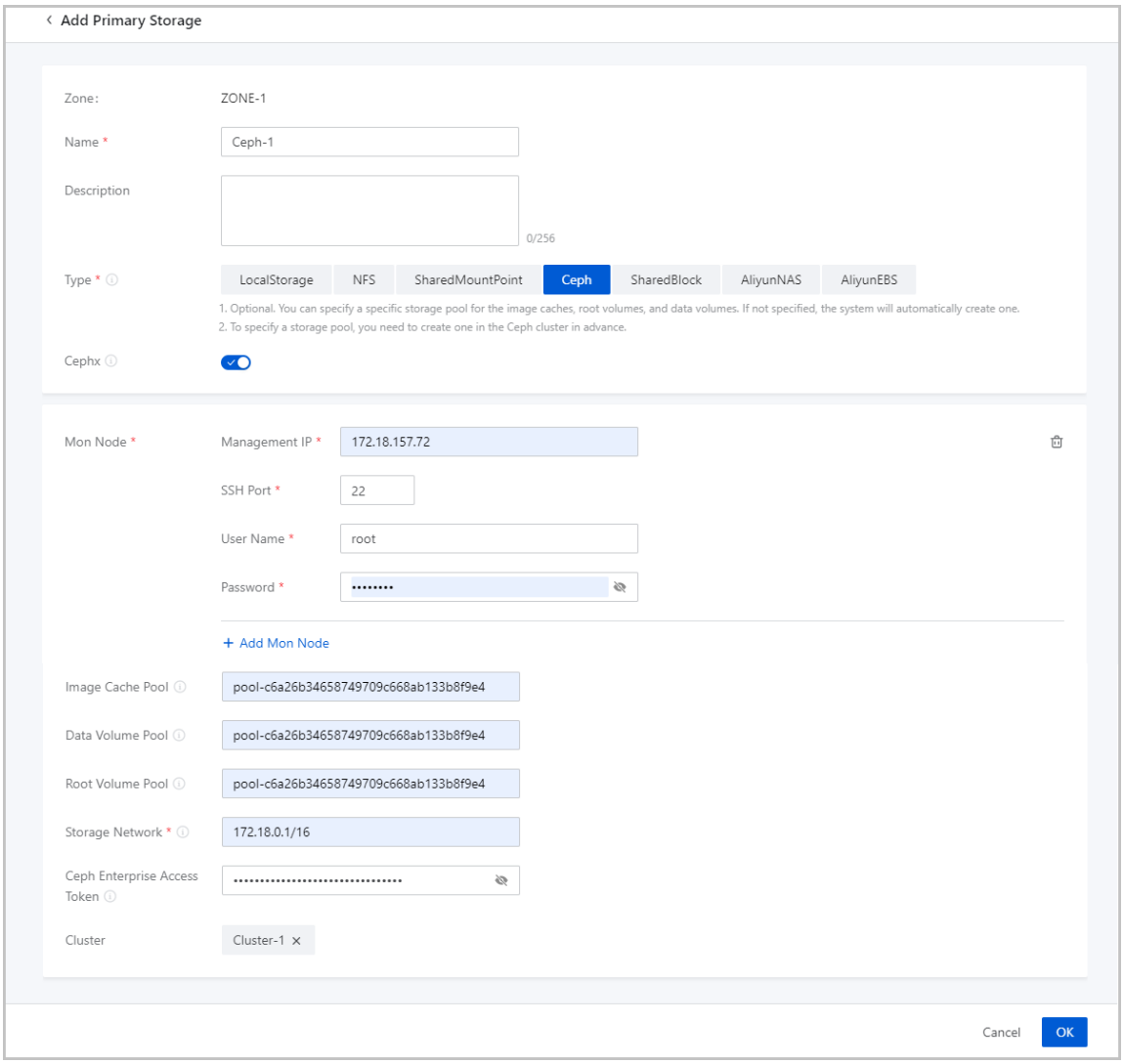


Figure 7-121: Add ZStack Ceph Enterprise Primary Storage



- Make sure that the NIC name of the L2 network is consistent with the NIC name of the gateway node.

7. Elastic Baremetal Instance

Elastic Baremetal Instance: An elastic baremetal instance has the same performance as physical servers and allows elastic scaling. You can apply for and scale resources based on your needs.

- The following two startup methods are supported for elastic baremetal instances:
  - Volume: Uses a volume as the system volume of the elastic baremetal instance to install and deploy the operating system.
  - Local Disk: Uses a local disk as the system disk of the elastic baremetal instance to install and deploy the operating system.
  - The Local Disk (Non Take-Over) and Local Disk (Take-Over) methods are supported:
    - Local Disk (Non Take-Over): When you use a baremetal node to create the elastic baremetal instance, the operating system is downloaded from the Cloud and installed on the elastic baremetal instance. This method will format the local system disk.
    - Local Disk (Take-Over): When you use a baremetal node to create the elastic baremetal instance, the original operating system on the local system disk is used as the operating system of the elastic baremetal instance.
- The following describes the resources supplied to elastic baremetal instances of different startup methods:
  - For elastic baremetal instances of both the volume startup method and local disk startup method, baremetal nodes provide compute resources and L3 networks on the Cloud are used as the business networks.
  - For elastic baremetal instances of the volume startup method, SharedBlock or Ceph primary storages on the Cloud provide storage resources and the provision network provides support for PXE boot.
  - For elastic baremetal instances of local disk startup method, the local disks of the instances provide storage resoures. If you attach data volumes to the instances, SharedBlock or Ceph primary storages on the Cloud also provides storage resources
- We recommend that you create an elastic baremetal instance by using an image that has installed the agent. Otherwise, you cannot open the console of the elastic baremetal instance, modify the password of the instance, attach a volume to or detach a volume from the instance, or attach a network to or detach a network from the instance.

- By default, the supported BIOS mode of the image used to create an elastic baremetal instance is UEFI. To use an image whose BIOS mode is Legacy, contact the official technical support.
- You can configure business networks for elastic baremetal instances. If you attach an L2 network to the cluster where your baremetal nodes reside, elastic baremetal instances and VM instances that share the same L2 network with the elastic baremetal instances can access each other without using the gateway.
- Elastic baremetal instances of the volume startup method allow you to release the associated baremetal node upon instance power-off. If you enable this feature, when an elastic baremetal instance of the volume startup method is powered off, the associated baremetal node is automatically released and can be used by another elastic baremetal instance. This mechanism avoids resource idling.

On the displayed page, set the following parameters:

- **Name**: Set a name for the elastic baremetal instance. A name can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the elastic baremetal instance.
- **Tag**: Optional. Attach a tag to the elastic baremetal instance.
- **Elastic Baremetal Cluster**: Optional. Select an elastic baremetal cluster to filter baremetal nodes in the cluster.

  Note:
  If you do not select an cluster, the cluster where the selected baremtal node resides is used.

- **Creation Mode**: Select a creation mode. You can select Add By Baremetal Node or Add By Baremetal Offering.

  If you select Add By Baremetal Node, set the following parameters:

  - **Baremetal Node**: Select a baremetal node based on the startup method. Three startup methods are supported: Volume, Local Disk (Non Take-Over), and Local Disk (Take-Over).

    — If you select the Volume startup method, configure the following parameters:

- **Power Off To Release Baremetal Node**: When an elastic baremetal instance is powered off, the associated baremetal node is automatically released and can be used by another elastic baremetal instance. This mechanism avoids resource idling. By default, this feature is disabled.

  Note:

  If you choose to release a baremetal instance upon power-off, note that:

  - This feature may change the associated baremetal node. The operating system will clean up business NIC configurations of the elastic baremetal instance. If your resources are sufficient, we recommend that you do not use this feature.
  - If you select Add By Baremetal Node and enable this feature, you need to manually select a baremetal node and configure the business NIC when you restart the elastic baremetal instance.
  - If you select Add By Baremetal Offering and enable this feature, you do not need to manually select a baremetal node but need to configure the business NIC when you restart the elastic baremetal instance.

- **Image**: Select an image to create the elastic baremetal instance. The mainstream x86_64 operating systems and some ARM operating systems are supported. The following table lists the supported OSs.

CPU Architecture	OS
x86	• Windows 2012 • Windows 2016 • Windows 2019 • Ubuntu 18 LTS • Ubuntu 20 LTS • CentOS 8
ARM	• Kylin V10 • CentOS 7

  Note:

  When you select an image, note that:

- We recommend that you use images with the agent installed. Otherwise, you cannot launch the consoles, modify the password, attach or detach volumes , attach or detach networks, or view monitoring data of an elastic baremetal instance that uses the image.
- By default, the BIOS of the image that you can use to create an elastic baremetal instance is in UEFI mode. If you need to use an image whose BIOS is in Legacy mode, contact the official technical support.

- **Advanced**: Configure advanced settings for the elastic baremetal instance.
  - **Data Disk Offering**: Optional. Select a disk offering for the elastic baremetal instance. If you select a disk offering, a data volume is created and attached to the instance. By default, a disk offering is not selected.
  - **Storage Allocation Policy**: Optional. Select a primary storage where the root volume and data volume of elastic baremetal instance reside. Default: Random.
  - **Gateway Node Allocation Policy**: Optional. The policy that is used to allocate a gateway node when you create an elastic baremetal instance. Default: LeastBmPreferredGatewayAllocatorStrategy.
    Valid values: LeastBmPreferredGatewayAllocatorStrategy, LastGatewayPreferredAllocatorStrategy, and DefaultGatewayAllocatorStrategy.
  - **First Assigned Gateway Node**: Optional. Select a gateway node for the first startup of the elastic baremetal instance. If you do not specify a gateway node, the gateway node selected based on the gateway node allocation policy is used.

    Note:
    This option takes effect only on the first start-up of the elastic baremetal instance. Afterwards, gateway nodes are assigned based on the gateway node allocation policy.

— If you select the Local Disk (Non Take-Over) startup method, configure the following parameters:

- **System Disk**: Select a local disk as the system disk of the elastic baremetal instance.

  Note:

Make sure that the local disk selected as the system volume of the elastic baremetal instance is set as the first boot device in the BIOS.

- **Image**: Select an image to create the elastic baremetal instance. The mainstream x86_64 operating systems and some ARM operating systems are supported. The following table lists the supported OSs.

CPU Architecture	OS
x86	• Windows 2012 • Windows 2016 • Windows 2019 • Ubuntu 18 LTS • Ubuntu 20 LTS • CentOS 8
ARM	• Kylin V10 • CentOS 7

Note:

When you select an image, note that:

- We recommend that you use images with the agent installed. Otherwise, you cannot launch the consoles, modify the password, attach or detach volumes , attach or detach networks, or view monitoring data of an elastic baremetal instance that uses the image.
- By default, the BIOS of the image that you can use to create an elastic baremetal instance is in UEFI mode. If you need to use an image whose BIOS is in Legacy mode, contact the official technical support.

- **Advanced**: Configure advanced settings for the elastic baremetal instance.
  - **Gateway Node Allocation Policy**: Optional. The policy that is used to allocate a gateway node when you create an elastic baremetal instance. Default: LeastBmPreferredGatewayAllocatorStrategy.
    Valid values: LeastBmPreferredGatewayAllocatorStrategy, LastGatewayPreferredAllocatorStrategy, and DefaultGatewayAllocatorStrategy.
  - **First Assigned Gateway Node**: Optional. Select a gateway node for the first startup of the elastic baremetal instance. If you do not specify a gateway node,

the gateway node selected based on the gateway node allocation policy is used.

> **Note:**
> This option takes effect only on the first start-up of the elastic baremetal instance. Afterwards, gateway nodes are assigned based on the gateway node allocation policy.

— If you select the Local Disk (Take-Over) startup method, configure the following parameters:

- **Advanced**: Configure advanced settings for the elastic baremetal instance.
  - **Gateway Node Allocation Policy**: Optional. The policy that is used to allocate a gateway node when you create an elastic baremetal instance. Default: LeastBmPreferredGatewayAllocatorStrategy.
    Valid values: LeastBmPreferredGatewayAllocatorStrategy, LastGatewayPreferredAllocatorStrategy, and DefaultGatewayAllocatorStrategy.
  - **First Assigned Gateway Node**: Optional. Select a gateway node for the first startup of the elastic baremetal instance. If you do not specify a gateway node, the gateway node selected based on the gateway node allocation policy is used.

    > **Note:**
    > This option takes effect only on the first start-up of the elastic baremetal instance. Afterwards, gateway nodes are assigned based on the gateway node allocation policy.

If you select Add By Baremetal Offering, set the following parameters:

- **Baremetal Offering**: Select a baremetal offering based on the startup method. Three startup methods are supported: Volume, Local Disk (Non Take-Over), and Local Disk (Take-Over).

  — If you select the Volume startup method, configure the following parameters:

  - **Quantity**: Enter the number of baremetal instances you need to create.
  - **Power Off To Release Baremetal Node**: When an elastic baremetal instance is powered off, the associated baremetal node is automatically released and can

be used by another elastic baremetal instance. This mechanism avoids resource idling. By default, this feature is disabled.

Note:

If you choose to release a baremetal instance upon power-off, note that:

- This feature may change the associated baremetal node. The operating system will clean up business NIC configurations of the elastic baremetal instance. If your resources are sufficient, we recommend that you do not use this feature.
- If you select Add By Baremetal Node and enable this feature, you need to manually select a baremetal node and configure the business NIC when you restart the elastic baremetal instance.
- If you select Add By Baremetal Offering and enable this feature, you do not need to manually select a baremetal node but need to configure the business NIC when you restart the elastic baremetal instance.

- **Image**: Select an image to create the elastic baremetal instance. The mainstream x86_64 operating systems and some ARM operating systems are supported. The following table lists the supported OSs.

CPU Architecture	OS
x86	• Windows 2012 • Windows 2016 • Windows 2019 • Ubuntu 18 LTS • Ubuntu 20 LTS • CentOS 8
ARM	• Kylin V10 • CentOS 7

Note:

When you select an image, note that:

- We recommend that you use images with the agent installed. Otherwise, you cannot launch the consoles, modify the password, attach or detach volumes

, attach or detach networks, or view monitoring data of an elastic baremetal instance that uses the image.

- By default, the BIOS of the image that you can use to create an elastic baremetal instance is in UEFI mode. If you need to use an image whose BIOS is in Legacy mode, contact the official technical support.

- **Advanced**: Configure advanced settings for the elastic baremetal instance.
  - **Data Disk Offering**: Optional. Select a disk offering for the elastic baremetal instance. If you select a disk offering, a data volume is created and attached to the instance. By default, a disk offering is not selected.
  - **Storage Allocation Policy**: Optional. Select a primary storage where the root volume and data volume of elastic baremetal instance reside. Default: Random.
  - **Gateway Node Allocation Policy**: Optional. The policy that is used to allocate a gateway node when you create an elastic baremetal instance. Default: LeastBmPreferredGatewayAllocatorStrategy.
    Valid values: LeastBmPreferredGatewayAllocatorStrategy, LastGatewayPreferredAllocatorStrategy, and DefaultGatewayAllocatorStrategy.
  - **First Assigned Gateway Node**: Optional. Select a gateway node for the first startup of the elastic baremetal instance. If you do not specify a gateway node, the gateway node selected based on the gateway node allocation policy is used.

    Note:
    This option takes effect only on the first start-up of the elastic baremetal instance. Afterwards, gateway nodes are assigned based on the gateway node allocation policy.

— If you select the Local Disk (Non Take-Over) startup method, configure the following parameters:

- **Quantity**: Enter the number of baremetal instances you need to create.
- **Image**: Select an image to create the elastic baremetal instance. The mainstream x86_64 operating systems and some ARM operating systems are supported. The following table lists the supported OSs.

CPU Architecture	OS
x86	• Windows 2012

CPU Architecture	OS
	• Windows 2016 • Windows 2019 • Ubuntu 18 LTS • Ubuntu 20 LTS • CentOS 8
ARM	• Kylin V10 • CentOS 7

Note:

When you select an image, note that:

- We recommend that you use images with the agent installed. Otherwise, you cannot launch the consoles, modify the password, attach or detach volumes , attach or detach networks, or view monitoring data of an elastic baremetal instance that uses the image.
- By default, the BIOS of the image that you can use to create an elastic baremetal instance is in UEFI mode. If you need to use an image whose BIOS is in Legacy mode, contact the official technical support.

- **Advanced**: Configure advanced settings for the elastic baremetal instance.
  - **Gateway Node Allocation Policy**: Optional. The policy that is used to allocate a gateway node when you create an elastic baremetal instance. Default: LeastBmPreferredGatewayAllocatorStrategy. Valid values: LeastBmPreferredGatewayAllocatorStrategy, LastGatewayPreferredAllocatorStrategy, and DefaultGatewayAllocatorStrategy.
  - **First Assigned Gateway Node**: Optional. Select a gateway node for the first startup of the elastic baremetal instance. If you do not specify a gateway node, the gateway node selected based on the gateway node allocation policy is used.

    Note:

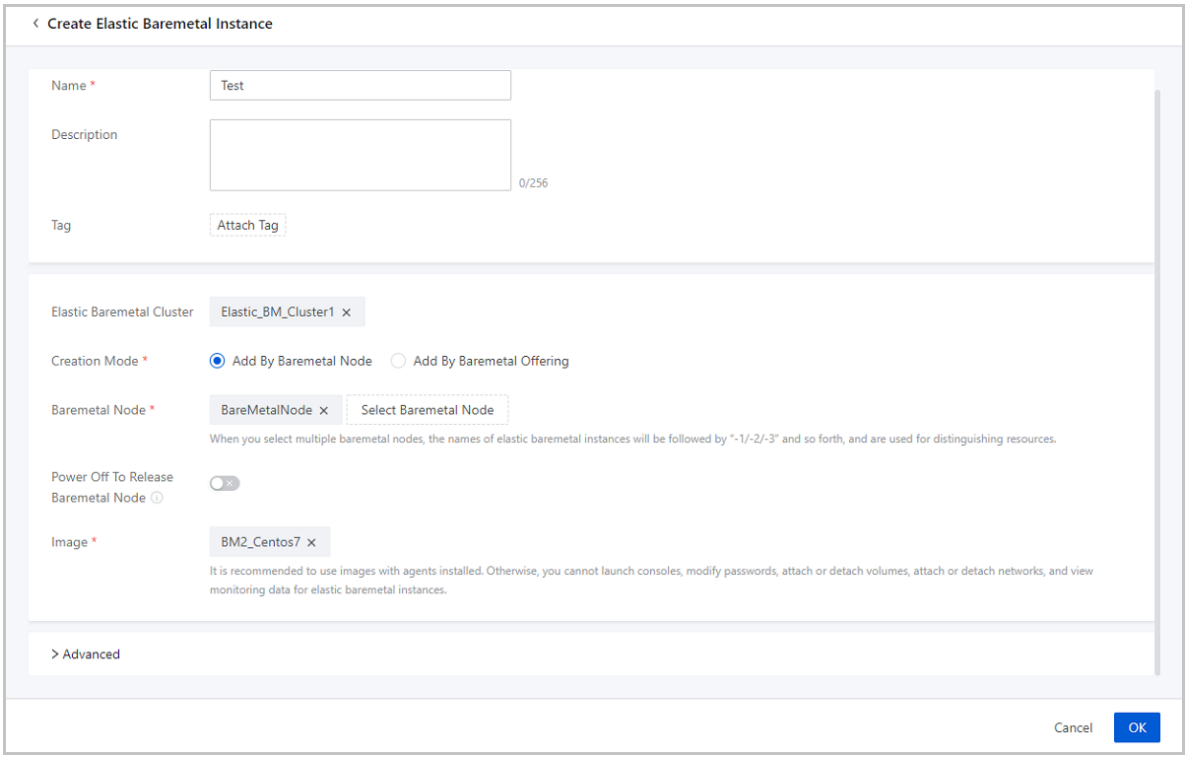
    This option takes effect only on the first start-up of the elastic baremetal instance. Afterwards, gateway nodes are assigned based on the gateway node allocation policy.

— If you select the Local Disk (Take-Over) startup method, configure the following parameters:

- **Quantity**: Enter the number of baremetal instances you need to create.
- **Advanced**: Configure advanced settings for the elastic baremetal instance.
  - **Gateway Node Allocation Policy**: Optional. The policy that is used to allocate a gateway node when you create an elastic baremetal instance. Default: LeastBmPreferredGatewayAllocatorStrategy.
    Valid values: LeastBmPreferredGatewayAllocatorStrategy, LastGatewayPreferredAllocatorStrategy, and DefaultGatewayAllocatorStrategy.
  - **First Assigned Gateway Node**: Optional. Select a gateway node for the first startup of the elastic baremetal instance. If you do not specify a gateway node, the gateway node selected based on the gateway node allocation policy is used.

    Note:
    This option takes effect only on the first start-up of the elastic baremetal instance. Afterwards, gateway nodes are assigned based on the gateway node allocation policy.

Figure 7-122: Create Elastic Baremetal Instance



7.8 vCenter

7.8.1 What is vCenter?

VMware Management: manipulates VMware vCenter via VMware public API interfaces and seamlessly integrates some features of VMware vCenter Server to achieve a unified management of multiple virtualization platforms on ZStack Cloud. is a centralized management platform of a VMware vCenter Server. If you deployed a VMware vCenter Server, you can use VMware Management of ZStack Cloud to take over the VMware vCenter Server. Then you can view vSphere servers and virtual machines managed by the VMware vCenter Server, use VMware vSphere resources in the virtual data center, and perform operations on virtual machines in the VMware Center clusters.

- You can manage VMware virtualization environments in an existing data center, and view vSphere server resources and VM resources managed by VMware vCenter Server. In addition , you can use VMware vSphere resources in a virtual data center, and perform common operations on VM instances in your VMware vCenter cluster.
- ZStack Cloud supports multiple vCenter versions, including 5.5, 6.0, 6.5, 6.7, and 7.0.

Note:

If you took over vCenter 7.0, to ensure that the VM console can open properly, we recommend that you download the trusted root CA certificate when you log into vCenter.

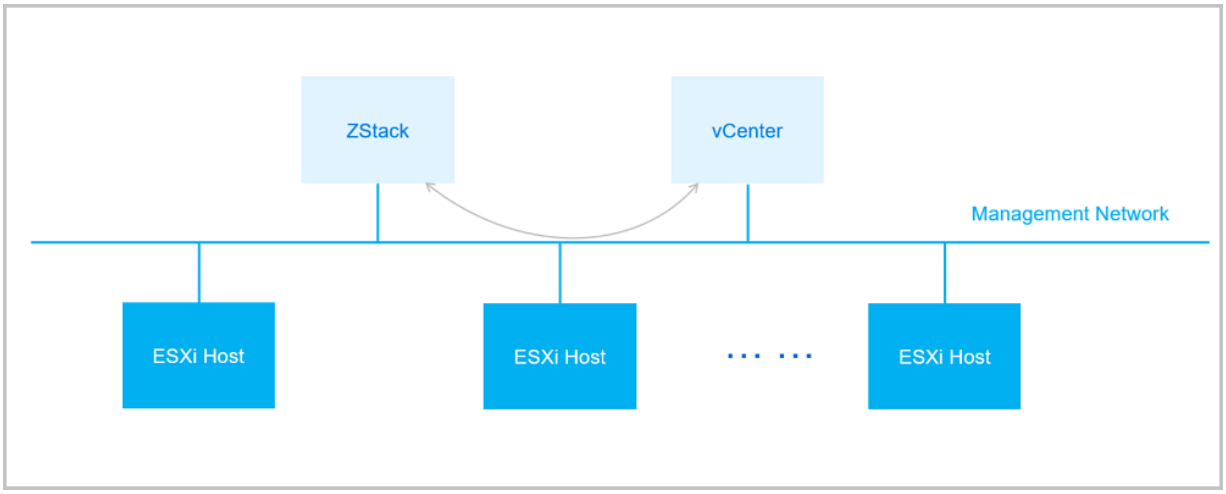
Concepts

- vSphere: an enterprise-class virtualization platform provided by VMware. It can convert a data center into an integrated computing infrastructure that includes compute, storage, and network resources. VMware vSphere consists of a batch of software applications, with ESXi and Center being the two core components.
- EXSi: type 1 hypersivor (bemetal hypervisor) that is installed directly on a baremetal server. It allows the creation and management of multiple virtual machines on an ESXi host.
- vCenter Server: a centralized management platform of physical and virual resources on a VMware vCenter. It allows one-click access and management of ESXi hosts, virtual machines, datastores, networks, and other resources.

External Access Fundamentals

ZStack Cloud sends cloud resource control requests to a vCenter by using the asynchronous event listening methods and receives the returned event contents. In addition, ZStack Cloud can also receive contents that are intuitively pushed by vCenters. This way, ZStack Cloud achieves bidirectional data synchronization.

Figure 7-123: ZStack Cloud Managing vCenter Diagram



7.9 Hybrid Cloud Management

7.9.1 What is Hybrid Cloud Management?

Hybrid Cloud Management provided by ZStack Cloud integrates the simple, strong, scalable, and smart (4S) features of ZStack Cloud Private Cloud and the advanced, secure, and stable features of Alibaba Cloud Public Cloud. It is a hybrid cloud management solution that seamlessly integrates **cloud services and terminals**, interconnecting the control panel and data panel.

Concepts

- ZStack Cloud Hybrid Cloud Management provides the following cloud computing products of Alibaba Cloud:
  - ECS Instance: An elastic compute server (ECS) instance is a VM instance created on Alibaba Cloud.
  - Disk: A disk provides storage space for an ECS instance created on Alibaba Cloud.
  - Image: An image is a template file that is used to create ECS instances. Images are categorized into custom images and Alibaba Cloud images.
  - Security Group: A security group provides security control services for ECS instances on the L3 network layer. It filters the inbound or outbound packets of ECS instances based on specified security rules.
  - VPC: A virtual private cloud (VPC) is a private network used for ECS instances created on Alibaba Cloud.
  - VIP: An elastic IP address (EIP) is an IP address in Alibaba Cloud public networks. You can attach EIPs to ECS instances so the ECS instances can access public networks by using the EIPs.
- VPN: establishes a site-to-site IPsec VPN channel to enable communications between private networks in a local data center and Alibaba Cloud VPCs. This section includes the following services:
  - VPN Gateway: A virtual private network (VPN) gateway establishes a secure connection between a local data center and Alibaba Cloud VPC by using an encrypted channel.
  - VPN Customer Gateway: A VPN customer gateway provides services for a local data center .
  - VPN Connection: A VPN connection is an encrypted communication channel established between a VPN gateway and VPN customer gateway.

- Express Connect: Express Connect uses physical connections (electric cables or optical fibers leased from operators) to connect local data centers with Alibaba Cloud access points and Alibaba Cloud VPCs. This way, private networks on the Cloud and in local data centers can communicate with each other in a fast, stable, and secure manner. This section includes the following services:
  - Router Interface: A router interface is a virtual device that is used to establish communicat ion channels and control their status.
  - Virtual Border Router: A virtual border router (VBR) is virtualized from a switch port that is connected with an Alibaba Cloud physical connection. A VBR forwards data between a VPC and local data center.
- Alibaba Cloud NAS: Alibaba Cloud NAS is a network-attached file storage service. It provides highly reliable and available distributed file systems that can be accessed by using standard file access protocols. In addition, Alibaba Cloud NAS is scalable in storage space and performance and can be managed in a namespace while shared with multiple users. ZStack Cloud seamlessly integrates with Alibaba Cloud NAS. In ZStack Cloud Private Cloud environments, you can add primary storages of the **Aliyun NAS** type to the Cloud and thus use Alibaba Cloud distributed storage deployed independently from the Cloud. This section includes the following services:
  - File System: A file system is a backend storage system used for Alibaba Cloud NAS primary storage. Before you add an Alibaba Cloud primary storage, you need to add an NAS file system.
  - Permission Group: A permission group is a whitelist mechanism that Alibaba Cloud provides for IP addresses or ranges. ECS instances of specific IP addresses or in specific IP ranges are granted access to file systems based on specified permission rules.
- Data Center: Data centers are resources associated with Alibaba Cloud regions and zones. The following describes regions and zones:
  - Region: A region is a physical area where data centers reside. A region in ZStack Cloud Hybrid Cloud corresponds to a region in Alibaba Cloud.
  - Zone: A zone is a physical area in a region that is independent from other zones in the region in terms of electricity and network supplies.
- Setting: ZStack Cloud Hybrid Cloud provides the following basic settings:

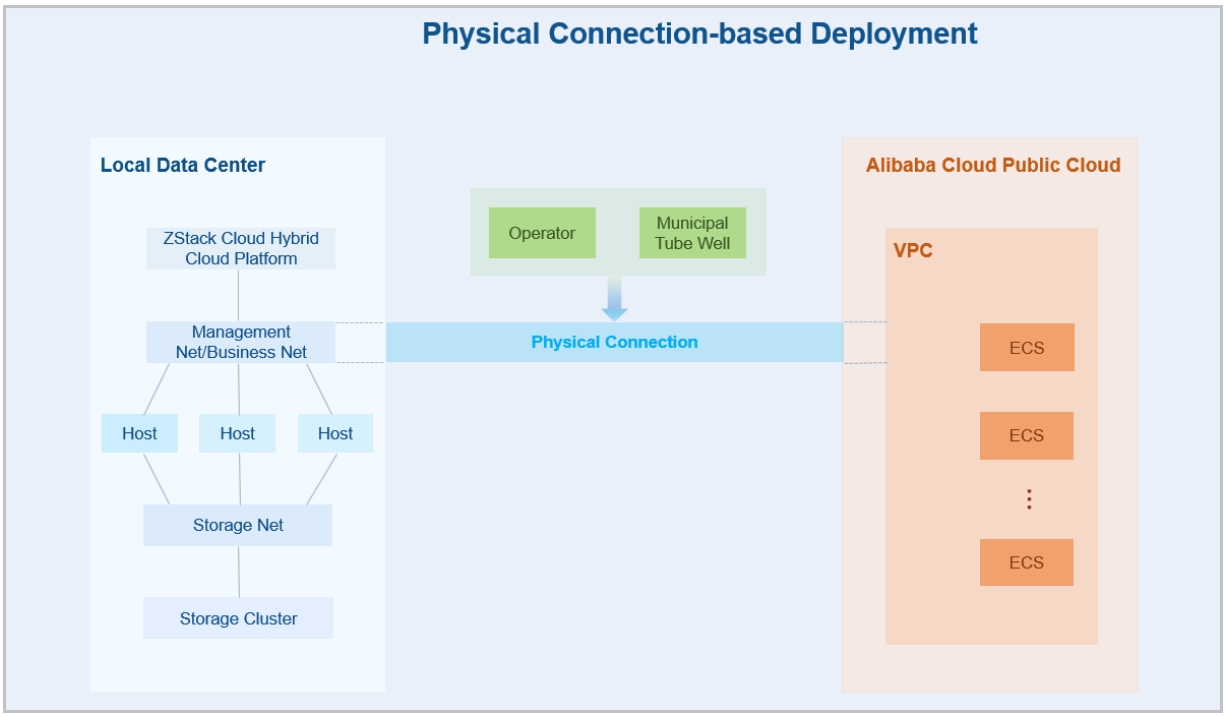
- AccessKey Management: An AccessKey pair is an identity credential that has access to APIs of Alibaba Cloud or Private Alibaba Cloud. It has full access to the Cloud. An AccessKey pair consists of AccessKey ID and AccessKey secret.
- Hybrid Cloud Setting: Hybrid cloud setting allows you to configure settings that take effect on the whole platform.

Physical Deployment

ZStack Cloud Hybrid Cloud uses the in-process micro-services architecture and does not include other modules. ZStack Cloud management nodes need to access the Internet so they can call Alibaba Cloud Public Cloud APIs.

Physical connection-based deployment: uses physical connections to establish **local-remote** inter-connected networks, thereby connecting a local data center with Alibaba Cloud Public Cloud.

Figure 7-124: Physical Connection-based Deployment



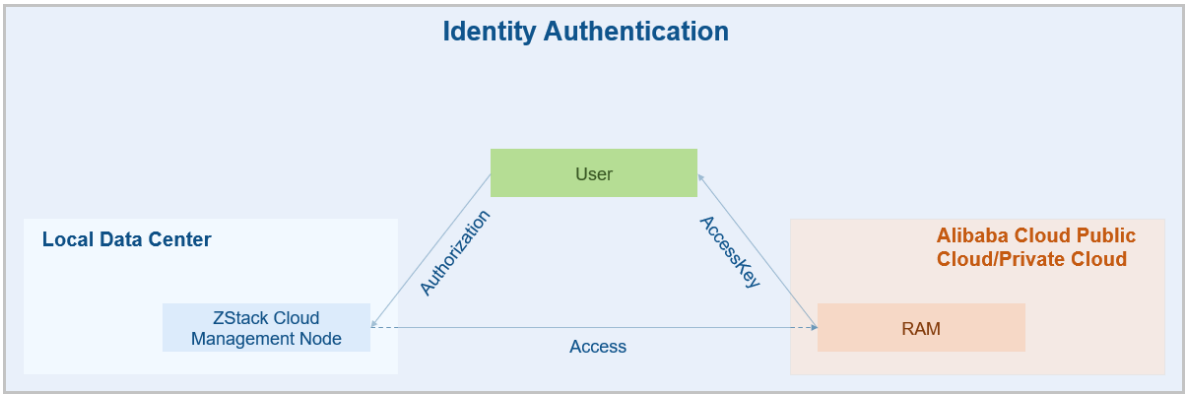
Architecture

ZStack Cloud Hybrid Cloud includes the following modules:

- **Identity Authentication**:

Alibaba Cloud AccessKey: integrates Resource Access Management of Alibaba Cloud Public Cloud or Alibaba Cloud Private Cloud. A user authorized with an Alibaba Cloud AccessKey pair can access remote resources.

Figure 7-125: Identity Authentication



- **Network Interconnection**:

  You can use IPsec tunnels or Alibaba Cloud Express Connect to connect local Private Cloud to Alibaba Cloud Public Cloud. This way, L3 **local-remote** networks can access each other. **Local-remote** network interconnection is the foundation of ZStack Cloud Hybrid Cloud.

  ZStack Cloud Hybrid Cloud allows you to use IPsec tunnels or Alibaba Cloud Express Connect to establish interconnected networks.

Figure 7-126: IPsec Tunnel

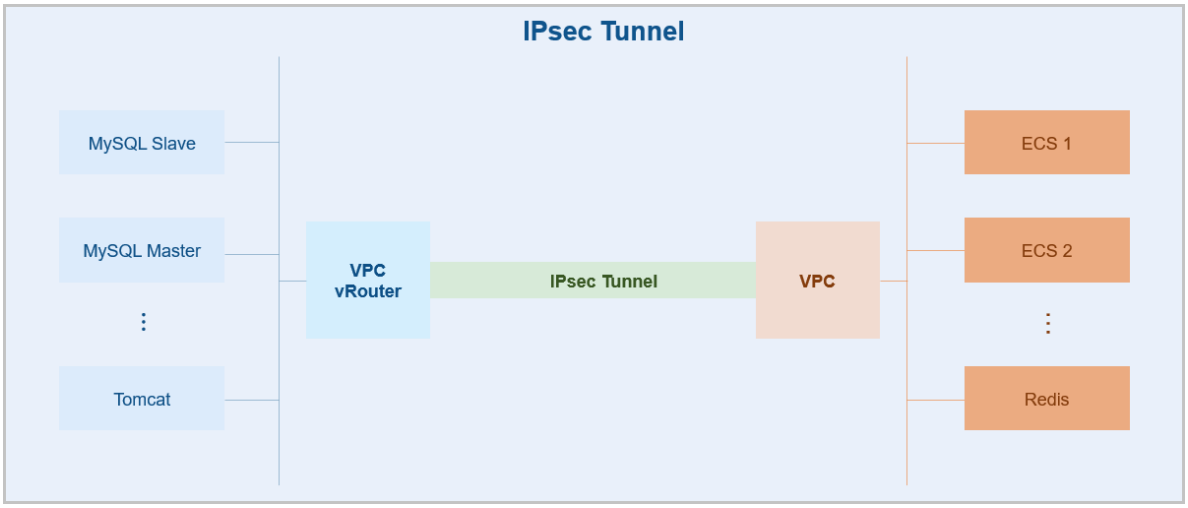
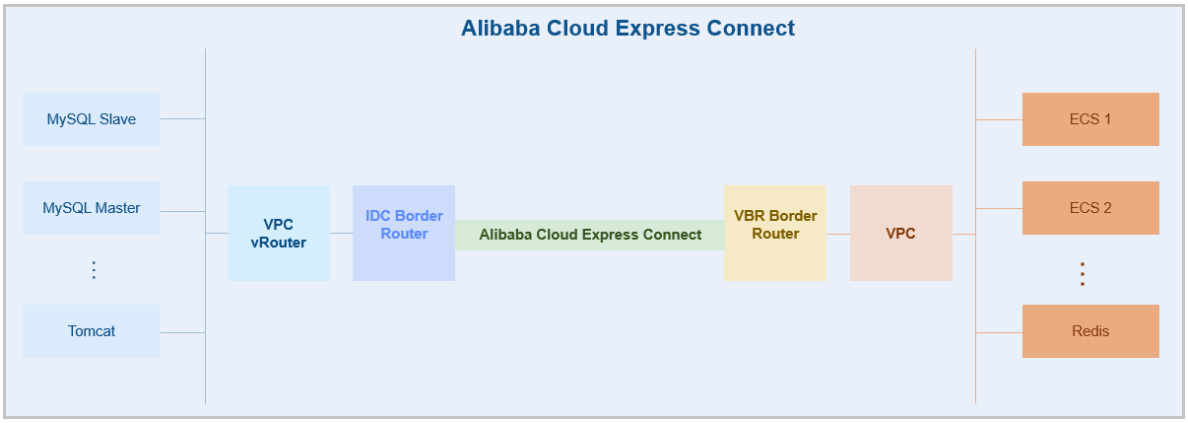


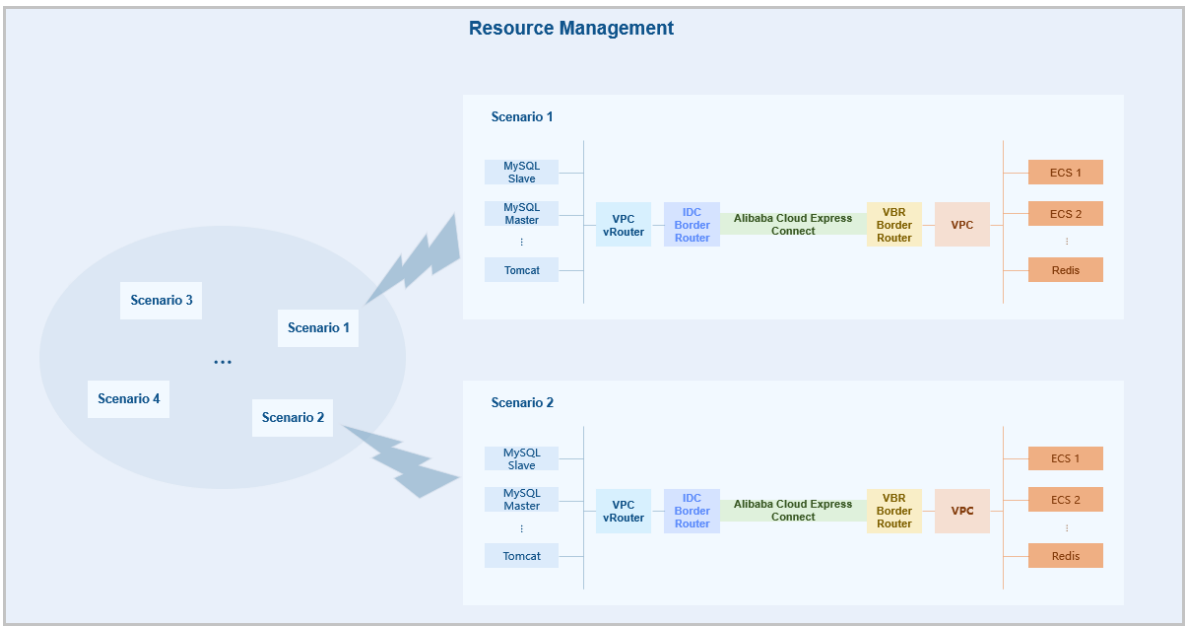
Figure 7-127: Alibaba Cloud Express Connect



- **Resource Management**:

  You can authorize a RAM user to manage Alibaba Cloud Public Cloud resources, including ECS instances, VBR, VPC, and virtual switches.

  Resource Management



- **Business Implementation**:

  The identity authentication, network interconnection, and resource management mechanisms combined allow for the establishment of a flexible and elastic business system architecture. After the hybrid cloud platform is established, you can deploy flexible and multi-dimensional business modes.

Characteristics

ZStack Cloud Hybrid Cloud have the following characteristics:

- Seamless integration:

  ZStack Cloud Hybrid Cloud seamlessly integrates Public Cloud with ZStack Cloud hybrid cloud platform, combining the benefits ZStack Cloud Private Cloud. This way, users can manage public clouds and private clouds in a unified platform.
- Seamless integration:

  ZStack Cloud Hybrid Cloud allows seamless upgrading without affecting business continuity.
- Ease of use:

  ZStack Cloud Hybrid Cloud seamlessly integrates **cloud services and terminals** in a unified cloud platform. You can easily manage local private clouds and access various resources on the public cloud based on your business needs.

Scenarios

- Data backup on the Cloud

  In financial and medical industries, data retention must meet compliance requirements. However, backing up data in local data centers has high data risks, incurs high costs, and is hard for operations and maintenance. In these scenarios, you can use ZStack Cloud Hybrid Cloud to back up data on the Cloud, ensuring stable data storage and lowering the storage cost.
- Data storage on the Cloud

  Enterprises and institutions need to store large amounts of data. In these scenarios, you can use ZStack Cloud Hybrid Cloud to store data on the Cloud, lowering your investment and management costs and allowing data access from multiple regions and zones.
- Data migration on the Cloud

  Enterprises and institutions need to exchange data in different places. In these scenarios, you can use ZStack Cloud Hybrid Cloud to migrate data on the Cloud, ensuring that data can be transmitted in a stable manner without data loss.

8 Platform O&M

8.1 Network Topology

8.1.1 Global Network Topology

Global Topology

On the ZStack Cloud main menu, choose **Platform O&M** > **Network Topology** > **Global Topology**. Then the **Global Topology** page appears.

Supported Operations

The following table lists the operations that you can perform on the global topology.

Operations	Description
View	• You can view the global topology of the Cloud and drag and drop a resource for more flexible display of the topology. • **Directly Connected VM** shows the number of VM instances that are directed connected to a network.
Refresh	You can click the Refresh button to view the latest the global topology.
Export Picture	You can export the current global topology as an image in **png** format.
Show/Hide VM Instance	You can show or hide VM instances in the global topology. **Note:** If the number of VM instances directly connected to a network exceeds 50, the VM instances are hidden by default. To show the VM instances, you can click the plus sign (**+**) under the network.
Search	You can search for resources based on the resource type and properties. **Note:** • Supported types of resources include flat networks, VPC networks, public networks, VPC vRouters, and VM instances. • Supported resource properties include resource name and resource UUID.
Fit to Window	You can click the Fit to Window icon on the canvas to resize the topology to a proper size.
Zoom out	You can zoom out the network topology.

Operations	Description
Zoom in	You can zoom in the network topology.
Highlight Resource	You can select a resource and highlight the resource and its associated resources.
Hover resource details	You can hover your pointer over a resource and the details of the resource will be displayed.
View VPC vRouter/VM status	You can view the status of a VPC vRouter or VM instance by checking the color of the dot on the VPC vRouter or VM icon. For more infromation, see *VPC vRouter/VM Status and Dot Color Mappings*

VPC vRouter/VM Status and Dot Color Mappings

VPC vRouter/VM Status	Dot Color
Created	Blue
Starting	Blue
Running	Green
Stopping	Red
Stopped	Red
Restarting	Blue
Deleting	Neutral Color
Deleted	Neutral Color
Migrating	Blue
Expunging	Neutral Color
Pausing	Yellow
Paused	Yellow
Recovering from Paused State	Neutral Color
Volume Migrating	Neutral Color
Unknown	Neutral Color

8.2 Cloud Monitoring

8.2.1 Performance Analysis

Performance Analysis displays the performance metrics of key resources under monitoring in the Cloud. Cloud resources can be externally or internally monitored. You can use either method to monitor the performance of resources in the Cloud and improve O&S efficiency.

8.2.2 Capacity Management

Capacity Management visualizes the capacities and usages of key resources in the Cloud. You can use this feature to improve O&S efficiency.

Capacity Management displays the physical capacities and usages of key resources by using cards, and displays Top 10 resource capacities and usages, providing you a commanding view of your resource usages and greatly improving O&S efficiency.

8.2.3 MN Monitoring

MN monitoring allows you to view the health status of each management node when you use multiple management nodes to achieve high availability.

8.2.4 Monitoring and Alarm

The Monitoring and Alarm feature monitors time-series data and events and sends alarm messages to specified endpoints by using SNS. Resource alarms, event alarms, and extended alarms are supported. The supported endpoints include the system, emails, DingTalk, HTTP applications, text messages, and Microsoft Teams. For some resource alarms, you need to install the agent before they can work as expected.

Concepts

- **Monitoring System**:

  A monitoring system provides the following features:

  - Monitor the following two types of time-series data:
    - Resource utilizations such as CPU utilization of VM instances and memory utilization of hosts
    - Resource capacities such as available number of IP addresses and total number of running VM instances

- Event collection: collects events predefined on the Cloud, such as host disconnection and VM HA enabling.
- Alarm: triggers alarms on time-series data or events.
- Audit: records all operations and allows queries.
- Customization: allows you to customize alarms and message templates and use predefined alarm templates and resource groups.
  - The following three types of alarms are supported:
    - Resource alarm: triggers alarms on time-series data. For example, you can configure an alarm for VM instances. If the CPU utilization of a VM instance exceeds 80% by five consecutive minutes, send an alarm message to an email address.
    - Event alarm: triggers alarms on events, also called event subscription. For example, you can configure an alarm for host disconnection. If a host is disconnected, an alarm message is sent to DingTalk.
    - Extended alarm: receives alarm messages from message sources. For example, if a Ceph Enterprise storage pool is downgraded, an alarm message is sent to the system of the Cloud.
  - A message template specifies the text template of a resource alarm message or event alarm message sent to an SNS system.
    - A message template and message recovery template are provided by the system. If you do not create a template, the system uses the predefined templates.
    - You can create multiple message templates and can set only one template as the default template. Messages are formatted by using the default template.
    - You can use `${}` in a template to quote variables configured in an alarm or event.
    - You can configure email, DingTalk, text message, and Microsoft Teams as an endpoint in a message template. Messages sent by using email, DingTalk, text message, or Microsoft Teams are sent in the specified format.
  - A message source is used to take over extended alarm messages. If you configure alarms for message sources, extended alarm messages can be sent to various endpoints. This enables centralized management of alarm messages and improves O&M efficiencies. You can configure a message source to take over alarm messages of Ceph Enterprise.
  - An alarm template is a template of alarm rules. If you associate an alarm template with a resource group, an alarm is created to monitor the resources in the group.

— A resource group consists of resources grouped based on your business needs. If you associate an alarm template with a resource group, the alarm rules specified by the template take effect on all the resources in the group.

- **SNS**:

  SNS sends alarm messages to the specified endpoints. The supported types of endpoints include the system, emails, DingTalk, HTTP applications, text messages, and Microsoft Teams.

  Endpoints:

  - The system provides the system-type endpoint. If you associate an alarm with this endpoint , alarm messages will be displayed below the Recent Message button in the top right corner of the UI.
  - You can also create an endpoint of the email, DingTalk, HTTP application, text message, or Microsoft Teams type.

8.2.4.1 Alarm

8.2.4.1.1 Create an Alarm

On the main menu of ZStack Cloud, choose **Platform O&M** > **Cloud Monitoring** > **Alarm Service** > **Alarm**. Then, the **Alarm** page is displayed.

The following lists the three alarm creation scenarios:

- Create a resource alarm
- Create an event alarm
- Create an extended alarm

Create Resource Alarm

The system provides default resource alarms. In addition, you can customize resource alarms based on your needs. On the **Resource Alarm** tab, click **Create Resource Alarm**. Then, the **Create Resource Alarm** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the resource alarm.
- **Description**: Optional. Enter a description for the resource alarm.
- **Resource Type**: Select a resource type. Valid values: VM Instance, Baremetal Instance, Elastic Baremetal Instance, VPC vRouter, Image, Backup Storage, System Data Directory,

Host, L3 Network, Volume, VIP, Primary Storage, Listener, Management Node, Project Resource, and CDP Task.

Note that you can select Project Resource and CDP Task only after you have purchased Enterprise Management License and Continuous Data Protection (CDP) License, respectively.

- **Metric Item**: Select a metric item of the selected resource type.

  Note:

  - Multiple metric items are available for every type of resources. You can select a metric item based on your business needs.
  - Some metric items are associated with additional parameter settings. If you select such metric items, you need to configure the additional parameter settings.
  - Some metrics items are available only after the agent is installed on the related resource. .
  - If you need to monitor memory data, we recommend that you use internal monitoring for this purpose. This is because internal monitoring yields a more accurate memory data than external monitoring.
  - You can create resource alarms for key cloud resources such as VM instances, hosts, and primary storages on the details page of the resources.

- **Alarm Coverage**: Select one or more resources on which the alarm takes effect.

  — If you select multiple resources of the specified type, all the resources for which the alarm is configured are monitored. If the trigger condition of a resource is met, the alarm is triggered.

  — If you select only one resource of the specified type, the resource for which the alarm is configured is monitored. If the trigger condition of the resource is met, the alarm is triggered.

  Note:

  - You can configure fine-grained alarms for a resource.
  - For example, you can configure an alarm to monitor the utilization of a CPU of a VM instance.

- **Alarm Trigger Rule**: Select a comparison symbol and specify a threshold and duration.
- **Alarm Period**: Select an alarm period.

  — **Only 1 time**:

  ■ Alarm is triggered only once for a resource.

  For example,

- Assume that you configure an alarm for multiple resources. If the trigger condition of a resource is met, the alarm is triggered. After that, even if the trigger condition of this resource is met again, the alarm is no longer triggered.

  Assume that you configure an alarm for a resource. If the trigger condition of the resource is met, the alarm is triggered. After that, even if the trigger condition of the resource is met again, the alarm is no longer triggered.

- The alarm message is sent to the endpoint (if specified) for only once. In addition, the alarm message is displayed on Message Center only once.
- If the resource recovers but later meets the trigger condition again, the one-time alarm is triggered again.

— **Repetitive Alarm** :

- Alarm is triggered multiple times for a resource.

  For example,

  - Assume that you configure an alarm for multiple resources. If the trigger condition of a resource is met, the alarm is triggered. If the resource keeps meeting the trigger condition, the alarm is repetitively triggered based on the alarm period.

    Assume that you configure an alarm for a resource. If the trigger condition of the resource is met, the alarm is triggered. If the resource keeps meeting the trigger condition, the alarm is repetitively triggered based on the alarm period.

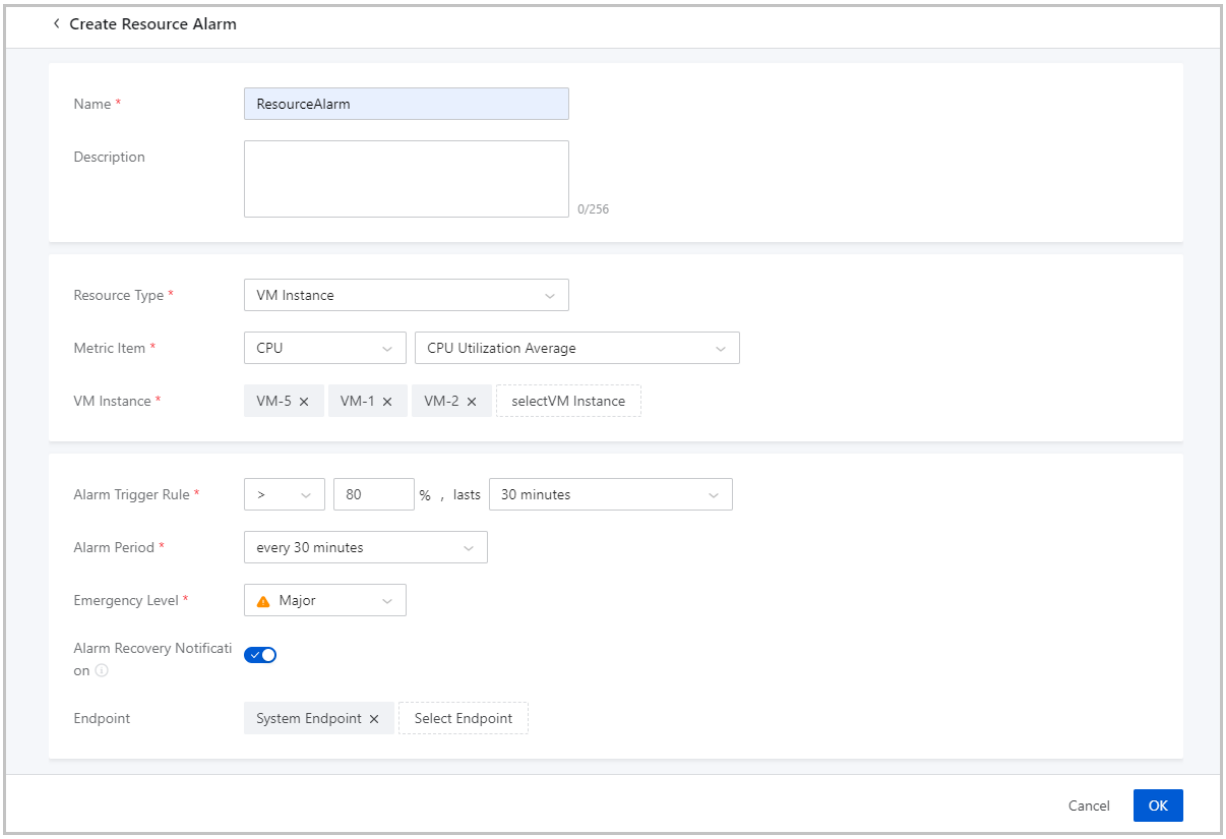
- Each time the alarm is triggered, the alarm message is sent to the endpoint (if specified). In addition, every alarm message is displayed on Message Center.

- **Emergency Level**: Set an emergency level. Valid values: Emergent, Major, and Info. Alarms of different emergency levels correspond to alarm messages of different emergency levels.
- **Alarm Recovery Notification**: Optional. If enabled, when a resource monitored by a resource alarm recovers from alarmed status, the system receives a notification. The recovery notification is sent according to the default recovery message template. You can customize the message content on the Message Template page.
- **Endpoint**: Optional. If specified, alarm messages are sent to the specified endpoint.

Note:

- You can specify multiple endpoints.
- You can specify the system endpoint or customize an endpoint.

Figure 8-1: Create Resource Alarm



Create Event Alarm

The system provides default event alarms. In addition, you can customize event alarms based on your needs. On the **Event Alarm** tab, click **Create Event Alarm**. Then, the **Create Event Alarm** page is displayed.

On the displayed page, set the following parameters:

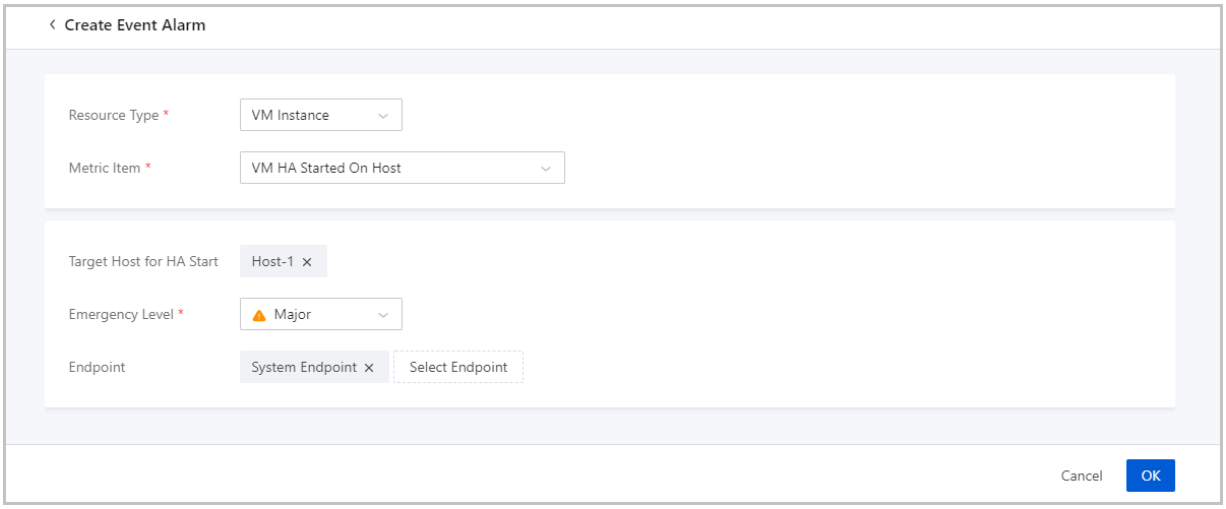
- **Resource Type**: Select a resource type. Valid values: VM Instance, VPC vRouter, Backup Storage, Management Node, Host, Primary Storage, vCenter, Backup Job, HA, Project Resource, and CDP Task.

  Note that you can select Project Resource and CDP Task only after you have purchased Enterprise Management License and Continuous Data Protection (CDP) License, respectively.
- **Metric Item**: Select a metric item of the selected resource type.
- **Emergency Level**: Set an emergency level. Valid values: Emergent, Major, and Info. Alarms of different emergency levels correspond to alarm messages of different emergency levels.
- **Endpoint**: Optional. If specified, alarm messages are sent to the specified endpoint.

Note:

- You can specify multiple endpoints.
- You can specify the system endpoint or customize an endpoint.

Figure 8-2: Create Event Alarm



Note:

- An event alarm is triggered only when the configured event occurs. The repetitive alarm mechanism is not available for event alarms.
- When a resource monitored by an event alarm recovers from alarmed status, the system receives a notification. The recovery notification is sent according to the default recovery message template. You can customize the message content on the Message Template page.
- If the configured event occurs again, the event alarm is triggered again.

Create Extended Alarm

Before you can create an extended alarm, you need to enable the extended alarm feature. To do this, choose **Settings** > **Platform Setting** > **Global Setting** > **Advanced** and turn on the **Extended Alarm Notification** switch.

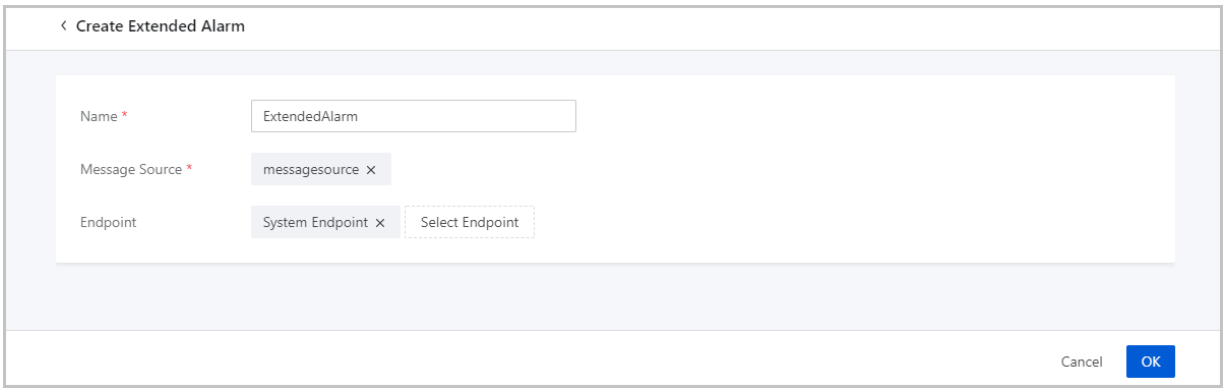
Then you can create an extended alarm to receive extended alarm messages. On the **Extended Alarm** tab, click **Create Extended Alarm**. Then the **Create Extended Alarm** page is displayed. On the displayed page, set the following parameters:

- **Name**: Enter a name for the extended alarm.

- **Message Source**: Select a source where you need to receive alarm messages.
- **Endpoint**: Optional. If specified, alarm messages are sent to the specified endpoint.

> **Note:**
>
> - You can specify multiple endpoints.
> - You can specify the system endpoint or customize an endpoint.

Figure 8-3: Create Extended Alarm



8.2.4.2 One-click Alarm

A one-click alarm integrates multiple metrics of a resource. You can create one-click alarms for multiple resources to monitor these resources.

8.2.4.3 Alarm Template

8.2.4.3.1 Create an Alarm Template

On the main menu of ZStack Cloud, choose **Platform O&M** > **Cloud Monitoring** > **Alarm Service** > **Alarm Template**. On the **Alarm Template** page, click **Create Alarm Template**. Then, the **Create Alarm Template** page is displayed.

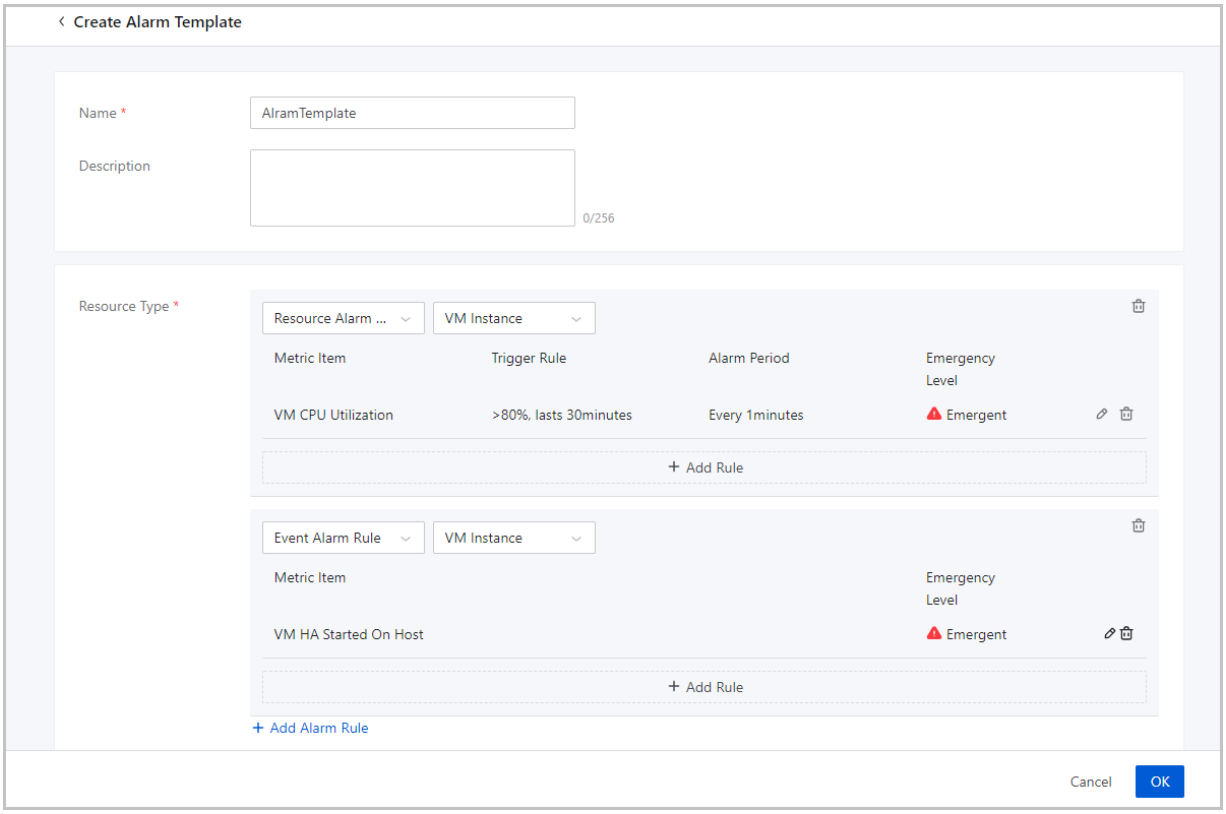
On the displayed page, set the following parameters:

- **Name**: Enter a name for the alarm template.
- **Description**: Optional. Enter a description for the alarm template.
- **Resource Type**: add an alarm rule to the template.
  - **Alarm Type**: Select resource alarm or event alarm.
  - **resource Type**: Select a resource type.

- If you create a resource alarm rule, you can select the following resource types: VM Instance, Baremetal Instance, Elastic Baremetal Instance, VPC vRouter, Backup Storage , Host, L3 Network, VIP, Primary Storage, Listener, and License.
- If you create an event alarm rule, you can select the following resource types: VM Instance, VPC vRouter, Backup Storage, Host, and Primary Storage.

— **Add Rule**: Add an alarm rule for the selected resource.

Figure 8-4: Create Alarm Rule



8.2.4.4 Resource Group

8.2.4.4.1 Create a Resource Group

On the main menu of ZStack Cloud, choose **Platform O&M** > **Cloud Monitoring** > **Alarm Service** > **Resource Group**. On the **Resource Group** page, click **Create Resource Group**. Then, the **Create Resource Group** page appears.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the resource group.
- **Description**: Optional. Enter a description for the resource group.

- **Resource**: Add a resource to the resource group.
- **Alarm Template**: Optional. Associate a resource group with an alarm template. Then the alarm template applies to all resources in the group. You can also associate an alarm template after the resource group is created.

  Note:

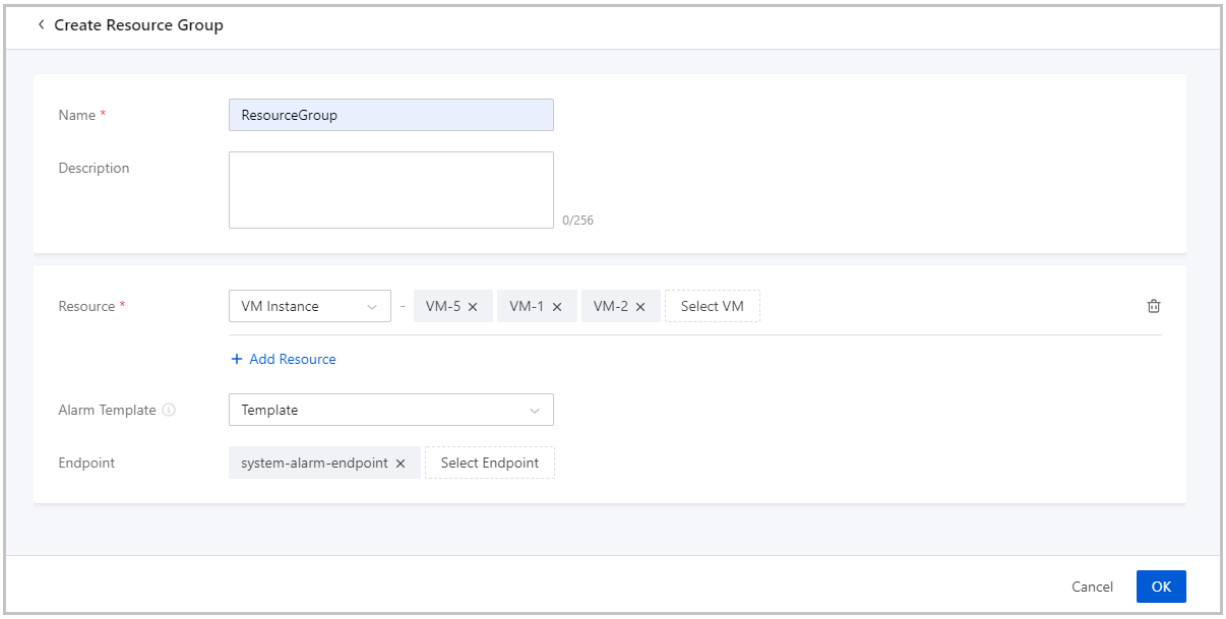
  You can associate a resource group with only one alarm template.

- **Endpoint**: Optional. If specified, alarm messages are sent to the specified endpoint.

  Note:

  - You can specify multiple endpoints.
  - You can specify the system endpoint or customize an endpoint.

Figure 8-5: Create Resource Group



8.2.4.5 Message Template

8.2.4.5.1 Create a Message Template

On the main menu of ZStack Cloud, choose **Platform O&M** > **Cloud Monitoring** > **Alarm Configuration** > **Message Template**. On the **Message Template** page, click **Create Message Template**. Then, the **Create Message Template** page appears.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the message template.
- **Description**: Optional. Enter a description for the message template.
- **Type**: Select the platform type of an endpoint. Valid values: Email, DingTalk, Microsoft Teams, and SMS.
- **Alarm Type**: Select an alarm type. Valid values: Resource Alarm and Event Alarm.
- **Alarm Message Text**: Customize an alarm message text template or use the system template.

  The following is a message template for endpoints of the email and DingTalk types:

```
Alarm ${ALARM_NAME} State Changes To ${ALARM_CURRENT_STATUS}

Alarm Details
UUID: ${ALARM_UUID}
Resource Namespace: ${ALARM_NAMESPACE}
Trigger Condition: ${ALARM_METRIC} ${ALARM_COMPARISON_OPERATOR} ${
ALARM_THRESHOLD}
Trigger Condition Duration: ${ALARM_DURATION} seconds
Previous Status: ${ALARM_PREVIOUS_STATUS}
Current Value: ${ALARM_CURRENT_VALUE}
Tag: ${ALARM_LABELS.join(",")}
```

  Note:

  Message templates for DingTalk-type endpoints must follow the Markdown syntax. DingTalk supports the subset of Markdown syntax. For more information, see DingTalk official website.

  The following is a message template for endpoints of the Microsoft Teams type:

  - Resource alarm:

```
{
  "activityTitle": "Alarm ${ALARM_NAME} ${TITLE_ALARM_RESOURCE
_NAME} State Changes To ${ALARM_CURRENT_STATUS}",
  "facts": [
    {
      "name": "Alarm Details",
      "value": null
    },
    {
      "name": "UUID",
      "value": "${ALARM_UUID}"
    },
    {
      "name": "Resource Type",
      "value": "${ALARM_NAMESPACE}"
    },
    {
      "name": "Trigger Condition",
      "value": "${ALARM_METRIC} ${ALARM_COMPARISON_OPERATOR} ${
ALARM_THRESHOLD}"
    },
    {
      "name": "Trigger Condition Duration",
```

```
      "value": "${ALARM_DURATION} seconds"
    },
    {
      "name": "Previous Status",
      "value": "${ALARM_PREVIOUS_STATUS}"
    },
    {
      "name": "Current Value",
      "value": "${ALARM_CURRENT_VALUE}"
    },
    {
      "name": "Alarm Resource UUID",
      "value": "${ALARM_RESOURCE_ID}"
    },
    {
      "name": "Alarm Trigger Time",
      "value": "${ALARM_TIME}"
    },
    {
      "name": "Alarm Resource Name",
      "value": "${ALARM_RESOURCE_NAME}"
    },
    {
      "name": "Emergency Level",
      "value": "${ALARM_EMERGENCY_LEVEL}"
    },
    {
      "name": "Tag",
      "value": "${ALARM_LABELS.join(\",\")}"
    }
  ]
}
```

- Even alarm:

```
{
  "activityTitle": "Event ${EVENT_NAME} Happened",
  "facts": [
    {
      "name": "Event Details",
      "value": null
    },
    {
      "name": "Name",
      "value": "${EVENT_NAME}"
    },
    {
      "name": "Resource Type",
      "value": "${EVENT_NAMESPACE}"
    },
    {
      "name": "Emergency Level",
      "value": "${EVENT_EMERGENCY_LEVEL}"
    },
    {
      "name": "Alarm Resource UUID",
      "value": "${EVENT_RESOURCE_ID}"
    },
    {
      "name": "Alarm Resource Name",
      "value": "${EVENT_RESOURCE_NAME}"
    },
```

```
    {
      "name": "Alarm Trigger Time",
      "value": "${EVENT_TIME}"
    },
    {
      "name": "Event Subscription UUID",
      "value": "${EVENT_SUBSCRIPTION_UUID}"
    },
    {
      "name": "Error",
      "value": "${EVENT_ERROR}"
    }
  ]
}
```

Note:

Message template for endpoints of the Microsoft Teams type must follow the Webhook syntax of Microsoft Teams. For more information, see Microsoft Teams official website.

The following is a message template for endpoints of the SMS type:

- Resource alarm:

```
Alarm: ${ALARM_NAME}, Name: ${ALARM_RESOURCE_NAME}, Trigger
Condition: ${ALARM_CONDITION}, Emergency Level: ${ALARM_EMER
GENCY_LEVEL}, Current Value: ${ALARM_CURRENT_VALUE}
```

- Event alarm:

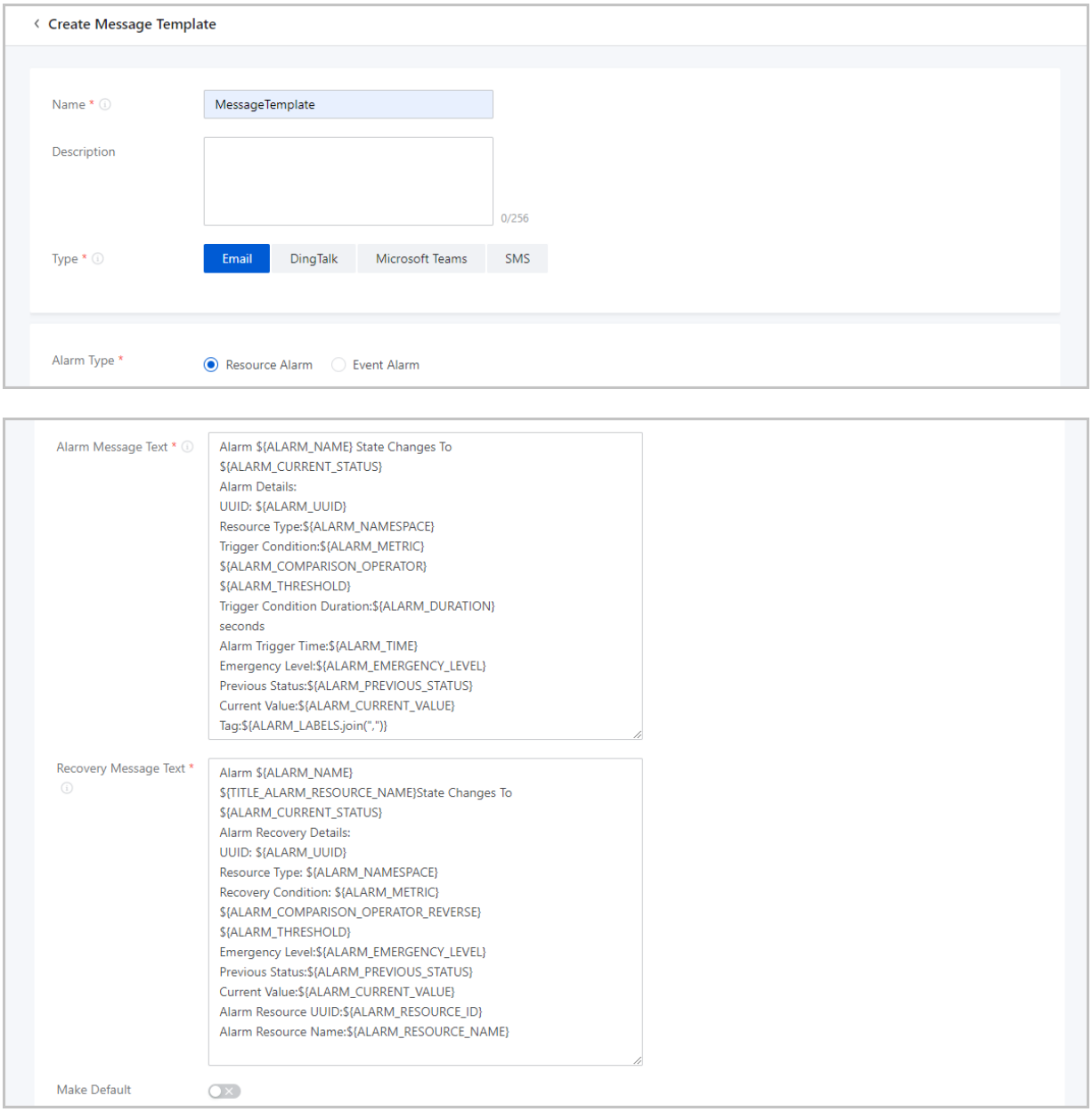
```
Event Name: ${EVENT_NAME}, Name: ${EVENT_RESOURCE_NAME}, Emergency
 Level: ${EVENT_EMERGENCY_LEVEL}, Error: ${EVENT_ERROR}
```

Note:

Before you can customize a message template for SMS endpoint, you need to apply for and obtain a third-party SMS signature and SMS template. Currently, only Alibaba Cloud SMS is supported. If you need to modify a template, you need to modify on the third-party side. In addition, you need to apply for the signature and template again.

- **Recovery Message Text**: When a monitored resource recovers from an alarm status, the Cloud sends alarm recovery messages to the selected endpoint. You can customize the text of the recovery messages as needed. When a resource monitored by an alarm recovers from alarmed status, the specified endpoint receives a notification. The recovery notification is sent according to the default or customized recovery message template. SMS-type endpoints do not support recovery messages.
- **Make Default**: Optional. Set the current message template as the default template.

Figure 8-6: Create Message Template



8.2.4.6 Message Source

8.2.4.6.1 Create a Message Source

Before you can create a message source, you need to enable the extended alarm feature. To do this, choose **Settings** > **Platform Setting** > **Global Setting** > **Advanced** and turn on the **Extended Alarm Notification** switch.

On the main menu of ZStack Cloud, choose **Platform O&M** > **Cloud Monitoring** > **Alarm Configuration** > **Message Source**. On the **Message Source** page, click **Create Message Source**. Then, the **Create Message Source** page appears.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the message source.
- **Description**: Optional. Enter a description for the message source.
- **Message Source Type**: Select the type of message source. Currently, only Ceph Enterprise is supported.
- **Login Address and Token**: Enter the login address of the message source and the access token obtained on the message source page, in the format of `http://{Message Source IP Address}:{Port}/v1/alerts/?token={Access Token}`
- **Alarm Message Conversion Template**: Convert third-party alarm messages into alarm messages that conform to the format required on the cloud. The system provides a conversion template that you can use to customize the parameters.

  Example:

```
{
    "product":"Ceph Enterprise",
    "service":"Ceph Enterprise",
    "message":"${resource_type + '[' + resource_name+'] ' + group +
 ' ' + alert_value}",
    "metric":"${resource_type + '::' + group}",
    "alertLevel":"${level == 'info' ? 'Normal' : level == 'warning
' ? 'Important' : 'Emergent'}",
    "alertTime":"${create}",
    "dimensions":"{'resource_name':'${resource_name}'}",
    "dataSource":"Ceph Enterprise"
}
```

8.2.4.7 Endpoint

8.2.4.7.1 Create an Endpoint

On the main menu of ZStack Cloud, choose **Platform O&M** > **Cloud Monitoring** > **Alarm Configuration** > **Endpoint**. On the **Endpoint** page, click **Create Endpoint**. Then, the **Create Endpoint** page appears.

The following lists the four endpoint creation scenarios:

- Create an endpoint of the email type
- Create an endpoint of the DingTalk type
- Create an endpoint of the HTTP application type
- Create an endpoint of the SMS type
- Create an endpoint of the Microsoft Teams type

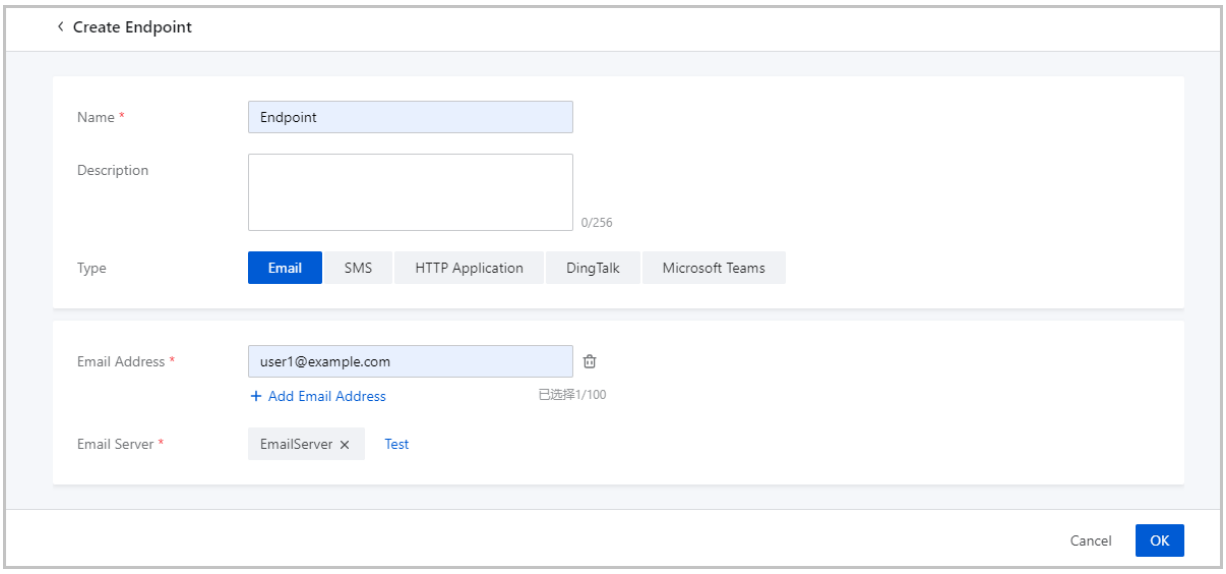
Create Endpoint of Email Type

- Messages sent to topics are sent to the specified email address via an email server.
- You can customize a message template or use the system message template to send email messages in a unified format.
- You need to add an email server to the Cloud and test the availability of the server before you can use the email server to send messages.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the endpoint.
- **Description**: Optional. Enter a description for the endpoint.
- **Type**: Select Email.
- **Email Address**: Enter one or more email addresses. You can enter a maximum of 100 email addresses.
- **Email Server**: Enter an email server that is added to the Cloud.
- **Test**: Test the availability of the email server.

Figure 8-7: Create Endpoint of Email Type



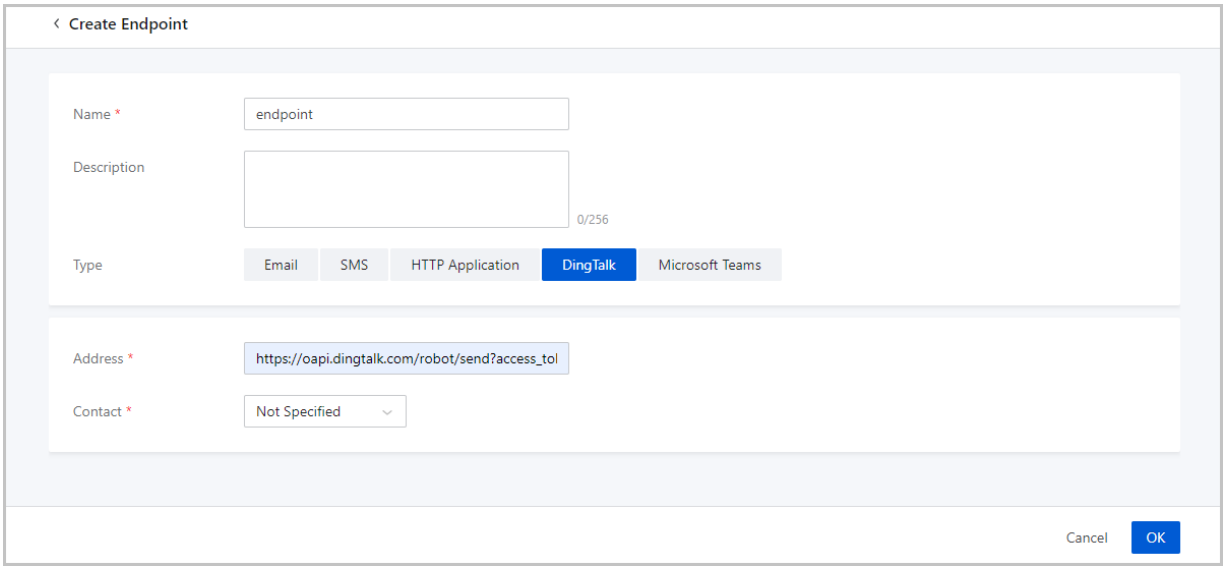
Create Endpoint of DingTalk Type

- Messages sent to topics are sent to the specified DingTalk robot address via DingTalk. If you specify a contact, the DingTalk user that owns the phone number will be notified of the messages.

- You can customize a message template or use the system message template to send email messages in a unified format.
- You need to create an alarm message template of DingTalk type that follows the Markdown syntax. DingTalk supports the subset of Markdown syntax. For more information, see DingTalk official website.
- **Name**: Enter a name for the endpoint.
- **Description**: Optional. Enter a description for the endpoint.
- **Type**: Select DingTalk.
- **Address**: Enter a DingTalk robot address.
- **Contact**: Optional. Specify all members or specific members in the group.

> **Note:**
> If you need to specify a member, enter the phone number of the member, for example, **+86-13800000000**.

Figure 8-8: Create Endpoint of DingTalk Type



Create Endpoint of HTTP Application Type

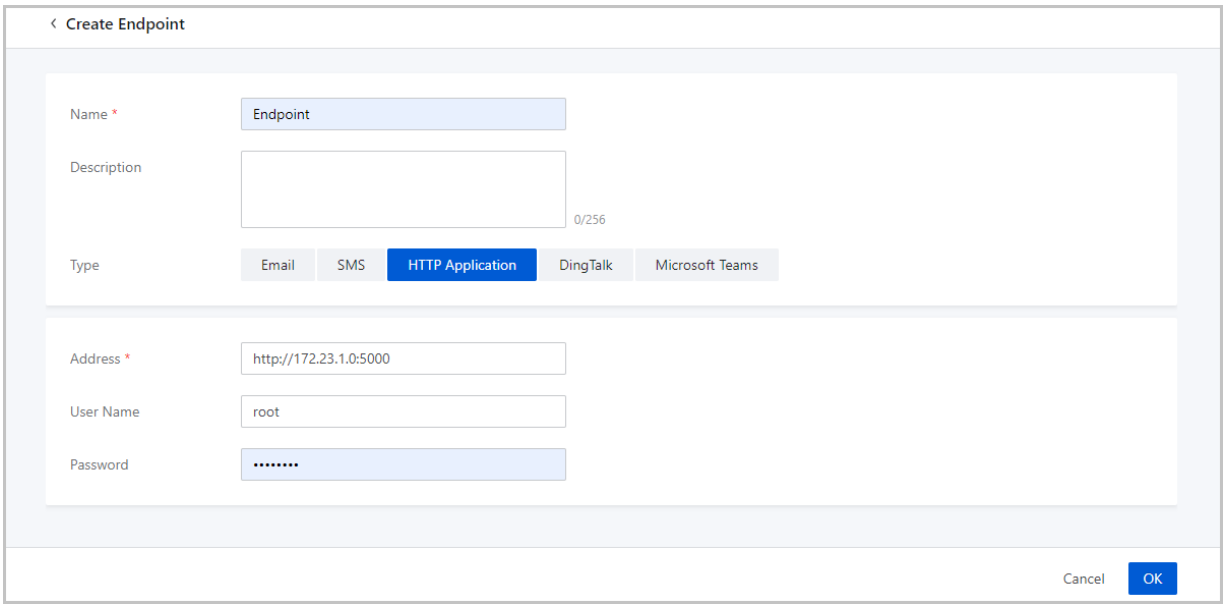
- Messages sent to topics are sent to the specified HTTP address by using the HTTP POST method.
- If you set a username and password for the specified HTTP application, enter the username and password for the endpoint.
- **Name**: Enter a name for the endpoint.

- **Description**: Optional. Enter a description for the endpoint.
- **Type**: Select HTTP Application.
- **Address**: Enter the address of an HTTP application.

> **Note:**
>
> - If the HTTP application is managed by a single management node, the IP address is 127.0.0.1 by default.
> - If the HTTP application is managed by a twin management node, the IP address is a VIP.

- **User Name**: Optional. Enter the username of the HTTP application.
- **Password**: Optional. Enter the password of the HTTP application.

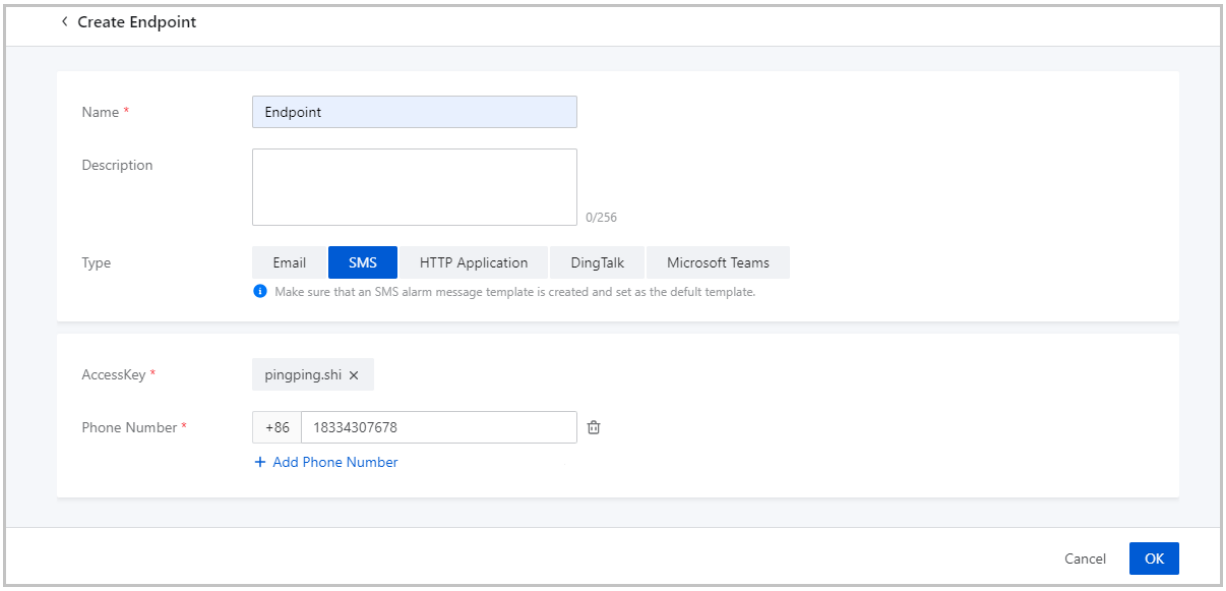
Figure 8-9: Create Endpoint of HTTP Application Type



Create Endpoint of SMS Type

- Messages sent to topics are sent to the specified phone numbers via text messages.
- You need to create a message template and set it as the default template. Then text alarm messages are sent according to the template.
- **Name**: Enter a name for the endpoint.
- **Description**: Optional. Enter a description for the endpoint.
- **Type**: Select SMS.
- **AccessKey**: Enter a third-party AccessKey pair.
- **Phone Number**: Enter the phone numbers that receive text messages.

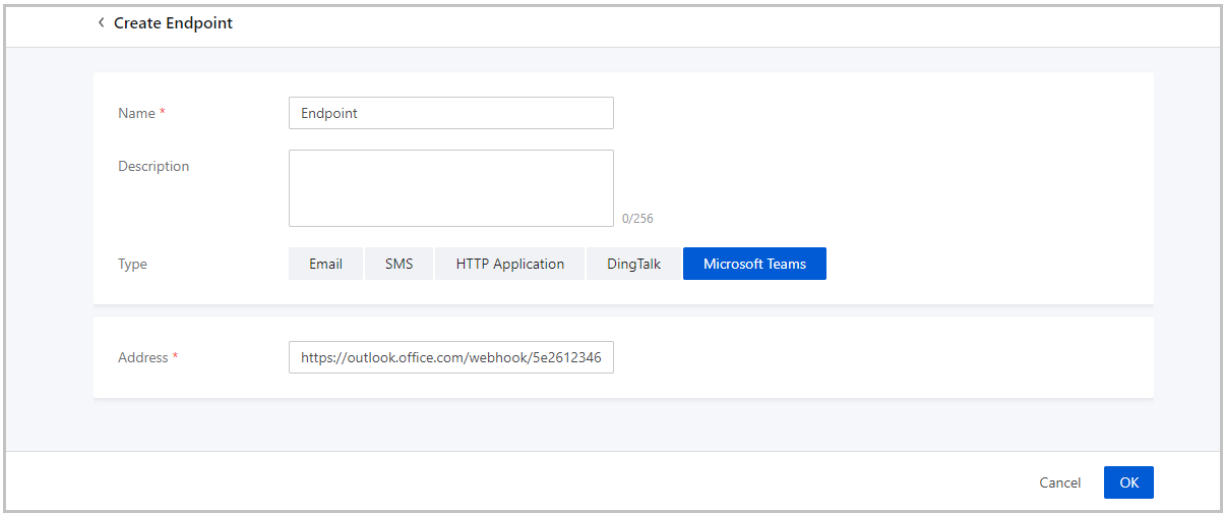
Figure 8-10: Create Endpoint of SMS Type



Create Endpoint of Microsoft Teams Type

- Messages sent to topics are sent to the specified Microsoft teams via Webhook.
- You can create a message template or use the system template for alarm messages to be sent in a unified format.
- **Name**: Enter a name for the endpoint.
- **Description**: Optional. Enter a description for the endpoint.
- **Type**: Select Microsoft Teams.
- **Address**: Enter the Webhook address obtained in the Microsoft team.

Figure 8-11: Create Endpoint of Microsoft Teams Type



8.3 Message Log

8.3.1 Alarm Message

An alarm message is a message sent the time when an alarm is triggered. You can view the statistical graphs and details of alarm messages on the Cloud. You can also view third-party alarm messages on the Extended Alarm Message page.

8.3.2 Operation Log

An operation log is a chronological record of operations on the specified objects and their operation results. You can implement fine-grained operation tracking and troubleshooting by viewing the current tasks and historic operation logs together with audits improve your O&M efficiency.

8.3.3 Audit

Audit monitors and records all activities on the Cloud. You can use this feature to implement operation tracking, cybersecurity classified protection compliance, security analysis, troublesho oting, and automatic O&M. The operations that can be tracked include operations performed by using the console, API calls, accessing and managing cloud resources by using developer tools.

8.4 Backup Management

8.4.1 Backup Service

8.4.1.1 What is Backup Service?

Backup management integrates multiple disaster recovery technologies such as incremental backup and full backup that are suitable for multiple business scenarios. You can implement local backup and remote backup based on your business needs.

Backup Service is a separate feature module. To use this service, purchase both the Base License and the Plus License of Backup Service. The Plus License cannot be used independently.

Typical Backup Scenarios

Backup Service can be applied to the following three typical scenarios: local backup, remote backup, and Public Cloud backup.

Note:

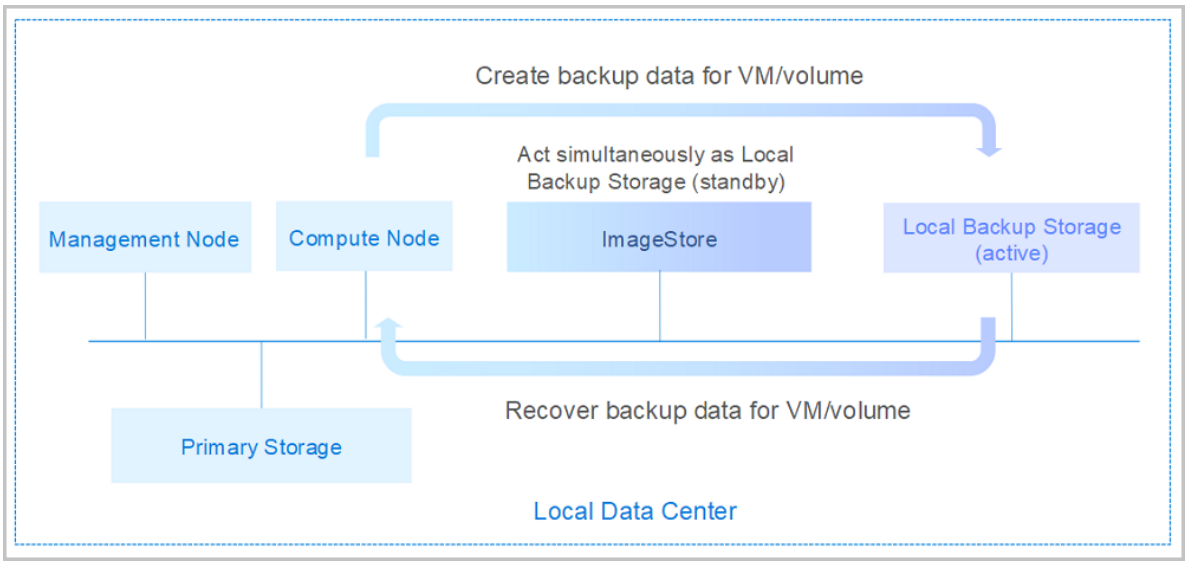
If you have the Enterprise Management Plus license at the same time, the project members (project managers, project admins, and general project members) can perform local backup for VM instances and volumes in the project.

- **Local Backup**

  A local ImageStore backup storage can act as the **Local Backup Storage** to store scheduled backup data of the local VM instances, volumes, and management node databases. Meanwhile, the seamless switchover between the master local backup storage and the standby local backup storage is supported, which effectively ensures your business continuity.

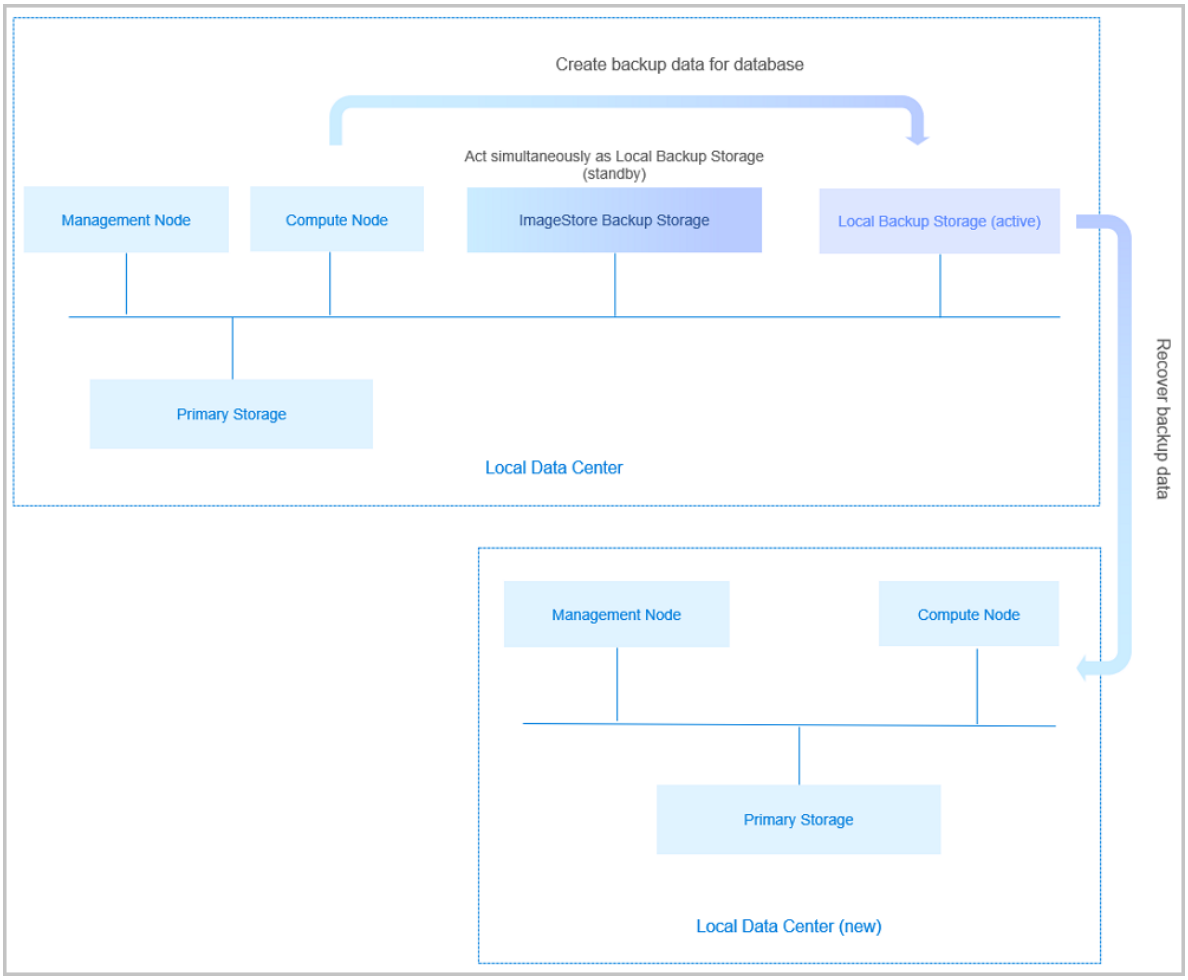
  If your local data is mistakenly deleted, or data in the local primary storage is damaged, you can recover the backup data from the local backup storage, as shown in *Local Backup Scenario-1*

  Figure 8-12: Local Backup Scenario-1



  If you encounter a disaster in your local data center, you can rely totally on your local backup storage to rebuild your data center and recover your business, as shown in *Local Backup Scenario-2*.

Figure 8-13: Local Backup Scenario-2

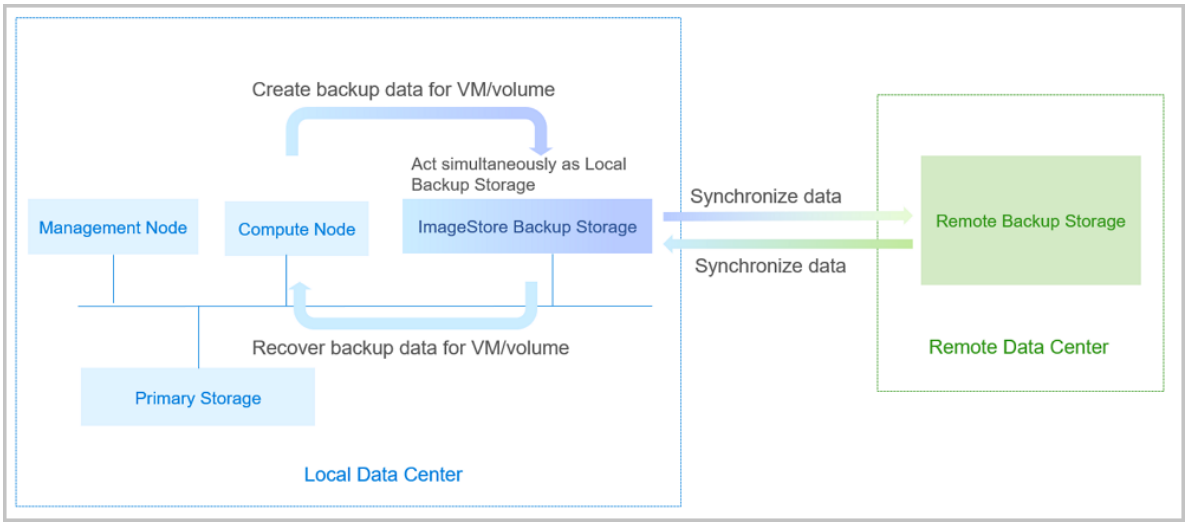


- **Remote Backup**

  A storage server in a remote data center can act as the **Remote Backup Storage** to store the scheduled backup data of the local VM instances, volumes, and databases. The backup data needs to be synchronized to the remote backup storage from the local backup storage.

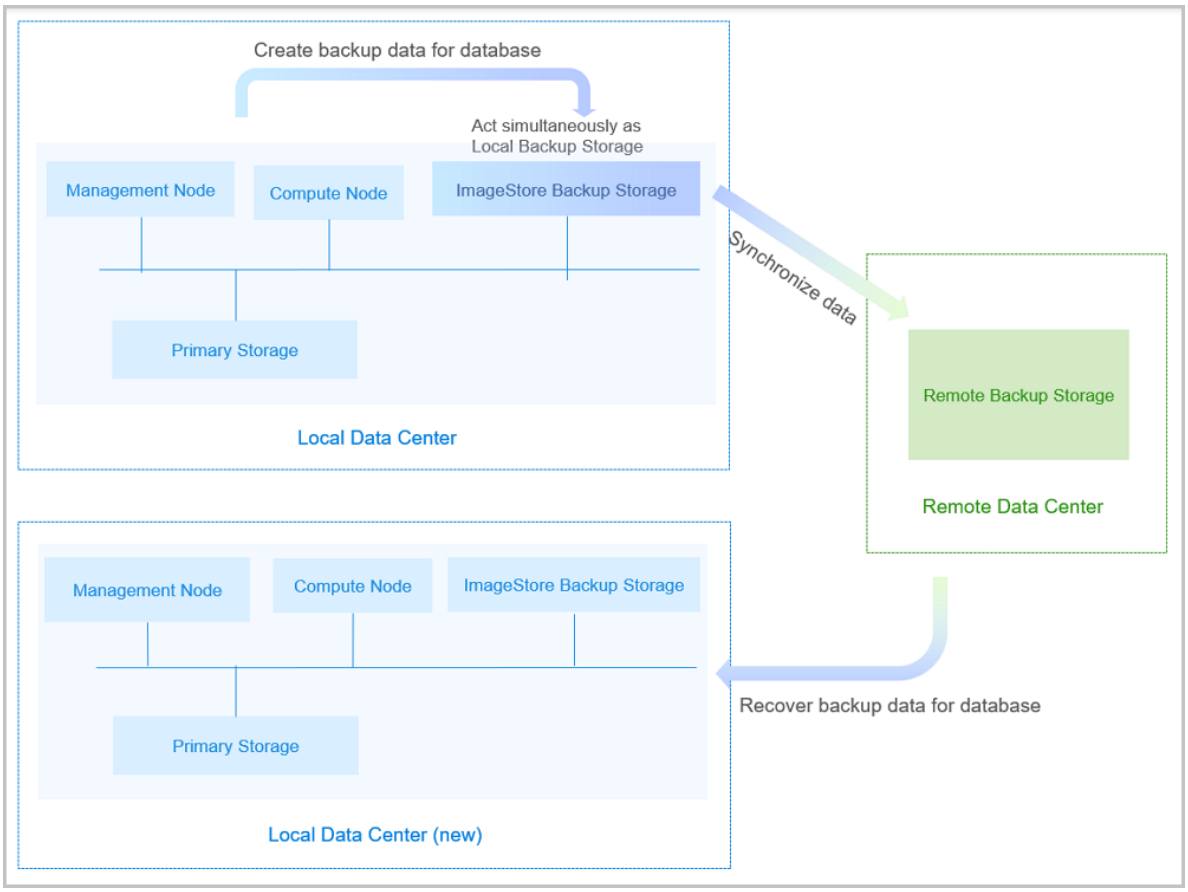
  If your local data is mistakenly deleted, or data in the local primary storage is damaged, you can recover the backup data from the remote backup storage, as shown in *Remote Backup Scenario-1*

Figure 8-14: Remote Backup Scenario-1



If you encounter a disaster in your data center, you can rely totally on your remote backup storage to rebuild your data center and recover your business, as shown in *Remote Backup Scenario-2*.

Figure 8-15: Remote Backup Scenario-2

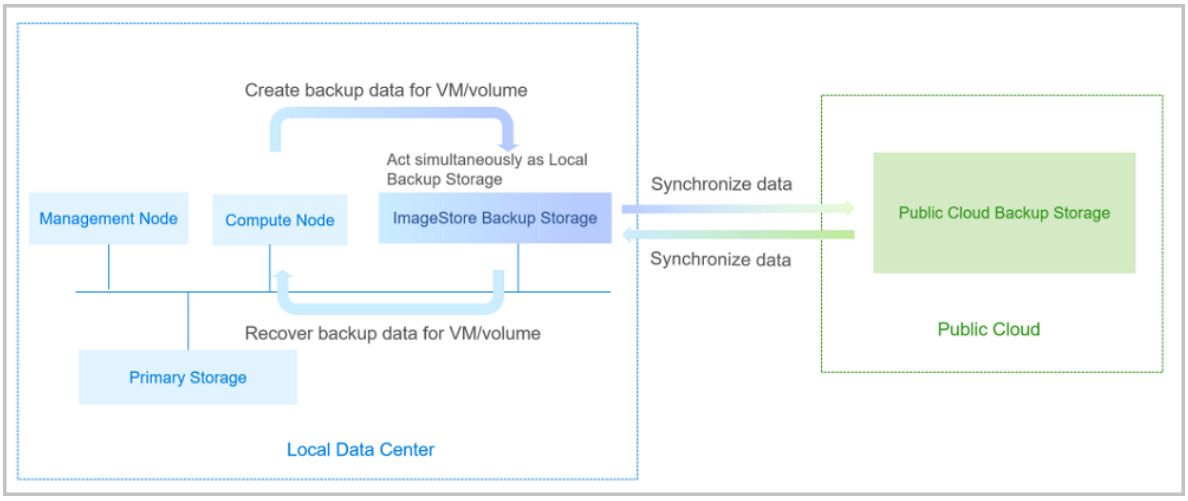


- **Public Cloud Backup**

  The storage server in the Public Cloud can act as the **Public Cloud Backup Storage** to store the scheduled backup data of the local VM instances, volumes, and databases. The backup data can be synchronized to the Public Cloud backup storage from the local backup storage.

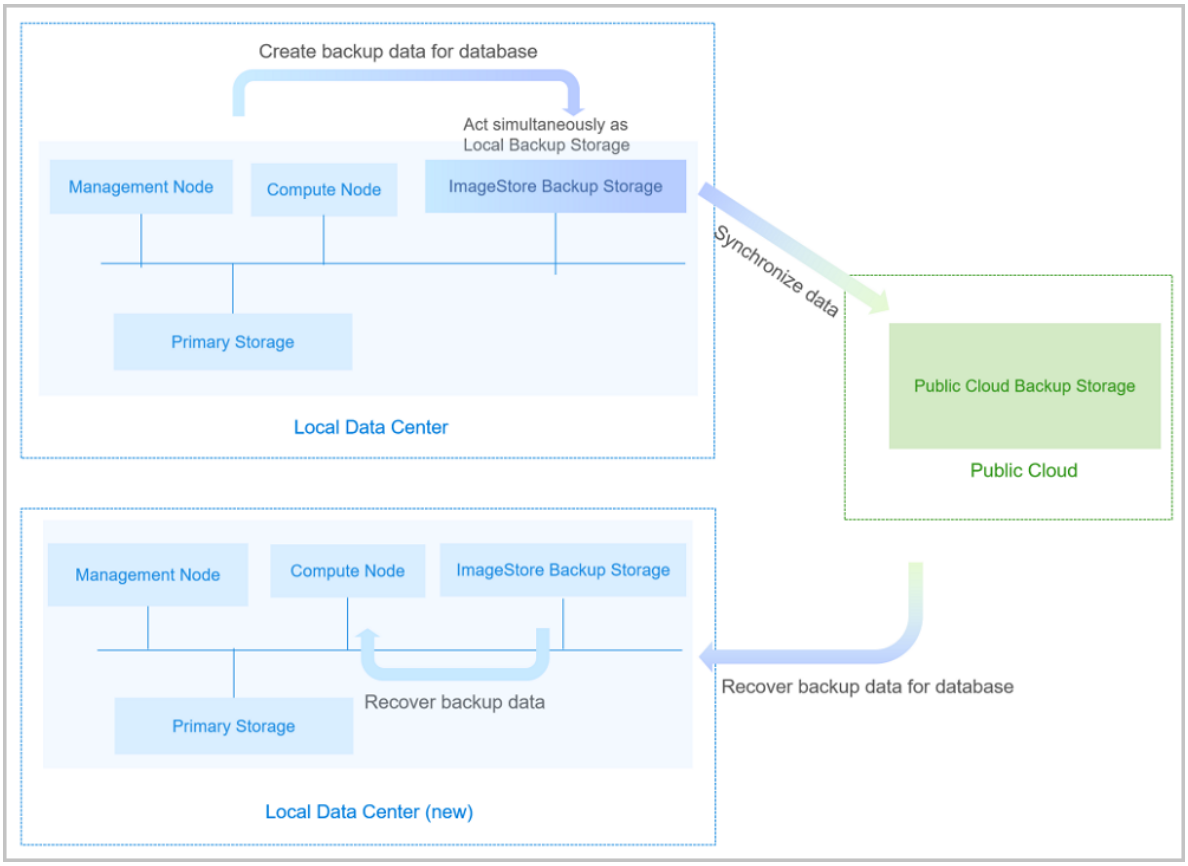
  If your local data is mistakenly deleted, or data in the local primary storage is damaged, you can recover the backup data from the Public Cloud backup storage, as shown in *Public Cloud Backup Scenario-1*.

  Figure 8-16: Public Cloud Backup Scenario-1



  If you encounter a disaster in your data center, you can rely totally on your Public Cloud backup storage to rebuild your data center and recover your business, as shown in *Public Cloud Backup Scenario-2*.

Figure 8-17: Public Cloud Backup Scenario-2



8.4.1.2 Backup Job

8.4.1.2.1 Create a Backup Job

On the main menu of ZStack Cloud, choose **Platform O&M** > **Backup Management** > **Backup Service** > **Backup Job**. Then the **Backup Job** page appears. On the page, choose **VM/ Volume** > **Create Backup Job**. Then the **Create Backup Job** page appears.

You can create the following two types of backup jobs:

- Backup jobs for local VM instances and volumes
- Backup jobs for the management node database

Create Backup Job for Local VM Instance and Volume

Follow the following four steps to create a backup job for VM instances and volumes:

1. Set Basic Information.
   - **Name**: Enter a name for the backup job.

The name must be 1-128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).

- **Description**: Optional. Enter a description for the backup job.
- **Local Backup Server**: Specify one or more local backup servers.

  Note:

  - You can specify up to two local backup servers for a backup job.
  - Before you can specify a local backup server, you need to add the server to ZStack Cloud Private Cloud.
  - If you specify two local backup servers, by default, the first server added to the Cloud is the primary backup server and the second server added to the Cloud is the secondary backup server.
  - If you specify two local backup servers, the two servers apply the fail-over mechanism.
    - When the primary backup server works as expected, data is backed up on the primary backup server.
    - If the primary backup server is disabled, removed, or disconnected, data is backed up on the secondary backup server.
    - When the primary backup server resumes working as expected, data backup is auto-switched to the primary backup server.
- **Sync to Remote Backup Server**: Choose whether to sync local backup data to a remote backup server. A remote backup server can be a server that is in another data center or a public cloud backup server. By default, the switch is turned off.

  Note:

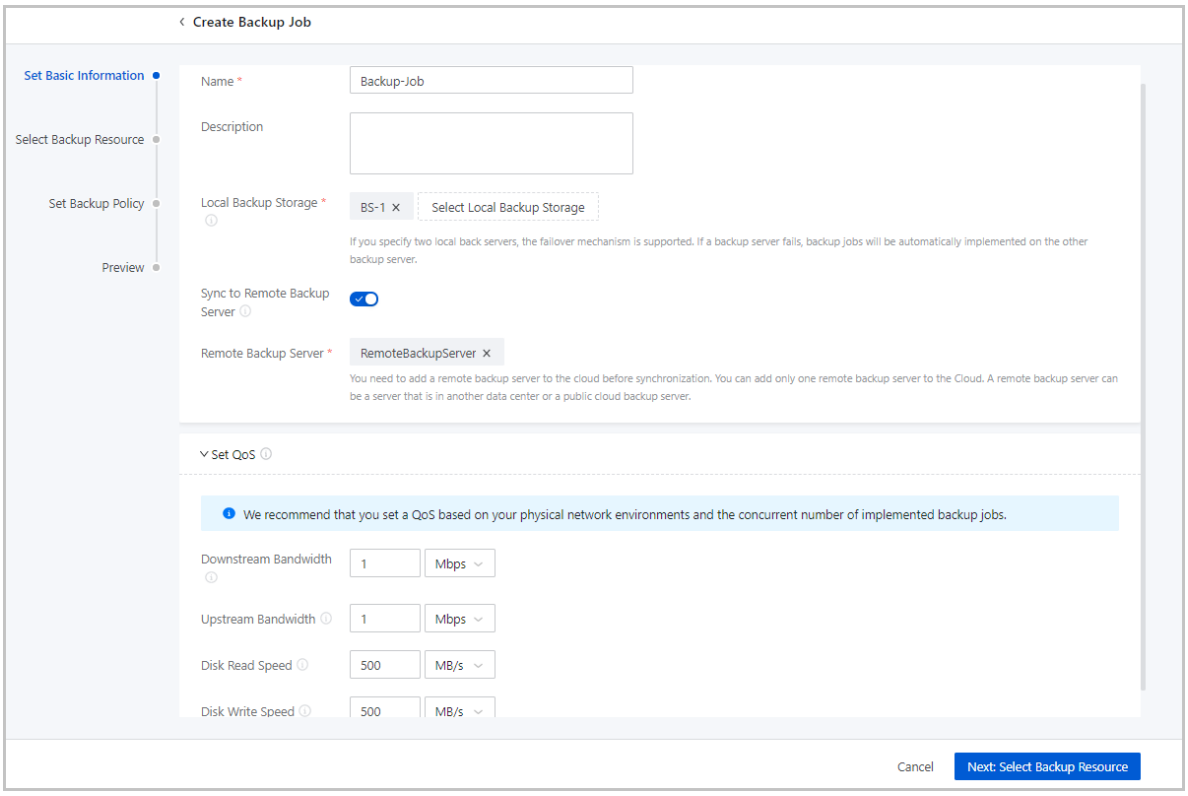
  Before you can sync backup data to a remote backup server, you need to add a remote backup server to the Cloud. Note that you can add only one remote backup server to the Cloud.
- **Set QoS**: Optional. You can set network QoS and disk QoS for the backup job.
  - **Downstream Bandwidth**: Set the maximum downstream bandwidth. Unit: kilobits per second (Kbps), Mbps, and Gbps. Valid values: 8 Kbps to 30 Gbps. If you do not specify the downstream bandwidth, this bandwidth is unlimited.

- **Upstream Bandwidth**: Set the maximum upstream bandwidth. Unit: kilobits per second (Kbps), Mbps, and Gbps. Valid values: 8 Kbps to 30 Gbps. If you do not specify the upstream bandwidth, this bandwidth is unlimited.
- **Disk Read Speed**: Set the maximum read speed. Unit: Megabyte per second (MB/s) and GB/s. Valid values: 1MB/s to 100GB/s. If you do not specify the disk read speed, this speed is unlimited.
- **Disk Write Speed**: Set the maximum write speed. Unit: Megabyte per second (MB/s) and GB/s. Valid values: 1MB/s to 100GB/s. If you do not specify the disk write speed, this speed is unlimited.

Note:

We recommend that you set a QoS based on your physical network environments and the concurrent number of implemented backup jobs.

Figure 8-18: Set Basic Information



2. Select Backup Resource.

   Select local VM instances or volumes that you need to back up.

- **Backup Resource**: Select the type of resource that you need to back up. You can select VM Instance or Volume.
  - If you select VM Instance, you need to set the following parameters:
    - **VM Instance**: Select one or more VM instances that you need to back up.

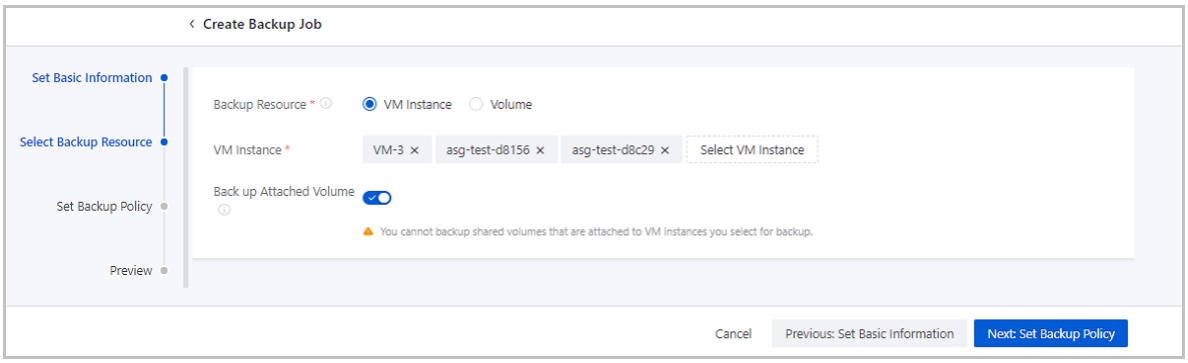
      Note:
      You can only back up running VM instances.
    - **Back up Attached Volume**: You can back up all volumes that are attached to a VM instance. By default, this switch is turned on.

      Note:
      You cannot back up shared volumes that are attached to a VM instance.
  - If you select Volume, you need to set the following parameter:

    Volume: Select one or more volumes that you need to back up.

    Note:
    You can only back up volumes that are attached to running VM instances.

Figure 8-19: Select Backup Resource



3. Set Backup Policy.

   You can create a backup job in one of the following two modes:

   - Incremental Backup + Default Full Backup
   - Incremental Backup + Custom Full Backup

   If you select **Incremental Backup + Default Full Backup**, you need to set the following parameters:

- **Backup Mode**: Select Incremental Backup + Default Full Backup.
- **Backup Retention Policy**: Select By Count or By Time:
  - By Count: Set the number of retained data backups of selected resources.

    Note:
    You can retain a minimum of one backup of selected resources.
  - By Time: Set the retention period of the backup data.
- **Incremental Backup Policy**: Customize an incremental backup policy.
  - **Backup Cycle**: Select a backup cycle. You can select Backup by Month, Backup by Week, Backup by Day, and Backup by Minute.

    If you select Backup by Month, Backup by Week, or Backup by Day, you can set the backup execution time and schedule the effective time of the backup job to the accuracy of a minute.

    - **Execution Time**:
      - If you select Backup by Month and set the execution time to 00:00 of the first day of each month, the incremental backup job is executed at 00:00 of the first day of each month.

        Note:
        If you set the execution time to the 31th day of each month, the incremental backup job is executed only in the month that has 31 days.
      - If you select Backup by Week and set the execution time to 00:00 of Sunday and Tuesday of each week, the incremental backup job is executed at 00:00 of Sunday and Tuesday of each week.
      - If you select Backup by Day and set the execution time to 00:30, the incremental backup job is executed at 00:30 of each day.
    - **Schedule Effective Time**: Choose whether to schedule effective time.

      If you specify data backup by month, week, or day, you can schedule the time when the backup job takes effect. After the backup job takes effect, data backup is executed based on the specified cycle and time.

  If you select Backup by Hour or Backup by Minute, you can set finer-grained incremental backup cycle.

- **Start Time to Implement**:
  - If you select Backup Every 6 Hour and set Start Time at 2020-12-30 00:00, incremental backup is implemented starting from 00:00, Dec 30, 2020 at an interval of 6 hours.
  - If you select Backup Every 30 Minute and set Start Time at 2020-12-30 00:00, incremental backup is implemented starting from 00:00, Dec 30, 2020 at an interval of 30 minutes.

  Note:
  The minimum backup interval is 15 minutes.

If you select **Incremental Backup + Custom Full Backup**, you need to set the following parameters:

- **Backup Mode**: Select Incremental Backup + Custom Full Backup.
- **Backup Retention Policy**: Select By Count or By Time:
  - By Count: Set the number of retained data backups of selected resources.

    Note:
    You can retain a minimum of one backup of selected resources.
  - By Time: Set the retention period of the backup data.
- **Incremental Backup Policy**: Customize an incremental backup policy.
  - **Backup Cycle**: Select a backup cycle. You can select Backup by Month, Backup by Week, Backup by Day, and Backup by Minute.

    If you select Backup by Month, Backup by Week, or Backup by Day, you can set the backup execution time and schedule the effective time of the backup job to the accuracy of a minute.

    - **Execution Time**:
      - If you select Backup by Month and set the execution time to 00:00 of the first day of each month, the incremental backup job is executed at 00:00 of the first day of each month.

        Note:

If you set the execution time to the 31th day of each month, the incremental backup job is executed only in the month that has 31 days.

- If you select Backup by Week and set the execution time to 00:00 of Sunday and Tuesday of each week, the incremental backup job is executed at 00:00 of Sunday and Tuesday of each week.
- If you select Backup by Day and set the execution time to 00:30, the incremental backup job is executed at 00:30 of each day.

- **Schedule Effective Time**: Choose whether to schedule effective time.

  If you specify data backup by month, week, or day, you can schedule the time when the backup job takes effect. After the backup job takes effect, data backup is executed based on the specified cycle and time.

If you select Backup by Hour or Backup by Minute, you can set finer-grained incremental backup cycle.

- **Start Time to Implement**:
  - If you select Backup Every 6 Hour and set Start Time at 2020-12-30 00:00, incremental backup is implemented starting from 00:00, Dec 30, 2020 at an interval of 6 hours.
  - If you select Backup Every 30 Minute and set Start Time at 2020-12-30 00:00, incremental backup is implemented starting from 00:00, Dec 30, 2020 at an interval of 30 minutes.

  Note:
  The minimum backup interval is 15 minutes.

- **Full Backup Policy**: Customize a full backup policy.
  - **Backup Cycle**: Select a backup cycle. You can select Backup by Month and Backup by Week
    - If you select Backup by Month and set the execution time to 00:00 of the first day of each month, the full backup job is executed at 00:00 of the first day of each month.

      Note:
      If you set the execution time to the 31th day of each month, the full backup job is executed only in the month that has 31 days.

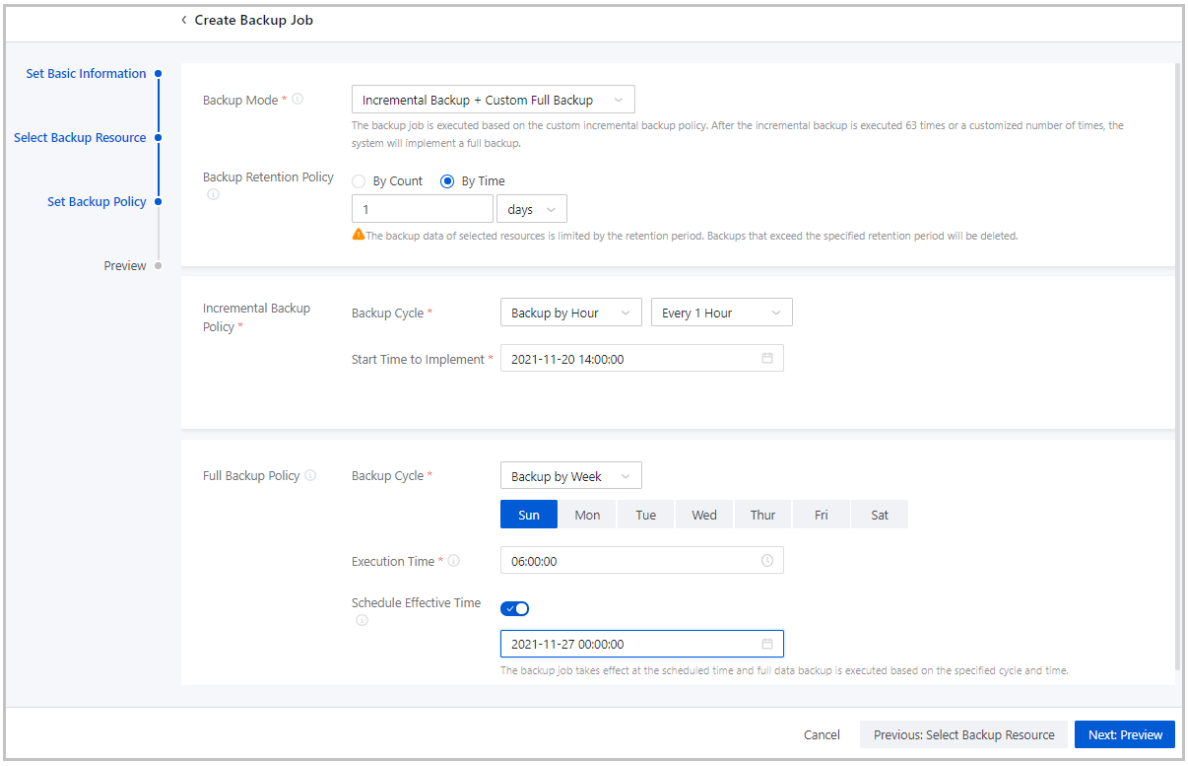
- If you select Backup by Week and set the execution time to 00:00 of Sunday and Tuesday of each week, the full backup job is executed at 00:00 of Sunday and Tuesday of each week.

— **Execution Time**: Set the execution time of the backup job.

— **Schedule Effective Time**: Choose whether to schedule effective time.

You can schedule the time at which the backup job takes effect. After the backup job takes effect, data backup is executed based on the specified cycle and time.

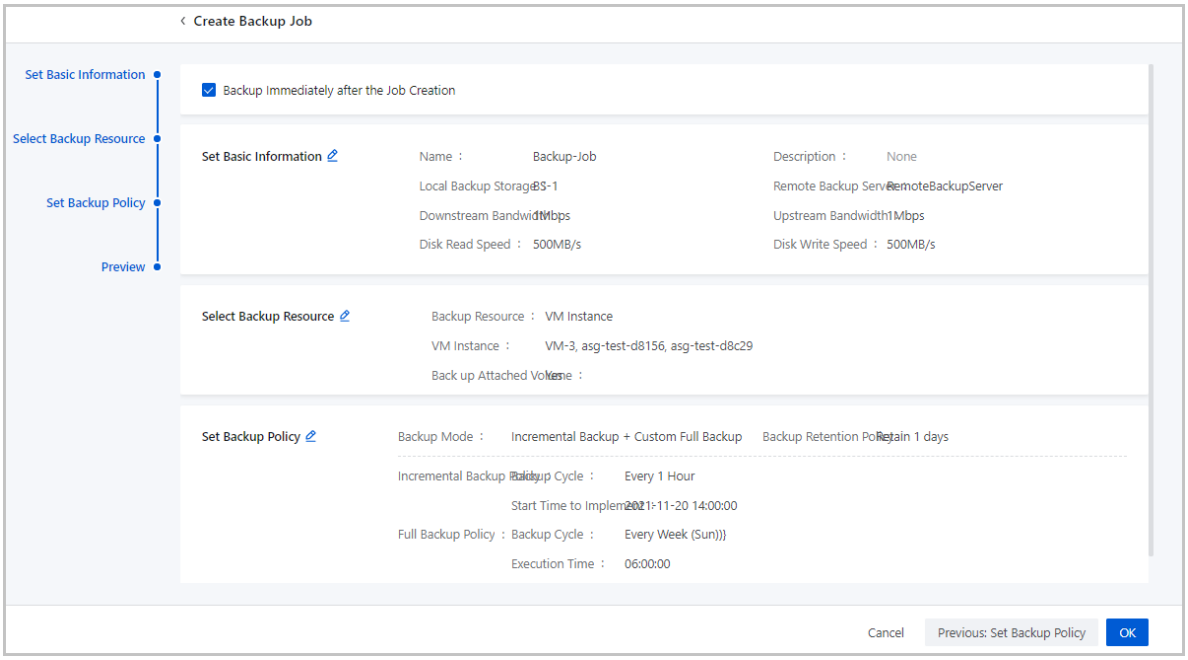
Figure 8-20: Set Backup Policy



4. Preview.

Preview the backup job. You can select Backup Immediately after the Job Creation and click the Edit icon to modify the job.

Figure 8-21: Preview



Create Backup Job for Management Node Database

On the main menu of ZStack Cloud, choose **Platform O&M** > **Backup Management** > **Backup Service** > **Backup Job**. Then the **Backup Job** page appears. On the page, choose **Database** > **Create Backup Job**. Then the **Create Backup Job** page appears.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the backup job.
- **Description**: Optional. Enter a description for the backup job.
- **Backup Resource**: The management node database is displayed
- **Local Backup Server**: Specify one or more local backup servers.

Note:

- You can specify up to two local backup servers for a backup job.
- Before you can specify a local backup server, you need to add the server to ZStack Cloud Private Cloud.
- If you specify two local backup servers, by default, the first server added to the Cloud is the primary backup server and the second server added to the Cloud is the secondary backup server.
- If you specify two local backup servers, the two servers apply the fail-over mechanism.

— When the primary backup server works as expected, data is backed up on the primary backup server.

— If the primary backup server is disabled, removed, or disconnected, data is backed up on the secondary backup server.

— When the primary backup server resumes working as expected, data backup is auto-switched to the primary backup server.

- **Sync to Remote Backup Server**: Choose whether to sync local backup data to a remote backup server. A remote backup server can be a server that is in another data center or a public cloud backup server. By default, the switch is turned off.

  Note:
  Before you can sync backup data to a remote backup server, you need to add a remote backup server to the Cloud. Note that you can add only one remote backup server to the Cloud.

- **Execution Policy**:

  — **Backup Retention Policy**: Select By Count or By Time:

  ■ By Count: Set the number of retained data backups of selected resources.

  Note:
  You can retain a minimum of one backup of selected resources.

  ■ By Time: Set the retention period of the backup data.

  — **Backup Cycle**: Select a backup cycle. You can select Backup by Week, Backup by Day, and Backup by Hour.

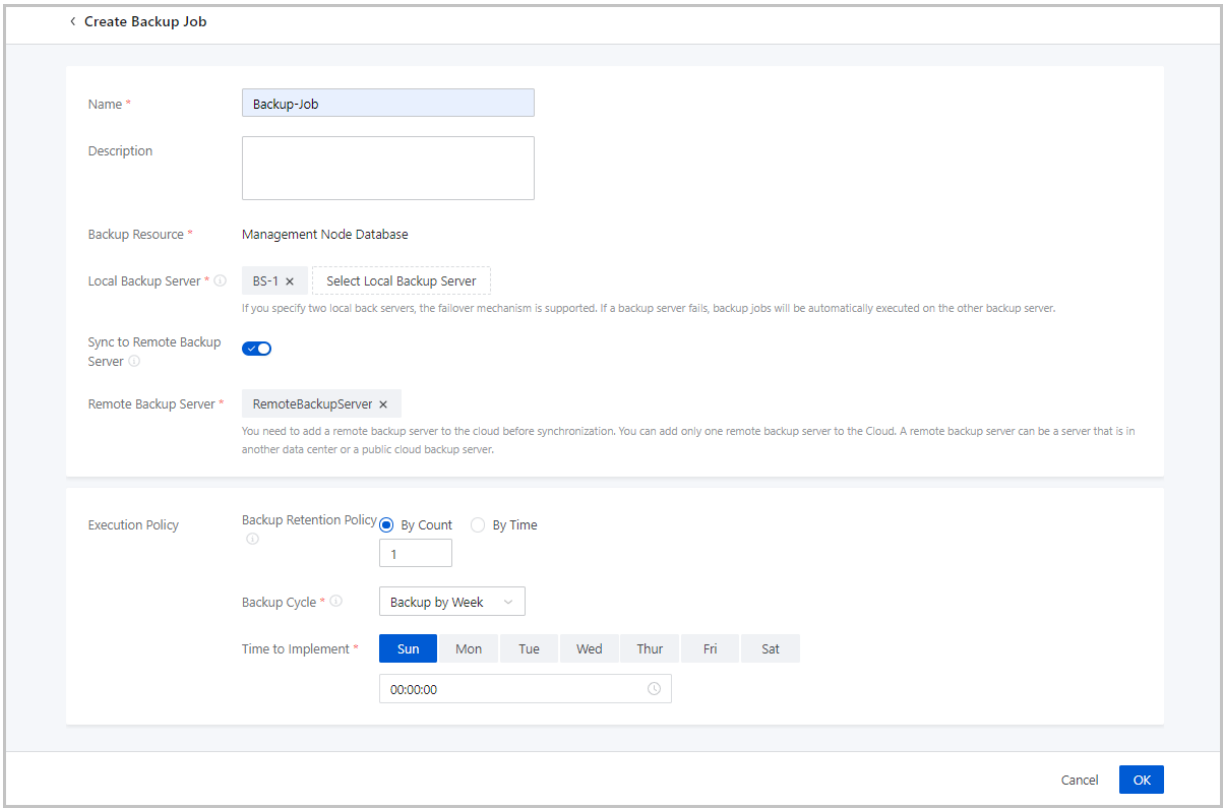
  — **Time to Implement**: Set the execution time and interval of the backup job.

  ■ If you select Backup by Week and set the execution time to 00:00 of Sunday and Tuesday of each week, the backup job is executed at 00:00 of Sunday and Tuesday of each week.

  ■ If you select Backup by Day and set the execution time to 00:30, the backup job is executed at 00:30 of each day.

  ■ If you select Backup Every 2 Hour, the backup job is implemented at an interval of 2 hours.

Figure 8-22: Create Backup Job for Management Node Database



Notes

- Incremental Backup + Default Full Backup
- Incremental Backup + Custom Full Backup
- Incremental Backup + Default Full Backup:
  - You only need to customize the incremental backup policy.
  - After you set the incremental backup policy, incremental backup is executed based on the policy.
- Incremental Backup + Custom Full Backup
  - After you set the backup policy, incremental backup and full backup are executed based on the policy.
- By default, the system implements a full backup when the incremental backup is executed 63 times. You can modify the execution time in Global Setting.

Note:

- By default, the value of `incrementalBackup.maxNum` is 64. This value indicates that the system implements a full backup when the incremental backup is executed 63 times.
- You can also use zstack-cli to modify the value:

```
[root@localhost ~]# zstack-cli  #Use zstack-cli

admin>>> LogInByAccount accountName=admin password=password # Log
 into the system.The default username and password combination
 is admin/password.

admin >>>UpdateGlobalConfig category=volumeBackup
 name=incrementalBackup.maxNum value=10 # Update the maximum
 times of incremental backup.
{
    "inventory": {
        "category": "volumeBackup",
        "defaultValue": "64",
        "description": "the maximum numbers of continuous
 incremental backup",
        "name": "incrementalBackup.maxNum",
        "value": "10"
    },
    "success": true
}
```

- If a full backup and incremental backup are triggered at the same time, the two backups are executed in queue.
- You can check the incremental backup data and full backup data on the **Local Backup Data** page. If you have selected Sync to Remote Backup Server, you can check the backup data on the remote backup server.

8.4.1.2.2 Manage a Backup Job

On the main menu of ZStack Cloud, choose **Platform O&M** > **Backup Management** > **Backup Service** > **Backup Job**. Then the **Backup Job** page appears.

You can perform the following operations on backup jobs for VM instances and volumes.

Action	Description
Edit Backup Job	Edit the name and description of a backup job.
Enable Backup Job	Enable a backup job.
Disable Backup Job	Disable a backup job. If you disable a backup job, data backup will not be implemented for the associated resources. In addition, you cannot create new backup jobs for the resources.
Set Backup Policy	Update the backup policy of the backup job. You can edit the backup mode, backup retention policy, incremental backup policy, and full backup policy.

Action	Description
	Note: New backup policies do not affect backup jobs that have been triggered.
Set Backup Storage	Configure local backup servers and remote backup servers for the backup job.
Execute Now	Implementing a backup job right now will generate a new backup in the backup chain. **Note:** • If the backup mode of the backup job is Incremental Backup + Default Full Backup, the manual backup is implemented in the mode the same as the next backup. Full backup is not supported. • If the backup mode of the backup job is Incremental Backup + Custom Full Backup, you can choose whether to implement full backup. If you do not choose to implement full backup, the manual backup is implemented in the mode the same as the next backup. Full backup is not supported.
Delete Backup Job	Delete a backup job. If you delete a backup job, data backup is terminated for the associated resources. You can create new backup jobs for the resources. **Note:** • If you have already created a backup job for a resource, you cannot create another backup job for the resource. • After you delete a backup job for a resource, you can create a new backup job for the resource.

You can perform the following operations on backup jobs for the database.

Action	Description
Edit Backup Job	Edit the name and description of a backup job.
Enable Backup Job	Enable a backup job.
Disable Backup Job	Disable a backup job. If you disable a backup job, data backup will not be implemented for the associated resources. In addition, you cannot create new backup jobs for the resources.

Action	Description
Execute Now	Implementing a backup job right now will generate a new backup in the backup chain.
Delete Backup Job	Delete a backup job. If you delete a backup job, data backup is terminated for the associated resources. You can create new backup jobs for the resources. **Note:** • If you have already created a backup job for a resource, you cannot create another backup job for the resource. • After you delete a backup job for a resource, you can create a new backup job for the resource.

8.4.2 Continuous Data Protection (CDP)

8.4.2.1 What is CDP?

Continuous Data Protection (CDP) provides second-level and fine-grained continuous backups for important business systems in VM instances, allowing users to restore VM data to any time state and retrieve files without restoring the system.

Note:

- The Continuous Data Protection (CDP) service is a separate feature module. To use this service, purchase both the Base License and the Plus License of Continuous Data Protection (CDP). The Plus License cannot be used independently.
- If you also purchased the Enterprise Management Plus License, note that the project members (project admins, project managers, and other members) cannot create CDP tasks for VM instances in the project currently.

Concepts

- CDP task: You can create a CDP task to continuously back up your VM data to a specified backup storage to achieve continuous data protection and restoration.
- CDP data: The backup data generated from continuous data protection on VM instances is stored in local backup storages.
- Recovery point: A recovery point is a data point generated during continuous data protection. A recovery point corresponds to a data record within the recovery point interval specified by the user.

The recovery point data is retained according to the recovery point retention period. The details are as follows:

- All the recovery point data within the retention time is retained.
- If the retention time is less than 7 days, note that: From the end of the last retention day to the 7th day, a recovery point is retained on an hourly basis at the sharp time. From the 8th day to the 30th day, a recovery point is retained on a daily basis at 00:00. After 30 days, the recovery point data is automatically cleared.
- If the retention time is greater than 7 days, note that: From the end of the last retention day to the 30th day, a recovery point is retained on a daily basis at 00:00. After 30 days, the recovery point data is automatically cleared.

- Protected recovery point: After a recovery point is protected, it will not be automatically cleared or deleted.

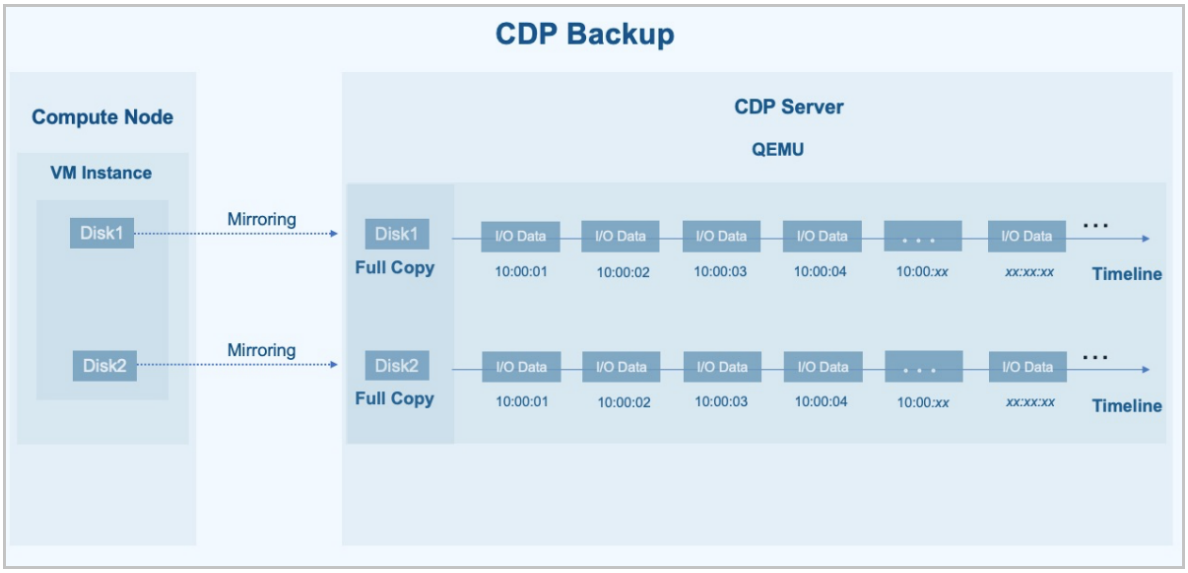
How CDP Works

ZStack Cloud provides block-level continuous data protection. You can restore both the VM data and volume data according to a specified time point.

1. CDP backup

After continuous data protection is performed on a VM instance, the CDP server first performs a full copy of the VM data, continuously captures I/O data changes through QEMU, and timestamps, saves the I/O data of each change, thereby achieving continuous data backup.

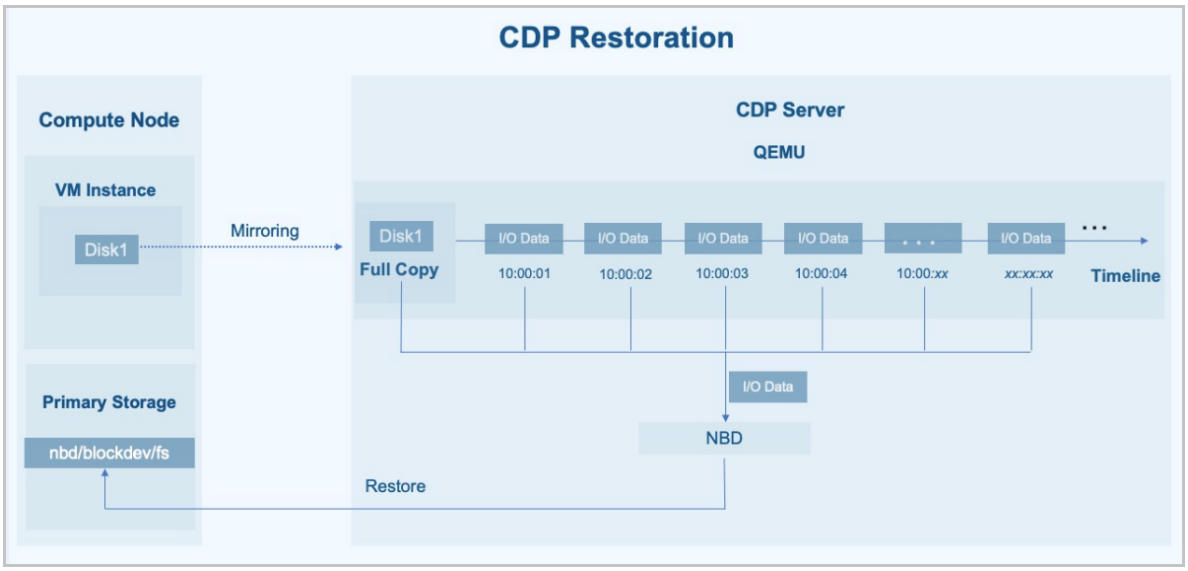
Figure 8-23: CDP Backup



2. **CDP restoration**

When data restoration is performed, the CDP server exposes the CDP data as a network block device (NBD) and then restores the I/O data at a specified time to the disk or file system of a primary storage.

Figure 8-24: CDP Restoration



Advantages

- Agentless backup: To use the CDP service, you do not need to install an agent for your VM instances or couple with other applications. This helps reduce the configuration complexity, lower the VM performance loss, and guarantee the business security.
- Near-zero backup window: The CDP service provides second-level, fine-grained continuous backup, recording important business data changes in real time.
- File retrieving: Allows you to retrieve files without restoring the system. Both Windows and Linux file system formats are supported.
- File Preview: Allows you to preview files of different types when you retrieve a file. Supported file formats: pictures (.png, .jpg, .bmp, .gif, etc.), PDF files, and text files (equal to or smaller than 10 MB).

Scenarios

The CDP service can be applied in the following scenarios:

- Continuous protection of critical business data

You can use the CDP service to continuously back up and protect critical business data, such as banking system data and financial transaction data, minimizing data loss and ensuring your business continuity.

- Anti-virus and data restoration

  In case of virus invasion, such as a ransomware attack, you can use CDP to restore data to any point in time to reduce the loss caused by the virus.

Limits

Currently, you can only create CDP tasks for VM instances that use Ceph primary storages. Before you use CDP for your VM instances, we recommend that you check the primary storage type to better use the restoration feature.

8.4.2.2 CDP Task

8.4.2.2.1 Create a CDP Task

On the main menu of ZStack Cloud, choose **Platform O&M** > **Backup Management** > **CDP Service** > **CDP Task**. On the **CDP Task** page, click **Create CDP Task**. Then, the **Create CDP Task** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the CDP task.

  The CDP task name must be 1 to 128 characters in length and can contain Chinese characters , letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the CDP task.
- **VM Instance**: Select the VM instance to be protected.

  Note:

  - You can create a CDP task for VM instances that use any primary storages in the Cloud. Currently, you can restore data of VM instances that use Ceph primary storages only.
  - After you create a CDP task for a VM instance, the Cloud performs a full backup on the VM instance.
  - You could not create a CDP task for VM instances with running backup jobs.

- If a VM instance is in the stopped state, the CDP task created for the VM instance is also in the stopped state and can start with the VM instance.

- **Local Backup Storage**: Specify a local backup storage to store CDP data.

  Note:

  - Before you can specify a local backup storage, add one to ZStack CloudPrivate Cloud.
  - To ensure the continuity of CDP tasks, we recommend that you do not reuse the backup storage as a host.

- **CDP Task Planned Size**: Set the size required by a CDP task. If the planned size is exceeded, the CDP task is automatically stopped.

  Note:

  - The planned size per CDP task must be greater than the full backup size and smaller than the available size of the selected local backup storage.
  - If a local backup storage is used by many CDP task, you need to plan the size of a CDP task properly. Note that the total planned size of the current VM instance must be smaller than total size of the current backup storage.
  - If the size occupied by the CDP task exceeds the available size of the backup storage, the CDP task will automatically stop.

- **Recovery Point Retention Time**: Set how long the recovery point can be retained. Value range: 1-14, integer. By default, the recovery point can be retained for one day.

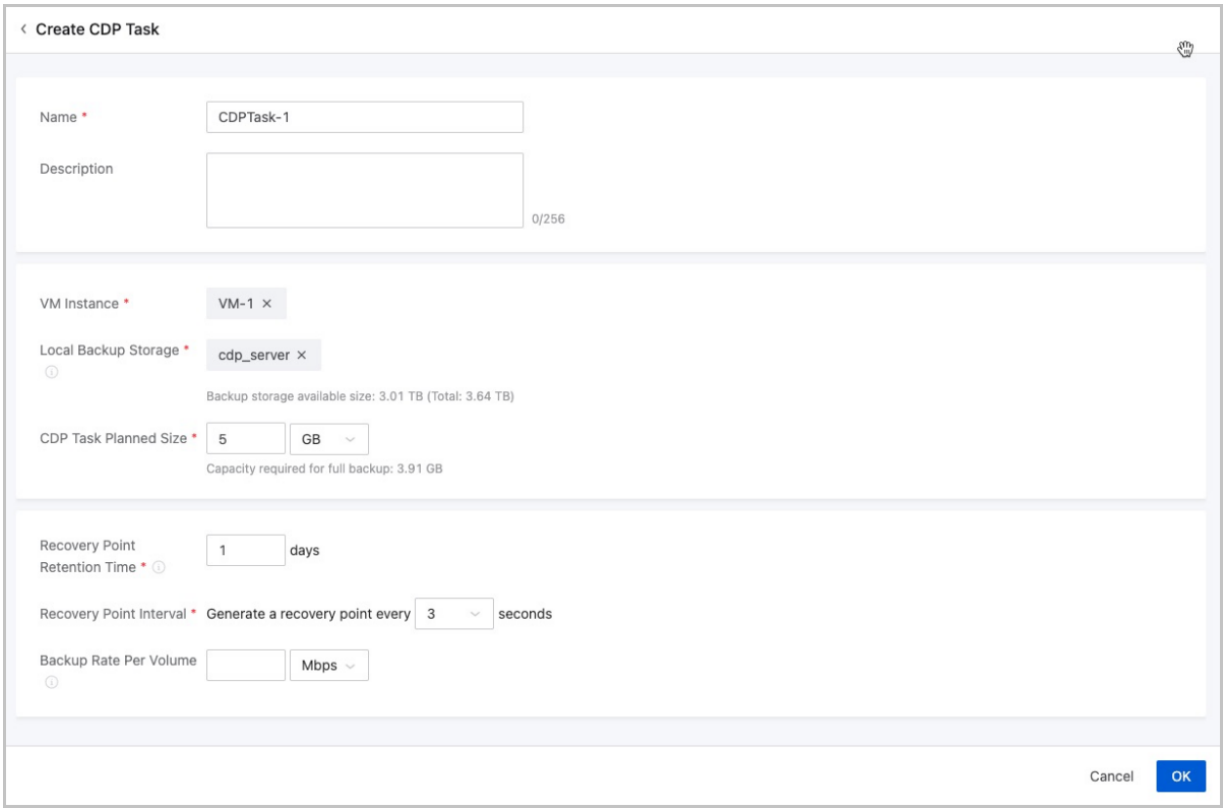
  Note:

  - All the recovery point data within the retention time is retained.
  - If the retention time is less than 7 days, note that: From the end of the last retention day to the 7th day, a recovery point is retained on an hourly basis at the sharp time. From the 8th day to the 30th day, a recovery point is retained on a daily basis at 00:00. After 30 days, the recovery point data is automatically cleared.
  - If the retention time is greater than 7 days, note that: From the end of the last retention day to the 30th day, a recovery point is retained on a daily basis at 00:00. After 30 days, the recovery point data is automatically cleared.

- **Recovery Point Interval**: Select the interval for generating recovery points. Unit: second. Valid values: 1, 3, and 5. By default, a recovery point is generated at an interval of 3 seconds.

- **Backup Rate Per Volumes**: Optional. You can limit the upstream bandwidth of each volume when CDP is performed on the VM instance. Unit: Mbps/Gbps. If not set, the bandwidth is not limited.

Figure 8-25: Create CDP Task



8.4.2.2.2 Manage a CDP Task

On the main menu of ZStack Cloud, choose **Platform O&M** > **Backup Management** > **CDP Service** > **CDP Task**. Then, the **CDP Task** page is displayed.

The following table lists the actions that you can perform on a CDP task.

Action	Description
Create CDP Task	Create a CDP task for a VM instance to protect the VM instance continuously. **Note:** • You can create a CDP task for VM instances that use any primary storages only. • VM instances with a CDP task can have only Ceph volumes attached.

Action	Description
	• VM instances with a CDP task can be migrated to Ceph primary storages only.
Edit CDP Task	Edit the name and description of a CDP task.
Enable CDP Task	Enable a CDP task that is disabled.
Disable CDP Task	Disable a CDP task that is enabled. Then, the continuous data protection is stopped for the VM instance.
Modify Protection Policy	Modify the protection policy of a CDP task, including the recovery point retention time, recovery point interval, and the CDP task planned size. **Note:** • Before you can modify a protection policy, disable the CDP task. • The new protection policy takes effect the next time the CDP task is enabled. • If you modify the planned capacity, make sure that the newly planned capacity is not smaller than the capacity used by the current task and the capacity required for full backup, and cannot be greater than the sum of the capacity used by the current task and the backup storage available size.
Delete CDP Task	Delete a CDP task. Then, all the CDP data of the VM instance that running this CDP task is also deleted. Please exercise caution. **Note:** • If a VM instance already has a CDP task, you could not create new CDP tasks for the VM instance. • After you delete the CDP task of a VM instance, you can create a new one for the VM instance.

8.5 Scheduled O&M

8.5.1 Scheduled Job

8.5.1.1 What is Scheduled O&M?

ZStack Cloud provides two types of scheduled O&M resources: scheduled jobs and schedulers. These two types of resources are independent from each other. You can create schedulers and scheduled jobs based on different rules and associate or disassociate scheduled jobs with or from schedulers.

Concepts

- A scheduled job defines that a specific action be implemented at a specified time based on a scheduler.
  - You can associate any available scheduled job with a scheduler.
  - You can select Disable, Enable, Attach, and Detach actions for a scheduled job based on your actual production environments.
  - If you delete a scheduler, the scheduled jobs associated with the scheduler will be disassociated. You can associate the scheduled jobs with other schedulers.
  - Operations triggered by scheduled jobs are all recorded by the Audit feature.
- A scheduler is used to schedule jobs. It is suitable for business scenarios that last for a long time.
  - A scheduler defines the implementation rules for a scheduled job.
  - A scheduler can be used for long-term operations, for example, creating snapshots at a specified interval for a VM instance.
  - If you delete a scheduler, the scheduled jobs associated with the scheduler will be disassociated. You can associate the scheduled jobs with other schedulers.
  - Operations triggered by schedulers are all recorded by the Audit feature.

Considerations

In the production environment, we recommend that you create a maximum of five snapshots for a volume and do not configure frequent scheduled snapshotting. Creating an excessive number of snapshots will lower I/O performance of VM instances or volumes, increase data security risks , and occupies the storage space of primary storage. To back up data for the long term, you can use Backup Service.

8.5.1.2 Create a Scheduled Job

On the main menu of ZStack Cloud, choose **Platform O&M** > **Scheduled O&M** > **Scheduled Job**. On the **Scheduled Job** page, click **Create Scheduled Job**. Then, the **Create Scheduled Job** page appears.

On the displayed page, set the following parameters:

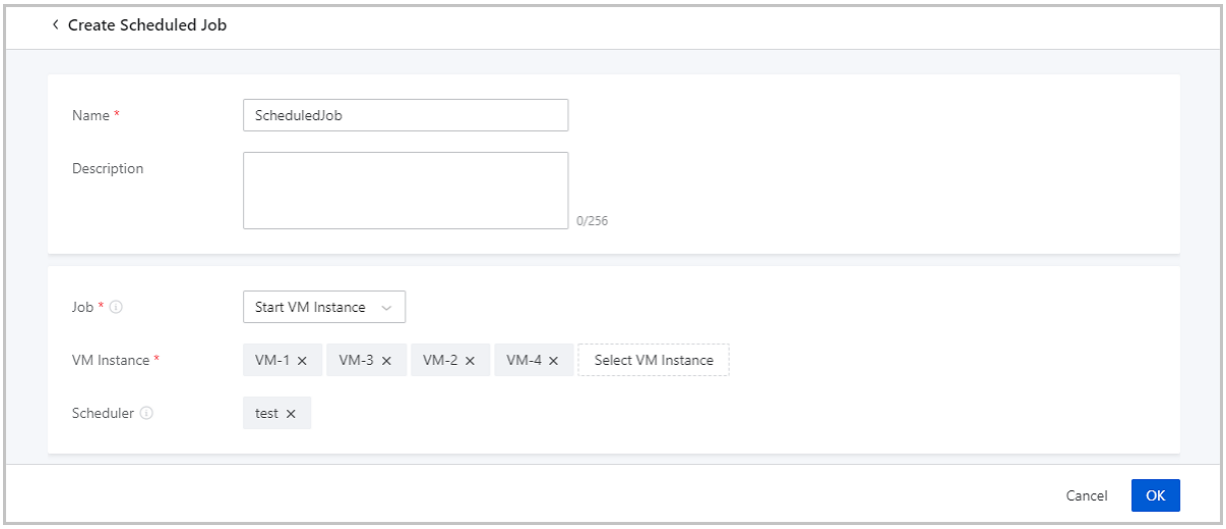
- **Name**: Enter a name for the job.
- **Description**: Optional. Enter a description for the job.

- **Job**: Select a job type. Valid values: Start VM Instance, Stop VM Instance, Reboot VM Instance, Create Snapshot for VM Instance, and Create Volume Snapshot.
- **VM Instance/Volume**: Select one or more VM instances or volumes for the scheduled job.
- **Reserved Snapshots**: Enter the maximum number of snapshots that you want reserve.

  Note:

  - If you create a scheduled job for a VM instance that uses a Ceph primary storage, you need to set reserved snapshots.
  - We recommend that you reserve 1-32 snapshots.
- **Scheduler**: Optional. Associate a scheduler to the scheduled job.

Figure 8-26: Create Scheduled Job



8.6 Tag Management

8.6.1 What is Tag?

A tag is used to mark resources. You can use a tag to search for and aggregate resources. Specifically, you can quickly locate the required resources by tag type and tag name.

- You can create tags with different colors, simple style, and brief description. You can also attach tags to resources and search resources by using tags. This will improve the search efficiency.
- Two types of tag are available: admin tags and tenant tags.

  - Admin tags are created and owned by administrators, and can be attached to VM instances, volumes, hosts, baremetal instances, and elastic baremetal instances.
  - Tenant tags are created and owned by tenants, and can be attached to VM instances and volumes.
- Currently, you can attach tags to or detach tags from VM instances, volumes, hosts, baremetal instances, and elastic baremetal instances.

Considerations

- Admin tags are created and owned by administrators while tenant tags are created and owned by tenants.
- Tags created by tenants can only be attached to resources of the corresponding tenants, while admin tags can be attached to all of the resources in the Cloud.
- Administrators can detach or delete tenant tags.
- Tags in a project are owned by the project. Therefore, everyone in the project, including the project manager, project administrator, and project member, can perform operations on these tags.
- Currently, tag owners cannot be changed.
- When you change a resource owner, all tenant tags attached to the resource will be detached. However, the admin tags are not affected.
- After the Cloud is upgraded seamlessly, the existing tags will be updated accordingly and displayed in the latest way. If an exception occurs, refresh your browser or create a new tag.

8.6.2 Create a Tag

On the main menu of ZStack Cloud, choose **Platform O&M** > **Tag Management** > **Tag**. On the **Tag** page, click **Create Tag**. Then, the **Create Tag** page is displayed.

On the displayed page, set the following parameters:

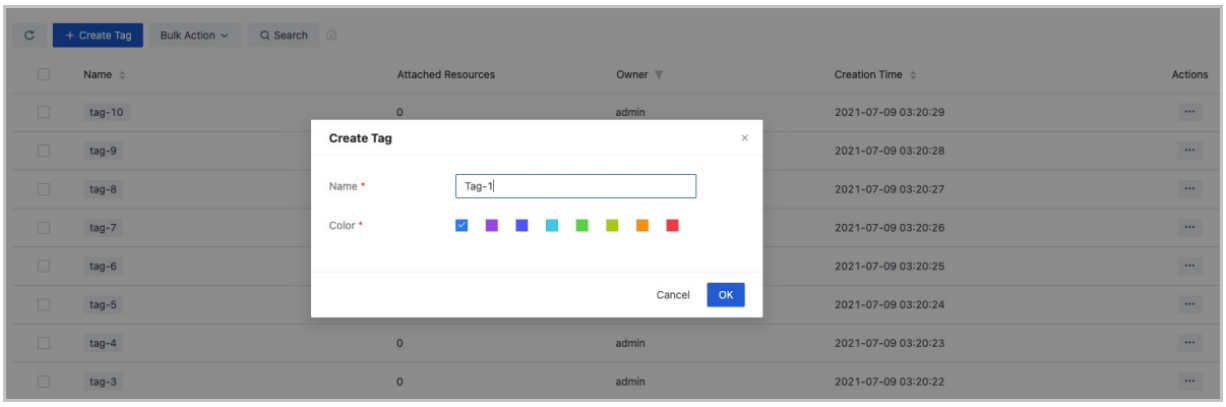
- **Name**: Enter a name for the tag.

  Note:

  - The tag name must be 1 to 20 characters in length.
  - The tag name is case sensitive.
  - A tag is unique. That is, the same role can have only one tag with the same name and color.

- **Color**: Select the tag color.

Figure 8-27: Create Tag



8.7 Migration Service

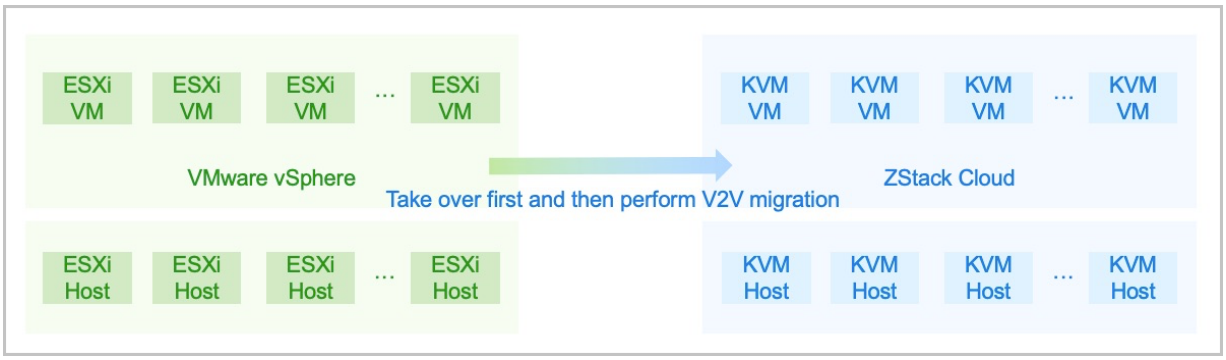
8.7.1 What is Migration Service?

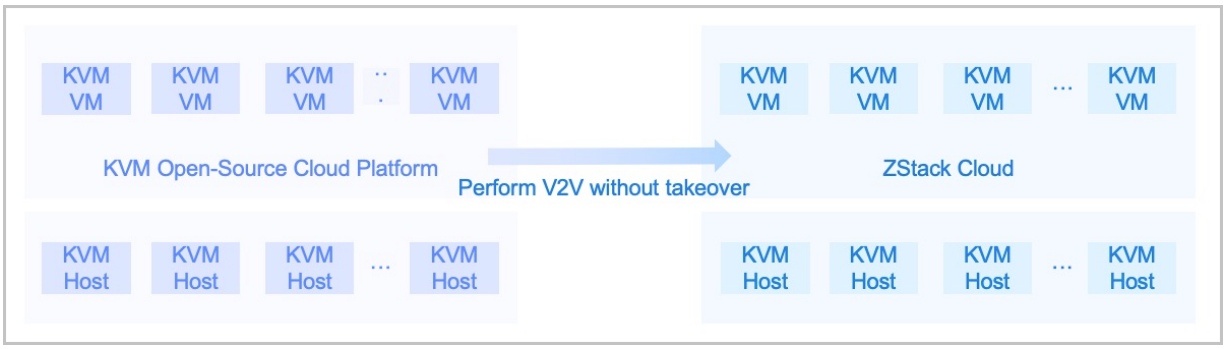
The Cloud provides V2V migration service that allows you to migrate VM instances and data from other virtualized platform to the current cloud platform.

You can use V2V Migration to:

- Migrate VM instances from vCenters that are took over by the Cloud. The supported versions of the source vCenter platform include 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0. Note that the version of vCenter Server must be consistent with that of ESXi hosts.
- Migrate VM instances from a KVM cloud platform to the Cloud.

Figure 8-28: V2V Migration





Characteristics

- You can migrate VM instances in bulk from a cloud platform to the Cloud with one click.
- You only need to add a conversion host and create a V2V job. The Cloud will do the migration for you.
- You can configure an independent migration network and a network QoS for a conversion host to manage transmission obstacles and improve migration efficiencies.
- You can customize configuration settings for destination VM instances when you create a V2V job.
- You can monitor and manage the entire migration process by using the UI.

Considerations

The Migration Service feature is provided in a separate module. Before you can use this feature, you need to purchase the Plus License of Migration Service, in addition to the Base License.

9 Operational Management

9.1 Enterprise Management

9.1.1 What is Enterprise Management?

Enterprise Management allows enterprise users to create and manage their organization structures based on their actual situation. It also provides project-based resource access control, ticket management, and independent zone management features.

The Enterprise Management feature is provided in a separate module. Before you can use this feature, you need to purchase the Plus License of Enterprise Management, in addition to the Base License.

9.2 Billing Management

9.2.1 What is Billing Management?

ZStack Cloud provides a quasi-public cloud billing experience. You can customize the unit price for different resources by using a pricing list and obtain related bills after you associate the pricing list with a project or an account. Currently, the following resources in the Cloud can be billed: CPU, memory, root volume, data volume, GPU device, elastic baremetal instances, and public IP, (VM IP),and public IP (VIP).

Concepts

- Pricing list: A pricing list is a list of unit prices of different resources. The unit price of a resource is set based on the specification and usage time of the resource.
- Bill: A bill is the expense of resources totaled at a specified time period. Billing is accurate to the second. Bills can be categorized into project bills, department bills, and account bills.

Characteristics

ZStack Cloud Billing Management has the following characteristics:

- You can centrally and efficiently manage the unit price of a group of resources by using a pricing list.
- A pricing list includes the unit price of multiple resources. You can set a unit price for root volumes and data volumes, respectively, by disk performance.
- You can create multiple pricing lists and use separate pricing lists for projects and accounts. Note that you can associate a pricing list with multiple projects and accounts.

- After you configure a pricing list, bills can be generated in real time by account.
- After you configure a pricing list, bills can be generated in real time by project. You can also add the project to a department. Then, bills are generated by department.
- You can customize the time when the billing details are generated. You can also view the billing details by resource.
- You can set the currency symbol displayed on the UI by modifying the value of **Currency Symbol** in the global settings. Default value: ¥. Valid values: ¥, $, €, £, A$, HK$, ¥, CHF, and C $.

Billing Mechanism

- If you disable **Billing** on Global Setting, the system stops billing resources and bills are no longer generated.
- If a VM instance is deleted but not expunged, the compute resources (memory and CPU) and IP resources that the VM instance occupied are released but storage resources are still occupied. Therefore, CPU, memory, and public IP resources are not billed but the root volume is still billed.
- If a VM instance is stopped, the compute resources of the VM instance are released but the storage and IP resources are still occupied. Therefore, CPU and memory resources are not billed but the root volume and public IP resources are still billed.
- Elastic baremetal instances are created from and function based on baremetal nodes. If you power off and release a baremetal node, the system stops billing the associated elastic baremetal instance.
- If a volume is deleted but not expunged, the storage resources are still occupied. Therefore, the data volume is still billed. If the volume is expunged, the system stops billing the volume.
- A public IP address is billed based on the bandwidth consumed by the IP address. You need to set QoS for public IPs (VIPs) or public IPs (VM IPs) before you can set unit prices for the public IP addresses.
- Uninstantiated volumes are not billed. If you instantiate a volume, the volume is billed even if the volume is not attached to a volume.
- If you change the owner of a resource, the bills generated for the resource usage before the owner change is reserved in the previous account or project and the bills generated for the resource usage after the owner change is reserved in the new account or project,.

9.2.2 Pricing List

9.2.2.1 Create a Pricing List

Create Pricing List

On the main menu of ZStack Cloud, choose **Operational Management** > **Billing Management** > **Pricing List**. On the **Pricing List** page, click **Create Pricing List**. Then, the **Create Pricing List** page appears.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the pricing list.
- **Description**: Optional. Enter a description for the pricing list.
- **Unit Price**: Click **Add Unit Price** and add unit prices for resources.

  The resources include CPU, memory, root volume, data volume, GPU device, elastic baremetal instances, public IP of VM instance, and public VIP.

  - To set unit price for CPU, configure the following:
    - Price: 0 to 10000, accurate to five decimal points.
    - Time Unit: second, minute, hour, day, week, and month (30 days).
  - To set unit price for memory, configure the following:
    - Price: 0 to 10000, accurate to five decimal points.
    - Resource Unit: MB, GB, and TB.
    - Time Unit: second, minute, hour, day, week, and month (30 days).
  - To set unit price for root volume, configure the following:
    - Advanced: Configure advanced parameters in JSON format based on disk performance.

      Sample:

```
{
    "priceUserConfig": {
        "priceKeyName": "Enter a value for the priceKeyName
field."
    }
}
```

Note:

Make sure the value of the **`priceUserConfig`** parameter is consistent with the configuration in the advanced parameter settings in the instance offering. Otherwise, bills cannot be generated.

- Price: 0 to 10000, accurate to five decimal points.
- Resource Unit: MB, GB, and TB.
- Time Unit: second, minute, hour, day, week, and month (30 days).

- To set unit price for data volume, configure the following:
  - Advanced: Configure advanced parameters in JSON format based on disk performance.

    Sample:

```
{
    "priceUserConfig": {
        "priceKeyName": "Enter a value for the priceKeyName
field."
    }
}
```

Note:

Make sure the value of the **`priceUserConfig`** parameter is consistent with the configuration in the advanced parameter settings in the disk offering. Otherwise, bills cannot be generated.

  - Price: 0 to 10000, accurate to five decimal points.
  - Resource Unit: MB, GB, and TB.
  - Time Unit: second, minute, hour, day, week, and month (30 days).
- To set unit price for GPU, configure the following:
  - GPU Type: Select Desktop GPU or Compute GPU.
  - GPU Model: Enter the model of the passed-through GPU.
  - Price: 0 to 10000, accurate to five decimal points.
  - Time Unit: second, minute, hour, day, week, and month (30 days).
- To set unit price for public IP, configure the following:
  - Resource Type: Select Public IP (VM IP) or Public IP (VIP).
    - If you select Public IP (VM IP), you can bill public IP addresses of VM instances that are created by using public networks. You can set QoS for VM NICs. Then the IP addresses are billed.

- If you select Public IP (VIP), you can bill VIPs that are created by using public networks and are used to provide network services. You can set QoS for the VIPs. Then the VIPs are billed.

— Upstream Bandwidth price: 0 to 10000, accurate to five decimal points.

— Downstream Bandwidth price: 0 to 10000, accurate to five decimal points.

Note:

If you configure unit price for public IP addresses, you must configure upstream bandwidth, downstream bandwidth, or both for the public IP addresses.

— Resource Unit: Kbps, Mbps, and Gbps.

— Time Unit: second, minute, hour, day, week, and month (30 days).

Note:

VM public IP addresses and public VIPs are billed based on the consumed bandwidth resources. Before you configure unit prices for the public IP addresses, note that：

- You need to set QoS for the public IP addresses.
- IPv6 VIPs do not support billing.

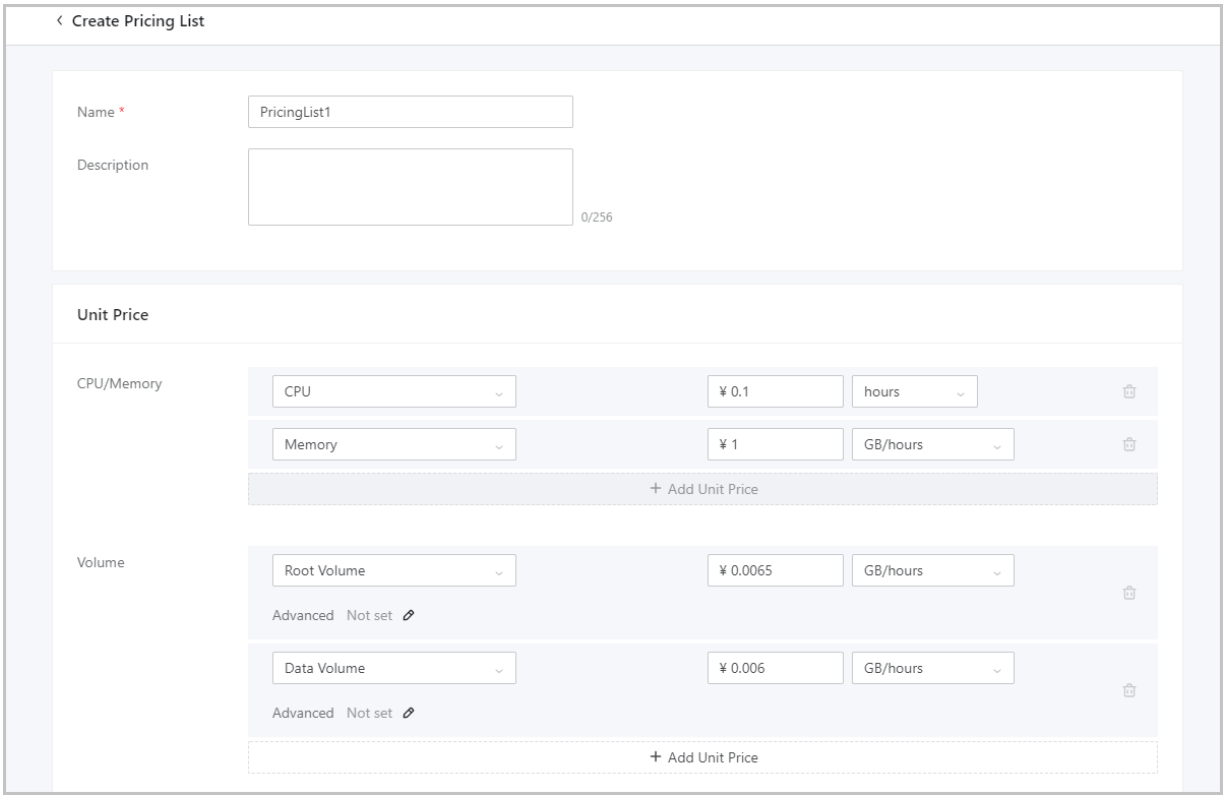
- To set unit price for elastic baremetal instance, configure the following:

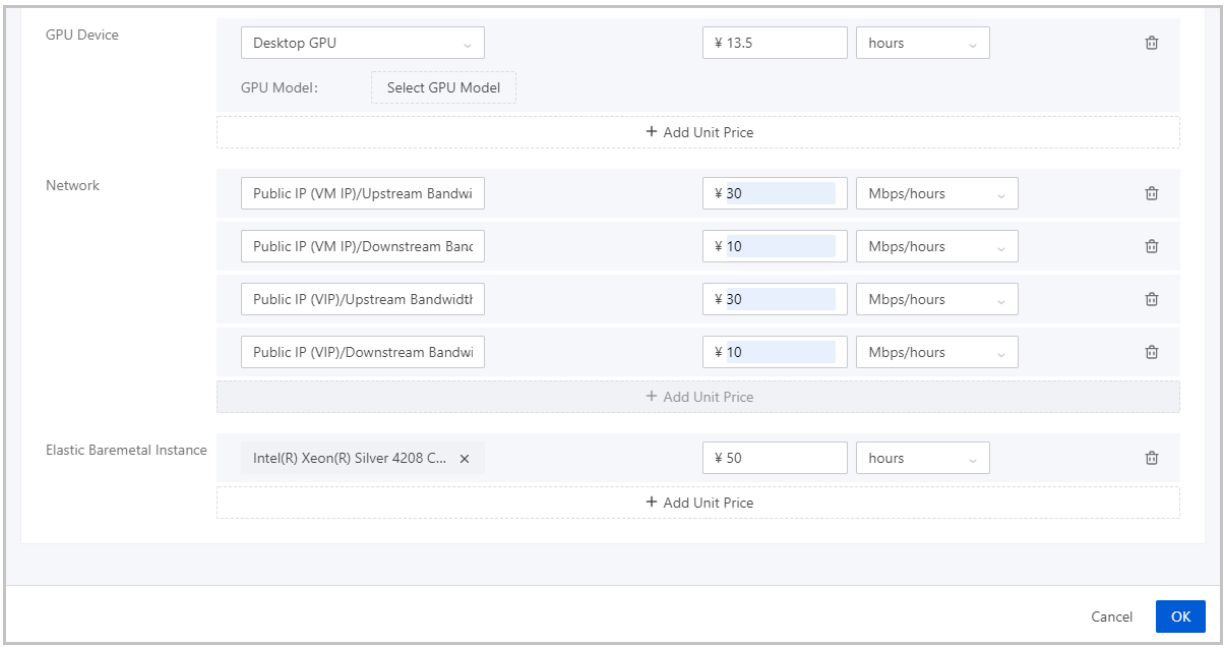
— Elastic Baremetal Instance Offering: Select an elastic baremetal instance offering and set a unit price for the offering.

— Price: 0 to 10000, accurate to five decimal points.

— Time Unit: second, minute, hour, day, week, and month (30 days).

Figure 9-1: Create Pricing List





9.3 Access Control

9.3.1 Console Proxy

Console proxy allows you to log in to a VM instance by using the IP address of a proxy.

9.3.2 AccessKey Management

An AccessKey pair is a security credential that one party authorizes another party to call API operations and access its resources in the Cloud. AccessKey pairs shall be kept confidential.

9.3.3 IP Allowlist/Blocklist

An IP blocklist or allowlist identifies and filters IP addresses that access the Cloud. You can create an IP allowlist or blocklist to improve access control of the Cloud.

9.4 Application Center

9.4.1 What is Application Center?

Application Center allows you to add third-party applications to the Cloud and then access the applications by using the Cloud. It extends the functionality of the Cloud.

9.4.2 Add an Application

On the main menu of ZStack Cloud, choose **Operational Management** > **Application Center**. On the **Application Center** page, click **Add Application**. Then, the **Add Application** pane appears.

On the displayed pane, set the following parameters:

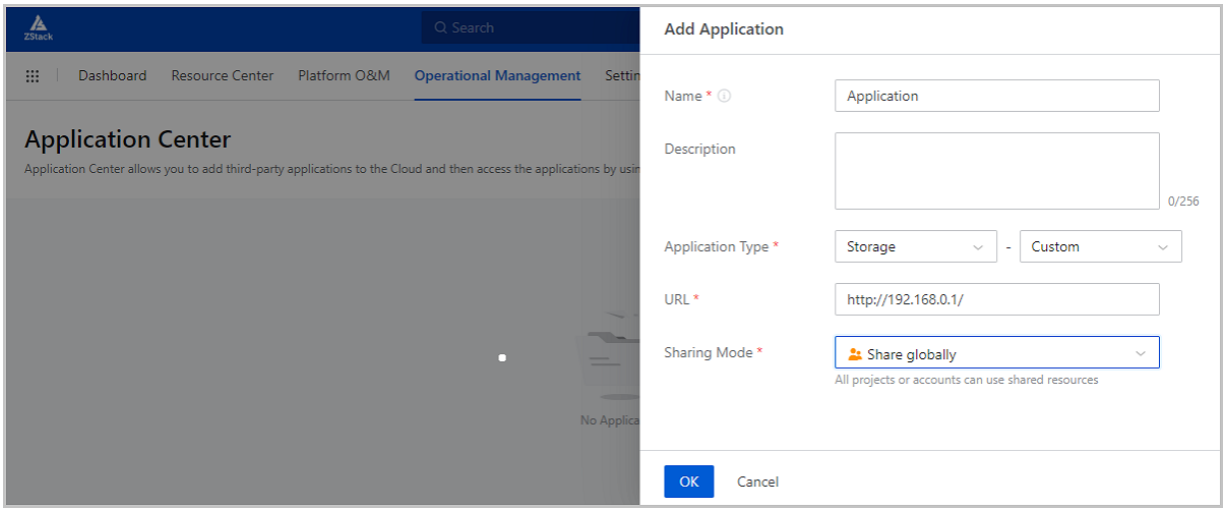
- **Application Type**: Select an application type. Valid values: Storage, Database, Security, IaaS, PaaS, and SaaS.
- **Name**: Enter an application name.

  The name must be 1-128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the application.
- **URL**: Enter the URL of the application.
- **Sharing Mode**: Set the sharing mode of the resource. Valid values:
  - Share globally: Share the resource with all projects and accounts.
  - Share to specified projects/accounts: Share the resource with specified projects and accounts.
  - Not share: Revoke the shared resource. If revoked, other projects and accounts cannot use the resource.

Note:

1. If you change the sharing mode of a resource from Share Globally to Share to Specified Projects or Accounts, the resource is visible only to the specified projects or accounts.
2. If you modify the sharing mode, resources that are used by projects or accounts before the modification are not affected until the resources are released.

Figure 9-2: Add Application



10 Settings

10.1 Sub-Account Setting

10.1.1 What is Sub-Account?

A sub-account is created and managed by the admin. Resources created under a sub-account is managed by the sub-account. You can use a sub-account to create, share, delete, and revoke resources under its management and implement fine-grained control over the permissions on resources.

Concepts

- **admin**: The admin has super privileges over resources and shall be owned by the IT system administrator.
  - The admin can share instance offerings, disk offerings, networks, images, and other cloud resources with sub-accounts or unshare the resources from sub-accounts. Sub-accounts can only manage resources to which they are granted access.
  - The admin can modify resource quotas granted to a sub-account based on different business scenarios.
  - After the admin created a VXLAN pool, sub-accounts can create VXLAN networks based on the VXLAN pool.
  - Changing the owner of a VM instance will change the owner properties of the EIPs associated with the VM instance.
- **Sub-Account**: A sub-account is created by the admin.
  - A sub-account has management permissions on VM instances, images, volumes, and security groups created under the sub-account. A sub-account can perform read operations on resources shared by the admin, but cannot delete the resources.
  - Deleting a sub-account will delete all resources created by the sub-account, such as VM instances, volumes, and images.
  - The names of sub-accounts must be unique.
  - Resource quotas that the admin shares with a sub-account is displayed on the homepage of the sub-account.

- Before a sub-account can create a VM instance, the admin must share an instance offering, disk offering, network, and other required resources with the sub-account. Otherwise, a VM instance cannot be created.
- A sub-account can use an image that it adds to the Cloud or use an image shared by the admin.

- **Sub-Account Quota**:

  Resource quotas that the admin shares with a sub-account specify the maximum resources that the sub-account can manage, including computing resource quotas, storage resource quotas, network resource quotas, and other resource quotas.

  The admin uses the preceding resource quota settings to manage the maximum resources granted to sub-accounts. If a resource is deleted but not expunged, the resource still occupies storage space of primary storage and volumes.

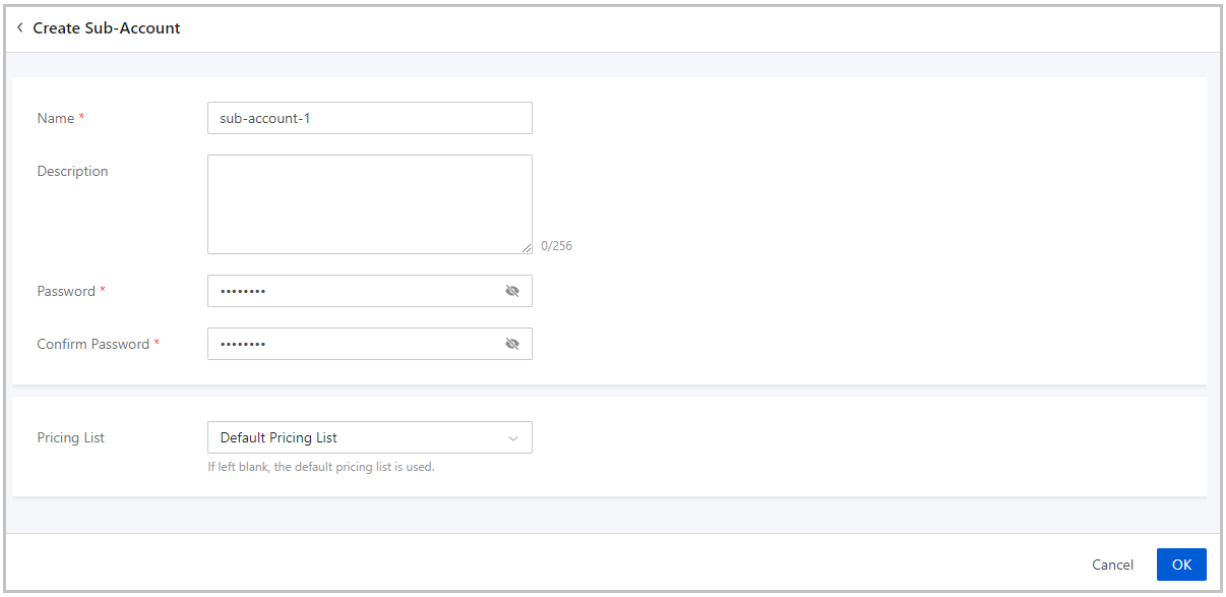
10.1.2 Create a Sub-Account

On the main menu of ZStack Cloud, choose **Settings** > **Sub-Account Setting** > **Sub-Account Management**. On the **Sub-Account** page, click **Create Sub-Account**. Then, the **Create Sub-Account** page is displayed.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the sub-account.
- **Description**: Optional. Enter a description for the sub-account.
- **Password**: Enter a password for the sub-account.
- **Confirm Password**: Confirm the sub-account password.
- **Pricing List**: Optional. Select a pricing list. If left blank, the default pricing list is used.

Figure 10-1: Create Sub-Account



10.2 Theme and Appearance

10.2.1 What is Theme and Appearance?

You can customize the theme and appearance of the Cloud.

10.3 Email Server

10.3.1 What is Email Server?

If you select Email as the endpoint of an alarm, you need to set an email server. Then alarm messages are sent to the email server.

10.3.2 Add an Email Server

On the main menu of ZStack Cloud, choose **Setting** > **System Setting** > **Email Server**. On the **Email Server** page, click **Add Email Server**. Then, the **Add Email Server** page appears.

On the displayed page, set the following parameters:

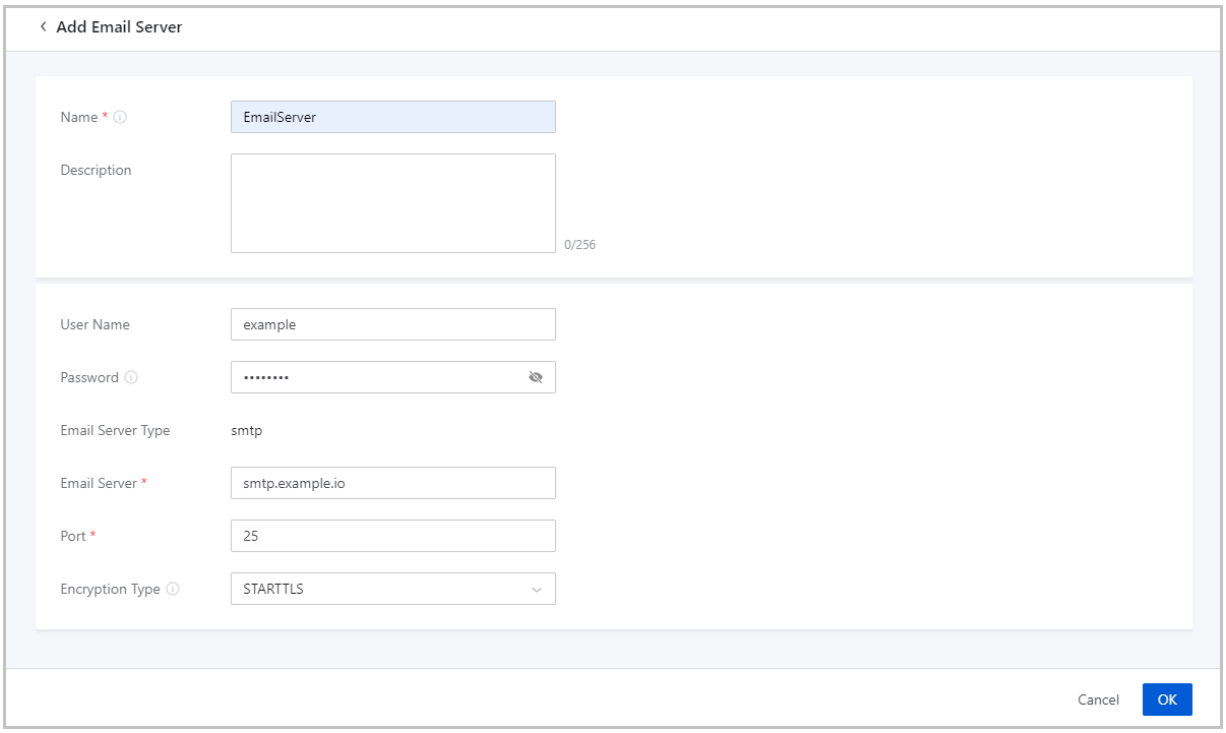
- **Name**: Enter a name for the email server.
- **Description**: Optional. Enter a description for the email server.
- **User Name**: Enter a user name.
- **Password**: Enter the password for the user.

Note:

If you add a third-party email server to the Cloud, you need to enable the SMTP service in advance. In addition, enter the authentication code in the Password field.

- **Email Server Type**: Valid value: smtp.
- **Email Server**: Enter the IP address of the email server.
- **Port**: Enter the port of the email server. Default value: 25.
- **Encryption Type**: Optional. Select an encryption type to encrypt data communications of the email server port. Valid values: STARTTLS, SSL/TLS, and NONE.
  - STARTTLS is selected by default. The corresponding port is 25 by default.
  - If you select SSL/TLS, the corresponding port is 465 by default.
  - If you do not need encrypted communications, select NONE.

Figure 10-2: Add Email Server



After you click **OK**, the system automatically checks whether the user name, password, email server IP address and port, and encryption type parameters are correct. The response time is expected to be no longer than five seconds. If a parameter setting is incorrect, modify the setting based on the tips propped out on the upper-right corner of the page and then submit again. If the configuration settings are correct, you are automatically redirected to the **Email Server** page. The email server is successfully added to the Cloud.

Note:

Configure the settings as needed. Contact the email server provider for support in case of any email server related problems.

10.4 Log Server

10.4.1 What is Log Server?

A log server is used to collect logs of the management node. You can add a log server to the cloud and use the collected logs to locate errors and exceptions. This makes your O&M more efficient.

10.4.2 Add a Log Server

On the main menu of ZStack Cloud, choose **Setting** > **System Setting** > **Log Server**. On the **Log Server** page, click **Add Log Server**. Then, the **Add Log Server** page appears.

On the displayed page, set the following parameters:

- **Name**: Enter a name for the log server.

  The name must be 1 to 128 characters in length and can contain letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description**: Optional. Enter a description for the log server.
- **IP Address**: Enter the IP address of the log server.
- **UDP Port**: Enter a port that uses the UDP protocol to provide services.
- **Log Severity**: Specify the log severity.

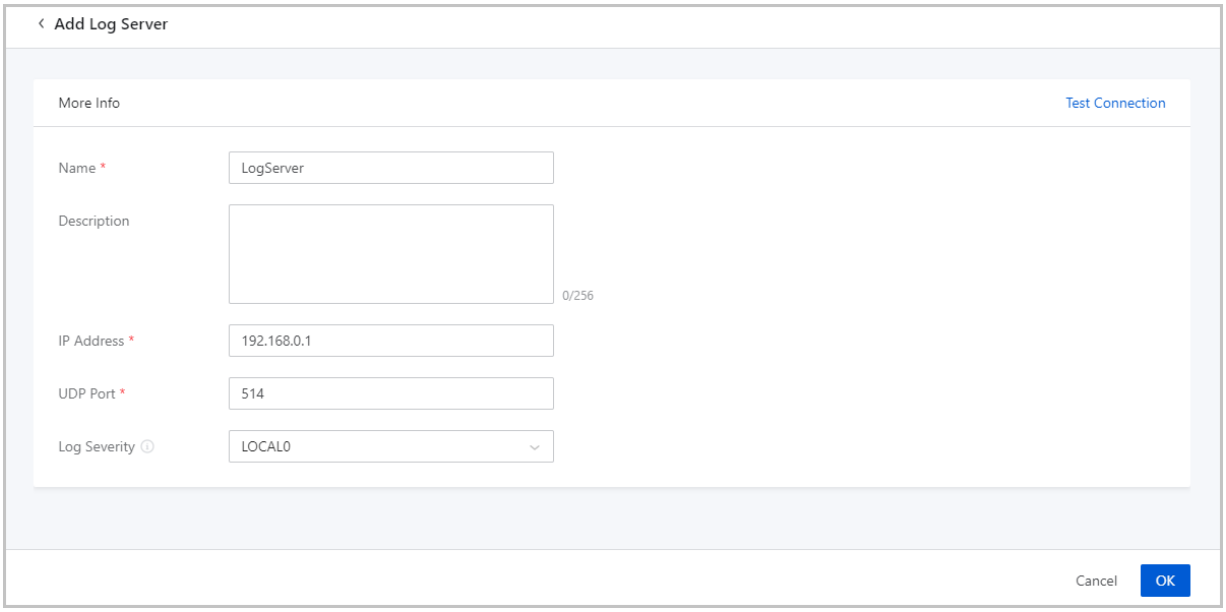
  Note:

  The log severity must be consistent with the setting configured in the log server. Otherwise, log information cannot be received as expected.
- **Test Connection**: Check whether the configured IP address is reachable.

  Note:

  - If the IP address is unreachable, check whether the IP address is correct, the network is normal, and the log severity setting is consistent.
  - Configure the settings as needed. Contact the log server provider for support in case of any email server related problems.

Figure 10-3: Add Log Server



10.5 Global Setting

Global Setting allows you to configure settings that take effect on the whole platform.

In the top-right corner of the **Global Setting** page, click **Reset to Default Settings**. Then all settings are reset to the initial settings.

Global Setting provides **basic settings** and **advanced settings**. ZStack Cloud provides over a hundred of advanced settings. You can configure the settings based on your business needs.

10.6 Scenario Template

Scenario Template provides multiple templates that encapsulate scenario-based global settings . You can apply a template globally with one click based on your business needs. This improves your O&M efficiency.

Glossary

VM Instance

A VM instance is a virtual machine instance running on a host. A VM instance has its own IP address and can access public networks and run application services.

Volume

A volume provides storage space for a VM instance. Volumes are categorized into root volumes and data volumes.

Root Volume

A root volume provides support for the system operations of a VM instance.

Data Volume

A data volume provides extended storage space for a VM instance.

Image

An image is a template file used to create a VM instance or volume. Images are categorized into system images and volume images.

Instance Offering

An instance offering defines the number of vCPU cores, memory size, network bandwidth, and other configuration settings of VM instances.

Disk Offering

A disk offering defines the capacity and other configuration settings of volumes.

GPU Specification

A GPU specification defines the frame per second (FPS), video memory, resolution, and other configuration settings of a physical or virtual GPU. GPU specifications are categorized into physical GPU specifications and virtual GPU specifications.

Auto-Scaling Group

An auto-scaling group is a group of VM instances that are used for the same scenarios. An auto-scaling group can automatically scale out or in based on application workloads or health status of VM instances in the group.

Snapshot

A snapshot is a point-in-time capture of data status in a volume.

Affinity Group

An affinity group is an orchestration policy for IaaS resources to ensure the high performance and high availability of businesses...

Zone

A zone is a logical group of resources such as clusters, L2 networks, and primary storages. Zone is the largest resource scope defined in the Cloud.

Cluster

A cluster is a logical group of hosts (compute nodes).

Host

A host provides compute, network, and storage resources for VM instances.

Primary Storage

A primary storage is one or more servers that store volume files of VM instances. These files include root volume snapshots, data volume snapshots, image caches, root volumes, and data volumes.

Backup Storage

A backup storage is one or more servers that store VM image templates, including ISO image files .

iSCSI Storage

iSCSI storage is an SAN storage that uses the iSCSI protocol for data transmission. You can add an iSCSI SAN block as a Shared Block primary storage or pass through the block to a VM instance.

FC Storage

FC storage is an SAN storage that uses the FC technology for data transmission. You can add an FC SAN block as a Shared Block primary storage or pass through the block to a VM instance.

L2 Network

An L2 network is a layer 2 broadcast domain used for layer 2 isolation. Generally, L2 networks are identified by names of devices on the physical network.

VXLAN Pool

A VXLAN pool is a collection of VXLAN networks established based on VXLAN Tunnel Endpoints (VTEPs). The VNI of each VXLAN network in a VXLAN pool must be unique.

L3 Network

An L3 network includes IP ranges, gateway, DNS, and other network configurations that are used by VM instances.

Public Network

Generally, a public network is a logical network that is connected to the Internet. However, in an environment that has no access to the Internet, you can also create a public network.

Flat Network

A flat network is connected to the network where the host is located and has direct access to the Internet. VM instances in a flat network can access public networks by using elastic IP addresses.

VPC Network

A VPC network is a private network where VM instances can be created. A VM instance in a VPC network can access the Internet through a VPC vRouter.

Management Network

A management network is used to manage physical resources in the Cloud. For example, you can create a management network to manage access to hosts, primary storages, backup storages, and VPC vRouters.

Flow Network

A flow network is a dedicated network for port mirror transmission. You can use a flow network to transmit the mirrors of data packets of NIC ports to the target ports.

VPC vRouter

A VPC vRouter is a dedicated VM instance that provides multiple network services.

VPC vRouter HA Group

A VPC vRouter HA group consists of two VPC vRouters. Either VPC vRouter can be a primary or secondary VPC vRouter for the group. If the primary VPC vRouter does not work as expected, the VPC vRouter becomes the secondary VPC vRouter in the group to ensure high availability of business.

vRouter Image

A vRouter image encapsulates network services and can be used to create VPC vRouters and load balancers. vRouter images can be categorized into VPC vRouter images and load balancer (LB) images.

Dedicated-Performance LB Image

A dedicated-performance load balancer (LB) image encapsulates dedicated-performance load -balancing services and can be used to create load balancer instances. However, a dedicated-performance load balancer image cannot be used to create VM instances.

vRouter Offering

A vRouter offering defines the number of vCPU cores, memory size, image, management network , and public network configuration settings of VPC vRouters. You can use a vRouter offering to create VPC vRouters that can provide network services for public networks and VPC networks.

LB Instance Offering

A load balancer (LB) instance offering defines the CPU, memory, image, and management network configuration settings used to create LB instances. LB instances provide load balancing services for the public network, flat network, and VPC network.

SDN Controller

An SDN controller is used to control network devices such as switches. You can add an external SDN controller to the Cloud and use the controller to control external switches and other network devices.

Security Group

A security group provides security control services for VM instances on the L3 network. It filters the ingress or egress TCP, UDP, and ICMP packets of specified VM instances in specified networks based on the specified security rules.

VIP

In bridged network environments, a virtual IP address (VIP) provides network services such as serving as an elastic IP address (EIP), port forwarding, load balancing, IPsec tunneling. When a VIP provides the preceding network services, packets are sent to the VIP and then routed to the destination network where VM instances are located.

EIP

An elastic IP address (EIP) functions based on the NAT technology. IP addresses in a private network are translated into an EIP that is in another network. This way, private networks can be accessed from other networks by using EIPs.

Port Forwarding

Port forwarding functions based on the layer-3 forwarding service of VPC vRouters. This service forwards traffic flows of the specified IP addresses and ports in a public network to specified ports of VM instances by using the specified protocol. If your public IP addresses are insufficient, you can configure port forwarding for multiple VM instances by using one public IP address and port.

Load Balancer

A load balancer distributes traffic flows of a virtual IP address to backend servers. It automatically inspects the availability of backend servers and isolates unavailable servers during traffic distributi on. This way, the load balancer improves the availability and service capability of your business.

Listener

A listener monitors the frontend requests of a load balancer and distributes the requests to a backend server based on the specified policy. In addition, the listener performs health checks on backend servers.

Forwarding Rule

A forwarding rule forwards the requests from different domain names or URLs to different backend server groups.

Backend Server Group

A backend server group is a group of backend servers that handles requests distributed by load balancers. It is the basic unit for traffic distribution by load balancer instances.

Backend Server

A backend server handles requests distributed by a load balancer. You can add a VM instance on the Cloud or a server on a third-party cloud as a backend server.

Frontend Network

A frontend network is a type of network that is associated with a load balancer. Requests from the network are distributed by the load balancer to backend servers based on a specified policy.

Backend Network

A backend network is a type of network that is associated with a load balancer. Requests from frontend networks are distributed by the load balancer to servers in the backend network.

Load Balancer Instance

A load balancer instance is a custom VM instance used to provide load balancing services.

Certificate

If you select HTTPS for a listener, associate it with a certificate to make the listener take effect. You can upload either a certificate or certificate chain.

Firewall

A firewall is an access control policy that monitors ingress and egress traffic of VPC vRouters and decides whether to allow or block specific traffic based on a defined set of security rules.

IPsec Tunnel

An IPSec tunnel encrypts and verifies IP packets that transmit over a virtual private network (VPN) from one site to another.

OSPF Area

An OSPF area is split from an autonomous system based on the OSPF protocol. This splitting simplifies the management of vRouters.

NetFlow

An NetFlow monitors the ingress and egress traffic of the NICs of VPC vRouters. The supported versions of data flows are V5 and V9.

Port Mirroring

Port mirroring mirrors the traffic data of VM NICs and sends the traffic data to the target ports. This allows for the analysis of data packets of ports and simplifies the monitoring and management of data traffic and makes it easier to locate network errors and exceptions.

Route Table

A route table contains information about various routes that you configure. Route entries in a route table must include the destination network, next hop, and route priority.

CloudFormation

CloudFormation is a service that simplifies the management of cloud resources and automates deployment and O&S. You can create a stack template to configure cloud resources and their dependencies. This way, resources can be automatically configured and deployed in batches. CloudFormation provides easy management of the lifecycle of cloud resources and integrates automatic O&S into API and SDK.

Resource Stack

A resource stack is a stack of resources that are configured by using a stack template. The resources in the stack have dependencies with each other. You can manage resources in the stack by managing the resource stack.

Stack Template

A stack template is a UTF8-encoded file based on which you can create resource stacks. The stack template defines the resources that you want, the dependencies between the resources , and the configuration settings of the resources. When you use a stack template to create a resource stack, CloudFormation parses the template and the resources are automatically created and configured.

Sample Template

A sample template is a commonly used resource stack. You can use a sample template provide by the Cloud to create resource stacks.

Designer

A designer is a CloudFormation tool that allows you to orchestrate cloud resources. You can drag and drop resources on a canvas and use lines to establish dependencies between the resources.

Baremetal Cluster

A baremetal cluster consists of baremetal chassis. You can manage baremetal chassis by managing a baremetal cluster where the chassis reside.

Deployment Server

A deployment server is a server that provides PXE service and console proxy service for baremetal chassis.

Baremetal Chassis

A baremetal chassis is used to create a baremetal instance and is identified based on the BMC interface and IPMI configuration setting.

Preconfigured Template

A preconfigured template is used to create a preconfigured file that allows for unattended batch installation of an operating system for baremetal instances.

Baremetal Instance

A baremetal instance is an instantiated baremetal chassis.

Elastic Baremetal Management

Elastic Baremetal Management provides dedicated physical servers for your applications to ensure high performance and stability. In addition, this feature allows elastic scaling. You can apply for and scale resources based on your needs.

Provision Network

A provision network is a dedicated network for PXE boot and image downloads while creating elastic baremetal instances.

Elastic Baremetal Cluster

An elastic baremetal cluster consists of elastic baremetal instances. You can manage elastic baremetal instances by managing an elastic baremetal cluster where the instances reside.

Gateway Node

A gateway node is a node where the ingress and egress traffic of the Cloud and elastic baremetal instances is forwarded.

Baremetal Node

A baremetal node is used to create a baremetal instance and is identified based on the BMC interface and IPMI configuration setting.

Elastic Baremetal Instance

An elastic baremetal instance has the same performance as physical servers and allows elastic scaling. You can apply for and scale resources based on your needs.

Elastic Baremetal Offering

An elastic baremetal offering defines the number of vCPU cores, memory size, CPU architecture, CPU model, and other configuration settings of elastic baremetal instances.

vCenter

The Cloud allows you to take over vCenter and manage resources on the vCenter.

VM Instance

A VM instance is an ESXi virtual machine instance running on a host. A VM instance has its own IP address to access public networks and can run application services.

Network

A vCenter network defines the network settings of VM instances on vCenter, such as IP range, gateway, DNS, and network services.

Volume

A volume provides storage space for a VM instance on vCenter. A volume attached to a VM instance can be used as a root volume or data volume. A root volume provides support for the system operations of a VM instance. A data volume provides extended storage space for a VM instance.

Image

An image is a template file used to create a VM instance or volume on vCenter. Images are categorized into system images and volume images.

Event Message

Event Message displays event alarm messages of vCenter that is took over by the Cloud. This feature allows you to locate errors and exceptions efficiently.

Network Topology

A network topology visualizes the network architecture of the Cloud. It allows for efficient planning , management, and improvement of network architecture. Network topologies can be categorized into global topologies and custom topologies.

Performance Analysis

Performance Analysis displays the performance metrics of key resources under monitoring in the Cloud. Cloud resources can be externally or internally monitored. You can use either method to monitor the performance of resources in the Cloud and improve O&S efficiency.

Capacity Management

Capacity Management visualizes the capacities and usages of key resources in the Cloud. You can use this feature to improve O&S efficiency.

MN Monitoring

MN monitoring allows you to view the health status of each management node when you use multiple management nodes to achieve high availability.

Alarm

An alarm is used to monitor the status of time-series data and events and respond to the status change. Alarms can be categorized into resource alarm, event alarm, and extended alarm.

One-Click Alarm

A one-click alarm integrates multiple metrics of a resource. You can create one-click alarms for multiple resources to monitor these resources.

Alarm Template

An alarm template is a template of alarm rules. If you associate an alarm template with a resource group, an alarm is created to monitor the resources in the group.

Resource Group

A resource group consists of resources grouped based on your business needs. If you associate an alarm template with a resource group, the alarm rules specified by the template take effect on all the resources in the group.

Message Template

A message template specifies the text template of a resource alarm message or event alarm message sent to an SNS system.

Message Source

A message source is used to take over extended alarm messages. If you configure alarms for message sources, extended alarm messages can be sent to various endpoints.

Endpoint

An endpoint is a method that users obtain subscribed messages. Endpoints are categorized into system endpoints, email, DingTalk, HTTP application, short message service, and Microsoft Teams.

Alarm Message

An alarm message is a message sent the time when an alarm is triggered.

Operation Log

An operation log is a chronological record of operations on the specified objects and their operation results.

Audit

Audit monitors and records all activities on the Cloud. You can use this feature to implement operation tracking, cybersecurity classified protection compliance, security analysis, troublesho oting, and automatic O&M.

Backup Management

Backup management integrates multiple disaster recovery technologies such as incremental backup and full backup that are suitable for multiple business scenarios. You can implement local backup and remote backup based on your business needs.

Backup Job

You can create a backup job to back up local VM instances, volumes, or databases to a specified storage server on a regular basis.

Local Backup Data

Local backup data of VM instances, volumes, and databases is stored in the local backup storage.

Local Backup Storage

A local backup storage is located at the local data center and is used to store local backup data.

Remote Backup Storage

A remote backup storage is located at a remote data center or a public cloud and is used to store remote backup data.

Continuous Data Protection (CDP)

Continuous Data Protection (CDP) provides second-level and fine-grained continuous backups for important business systems in VM instances, allowing users to restore VM data to any time state and retrieve files without restoring the system.

CDP Task

You can create a CDP task to continuously back up your VM data to a specified backup storage to achieve continuous data protection and restoration.

CDP Data

The backup data generated from continuous data protection on VM instances is stored in local backup storages.

Scheduled Job

A scheduled job defines that a specific action be implemented at a specified time based on a scheduler.

Scheduler

A scheduler is used to schedule jobs. It is suitable for business scenarios that last for a long time.

Tag

A tag is used to mark resources. You can use a tag to search for and aggregate resources.

Migration Service

The Cloud provides V2V migration service that allows you to migrate VM instances and data from other virtualized platform to the current cloud platform.

V2V Migration

V2V Migration allows you to migrate VM instances from the VMware or KVM platform to the current cloud platform.

V2V Conversion Host

A V2V conversion host is a host in the destination cluster that you need to specify during V2V migration to cache VM instances and data when you implement V2V migration. After the VM instances and data are cached in the V2Vconversion host, they are migrated to the destination primary storage.

User

A user is a natural person that constructs the most basic unit in business management.

Member Group

A member group is a collection of natural persons or a collection of project members. You can use a member group to grant permissions.

Role

A role is a collection of permissions that can be granted to users. A user that assumes a role can call API operations based on the permissions specified by the role. Roles are categorized into system roles and custom roles.

3rd Party Authentication

The 3rd party authentication feature allows you to integrate third-party authentication systems to the Cloud. Then you can use a third-party account to log in to the Cloud and use the resources in the Cloud. You can add an AD or LDAP server to the Cloud.

Project

A project is a task that needs to be accomplished by specific personnel at a specified time. Resources and budgets are also specified for projects. In business management, you can plan resources at the project granularity and allocate an independent resource pool for a project.

Project Member

A project member is a member in a project who is granted permissions on specific project resources and can use the resources to accomplish tasks. Project members include the project admin, project managers, and normal project members.

Process Management

Process management is part of ticket management that manages the processes related to the resources of projects. Processes can be categorized into default processes and custom processes .

My Approvals

In the Cloud, only the administrator and project administrators are granted approval permissions. the administrator and project administrators can approve or reject a ticket. If a ticket is approved, resources are automatically deployed and allocated to the specified project.

Bills

A bill is the expense of resources totaled at a specified time period. Billing is accurate to the second. Bills can be categorized into project bills, department bills, and account bills.

Pricing List

A pricing list is a list of unit prices of different resources. The unit price of a resource is set based on the specification and usage time of the resource.

Console Proxy

Console proxy allows you to log in to a VM instance by using the IP address of a proxy.

AccessKey Management

An AccessKey pair is a security credential that one party authorizes another party to call API operations and access its resources in the Cloud. AccessKey pairs shall be kept confidential.

IP Blocklist/Allowlist

An IP blocklist or allowlist identifies and filters IP addresses that access the Cloud. You can create an IP allowlist or blocklist to improve access control of the Cloud.

Application Center

Application Center allows you to add third-party applications to the Cloud and then access the applications by using the Cloud. It extends the functionality of the Cloud.

Sub-Account Management

A sub-account is created and managed by the admin. Resources created under a sub-account is managed by the sub-account.

Theme and Appearance

You can customize the theme and appearance of the Cloud.

Email Server

If you select Email as the endpoint of an alarm, you need to set an email server. Then alarm messages are sent to the email server.

Log Server

A log server is used to collect logs of the management node. You can add a log server to the cloud and use the collected logs to locate errors and exceptions. This makes your O&M more efficient.

Global Setting

Global Setting allows you to configure settings that take effect on the whole platform.

Scenario Template

Scenario Template provides multiple templates that encapsulate scenario-based global settings . You can apply a template globally with one click based on your business needs. This improves your O&M efficiency.