Maintenance Manual

Version: ZStack 3.10.0

Issue: V3.10.0

ZStack

Copyright Statement

Copyright © 2020 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 System Architecture.....49
3.1 ZStack Functional Architecture..... 49
3.2 ZStack Resource Model.....52
4 Network Configuration.....57
5 Installation and Deployment..... 62
5.1 Prepare Environment..... 62
5.1.1 Network Bonding (Optional).....75
5.2 Install ZStack.....87
5.2.1 ZStack (Enterprise/Community) Management Node..... 90
5.2.2 ZStack Compute Node..... 124
5.2.3 ZStack Expert Mode..... 126
5.3 Manage ZStack..... 128
5.4 Upgrade ZStack..... 129
6 System Login.....137
6.1 UI Login via HTTPS.....139
7 Resource Pool..... 142
7.1 VM Instance..... 142
7.2 Volume.....169
7.3 Image.....176
7.4 Affinity Group.....183
7.5 Instance Offering.....187
7.6 Disk Offering.....189
7.7 GPU Specifications..... 190
7.8 Auto Scaling Group.....190
7.9 Snapshot.....195
8 Hardware..... 197
8.1 Zone.....197
8.2 Cluster..... 199
8.3 Host..... 204
8.3.1 Host Maintenance (Advanced).....209
8.3.1.1 Single Host Maintenance.....209
8.3.1.2 Bulk Host Maintenance.....210
8.3.1.3 Planned Shutdown of Hosts..... 213
8.3.1.4 Host Capacity Expansion.....214
8.3.1.5 Host Replacement.....215
8.3.1.6 Host Reconnection.....215

8.4 Primary Storage..... 216
8.4.1 Shared Block.....219
8.4.2 Primary Storage Maintenance (Advanced).....220
8.4.2.1 Shared Block Maintenance.....220
8.4.2.2 Primary Storage Reconnection.....220
8.5 Backup Storage.....221
8.5.1 ImageStore.....224
8.5.2 Backup Storage Maintenance (Advanced)..... 225
8.5.2.1 ImageStore Maintenance.....225
8.5.2.2 Backup Storage Reconnection..... 226
8.6 SAN Storage..... 226
8.6.1 SAN Storage Maintenance (Advanced).....226
9 Network Resource.....228
9.1 Network Diagram.....228
9.2 L2 Network Resource..... 230
9.2.1 VXLAN Pool..... 230
9.2.2 L2 Network.....232
9.3 L3 Network..... 235
9.4 Flat Network..... 240
9.5 VPC..... 242
9.5.1 VPC vRouter..... 245
9.5.2 VPC Network..... 248
9.5.3 Routing Protocol Resource.....250
10 Network Service..... 252
10.1 Security.....255
10.1.1 VPC Firewall..... 255
10.1.2 Security Group..... 258
10.2 VIP.....260
10.3 EIP.....262
10.4 Port Forwarding.....264
10.5 Load Balancing.....267
10.6 IPsec Tunnel..... 269
10.7 Flow Monitoring.....271
10.7.1 Flow Network..... 271
10.7.2 Port Mirroring..... 272
10.7.3 Netflow..... 272
11 Platform O&M..... 274
11.1 Performance TOP5..... 274
11.2 Performance Analysis..... 277
11.3 Capacity Management..... 277
11.4 ZWatch..... 278
11.5 Notification Service.....280
11.6 Notification Center.....282

11.7 Operation Log....283
11.8 CloudFormation....285
11.8.1 Resource Stack....285
11.8.2 Stack Template....286
11.8.3 Sample Template....286
12 Platform Management....287
12.1 Billing Management....287
12.2 Tag....290
12.3 Application Center....291
12.4 Email Server....291
12.5 Log Server....292
12.6 Console Proxy....292
12.7 IP Blacklist/Whitelist....293
12.8 MN Monitoring....294
12.9 Certificate....295
12.10 Access Key Management....295
13 Advanced Function (Plus)....297
13.1 Enterprise Management....297
13.1.1 Organization....302
13.1.2 User....305
13.1.3 Role....308
13.1.4 Project Management....311
13.1.5 Ticket Management....314
13.1.6 3rd Party Authentication....316
13.2 Bare Metal Management....320
13.2.1 Bare Metal Cluster....322
13.2.2 Deployment Server....323
13.2.3 Bare Metal Chassis....324
13.2.4 Preconfigured Template....327
13.2.5 Bare Metal Instance....330
13.3 Backup Service....335
13.3.1 Backup Task....340
13.3.2 Local Backup Data....343
13.3.3 Local Backup Storage....345
13.3.4 Remote Backup Storage....346
13.4 Migration Service....347
13.4.1 V2V Migration....348
13.4.2 V2V Conversion Host....352
14 MN Maintenance....354
14.1 MN High Availability....354
14.1.1 Multi-MN High Availability....354
14.2 MN Disaster Recovery....356
14.2.1 Preparations....357

14.2.2 MN Disaster Recovery....358
14.3 Change MN IP Address....359
14.3.1 Single-MN Scenario....359
14.3.2 Multi-MN HA Scenario....362
14.4 Switch MN....365
14.5 Upgrade Compute Node to MN....366
15 Basic Maintenance....368
15.1 Installation and Deployment....368
15.2 Start Service....371
15.3 zstack-ctl Commands....372
15.4 zstack-cli Commands....373
15.5 VM Instance Abnormality....374
15.6 Log Analysis....382
15.7 Port Occupation....383
15.8 Network Script....385
15.9 Delete Resource....389
15.10 Detach Resource....392
16 Other Maintenance Scenarios in the Cloud....394
16.1 Configuration Maintenance....394
16.1.1 Upgrading Prometheus....394
16.1.2 zstack.properties Core Configuration File....395
16.1.3 zstack.ui.properties Core Configuration File....400
16.1.4 Changing Password for Hardware Resources in the Cloud....402
16.1.5 Changing Physical Environment in Management Node....402
16.1.6 Database Backup and Recovery....402
16.1.7 Expanding Local Storage Capacity....403
16.1.8 Resizing Root Volume....404
16.2 Upgrading Shared Block Shared Volumes....411
16.3 Changing Time in Ceph Enterprise....411
17 Physical Infrastructure Maintenance....414
17.1 Power Maintenance in Equipment Room....414
17.2 Equipment Room Relocation....415
17.3 Switch Maintenance....415
18 FAQ....418
18.1 Quick Start....418
18.2 Installation and Deployment....420
18.3 System Login....428
18.4 Resource Pool....431
18.5 Hardware....452
18.6 Network....464
18.7 Platform Management O&M....469
18.8 Advanced Function....472

Glossary..... 473

1 Introduction

Production Version

This documentation applies to ZStack 3.10.0.

Intended Audience

This documentation elaborates on the precautions to be taken during the installation and deployment of ZStack 3.10.0, as well as solutions to frequently asked questions in management and maintenance. The intended audiences are as follows:

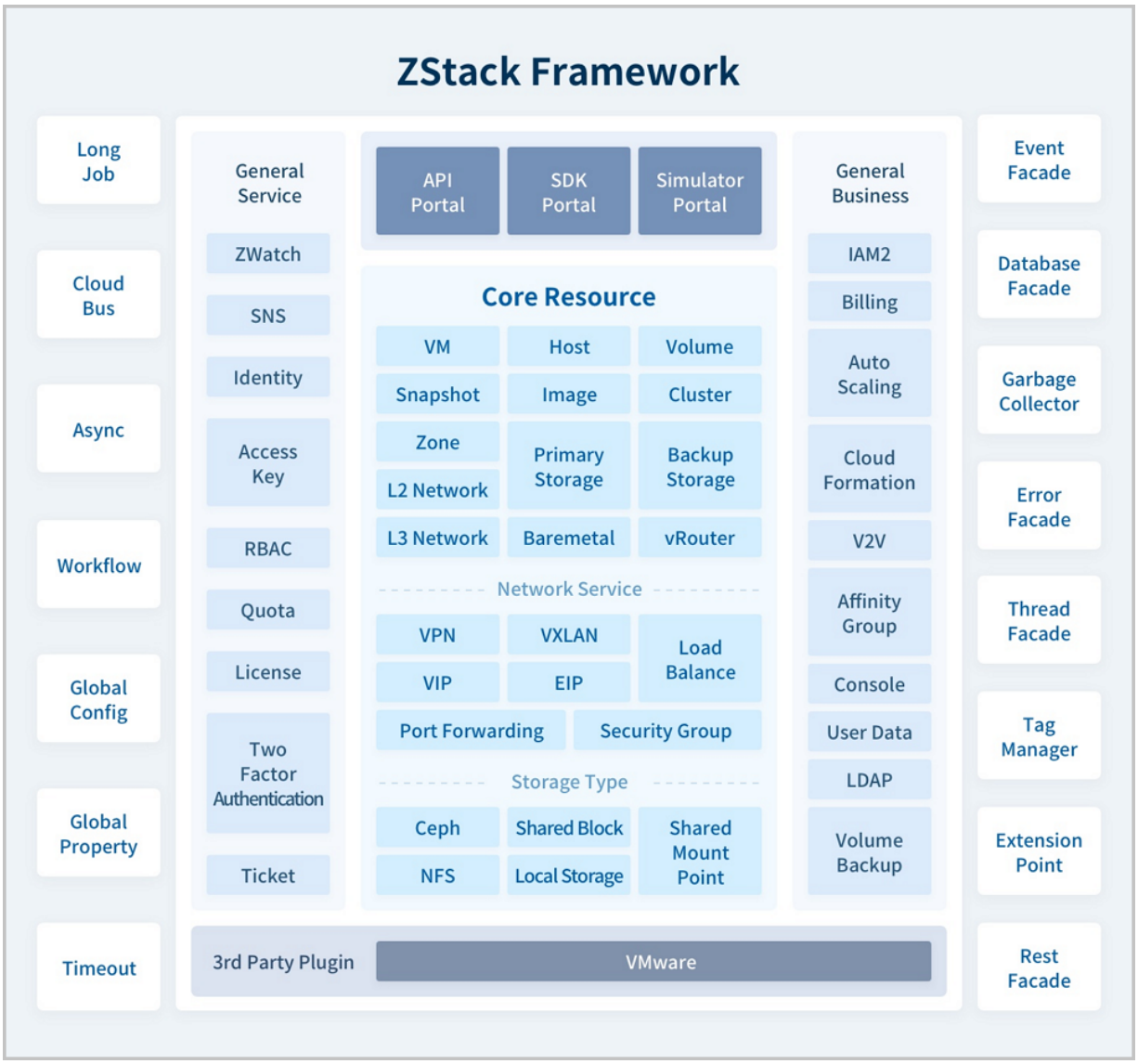
- Deployment and maintenance engineers
- Technical support engineers
- People who are interested in ZStack

2 Overview

Product Overview

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

Figure 2-1: ZStack Framework



Product Features

As a productionized private cloud, ZStack allows you to manage and schedule the compute, storage, network, and other resources in your data center. By using ZStack, you can quickly configure your private cloud environment, create VM instances, allocate volumes, and automatica lly configure the networks of the VM instances.

The following table lists the features of ZStack Enterprise.

Type	Feature	ZStack Enterprise
Zone	Multi-zone management	• Supports multi-zone creation and manipulation. We recommend that you use a zone to manipulate a physical data center. • Supports zone isolation. You can create an independent cluster, primary storage, network, and other resources in a zone.
vCenter	vCenter management	Takes over multiple VMware vCenters via public APIs provided by VMware. In addition, highly compatible with and manipulates a portion of features of VMware vCenter Server to achieve unified managements of multiple virtualization platforms. • Allows you to manipulate vSphere servers, VM instances, volumes, and image resources managed by VMware vCenter Server, and to perform common operations on the manipulated resources in your virtual data center. • Allows you to check VM instances, volumes, images, and other resources by vCenter. • Allows you to manually synchronize all or some vCenter data, ensuring information consistencies. • Allows you to configure vCenter to automatically synchronize data on the global settings. After the setting, the cloud automatically synchronizes all vCenter data periodically.
	vCenter multiple-tenant management	Tenants (normal accounts or project members) can manipulate the resources of the vCenter that you took over. • Tenants can perform common operations on VM instances and volume resources in the vCenter that you took over.

Type	Feature	ZStack Enterprise
		• Tenants can use vCenter networks and image resources shared by administrators. • The home page of the tenant view can display KVM VM utilizations and vCenter VM utilizations, respectively. • The tenant view can display KVM billing information and vCenter billing information, respectively. • Project members can apply for vCenter VM instances via ticket managements.
	vCenter resource pool	• Synchronizes the resource pool information and the related VM information from the vCenter that you took over and displays the information in tier. • Displays the CPU capacity limitations, memory capacity limitations, and other resource quotas.
	ESX VM instance	• Allows you to manage the lifecycle of ESX VM instances, including creating, starting, stopping, rebooting, pausing, resuming, powering off, and deleting an ESX VM instance. • Allows you to perform operations on an ESX VM instance, such as migrating or cloning an ESX VM instance, changing the instance offering for an ESX VM instance, setting the high availability level, opening consoles, and setting a console password.
	Network	• Allows you to create networks according to vSwitches or dvSwitches. • Allows you to create public networks and private networks. Specifically, a private network includes two types of network: flat network and vRouter network. • A vRouter supports all network services, including VIP, EIP, port forwarding, load balancing, and IPsec tunnel.
	Storage	Differentiates primary storages from backup storages according to datastore.
	Image	Allows you to manage the lifecycle of images, such as adding, deleting, enabling, and disabling an image.

Type	Feature	ZStack Enterprise
	Host	Allows you to manage the lifecycle of hosts, such as placing a host in maintenance mode.
	Volume	Allows you to manage the lifecycle of volumes, such as creating, deleting, attaching, and detaching a volume.
	Real-time performance monitoring	Collects data of the ESX VM CPU, memory, storage, and network, and provides a visual, real-time display of these data in the UI.
Cluster	Storage infrastructure	Uses homogeneous storage services within clusters, allows you to attach storage services to the clusters, and provides high availability features for VM instances.
	Host	Supports host managements within a cluster. For a host, provides real-time display of all CPU utilizations, all memory utilization percentages, all inbound and outbound speeds of NICs, and all write or read IOPS.
	VM instance	Supports VM managements within a cluster. For a VM instance, provides real-time display of all CPU utilizations, all memory utilization percentages, all inbound and outbound speeds of NICs, and all write or read IOPS.
	Cluster functionality	• Provides the high availability feature, and defines cluster attributes based on the CPU architecture of a host. • Allows you to appropriately optimize configuration parameters based on your cluster deployment size such as small, medium, and large.
	Network service	• Allows you to attach a VLAN network and a VXLAN network to the same cluster for a unified management, and provides self-service networks (IP pool management and elastic network). • Allows you to specify a migration network for a cluster.
	Distributed resource scheduler (DRS)	Monitors and manages CPUs or memory workloads of hosts by cluster, and offers scheduling suggestions according to the configured scheduling strategies. You can manually migrate VM instances according to

Type	Feature	ZStack Enterprise
		the scheduling suggestions to effectively improve your cloud stability while balancing cluster workloads.
	Advanced settings	Configures parameters for cluster resources by cluster: • Configures parameters for cluster resources, such as memory overcommitment ratios, reserved memories of hosts, CPU overcommitment ratios, and hyper-V switches of VM instances within a cluster. • Provides no corresponding global settings, but allows you to enable the huge page switch, DRS switch, zero copy switch, and other switches for clusters.
Host	Virtualization	Supports KVM and VMware virtualization technologies.
	Custom ISO	ZStack Custom ISO has two versions: c76 ISO and c74 ISO. • c76 ISO is a type of ZStack custom ISO based on an in-depth customization of CentOS 7.6. If you install ISO for the first time, we recommend that you use c76 ISO. • c74 ISO is a type of ZStack custom ISO based on an in-depth customization of CentOS 7.4. If you deployed ZStack by using c74 ISO, use this version to upgrade your cloud.
	Resource overcommitment settings	Allows you to set overcommitment ratios for CPUs, memories, and primary storages to meet different resource usage requirements in cloud environments.
	Nested virtualization	Supports KVM or ESXi nested virtualizations. You can enable CPU hardware virtualization within VM instances.
	Real-time monitoring	Collects data of the host CPU, memory, disk I/O, disk capacity, and associated network, and provides a visual, real-time display of these data in the UI.
	Disable and enable	• Allows you to set host properties for better management.

Type	Feature	ZStack Enterprise
		• After a host is disabled, you cannot create resources on this host. Note that the existing resources on this host are not affected.
	Maintenance mode	• Places a host in maintenance mode, which applies to scenarios such as scheduled O&M operations for hosts. • After a host enters maintenance mode, VM instances that are running on the host will be automatically migrated (shared storage).
	Physical GPU passthrough	Entirely passes through all peripheral devices (GPU graphics cards, GPU sound cards, and other small devices on other GPUs) on physical GPU devices as a group to effectively improve high-performance compute and graphics processing capabilities.
	vGPU	• Allows you to generate vGPUs for both NVIDIA graphics cards and AMD graphics cards at the same time. • Allows you to attach vGPUs to VM instances by either specifying specifications or devices.
	SR-IOV	Generates multiple VF NICs from a physical NIC based on the SR-IOV specification, and allocates these VF NICs to VM instances. This helps to use resources more flexibly, improve resource utilization, and save costs.
	PCI whitelist	Passes through any VT-D device, such as Ali-NPU card, IB card (PCI mode), and FPGA card, to VM instances according to a whitelist.
	USB passthrough	• Directly passes through USB devices to VM instances to cater to application scenarios of multiple USB types. • Supports direct passthrough and transmission passthrough.
	Intel EPT hardware support	Allows you to disable the Intel EPT hardware support to effectively address the problem of VM creation failure due to the CPU models are too old.
	Encrypted password storing	Allows you to store encrypted passwords for hosts.

Type	Feature	ZStack Enterprise
	Operation logs	Displays audit information associated with event login operations when you manage and operate hosts.
	CSV file exporting	Allows you to export host lists in CSV format to facilitate the statistics analysis of your hosts.
VM instance	Batch operation	Manages VM instances in bulk.
	VM instance creation	• Provides multiple strategies to create VM instances to effectively utilize resources. • Allows you to create VM instances through system disk images generated from special data volumes.
	VM lifecycle	Allows you to manage the lifecycle of VM instances , such as creating, stopping, booting, rebooting, powering off, deleting, pausing, and recovering VM instances.
	Online resizing for root volume	Allows you to resize the capacity for a VM root volume online to change VM configurations.
	Online resizing for data volume	Allows you to resize the capacity for a VM data volume online, which will take effect immediately after the resizing.
	VM console	• Allows you to access VM instances through terminals without using remote tools. • Supports three types of console mode: SPICE , VNC, and SPICE+VNC. Specifically, an SSL encryption tunnel is added to the SPICE protocol to further protect your desktop securities. • Allows you to set console passwords and configure the password strategy such as the password complexity and password length. Also, allows you to determine whether to set a password for the VNC console by force.
	VM snapshot	• Allows you to reserve temporarily the state of root volumes or data volumes at a specific time point before you perform important operations. In this regard, you can quickly perform rollback on failures. • Includes two types of snapshot: single snapshot and batch snapshot. Specifically, a batch snapshot can be recovered in bulk as a group.

Type	Feature	ZStack Enterprise
		• Takes snapshots for VM instances that are in the running state (ImageStore and Ceph backup storages are supported). • Takes snapshots for VM instances that are in the stopped state (ImageStore, SFTP, and Ceph backup storages are supported). • Automatically boots VM instances after restoring from snapshots. • Allows you to delete VM snapshots in bulk.
	CPU binding	Binds a logical CPU of a VM instance to a physical CPU of a compute node.
	Online password changing	Allows you to change passwords online for Windows or Linux VM instances.
	Online image creation	Allows you to create images online for running VM instances.
	QGA switch	Flexibly controls and manages the state of the QEMU guest agent.
	RDP mode switch	For a VDI UI, opens consoles in RDP mode by default after the RDP switch is enabled.
	Graphics card changing	Provides multiple VM graphics card types, including QXL, Cirrus, and VGA.
	Graphics card passthrough	Passes through a NVIDIA GPU device or an AMD GPU device directly to a VM instance.
	User data importing	Allows you to import user data when you create a VM instance.
	VM cloning without data volume	• Quickly creates multiple VM instances by cloning a VM instance. • Clones a VM instance that is in the running state (ImageStore and Ceph backup storages are supported). • Clones a VM instance that is in the stopped state (ImageStore and Ceph backup storages are supported).
	VM cloning with data volume	• Clones both root volumes and data volumes of VM instances. If a VM instance has shared volumes

Type	Feature	ZStack Enterprise
		attached, the data volumes of the VM instance cannot be cloned with the VM instance. • Supports only ImageStore backup storages. • For LocalStorage, NFS, SMP, Ceph, and Shared Block primary storages, allows you to clone VM instances that are running, paused, or stopped.
	Operating system changing	Allows you to change the operating system for a VM instance that is in the stopped state.
	VM resetting	Resets VM instances to their initial image state, and overwrites all data in root volumes.
	Root volume resizing	Allows you to resize a root volume of a VM instance that is running or stopped to change VM configurations .
	ISO-based deployment	• Deploys VM instances based on ISO system disk to instruct you to install the operating system. • Allows you attach multiple ISO images to the same VM instance to improve business deployment efficiencies.
	Template-based deployment	Creates VM instances based on system templates.
	BIOS mode	• Inherits the chosen BIOS mode when you create a VM instance. The BIOS mode includes Legacy and UEFI. • Inherits the BIOS mode of the original image when you create a VM image or clone a VM instance. • Allows you to dynamically change the BIOS mode on the VM details page.
	VM image creation	Makes a template image based on the current VM instance so that you can create VM instances in bulk in a custom manner. • Allows you to create an image for a VM instance that is in the running state (ImageStore and Ceph backup storages are supported). • Allows you to create an image for a VM instance that is in the stopped state (ImageStore, SFTP, and Ceph backup storages are supported).

Type	Feature	ZStack Enterprise
	Custom MAC	• Allows you to specify an MAC address when you create a VM instance. • Allows you to change the MAC address for existing VM instances.
	VM boot order	Adjusts VM boot orders to change the ISO boot mode . Currently, the following boot devices are supported: CD-ROM, hard disk, and network.
	Dynamically attaching or detaching volume	Allows you to dynamically attach a volume to or detach a volume from a VM instance, to optimize drive models, and to identify a volume by its SCSI WWN.
	Dynamically attaching or detaching NIC	Allows you to dynamically attach a NIC to or detach a NIC from a VM instance, and to set the default NIC.
	Dynamically attaching or detaching virtual drive	Allows you to dynamically attach a virtual drive to or detach a virtual drive from a VM instance, and attach ISOs to or detach ISOs from each virtual drive. This will meet your needs, enhance the flexibilities, and improve the user experience.
	Attaching GPU card	Allows you to attach a GPU device when you create a VM instance.
	Shared volume	For Ceph and Shared Block primary storages, multiple VM instances can share the same data volume.
	Real-time performanc e monitoring	Displays VM workloads in real time for popular systems, such as Linux, Windows, and Chinese domestic operating systems. • External monitoring: Collects VM data, such as the VM CPU, memory, disk I/O, and network by using libvirt, and provides a visual display of these data in the UI. • Internal monitoring: Collects VM data, such as the VM CPU, memory, and disk capacity by using an agent, and provide a visual display of these data in the UI. Note that you can manually install the agent by using a performance optimization tool (guest tool).

Type	Feature	ZStack Enterprise
	High availability(HA)	Automatically reboots a VM instance if its host encounters failures, and displays the rebooting process in the UI.
	Online changing for VM CPU or memory	Changes CPU or memory configurations online without rebooting a VM instance.
	Real-time update of volume QoS and network QoS	Allows you to set QoS for the root volume and NIC of a VM instance, avoiding that a single VM instance occupies too many resources.
	SSH key injection	• Allows you to perform SSH key injection for VM instances in both Linux and BSD operating systems . • Allows you to create or delete a key for a VM instance. • Disables VyOS SSH login authentication by default to improve the cloud security.
	Custom instance offering	Allows you to customize an instance offering to meet the resource consumption requirements.
	Custom tag	Allows you to customize tags to meet the querying and compiling scheduler tasks.
	Custom VM list	Allows you to either customize display items of a VM list or to export the VM list in CSV format.
	Resource deleting protection	Moves deleted VM instances to a recycle bin, allowing you to recover or completely delete the VM instances as needed.
	Cold migration	• Allows you to migrate a VM instance that is attached to a local storage when the VM instance is in the stopped state. • Allows you migrate a VM instance or volume according to the workload of the destination compute node.
	Online migration	• Allows you to migrate online VM instances that are attached to a primary storage. • Allows you to migrate a VM instance or volume according to the workload of the destination compute node.

Type	Feature	ZStack Enterprise
		• Provides specific support for Windows failover clusters. Hot migration of VM instances will not have any adverse effects.
	Storage migration	• Supports cold migration of VM instances across primary storages of the same type in the Cloud. — You can cold migrate a VM instance across multiple NFS primary storages without migrating the attached volumes. — You can cold migrate a VM instance across multiple Ceph primary storages without migrating the attached volumes. — You can cold migrate a VM instance as well as its attached volumes (except for shared volumes) across multiple Shared Block primary storages. • Supports hot migration (without snapshots) of VM instances across multiple primary storages of different types. For example, migration between Ceph primary storage and Shared Block primary storage, between LocalStorage primary storage and Shared Block primary storage, and between LocalStorage primary storage and Ceph primary storage. • Displays the original data reserved during storage migrations in the UI, and allows you to clean up the data. You can manually clean up the data to release storage space after verifying that the data is complete and intact.
	Cross-cluster HA policy	Allows you to configure a cross-cluster HA policy for a VM instance or VPC vRouter. Then, the VM instance or VPC vRouter will be stuck to the cluster to which the VM instance or VPC vRouter belongs when the policy takes effect.
	Operation logs	Displays audit information that is associated to an operation process event and a login operation of a VM instance.
	Guest tools	• Provides guest tools for Windows and Windows Virtio operating systems, and supports one-click installation of Virtio drive, agent, and QGA.

Type	Feature	ZStack Enterprise
		• Provides guest tools for Linux operating systems , and allows you to install agents. After you install the agents successfully, you can obtain internal monitoring data from VM instances.
	USB redirection	Redirects a USB device on a VDI client to a VM instance.
	CSV file exporting	Allows you to export a VM list in CSV format, which facilitates statistics analysis.
	Anti-spoofing	• Allows you to set the anti-spoofing switch for a VM instance on the global settings to improve the cloud security. • Allows you to set the anti-spoofing switch for a single VM instance to increase flexibilities.
	VM priority	• Provides two types of VM priority: normal and high. When resources contend with each other, VM instances with the **High** resource priority will be prioritized than those with the **Normal** resource priority. • Improves the resource priority of a VPC vRouter by default to ensure that resources of the VPC vRouter will be higher than those of a VM instance.
	VM multi-gateway	Allows you to enable multi-gateway by running `zstack-cli`. After enabled, each NIC has an independent gateway.
	NIC multiqueue	Allows you to set the number of queues when Virtio NIC traffics are allocated to multiple CPUs. This helps to improve the NIC performance.
	Setting VM NIC model	Allows you to set the NIC model for Linux and Paravirtualization VM instances. Supported NIC models include Virtio, E1000, and RTL8139.
	Setting hostname or password	• Allows you to log in to the Cloud via SSH. When you create a VM instance, you can set a hostname or password on the UI through simple operations, thereby improving user experiences. • Allows you to configure the password strategy such as the password complexity and password length

Type	Feature	ZStack Enterprise
		. Also, allows you to determine whether to set the root password for a VM instance by force.
	Advanced settings	Allows you to configure parameters for VM resources by VM instance. • Configures VM parameters independently, such as the NUMA and hyper-V switches of VM instances. • Provides no corresponding global settings, but allows you to configure VM parameters, such as the NIC multiqueue number, by VM instance.
Auto scaling group	Lifecycle management	Allows you to manipulate the lifecycle of auto scaling groups, including creating, enabling, disabling, and deleting an auto scaling group.
	Health check	Allows you to customize the health check method, health check time, and health check grace period.
	Auto scaling policy	• Supports scale-out policy by which you can customize a trigger metric, trigger condition, duration, cooldown time, and the number of VM instances to be added each time. • Supports scale-in policy by which you can customize a trigger metric, trigger condition, duration, cooldown time, removal policy, and the number of VM instances to be removed each time. • After a scaling policy is triggered, automatica lly adds or removes a specified number of VM instances according to the scaling policy. • Determines the monitoring conditions based on the VM CPU usage and memory usage, and then triggers auto scaling (scaling in or scaling out) accordingly. Note that you can choose external or internal (recommended) monitoring data.
	Notification	• Allows you to view scaling records. • Allows you to select whether to receive notifications of scaling activities. • Sends notifications of scaling activities via ZWatch and cloud messages.
Volume	Batch operation	Manipulates volumes in bulk.

Type	Feature	ZStack Enterprise
	Volume management	• Allows you to manipulate the lifecycle of volumes, including creating, enabling, disabling, attaching, detaching, and deleting a volume. • Allows you to perform common operations on a volume, including migrating the volume, creating a snapshot, creating a volume image, resizing the volume, changing the volume owner, and migrating the volume storage. • Allows you to create shared volumes based on Ceph storages or Shared Block primary storages. Multiple VM instances can share and use the same data volume. • Allows you to create shared volumes by using disk offerings or volume images.
	Volume snapshot	• Allows you to create a snapshot for a volume when the volume is in use. • Allows you to delete volume snapshots in bulk.
Snapshot	Unified snapshot management	Uniformly manages VM snapshots and volume snapshots. All VM instances or volumes that have snapshots will be displayed on the snapshot management page. In addition, the VM instances or volumes can be sorted by the number of the snapshots or total capacities to improve O&M efficiencies. Doing so can help you to quickly identify snapshots that need to be cleared.
	Batch snapshot	• Allows you to create batch snapshots for VM instances and the attached volumes. You can restore a VM instance and its attached snapshots by recovering the batch snapshot of the VM instance. • Allows you to unbind a batch snapshot and recover the batch snapshot to a single snapshot.
Disk offering	Disk offering management	• Allows you to create, enable, disable, delete a disk offering, share a disk offering globally, recall a disk offering globally, and set QoS for a disk offering. • Allows you to classify different types of data volumes via advanced parameters for independen t billing or display. The supported types of primary

Type	Feature	ZStack Enterprise
		storages include Ceph, LocalStorage, NFS, and SharedBlock.
	QoS setting	Allows you to set QoS for a volume by configuring the total bandwidth or read/write bandwidth when you create a disk offering.
Instance offering	Instance offering management	• Allows you to create, enable, disable, delete an instance offering, share an instance offering globally, recall an instance offering globally, and set the disk QoS and network QoS for an instance offering. • Allows you to select the host allocation strategy, including host with minimum number of running VMs, host with minimum CPU utilization, host with minimum memory utilization, host with maximum number of running VMs, host where the VM is located last time, and random host allocation to create VM instances. • When the host allocation strategy is the host with minimum CPU utilization or host with minimum memory utilization, you can select the mandatory strategy mode or non-mandatory strategy mode. • Allows you to classify different types of root volumes via advanced parameters for independen t billing or display. The supported types of primary storages include Ceph, LocalStorage, NFS, and SharedBlock.
GPU specification	GPU specification	• Automatically detects available physical GPU specifications and vGPU specifications on the Cloud and then manages both specifications in a unified way. When you create a VM instance, you can add a GPU device for the VM instance by specifying a GPU specification. • If you attached a GPU device to a VM instance by using a GPU specification, you can configure the advanced setting to uninstall the GPU device automatically after the VM instance is stopped.
Image management	System template	Supports system templates, including qcow2 and raw formats, and automatically matches image types.

Type	Feature	ZStack Enterprise
	ISO image	Guides a VM instance to install an operating system via an ISO image.
	BIOS mode	• Provides two types of BIOS mode, including Legacy and UEFI, to add an image. • Inherits the BIOS mode of the original image when you create a VM instance, a VM image, or clone a VM instance.
	System image uploading	Allows you to upload a system image by using a URL or a local browser.
	Volume image uploading	Allows you to upload a volume image by using a URL or a local browser.
	Image migration	Allows you to migrate images on a Ceph primary storage across multiple storage devices.
ImageStore	Image storing	Stores image data, including ISO and system template .
	Exporting image	• Exports an image URL. • Provides MD5 checksum for exported images. You can check the MD5 checksum on the details page of an exported image to verify the integrity of the downloaded image.
	Obtaining existing image	When you add an ImageStore backup storage, you can obtain the existing image file under the URL of the backup storage.
	Image synchronization	• Supports image transmissions among ImageStore s. Note that the image transmissions can be completed across multiple zones. • Supports image synchronization among different ImageStores in the same management node.
	ImageStore cleaning	Visually cleans up the expunged invalid data in a backup storage to release storage spaces.
	Standard system image	Supports Windows, Red Hat, Ubuntu, and other open source Linux operating systems.
	Running image preset	Supports the following software operating environments:

Type	Feature	ZStack Enterprise
		• Windows IIS and Dot Net Framework operating environments • Linux Tomcat, JAVA, Apache Web, Jboss, PHP, Node JS, Golang, Python, and other languages or operating environments • Oracle, MySQL, Postgres, Mongodb, Influxdb, Cassandra, Redis, and other database services • A wide range of application middlewares
	Application image preconfiguration	Supports the following application systems: • Commonly used application systems, such as BBS , SNS, blog, and the twitter-like Weibo • Multiple O&M management applications, such as phpmyadmin • Multiple application images provided by vendors
	Custom image	Allows administrators to store image files with the incremental method and realize the duplication feature intelligently by customizing images that are suitable for the operating environments of self business systems according to the standard system image and the preconfigured running image.
	Primary storage support	Seamlessly supports primary storages of the LocalStorage, NFS, SMP, Ceph, Shared Block types.
Storage management	LocalStorage primary storage	• Allows you to store your volumes to local hosts. • Provides real-time display of used capacity percentages of the LocalStorage primary storage. • Allows you to set the volume allocation policy, including thick provisioning and thin provisioning.
	NFS primary storage	• Allows you to store your volumes to NFS protocol storage through which hosts can intercommunicate. • Allows you to specify a storage network, and supports network isolation between the storage network and the management network to improve high availability of VM instances. • Provides real-time display of used capacity percentages of the NFS primary storage.

Type	Feature	ZStack Enterprise
	Shared Mount Point primary storage	• Allows you to store your volumes to shared storages that are compatible with POSIX, and supports iSCSI and FC storage. • Allows you to specify a storage network, and supports network isolation between the storage network and the management network to improve high availability of VM instances. • Provides real-time display of used capacity percentages of the Shared Mount Point primary storage.
	Shared Block primary storage	• Allows you to add an iSCSI or FC protocol storage through which hosts can intercommunicate. • Allows you to add an iSCSI storage, to automatica lly scan and discover disks online, and to automatically configure iSCSI. • Supports shared volumes. • Allows you to add multiple LUN devices. • Displays a candidate list of LUN devices when you add Shared Block primary storage. • Allows you to set the provisioning method, including thin provisioning and thick provisioning, when you create VM instances or volumes by using Shared Block primary storage. • Supports FC SAN passthrough, provides direct display of passthrough FC storages, and allows you to attach the passthrough LUN devices to VM instances. • Supports iSCSI passthrough. The passthroug h LUN devices can be directly attached to VM instances. • Allows you to clean up VG data when you add Shared Block primary storage. • Allows you to specify a storage network, and supports network isolation between the storage network and the management network to improve high availability of VM instances. • Provides real-time display of used capacity percentages of the Shared Block primary storage.

Type	Feature	ZStack Enterprise
	Ceph primary storage	• Supports shared volumes. • Allows you to specify disk volumes with different performances when you create volumes. • Allows you to store your volumes to Ceph distributed storages. • Supports cold migration for data. • Allows you to specify a storage network, and supports network isolation between the storage network and the management network to improve high availability of VM instances. • Allows you to create a Ceph pool, to calculate capacities via the pool, and to set the display name. • Supports LUN device clearing. You can force to clear file systems, RAID, or signatures of partition tables. • Resizes a Ceph primary storage by adding a pool, and allows you to specify a pool when you create a VM instance or volume. • Provides real-time display of used capacity percentages of the Ceph primary storage. • Provides expiration notifications of storage license services and collaborates with Ceph ZStack Enterprise.
	Multiple primary storage support	• The same cluster can attach multiple LocalStorage primary storages. • The same cluster can attach multiple NFS primary storages. • The same cluster can attach multiple Shared Block primary storages. • The same cluster can attach one LocalStorage primary storage and one NFS, SMP, or Shared Block primary storage. • The same cluster can attach one Ceph primary storage and multiple Shared Block primary storages.
Network management	VLAN L2 isolation	Uses VLAN 802.1q for network isolation.
	VXLAN network	• Supports VXLAN networks to effectively address the shortage of logical network segments in the

Type	Feature	ZStack Enterprise
		cloud data center and MAC flooding of a upper layer switch. • Allows you to change a VNI name. Specifically, you can either customize the VNI name that you created before or enter a VNI name when you create a VNI range.
	Hardware VXLAN network	Takes over SDN networks of hardware switches to the Cloud by adding SDN controller. This helps to lower network latencies and improve VXLAN network performances.
	Distributed flat network	• Provides three types of IP address: IPv4, IPv6, and double stack (IPv4+IPv6), three of which can be selected for a flat network as required. • Allows a VM instance to use an actual network IP address. • Provides multiple network services: security group, VIP in private flat networks, EIP, and intranet load balancing.
	Distributed elastic network	Allows a VM instance to use a virtual network address which can map a real network.
	Distributed DHCP service	• Allows a VM instance to automatically obtain the allocated IP address. • Allows you to specify an IP address for the DHCP service to avoid IP conflicts during your network planning when you create an L3 network.
	Network address space reservation	Reserves network address spaces to couple with physical networks.
	Dynamic and static IP allocation	Not only allows you to dynamically allocate an IP address, but also allows you to specify an IP address.
	Multi-level network management	A VM instance can connect to multiple networks to build businesses of complex scenarios.
	VIP QoS setting	Limits QoS for a VIP to achieve effective allocation managements of network services.
	MTU	Customizes the limit of network packets.
	Custom gateway	• Allows you to specify a gateway when you add a network range by using an IP range.

Type	Feature	ZStack Enterprise
		• Allows you to specify a gateway when you add a network range by using a CIDR, and uses the first or the last address of the CIDR as the gateway.
	VPC vRouter	• Allows you to manipulate the lifecycle of VPC vRouters, such as creating, deleting, starting, stopping, and rebooting a VPC vRouter. • Allows you to perform common operations on a VPC vRouter, including migrating a VPC vRouter, attaching or detaching a VPC network, and setting east-west traffics. • Supports all network services. • Allows you to uniformly set DNS on a VPC vRouter. • Allows you to enable or disable the SNAT network service in a custom manner. • Supports the OSPF dynamic routing protocol. • Supports the multicast feature. You can forward multicast messages sent by a multicast source to a VM instance. • Supports the advanced feature of a distributed routing to optimize east-west traffics. • Specifies a default IP address when you create a single VPC vRouter. • By default, the resource priority of a VPC vRouter is higher than that of a normal VM instance. When resources contend with each other on hosts, a VPC vRouter has higher resource grabbing capability. • Allows you to attach multiple public networks to a VPC vRouter, to specify a default route, and to configure the source-in and source-out policy. • Allows you to set QoS for the public network interface and VPC network interface for a VPC vRouter to achieve more granular network traffic controls.
	Firewall	• Allows you to configure a firewall for a VPC vRouter . Specifically, after you create a VPC firewall, the system will automatically configure an inbound rule set for the VPC vRouter. In addition, you can flexibly configure an outbound rule set for the VPC vRouter.

Type	Feature	ZStack Enterprise
		• Each interface direction of a VPC vRouter is allowed to use a rule set. In addition, the south -north traffics of the interface will be filtered to effectively protect the communication security of the entire VPC and the security of the VPC vRouter . • By default, the inbound direction of a VPC vRouter NIC will bind one rule set. • Allows you to add a firewall rule via an IP address, IP range, and CIDR. In addition, multiple IP formats are supported to simplify the rule configurations, thus improving the feature usability. • Allows you to select whether to take effect a firewall rule immediately.
	VPC vRouter HA group	• Supports the high availability feature of a VPC vRouter. Specifically, a pair of VPC vRouters with the active-backup mode are deployed within a VPC vRouter HA group. • When the active VPC vRouter is abnormal, the high availability will be triggered in seconds to ensure your business continuity, and the active VPC vRouter will be automatically switched to the backup VPC vRouter. • Allows you to specify a VIP when you create a VPC vRouter HA group.
	VPC network	• Supports three types of IP address: IPv4, IPv6, and double stack (IPv4+IPv6), three of which can be selected for a VPC network as required. • Allows you to create or delete a VPC network, add a network range, and attach or detach a VPC vRouter. • A VPC network supports multiple network services, including security group, VIP, EIP, port forwarding, and load balancing. • Load balancing supports TCP, HTTP, HTTPS, or UDP protocol. • TUI supports real-time traffic monitoring of a load balancer.

Type	Feature	ZStack Enterprise
	Public network	• Supports three types of IP address: IPv4, IPv6, and double stack (IPv4+IPv6), three of which can be selected for a public network as required. • Allows you to create a VM instance. • Provides VIPs for network services. • Provides two types of IP address type: IPv4 and IPv6. • Supports IP address pools. An IPv4 public network lets you add an IP address pool based on the common IP range. The IP address pool can be used to create VIPs and provide various network services based on a VPC network.
	System network	Acts as a management network, storage network, and migration network.
	vRouter network	• A vRouter supports multiple network services, including security group, VIP, EIP, port forwarding, and load balancing. • Load balancing supports TCP, HTTP, HTTPS, or UDP protocol. • TUI supports real-time traffic monitoring of a load balancer. • Supports the IPsec tunnel service based on a vRouter. • Allows you to associate multiple EIPs to one VM NIC. • Allows one vRouter to connect to multiple public networks. • Allows you to configure a static routing table. • Supports distributed DHCP to improve service performances.
	Network diagram	• Displays the global network diagram of your cloud, and supports highlighting display of a resource. • Allows you to select the resources that you need to display their network diagram in a custom manner.
	Load balancing	• Supports the following load balancing network services:

Type	Feature	ZStack Enterprise
		— Internet load balancing: Uses a public network as the frontend network to provide Internet-facing load balancing services through routers (VPC vRouters or vRouters). — Intranet load balancing (VPC private network): Uses a VPC network as the frontend network to provide intranet load balancing services through VPC vRouters. — Intranet load balancing (flat network): Uses a flat network as the frontend network to provide intranet load balancing services through vRouters. • The load balancing service supports four types of protocols: TCP, HTTP, HTTPS, and UDP. The health check protocol can be TCP, UDP, or HTTP. • Supported load balancing algorithms: round robin , least number of connections, source hashing scheduling, weighted round robin. • You can use zstack-cli commands to configure blacklist and whitelist for listeners to control IP access, prevent malicious attacks, and improve system security.
	Netflow	• A VPC vRouter has a new added network service , namely Netflow. You can analyze and monitor inbound and outbound traffics of a VPC vRouter NIC by using Netflow. • Supports two types of data flow output format, including Netflow V5 and Netflow V9.
	IP statistics	• Allows you to check the IP utilization of an L3 network (private network, public network, and VPC network) in the UI. • On the IP statistics details page of an L3 network , you can quickly check used IP addresses, associated resources, and unused IP addresses.
	Port mirroring	• Analyzes the obtained business messages via port mirroring to facilitate your monitoring and management of internal enterprise network data and to quickly locate network failures.

Type	Feature	ZStack Enterprise
		• Allows you to configure independent traffic networks which can be used by port mirroring to transfer data.
Scheduled job	Scheduled subject	Provides scheduling operations on VM instances and volumes.
	Scheduling operations	• Allows you to create scheduled jobs to stop or reboot a VM instance, and to create volume snapshots. • When you create a scheduled job for VM instances or volume snapshots, allows you to set the number of snapshots to be reserved if all VM instances or volumes that you selected use a Ceph primary storage.
CloudFormation	Resource stack	• Allows you to create a resource stack online or by using a template. • Allows you to preview or check resource contents, and to inject user data into a VM instance. • Allows you to delete resource stacks and cascade the delete operation on all resources in a resource stack.
	Custom template	Allows you to create a resource stack template by using a designer or by uploading a local file, and to create, check, change, delete, and preview a stack template.
	Sample template	The resource stack template sample that is provided by the Cloud by default can be used as a reference template.
	Visual resource scheduling	• Allows you to create a resource stack template by dragging and dropping resources. • Allows you to review templates, generate resource stacks, and save as resources templates. • Allows you to undo, redo, delete, and clear canvas.
Security management	L3 security policy	Supports security policies based on TCP or UDP port.
	Unified management of security group	• Allows a security group to uniformly manage VM security policies to achieve intercommunication within the security group. Specifically, a security

Type	Feature	ZStack Enterprise
		policy can be applied to all resources within the same security group. • Allows you to enable and disable a security group.
Performance TOP5 and performance analysis	Performance TOP5	• Sorts multiple resources, including host, VM instance, vRouter, VIP, and L3 network in sequence, and allows you to customize data source display at different periods. • Allows you to switch data sources, including external monitoring and internal monitoring. For internal monitoring, you need to install an agent.
	VM performance analysis	• Allows you to customize data source display at different periods, to specify a resource range, and to specify an owner range. By using the filter, analyzes and sorts VM CPU utilization, memory utilization, disk read speed, disk write speed, NIC in speed, NIC out speed, NIC in packets, NIC out packets, NIC in errors, and NIC out errors. • Allows you to switch data sources, including external monitoring and internal monitoring. For internal monitoring, you need to install an agent.
	Router performance analysis	• Allows you to customize data source display at different periods, to specify a resource range, and to specify an owner range. By using the filter, analyzes and sorts router CPU utilization, memory utilization, disk read speed, disk write speed, NIC in speed, NIC out speed, NIC in packets, NIC out packets, NIC in errors, and NIC out errors. • Allows you to switch data sources, including external monitoring and internal monitoring. For internal monitoring, you need to install an agent.
	Host performance analysis	Allows you to customize data source display at different periods, and to specify a resource range. By using the filter, analyzes and sorts host CPU utilization, memory utilization, disk read speed, disk write speed, disk used capacity, disk read IOPS, disk write IOPS, disk used capacity in percent, NIC in speed, NIC out speed, NIC in packets, NIC out packets, NIC in errors, and NIC out errors.

Type	Feature	ZStack Enterprise
	L3 network performance analysis	Allows you to customize data source display at different periods, and to specify a resource range. By using the filter, analyzes and sorts used IP count, used IP in percent, available IP count, and available IP in percent.
	VIP performance analysis	Allows you to customize data source display at different periods, to specify resource range, and to specify owner range. By using the filter, analyzes and sorts VIP inbound traffic in bytes, inbound traffic in packages, outbound traffic in bytes, and outbound traffic in packages.
	Backup storage performance analysis	Allows you to customize data source display at different periods, and to specify a resource range. By using the filter, analyzes and sorts available backup storage capacity in percent.
Capacity management	Capacity management	Intuitively displays the capacity information about core resources in the Cloud. • Displays detailed capacity information of various core resources in the form of cards. • Displays Top10 resources according to their resource capacity so that you can better control the resource usage in the Cloud and improve the management and maintenance efficiency.
ZWatch	Host monitoring	Provides real-time monitoring of running hosts, and displays sequential diagram for monitoring CPU, memory, disk, and network.
	VM monitoring	Provides real-time monitoring of running VM instances , and displays a sequential diagram for monitoring CPU, memory, disk, and network.
	Monitoring	• Monitors the system metric data, such as the VM memory utilization and host CPU utilization. • Monitors system events, such as the VM state event and host disconnection event. • Allows you to check the visual diagram of host workloads according to different periods of time on the main page.

Type	Feature	ZStack Enterprise
	Alarm	• Provides resourceful metric items so that you can monitor and create alarms for the following resources and events: — Resources: VM instance, Bare Metal instance , router, image, backup storage, system data directory, host, L3 network, volume, VIP, primary storage, load balancer listener, and project resource. — Events: VM instance, router, backup storage , management node, host, primary storage, vCenter, backup task, and project resource. • Sets alarms for time-series data and events, and receives alarm messages via SNS notification, such as email, DingTalk, HTTP application, Aliyun short message, and Microsoft Teams. • Provides commonly used, default alarms to monitor states of basic resources in real time. • Selects the monitoring range as needed, and allows you to monitor a single resource or all resources of a monitoring object. • Converges ZWatch alarm messages, and adjusts the event alarm message policy to notify you once. Adds the **Once** option to the alarm period type for resource alarms. Specifically, you can flexibly configure an alarm policy as needed. • Displays the read status of ZWatch alarm messages. You can quickly locate problems to improve O&M efficiencies via the notifications. • Sends notifications after ZWatch alarm recovers. • Allows you to view alarm messages in Chinese or English as needed. This improves the readabilit y and understandability and helps quickly locate problems. • Allows you to select an emergency level for resource alarms and event alarms. Different emergency levels of alarms will send out the corresponding emergency levels of alarm messages. In this regard, you can classify and check alarms as needed to improve O&M efficienci es.

Type	Feature	ZStack Enterprise
	Multiple endpoints	• Supports multiple endpoints, including email, DingTalk, HTTP application, Aliyun short message, and Microsoft Teams. • Allows you to add multiple endpoint addresses to email endpoints and Aliyun short message endpoints.
	SNS text template	Endpoints such as email, DingTalk, Aliyun short message, and Microsoft Teams let you customize the SNS text template to facilitate your configurat ions as required and improve the readability of alarm messages.
	3rd-party alarm message integration	• Allows you to connect with 3rd-party message sources, take over 3rd-party alarm messages, and uniformly push these messages, whereby achieving unified managements and enhancing operation and maintenance efficiencies for alarm messages. • Allows you to create 3rd-party alarms and push 3rd -party alarm messages via various endpoints.
Audit	Resource audit	• Supports audit queries for all resources. You can audit all operation behaviors of a resource to effectively protect your core data security in the Cloud. • Allows you to check call API name, time consumed , task result, operator, creation time, completion time, and message details of API actions. In addition, allows you to export the preceding information with the CSV format.
Operation log	Operation log	• Displays the operation description, task result, operator, login IP, creation time, completion date , and message details of operations responses . In this regard, you can achieve fine-grained managements for resources and can export the operation information with the CSV format. • Allows you to configure log reservation time as needed. • Displays event audits and login audits of performed operations.

Type	Feature	ZStack Enterprise
		• Global settings allows you to set log reservatio n time of a management node and reservation capacities as needed.
Account management	Account and user management	The account management feature includes account and user. Specifically, an account is a resource billing group, while a user can define operation permissions.
	AD/LDAP account	• Allows you to add an AD or LDAP account, and to bind regular accounts. • Allows you to clean binding filters in a custom manner.
	Account resource quota	Allows you to allocate the largest amount of available resources to an account in a custom manner, including the number of running VM instances, CPU, memory, volume count, total capacity of a volume, image count , total capacity of an image, and EIP count.
	Permission allocation of user group	Supports permission allocation of a user group to uniformly manipulate user permissions.
	Permission allocation of user	Allows you to allocate permissions for users.
	Changing VM owner	Allows you to change a VM owner and specify an account where the VM instance belongs.
	Changing volume owner	Allows you to change volume owner, and to specify the account where the volume belongs.
	Specified allocation of instance offering	Allows you to share an instance offering to others. Specifically, you can specify whether an account can use the instance offering.
	Specified allocation of image resource	Allows you to share an image resource. Specifically , you can specify whether an account can use the image resource.
	Specified allocation of disk offering	Allows you to share a disk offering. Specifically, you can specify whether an account can use the disk offering.
	Specified allocation of network resource	Allows you to share an L2 network resource and an L3 network resource. Specifically, you can specify

Type	Feature	ZStack Enterprise
		whether an account can use the L2 network resource and the L3 network resource.
	Global settings	Allows you to directly perform global settings on various properties in the UI. • Each global setting has one default value. You can restore a default settings with one click. • If you want to update global settings, do not need to restart your management node. • Supports templates, and provides one-click template settings in the global settings according to your real production scenarios. This will quickly set the Cloud to meet your requirements, which can improve O&M inefficiencies.
	Changing password for admin account	If you forget the login password of an administrator, run `zstack-ctl reset_password` to restore the default setting.
Billing	Custom pricing list	• Each resource pricing unit will be integrated as one pricing list to provide the billing experience of a quasi public cloud. The supported billing resource type includes CPU, memory, root volume, data volume, GPU device, public IP (flat network), and public IP (VIP). • A pricing unit includes second, minute, hour, day, week, and month (30 days). • The pricing unit that can be dynamically adjusted can meet the need of periodical promotions.
	Billing method	• Provides quasi-public cloud billings, and covers a diversity of typical usage scenarios such as multi-unit, disk-based, and public IP billings. • Supports project-based or account-based billings for each resource. Different pricing lists can be used to customize different pricing strategies for different projects and accounts. • Allows you to enable or disable the billing feature as required.
	Disk performance-based pricing	Allows you to set different pricing units independently for different types of disks.

Type	Feature	ZStack Enterprise
	Billing currency symbol	Allows you to set a billing currency symbol on the global settings. Supported currencies: CNY (￥), USD ($), EUR (€), GBP (£), AUD (A$), HKD (HK$), JPY (¥), CHF (CHF), and CAD (C$).
	Bills	Calculates and displays resource expense information of an administrator and all tenants by billing price and time of usage. • Provides real-time display of bills. • Supports project bills, department bills (bills of departments that have projects attached), and account bills. • By default, billing details are generated once at 00:00 each day. You can change the time for generating billing details in global settings.
Access	TUI	Supports common O&M operations and custom OS UI .
	GUI	Allows you to access a graphical user interface (GUI) via HTTP or HTTPS to manage the Cloud.
	UI language	• Ensures that the default UI language is consistent with that of your current browser. • Allows you to customize the UI language and records your operation. This can improve user experiences.
	Login security	• Allows you to authenticate with dynamic authentica tion codes. Specifically, if the login fails for 6 consecutive times, an authentication would be required to avoid malicious logins. • Supports two-factor authentication, adding extra security codes for authenticating your identity to further increase your account security. • Supports complexity settings for login password . You can set the password length in a custom manner, and use the password strategy with a combination of numeric, case-sensitive, and special characters. • Supports password expiration settings. You can set the password update cycle in a custom manner.

Type	Feature	ZStack Enterprise
		We recommend that you change the cloud login password regularly to ensure the login security. • Allows you to set the history password check. You can set unrepeated times of failed logins in a custom manner. • Allows you to set the password lock mechanism. You can set the maximum number of failed logins and the maximum login number of locking a user for a period of time. When your continuous failed logins exceed the value that you set, your user account will be locked for a period of time to ensure the login security. • Supports the IP blacklist or whitelist. You can set IP blacklist or whitelist as needed to detect and filter visitor identities and to improve the cloud access control security. • Supports multiple session logins for the same user, and allows you to disable multiple session logins.
	Command line	Allows you to access the Cloud via command line. The command line supports full feature accesses. In addition, an account and a user can be logged in via command lines.
	API	Provides comprehensive APIs where APIs support Java SDK (compatibility version: Java 8), Python SDK (compatibility version: Python 2.7), and standard RESTful interface accesses.
Operation assistant	Intelligent notification	Provides intelligent environment checks and operation guides for key cloud operations.
Affinity group	Anti-affinity group	Provides two types of affinity group strategy: anti-affinity (soft) and anti-affinity (hard) to reasonably schedule cloud resources.
UI augmentation	Custom product information	Allows you to customize the product logo, product name, and other information via custom UI.
	Large-screen home page	• Provides multiple magnificent themes of a large screen to display your cloud resource information. • Allows you to switch virtualizations to display KVM or vCenter large screen respectively. • Allows you switch zones to display the large screen of all zones or a zone.

Type	Feature	ZStack Enterprise
		• Allows you switch data sources, including external monitoring and internal monitoring. For internal monitoring, you need to install an agent.
	Encryption access	Allows you to securely log in to the Cloud via HTTPS.
	In-process display	Adds progress bars of multiple scenarios.
VDI	Solution	• Supports SPICE, RDP, and VNC, and has optimized them via custom client side. • Allows you to specify a VDI network. • Supports USB redirection, which means multiple USB devices are compatible. • Allows you to set an independent VDI network. • Supports multi-screen display. • Supports microphones. • Supports SPICE to optimize traffics.
UI navigation	Quick entrance	Adds a quick entrance to the product and service, and highlights important resources.
UI informatio n exporting	List information exporting with CSV format	Exports VM and host main list information, making it more convenient to manage and edit parameters in list offline.
Tag	Resource tag	• Allows you to create tags with different names or colors, and binds them to resources (such as VM instances, volumes, hosts, and Bare Metal instance) to conveniently manage and search these resources. • Allows you to sort resource tags according to the bound time or names.
Application center	Application center	Allows you to add application plugins, such as storage , database, security, IaaS, PaaS, and SaaS.
AccessKey	AccessKey management	Allows you to generate an AccessKey that other clouds can call APIs. This AccessKey has the same permission as the creator who generated the AccessKey.
License	Cloud license (Basic License)	• Includes enterprise edition and hybrid edition. • Allows you to upload Basic License via a local browser. • Supports expiration notifications of Basic License.

Type	Feature	ZStack Enterprise
		• Supports all features for Enterprise, standalone version with unlimited trials. • Supports two types of authorization method: CPU and host.
	Module license (Plus License)	• Provides additional functionality. • Depends on Basic License. • Currently includes Enterprise Management module , VMware Management module, BareMetal Management module, Backup Service module, Migration Service module, ARM64 Management module, and After-Sales Service (5x8 and 7x24). • Allows you to upload Plus License via a local browser. • Supports expiration notifications of the Plus License .
	CPU infrastructure license	• Supports x86 server infrastructure license. KVM and vCenter can be used separately to provide independent CPU permissions for a compute node. • Supports ARM64 server management license. In addition, allows you to add an ARM64 server to the Cloud via a license. You can specify CPU counts or host counts for the ARM64 server.
	License uploading	• Allows you to package licenses as needed. • For dual management nodes, allows you to download request code and upload license in any management node.
Management node	Multi-host management node HA	• Supports multi-host management node (MN) HA . You can use the active-backup mode. Specifically, after a management node fails, another management node will be used to ensure your business continuity. • Allows you to add licenses for the active management node and the backup management node respectively via VIP login. • A multi-MN HA environment allows you to monitor the management node HA and check the health status. In addition, by default, a resource alarm will

Type	Feature	ZStack Enterprise
		be triggered if the monitor IP cannot be reached, or if dual MN database cannot synchronize.
	Management node	• A management node supports coexistence of different versions of source files. • A management node database lets you configure access restrictions. Also, the account of this database can be included in a whitelist to ensure security of this database.
Compute node	Batch host addition	• Allows you to add hosts in bulk according to the network range that you entered. • Allows you to add hosts in bulk with a template.
Log server	Log server	Allows you to collect logs of a management node. You can easily collect logs of a management node to quickly locate issues and to improve O&M efficiencies of the Cloud.
Installation	One-click installation	• Allows you to run just one command to complete installing and deploying the Cloud from scratch within just 30 minutes. • Supports three installation modes: ZStack Enterprise Management Node, ZStack Community Management Node, ZStack Compute Node, and ZStack Expert Mode.
Upgrade	Seamless upgrade	Allows you to seamlessly upgrade your cloud from an earlier version to a later version.
	Incremental upgrade	Supports incremental upgrade to improve the upgrade speed greatly.
	Environment upgrade	Allows you to customize installation and upgrade via ZStack Expert Mode.

The following table lists the features of ZStack Enterprise Management module.

Type	Feature	Enterprise Management Module
Organization	User	• A user is the most basic unit in Enterprise Management. • An administrator or platform user can create users, and builds the corresponding organization structure based on users.

Type	Feature	Enterprise Management Module
		• You can add users, delete users, change user names, change passwords, change personal information, add users to departments, remove users from departments, add users to projects, and remove users from projects. • Personal information of a user includes name, mobile phone number, email address, and identifier . • You can create users manually or by importing a template. Specifically, if you import a template , organization relationship among users and the information of projects where the users belong can be synchronously imported.
	Organization	• An organization is the basic unit in Enterprise Management. An administrator or platform user can see all organization structure trees of the Cloud, while a regular platform user or project member can only see the structure tree of the organization where regular users or project members belong. • An organization can be displayed by an organizati on structure tree, and includes a top-level department and subsidiary departments. The top-level department is the first level department where you can add multiple subsidiary departments. You can create multiple top-level departments. • The binding relationship between a department head and a department is weakened to allow the department to not set the head of department. • You can add an organization, delete an organizati on, change a parent department, create a subsidiary department, delete a subsidiary department, add a user, and remove a user.
	Role	• A role is a group of permissions and can endow users with permissions used for calling related APIs to manipulate resources. • Tenants and roles are separated in Enterprise Management. Roles can be bound to tenants or removed from tenants in Enterprise Management. A role includes system role and custom role.

Type	Feature	Enterprise Management Module
		• The GUI provides API-level permission control for tenants to flexibly meet permission configurations of various scenarios. • A super administrator (admin), platform admin, or regular platform user can have permission controls on a project member (project admin, project operator, or regular project member). • A platform admin can serve as a user. If you bind a platform admin role to a user, this user can be endowed with the corresponding role and the corresponding permissions. • Provides platform admin role, project admin role, project operator role, and dashboard role. Specifically, a user with the dashboard role can only have the permission to check the dashboard. If you log in to the Cloud via this user, you will jump to the dashboard page.
	3rd party authentication	• Allows you to add an AD or LDAP server. After you add an AD or LDAP server successfully, you can automatically import 3rd party users or organizations (only for AD server) to the Cloud. • Allows you to set a user mapping and organization mapping (only for AD server). You can synchronize 3rd party users or organizations (only for AD server) according to the mapping rule that you set. • Allows you to customize filter rules to filter out users that you do not need to synchronize.
Project management	Project	• Specifies related people to accomplish specific target tasks at a specific time, and with a specific resource and budget. • Enterprise Management is project-driven to schedule resources. You can build an independent resource pool for a specific project. • Allows you to create a project, delete a project, enable a project, disable a project, change a project admin, generate a project template, add a member, remove a member, stop project resources, recover the expired project, attach an organization, and detach an organization.

Type	Feature	Enterprise Management Module
		• The binding relationship between a project admin and a project is weakened to allow the project to not set the project admin. • Allows you to recover a project via job scheduling recovery or billing recovery. • Allows you to create projects in bulk by using official scripts.
	project template	• Identifies the template of each resource quota. • Allows you to directly use the quota defined by the template to quickly create a project. • Allows you to create a project template and delete a project template.
	project member	• A project member is the basic member of a project. Generally, an admin, platform user, project admin, or project operator can be added to a project. • Permissions of a project member can be controlled correspondingly by an admin, platform user, project admin, or project operator.
	Member group	• An admin, platform user, project admin, or project operator can create multiple member groups in a project and manages users by groups. • You can endow a member group as a unit with a role on which you can have permission controls.
	QoS setting	• An admin or platform user can set QoS for a VM, volume, and NIC. • You can set the total bandwidth or read and write bandwidth for a disk QoS. • You can control QoS setting range. QoS limit of a regular account or project member must not exceed the values that are set by an admin or platform admin.
Ticket management	Ticket applying	• A project member (project admin, project operator, or regular project member) can apply for tickets for cloud resources. • A project member can create, reject, reopen, and delete a ticket.

Type	Feature	Enterprise Management Module
	Ticket approval	• An admin or project admin can approve, deploy, and reject tickets. • Supports the default process approval and custom process approval. • Default process approval: A project member submits a ticket application. Then, an admin can perform a one-click approval. After the ticket process is approved, resources will be automatica lly deployed successfully and distributed to the corresponding project. • Custom process approval: A project member submits a ticket application. Then, approvers of each approval flow will perform approvals according to the custom process approval. Finally, an admin or project admin will perform one-click approvals. After all ticket processes are approved, resources will be automatically deployed successfully and distributed to your project.
	Custom process management	• An admin can set different types of custom ticket process for different projects. • Supports multiple ticket types, for example, apply for a VM instance, delete a VM instance, change a project cycle, change VM configurations, and modify a project quota. • The custom ticket process allows you to add project members to each approval flow. • Allows you to enable, disable, change, and delete custom ticket process.
Independent zone management	Platform admin	• A platform admin is mainly an administrator who can add or remove zones. • An admin can allocate different zones to different platform admins. In this regard, these platform admins can manipulate data centers of different zones. • Allows you to create or delete a platform admin, change passwords, add a zone, and remove a zone .

Type	Feature	Enterprise Management Module
	Resource isolation	• Allows you to specify the corresponding zone admins for each zone based on the fact that resources are isolated on zones. Doing so will achieve independent managements for each machine room. • Meanwhile, an admin can check and manage all zones.

The following table lists the features of ZStack BareMetal Management module.

Type	Feature	BareMetal Management Module
BareMetal management	Bare Metal cluster	• Manages Bare Metal hosts by creating a Bare Metal cluster. • Allows you to attach a Bare Metal cluster to an L2 network.
	Deployment server	• Automatically installs and deploys the system for newly-created Bare Metal chassis via a deployment server. • Allows you to deploy a deployment (PXE) server independently.
	Bare Metal chassis	• Deploys Bare Metal chassis in bulk via an IPMI network. • Allows you to manage powers of Bare Metal chassis remotely. • Adds Bare Metal chassis in bulk according to the network range that you entered. • Allows you to add Bare Metal chassis in bulk via template importing. • Allows you to open the IPMI management page (login page) of Bare Metal chassis via a console . You can log in to the Bare Metal chassis by entering the configured IPMI user name and the IPMI password.
	Bare Metal instance	• Allows you to install Linux operating system for Bare Metal chassis with an ISO image. • Allows you to install Ubuntu, CentOS, and SUSE in an unattended manner.

Type	Feature	BareMetal Management Module
		• Allows you to add network configurations for a Bare Metal instance. • Provides real-time monitoring of internal workloads . For Bare Metal instance monitoring, you need to install an agent. You can check CPU, memory, disk , NIC, and other performance inductors of a Bare Metal instance. • Provides associated monitoring items of a Bare Metal instance, including CPU, memory, disk, and NIC. • Allows you to create tags (for admin tags only) for Bare Metal instances and quickly search target Bare Metal instances via these tags.

The following table lists the features of ZStack Backup Service module.

Type	Feature	Backup Service Module
Backup service	Backup	• Allows you to create a backup job for a VM instance, volume, and management node database . Specifically, supports backups of entire VM instances. • Displays the current backup jobs in a unified manner so that you can quickly control the overall status of current backup jobs and improve the O&M efficiency. • Greatly improves the backup performance of large files by optimizing the backup mechanism of large files, and supports physical tape library (PTL) and virtual tape library (VTL). • Allows you to set the backup strategy for a backup job according to week, day, or hour. The backup job that you created allows you to update the backup strategy. • Saves backup file data according to count or time. • Allows you to perform backups immediately and fully back up your data on schedule after you create a backup job. • Allows you to back up your data on the local backup storage and synchronize the data to the remote backup storage.

Type	Feature	Backup Service Module
		• Allows you to check the local backup data or remote backup data of a VM instance, volume, and database. • Allows you to delete a local backup data or remote backup data. • Allows you to either use the ImageStore backup storage that you have deployed on the local data center as a local backup storage or to deploy a new local backup storage directly. • Supports active backup seamless switch when you specify multiple local backup storages for a backup job. • Only allows you to add a remote backup storage, including remote backup and Aliyun backup. • Allows you to synchronize backup data only from a local backup storage to a remote backup storage. • Cleans up the invalid backup data that were completely deleted and the temporary data that were expired on a local backup storage or remote backup storage to release more storage spaces. • Allows you to set disk QoS and network QoS for a backup job. • Allows you to check the backup progress of a backup job. • Allows you to automatically obtain backup data when you add the existing backup storages. • Allows you to create event alarms for backup jobs . When a backup job fails, you can receive alarm details about the backup job at an endpoint.
	Recovery	• Allows you to create new resources or overwrite original resources when you recover resources from local backup data or remote backup data of a local VM instance or volume. • Allows you to recover an entire VM instance. • The remote backup data of a local VM instance or volume must be synchronized to a local backup storage in advance before you recover the remote backup data to the local backup storage. The remote backup data of database can be recovered directly to the local backup storage.

Type	Feature	Backup Service Module
		• Allows you to perform one-click recovery for the data center via the local or remote backup storage of a database. This is applied to the scenario that the local backup storage attaches a zone and has data. • Allows you to recover the data center by means of the Wizard guidance page via the local backup data of the database or remote backup data of the database. This is applied to the scenario that the local backup storage has no any zone and any data . • Allows you to export and then manually recover the local backup data or remote backup data of a database.

The following table lists the features of ZStack Migration Service module.

Type	Feature	Migration Service Module
Migration service	V2V conversion host	• Decouples from the state of the corresponding host. When a V2V conversion host is enabled but the corresponding host is disabled, the V2V conversion host will be dedicated to V2V migration scenarios, and other appliance VM instances will not be dispatched to the V2V conversion host. This effectively improves the migration efficiency. • Allows you to set a separate migration network to convert data from the source primary storage to the V2V conversion host. • Supports real-time capacity monitoring. You can select different time spans to monitor the percentage of used capacity of a V2V conversion host. • Displays the total capacity and available capacity of a V2V conversion host.
	V2V migration for VMware	• Migrates vCenter VM instances that you took over to the current Cloud. • Allows you to perform one-click V2V bulk migrations for VM instances. After the migrations were completed successfully, the provisioning method keeps unchanged.

Type	Feature	Migration Service Module
		• Allows you to customize configurations for target VM instances when you create a V2V migration job. • Allows you to set a migration network and QoS. • Allows you to cancel and restart a V2V migration job. • Provides safe, resource-efficient migration services . Files that are migrated will be compressed and saved on the source primary storage. • Supports multiple versions of source vCenter platform, including 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7. • Allows you to perform V2V migrations for VM instances with multiple types of operating system. The supported types of operating system for V2V migrations include RHEL/CentOS 5.x/6.x/7.x, SLES 11/12/15, Ubuntu 12/14/16/18, and Windows 7/ 2003/2008/2012/2016. • Provides unlimited types of source primary storage . Currently, the target primary storage supports Ceph, Shared Block, NFS, and LocalStorage.
	V2V migration for KVM	• Does not need you to take over KVMs. You can migrate VM instances online from a KVM cloud to the current Cloud. • Allows you to perform V2V migrations (KVM) for VM instances that are in the running state and the stopped state. • Supports unlimited types of primary storage. • Migrates data volumes synchronously that you attached when you perform V2V migrations for KVMs, and allows you to modify CPUs and memories. • Does not migrate VM snapshots synchronously when you perform V2V migrations for KVMs. • Provides unlimited types of primary storage. Currently, the target primary storage supports Ceph , SharedBlock, NFS, and LocalStorage.

The following table lists the features of ZStack Rights Separation module.

Type	Feature	Rights Separation
Rights Separation	Rights management	Permissions of a super admin (admin) are separated into three roles: system administrator (sysadmin), security administrator (secadmin), and security auditor (secauditor). These three roles are mutually independent and mutually balanced to further enhance the cloud security. Doing so will effectively lower the security risk that permissions of a super administrator are too large.
	System admin	The sysadmin manages resources on the Cloud and manipulates the lifecycle of resources on the cloud excluding managements of associated permissions.
	Security admin	The secadmin manages cloud permissions, and allocates permissions to users or roles.
	Security auditor	The secauditor manages cloud auditing, and has permission controls to check and export logs that are used to audit operations of other users.

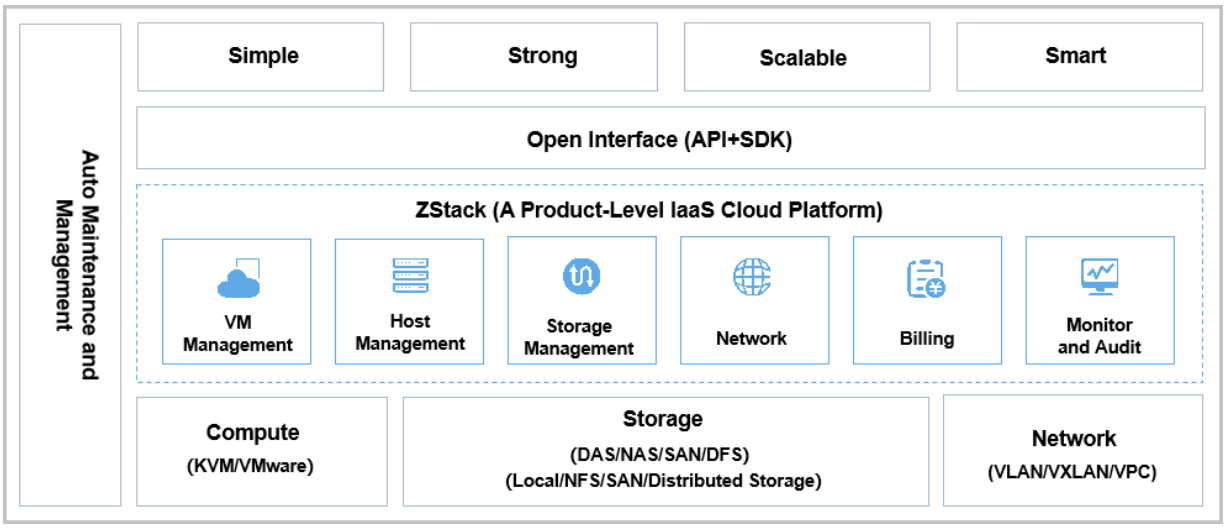
3 System Architecture

ZStack is a next-generation product-level private cloud management platform that aims to manage various resources, such as compute, storage, and network resources in data centers by providing flexible and comprehensive APIs.

3.1 ZStack Functional Architecture

The functional architecture of ZStack is shown in *Figure 3-1: ZStack Functional Architecture*.

Figure 3-1: ZStack Functional Architecture



ZStack helps enterprises better manage infrastructure resources, such as the compute, storage, and network resources, in their data centers. The bottom layer of ZStack supports both KVM and VMware virtualization technologies. In addition, ZStack supports various storage types, such as DAS, NAS, SAN, and DFS. To be more specific, local storage, NFS storage, SAN storage, and distributed block storage are supported. ZStack also supports various network models, such as VLAN and VXLAN.

ZStack uses a message bus to communicate with the MariaDB database and different service modules, providing diversified features such as VM instance management, host management, storage management, network management, billing management, and real-time monitoring. That is the core Cloud engine of ZStack. In addition, ZStack provides Java SDKs and Python SDKs, and allows you to schedule and manage resources by using RESTful APIs. With ZStack, you can build a private Cloud that is Simple, Strong, Scalable, and Smart.

Highlights of ZStack functional architecture:

1. **Asynchronous Architecture:** asynchronous message, asynchronous method, and asynchronous HTTP call
   - ZStack uses a message bus to connect various services. When a service calls another service, the source service sends a message to the destination service, registers a callback function, and then returns back immediately. Once the destination service finishes the task, it gives a feedback on the task result by triggering the callback function that was registered by the source service. Asynchronous messages can be processed in parallel.
   - Services in ZStack communicate with each other through asynchronous messages. Inside services, the associated components and plugins are also called by using asynchronous methods. These methods are consistent with that of calling asynchronous messages.
   - Every plugin in ZStack has a corresponding agent. ZStack puts a callback URL in the HTTP header of every request. Therefore, agents can send responses to the URL of the caller when tasks are finished.
   - Based on asynchronous message, asynchronous method, and asynchronous HTTP call , ZStack builds a layered architecture to ensure that asynchronous operations can be performed on all components.
   - Based on the asynchronous architecture, a single ZStack management node can process tens of thousands of concurrent API requests per second, and simultaneously manage tens of thousands of servers and hundreds of thousands of VM instances.
2. **Stateless Service:** A single request does not rely on other requests.
   - In ZStack, requests sent by compute node agents, storage agents, network services, console agent services, and configuration services can be processed without relying on other requests. The sent requests contain all the required information, and related nodes do not need to maintain and store any information.
   - ZStack authenticates resources such as management nodes and compute nodes through consistent hashing ring by using their UUIDs as the unique ID. Because of the consistent hashing ring, a message sender does not need to know which service instance is about to handle the message. Services do not need to maintain and exchange information about what resources they are managing. All the services need to do is to handle the incoming messages.
   - Little information is shared among ZStack management nodes. Therefore, a minimum of two management nodes can meet the requirements of high availability and scalability.

- The stateless service mechanism makes the system more robust. Restarting the server will not lose any state information. This also simplifies the scaling out and scaling in of a data center.

3. **Lock-free Architecture:** consistent hashing algorithm

- The consistent hashing algorithm guarantees all messages of the same resource are always handled by the same service instance. In this way, messages are congregated to a specified node, reducing the complexity of synchronization and concurrency.
- ZStack uses work queue to avoid lock contention. Serial tasks are stored in memory as work queues. Work queues can process any operation of any resource in parallel to improve system concurrency.
- The queue-based lock-free architecture enables tasks to run in parallel, thereby improving the system performance.

4. **In-Process Microservices Architecture:** microservices decoupling

- ZStack uses a message bus to isolate and control various services, such as VM instance services, identity authentication services, snapshot services, volume services, network services, and storage services. All microservices are enclosed in the same process of a management node. These services communicate with each other through the message bus . After all messages are sent to the message bus, the destination service is selected by the consistent hashing ring for message forwarding.
- In-process microservices provide a star-like architecture, ensuring every service in microservices to run independently. This architecture also decouples the highly centralize d control business, and achieves a high degree of autonomy and isolation of the system. Failure of any service does not affect other components. This effectively guarantees the system reliability and stability.

5. **Versatile Plugin System:** supports horizontal expansion of plugins

- In ZStack, every plugin provides services independently. Any newly added plugin has no impact on other existing plugins.
- ZStack concludes plugins into two patterns: strategy pattern and observer pattern. Strategy pattern plugins will inherit parent-class interfaces and then perform specific implementations . Observer pattern plugins will register a listener to monitor event changes of the internal business logic in an application. Once an event is detected inside the application, the observer pattern plugins will respond to this event automatically and execute a piece of code to affect the corresponding business flow.

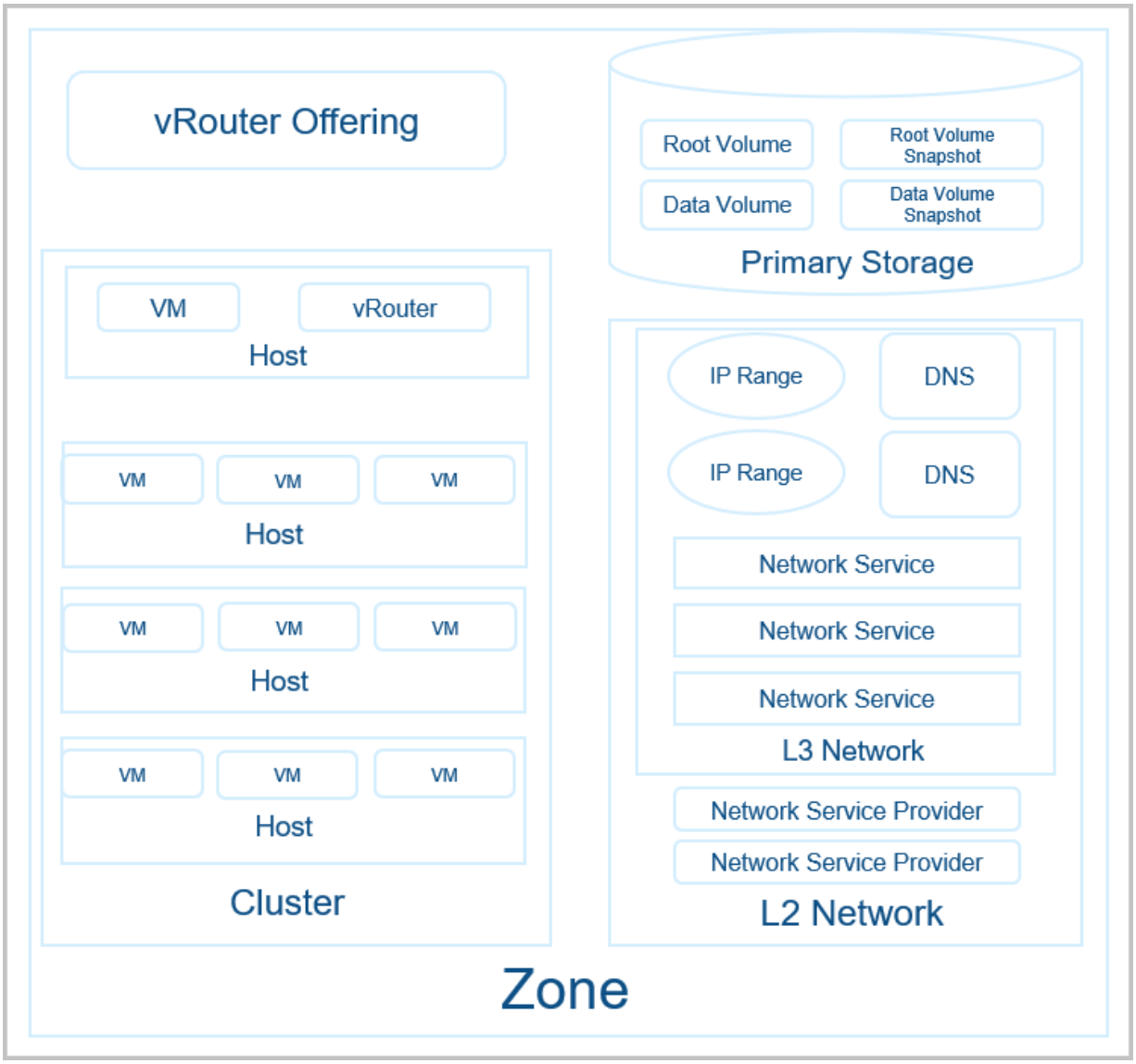
- ZStack supports horizontal expansion of plugins. The Cloud can be quickly upgraded, and the overall system architecture still remains robust.

6. **Workflow Engine:** sequence-based management, rollback on errors
   - ZStack clearly defines every workflow by using XML files. Every flow can be rolled back on errors. A workflow can roll back all prior executed steps and clean up the garbage resources during the execution when an error happens in a step.
   - Every workflow can contain sub-flow to decouple the business logic further.
7. **Tag System:** extends the business logic and adds resource properties
   - ZStack uses system tags and plugins to extend the original business logic.
   - You can use tags to group your resources and search for resources with specific tags.
8. **Cascade Framework:** supports cascading operations on resources
   - ZStack uses a cascade framework to perform cascading operations on resources. The cascade framework allows an operation to be cascaded from one resource to other resources. For example, the operation of uninstalling or deleting a resource can be cascaded to the descendant resources.
   - Resources can join a cascade framework through a plugin. Joining or quitting the cascade framework will not affect other resources.
   - The cascading mechanism makes the configuration of ZStack more flexible and simple, meeting the requirements of resource configuration changes.
9. **Full Automation By Ansible:** automated deployment by agentless Ansible
   - Being seamlessly integrated with Ansible (which is agentless), ZStack can automatically install dependencies, configure physical resources, and deploy agents. This whole process is transparent to users and requires no additional intervention. You can upgrade your agents simply by reconnecting the agents.
10. **Comprehensive Query API:** Every property of every resource can be queried.
    - ZStack supports millions of query conditions, comprehensive query APIs, and any way of condition combinations.

3.2 ZStack Resource Model

ZStack is essentially a configuration management system for resources in the Cloud. The following figure describes the resource model managed by ZStack, as shown in *Figure 3-2: ZStack Resource Model*.

Figure 3-2: ZStack Resource Model



ZStack mainly has the following resources:

- Zone: the largest resource scope defined in ZStack. A zone is a logical group of resources, such as clusters, L2 networks, and primary storages.
- Cluster: a logical group of analogy hosts (compute nodes).
- Host: also known as a compute node, is a physical server that provides VM instances with compute, network, and storage resources.
- Primary storage: a storage system that stores disk files, including root volumes, data volumes , root volume snapshots, data volume snapshots, and image caches, for VM instances. The types of primary storage include local storage, NFS, Shared Mount Point, SharedBlock, and Ceph.

- Backup storage: a storage system that stores image templates. The types of backup storage include ImageStore, SFTP, and Ceph.
- VXLAN pool: an underlay network in VXLAN. You can create multiple VXLAN overlay networks (VXLAN) in a VXLAN pool. The overlay networks can operate on the same underlay network device. The types of VXLAN pool include software SDN and hardware SDN.
- L2 network: a layer 2 broadcast domain used for layer 2 isolation. Generally, L2 networks are identified by names of devices on the physical network. The types of L2 network include L2NoVlanNetwork, L2VlanNetwork, VxlanNetwork, and HardwareVxlanNetwork.
- L3 network: a collection of network configurations for VM instances, including the IP range, gateway, DNS, and network services.
- Instance offering: a specification of the VM instance CPU, memory, disk bandwidth, and network bandwidth.
- Disk offering: a specification of a volume, which defines the size of a volume and how the volume will be created.
- VM instance: a virtual machine instance running on a host. A VM instance has its own IP address to access public network and run application services. VM instances are core components of ZStack.
- Image: an image template used by a VM instance or volume. Image template includes root volume images and data volume images. The types of root volume image include ISO and Image, while the type of data volume image is Image.
- Root volume: the system disk where the VM instance operating system is installed.
- Data volume: the data disk that provides additional storage for a VM instance.
- Snapshot: a point-in-time capture of data in a disk. Snapshots are captured incrementally.
- Network service module: a module for providing network services. This resource is hidden in the UI.
- Network service: provides various network services for VM instances, including VPC firewall, security group, virtual IP (VIP), elastic IP (EIP), port forwarding, load balancing, IPsec tunnel, and flow monitoring.
- VPC firewall: manages north-south traffic of the VPC network. You can manage the network access policy by configuring rule sets and rules.
- Security group: provides L3 network firewall control over the VM instances, and controls TCP, UDP, and ICMP data packets for effective filtering. You can use a security group to effectively control specified VM instances on specified networks according to specified security rules.

- Virtual router offering: an instance offering that defines the CPU, memory, virtual router (vRouter) image, management network, and public network used by a vRouter (including ordinary vRouter, VPC vRouter, and ARM vRouter).
- Virtual router (vRouter): a custom Linux VM instance that provides network services such as DHCP, DNS, SNAT, route table, EIP, port forwarding, load balancing, and IPsec tunnel.
- VPC vRouter: a router created directly from vRouter offering. VPC vRouter, which has a public network and a management network, is the core of VPC. VPC vRouter provides various network services, including DHCP, DNS, SNAT, route table, EIP, port forwarding, load balancing, IPsec tunnel, dynamic routing, multicast routing, VPC firewall, and Netflow.

The resource relationships in ZStack are as follows:

- Parent-child: A resource can be the parent or child of another resource. For example, a host is the child resource of cluster, while a host is the parent resource of VM instance.
- Sibling: Resources sharing the same parent resource are siblings. For example, clusters and L2 networks are sibling resources because all of them are child resources of zone.
- Ancestor-descendant: A resource can be the lineal ancestor or lineal descendant of another resource. For example, a cluster is the ancestor resource of VM instance, while a host is a descendant resource of zone.
- Friend: Resources that do not have the above three relationships but still need to cooperate with each other in some scenarios are friends. For example, primary storage and backup storage are friends. Also, zone and backup storage are friends.

> **Note:**
> Relationship between primary storage and backup storage:
>
> - When you create a VM instance, primary storage needs to download images of the VM instance as caches from backup storage.
> - When you create an image, primary storage needs to copy the root volume to backup storage and save it as a template.

The following properties are common to almost all resources in ZStack:

- UUID: the universally unique identifier. ZStack uses version 4 UUIDs to uniquely identify a resource.
- Name: a human readable string that is used to identify resources. Names can be duplicated and are usually required.

- Description: also known as a brief introduction that is used to briefly describe a resource. Description is usually optional.
- Creation date: the date and time when a resource was created.
- Last operation date: the date and time when a resource was updated last time.

Resources support full or partial Create, Read, Update, Delete (CRUD) operations.

- Create: create or add a new resource.
- Read: read or query information about a resource.
- Update: update information about a resource.
- Delete: delete a resource. Due to the cascade framework provided by ZStack, if a parent resource is deleted, its associated child resources and descendant resources will also be deleted.

4 Network Configuration

ZStack supports complex network scenarios. This topic lists several common network architectures according to business requirements and practical environments.

1. **LocalStorage+Flat Network**

   Features of this architecture are as follows:

   - Hosts use LocalStorage to store the system disks and data disks of VM instances.
   - The RAID array technology of hosts is required to protect VM data.
   - Hosts and VM instances are in the same L2 network. Therefore, VM IP addresses and host IP addresses can ping each other.
   - This architecture supports distributed DHCP, distributed EIP, and Userdata services.
   - By default, VM online migration is not supported. But you can enable VM online migration in global settings.
   - Featuring low costs and high concurrency performance, this architecture can be applied to software development and testing environments, and the scenario where the application layer can provide high availability.

   Management Network:

   - The management network manages resources in each compute node and storage node.
   - In the preceding figure, em01 is the NIC used by the management node to communicate with the compute nodes and the backup storage.

   Business Network:

   - The business network is used by the compute nodes and the backup storage for data communication.
   - In the preceding figure, em02 is the network used for creating VM instances. If the VM network and host network are in the same network segment, the corresponding VM instances and hosts can ping each other. Note that the IP ranges of the VM network and host network cannot be overlapped when you ping the VM instances and hosts.
   - You can set VLAN or VXLAN for L2 isolation. After L2 isolation is implemented, VM instances can only be used in private networks and cannot directly access the Internet. In this case, EIPs are required to achieve network interconnection.

   Backup Storage:

- The backup storage can use an independent server to provide services.
- In small data centers, the backup storage can also share the same server with the management node.

2. **NAS/SAN+vRouter Network**

Features of this architecture are as follows:

- The VM data is stored in a centralized storage, and volume data is protected by the dual-controller of the storage and the RAID technology.
- A storage network and a centralized storage are required. We recommend that the storage network be equal to or greater than 10 Gigabit. VM instances are protected by high availabili ty.
- When you add a primary storage to ZStack, you can add it as NFS or Shared Mount Point primary storage.
- This architecture sets up a storage network, supports VM high availability, and protects VM data. However, the I/O performance has bottlenecks. Therefore, we recommend that 8 to 10 compute nodes share a storage.
- This architecture uses vRouters to provide network services such as DNS, SNAT, EIP, port forwarding, load balancing, IPsec, and security group.
- This architecture supports distributed DHCP network.
- This architecture requires some investments, and is suitable for traditional applications, intensive data, SLA high availability guarantee, and data security scenarios.

Management Network:

- The management network manages resources in each compute node and storage node.
- In the preceding figure, em01 is the NIC used by the management node to communicate with the compute nodes and the backup storage.

Business Network:

- The business network is used by the compute nodes and the backup storage for data communication.
- You can set public and private networks for the same hosts by setting VLAN. Note that the hosts are connected by the same physical cable.
- In the preceding figure, the em02 without a VLAN tag is the public network, which can access the Internet. The em02 tagged with VLAN 10 is the private network. You need to set

the switch to Trunk mode. Then, VM instances can access the Internet through the vRouter , and the vRouter network uses the vRouter to provide various network services. The default IP address of the vRouter network is the IP address of the public network.

Note:

If the host NICs are insufficient, you can combine the management network and business network into one.

Storage Network:

- The storage network is used to provide NAS and SAN storages.
- We recommend that you use a 10 Gigabit Ethernet or Fibre Channel (FC) to accelerate storage access. In the preceding figure, em03 is dedicated to providing access to storage network traffics.

Backup Storage:

- The backup storage can use an independent server to provide services.
- In small data centers, the backup storage can also share the same server with the management node.

3. **Ceph+VXLAN vRouter Network**

Features of this architecture are as follows:

- The VM data is stored in distributed storages and protected by multiple copies or erasure coding mechanisms.
- A storage network is required. VM instances are protected by high availability.
- The Ceph primary storage and the Ceph backup storage use the same distributed storage.
- This architecture sets up a storage network, and supports VM high availability and multiple copies for data. Both computing and storage can be scaled horizontally.
- This architecture uses the VXLAN VTEP to provide L2 logical subnet. The VXLAN underlay network is accessed by VM instances.
- This architecture uses vRouters to provide network services such as DNS, SNAT, EIP, port forwarding, load balancing, IPsec, and security group.
- This architecture supports distributed DHCP network.
- This architecture is suitable for renting platforms, general-purpose applications, intensive data, SLA high availability guarantee, and large scale scenarios.

Management Network:

- The management network manages resources in each compute node and storage node.
- In the preceding figure, em01 is the NIC used by the management node to communicate with the compute nodes and the distributed storage nodes.

Public Network:

- The public network can access the Internet.
- VM instances can access the Internet through the vRouter. The vRouter network uses the vRouter to provide various network services. The default IP address of the vRouter network is the IP address of the public network.
- In the preceding figure, em02 is used to provide public network services. If the NICs are insufficient, you can combine the management network and the public network into one.

VXLAN Underlay Network

- The VXLAN underlay network is a private network used by VM instances.
- The VXLAN underlay network is an L2 logical network based on L3 IP addresses. For example, in the preceding figure, the VTEP of *192.168.1.x/24* is used to provide the private network whose VNI is 201.

Storage Network:

- The storage network is used to provide distributed block storages.
- The storage networks provides distributed block storages. We recommend that you use a 10 Gigabit Ethernet or FC to accelerate storage access.
- In the preceding figure, em03 is the storage network. A Ceph distributed storage needs at least one Mon IP to interconnect with the management network.

4. **Ceph+VPC Network**

   Features of this architecture are as follows:

   - The VM data is stored in distributed storages and protected by multiple copies or erasure coding mechanisms.
   - A storage network is required. VM instances are protected by high availability.
   - The Ceph primary storage and the Ceph backup storage use the same distributed storage.
   - This architecture sets up a storage network, and supports VM high availability and multiple copies for data. Both computing and storage can be scaled horizontally.

- This architecture uses vRouters to provide network services such as DNS, SNAT, EIP, port forwarding, load balancing, IPsec, and security group.
- This architecture supports distributed DHCP network.
- This architecture is suitable for renting platforms, general-purpose applications, intensive data, SLA high availability guarantee, and large scale scenarios.

Management Network:

- The management network manages resources in each compute node and storage node.
- In the preceding figure, em01 is the NIC used by the management node to communicate with the compute nodes and the backup storages of the distributed storage type.

Business Network:

- You can set public and private networks for the same hosts by setting VLAN. Note that the hosts are connected by the same physical cable.
- In the preceding figure, the em02 without a VLAN tag is the public network, which can access the Internet. The em02s tagged with VLAN 10 and 20 are the private network (VPC network). You need to set the switch to Trunk mode. Then, VM instances can access the Internet through the VPC vRouter, and the VPC network uses the VPC vRouter to provide various network services. The default IP address of the VPC network is the IP address of the public network.

Note:

If the host NICs are insufficient, you can combine the management network and business network into one.

Storage Network:

- The storage network is used to provide distributed block storages.
- The storage network provides distributed storages. We recommend that you use a 10 Gigabit Ethernet or FC to accelerate storage access.
- In the preceding figure, em03 is the storage network. A Ceph distributed storage needs at least one Mon IP to interconnect with the management network.

5 Installation and Deployment

This chapter mainly describes the installation and upgrade process of ZStack 3.10.0.

5.1 Prepare Environment

Prerequisites

To install or upgrade ZStack, use ZStack Custom ISO. ZStack Custom ISO has the following properties:

1. ZStack Custom ISO has two versions.
   - c76: ZStack-x86_64-DVD-3.10.0-c76.iso
   - c74: ZStack-x86_64-DVD-3.10.0-c74.iso

   Note:

   - Based on all c74 features, c76 uses a new operating system (OS) kernel and supports NVIDIA vGPU.
   - **If you install ZStack for the first time, we recommend that you install the c76 ISO.** If you already deployed ZStack, you could upgrade it to the latest version within c74 or c76. For more information, see *Upgrade Tutorial*.
   - From version 3.7.1, we stop providing c72 ZStack Custom ISO. If you already deployed c72 ISO, contact our official technical support for upgrade.
2. ZStack provides a friendly, text-based user interface (TUI) that supports multiple system configurations.
3. You can install ZStack offline without connecting to the Internet or configuring the YUM repository.
4. ZStack provides several installation modes: ZStack Enterprise Management Node, ZStack Community Management Node, ZStack Compute Node, ZStack Expert Node. You can choose a proper mode as needed.
5. No eth configuration is required. You can use the default NIC naming convention.
6. Default options:
   - **DATE & TIME**: UTC/GMT +08:00
   - **LANGUAGE**: English (United States)
   - **KEYBOARD**: English (United States)

This documentation mainly describes how to install c76 ISO. Note that the basic steps for installing c74 ISO and c76 ISO are almost the same.

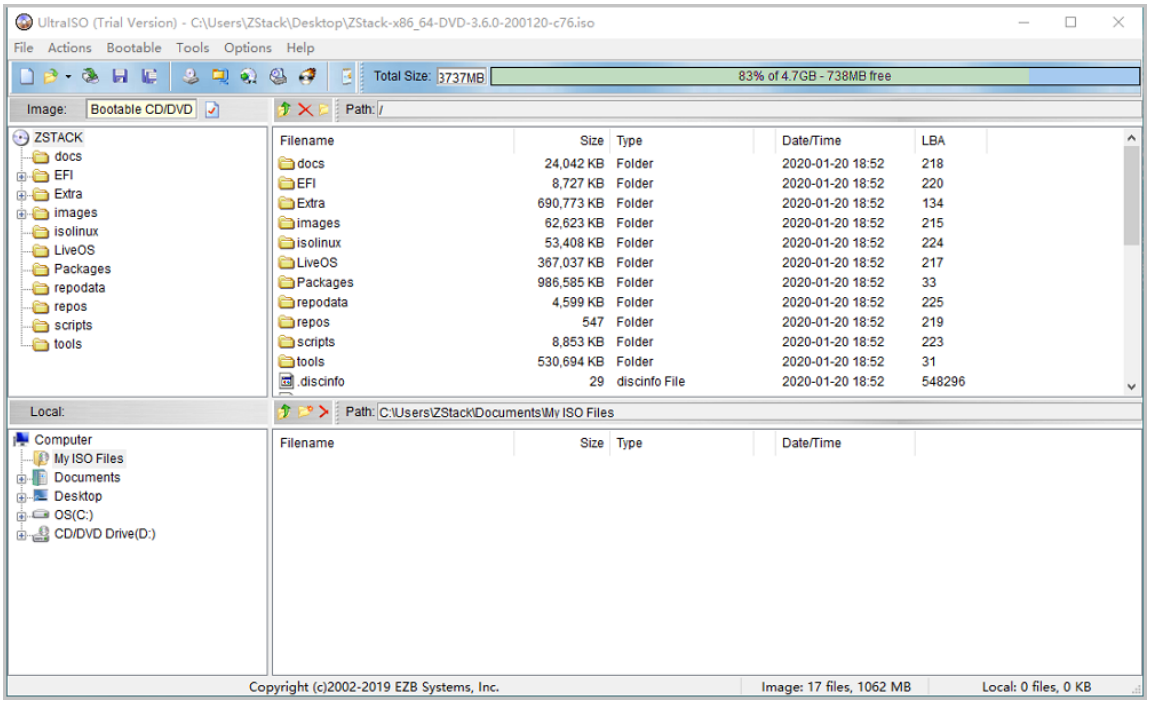
Procedure

1. Before you install ZStack, prepare the necessary software packages as follows to smoothen the process of installation and deployment.
   - ZStack Custom ISO
     - File name: ZStack-x86_64-DVD-3.10.0-c76.iso
     - Download address: Click *here*.
   - ZStack Installation Package
     - File name: ZStack-installer-3.10.0.bin
     - Download address: Click *here*.

   Note:
   After you download the installation package, confirm the integrity of the file by using the MD5 checksum tool.
2. Burn an ISO image to a USB drive by using UltraISO.
   a) Open an ISO image in UltraISO.

      Launch UltraISO, and choose **File** > **Open** to open the downloaded ISO file, as shown in *Open ISO Image in UltraISO*.

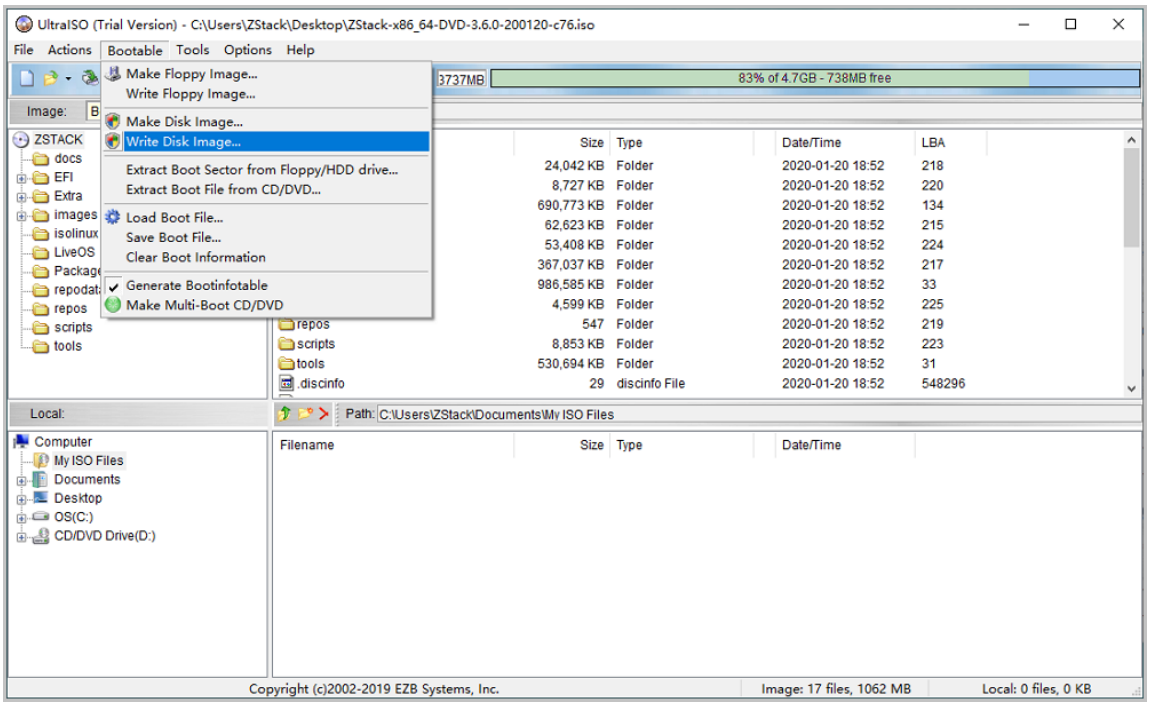
Figure 5-1: Open ISO Image in UltraISO



b) Write the ISO image to the USB drive.

In UltraISO, choose **Bootable** > **Write Disk Image**, as shown in *Figure 5-2: Write Disk Image in UltraISO*.

Figure 5-2: Write Disk Image in UltraISO



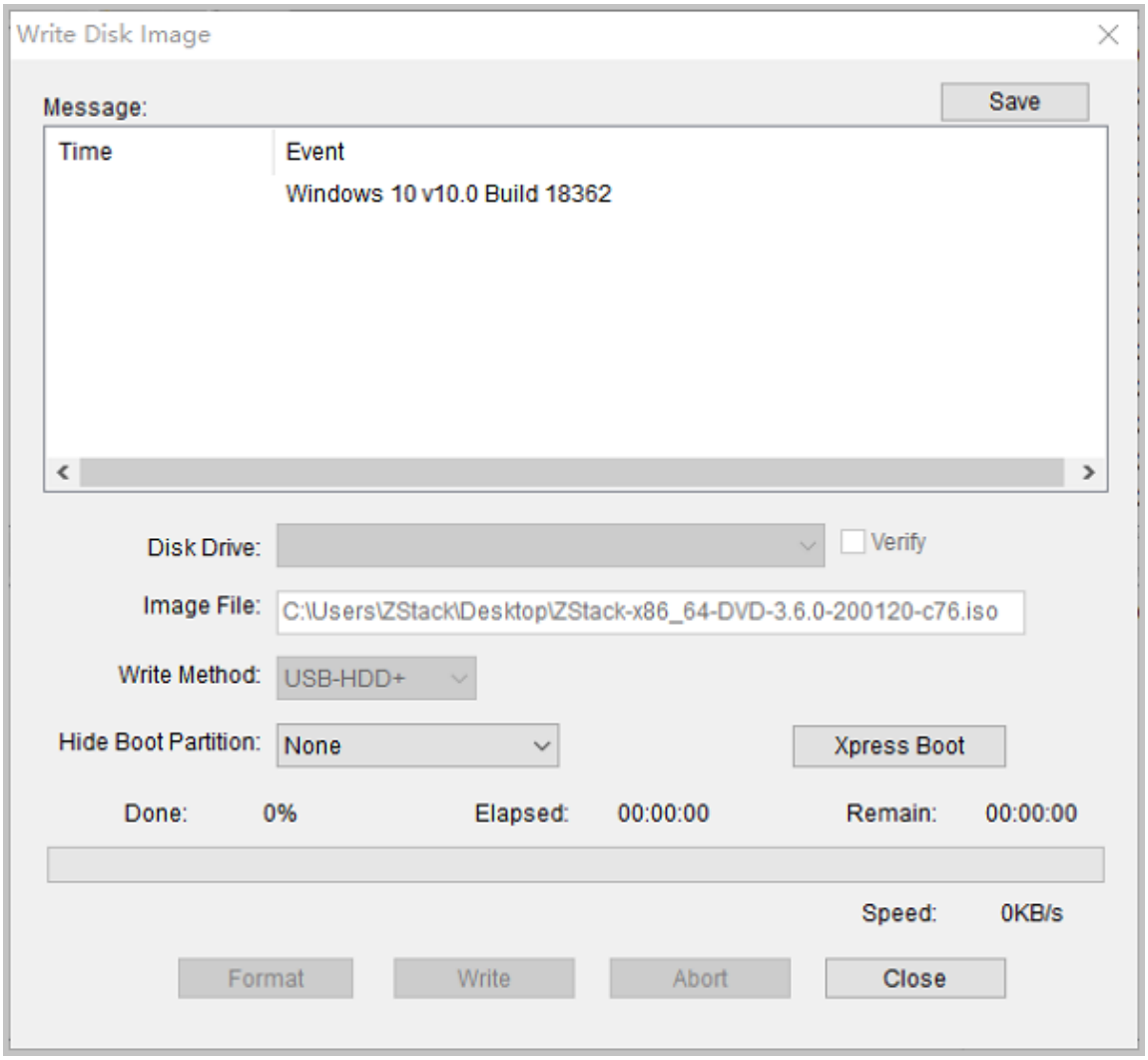
c) From the **Disk Drive** drop-down list, select the target USB drives.

Note:

- If the system has only one USB drive plugged in, the USB drive will be burned and written by default. Before you burn the image to the USB drive, **make sure that the USB drive is backed up.**
- For other options, use the default settings. After the settings are completed, click **Write**.

As shown in *Figure 5-3: Verify the Writing of ISO Image in UltraISO*.

Figure 5-3: Verify the Writing of ISO Image in UltraISO



d) On the popup page, click **Yes**. Then, UltraISO will burn the ISO image to the target USB drives.

e) Here, the target USB drives can be used as boot disks and support Legacy and UEFI modes.

3. Install the operating system.

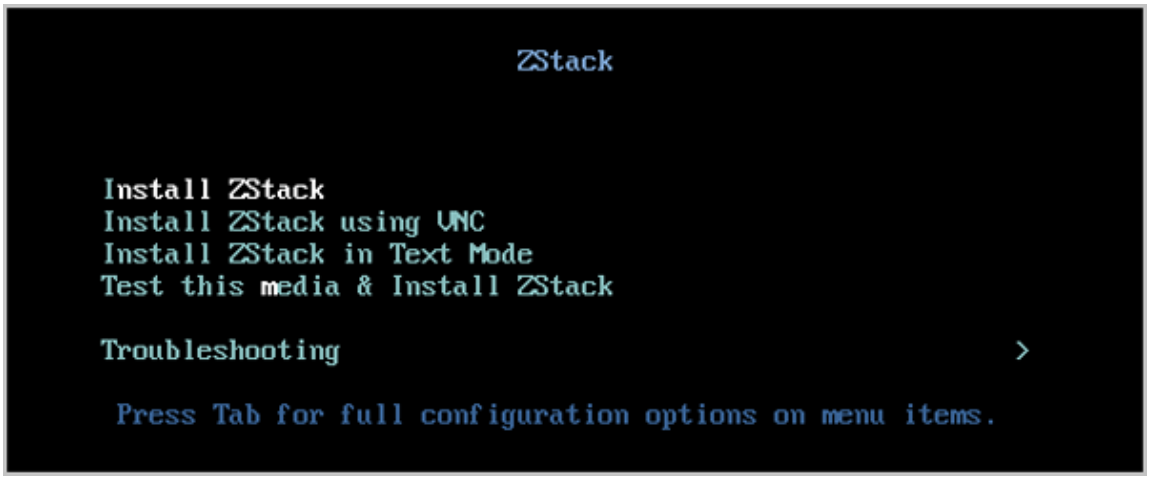
a) Before you (the administrator) install the operating system, configure the server as follows:

- Data on your hard drive of your server will be overwritten during the installation process. Therefore, make sure that the hard drive data is backed up.
- Enter BIOS, and enable CPU VT and hyper-threading (HT).
- Enter the RAID controller and configure the RAID levels to provide data redundancy.
- Set USB drives as the first device to boot in the boot sequence.

b) After you complete the preceding configurations, reboot or power on the server, and enter the installation wizard.

On the ISO installation page, the **Install ZStack** option is selected by default, and then the operating system starts to install, as shown in *USB Drive Guide Page*.

Figure 5-4: USB Drive Guide Page



Note:

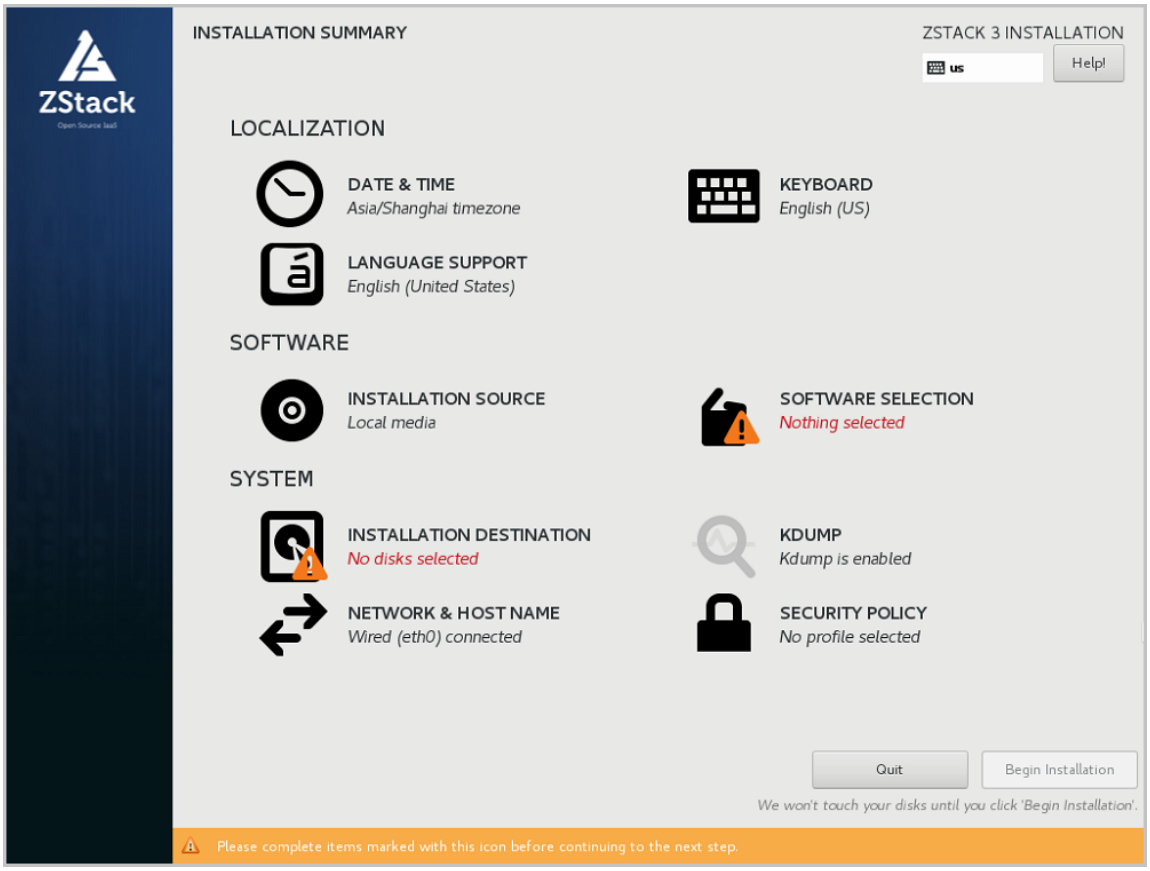
- As shown in the preceding figure, ZStack allows you to install the operating system by using one of the following methods: install ZStack, install ZStack by using VNC, or install ZStack in text mode.
- We recommend that you use the **Install ZStack** method.
- Some servers that do not have VGA ports can only be connected through serial ports. In this case, you can install the operating system in text mode, or by using VNC.

c) On the installation summary page, some options are preconfigured as below. You can modify the configuration as needed.

- **DATE & TIME**: UTC/GMT+8. We recommend that you check the date and time of your host in advance and then configure them to the current date and time.
- **LANGUAGE SUPPORT**: English (United States)
- **KEYBOARD**: English (United States)

As shown in *Installation Summary Page*.

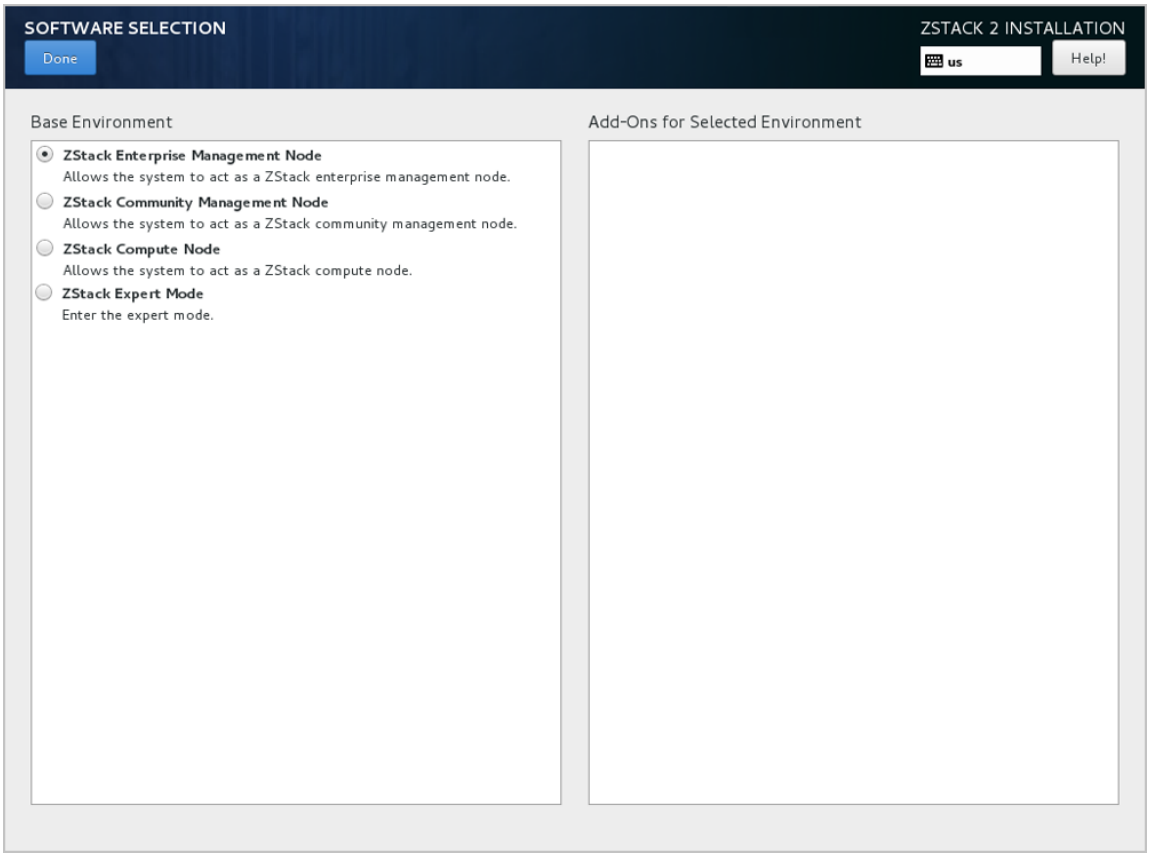
Figure 5-5: Installation Summary Page



d) Select an installation mode.

On the installation summary page, click **SOFTWARE SELECTION**, and go to the software selection page, as shown in *Select Installation Mode*.

Figure 5-6: Select Installation Mode



The available installation modes are as follows:

1. ZStack Enterprise Management Node

   Note:

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

2. ZStack Community Management Node
3. ZStack Compute Node
4. ZStack Expert Node

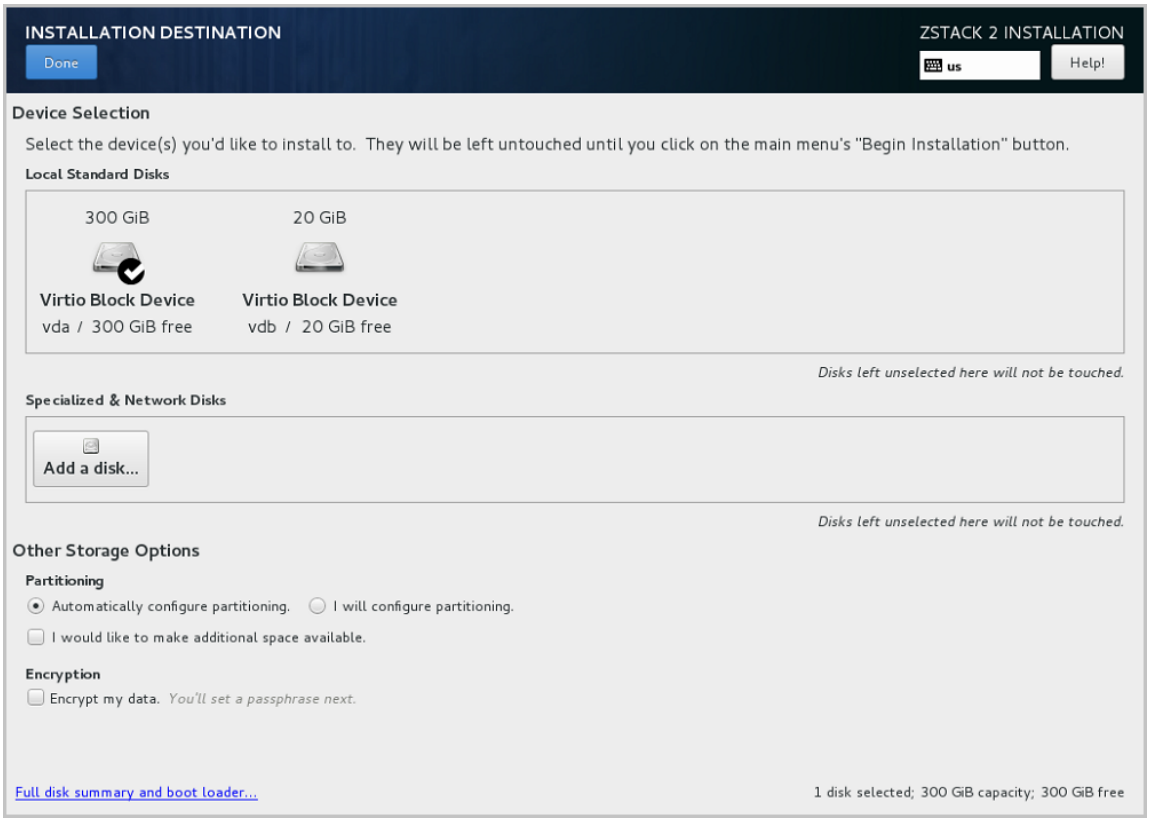
   Note:

   If you select **No ZStack Local Repo** on the right, the ISO will not be copied and no internal repositories will be produced. This saves the installation time efficiently.

e) Configure disk partitioning.

On the installation summary page, click **INSTALLATION DESTINATION**, and go to the disk partitioning configuration page, as shown in *Default Setting - Automatically Configure Partitioning*.

Figure 5-7: Default Setting - Automatically Configure Partitioning



Note:

When you install the OS, we recommend that you select only the hard disk or disks that are required by the system disk. You are not advised to select the hard disks that have special usage.

Default setting: **Automatically configure partitioning**. We recommend that you use the default setting to automatically configure the disk partitioning.

If you select "I will configure partitioning", we recommend that you do the following:

- Make sure that the partitioning mode (which includes UEFI and Legacy) is consistent with that configured by BIOS.
  - UEFI
    - */boot*: create a 1 GB partition

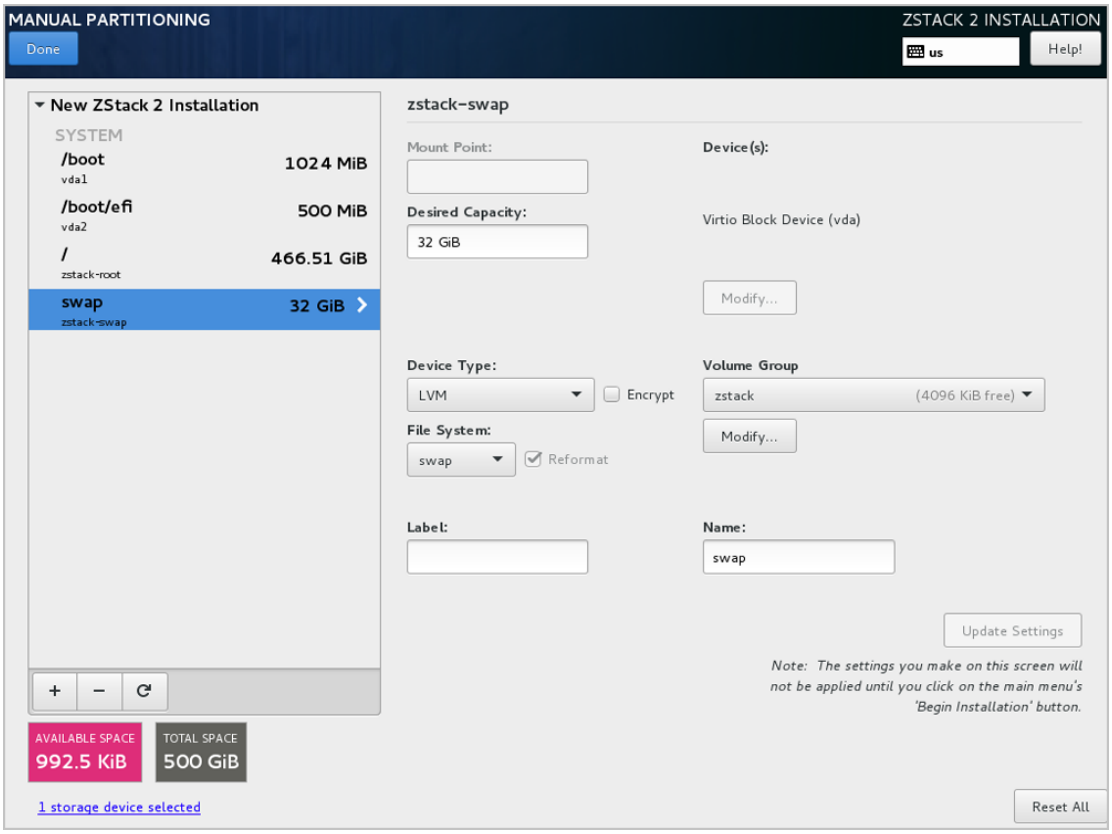
- */boot/efi*: create a 500 MB partition
- *swap* (exchange partition): create a 32 GB partition
- */* (root partition): configure the remaining capacity

— Legacy

- */boot*: create a 1 GB partition
- *swap* (exchange partition): create a 32 GB partition
- */* (root partition): configure the remaining size

- The preceding values are recommended partition sizes. (The total disk capacity is more than 300 GB.)
- In Legacy mode, the system disk capacity is more than 2 TB. In this mode, a BIOS boot partition needs to be configured to support the GPT partition. The UEFI mode can directly support the GPT partition, as shown in *UEFI Partition*.

Figure 5-8: UEFI Partition



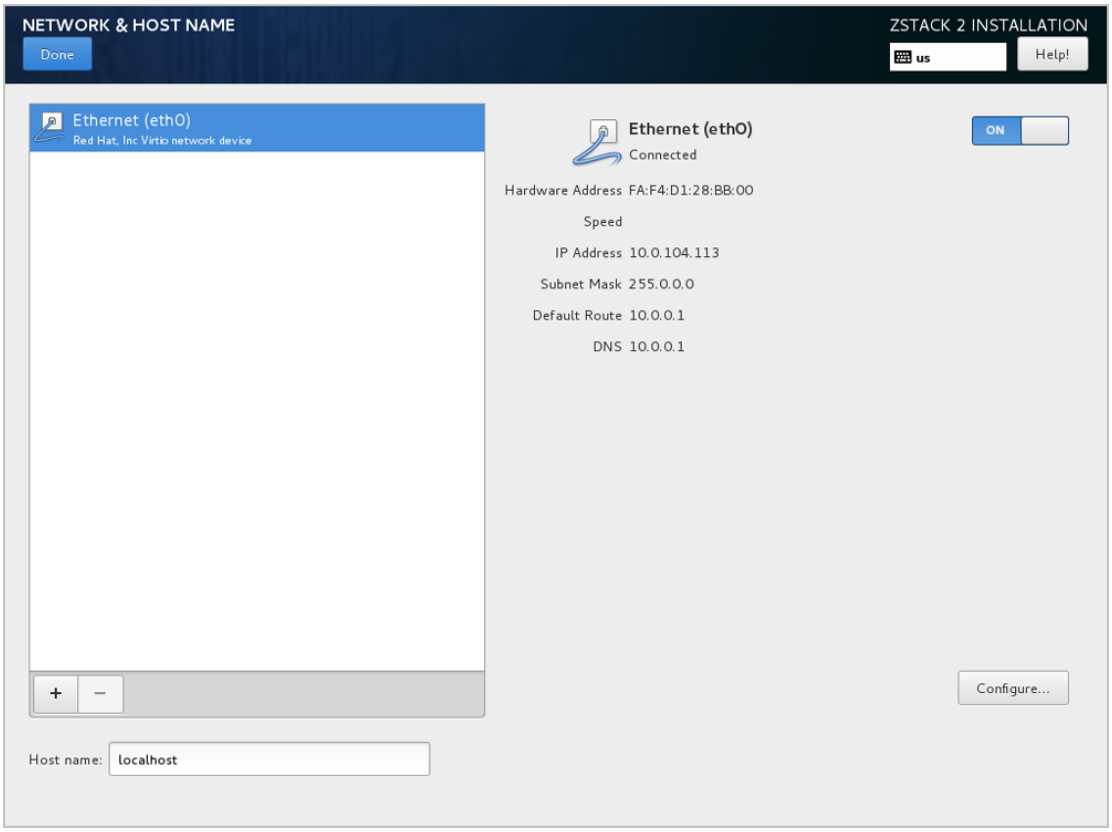
f) Configure the network.

1. Configure the NIC.

On the installation summary page, click **NETWORK & HOST NAME**, and go to the NIC configuration page, as shown in *NIC Configuration*.

1. Select the NIC to be configured, for example, **eth0**.
2. Check the obtained DHCP address.

Figure 5-9: NIC Configuration



2. Optional. Perform network bonding.

   If you install and deploy ZStack in your actual production environment, we recommend that you perform network bonding. This is because network bonding can improve the network bandwidth and network reliability. For more information about the network bonding procedure, see *Network Bonding*.

   For POC testing, you can proceed without network bonding.

3. If **eth0** cannot obtain the DHCP address, manually configure a static IP address for **eth0**.

   a. On the *NIC Configuration* page, select **Ethernet (eth0)**, click **Configure...**, and go to the **eth0** configuration page, as shown in *Configure a Static IP Address of eth0*.

   b. Choose the **IPv4 Settings** tab page under **eth0**.

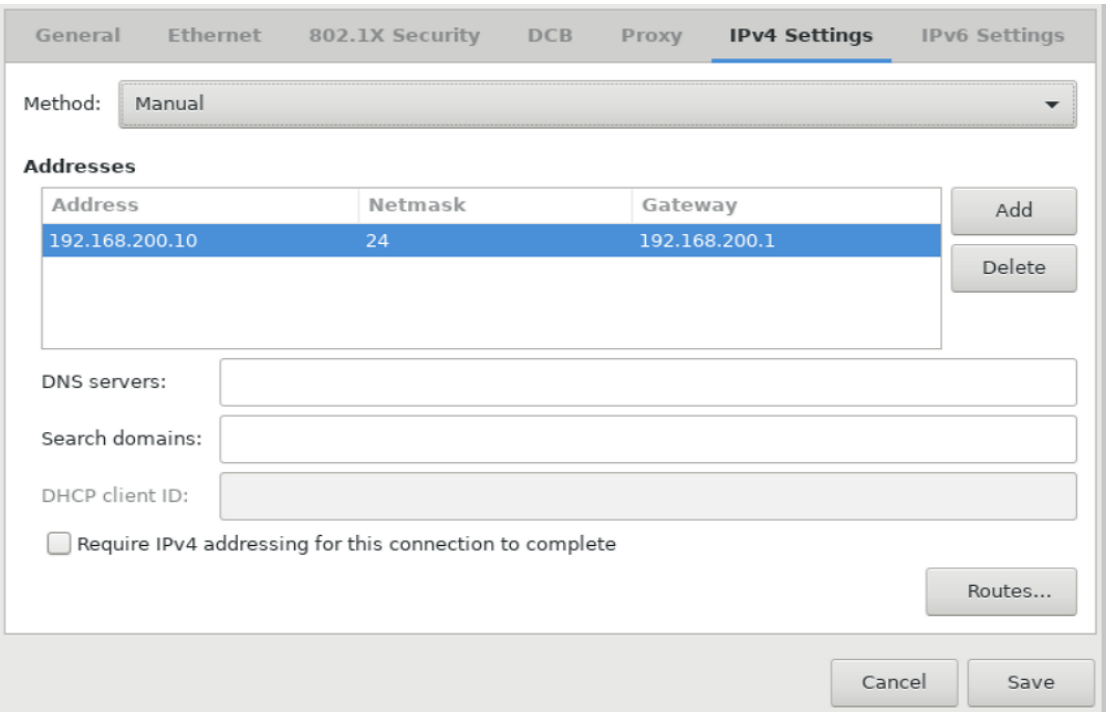
   c. From the **`Method`** drop-down list, select **Manual**.

d. Click **Add** to add new configuration items.

e. Configure the IP address of the NIC as needed.

f. Click **Save**.

Figure 5-10: Configure a Static IP Address for eth0



4. Configure eth0 to automatically connect to the network.

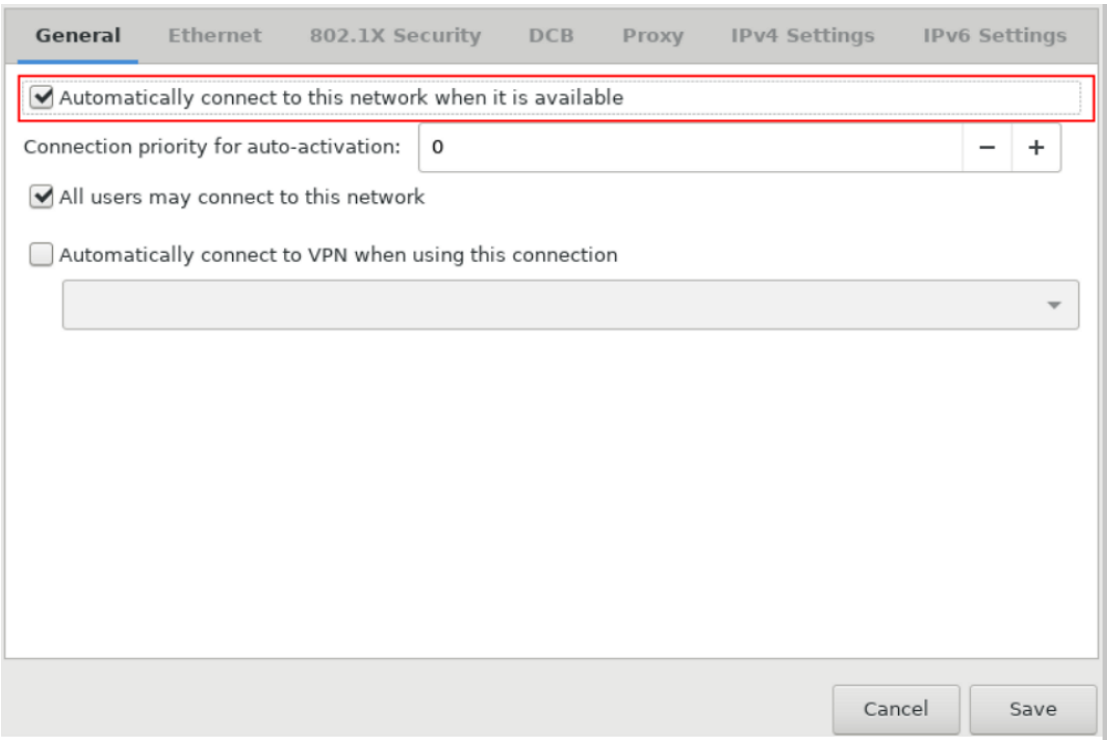
a. On the *NIC Configuration* page, select **Ethernet (eth0)**, click **Configure...**, and go to the **eth0** configuration page, as shown in *Configure eth0 to Automatically Connect to Network*.

b. Choose the **General** tab page.

c. Verify that you selected **Automatically connect to this network when it is available**.

d. Click **Save**.

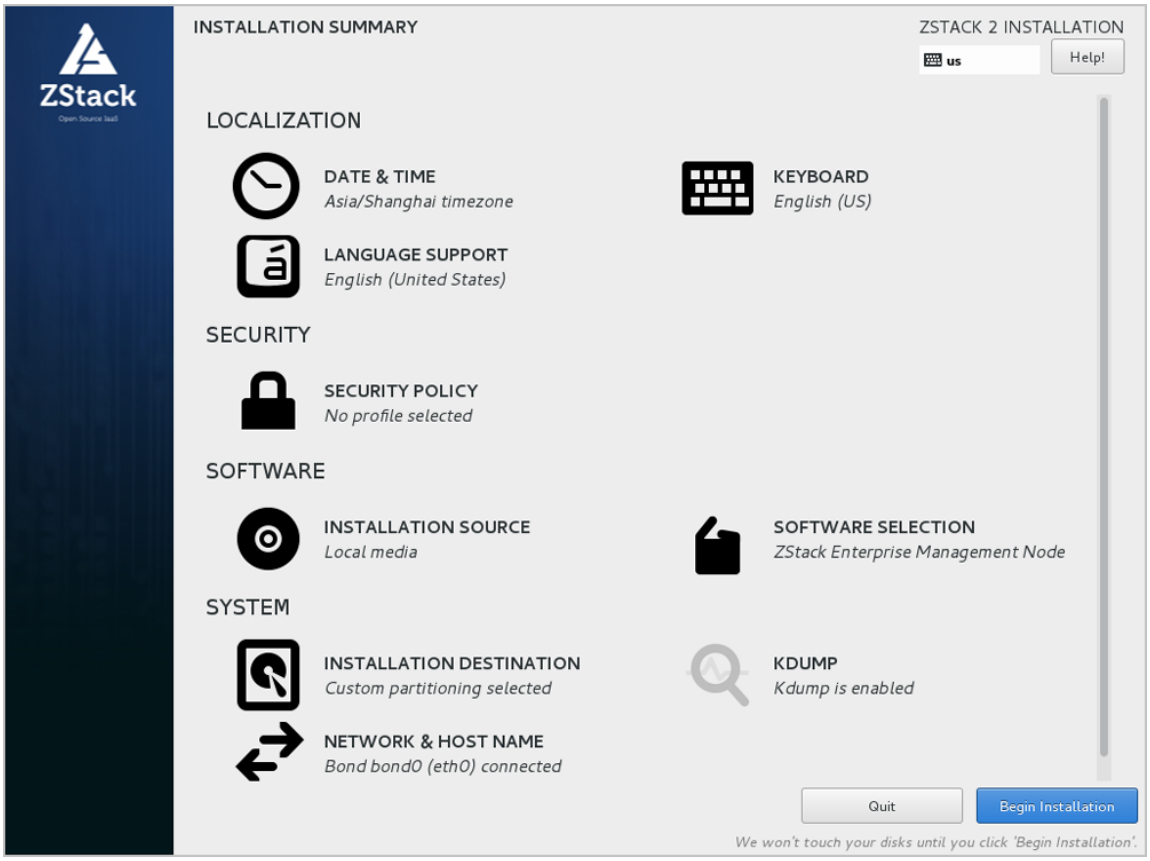
Figure 5-11: Configure eth0 to Automatically Connect to Network



g) After the network configuration is completed, go back to the installation summary page, and click **Begin Installation**.

As shown in *Begin Installation*.

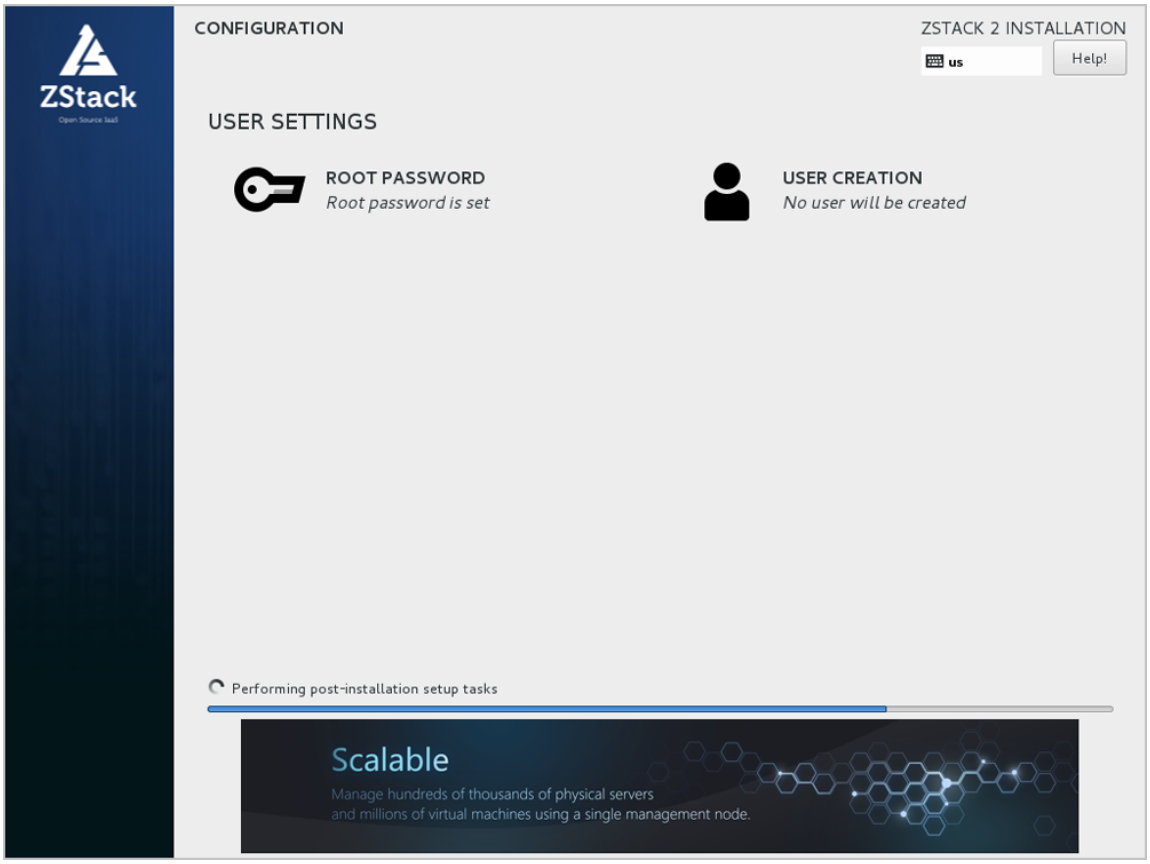
Figure 5-12: Begin Installation



h) Set **ROOT PASSWORD** during the automatic installation process.

As shown in *Configuration*.

Figure 5-13: Configuration



i) After the installation is completed, click **reboot**. Then, you can start and enter the system of ZStack Custom c76.

What's next

- If you select ZStack Enterprise Management Node, ZStack Community Management Node, or ZStack Compute Node, the system will automatically install the corresponding ZStack Installati on Package after rebooting.
- If you select ZStack Expert Mode, the system will enter a shell interface after rebooting. This method is applicable to advanced users who want to install the system in a custom way.

5.1.1 Network Bonding (Optional)

This topic mainly describes the configuration method of the network bonding. If you want to install and deploy ZStack in your real production environments, we recommend that you use the network bonding method to configure your networks. If you use the cloud for POC test only, skip this topic.

The network bonding has the following two configuration methods: command line and TUI.

Command Line Method

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

```
# Create a link aggregation virtual interface according to the LACP
mode.
zs-bond-lacp -c [bond-name]
zs-bond-lacp -c bond0

# Create another link aggregation virtual interface according to the
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
```

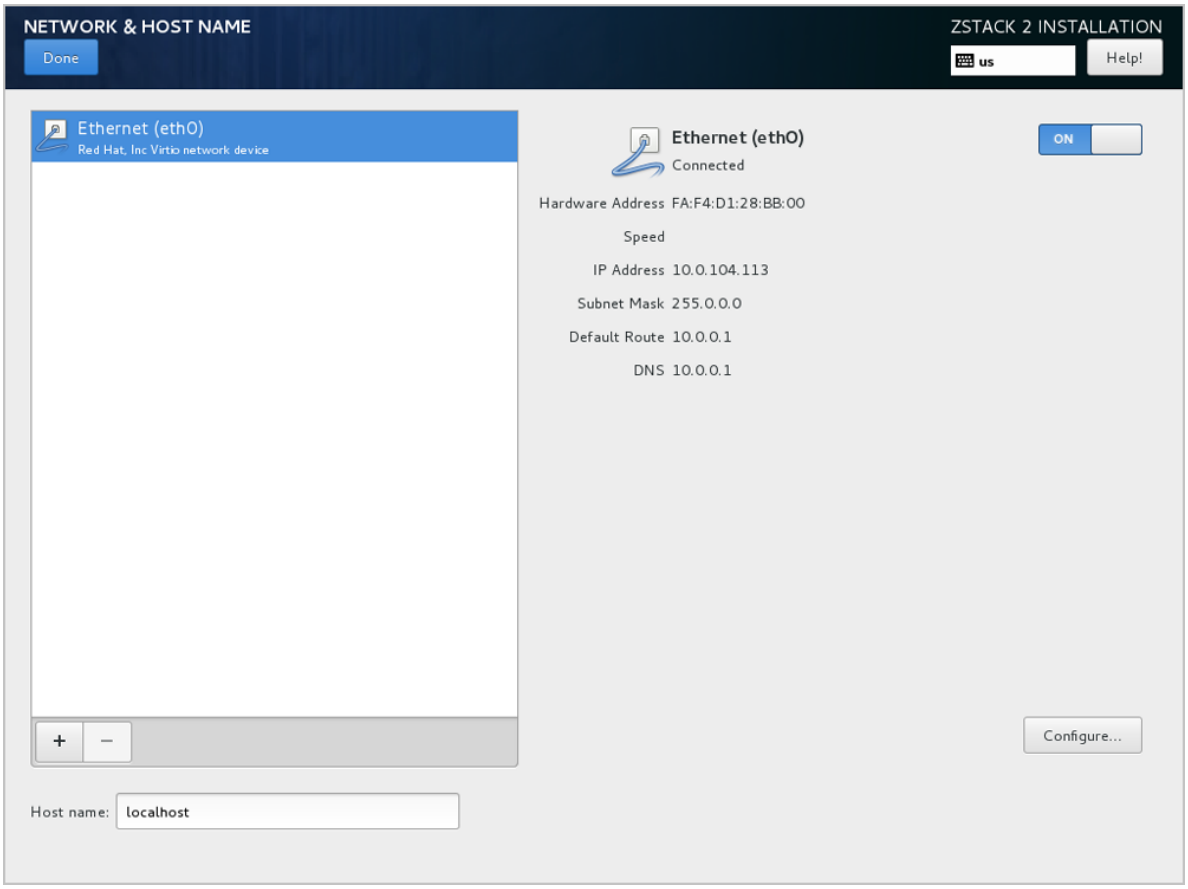
TUI Method

1. Configure NICs.

   On the installation summary page, click **NETWORK & HOST NAME**. Then, the main page of the NIC configuration is displayed, as shown in *Main Page of NIC Configuration*.

   1. Select the NIC that you need to configure, such as **eth0**.
   2. Enable the NIC by selecting **On**.
   3. Check the DHCP address that you have obtained.

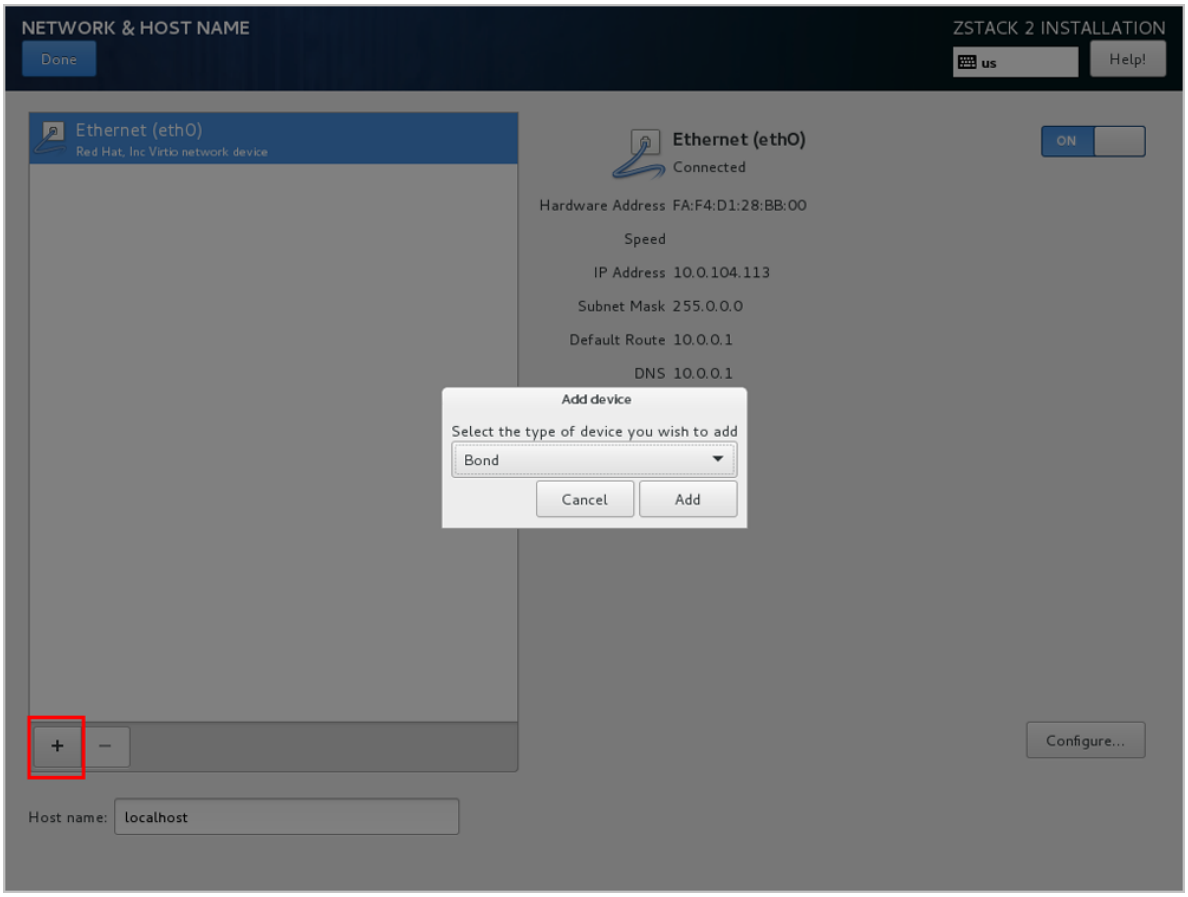
Figure 5-14: Main Page of NIC Configuration



2. Add a Bond device.

   Click the plus sign (**+**) at the lower left, select **Bond** from the prompted **Add device** drop-down list, and click **Add**, as shown in *Add a Bond Device*.

Figure 5-15: Add a Bond Device



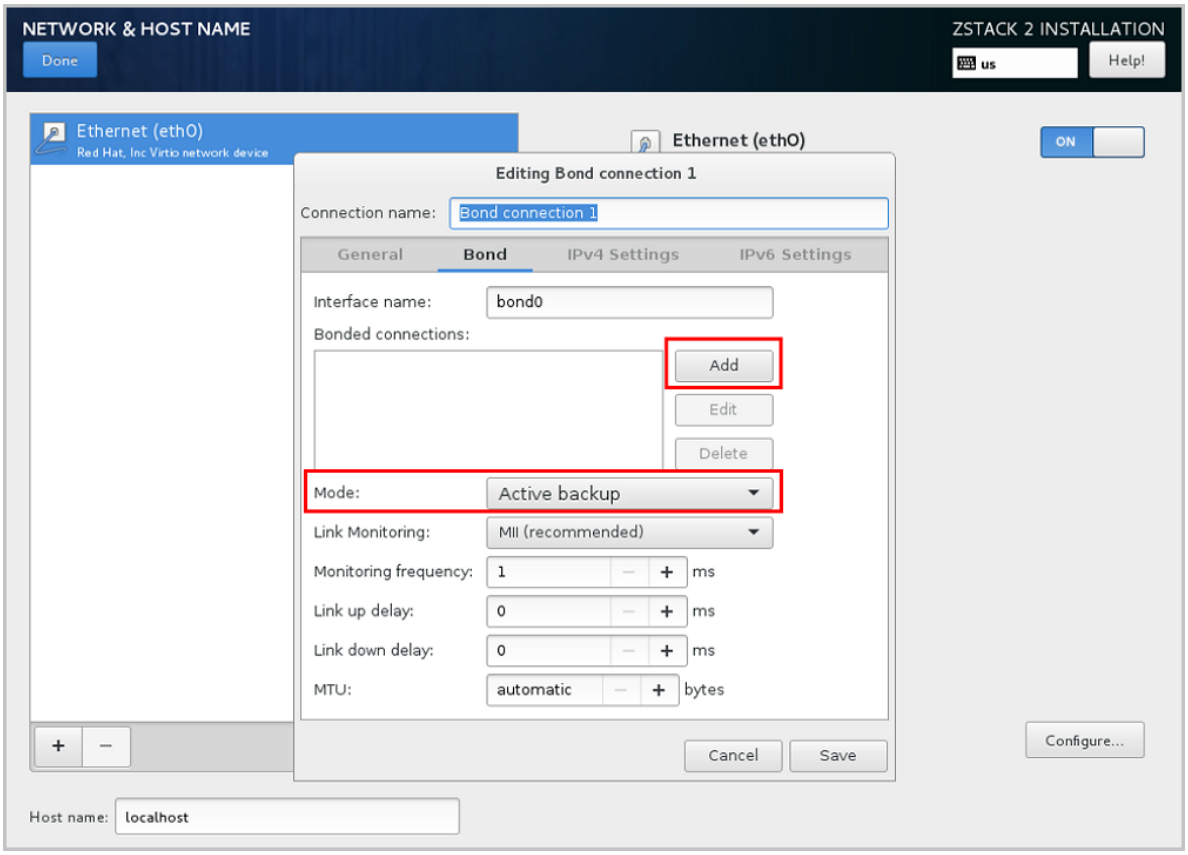
3. Configure Bond.

   You need to manually make two configurations as follows on the **Bond** tab of the prompted **Editing Bond connection 1** page, as shown in the *Configure Bond*.

   - **Add**: Add Bond Slave, as shown in *Add Bond Slave*.
   - **Mode**: Select the Bond mode, as shown in *Select Bond Mode*.

   For other options, you can either use the default settings or customize your settings as needed.

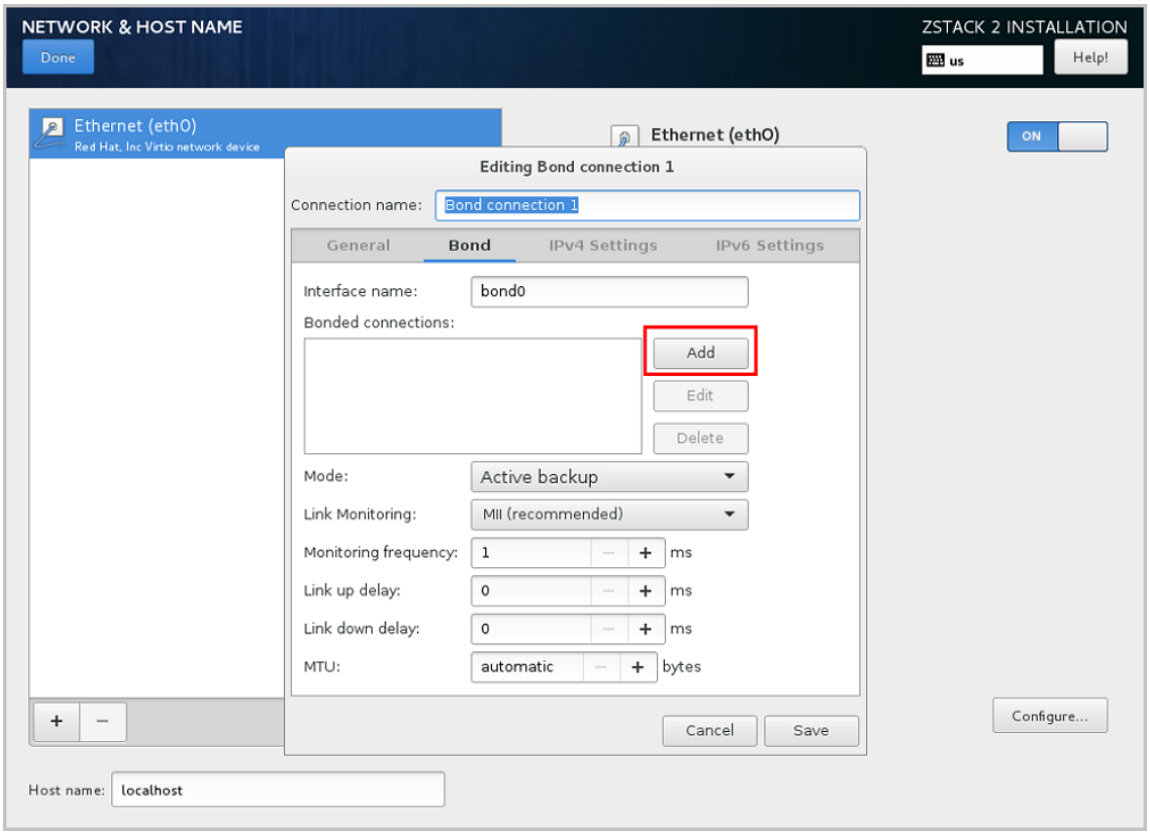
Figure 5-16: Configure Bond



4. Add Bond Slave.

   - On the Bond tab, click **Add** to add Bond Slave, as shown in *Add Bond Slave*.

Figure 5-17: Add Bond Slave

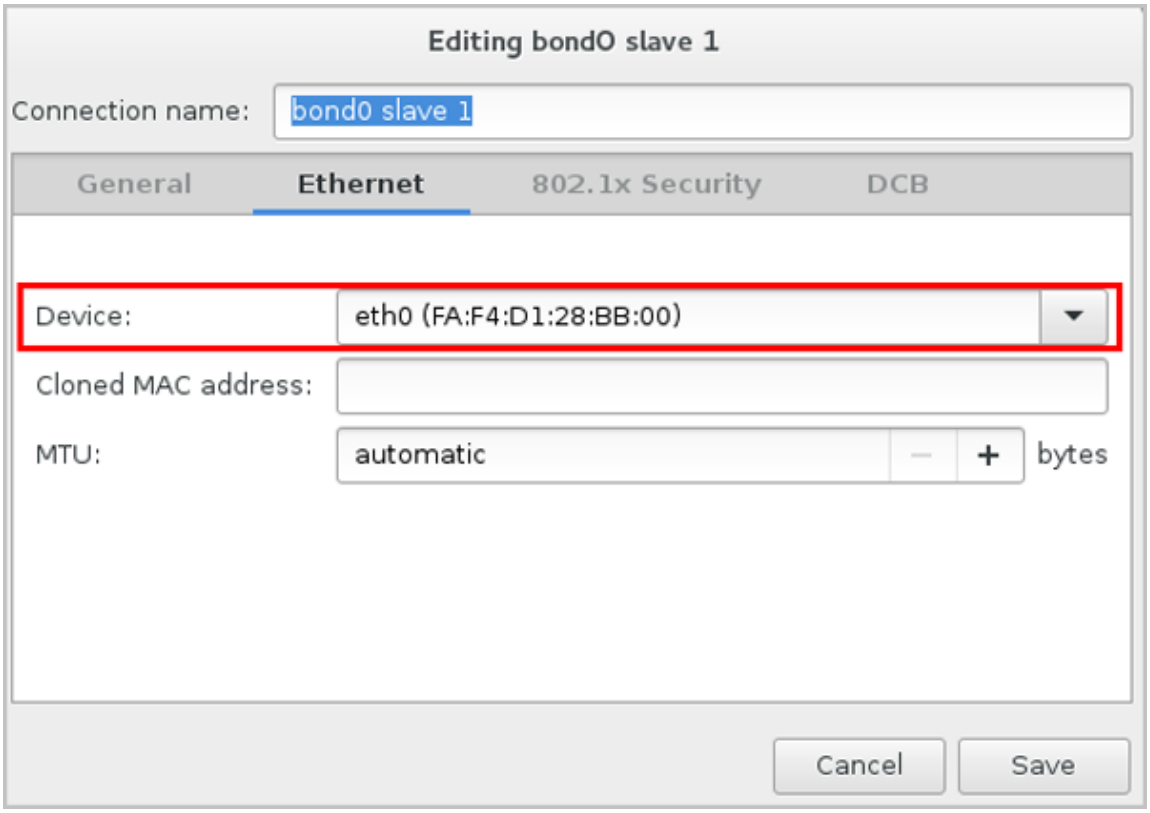


- On the displayed **Choose a Connection Type** page, select a connection type for the Bond Slave, such as **Ethernet**, and click **Create...**, as shown in *Select Connection Type for Bond Slave*.

Figure 5-18: Select Connection Type for Bond Slave

- On the **Ethernet** tab of the **Editing bond0 slave 1** page, select the Slave device that needs to be bound from the **`Device`** drop-down list, such as **eth0 (the corresponding MAC address)**. On the **Ethernet** tab, you can use the default settings or customize your settings as needed. Finally, click **Save**, as shown in *Select Bond Slave Device*.

Figure 5-19: Select Bond Slave Device

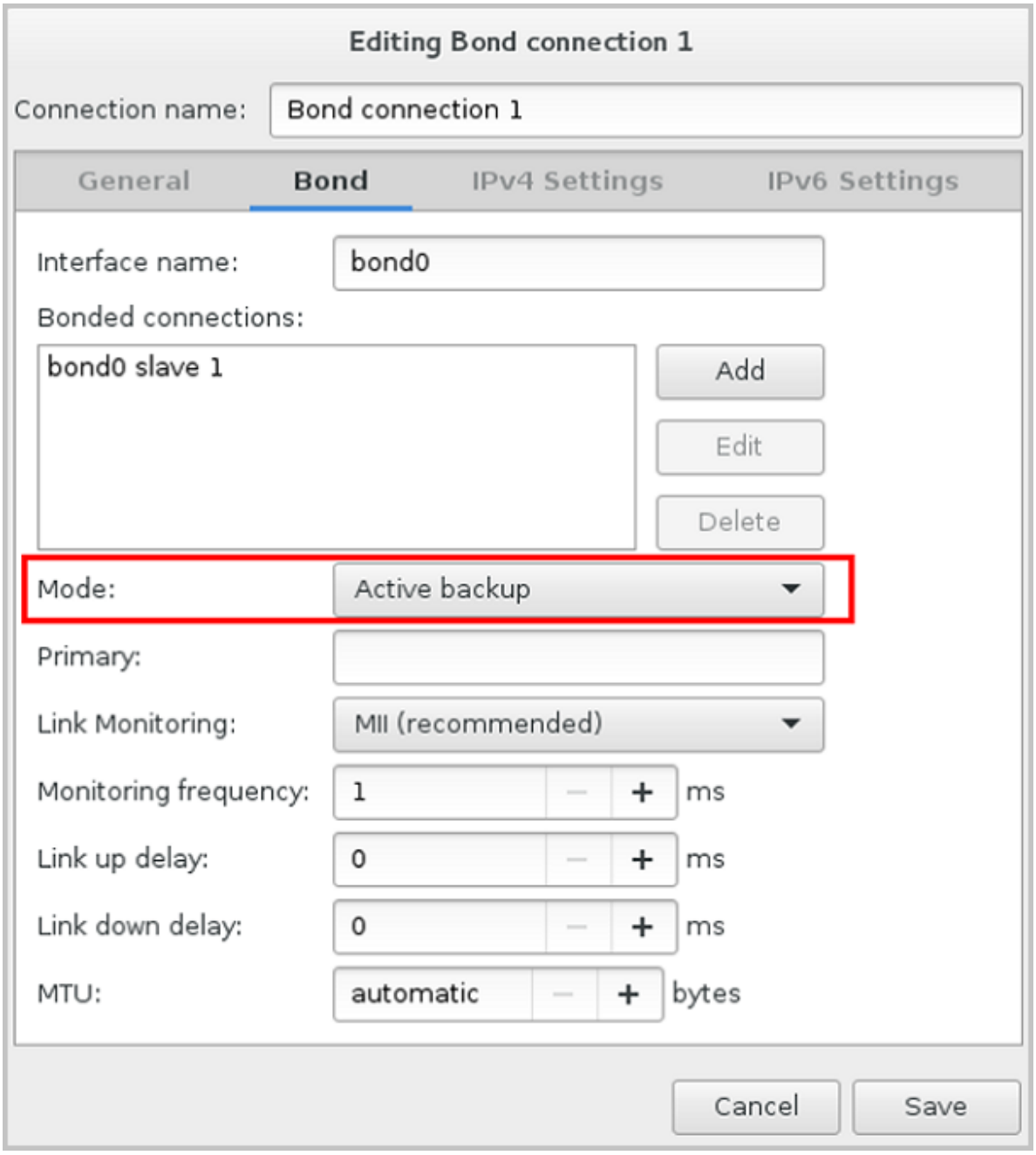


- So far, Bond Slave is added successfully.

5. Select the Bond mode.

From the **`Mode`** drop-down list of the Bond tab, select the Bond mode as need, such as **Active backup**. On the Bond tab, you can use the default settings or customize your settings as needed. Finally, click **Save**, as shown in *Select Bond Mode*.

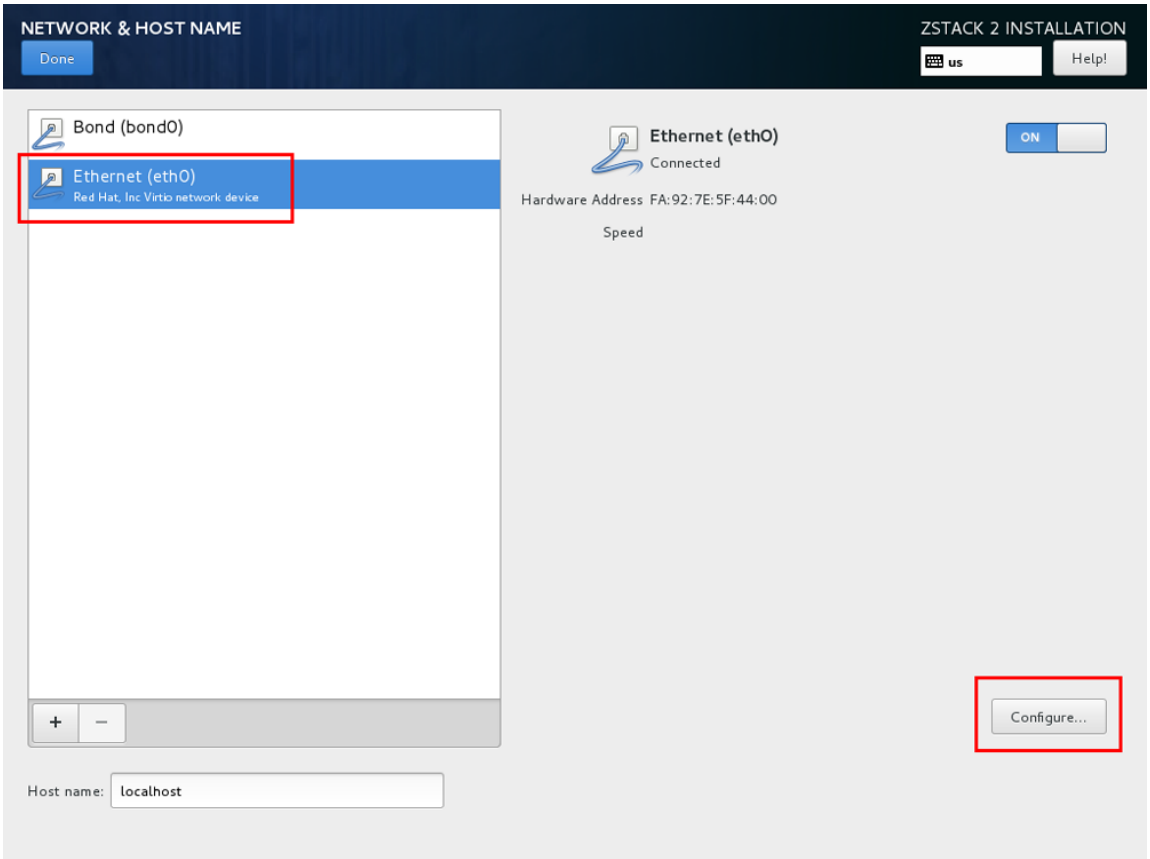
Figure 5-20: Select Bond Mode



6. Disable the IPv4 settings of Bond Slave.

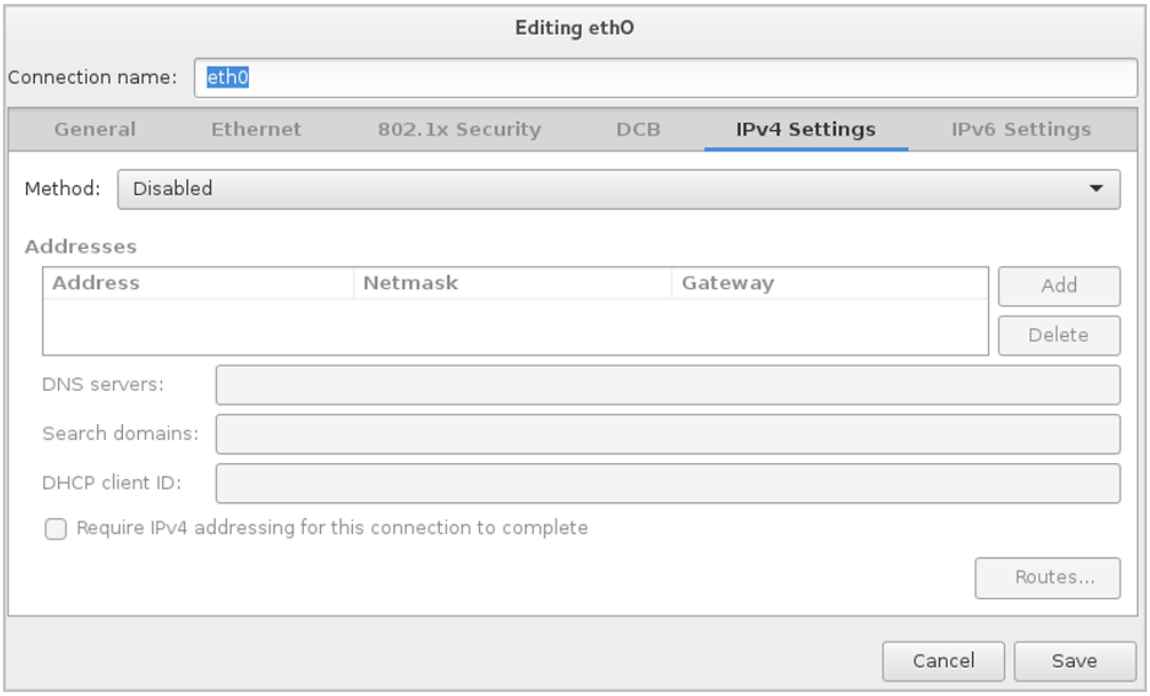
   - Go back to the main page of the NIC configuration, select Bond Slave such as eth0, and click **Configure...**, as shown in *Open Configuration Page of Bond Slave*.

Figure 5-21: Open Configuration Page of Bond Slave



- On the **IPv4 Settings** tab in the **Editing eth0** page, select **Disabled** from the **`Method`** drop-down list, and click **Save**, as shown in *Disable IPv4 Settings of Bond Slave*.

Figure 5-22: Disable IPv4 Settings of Bond Slave

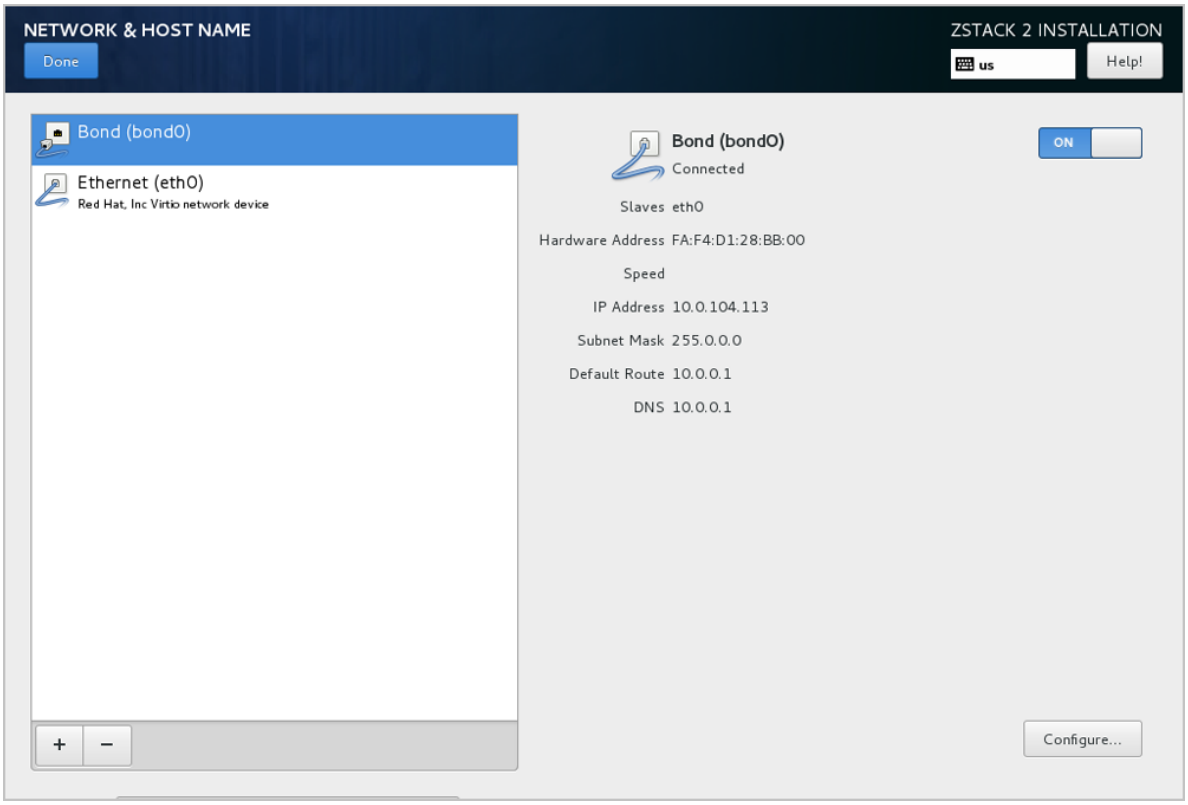


7. Complete the network bonding.

   As shown in *Complete Network Bonding*.

> **Note:**
>
> To check Bond configuration options, verify that you have selected **On** and configured the IP address. At the same time, make sure that Bond Slave such as eth0 has been enabled by selecting **On**. Or otherwise, you might fail to install ZStack properly.

Figure 5-23: Complete Network Bonding



8. If the Bond device cannot obtain DHCP addresses, you need to manually configure the static addresses of the Bond device.

   a. On the *Main Page of NIC Configuration*, select **Bond (bond0)**, and click **Configure...** to open the Bond configuration page, as shown in *Configure Static IP Address of Bond Device*.

   b. Go to the **IPv4 Settings** tab of the Bond device.

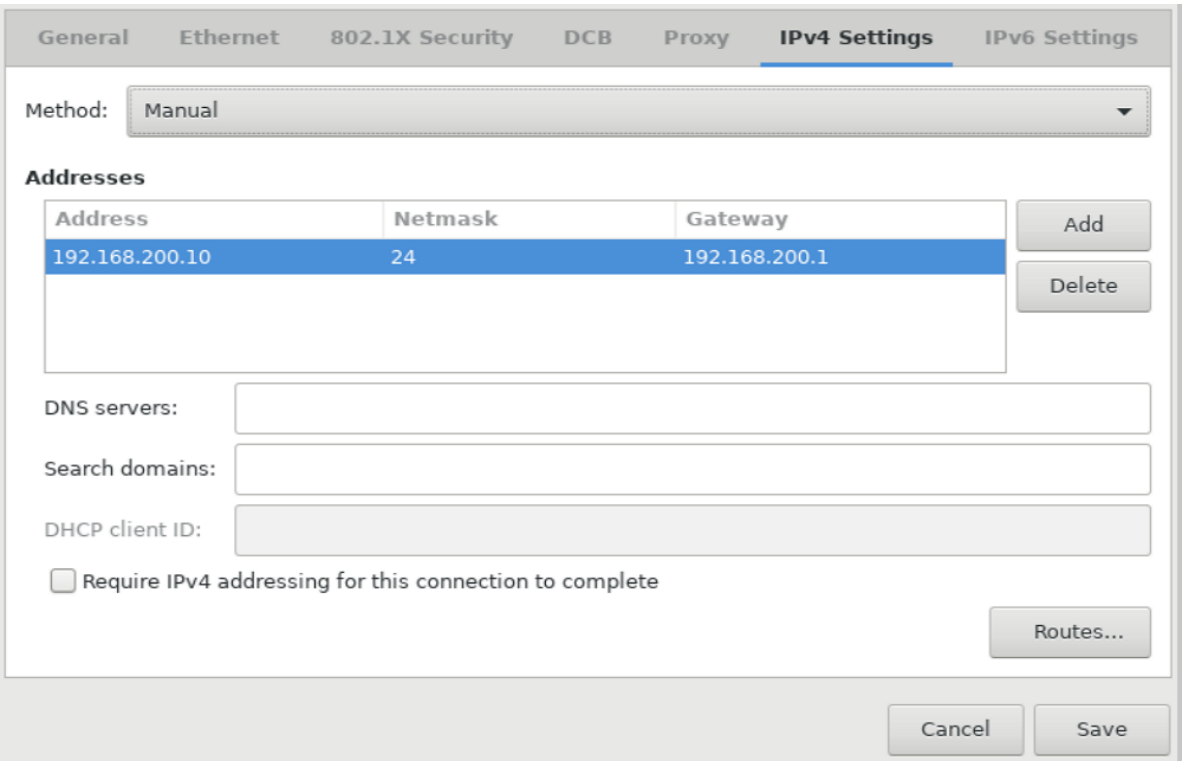
   c. From the **`Method`** drop-down list, select **Manual** to make manual configurations.

   d. Click **Add** to add new configuration items.

   e. Configure the NIC address information as needed.

   f. Click **Save** to save your configurations.

Figure 5-24: Configure Static IP Address of Bond Device



9. Configure the automatic connection for the Bond device.

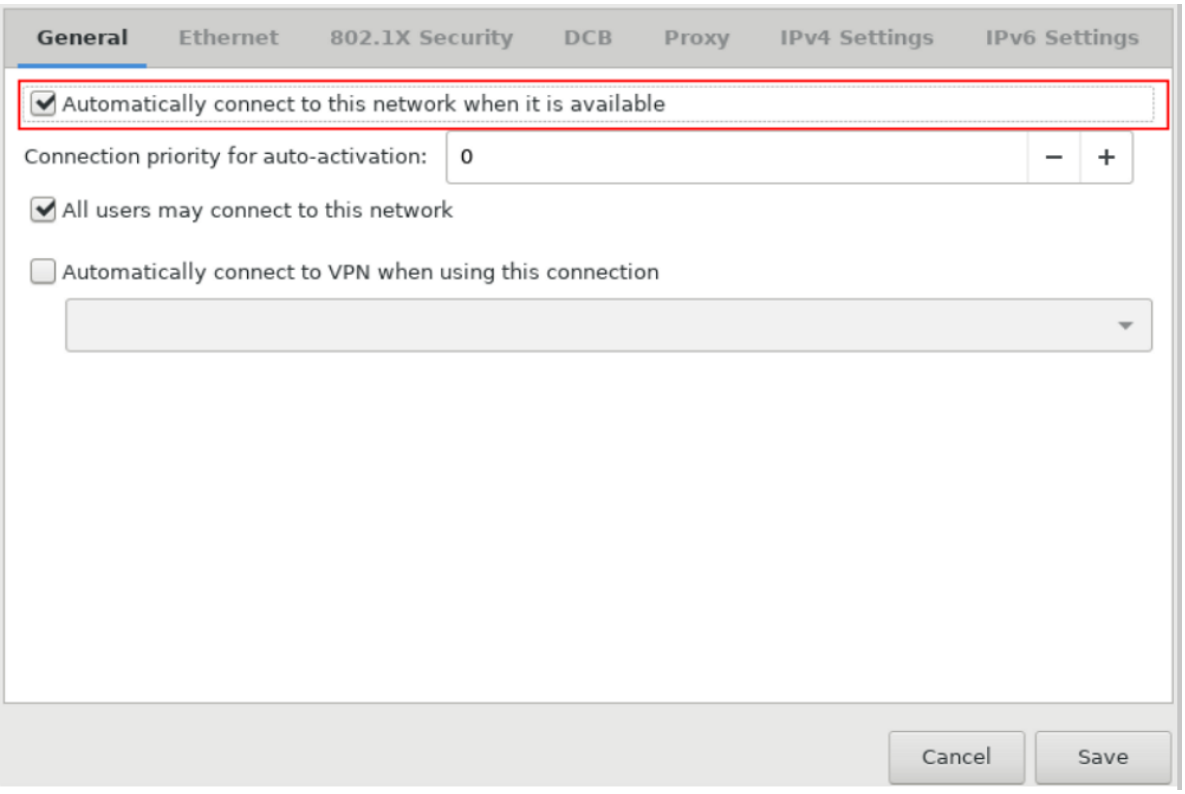
   a. On the *Main Page of NIC Configuration*, select **Bond (bond0)**, and click **Configure...** to open the Bond configuration page, as shown in *Configure Automatic Connection for Bond*.

   b. Go to the **General** tab.

   c. Make sure you selected **Automatically connect to this network when it is available**.

   d. Click **Save** to save your settings.

Figure 5-25: Configure Automatic Connection for Bond



10. So far, we have introduced the network configuration method based on the network bonding.

5.2 Install ZStack

This topic mainly describes four installation modes of ZStack 3.10.0 and the TUI features.

ZStack TUI Introduction

ZStack TUI is a set of UIs prepared for physical servers in ZStack clusters. The significance of the TUI includes the following two aspects:

- **Distribute a portion of UI features.**

  To uniformly display on the TUI, operations such as configuring passwords for servers, configuring networks, and rebooting servers are ripped out from the UI.

- **Lower the frequency that an administrator logs in to servers.**

  For this feature, you can lower the maintenance difficulties of hosts. In addition, you can protect the internal configurations of the hosts from being damaged.

You can enter the command line mode by pressing **Ctrl + Alt + F2**, and exit the mode by pressing **Ctrl + Alt + F1**. In addition, you can enter the reserved terminal by pressing **Ctrl + Alt + F11** to

run common commands. Exercise caution when you use the terminal. Doing so may damage the system and influence the running ZStack services.

Four Installation Modes of ZStack Custom ISO

ZStack Custom ISO provides the following four installation modes:

- ZStack Enterprise Management Node
- ZStack Community Management Node
- ZStack Compute Node
- ZStack Expert Node

The procedures of the four installation modes are as follows:

1. **ZStack Enterprise Management Node**
   - Install the base system.
   - Install MariaDB, CloudBus, and other dependency packages.
   - Install the TUI of ZStack Enterprise Management Node.
   - Automatically install and start the ZStack and its UI.
2. **ZStack Community Management Node**
   - Install the base system.
   - Install MariaDB, CloudBus, and other dependency packages.
   - Install the TUI of ZStack Community Management Node.
   - Automatically install and start the ZStack and its UI.

   Note:

   - The difference between ZStack Enterprise Management Node and ZStack Community Management Node: **Different licenses have their different corresponding features.**
   - In terms of the installation procedure, both ZStack Enterprise Management Node and ZStack Community Management Node are the same.
3. **ZStack Compute Node**
   - Install the base system.
   - Install libvirt, QEMU, and other virtual components.
   - Install the TUI of ZStack Compute Node.
4. **ZStack Expert Node**

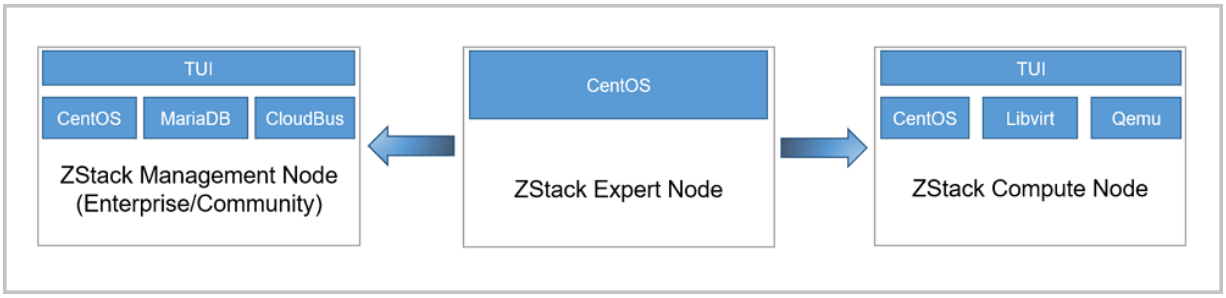
- Install the base system.

Note:

- ZStack Expert Node is equal to the minimum installation mode of CentOS 7.x.
- When you need to make deeper customizations for your clouds, select ZStack Expert Node and then manually transform it to one of the three installation modes.

The four installation modes are shown in *Diagram of Four Installation Modes*.

Figure 5-26: Diagram of Four Installation Modes



Different installation modes can be applied to different installation scenarios, as shown in *Installation Scenarios*.

Table 5-1: Installation Scenarios

Mode	Scenario
ZStack Enterprise Management Node	Only applies to install ZStack Enterprise Management Node.
ZStack Community Management Node	Only applies to install ZStack Community Management Node.
ZStack Compute Node	Applies to install other nodes apart from the management node in the cloud. For example, • Compute node. • ImageStore backup storage, SFTP backup storage, Ceph backup storage node, and Mount node of Ceph backup storage. • Ceph primary storage node and Mount node of Ceph primary storage. • PXE server node, local backup storage node, and remote backup storage node (offsite).
ZStack Expert Node	

5.2.1 ZStack (Enterprise/Community) Management Node

This topic mainly describes ZStack Enterprise Management Node and ZStack Community Management Node. We will elaborate on their features and usage methods with a focus on the TUI of management nodes. As previously state, we have covered:

- The difference between ZStack Enterprise Management Node and ZStack Community Management Node: **Different Licenses have their different corresponding features.**
- In terms of the installation procedure, both ZStack Enterprise Management Node and ZStack Community Management Node are the same.

Automatically Install ZStack Management Node

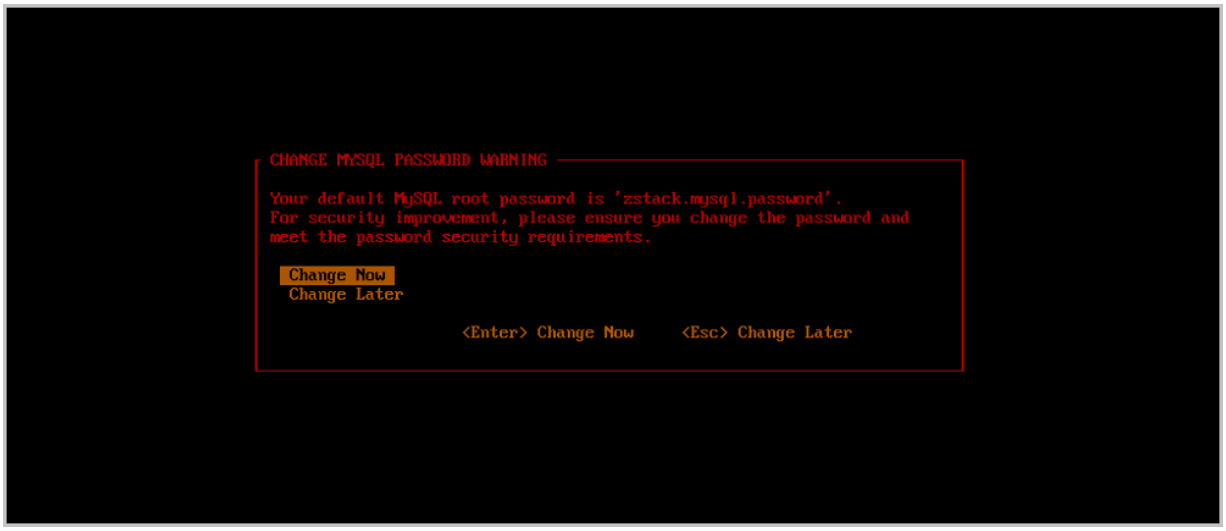
If you select ZStack Enterprise/ZStack Community Management Node, ZStack management nodes will be automatically installed after rebooting.

Figure 5-27: Automatically Install Management Node

Page of Changing MySQL Password

After you install the cloud, you will jump to the page that notifies you to change your MySQL password. Select **Change Now** to immediately change your MySQL password, or select **Change Later** to not change your MySQL password.

Figure 5-28: Page of Changing MySQL Password



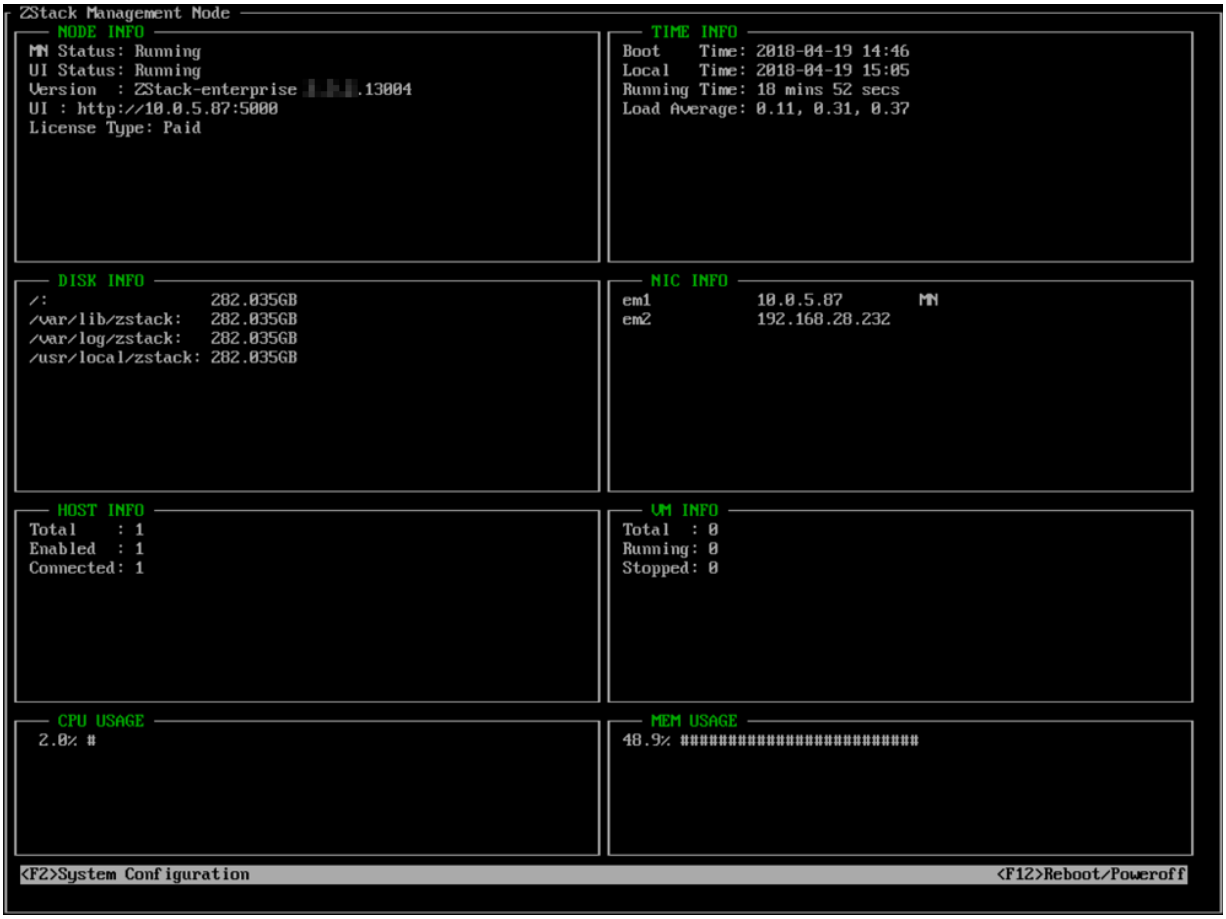
Note:

Your new password must contain at least 8 characters, including alphabetic, numeric, and special characters.

TUI Main Page of Management Node

The TUI main page of the management node provides a real-time display of the main information for the host.

Figure 5-29: TUI Main Page of Management Node



- **NODE INFO**:

  Display the current state of the management node, including whether the service is running, whether the UI is running, the version of ZStack, the UI address, and the license type.

- **TIME INFO**:

  Display the time when the server was started, the current time, the running time of the server, and the average load balancing of the server.

- **DISK INFO**:

  Display the remaining disk space of the default installation directory and the log directory.

- **NIC INFO**:

  Display all the NIC information of the management node, including the physical NIC and the logical NIC. Specifically, DOWN means that the NIC is disabled, UP means that the NIC is enabled, and MN means that the NIC is the management NIC.

- **HOST INFO**:

Display the number of management nodes in the current cluster. Specifically, you will know how many management nodes are **Enabled** or **Connected**.

- **VM INFO**:

  Display the number of VM instances in the current cluster. Specifically, you will know how many VM instances are **Running** or **Stopped**.

- **CPU USAGE** and **MEM USAGE**:

  Display the real-time resource utilization of the management node.

> **Note:**
>
> The bottom of the main page provides two entrances: **System Configuration** and **Reboot/Poweroff**. Press **F2** or **F12** to go to the corresponding page as prompted.

System Password

On the main page, when you press **F2** or **F12**, enter the system password first. Because either **System Configuration** or **Reboot/Poweroff** belongs to privilege operations.

The following page is an example of entering the system password. **Enter the root password as prompted and press the Enter key.**

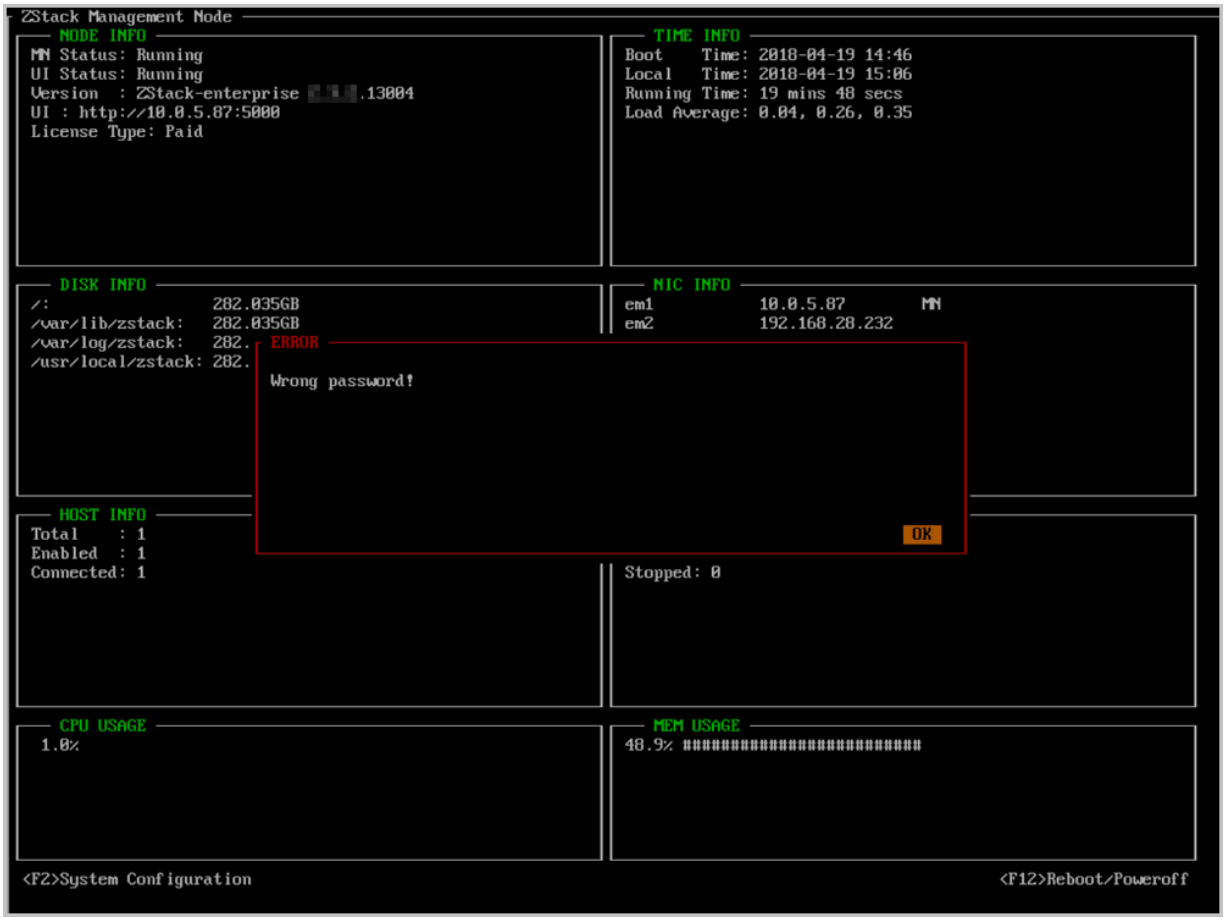
Figure 5-30: Enter Password

If the password that you entered is incorrect, this operation will be stopped. As a result, you will go back to the TUI main page.

Note:

Whenever you press the ESC key, you can exit the current page, and go back to the system configuration page.

Figure 5-31: Wrong Password



System Configuration

The features of the system configuration include:

- Change passwords.
- Rename NICs.
- Test networks.
- Configure networks.
- Set management networks.
- Configure console proxies.
- Back up databases.
- Start, stop, or restart ZStack services.
- Reset ZStack services.
- Reset ZStack services and drop databases.
- Display terminal information.

Note:

- The system configuration page provides multiple system configuration entrances. **Use the up and the down arrow keys to move your cursor, select the configuration buttons you need, and press the Enter key to go to the corresponding configuration page.** For those who are familiar with Vim, you can also use the **j** and **k** keys to move your cursor up and down.
- Press **F2** to go back to the main page as prompted. When you go back to the system configuration page again, you need to reenter the root password.

Figure 5-32: System Configuration

Next, we will elaborate on each feature item of the system configuration one by one.

1. **Change passwords**.

   Move your cursor to **Change Passwords**, and press **Enter** to go to the password configuration page.

   This configuration item allows you to change the following three passwords:

1. Change the system root password.
2. Change the MySQL password of the root account.
3. Change the MySQL password of the ZStack account.

Figure 5-33: Three Passwords Can Be Changed

We will elaborate on how to change these three passwords.

1. Change the system root password.

   Enter the old password and new password, confirm the new password as prompted, and press **Enter**.

Figure 5-34: Change System Root Password

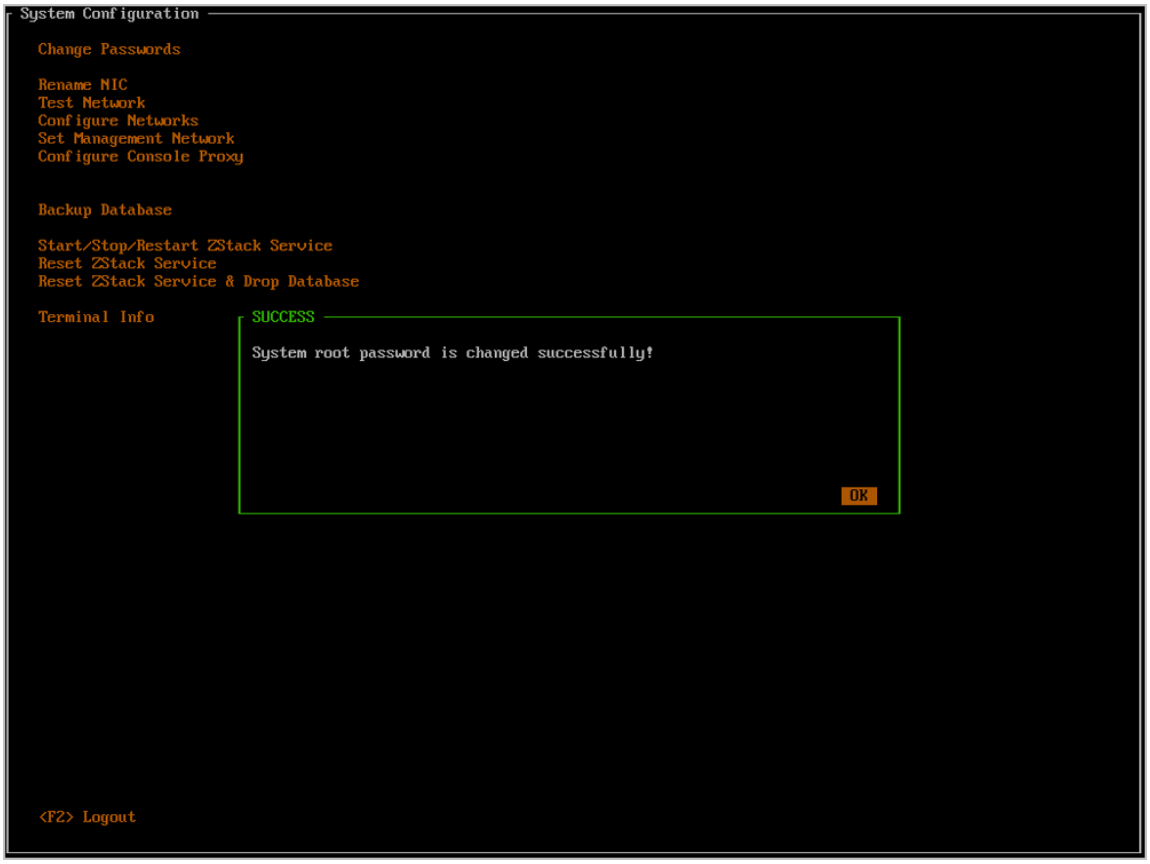
If the old password is incorrect, or if the new password you entered the first time is inconsistent with that you entered the second time, the error page will be prompted.

Figure 5-35: Error Page

Press **Y** to confirm your settings as prompted. Then, you succeeded in changing your system root password.

Figure 5-36: Confirmation Page of Changing System Root Password

Figure 5-37: Succeed in Changing System Root Password



2. Change the MySQL password of the root account or ZStack account.

   - To change the MySQL password of the root account or ZStack account, you need the root permission of MySQL. In this regard, **enter the MySQL root password first**, enter the new password, and confirm the password according to the prompt. Finally, press **Enter** to complete the change.
   - If the MySQL root password is incorrect, or if the new password you entered the first time is inconsistent with that you entered the second time, the error page will be prompted.
   - ZStack services will be restarted, which is time-consuming. Press **Y** to confirm the operation.

Figure 5-38: Change MySQL Password of Root Account or ZStack Account

2. Rename NICs.

   Move your cursor to **Rename NIC**, and press **Enter** to enter the page of renaming NICs.

   - You can change the NIC name on this page.
   - After you complete the change, press **Enter**. This operation requires you to press **Y** to confirm.

Figure 5-39: Rename NIC

3. Test networks.

   Move your cursor to **Test Network**, and press **Enter** to enter the page of testing networks.

   Default PING address: *114.114.114.114*, which can be used to test the Internet connections. If you need to test the internal network connections, enter manually the internal IP address.

Figure 5-40: Test Networks

4. Configure networks.

   Move your cursor to **Configure Networks**, and press **Enter** to enter the page of configuring networks.

Figure 5-41: Configure Networks

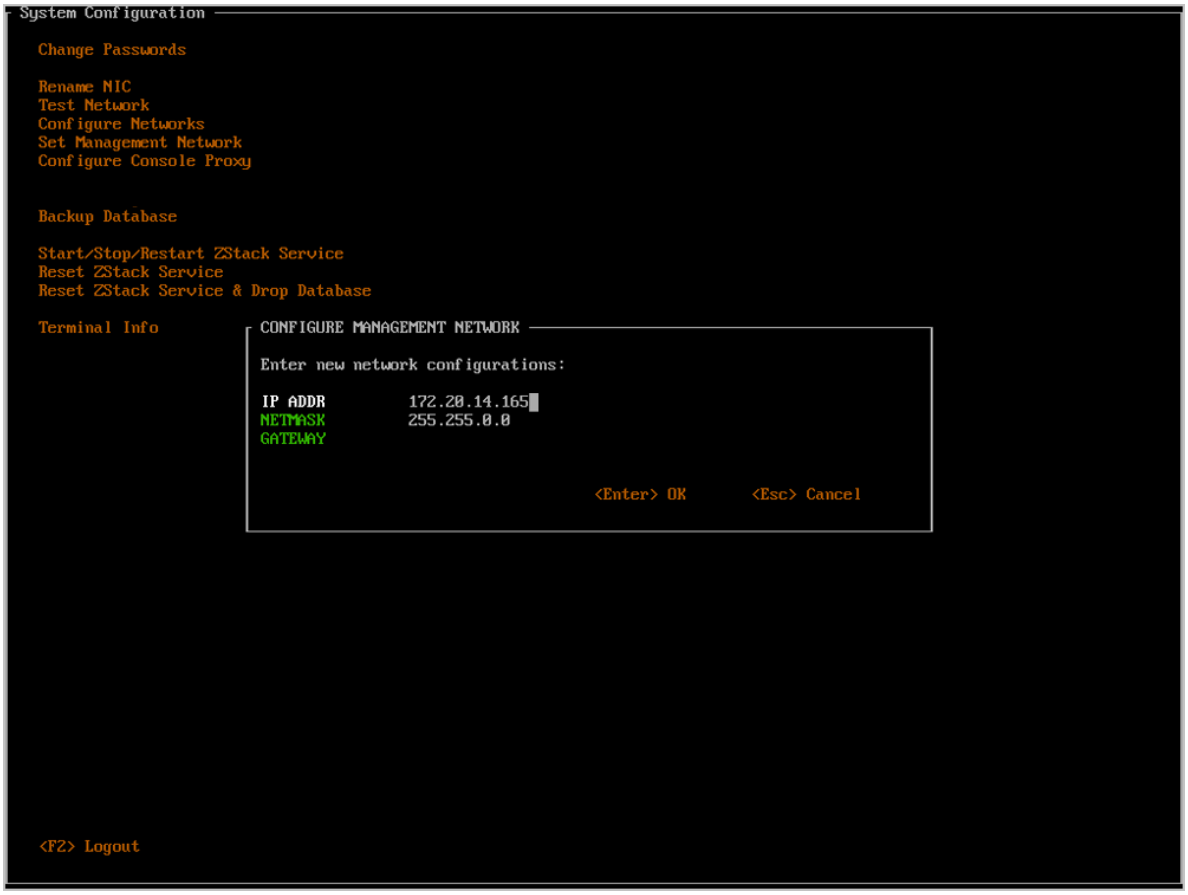
This page lists all the NICs that are in the enabled state in the management node, including the physical NIC and the logical NIC. For this operation, you need to focus on only the Bond configuration.

Move your cursor to the target Bond device, and press **Enter** to enter the configuration page of the Bond device.

Note:

If the target Bond device is tagged with MN, you need to change the management network configuration, which is time-consuming. Exercise caution when you perform this operation.

Figure 5-42: Enter Information

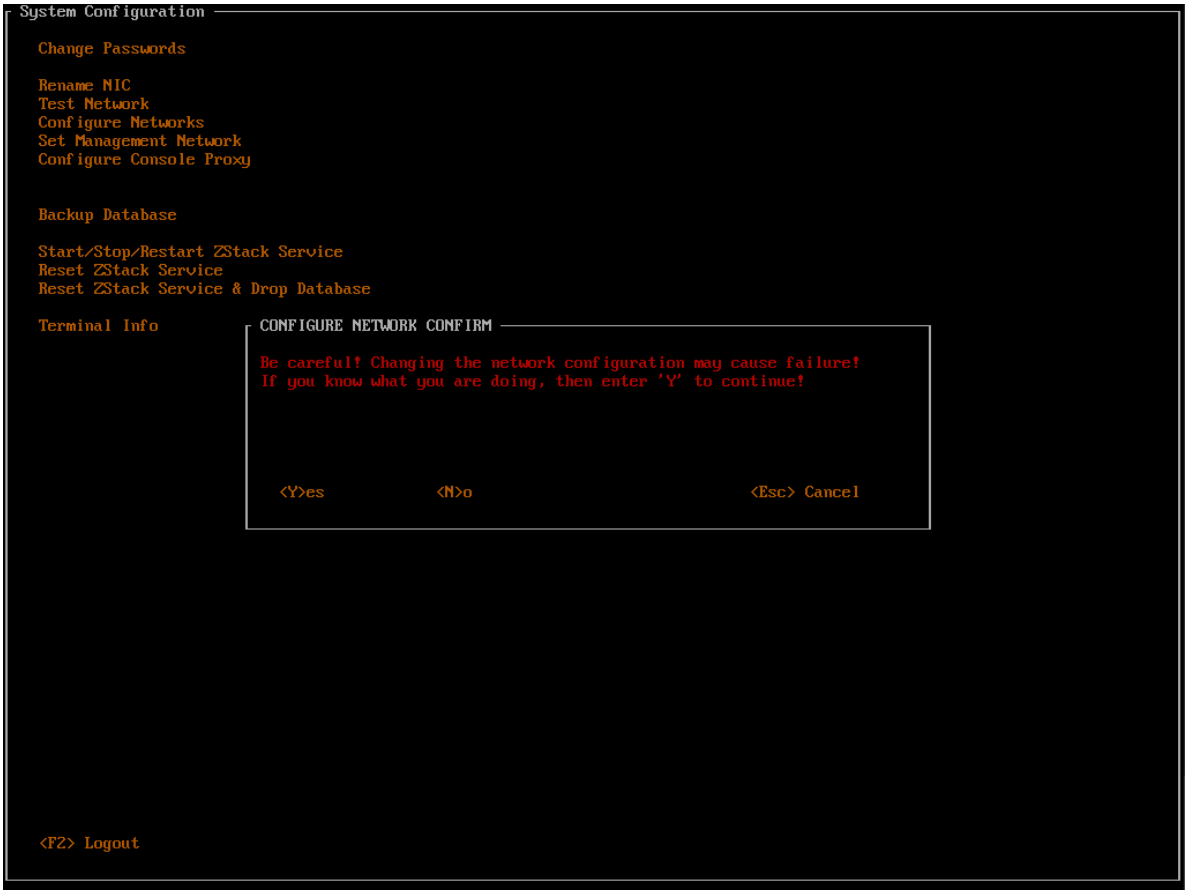


The existing Bond device that you selected will be displayed by default on the message box except for the gateway. You can make configurations for the device as needed.

If any one of the following conditions happens, input errors will be reported:

- An or some input items are null.
- An or some input items are invalid IP addresses.
- Both IP addresses and the gateway are not in the same subnet determined by the netmask.

Figure 5-43: Confirmation Page



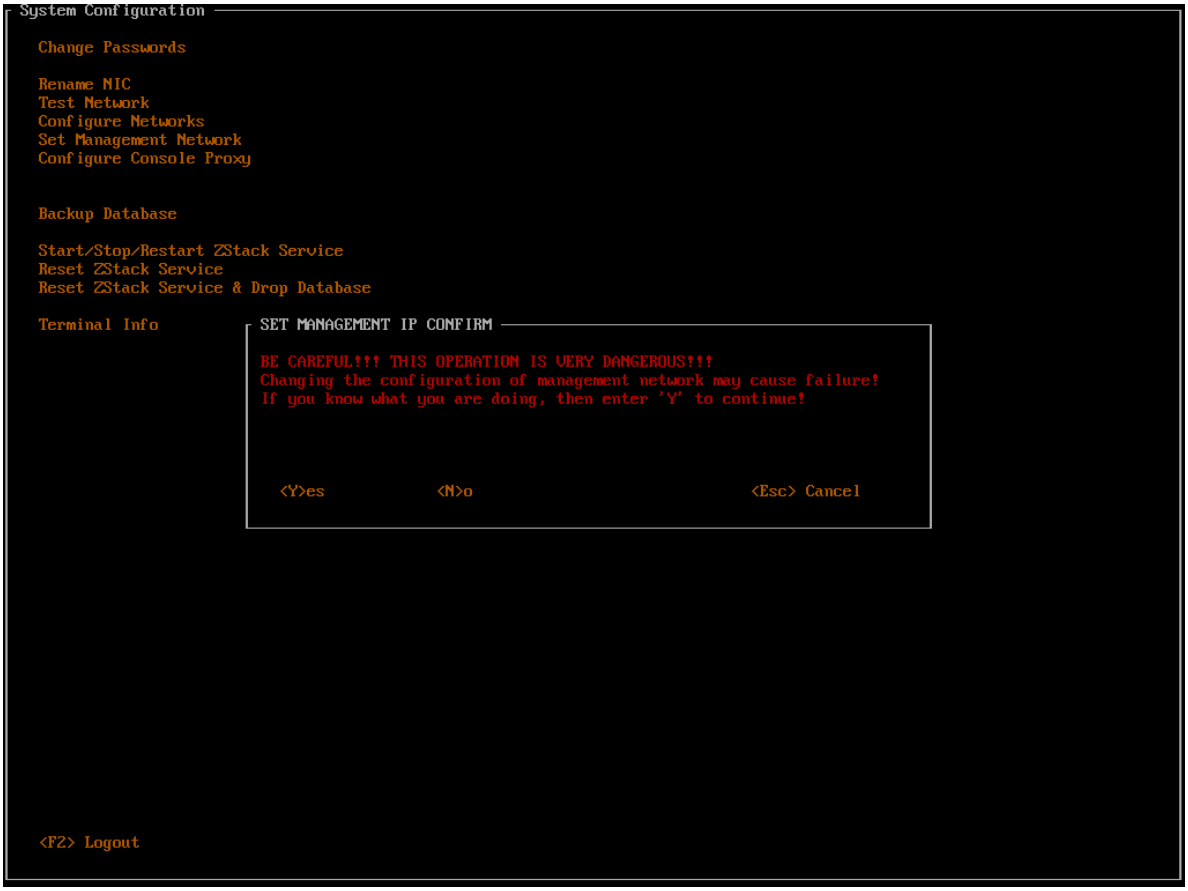
5. Set the management network.

   Move your cursor to **Set Management Network**, and press **Enter** to enter the configuration page of the management network.

> **Note:**
>
> Exercise caution. Configuring the management network is time-consuming.

Figure 5-44: Set Management Network

Figure 5-45: Confirmation Page



6. Configure the console proxy.

   Move your cursor to **Configure Console Proxy**, and press **Enter** to enter the configuration page of the console proxy.

   Enter the proxy IP address and the proxy port, and press **Enter** to finish this configuration.

   The original values of the console proxy will be read and filled in the message box. You can make configurations for the values as needed.

   If any one of the following conditions happens, input errors will be reported:

   - Both the proxy IP address and the proxy port are null.
   - The proxy IP address is invalid.
   - The proxy port does not fall between 1024 and 65535.

   Note:

   - You need to perform this operation only in the management node.

- You need to press **Y** to confirm the operation.
- The domain name cannot be configured.
- You can configure the console proxy in the UI.

Figure 5-46: Configure Console Proxy

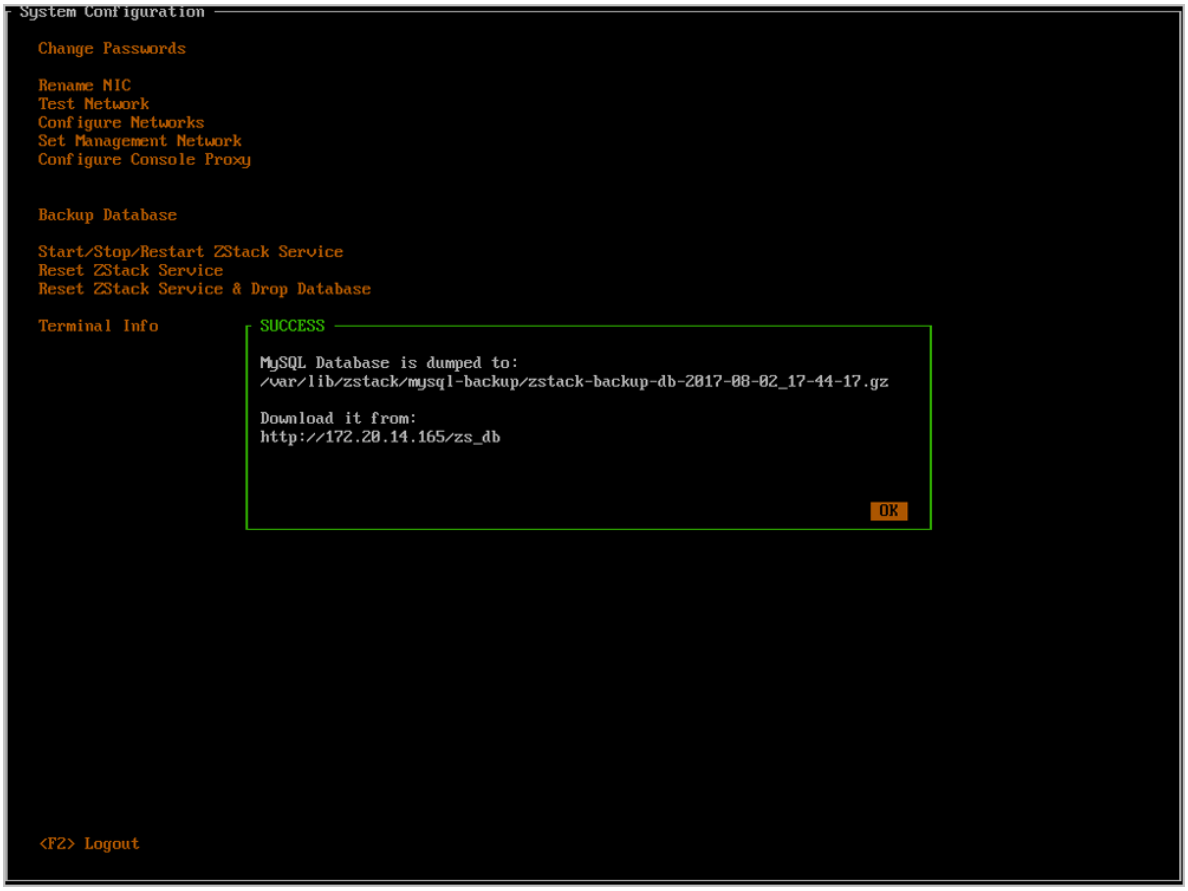
7. Back up the database.

   Move your cursor to **Backup Database**, and press **Enter** to enter the database backup page.

   Press **Enter** to export the database to the HTTP server from which you can download the database.

Figure 5-47: Back up Database

Figure 5-48: Succeed in Backing up Database



Note:

Currently, ZStack allows you to back up the database of the management node to a remote server by using CLI commands.

Run the following commands to automatically back up the database of the management node to a remote server, and to automatically perform the remote backup on a regular basis.

1. Manually run the following command to back up the database of the management node to a remote server.

```
#10.0.50.0 is the IP address of the remote server.
```

```
zstack-ctl dump_mysql --host root@10.0.50.0 --d --keep-amount 24
```

2. Run the `crontab -e` command to change the automatic backup script of the management node database to the following format:

```
30 */2 * * * zstack-ctl dump_mysql --host root@10.0.50.0 --d --
keep-amount 24
```

This operation means that the database of the management node will be automatically backed up to the *`/var/lib/zstack/from-zstack-remote-backup/`* directory of the remote backup storage (IP address: *10.0.50.0*) at an interval of two hours.

Note:

- **`-d`** means that only the specified count of the latest backup will be reserved.
- You need to configure the SSH password-free login in advance from the management node to the remote backup storage.
- If you need more technical supports, contact the official technical support team.

8. Start, stop, or restart ZStack services.

Move your cursor to **Start/Stop/Restart ZStack Service**, and press **Enter** to enter the page of starting, stopping, or restarting ZStack services.

After you press **Enter**, move your cursor again to select the concrete operation. Finally, press **Enter** to finish this operation.

Figure 5-49: Start, Stop, or Restart ZStack Service

According to the prompt, enter **start zstack** to confirm to start the cloud, enter **stop zstack** to confirm to stop the cloud, and enter **restart zstack** to restart the cloud.

Figure 5-50: Start ZStack Service

Figure 5-51: Stop ZStack Service

Figure 5-52: Restart ZStack Service

9. Reset ZStack services.

   Move your cursor to **Reset ZStack Service**, and press **Enter** to enter the page of resetting ZStack services.

   This operation is extremely dangerous. You need to enter **reset zstack**, and then press **Enter** to confirm this operation.

Figure 5-53: Reset ZStack Service

10. Reset ZStack services and drop databases.

Move your cursor to **Reset ZStack Service** & **Drop Database**, and press **Enter** to enter the page of resetting ZStack services and dropping databases.

This operation is extremely dangerous as well. When you reset ZStack services, the existing databases will be cleansed as well. You need to enter **reset zstack drop database** to confirm this operation.

Figure 5-54: Reset ZStack Service and Drop Database

Note:

Exercise caution when you use this feature.

11. Enter the terminal.

ZStack TUI reserves the terminal entrance for you. Move your cursor to **Terminal Info**, and press **Enter** to see the entrance information.

- Press **Ctrl+Alt+F2** to enter the reserved terminal where you can run common commands. Be careful to perform these operations. These operations may damage your system, and influence ZStack services.
- Press **Ctrl+Alt+F3** to enter the `zstack-cli` page.
- Press **Ctrl+Alt+F1** to go back to TUI at any time if needed.

Figure 5-55: Enter Terminal Information

Reboot or Power Off

On the main page, press **F12** to enter the rebooting or power-off page.

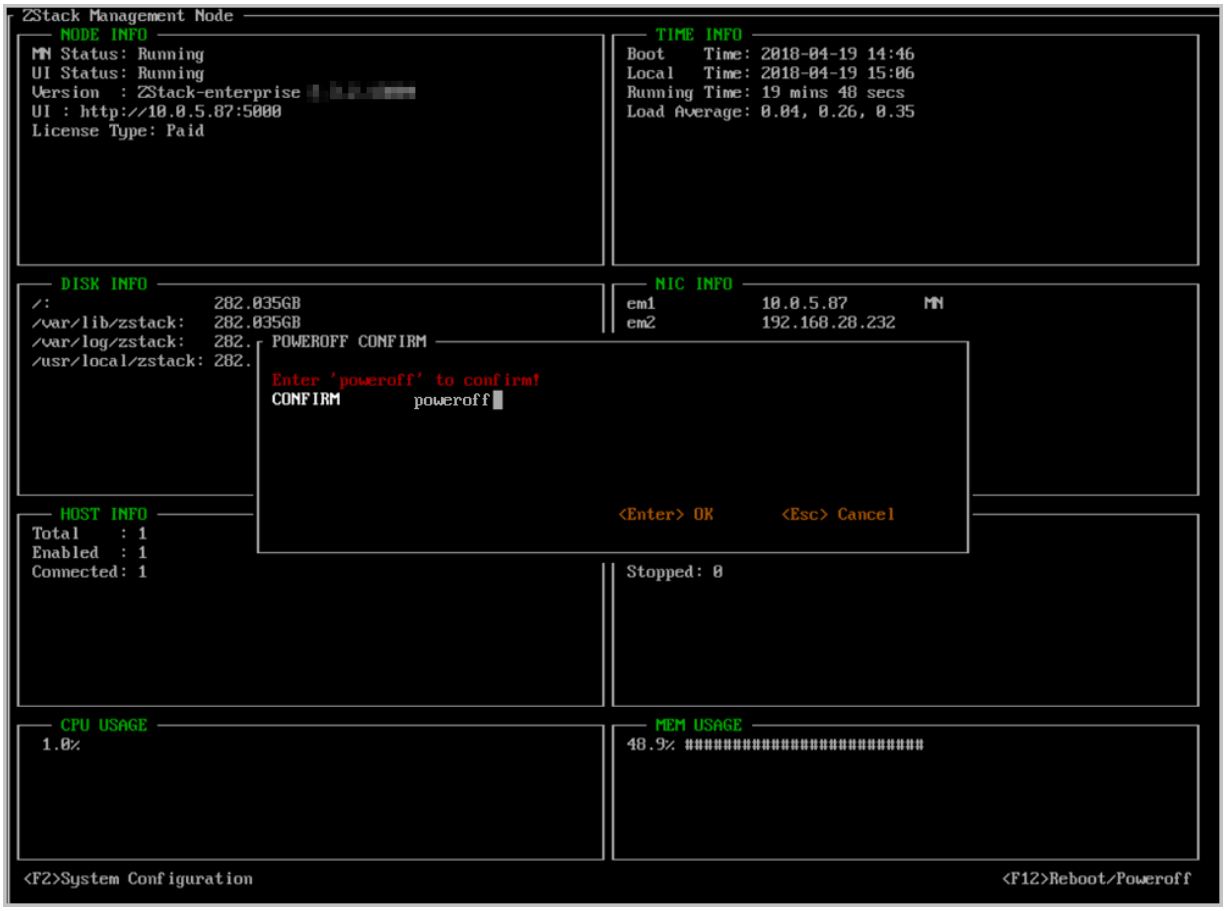
Move your cursor to **Reboot** or **Poweroff**, and press **Enter** to enter the confirmation page.

Figure 5-56: Reboot/Poweroff

According to the prompt, both rebooting and poweroff operations require you to enter **REBOOT** or **POWEROFF** to confirm whether you want to reboot or power off the cloud to avoid error operations.

Figure 5-57: Rebooting Confirmation

Figure 5-58: Poweroff Confirmation



Abnormal NIC Solution

Under the management node mode, if the cloud fails to be installed due to a lack of NIC configurat ions or other reasons, the terminal will be exited.

For example, when you install ISO, if your servers have no available IP addresses, you cannot normally install ZStack management nodes. Before you run the following commands to install ZStack Installation Package, configure well the networks in advance.

- For ZStack Enterprise Management Node, run `bash /opt/zstack*installer.bin -E`.
- For ZStack Community Management Node, run `bash /opt/zstack*installer.bin`.

The solution to solve the problem of abnormal NICs is provided, as shown in *Abnormal NIC Solution*.

Figure 5-59: Abnormal NIC Solution

```
Try the following steps to install ZStack:
- Make sure at least one NIC is up and have IP
- Check /tmp/zstack_installation.log if it exists
- Run command 'bash /opt/zstack-*installer.bin -E -I NIC_NAME' to install ZStack Enterprise
- Or run command 'bash /opt/zstack-*installer.bin -I NIC_NAME' to install ZStack Community

localhost login:
```

5.2.2 ZStack Compute Node

If you select ZStack Compute Node, ZStack compute nodes will be automatically installed after rebooting. After you install the cloud with ZStack Compute Node successfully, the TUI of the compute nodes will be automatically displayed.

Note:

Under some scenarios, you need the all-in-one mode to set up ZStack. At this time, select ZStack Management Node to install your cloud.

TUI Main Page of Compute Node

The compute node TUI provides a portion of features of the management node, and is deemed as the simplified version of the management node TUI. The usage method of the compute node TUI is the same to *ZStack (Enterprise/Community) Management Node*.

- **VM_INFO**:

  List the information of the VM instance running on the current compute node, including the UUID, CPU count, memory capacity, and the allowed state.

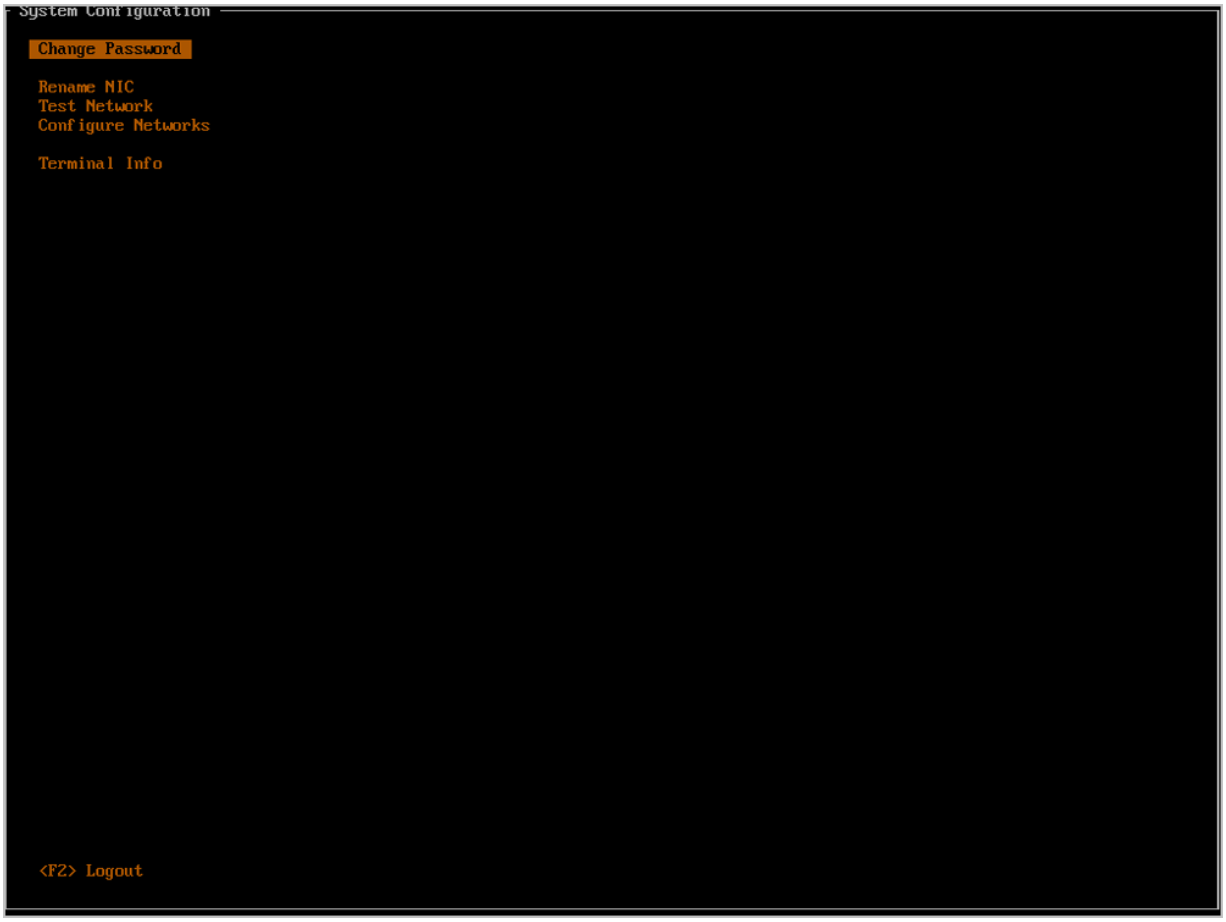
- The meanings of other information modules in the compute node are identical to that of the management node. We will not elaborate more on this part.

Figure 5-60: TUI Main Page of Compute Node

System Configuration

For the system configuration, the compute node only owns a portion of feature items of the management node.

Figure 5-61: System Configuration



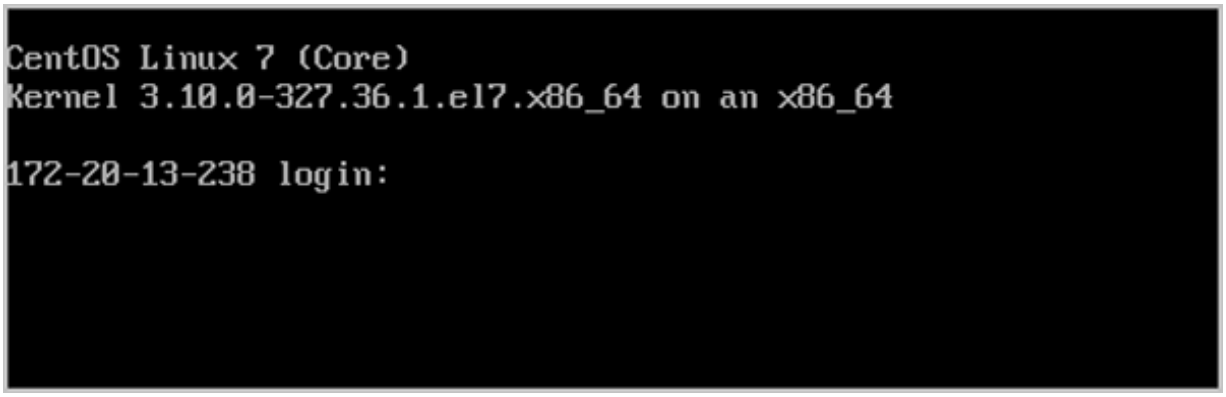
Additional Information

Technologically, the management node can add unlimited number of compute nodes. This is related to License.

5.2.3 ZStack Expert Mode

If you select ZStack Expert Node, the TUI page will be automatically displayed after the cloud reboots, as shown in *Figure 5-62: TUI Page*.

Figure 5-62: TUI Page

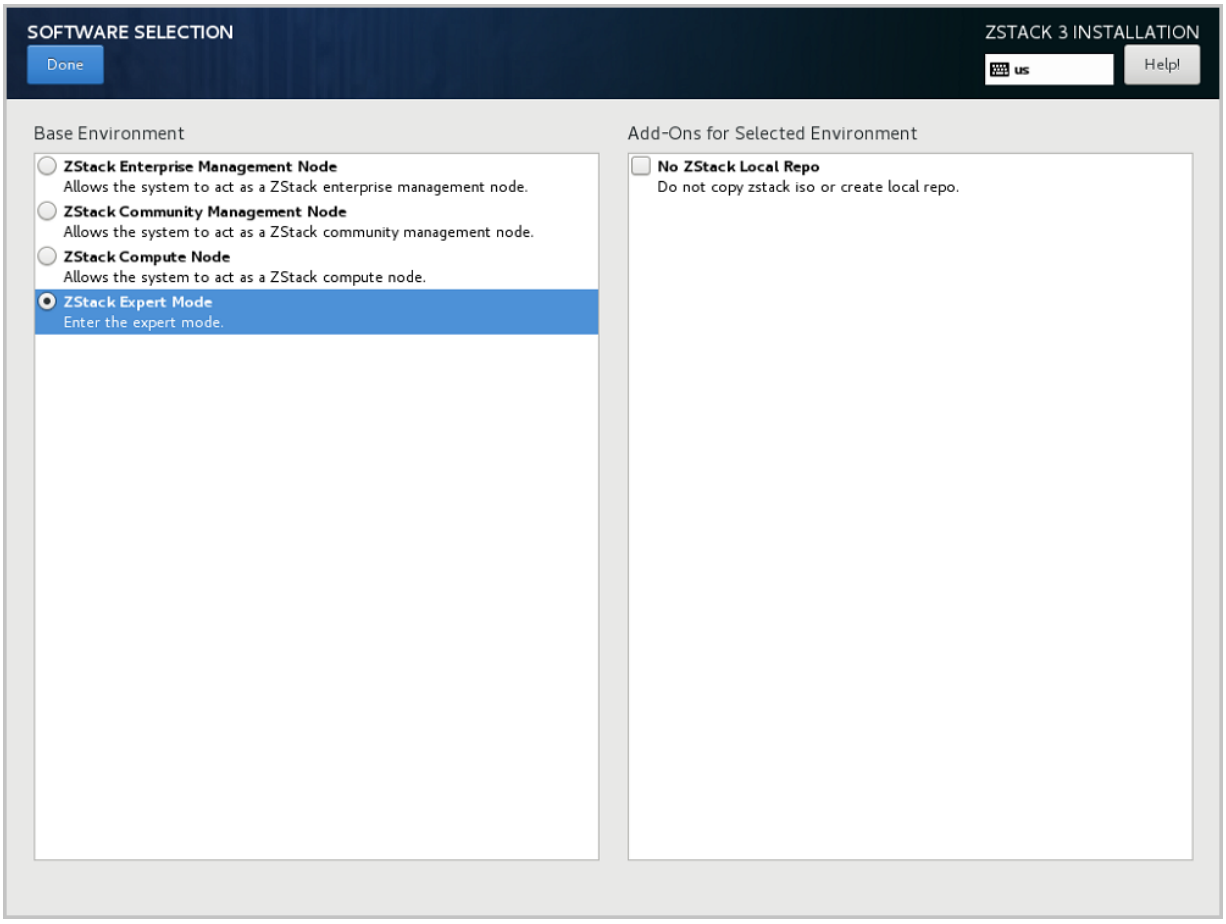


After the Expert Mode is installed, you can install the ZStack environment according to your actual needs.

Additional Information

The Expert Mode can be installed in a simple way. To use simplified installation, select **No ZStack Local Repo** on the right of the installation mode.

Figure 5-63: Simplified Expert Mode



Note:

During the installation process, the simplified Expert Mode does not copy the ISO in the `/opt/zstack-dvd/` directory, and configuration files such as **zstack-local.repo** are not generated in the `/etc/yum.repos.d/` directory. This effectively saves the installation time.

5.3 Manage ZStack

Procedure

1. After you install the cloud for the first time, the system will automatically start ZStack services.
2. After the management node reboots, ZStack services will be automatically booted after being powered on.
3. If the services in the management node are stopped due to O&M operations or other exceptions, you need to manually start the services.

The following sample is the method to start ZStack services:

```
[root@localhost ~]#zstack-ctl start
#This command will start both the management node and the web UI
service.
```

4. You can use `zstack-ctl status` to check the state of related services of ZStack management node.

```
[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: 2.4.0 (ZStack-enterprise 2.4.0.13004)
MN status: Running [PID:3498]
UI status: Running [PID:8459] http://10.0.5.87:5000
```

5. You can also use `zstack-ctl ui_status` to check the state of the web UI service.

```
[root@172-20-12-20 ~]# zstack-ctl ui_status
UI status: Running [PID:8459] http://10.0.5.87:5000
```

6. To start the management node service and to not start the web UI service, run the following command:

```
zstack-ctl restart_node
```

7. We do not recommend that you stop and restart all services when you use the cloud. To restart all the services, run the following command:

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

5.4 Upgrade ZStack

This topic describes how to upgrade the Cloud of c76 version. Note that the procedures for upgrading a c74 version are basically the same as those for upgrading a c76 version.

- Before the upgrade, make sure that the c76 OS is installed in both the management node and the compute node, and the management node is upgraded to the latest version of c76 OS.
- Upgrade the management node only. Then, the compute node will be upgraded automatically.
- Before the upgrade, back up the database.
- During the upgrade, you cannot access the Cloud UI and console. Note that the VM instances in the running state are not affected.
- After the upgrade, clear the browser caches or refresh the UI of the management node in time.

The Cloud supports **incremental upgrade** and **offline upgrade**.

Incremental Upgrade

ZStack supports **incremental upgrade**, which can improve your upgrade experience.

For **offline upgrade**, you need to download the corresponding ISO, upgrade the local repo, and then upgrade ZStack. With **incremental upgrade**, you only need to download the latest ZStack Installation Package. Then, the installation package automatically detects and matches the corresponding ISO version.

1. Before you upgrade ZStack online, save the following necessary software package to the `/opt/` directory of the management server:
   - ZStack Installation Package
     - File name: ZStack-installer-3.10.0.bin
     - Download address: Click *here*.
2. Then, make sure that the database is backed up.
   - 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 preceding command, a backup database will be created in `/var/lib/zstack/mysql-backup/`.
     - During the upgrade, the proxy server of ZStack will be upgraded without affecting data in the primary storage and backup storage.
   - You can use the Backup Service provided by ZStack to back up your database at a regular time.

     Note:

     - The Backup Service is a separate feature module. To use this service, you need to purchase the Plus License of the Backup Service module based on the Base License. The Plus License cannot be used independently.

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

```
[root@zstack-1 opt]# bash ZStack-installer-3.10.0.bin -u
```

Note:

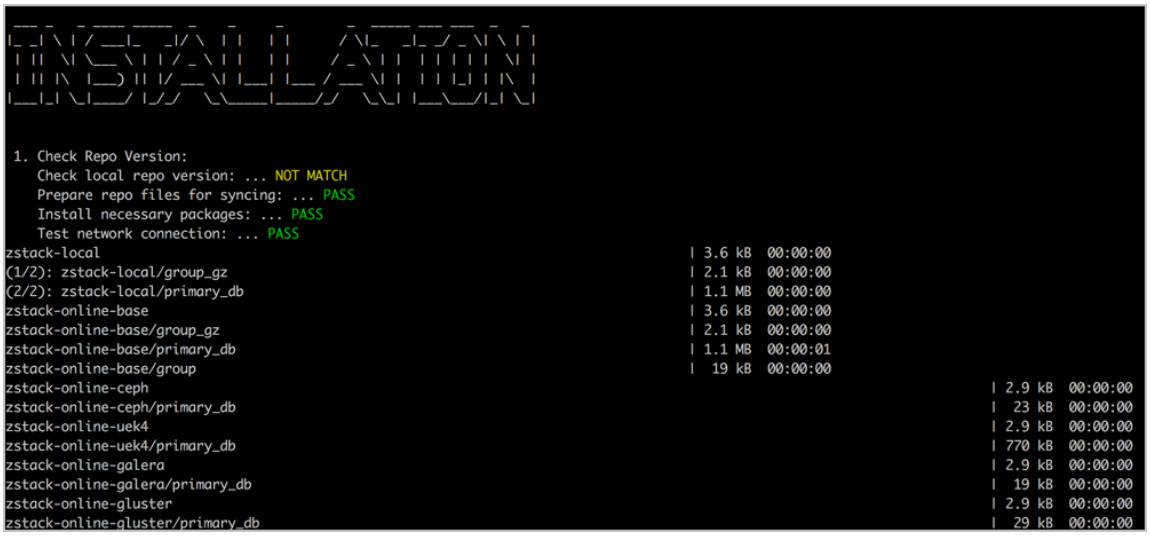
- If the root password of your database is the default password **zstack.mysql.password** of the system, the upgrade can be done by running the preceding command.
- If the root password of your database is a custom, nonblank password, run the following command to complete the upgrade:

```
[root@zstack-1 opt]# bash ZStack-installer-3.10.0.bin -u -P
 MYSQL_ROOT_PASSWORD
```

4. Upgrade the installation package. Then, the installation package automatically detects and matches the corresponding ISO version.

- If the ISO version is relatively old, the local repo will be automatically upgraded to the latest version, and then ZStack is installed.

Figure 5-64: Auto upgrade local repo to the latest version



- If an error is reported during the upgrade of the local repo, you will be promoted to perform offline upgrade.

Figure 5-65: An error is reported during the upgrade of the local repo

```
[root@10-0-182-41 ~]# bash ZStack-enterprise-installer-3.7-1911070336-173.bin -u

FAIL

 Reason: Cannot proceed offline installation: /opt/zstack-dvd/x86_64// folder not found.
        Use 'zstack-upgrade -r zstack-xxx.iso' (xxx>=3.7.0) and try again!

-------------
-------------
[root@10-0-182-41 ~]# _
```

Note:

- The whole process of incremental upgrade must be performed when necessary networks are **connected**.
- The incremental upgrade solution allows you to seamlessly upgrade the Cloud to the latest version.

Offline Upgrade

1. Before you upgrade ZStack offline, save the necessary software packages and scripts to the `/opt/` directory of the management server.
   - ZStack Custom ISO
     - File name: ZStack-x86_64-DVD-3.10.0-c76.iso
     - Download address: Click *here*.

     Note:

     Statement on c72 ISO upgrade:

     - Version 3.7.1 and later versions will no longer provide c72 ISO for you to install and deploy new Clouds. However, you can upgrade your existing c72 ISO to the latest version.
     - The local repo in c72 is redirected to c74. If you upgrade the Cloud offline, obtain c74 ISO to replace the local repo.
   - ZStack Installation Package
     - File name: ZStack-installer-3.10.0.bin
     - Download address: Click *here*.
   - Upgrade Script
     - File name: zstack-upgrade

— Download address: Click *here*.

Note:

The version of the upgrade script must be consistent with the version of the custom ISO and the installation package.

Note:

After you download the software, check the authentication code by using MD5 and verify that the code conforms with the release information.

2. Then, make sure that the database is backed up.

   - 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 preceding command, a backup database will be created in *`/var/lib/zstack/mysql-backup/`*.
- During the upgrade, the proxy server of ZStack will be upgraded without affecting data in the primary storage and backup storage.

   - You can use the Backup Service provided by ZStack to back up your database at a regular time.

Note:

- The Backup Service is a separate feature module. To use this service, you need to purchase the Plus License of the Backup Service module based on the Base License. The Plus License cannot be used independently.

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

```
#The following are two types of offline upgrades:
# 1. Upgrade the local repository and the management service at the
 same time:
[root@zstack-1 opt]# bash zstack-upgrade ZStack-x86_64-DVD-3.10.0-
c76.iso
# 2. Upgrade the local repository and then the management service:
[root@zstack-1 opt]# bash zstack-upgrade -r ZStack-x86_64-DVD-3.10.0
-c76.iso
```

```
[root@zstack-1 opt]# bash ZStack-installer-3.10.0.bin -u
```

Note:

- If the root password of your database is the default password **zstack.mysql.password** of the system, the upgrade can be done by running the preceding command.
- If the root password of your database is a custom, nonblank password, run the following commands to complete the upgrade:

```
#The following are two types of offline upgrades:
# 1. Upgrade the local repository and the management service at
 the same time:
[root@zstack-1 opt]# bash zstack-upgrade ZStack-x86_64-DVD-3.10.0
-c76.iso
# 2. Upgrade the local repository and then the management
 service:
[root@zstack-1 opt]# bash zstack-upgrade -r ZStack-x86_64-DVD-3.
10.0-c76.iso
[root@zstack-1 opt]# bash ZStack-installer-3.10.0.bin -u -P
 MYSQL_ROOT_PASSWORD
```

- Before executing the **`zstack-upgrade`** command, make sure that the ISO is based on c76. Do not overlap the local repo with c74 ISO.

4. If the upgrade succeeds, the *Upgrade succeeds* image is displayed.

Figure 5-66: Upgrade succeeds

```
 1. Check Repo Version:
    Check local repo version: ... PASS

 2. Check System:
    Pre-Checking: ... PASS
    Check System: ... PASS
    Update Package Repository: ... PASS

 3. Get ZStack-enterprise:
    Download ZStack-enterprise package: ... PASS
    Unpack ZStack-enterprise package: ... PASS

 4. Upgrade ZStack-enterprise:
    Upgrade apache-tomcat: ... PASS
    Upgrade zstack-ctl: ... PASS
    Install General Libraries (takes a couple of minutes): ... PASS
    Stop ZStack-enterprise: ... PASS
    Stop ZStack-enterprise UI: ... PASS
    Upgrade ZStack-enterprise: ... PASS
    Deploy yum repo for ZStack-enterprise: ... PASS
    Add cronjob to clean logs: ... PASS
    Install ZStack-enterprise management node: ... PASS
    Enable ZStack-enterprise bootstrap service: ... PASS
    Enable chronyd: ... PASS
    Config zstack.properties: ... PASS
    Append iptables: ... PASS
    Install ZStack-enterprise management node: ... PASS
    Enable ZStack-enterprise bootstrap service: ... PASS
    Enable chronyd: ... PASS
    Config zstack.properties: ... PASS
    Append iptables: ... PASS
    Install ZStack-enterprise Web UI (takes a couple of minutes): ... PASS
    Upgrade ZStack-enterprise UI Database: ... PASS
    Start ZStack-enterprise management node (takes a couple of minutes): ... PASS
    Start ZStack-enterprise Web UI: ... PASS

ZStack-enterprise in /usr/local/zstack has been successfully upgraded to version: [redacted]

 Management node has been started up again. You can use `zstack-ctl status` to check its status.

 zstack-ui has been upgraded.

 zstack-ui has been started up again.

 - chrony server sources is set to management node by default.

 Your old zstack was saved in /usr/local/zstack/upgrade/2018-07-30-16-23-54
```

Notice

- The libvirt version can be automatically upgraded during the upgrade of ZStack. Specifically, if you are using c74 ISO and QEMU 2.9, the libvirt version will be automatically upgraded to 4.9.0.

Note:

- If you deployed the Cloud with an open-source Ceph distributed storage and enabled Cephx (the Ceph authentication protocol), an error might be reported during CD-ROM hot swapping on a VM instance. **This error is caused because the new libvirt version currently does not support hot swapping.** For more information, contact the official technical support for help.

- From ZStack 3.2.0, the supported format of shared volumes is changed to raw. Therefore, the format of shared volumes created in a Shared Block primary storage is changed to raw. In this case, you cannot create snapshots for or resize the shared volumes. In addition, when the attached VM instances are in the running state, you cannot create images for these shared volumes. However, the preceding restrictions will be lifted, and more features will be provided in later versions of ZStack. For more information, follow our official website for updates.
- You can disable libvirt auto upgrade as needed. Method:

  Go to `/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`, and set the following parameter in **zstack.properties**:

  ```
  updatePkgWhenConnect = false
  # Disable libvirt auto upgrade. The default value is true.
  ```

  Restart the management node for the setting to take effect.

- From version 3.7.1, ZStack provides two ISO versions: c76 and c74, either of whose repos are compatible in both versions. When you upgrade the Cloud, note that:
  - Version 3.7.1 and later versions will no longer provide c72 ISO for you to install and deploy new Clouds. However, you can upgrade your existing c72 ISO to the latest version. For information about capacity expansion or system upgrade, contact the official technical support.
  - From 3.7.1, the local repo in c72 is redirected to c74. If you upgrade your Cloud offline, obtain c74 ISO to replace the local repo.

6 System Login

1. You can log in to the UI management page through HTTP or HTTPS.
   - HTTP defaults to support port 5000. Enter the corresponding URL address (*http://your_machine_ip:5000*) to open the UI management page. For a better product experience, we recommend that you use Chrome 49, Firefox 52, or their later versions.
   - HTTPS is disabled by default. .
2. When you log in to the Cloud for the first time, the default account name is **admin**, and the default password is **password**.
3. ZStack supports the following login methods:
   - Account login: Requires you to enter the account name and the account password.
   - User login: Requires you to enter the user name and the user password.
   - AD/LDAP login: Requires you to enter the login attribute name and the AD/LDAP password. For AD/LDAP, you need to configure the AD/LDAP server and bind the AD/LDAP account in advance.
   - Project login: Requires you to add the License of the Enterprise Management module, and to enter the user name and the password.

   Note:
   If the login fails, check the management node service. Make sure that both the management service and the UI service are running properly.
4. ZStack provides multiple login interfaces (main login and project login). For Enterprise Management users, you can set the UI login interface by choosing **Settings** > **Global Settings** > **Advanced**.

   On the **Advanced** tab page, locate **UI Login Interface Mode**, and select a mode as needed.
   - If **Show All** is selected, you can access all login interfaces, including **Main Login** and **Project Login**, through the default link *http(s)://management node_ip:port* .
   - If **Project Login** is selected, you can only access the **Project Login** interface through the default link *http(s)://management node_ip:port*. For **Main Login**, we provide an independent link *http(s)://management node_ip:port/#/accountlogin*. Please keep this link properly.
5. To further protect your account security, ZStack supports two factor authentication. If you enable two factor authentication, the Cloud will require you to enter the correct account name,

password, and a 6-digit security code provided by the identity authentication APP for each login.

Note:

- After you log in to the Cloud successfully for the first time, the QR code for authenticating your identity will no longer be displayed. Make sure that you save and keep it carefully.
- If the QR code of the administrator is lost, contact the official technical support to obtain another one.
- After you log in to the Cloud successfully as an administrator, you can check the QR code of the regular users on the account detailed page. If the QR code of the regular users is lost, contact the project administrator to obtain another one.
- After you log in to the Cloud successfully as an administrator, you can check the QR code of the project identity authentication on the project detailed page. If the QR code of the project is lost, contact the platform administrator to obtain another one.
- Each regular account or project must use its verification code for authenticating logins.

6. To increase the security of the login password, the Cloud supports the following password policies:

   - Enable the account lock for continuous failed logins. During the locking period, you cannot log in to the Cloud by using the account.

     Method: Go to **Settings** > **Global Settings** > **Advanced**, and enable the account lock for continuous failed logins.

     - On the **Advanced** tab page, set **Lock Login Attempt Maximum** to true to enable this feature. Default value: false.
     - On the **Advanced** tab page, set **Maximum Number of Failed Logins** to change the maximum number of failed logins. Default value: 6.
     - On the **Advanced** tab page, set **Account Locking Duration of Failed Logins** to modify the locking time of failed logins. Default value: 10 minutes.
   - Enable the password update cycle to change login passwords regularly.

     Method: Go to **Settings** > **Global Settings** > **Advanced** to set the cycles of password updates.

     - On the **Advanced** tab page, set **Password Update Cycle** to true to enable this feature. Default value: false.

- On the **Advanced** tab page, enter a value for **Password Update Cycle**. Default value: 90 days.

- Limit the number of repeated passwords to prevent the new password being duplicated with the old passwords.

  Method: Go to **Settings** > **Global Settings** > **Advanced** to set the number of allowed repeated passwords.

  - On the **Advanced** tab page, set **Password not Repeated Times** to true to enable this feature. Default value: false.
  - On the **Advanced** tab page, enter a value for **Password not Repeated Times**. If the value is 3, the new password cannot be repeated with the last 3 old passwords you specified before. Default value: 5.

- Enable the password strength to set the length of passwords and to choose whether to enable the password combination policy of numeric, alphabetic, and special characters.

  Method: Go to **Settings** > **Global Settings** > **Advanced** to set the password strength.

  - On the **Advanced** tab page, set **Password Strength** to true to enable this feature. Default value: false.
  - On the **Advanced** tab page, set **Password Strength** to choose the length of passwords, and to choose whether to enable the password combination policy of numeric, alphabetic, and special characters. Default value: 8-32.

- With the switch for only one login session, you can decide whether to disable the multi-login session. After enabling the switch, only one user can log in to the Cloud, while the historical login sessions will be forced to log out.

  Method: Choose **Settings** > **Global Settings** > **Advanced**, locate **Switch for Enable Unique Session**, and enable or disable the switch as needed.

7. After you log in to the Cloud successfully for the first time, select **Personal Center** > **Change Password** at the upper right of the UI. Then, you can change your password.

6.1 UI Login via HTTPS

Default HTTPS Method

This section describes how to log in to the UI via HTTPS by using the default certificate.

1. In the management node, run the following command to stop the management node service:

```
zstack-ctl stop
```

2. In the management node, run the following command to configure the certificate:

```
openssl pkcs12 -in /usr/local/zstack/zstack-ui/ui.keystore.p12 -out
 /usr/local/zstack/zstack-ui/ui.keystore.pem -nodes
```

Note:

During the configuration, you need to enter the default password: **password**.

3. Modify the **zstack.properties** configuration file to set the certificate path to an absolute path.

   Go to `/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties` and modify the **zstack.properties** configuration file to set the certificate path to an absolute path. Note that the absolute path points to the private key password file of the certificate.

```
consoleProxyCertFile = /usr/local/zstack/zstack-ui/ui.keystore.pem
```

4. Run the following command to configure the HTTPS login mode:

```
zstack-ctl config_ui --enable-ssl True
```

5. Run the following command to start the management node service:

```
zstack-ctl start
```

Custom HTTPS Method

This section describes how to log in to the UI via HTTPS by using a custom certificate.

1. Prepare a custom certificate. You can generate a signed certificate by using related tools, or purchase a certificate issued by CA. For example, you can use Keytool, a tool that manages Java data certificates, to generate a signed certificate by running the following command:

```
mkdir certs
$JAVA_HOME/bin/keytool -genkey -alias tomcat -storetype PKCS12 -
keyalg RSA -keysize 2048 -keystore ./certs/keystore.p12 -validity
365
```

Note:

By default, no environment variables are configured by Keytool. You need to add the JRE installation path to the `$JRE_HOMNE` variable. For example,

```
echo "export JAVA_HOME=/usr/local/jdk1.8.0_181" >> /etc/profile
```

```
source /etc/profile
```

2. In the management node, run the following command to stop the management node service:

```
zstack-ctl stop
```

3. In the management node, run the following command to configure the certificate:

```
openssl pkcs12 -in ./certs/keystore.p12 -out ui.keystore.pem -nodes
```

Note:

During the configuration, you need to enter a password.

4. Modify the **zstack.properties** configuration file to set the certificate path to an absolute path.

   Go to `/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties` and modify the **zstack.properties** configuration file to set the certificate path to an absolute path. Note that the absolute path points to the private key password file of the certificate.

```
consoleProxyCertFile = /usr/local/zstack/zstack-ui/ui.keystore.pem
```

5. Run the following command to configure the HTTPS login mode:

```
zstack-ctl config_ui --enable-ssl True \
--ssl-keyalias=tomcat --ssl-keystore=/root/certs/keystore.p12 --ssl-keystore-type=PKCS12 \
--ssl-keystore-password=password --server-port=8888
```

6. Run the following command to start the management node service:

```
zstack-ctl start
```

HTTP Method

If you need to cancel the HTTPS method and restore the HTTP login method, follow these steps:

1. Run the following command to disable the HTTPS login:

```
zstack-ctl config_ui --enable-ssl False
```

2. Run the following command to restart the management node service:

```
zstack-ctl stop_ui
zstack-ctl start_ui
```

7 Resource Pool

7.1 VM Instance

A VM instance is a virtual machine instance running on a host. A VM instance has its own IP address to access a public network and run application services. VM instances are core components of ZStack.

Three Core Attributes

1. **Instance Offering**:

   Define CPU and memory size for a VM instance. Before resources are allocated, ZStack will select the host that has these resources to act as a candidate host, and then use the candidate host to create a VM instance.

2. **Image**:

   Determine which image can be used to create a VM instance.

   When you select an image, note the following:

   - If a backup storage attached by the image is ImageStore, ZStack will automatically select a cluster that is attached by a type of primary storage such as LocalStorage, NFS, SharedMountPoint, Ceph, or SharedBlock to act as a candidate cluster.
   - If a backup storage attached by the image is SFTP (for Community version only), ZStack will automatically select a cluster that is attached by a type of primary storage such as LocalStorage, NFS, or SharedMountPoint to act as a candidate cluster.
   - If a backup storage attached by the image is Ceph, ZStack will automatically select the cluster attached by the Ceph primary storage that corresponds to the Ceph backup storage.

3. **Network**:

   Specify one or more networks for a VM instance. After you select an image, an available cluster has been assigned for the VM instance. Also, ZStack will provide available networks attached by the cluster.

Note:

- After you complete configuring the preceding three attributes, various resources necessary to create the VM instance are all ready. In that case, available resources can be filtered in

order of: the image attached to the backup storage->clusters available to the backup storage-> associated networks available to the cluster.

- If you select the network attached by multiple clusters that satisfy the preceding requirements, you can continue to filter the corresponding resources such as a cluster, primary storage, and host by expanding **Advanced**.
- When you fail to select the L3 networks that you created, we recommend that you check whether:

  1. The L2 network attached by an L3 network attaches the corresponding cluster.
  2. The corresponding cluster has attached the corresponding primary storage.

Multi-Primary Storage Strategy

- If a cluster has multiple LocalStorage primary storages attached:
  - You can specify any LocalStorage primary storage when you create a VM instance.
  - If you do not specify a primary storage, the system will automatically select the local primary storage that has the most available capacity.
- If a cluster has multiple shared primary storages attached (currently, multiple NFS primary storages or Shared Block primary storages are supported):
  - You can specify any NFS or Shared Block primary storage when you create a VM instance.
  - If you do not specify a primary storage, the system will automatically allocate an NFS or a Shared Block primary storage that is available.
- If a cluster has a combination of primary storages attached (currently, the supported combinations include: 1 LocalStorage + 1 NFS, 1 LocalStorage + 1 SMP, 1 LocalStorage + 1 Shared Block):
  - You can specify any primary storage when you create a VM instance.
  - When you create a VM instance, if you create a data volume and attach it to the VM instance at the same time, you need to specify a primary storage for the data volume.
  - If you do not specify a primary storage, the system will automatically use a local primary storage to create a VM instance.

VM Instance Operations

- Start:

Start a VM instance that is in the stopped state. Then, this VM instance will work normally. When you started a VM instance, the last host where the VM instance resides will be enabled by default.

When you start a VM instance, note the following:

Scenario	VM Start
The cluster where the VM instance resides only attaches one or more local storages.	The VM instance can only be started on the last host where the VM instance resides.
The cluster where the VM instance resides only attaches one or more shared storages . Currently, multiple NFS or SharedBlock primary storages are supported.	The VM instance can be started on the available hosts attached by the primary storage.
The cluster where the VM instance resides attaches different types of primary storages . Currently, a combination of 1 LocalStora ge + 1 NFS, 1 LocalStorage + 1 SMP, or 1 LocalStorage + 1 SharedBlock are supported.	**1.** If the VM instance uses the root volume or data volume of a local storage, this VM instance can only be enabled on the last host where the VM instance resides. **2.** If this VM instance only uses a shared storage or shared storage with a data volume, this VM instance can be started on the available hosts attached by the primary storage.

If you fail to start the VM instance, make sure that you check whether:

- Hosts are connected to and enabled in the cluster where the VM instance resides. If no connected hosts are available, you will prompt for the information that you cannot find any available hosts.
- Resources of the hosts running on the cluster, such as CPU and memory, are sufficient. Assume that all hosts running on the cluster have their own separate available CPUs and memories. If these CPUs and memories are insufficient to allocate to the VM instance, the Cloud will prompt you that you cannot find any available hosts.
- The cluster where the VM instance resides attaches an L2 network. If the cluster has not attached any L2 network, the corresponding L3 network will not be assigned for this VM instance. Then, the Cloud will prompt you that this VM instance has no available networks and cannot be started.
- The L2 network corresponded by the cluster where the VM instance resides is attached to an L3 network. If the L2 network attached by the cluster is not attached to any L3 network

, this VM instance cannot attach any L3 network. Then, you will prompt for the information that this VM instance has no available networks and cannot be started.

- The cluster where the VM instance resides is attached to a primary storage. If the cluster is not attached to any primary storage (generally, the case occurs after a primary storage is detached), you will prompt for the information that no root volumes of this VM instance are found. In that case, attach the original primary storage to the cluster before the VM instance can be normally started.
- The primary storage where the cluster resides has availably sufficient capacities. This can be judged when you create the VM instance. If the primary storage cannot provide sufficient ly required capacities for the VM instance, you will prompt for insufficient capacities of the primary storage.

- Stop:

  Stop the VM instance that is in the running state. The VM instance will be stopped normally.

- Reboot:

  Reboot the VM instance that is in the running state. During rebooting, all configurations for the VM instance will be updated, including boot order, console mode, USB redirection, and session count control.

- Power off:

  Power off the VM instance that is in the running state. That is, the VM instance will be forced to stop. Exercise caution. Performing this operation will put you at risk of losing data.

- Pause:

  Pause the VM instance. The VM instance will continue to consume memories or resources, but will temporarily not schedule hypervisors. Notice that the VM instance can be either resumed to the running or deleted state.

- Resume:

  Resume the VM instance that is in the paused state. Hence, the VM instance can continue to run normally.

- Delete:

  Delete the VM instance. If the VM instance is running, the VM instance will be powered off and enters deleted state. If the VM instance is in other states or statuses, the VM instance will enter directly deleted state.

- Restore:

Restore the VM instance that is in the deleted state to the stopped state.

- Expunge:

  Expunge the VM instance that is in the deleted state. Afterwards, the VM instance will be expunged from ZStack, and the storage space actually occupied by the root volume will be released.

- Open console:

  Let you access the VM instance via the VNC mode. Ensure that your browser can reach the IP address of the console proxy. If you open the console of the VM instance successfully, but do not receive any content, verify that the IP address specified by the console proxy can be normally accessible to your guests (laptop). Change the IP address of the console proxy as required.

  Note:
  To change the IP address of a console proxy, choose **Platform Management** > **Console Proxy**.

- Local storage migration:

  Mainly refer to the cold migration for root volumes or data volumes. Before cold migration, detach associated data volumes for the VM instance.

  Local storages also support hot migration. Make sure that you enable this service globally. Notice that this operation is not supported by the Windows VM instance. Before hot migration, detach associated data volumes from the Windows VM instances.

- Network shared storage migration:

  To achieve real-time hot migration, mainly copy memories and registers related to CPU.
  To support migrations across clusters, both destination cluster and source cluster are only required to attach a network and a primary storage used by the VM instance. If these clusters are attached to multiple types of primary storages, detach volumes for the VM instance before migrations are performed.

- Create image:

  Encapsulate the VM instance as an image which can be used to create more VM instances.

  - Create image online: When the VM instance is running, ImageStore and Ceph backup storages let you create an image online.

- Create image offline: When the VM instance is stopped, various types of backup storages let you create an image.

- Create VM snapshot:

  Before important operations are performed, ensure that the root volume or data volumes are temporarily reserved at a specific time, which can be used to quickly let you perform rollback after failures appear. If you need a long-term backup, use the related backup service. A VM snapshot includes the following types:

  - Single snapshot: Take only snapshots for the root volume of the VM instance.
  - Batch snapshot: Take batch snapshots for the root volume and all data volumes. While you create a VM snapshot, all data volumes attached by the VM instance will be taken snapshots as well. Batch snapshots can be recovered centrally as a unit.

  — You can create snapshots for running or stopped VM instances.

  — You cannot create batch snapshot for VM instances that have a shared volume attached.

  — In a production environment, we recommended that you limit the number of snapshots per disk within 5. Excessive snapshots might affect the I/O performance, data security, and primary storage capacity of the corresponding VM instances and volumes. For long-term backup, we recommend that you use disaster recovery related services.

  — To ensure data integrity in a production environment, we recommend that you do not take snapshots for VM instances with high I/O. When a high I/O operation is performed in a VM instance, some data in the VM memory might fail to be saved to the disk. In this case, these data will not be saved to the snapshot you created for the VM instance.

  — The snapshot of the VM instance on the Ceph primary storage does not occupy capacity . Therefore, the displayed snapshot capacity is the actual capacity of the VM root volume when the snapshot was created.

  — For Ceph primary storages, the VM snapshot capacity might fail to be obtained. Here are some statements:

    - Open source Ceph (version H) and enterprise-level Ceph (earlier than 3.2.0) cannot obtain VM snapshot capacity.
    - Due to the RBD format, enterprise-level Ceph (3.2.0 and later versions) may fail to obtain VM snapshot capacity.

Note:

- Snapshots, a **short-term solution**, mainly can be used in test and development environments. Specifically, these snapshots can quickly be used for packing, upgrading, or testing your Cloud. When normal failures appear, rollbacks can be performed. We recommend that you do not use snapshots in your production environment. However, under some circumstances, snapshots can still be applied to your production environment. For example, if you perform dangerous operations, the probable damage to the operating system may occur due to upgrading or configuration modifications. Then, snapshots are a preferred solution.
- We recommend that you do not use snapshots in your production environment. The following are the two probable considerations:
  - Data integrity

    When you use snapshots, you are not creating a copy of the virtual hard disk. But actually, you need to create a copy of the VM virtual disk. If the virtual disk is damaged, the snapshot will be invalid, which means that the snapshot cannot be used to recover the damaged disk. Notice that the snapshot cannot be used to solve disk failures. So, you will still encounter a **single point of failure**.
  - VM performance

    Using too many snapshots will influence the performance of a VM instance. For example, if the old snapshot runs on the VM instance with excessive overloads, this old snapshot will be increased in size, and then the performance of the VM instance will be definitely slowed down. Or, if you create a large number of snapshots, the performance of the VM instance will be also slowed down.

    Reserving a snapshot of a VM instance for a long time is a common mistake. The snapshot will increase in size as the time goes by. Also. the snapshot files will also be changed, and are not stored on the source disk. Hence, restoring the snapshot will take a long time. Also, during restoring, the VM instance may be forced to stop.

- Restore snapshot:

  Restore the VM instance to the current snapshot point. By doing so, the data related to the volume will be reverted to the snapshot point. Before restoring the snapshot, make sure that you back up the volume data of the VM instance.

Note:

- For a single snapshot, you can only restore the VM root volume to the time of point when the snapshot was taken.
- For a batch snapshot, you can restore both the root volume and data volume to the time of point when the snapshot was taken.
- You can restore snapshots only for VM instances that are stopped. Before you restore a snapshot, stop the corresponding VM instance.
- You can choose whether to automatically start the corresponding VM instance after restoring from a snapshot.
- If a VM batch snapshot is displayed as not restorable, the possible reasons are as follows:
  - At least one data volume snapshot in the batch snapshot was deleted. In this case, you can only restore single snapshots.
  - At least one data volume attached by the VM instance was deleted. In this case, you can only restore single snapshots.
  - At least one data volume attached by the VM instance was detached. In this case, you can only restore single snapshots. To restore the batch snapshot, attach the detached data volumes to the VM instance again.
  - The VM instance has a new data volume attached. In this case, you can only restore single snapshots. To restore the batch snapshot, detach the new data volume from the VM instance.

- Delete snapshot:

  Delete the unnecessary snapshots. Snapshots can be deleted in bulk.

  Note:

  - Snapshots created on local storage, NFS, SMP, and Shared Block storages have a tree structure. Deleting the root snapshot will also delete snapshots on the branches and detach the batch snapshots on the branches. Please exercise caution.
  - Snapshots created on the Ceph shared storage are independent and do not have a tree structure. Deleting a snapshot will not affect other snapshots.
  - When you delete snapshots in a tree structure in bulk, the cloud automatically calculates and deletes the candidate snapshots and cascades the delete operation to the associated snapshots.
  - If the snapshots to be deleted contain batch snapshots, note that:

- Deleting a batch snapshot will also delete the data volume snapshots in the batch snapshot and the snapshots on the branches. Please exercise caution.
- Deleting single snapshots and batch snapshots in bulk will also delete the single snapshots on the branches and detach the batch snapshots on the branches.

- Detach batch snapshot:

  Detach a VM batch snapshot to a single snapshot. Also, the group relationship between the VM instance and its related volume snapshots will be detached. Exercise caution. After detaching the relationship, you cannot restore snapshots in bulk.

- Clone:

  Copy the root volume and data volumes for the VM instance. Based on the instance offering of the VM instance, a new VM instance will be cloned from and then have the identical operating system as the VM instance.

  - Cloning VM instances online only applies to the disk data that have been written when a cloning job begins, excluding the real-time cache data. To ensure data integrity, high I/O VM instances are recommended to enter paused or stopped state before a cloning job is performed.
  - Configurations, installation programs, and passwords of a VM instance will be copied to the newly cloned VM instance. However, copies of other configurations are not included, such as tags and scheduled jobs.
  - Assume that the cloned VM instance is in the running state. After the VM instance is rebooted, the VM console password will take effect.
  - When a VM instance is cloned, if you use a SharedBlock primary storage, select a provision mode for the VM instance, including thick provision and thin provision.
    - Thick provision: Preallocate the required storage space, and provide sufficient storage capacities for the VM instance to ensure the storage performance.
    - Thin provision: Allocate the storage space to the VM instance as needed to achieve higher storage utilizations.
  - When a VM instance is cloned, if you use a Ceph primary storage, you can specify a storage pool.
    - When a VM instance is cloned without volumes, a Ceph storage pool (root volume pool) can be specified.

    - When you use an ImageStore backup storage to clone a VM instance with volumes, you can specify a data volume pool and a root volume pool.
  - When you clone a VM instance, ensure that you do not set a static IP address for the source VM instance. Otherwise, the IP address will be duplicated in multiple VM instances, which will lead to login errors.
- Create backup data: Backs up the VM instance on the Cloud to an off-site server or to Public Cloud remote disaster recovery server.
- Create volume:

  Create data volumes from the primary storage attached by a cluster where the VM instance resides.

  If you have multiple types of primary storages, you can specify a type of primary storage to create volumes.

  - For multiple LocalStorage primary storages, an availably large capacity of storage will be selected to create volumes for the VM instance by default.
  - For multiple NFS primary storages or multiple SharedBlock primary storages, a type of primary storage will be randomly selected to create volumes for the VM instance by default.
  - For LocalStorage +NFS/Shared Mount Point/Shared Block, a type of primary storage where the root volume of the VM instance currently does not reside will be selected.

  Volumes can be created based on the volume image. If the volume image is attached to an ImageStore backup storage, you can create the volumes on a Ceph primary storage.
- Attach or detach volume:
  - Attach volume: Create volumes for the VM instance on the primary storage attached by a cluster where the VM instance resides.
  - Detach volume: Detach volumes from the VM instance. To perform cold migrations and storage migrations for local storages, detach related data volumes.
- Resize volume:

  Resize data volumes as needed after the VM instance stops. Modifying capacities for the data volumes will take effect after the VM instance starts. Notice that data volumes can only be expanded on the Cloud.
- Create VM image:

Encapsulate a volume as an image. This image can be used to create more volumes. Also, volumes on a Ceph primary storage can be encapsulated as volume images on an ImageStore backup storage.

- Attach or detach ISO:
  - Attach or detach an ISO image. Make sure that you add an ISO image in advance. After the image is added successfully, the VM instance can detect and attach this image.
  - If you plan to repair the operating system or reinstall the operating system, you can attach an ISO image, adjust the boot order by prioritizing the ISO image, and reboot the VM instance with the ISO wizard.
  - Let you attach multiple ISO images. You can attach 3 ISO images to the VM instance at most. Also, you cannot attach ISO images in bulk.
- Create or delete vDrive:
  - Make sure that you stop the VM instance in advance. Then, you can create or delete the vDrive.
  - To set the maximum number of virtual drives for a VM instance as needed,

    Choose **Settings** > **Global Settings** > **Advanced**, and set **maximumCdRomNum**. Default value: 3. Options: 1 | 2 | 3.
  - Deleting CDROMs and modifying default devices will affect the device names and ISO mappings. Specifically, the influence is as follows:
    - Deleting CDROMs will change the order for the rest of CDROMs successively. For example, assume that you have three CDROMs: CDROM-1, CDROM-2, and CDROM-3 . If you delete CDROM-2, all ISO images attached to the CDROM-3 will be changed to CDROM-2.
    - Modifying default CDROMs will change the device serial numbers of the CDROMs. For example, assume that you have three CDROMs: CDROM-1, CDROM-2, and CDROM -3. If CDROM-2 is set as default, CDROM-2 with all its ISO images will be changed to CDROM-1, and the original CDROM-1 will become CDROM-2.
- **SSH Login Method**: Allow you to use the SSH key or password if you have image files preconfigured with Cloud-init.
  - If you use an SSH key, set the following parameter:
    - **SSH Key**: After an SSH key is injected to a VM instance, you can SSH in to the VM instance without entering a password when the VM instance is running.

— If you use a password, set the following parameters:

- **User Name**: By default, the user name is root.
- **Password**: After a root password is injected to a VM instance, you can SSH in to the VM instance by entering a password when the VM instance is running.

Note:

- The root password setting method only applies to Linux VM instances. For Windows VM instances, you can set passwords by using User Data.
- Before you set the password, make sure that the VM image has the Cloud-init installed. Recommended versions for Cloud-init: 0.7.9, 17.1, 19.4, and the later versions.
- After you set a password, do not set the password again in User Data to avoid conflicts.
- After you set a root password, a clear text password will be displayed in the User Data on the details page of the created VM instance. Keep your password confidential.

Note:

Different types of images support different SSH login methods.

- Images of different operating systems:
  - Linux image: Fixed user name: **root**. Supported SSH login methods: SSH key | password.
  - Windows image: Fixed user name: **administrator**. Supported SSH login method: setting password by using User Data.
- Images of different formats:
  - Image of the ISO type: Supported SSH login method: SSH key.
  - Image of the Image type: Supported SSH login methods: SSH key | password.

- Set host name:

— The rules for setting Linux hostname and Windows hostname are different.

- Linux hostname: The hostname must be 2 to 60 characters long, and can be uppercase, lowercase, numbers, 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 long, and can be uppercase, lowercase, numbers, and hyphens (-). Note that a hostname cannot contain

consecutive hyphens (-), cannot start or end with hyphens (-), and cannot contain only numbers.

- Before you set a hostname, make sure that the DHCP service of the L3 network corresponding to the VM instance 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.

- SSH key management:

  After you inject an SSH key into a VM instance, you can use the SSH key to log in to the VM instance without passwords via SSH.

  For your reference, to inject an SSH key into a VM instance:

  1. Install Cloud-init.

     Currently, you can inject an SSH Key into a VM instance by using Cloud-init. To inject the SSH Key into the VM instance, install Cloud-init in advance.

     1. Install Cloud-init by yourself. Recommended versions: 0.7.9, 17.1, 19.4, and their later versions.
     2. After you complete installing Cloud-init, the SSH password authentication defaults to be disabled. 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 the **`ssh-keygen`** command. By default, the SSH Key is stored in *`/root/.ssh/id_rsa.pub`*.
     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, enter an SSH Key under the **Advanced** option.
     - Method 2: If you have created a VM instance, enter an SSH Key by selecting **Add SSH KEY** under the **Actions** of the VM instance.

     After you inject the SSH Key, you can check the basic information of the corresponding SSH Key at the VM instance details page, such as user name and host information of the corresponding key.

Note:

- When you create a VM instance, injecting an SSH Key into the VM instance will take effect immediately.
- When you inject an SSH Key into the VM instance that is in the start state or running state, clean up the previous configurations by running `rm -rf /var/lib/cloud/instances`, and then reboot the VM instance. Finally, the SSH Key will take effect.
- On the VM actions page, click **Delete SSH KEY**. Only the SSH Key information recorded in the system is deleted, while the related information of the injected SSH Key is not deleted or removed.
- If you need to delete the SSH Key that has been taken effect, clean up manually the SSH Key under *`/root/.ssh/authorized_keys`* in the VM instance.

- Set high availability:

  If resources on hosts are sufficient, the VM instance configured with NeverStop will never be stopped.

  - Assume that the volumes of the VM instance are attached to a local storage. After the host where the VM instance resides is abnormally stopped, this VM instance will not be started again until the host recovers to the availably connected status.
  - Assume that the volumes of the VM instance are attached to a shared storage. When resources on hosts are sufficient, the VM instance will keep running normally. Even if the VM instance stops, it will be rebooted. If the host where the VM instance resides is abnormally powered off and stopped, this VM instance will be rebooted on other available hosts.
  - You can set the NeverStop VM instance to not be automatically rebooted.
  - The rebooting progress of the NeverStop VM instance can be displayed on the web UI.
- Change instance offering or change CPU and memory:

  Changes the CPU, memory, disk QoS, and network QoS.

  - Change online: Let you change the CPU, memory, disk QoS, and network QoS of the VM instance by enabling NUMA globally. These settings will take effect after the VM instance is rebooted or the new VM instance is created. We recommend that you do not change the CPU and memory for the Windows VM instance in your production environment. On the contrary, we recommend that you change online the configurations of the Windows VM

instance after the VM instance is stopped. If you change an instance offering online, you can only increase the CPU and memory rather than decrease them.

- Change offline: Change the configurations of the VM instance after the VM instance is stopped.

- Set boot order:

  After you attach an ISO to the VM instance, set the boot order for the VM instance. The boot order can be used to restore or reinstall the operating system. Set the boot order by prioritizing CDROM. After the VM instance reboots, all settings will take effect. Notice that these settings can only take effect once. If you reboot the VM instance next time, the VM instance will be booted from a hard disk by default. When you create a VM instance for the first time and select an ISO image without setting the boot order, the operating system will be automatically booted from the ISO image.

- Enable (Specify hosts):

  Select the specified host from the available host list to start the VM instance, which is applied to shared storages. If the VM instance uses a local storage, the host where the root volume resides can be used to start the VM instance.

- Set or cancel console password:

  Set or cancel the console password. After you set the console password, you can access the VNC console by entering the correct console password. On the contrary, after you cancel the console password, you can access the console of the VM instance without passwords.

  Note:
  When you set and cancel the console password, if you do not select Reboot, you need to manually reboot the VM instance on the web UI before all settings take effect.

- Reimage the VM instance:

  Restore the image template to the initial state against the stopped VM instance. By doing so, the data that are changed within the VM instance will be erased. To reimage the VM instance, back up volume data in advance.

- Change owner:

  Change the owner of the VM instance to another regular account.

- Set RDP mode:

Set the RDF mode under the VDI scenario. By default, the console of the VM instance is opened in RDF mode. The settings take effect immediately.

- USB redirection:

  Mainly used for VDI. Specifically, the USB device that plugs in a client can be redirected to the VM instance. After you change the USB redirection, restart the VM instance before all settings take effect.

- QGA option:

  Before you enable the QGA option, make sure that you have installed and run `qemu-guest-agent` on the VM instance. After the QGA option is enabled, the VM instance defaults to let you change its password online.

- Change password online:

  Enable the QGA option. Also, you must install and run `qemu guest agent` on a Linux or Windows VM instance. Make sure that the user name that you entered is existed.

- Resize root volume:

  Expand the root volume for the VM instance.

  - If you use a Linux VM instance partitioned by Logical Volume Manager (LVM), you can expand directly the operating system partitions by running lvextend.
  - A Windows VM instance can also let you right-click Disk Management to expand the root volume.

- Switch console mode:

  The console mode supports VNC, SPICE, and VNC+SPICE. Specifically, VNC lets you open the console of the VM instance via a browser, while SPICE allows you to open the console of the VM instance via an SPICE client. These three console modes are supported. The settings will take effect after the VM instance is rebooted.

- Migrate storage: Perform cold migrations for the VM instance across same types of primary storages, and perform hot migrations for the VM instance across different types of primary storages.

  - Perform cold migrations across the same types of primary storage: Let you perform cold migrations for a VM instance across the same types of primary storage, including Ceph-Ceph, NFS-NFS, and SharedBlock-SharedBlock.

Note:

- Storage migrations across Ceph primary storages:
  - Before you perform migrations, you must stop the VM instance and then detach all its data disks.
  - MON nodes between two Ceph primary storages must be interconnected.
- Storage migrations across NFS primary storages:
  - Before you perform migrations, you must stop the VM instance and then detach all its data disks.
  - The target NFS primary storage can be attached to the cluster where the VM instance to be migrated resides.
- Storage migrations across SharedBlock primary storages:
  - Before you perform migrations, you must stop the VM instance. You can perform migrations for the VM instance with volumes.
  - If the VM instance attaches shared volumes, the shared volumes cannot be migrated with the VM instance simultaneously.
  - The target SharedBlock primary storage can be attached to the cluster where the VM instance to be migrated resides.
- The cluster attached by the target primary storage can meet the network needs of the VM instance.

- Hot migrations across different types of primary storage: Let you perform hot migrations for the VM instance across different types of primary storages, including Ceph-SharedBlock, LocalStorage-SharedBlock, and LocalStorage-Ceph.

Note:

- Before you perform migrations, do not stop the VM instance.
- You can only perform migrations for the VM instance with the regular volumes. If the VM instance attaches shared volumes, the shared volumes cannot be migrated with the VM instance simultaneously.
- After you perform storage migrations for the running VM instance, snapshots for the VM instance will not be reserved.

- The cluster attached by the target primary storage can meet the network needs of the VM instance.

- Bind or unbind affinity group: Bind/unbind the VM instance to/from an affinity group.

  Currently, ZStack provides two affinity group policies to better manage VM instances and hosts: anti-affinity group (soft) and anti-affinity group (hard).

  - Anti-affinity group (soft):

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

- Change operating system:

  After the VM instance is stopped, you can change the operating system by specifying the target image. Notice that the target image must be the Image type: qcow2 and raw. After you change the operating system, the VM instance stays in the stopped state.

  - Changing the operating system for the VM instance will expunge all its original operating system disks and snapshots. Make sure that the related backups are performed before you confirm the change of the operating system to avoid data loss.
  - If a scheduled job to create snapshots for the VM instance is failed, ensure that you make configurations for the scheduled job again.
  - When the VM instance attaches data volumes, you can switch different types of the operating system, such as switching Linux to Windows.
  - When you switch across different types of the operating system, the partition format of data volumes will probably fail to be detected and identified.

- Set QoS:

  Limit the upstream bandwidth and downstream bandwidth of the VM volumes and networks. All settings will take effect without rebooting the VM instance. Underused QoS will probably lead to the abnormality of the VM instance.

- Inject User Data:

  ▬ Before you import User Data, make sure that both the User Data network service and DHCP network service are available.

- By default, the User Data network service and DHCP network service in the three network environments of flat network, vRouter network, and VPC network are enabled.
- If you set a hostname and password by using the User Data, do not set them again in **SSH Login Method** to avoid conflicts.
- After you set a root password by using the User Data, a clear text password will be displayed in the User Data field on the details page of the created VM instance. Very that you keep your password confidential.
- When you import the User Data to a Linux VM instance, note the following:
  - Cloud-init must be installed for the VM image. Recommended versions: 0.7.9, 17.1, 19.4 , and the later versions.
  - If you create a Linux VM instance by using a VM image that has Cloud-init installed, you must import the User Data. Otherwise, the Cloud-init task will wait until the task times out .
  - The following is an example of importing the 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 be realized by following the steps below:

    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 content to the file.

3. Set the hostname, enable the root user, allow the SSH login with passwords, and change the root password.
4. Run the `echo ls -l /` command.

— When you import the User Data to a Windows VM instance, note the following:

- Cloudbase-Init must be installed for the VM image. The version of the Cloudbase-Init is not enforced. For information about how to install Cloudbase-Init, see *Cloudbase Documentation*.
- If you create a Windows VM instance by using a VM image that has Cloudbase-Init installed, you must import the User Data. Otherwise, the Cloudbase-Init task will wait until the task times out.
- 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 script above creates **b64**, **b64_1**, and **gzip** files under C drive when the VM instance is started.

Note:

When the User Data is used, one L2 network can only let you configure one L3 network.

Note:

When you use the User Data, notice that you can configure only one L3 network for an L2 network.

- Change platform:

Change the platform of the VM instance. Options: Linux | Windows | WindowsVirtio | Other | Paravirtualization. Linux, WindowsVirtio, and Paravirtualization support Virtio drivers, while

Windows and Other use devices simulated by QEMU. Restart the VM instance before all settings take effect.

- Change session count:

  Set the maximum number of sessions accessible to the VM instance under the VDI scenario. Default value: 1. Once you change the value, the settings will take effect after the VM instance is rebooted. The SPICE mode is supported.

- Attach NIC:

  Select available networks to attach to the VM instance from the available L3 network list.

- Detach NIC:

  Detach the NICs from the VM instance. If the VM instance does not have any NIC, the VM instance will fail to be started after it is stopped. Make sure that you attach at least one NIC to the VM instance.

- Change default network:

  Let you change the default network for the VM instance. Ensure that you restart the network service before all settings take effect.

- Set MAC:

  Specify a MAC address when you create a VM instance. After you stop the VM instance, you can set or modify the MAC address.

- Set specified IP:

  Set a specified IP address for the VM instance. Select an available IP address for the VM instance from the available IP range to avoid IP conflicts.

- Attach GPU device:

  Attach the GPU device of a host to the VM instance. Hence, the GPU device is used solely by the VM instance. However, you cannot perform migrations for the VM instance that attaches the GPU device.

- Detach GPU device:

  Detach the GPU device from the VM instance.

- Attach USB device:

  Attach a USB device for the VM instance by enabling the USB passthrough feature. Once a USB device is attached to a VM instance, the USB device can be solely used by the VM instance. All USB devices attached by one VM instance can only run on the same host.

- Detach USB device:

  Detach the USB device from the VM instance.
- Attach GPU specification:

  Attach GPU specifications for one or more VM instance.

  Note:
  If the VM instance has already attached a GPU specification, GPU device, or if the VM instance is in the running state, this VM instance cannot attach another GPU specification.
- Change GPU specification:

  Change a GPU specification for one or more VM instances.

  Note:
  - If the VM instance has not attached any GPU specification, or if the VM instance is in the running state, you cannot change the GPU specification for the VM instance.
  - After you change the GPU specification, you can attach a GPU device by using the latest GPU specification to the VM instance when the VM instance is started next time. Also, you can detach the GPU device associated to the original GPU specification from the VM instance.
- Cancel GPU specification:

  Cancel the GPU specification of one or more VM instances.

  Note:
  If the VM instance has not attached any GPU specification, or if the VM instance is in the running state, you cannot cancel the GPU specification.
- Attach other peripheral devices:

  Attach other peripheral devices to the VM instance by enabling the feature of other peripheral devices.
- Detach other peripheral devices:

  Detach other peripheral devices from the VM instance.
- Scheduled job:

Create a scheduled job. Create a scheduled job based on a scheduler. Scheduled tasks such as stopping VM instances, starting VM instances, rebooting VM instances, and creating VM snapshots.

- Alarm:

  Create an alarm and add related alarm metrics. The system can automatically monitor multiple alarm metrics such as added CPU, disks, NICs, and memories of VM instances, and pushes alarm messages to you via email, DingTalk, HTTP application, and short message service.

  If you want to use some specific alarm metrics, install agents for your VM instances in advance. For more information about how to install an agent, see *Internal Monitoring*.

  Note:
  Compared to the external monitoring, the internal monitoring is more accurate. We recommend that if you want to monitor the internal data, use the internal monitoring.

- Audit:

  Let you audit all operations of a VM instance to effectively safeguard the security of your core data on your cloud environment.

A VM instance lets you perform multiple operations. All settings take effect after different constrains are followed, such rebooting the VM instance, stopping the VM instance, or keeping the VM instance running. Different operations can be performed according to different constrains as follows:

Reboot VM	Stop VM	Running VM
• Set the NUMA architecture • Change the graphics card type • Change the CPU mode of the VM instance • Change the cache mode of the VM instance • Change the console mode of the VM instance • Set or cancel the console password of the VM instance • Set the USB redirection	• Start the VM instance • Migrate storages • Change the operating system • Restore snapshots • Enable the specified host • Set the MAC address • Reimage the VM instance • Set or cancel the specified IP address	• Clone the VM instance • Network Anti-Spoofing • Bind or unbind affinity groups • Create or delete snapshots • Create, delete, attach, or detach volumes • Create volume images • Create VM images • Create backup tasks (Both the enterprise version and the hybrid version are supported)

Reboot VM	Stop VM	Running VM
• Set the platform type • Set the boot order		• Create or delete scheduled jobs • Change the owner • Change the password online • Attach or detach NICs • Attach or detach GPU devices • Attach or detach ISO images • Attach or detach USB devices • Set or cancel NIC QoS • Set or cancel volume QoS • Set QGA • Set the RDP mode • Set the maximum login sessions for VDI devices • Set high availability • Resize volumes • Set VM high availability in the Settings • Migrate the VM instance online (shared storages) • Set over-provisioning ration of primary storages in the Settings • Set the usage threshold for primary storages in the Settings • Change memories online • Change the expunge period • Change the instance offering • Resize the root volume • Attach or detach the tag • Create the backup • Add or delete the SSH Key • Set the resource priority

Reboot VM	Stop VM	Running VM
		• Set the cross-cluster high availability policy

Notice

When you use a VM instance, note the following:

- If the snapshot chain of the VM instance is long, the I/O performance of the VM instance may be getting poor.
- After you set a name for the host, make sure that you do not set the host name again with User Data to avoid conflicts.
- When you inject the User Data into the VM instance, note the following:
  - Before you inject the User Data, make sure that User Data network services and DHCP network services work normally. By default, User Data network services and DHCP network services are enabled in the scenarios of flat networks, vRouter networks, or VPC networks.
  - Install Cloud-init for the images of Linux VM instances in advance. Also, install Cloudbase-Init for the images of Windows VM instances in advance.
  - To check whether the User Data is injected into a Linux VM instance, go to *`/var/lib/cloud/instance/user-data.txt`*. If this file path does not contain the User Data, log in to the host where the VM instance resides, and run the following commands:
    - Run `ps -ef|grep http` to check whether the host has contained the User Data.
    - Run `ip netns` to obtain namespace.
    - Run `ip netns exec namespace ip a` to check whether namespace has obtained the target IP address.

      For example,

```
# Obtain namespace:
 br_eth0_1101_f8e41fc3a3b9431d9ea5f2bf090e085e
[root@localhost ~]# ip netns
br_eth0_1101_f8e41fc3a3b9431d9ea5f2bf090e085e (id: 0)
# Check whether namespace has obtained the target IP address:
169.254.169.254
[root@localhost ~]# ip netns exec
 br_eth0_1101_f8e41fc3a3b9431d9ea5f2bf090e085e ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
10: inner0@if11: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
 qdisc pfifo_fast state UP qlen 1000
    link/ether 2e:6d:a4:6c:ab:79 brd ff:ff:ff:ff:ff:ff link-
netnsid 0
    inet 10.1.164.230/24 scope global inner0
```

```
        valid_lft forever preferred_lft forever
    inet 169.254.169.254/32 scope global inner0
        valid_lft forever preferred_lft forever
    inet6 fe80::2c6d:a4ff:fe6c:ab79/64 scope link
        valid_lft forever preferred_lft forever
```

- By default, data volumes adopt Virtio devices. To detect and identify the Virtio devices, install the corresponding drivers. All Linux distributions have defaulted to integrate Virtio drivers. However, you need to install manually the Virtio drivers in your Windows.
- For shared volumes, you must use the Virtio SCSI volumes. VM instances that attach the Virtio SCSI volumes can read and write the volumes. Ceph primary storages support shared volumes .
- If you want to use the GPU passthrough feature, enable the IOMMU or VT-d options on BIOS of the host in advance.
- When a VM instance has multiple NICs, if you change the default NIC, restart the network services within the VM instances before all settings take effect.
- We recommend that Linux volumes that are automatically attached to your VM instance after the VM instance starts are written on `/etc/rc.d/rc.local`, and executable permissions are provided. However, we recommend that you do not change the `/etc/fstab` file of the VM instance. After you detach the volumes dynamically, if you reboot the VM instance, the VM instance may fail to be started in which the VM instance cannot find the volume information defined by `/etc/fstab`.

  — We recommend that you perform the following operations:

  Go to `/etc/rc.d/rc.local`, and run `mount` to mount volumes to your VM instance as follows:

  ```
  # chmod +x /etc/rc.d/rc.local
  # mount -t Target mount path of the volume ID
  ```

  Note:

  We recommend that you attach volumes by using their file system UUIDto VM instances rather than using drive letters similar to */dev/vdb*.

- The VM instance will inherit its BIOS mode, including Legacy and UEFI.

  Note:

  - You need to get the corresponding image ready, and select a proper BIOS mode. For more information, see *Add Image*.

- 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.
- For ZStack 3.3.0 and later versions:
  - For beginners who install the Cloud for the first time, if your VM instances are booted from the UEFI mode, the motherboard type defaults to Q35. If your VM instances are booted from the Legacy mode, the motherboard type defaults to i440FX.
  - For users who want to upgrade the Cloud, upgrade the Cloud from the historical versions to 3.3.0 or later versions. Assume that your VM instances are booted from the UEFI mode. If the previous motherboard type is i440FX, the motherboard type will change to Q35 by default after the Cloud is upgraded.
  - 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.

Operating System	BIOS Mode	Supported Version
Windows	UEFI	• Windows 8 or later versions
	UEFI (compatibility module)	• Windows 7 • Windows Server 2008 R2
Linux	UEFI	• CentOS 7.2 • CentOS 7.3 • CentOS 7.4 or later versions

- In the Global Settings, after you enable the NUMA option, you can change the CPU and memories for your VM instances online, and ensure that you note the following:
  - We recommend that you do not change the CPU and memories for Windows VM instances online in production environments.
  - You can only expand the CPU and memories for the running VM instances. If you need to downsize the CPU and memory for the running VM instances, stop the VM instances.

- If you want to expand the memories for the running VM instances, but VM instances cannot automatically activate the new memories, run the following two commands:

```
% echo online > /sys/devices/system/memory/auto_online_blocks
% echo online > /sys/devices/system/memory/memoryXXX/state
```

  For more information, see *How to online memory*.

- If an IPv6 network is used by VM instances, note the following:
  - If you want to create VM instances by using a network with the IPv6 type or IPv4+IPv6 type, run the dhclient -6 NIC_NAME command to manually obtain an IP address.
  - We recommend that you use only one IPv6 IP address for a VM instance to avoid potential risks.
  - If the IP address type of the L3 network (including public network, flat network, and VPC network) is changed, restart the VM instances that use this network for the configurations to take effect.

7.2 Volume

A volume provides storages for VM instances. A volume can either be a root volume or a data volume.

- Root volume: A system disk where the VM instance operating system is installed.
- Data volume: A data disk that provides additional storages for a VM instance.

Data volumes are mainly involved in the volume management.

Volume Operations

- Enable:

  Enable the disabled volumes. Afterwards, you can attach the volumes to a VM instance. If you have already attached the volumes to the VM instance, disabling the volumes will not affect your business continuity. After you detach the volumes from the VM instance, you can no longer attach the volumes to the VM instance.

- Disable:

  Disable the enabled volumes. Afterwards, the volumes cannot act as candidates that can be attached to other VM instances.

- Attach:

Attach volumes to a VM instance. You can attach the volumes to the VM instance that are in the running state or stopped state.

- Detach:

  Detach volumes from a VM instance. After you detach the volumes from the VM instance, you can attach the volumes to other VM instances.

- Migrate:

  Migrate volumes. After you detach the volumes attached by a local storage, you can migrate the volumes to other hosts. After migration, you can attach the volumes to other VM instances that run on the target host.

- Create backup task:

  Create a backup task for the current VM instances or volumes. The VM instances will be backed up as images, while the volumes will be backed up as volume backups.

- Create image:

  Create volume images. Volumes can be encapsulated as images which can be used to create more volumes. Also, the volumes on a Ceph primary storage can be encapsulated to an ImageStore backup storage.

- Resize volume:

  Let you resize volumes online. Resize data volumes as needed. After data volumes are resized, the capacities will take effect in real time. Data volumes can only be expanded at the minimum of 4 MB rather than be downsized.

- Create snapshot:

  Create volume snapshots. Before you perform any important operations, reserve the temporary state of the root volumes or data volumes at a specific time point. Hence, you can quickly perform rollbacks for the root volumes or data volumes when failures occur. If you need long-term backups, select related features of backup services.

  - In a production environment, we recommended that you limit the number of snapshots per disk within 5. Excessive snapshots might affect the I/O performance, data security, and primary storage capacity of the corresponding VM instances and volumes. For long-term backups, we recommend that you use disaster recovery related services.
  - Currently, you cannot create snapshots for shared volumes.

- The snapshot of the volume on the Ceph primary storage does not occupy capacity. Therefore, the displayed snapshot capacity is the real capacity of the volume when the snapshot was created.
- For Ceph primary storages, the volume snapshot capacity might fail to be obtained. Here are some statements:
  - Open source Ceph (version H) and enterprise-level Ceph (earlier than 3.2.0) cannot obtain volume snapshot capacity.
  - Due to the RBD format, enterprise-level Ceph (3.2.0 and later versions) may fail to obtain VM snapshot capacity.

Similar to creating snapshots for root volumes of a VM instance, after you detach the volumes from the running VM instance, you can also create snapshots.

Note:

- Snapshots, a **short-term solution**, mainly can be used in test and development environments. Specifically, these snapshots can quickly be used for packing, upgrading, or testing your Cloud. When normal failures appear, rollbacks can be performed. We recommend that you do not use snapshots in your production environment. However, under some circumstances, snapshots can still be applied to your production environment. For example, if you perform dangerous operations, the probable damage to the operating system may occur due to upgrading or configuration modifications. Then, snapshots are a preferred solution.
- We recommend that you do not use snapshots in your production environment. The following are the two probable considerations:
  - Data integrity

    When you use snapshots, you are not creating a copy of the virtual hard disk. But actually, you need to create a copy of the VM virtual disk. If the virtual disk is damaged, the snapshot will be invalid, which means that the snapshot cannot be used to recover the damaged disk. Notice that the snapshot cannot be used to solve disk failures. So, you will still encounter a **single point of failure**.
  - VM performance

    Using too many snapshots will influence the performance of a VM instance. For example, if the old snapshot runs on the VM instance with excessive overloads, this old

snapshot will be increased in size, and then the performance of the VM instance will be definitely slowed down. Or, if you create a large number of snapshots, the performance of the VM instance will be also slowed down.

Reserving a snapshot of a VM instance for a long time is a common mistake. The snapshot will increase in size as the time goes by. Also. the snapshot files will also be changed, and are not stored on the source disk. Hence, restoring the snapshot will take a long time. Also, during restoring, the VM instance may be forced to stop.

- Restore snapshot:

  Restore volumes to the current snapshot point. Before you restore snapshots, stop the VM instance that attaches the volumes or detach the volumes from the VM instance.

- Delete snapshot:

  Delete the unnecessary the volume snapshots.

  Note:

  - Snapshots created on local storage, NFS, SMP, and Shared Block storages have a tree structure. Deleting the root snapshot will also delete snapshots on the branches and detach the batch snapshots on the branches. Please exercise caution.
  - Snapshots created on the Ceph shared storage are independent and do not have a tree structure. Deleting a snapshot will not affect other snapshots.
  - When you delete snapshots in a tree structure in bulk, the cloud automatically calculates and deletes the candidate snapshots and cascades the delete operation to the associated snapshots.
  - If the snapshots to be deleted contain batch snapshots, note that:
    - Deleting a batch snapshot will also delete the data volume snapshots in the batch snapshot and the snapshots on the branches. Please exercise caution.
    - Deleting single snapshots and batch snapshots in bulk will also delete the single snapshots on the branches and detach the batch snapshots on the branches.

- Change owner:

  Change the owner of the volumes to other regular accounts.

- Migrate storage:

  Volumes support migrations across network shared storages. Currently, Ceph and NFS storage migrations are supported.

- Migration across Ceph primary storages:
  - Volumes to be migrated across Ceph primary storages cannot be attached to any VM instance.
  - Shared volumes that are not attached to VM instances can be migrated across Ceph primary storages. However, shared volumes that have been attached to VM instances cannot be migrated across Ceph primary storages.
  - To migrate between two Ceph primary storages, make sure that the Ceph MON nodes between these two Ceph primary storages are interconnected.
- Migration across NFS primary storages:
  - Volumes that are migrated across NFS primary storages cannot be attached to any VM instance.
  - To migrate volumes between two NFS primary storages, make sure that the destination NFS primary storage can be attached to the cluster of the volumes to be migrated.
- Migration across SharedBlock primary storages:
  - Volumes on SharedBlock primary storages can be attached to VM instances that are in the stopped state and migrated across SharedBlock primary storages.
  - Shared volumes that are not attached to VM instances can be migrated across SharedBlock primary storages. However, shared volumes that are attached to the VM instances cannot be migrated across SharedBlock primary storages.
  - To migrate volumes between two SharedBlock primary storages, make sure that the destination SharedBlock primary storage can be attached to the cluster of the volumes to be migrated.

- Delete:

  Delete the attached, unattached, or uninstantiated volumes. If you delete the uninstantiated volumes, the volumes will be deleted immediately. After deletion, the system will no longer record these volumes.
- Restore:

  Restore the deleted volumes to the running state.
- Expunge:

  Expunge the deleted volumes. The system will no longer record these volumes, and delete the actual data.

- Scheduled job:

  Create scheduled jobs based on schedulers. Currently, scheduled jobs of the volumes only support scheduled snapshot jobs of the data volumes, such as creating snapshots, enabling snapshots, disabling snapshots, and deleting snapshots.

Notice

When you use volumes, note the following:

- Volumes are hypervisor specific. That is, a volume that has been attached to a VM instance of one hypervisor type cannot be attached to a VM instance of another hypervisor type. For example, a volume of KVM VM instances cannot be attached to VMware VM instances.
- A volume can have two sizes: real size and virtual size. The real size is the size that a volume actually occupies in the storage system, while the virtual size is the size that a volume claims for. The virtual size is usually greater than or equal to the real size. As the number of written files increases, the real size will gradually increase.
- A volume (excluding shared volumes) can only be attached to one VM instance at any given time. Ceph and Shared Block primary storages support shared volumes. A shared volume can be identified and accessed by multiple VM instances at the same time.
- A root volume is always attached to its owner VM instance and cannot be detached.
- A data volume can be attached to or detached from different VM instances of the same hypervisor type.
- In the environment where multiple primary storages are available, you can specify a primary storage to create a volume. If no primary storage is specified, the default creation method is as follows:
  - For local primary storages, volumes are created from the primary storage with large capacity.
  - For NFS primary storages, volumes are created from a random primary storage.
  - For mixed primary storages (local + NFS/Shared Mount Point), volumes are created from the primary storage where the root volume of the volume does not locate.
- You can set QoS for data volumes to limit the disk bandwidth. Note that excessive low QoS might cause low I/O performance.
- When volumes are stored on a primary storage, verify that the primary storage is available and is in the connected status before the volumes can work normally.
- When you create volumes, specify disk offerings.

- When you create volumes, if you do not specify a primary storage, the created volumes are uninstantiated.
- Uninstantiated volumes do no occupy any storage space. Only if the volumes are attached to VM instances, the volumes will be instantiated and occupy actual storage spaces.
- After you specify a primary storage, if the specified disk offering exceed the availably virtual capacities of the current primary storage, you will prompt for insufficient capacities of the primary storage.
- If the specified primary storage is LocalStorage, select available hosts attached by the cluster in the primary storage.
- VirtioSCSI volumes adopt the VirtioSCSI bus. Volumes fall into the SCSI category, provides the I/O multi-queue support, and can be identified by WWN (World Wide Name).
- A Ceph primary storage supports shared volumes which can be identified and accessed simultaneously by multiple VM instances.
- After you detach the volumes in a local storage from a VM instance, these volumes can be migrated to other hosts. After migration, you can attach these volumes to the VM instances on a new host.
- You can create snapshots for volumes, indicating that you can back up data of the volumes at a specific time point. When the data are lost, you can effectively restore the data by using rollbacks. Notice that snapshots created on a LocalStorage primary storage, NFS primary storage, and Shared Mount Point primary storage are tree mode. Deleting the tree root snapshot (root snapshot in the tree) will delete the tree leaf snapshots (snapshots in the branch of the tree) as well. Snapshots created on a Ceph storage are independent. Deleting a snapshot will not affect other snapshots.
- Volume snapshots are all incremental. Exercise caution. After restoration, the data of the snapshot point will be recovered, and all data in the volumes will be overwritten.
- Volume strategy with multiple primary storages:
  - When you have multiple primary storages, you can specify a primary storage to create volumes.
  - Assume that a primary storage is not specified, note the following:
    - If you have multiple LocalStorage primary storages, a primary storage with availably large capacities will be prioritized to create a volume for a VM instance when you create the VM instance.

  - If you have multiple NFS primary storages or SharedBlock primary storages, a type of primary storage will be randomly selected to create a volume for a VM instance when you create the VM instance.
  - If you have LocalStorage+NFS/Shared Mount Point/Shared Block primary storages, a type of primary storage different from the same primary storage where the current root volume resides will be selected by default to create a volume for a VM instance.
- You can set QoS to limit the disk bandwidth for volumes. Notice that QoS must not be underused. The underused QoS will lead to poor I/O performance.
- Attaching or detaching volumes are dynamical, while `/etc/fstab` of a VM instance is a static configuration file. Assume that you change the fstab file of a VM instance after you attach a volume to the VM instance, and then detach the volume from the VM instance. Once the VM instance is rebooted, the VM instance will fail to be started. The VM instance is hung or suspended so that it cannot be started, because the fstab file does not contain any corresponding information.

  We recommend that you perform the following operations:

  - Go to `/etc/rc.d/rc.local`, and run the **`mount`** command to mount volumes to your VM instance as follows:

    ```
    # chmod +x /etc/rc.d/rc.local
    # mount -U UUID of the file system Target mount path
    ```

    Note:
    We recommend that you attach a volume to VM instances rather by using the file system UUID of the volume than using drive letters similar to `/dev/vdb`.

7.3 Image

An image is an image template used by a VM instance or volume.

- Image templates include root volume images and data volume images.
- Root volume images can be in the format of ISO or Image, while data volume images can be in the format of Image.
- The Image format can either be raw or qcow2.
- Images are stored on backup storage. If you are creating VM instances or volumes for the first time, the images will be downloaded to primary storage and stored as image caches.

When you create a VM instance, the type of the image platform decides whether to use a KVM Virtio driver (including disk driver and NIC driver). The supported image platforms are as follows:

- Linux: Uses a Virtio driver.
- Windows: Not to use a Virtio driver. Instead, QEMU is used. The image operating system is a Windows OS without a Virtio driver installed.
- WindowsVirtio: Uses a Virtio driver. The image operating system is a Windows OS with a Virtio driver (including disk driver and NIC driver) installed.
- Other: Not to use a Virtio driver. Instead, QEMU is used. The image operating system can be of any types.
- Paravirtualization: Uses a Virtio driver. The image operating system can be any operating system with a Virtio driver installed.

To add an image, add a URL or upload a local file.

1. URL: Adds an image through the specified URL.
   - *HTTP/HTTPS*:
     - Format: *http://path/file* or *https://path/file*
     - Example: *http://cdn.zstack.io/product_downloads/images/zstack-image.qcow2*
   - *FTP*:
     - Anonymous format: *ftp://hostname[:port]/path/file*

       Example: *ftp://172.20.0.10/pub/zstack-image.qcow2*
     - Non-anonymous format: *ftp://user:password@hostname[:port]/path/file*

       Example: *ftp://zstack:password@172.20.0.10/pub/zstack-image.qcow2*
   - *SFTP*:
     - Format with password specified: *sftp://user:password@hostname[:port]/path/file*

       Example: *sftp://root:password@172.20.0.10/pub/zstack-image.qcow2*
     - Password-free format: *sftp://user@hostname[:port]/path/file*

       Example: *sftp://root@172.20.0.10/pub/zstack-image.qcow2*
   - The absolute path on backup storage, which supports SFTP backup storage and ImageStore.

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

Note:

- Before you enter a URL, make sure that the URL can be accessed by a backup storage and the corresponding backup storage file exists.
- Before you upload an image by using the *SFTP* password-free method, make sure that password-free SSH access can be achieved between a backup storage and the SFTP server.
- Smooth, continuous display of progress bar, and breakpoint resume:
  - The ImageStore backup storage supports smooth, continuous display of progress bar, and breakpoint resume.
  - The Ceph backup storage supports smooth, continuous display of progress bar, but does not support breakpoint resume.
  - The SFTP backup storage does not support smooth, continuous display of progress bar , or breakpoint resume.
- If you upload an image by using `file:///`, make sure that:
  - The Ceph backup storage currently does not support the *file:///* format.
  - The `file:///` path contains three forward slashes (/), which correspond to the **absolute path** of the backup storage. For example, `file:///opt/zstack-dvd/zstack-image-1.4.qcow2`. The *zstack-image-1.4.qcow2* file needs to be stored in the `/opt/zstack-dvd` directory of the backup storage.

2. Upload a local file: You can upload an image that can be accessed by your current browser. Both ImageStore and Ceph backup storages are supported.

Note:

When you add an image by uploading a local file, you use the local browser as a transit point. Therefore, do not refresh or close the current browser, and do not stop the management node service. Otherwise, the image might fail to be added.

Image Operations

- Enable:

  Enable the disabled images. These images can act as candidates used to create VM instances .

- Disable:

Disable images. These images cannot act as candidates used to create VM instances.

- Export:

  Export ImageStore images. You can download the images directly. By default, the exported images are stored on the *export* subdirectory under the ImageStore directory. The details pages of the exported images can display MD5 values of the images. These values can be used to authenticate whether the downloaded images and the exported images are the same.

  For SFTP backup storages, you can copy directly the path where the images are stored, and export the images.

  For Ceph backup storages, you can export manually the images by running `rbd export` via the Pool information where the images are stored.

- Share to all:

  Share images to all accounts. Hence, all regular accounts and project users can use these images.

- Share:

  Share images to one or more regular accounts or project users.

- Recall from all:

  Recall images from all regular accounts and projects users. Recalling the images from all regular accounts and project users does not affect independent image sharing. You can specify some images. Hence, regular accounts and project users can still use these images.

- Recall:

  Recall images from the specified regular accounts and project users.

- Change owner:

  Change the owners of the images to the regular accounts and project users.

- Migrate storage:

  Migrate the data of the images across network shared storages. Currently, migrations for the images can be performed across Ceph backup storages.

  Migrate the images on a Ceph backup storage to other Ceph backup storages. After migration, the new Ceph backup storages can use these images, while the original Ceph backup storage will no longer reserve these original images. Before storage migrations are performed, make sure that the target Ceph backup storage has sufficient capacities.

- Delete:

  Delete images. To expunge or restore the images, delete them first.
- Restore:

  Restore the deleted images to the running state.
- Expunge:

  Expunge the deleted images. Then, the actual data on the backup storage will be deleted.
- Download exported image:

  Download the exported images to the corresponding local disk via a browser.
- Copy URL:

  Copy the URLs of the images, and add them to other clouds. Also, you can download these URLs by using wget directly.
- Delete exported image:

  Remove the exported images from a backup storage. These images will no longer occupy storage capacities.
- Change platform:

  Change the platform type for images. Afterwards, the new VM instances will determine which device drivers will be used according to the new type of platform. Platform options: Linux | Windows | WindowsVirtio | Other | Paravirtualization. Linux, WindowsVirtio, and Paravirtualization adopt Virtio drivers, while Windows and Other adopt QEMU emulation devices.
- Change QGA option:

  Enable the QGA option. Before you enable this option, make sure that you have preinstalled and run `qemu-guest-agent` in the images. After you enable this option, the VM instances with these images let you change the VM passwords.
- Refresh capacity:

  Refresh the actual capacities of the backup storage where the images reside.

Notice

When you use an image, note the following:

- The image URL that you entered must be accessible to backup storages, and contain this image. If the backup storages cannot access the URL, you will prompt for the image download failure.

- If you select `Qemu guest agent`, verify that you have installed `qemu-guest-agent` for the image. By default, the VM instances that you are creating let you change the VM passwords.
- An admin can share this image to a regular account. After sharing, the regular account can create VM instances by using this image.
- The regular account can create VM instances by either adding other images or using the image shared by the admin. The regular account can delete the images added by himself, but cannot delete the image shared by others.
- After you stop the image, this image cannot act as a candidate used to create VM instances.
- The image capacity is the virtual capacity, namely the virtual size of this image. The actual capacity of the image is the space of a backup storage occupied by this image, similar to the file size read by `du -sm`.
- ImageStore images can be exported. After you export the images, you can download the images via URLs.
- An image supports two types of BIOS mode: Legacy and UEFI. When you create VM instances, the BIOS mode in the image will be inherited to the VM instances. Exercise caution. Mismatch of the BIOS mode may lead to abnormalities of the VM instances.
  - Legacy: Support all operating systems. To ensure the usage stability, we recommend that you use the Legacy mode.
  - UEFI: Support two types of operating system, including Windows and CentOS. Specifically, Windows 7 and Windows Server 2008 R2 must use the Compatibility Support Module (CSM).
  - For a qcow2 image or raw image, select the BIOS mode that is consistent with the encapsulated image.
  - For an ISO image, select a BIOS mode as needed. The system will be installed in a wizard mode according to the BIOS mode that you selected.
  - If the VM instances that you created need to use the UEFI mode, we recommend that you select the corresponding VM image from the following list of operating system versions.

Operating System	BIOS Mode	Supported Version
Windows	UEFI	• Windows 8 or later versions
	UEFI (compatibility module)	• Windows 7 • Windows Server 2008 R2

Operating System	BIOS Mode	Supported Version
Linux	UEFI	• CentOS 7.2 • CentOS 7.3 • CentOS 7.4 or later versions

- For a Linux image of CentOS 7.4 or later versions with the UEFI mode, after you restart a created VM instance, the VM instance will probably enter the UEFI Shell. To reboot successfully and enter the operating system, follow the methods below:

  - Method 1: Add a script to automatically skip the UEFI Shell and directly enter the operating system.

    In the operating system that you installed successfully, run `vim /boot/efi/startup.nsh` to create a script and save the following contents. For the later VM rebooting operation, the VM instance will skip the UEFI Shell and directly enter the operating system.

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

  - Method 2: Manually exit the UEFI Shell.

    If the VM instance already entered the UEFI Shell, you could manually run the following commands to exit the UEFI Shell:

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

- For a Windows VM instance (such as Windows Server 2012 R2, Windows Server 2016, and Windows 10) with the UEFI mode, the following page will be displayed after the VM instance starts. Press any key to continue the installation of the VM operating system. Otherwise, the VM instance will enter the UEFI Shell, as shown in *Press Any Key to Continue*.

Figure 7-1: Press Any Key to Continue

If the VM instance already entered the UEFI Shell, you must run the following commands before you boot the operating system:

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

After you perform the preceding operations, press any key to continue the VM operating system installation. Otherwise, the VM instance will enter the UEFI Shell again.

7.4 Affinity Group

An affinity group is a simple orchestration policy designed for IaaS resources to ensure your business high performances or high availability.

Affinity Group Policy

Currently, ZStack provides two affinity group policies to better manage VM instances and hosts: anti-affinity group (soft) and anti-affinity group (hard).

- Anti-affinity group (soft):

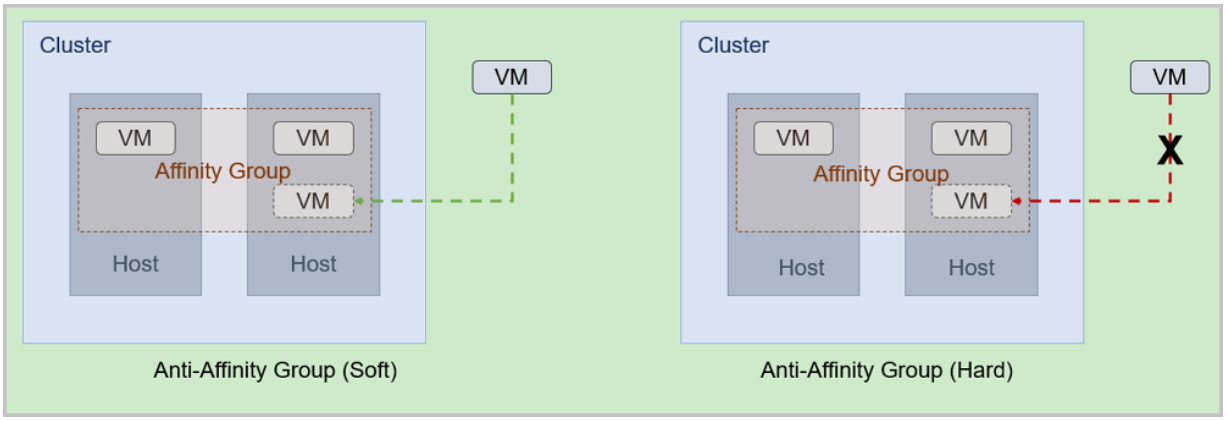
  Allocate VM instances in the affinity group to different hosts as much as possible. If no more hosts are available, the VM instances will be allocated randomly.

- Anti-affinity group (hard):

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

The logic of these two anti-affinity groups is shown in *Figure 7-2: Anti-Affinity Group (Soft) and Anti-Affinity Group (Hard)*.

Figure 7-2: Anti-Affinity Group (Soft) and Anti-Affinity Group (Hard)



Usage Scenario

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 nodes with different Hadoop 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, you might know that deploying these 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, which 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 business VM instances to run an active and a standby MySQL database respectively, and requires that the active and standby databases cannot be down at the same time. Therefore, 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.

Affinity Group Operations

You can perform the following operations on an affinity group:

- Create: Create a new affinity group in the current zone.
- Enable: Re-enable the selected affinity group to check whether VM instances within the affinity group can satisfy the affinity group policy. If the affinity group policy is met, the affinity group will be enabled successfully, or vice versa.
- Disable: Disable the affinity group that you selected. Then, VM instances within the group will stop following the affinity group policy.
- Bind VM instance: Bind new VM instances to the affinity group. Then, the affinity group policy will take effect immediately.
- Unbind VM instance: Unbind VM instances from the affinity group. Then, the affinity group policy will take effect immediately.
- Change owner: Change an owner for the affinity group.
- Delete: Delete the affinity group that you selected. Then, VM instances within the group will no longer follow the affinity group policy when starting next time.

A VM instance allows you to perform the following operations on an affinity group:

- Create VM instance by specifying affinity group: Specify an affinity group when you create a VM instance. Then, the VM instance will be created based on the specified affinity group policy.
- Clone VM instance by specifying affinity group: Specify an affinity group when you clone a VM instance. Then, the VM instance will be cloned based on the specified affinity group policy.
- Bind affinity group: Bind the VM instance to the affinity group. Then, the affinity group policy will take effect for the VM instance.
- Unbind affinity group: Unbind the VM instance from the affinity group. Then, the affinity group policy will take effect immediately for the VM instance.

Notice

- Currently, the affinity group policy supports two types of affinity group: affinity group (soft) and affinity group (hard). These two types support the HOST type, which means that an affinity relationship between VM instances and hosts can be formed.
- The number of VM instances that an affinity group can bind is not limited. In addition, the affinity group does not have quota limits, indicating that you can create limitless affinity groups.
- The scope of an affinity group is the entire zone where the effect object is all hosts that meet the constraints.

- One VM instance can be bound by only one affinity group at a time.
- To change an affinity group to which a VM instance belongs, make sure that this VM instance is in the running state or stopped state.
- After you change an affinity group for a VM instance on a local storage, the VM instance will be preferentially started on the host where the VM instance is running last time without following the new group policy. This helps to avoid unnecessary migrations.
- After you change an affinity group for a VM instance on a shared storage, the VM instance will be started according to the new group policy.
- If you bind or unbind a VM instance, the affinity group policy will take effect immediately. Only when you bind VM instances that are in the stopped state on a shared storage to an affinity group, the group policy takes effect when the VM instances are started next time.
- Migrating VM instances will also follow an affinity group policy.
- By default, all vRouters and VPC vRouters belong to one affinity group, known as system affinity group, where anti-affinity group (soft) is adopted. Specifically, this affinity group only allows you to perform enabling and disabling operations except for other operations.
- Admin accounts and regular accounts are all allowed to create affinity groups.
- Admin accounts can manage all affinity groups, while regular accounts can only manage the affinity groups owned by themselves.
- When you create a VM instance, if you specify an affinity group and a host simultaneously via the VM advanced settings, note the following:
  - With an anti-affinity group (soft),
    - When the specified host satisfies the condition to create VM instances, but does not meet the specified anti-affinity group policy (soft), you can create these VM instances successfully.
    - When the specified host does not satisfy the condition to create VM instances, you fail to create these VM instances.
  - With an anti-affinity group (hard),
    - When the specified host satisfies the condition to create VM instances, but does not meet the specified anti-affinity group (hard), you fail to create these VM instances.
    - When the specified host does not satisfy the condition to create VM instances, you fail to create the VM instance.

7.5 Instance Offering

An instance offering is the count or specification of the CPU, memory, the host allocation strategy, disk bandwidth, and network bandwidth, for a VM instance.

Host Allocation Strategy

The host allocation strategies include host with min. running VMs, host with min. CPU utilizatio n, host with min. memory utilization, host with max. running VMs, host where the VM located last time, and random allocation. Default strategy: Host with min. running VMs. Each strategy is described as follows:

- **Host with min. running VMs**: The host with the minimum number of running VM instances will be chosen to create VM instances.
- **Host with min. CPU utilization**: The host with the minimum CPU utilization will be chosen to create VM instances.

  Note:

  - The system collects the host CPU loads over a period of time, calculates the average CPU usage during this period, and then selects the host with the lowest CPU usage to create VM instances.
  - By default, the data collection cycle is 10 minutes. To change the collection cycle, go to **Settings** > **Global Settings** > **Advanced**, locate **Minimum interval of Host collecting CPU usage**, and click the **Edit** icon.
- **Host with min. memory utilization**: The host with the minimum memory utilization will be chosen to create VM instances.

  Note:

  - The system collects the host memory loads over a period of time, calculates the average memory usage during this period, and then selects the host with the lowest memory usage to create VM instances.
  - By default, the data collection cycle is 10 minutes. To change the collection cycle, go to **Settings** > **Global Settings** > **Advanced**, locate **Minimum interval of Host collecting Memory usage**, and click the **Edit** icon.
- **Host with max. running VMs**: The host with the maximum number of running VM instances will be chosen to create VM instances. To use this option, you need to set the maximum

number of VM instances that can run on a host. Then, the system 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. If you start a new VM instance for the first time, the system selects a host randomly.
- **Random allocation**: The system randomly selects a host to create VM instances.

Instance Offering Operations

You can perform the following operations on an instance offering:

- Create instance offering: Create an instance offering.
- Enable: Enable an instance offering that is in the disabled state. **Batch operations are supported.**
- Disable: Disable an instance offering. After an instance offering is disabled, you cannot use it to create a VM instance. However, existing VM instances are not affected. **Batch operations are supported.**
- Share to all: After an instance offering is shared globally, it can be used by all accounts. **Batch operations are supported.**
- Recall from all: After an instance offering is recalled globally, it becomes invisible to other accounts. **Batch operations are supported.**
- Delete: When you delete an instance offering, a dialog box will be displayed, prompting you to confirm the delete operation. **Batch operations are supported.**
- Search: You can search for an instance offering by its name, UUID, or by using the advanced search.

Notice

When you use an instance offering, note that:

- Make sure that the memory specified for the instance offering is greater than 16 MB. VM instances might fail to be started if the instance offering is excessively small.
- Both the disk bandwidth and network bandwidth are optional. Excessively low bandwidth might cause VM instances to work abnormally.
- If you are creating an instance offering for the first time, you can use the default configurations: 1 CPU and 1 GB memory.

- To modify an instance offering online, turn on NUMA in the global settings. Note that instance offerings of Windows VM instances cannot be modified online.
- Make sure that you fully understand the meaning of disk bandwidth and network bandwidth configurations before you can make corresponding settings. Otherwise, you might fail to download files from the VM instances.
- When you create a VM instance, if you specify both an affinity group policy and a host allocation policy, the priorities are as follows:
  - If the affinity group policy is anti-affinity group (soft), the host allocation policy takes precedence.
  - If the affinity group policy is anti-affinity group (hard), the affinity group policy takes precedence.

7.6 Disk Offering

A disk offering is a specification of a volume, which defines the size of a volume and how the volume will be created.

Disk offerings can be used to create both root volumes and data volumes.

Disk offerings can be enabled, disabled, shared globally, or recalled globally. When you install VM instances by using ISO, you need to specify a disk offering so as to determine the size of the root disk.

Disk Offering Operations

You can perform the following operations on a disk offering:

- Create disk offering: Create a new disk offering.
- Enable: Enable a disk offering that is in the disabled state. **Batch operations are supported.**
- Disable: Disable a disk offering. After a disk offering is disabled, you cannot use it to create a volume. However, existing volumes are not affected. **Batch operations are supported.**
- Share to all: After a disk offering is shared globally, it can be used by all accounts. **Batch operations are supported.**
- Recall from all: After a disk offering is recalled globally, it becomes invisible to other accounts. **Batch operations are supported.**
- Delete: When you delete a disk offering, a dialog box will be displayed, prompting you to confirm the delete operation. **Batch operations are supported.**

- Search: You can search for a disk offering by its name, UUID, or by using the advanced search .

7.7 GPU Specifications

A GPU specification defines the specification of the frame count, video memory, resolution, and other parameters of a GPU. A GPU specification can be either a physical GPU (pGPU) specificat ion or a virtual GPU (vGPU) specification.

- pGPU specification: The pGPU specification page displays a list of pGPU specifications scanned on all hosts in the cloud and the basic information about these pGPU specifications.
- vGPU specification: The vGPU specification page displays a list of available vGPU specificat ions generated from virtual segmentation and the basic information about these vGPU specifications.

7.8 Auto Scaling Group

ZStack offers auto-scaling capabilities that let you automatically add or remove VM instances from an auto scaling group (ASG) in response to load balancing of VM instances, your business load changes, and predefined scaling policies. With the auto scaling service, you can better leverage the Cloud resources, reduce the O&M costs, and ensure smooth business operations. Currently, the auto scaling service is applicable to KVM VM instances.

Scaling Mode

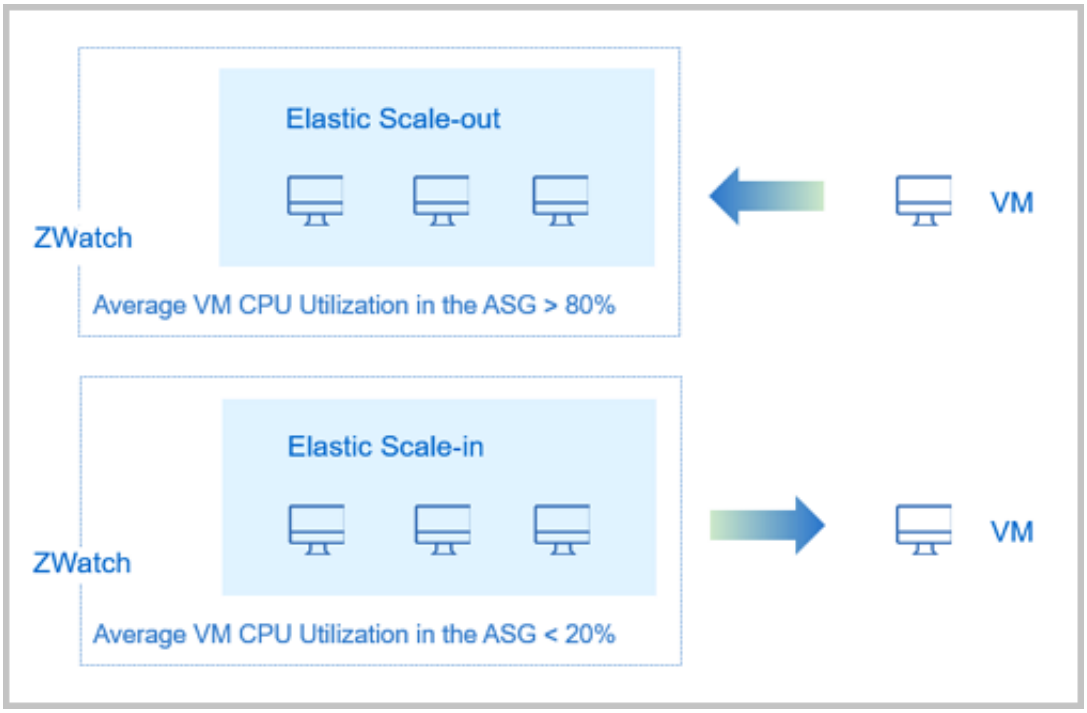
Currently, the Cloud supports the following two types of scaling mode:

1. **Auto Scaling**

   - Auto scaling includes elastic scale-out and elastic scale-in. For the elastic scale-out, when your businesses are growing, VM instances will be automatically added to ensure your business continuity. For the elastic scale-in, if your businesses decrease, VM instances will be automatically reduced.
   - With the ZWatch monitoring alarm, the auto scaling mode can be triggered. You can select an endpoint type as needed, including email, DingTalk, HTTP application, short message service (SMS), Microsoft Teams, and system endpoint.

   The auto scaling mode is shown in *Auto Scaling*.

Figure 7-3: Auto Scaling

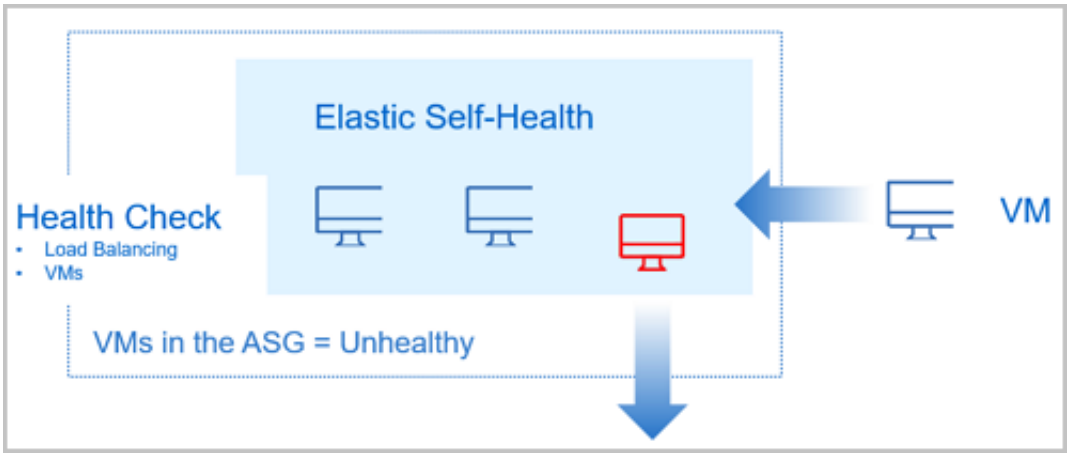


2. **Elastic Self-Health**

- In the elastic self-health mode, an auto scaling group monitors the health status of the VM instances within the group, automatically removes the unhealthy VM instances, and automatically adds additional VM instances. In this regard, healthy VM instances within the group will be ensured to be automatically adjusted not lower than the minimum specified number of VM instances.
- Two types of health check are provided to trigger the elastic self-health, including load balancer health check and VM health check. If an auto scaling group configures the load balancing service, we recommend that you select the health check mechanism native to a load balancer.

The elastic self-health is shown in *Elastic Self-Health*.

Figure 7-4: Elastic Self-Health



Scaling Policy

Scale-out Policy

- When your businesses are growing, an auto scaling group automatically adds additional VM instances to avoid access latency and resource overloading.
- An elastic scale-out activity can be triggered by setting the ZWatch monitoring alarm mechanism. For example, when the average memory usage of all VM instances in an auto scaling group is detected to exceed 80% continuously within a period of time, the cloud will automatically create an appropriate number of VM instances. Then, the auto scaling group will regain reasonable load balancing.
- You need to set a cooldown time, which is a period of time after an auto scaling group completes one scaling activity. During the cooldown time, the auto scaling group is locked and no other scaling activities are performed in this group.
- A minimum number of 1 VM instance can be added to an auto scaling group during each scale-out. If the value is too large, the scale-out activity might fail.

Scale-in Policy

- If your businesses decrease, an auto scaling group automatically reduces the number of VM instances to avoid a waste of resources.
- When you set a scale-in policy, the trigger metric is unselected in which this trigger metric must be consistent with that of the scale-out policy.
- An elastic scale-in activity can be triggered by setting the ZWatch monitoring alarm mechanism . For example, when the average memory usage of all VM instances in an auto scaling group is detected to be lower than 20% continuously within a period of time, the cloud will automatica

lly remove an appropriate number of VM instances. Then, the auto scaling group will regain reasonable load balancing.

- Currently, the following four removal policies are supported:
  - Earliest created VM instance: When an auto scaling group starts performing scale-in activities, the earliest created VM instances will be removed successively at first.
  - Most recent created VM instance: When an auto scaling group starts performing scale-in activities, the latest created VM instances will be removed successively at first.
  - VM instance with the minimum CPU utilization: When an auto scaling group starts performing scale-in activities, the VM instances with the minimum CPU utilization will be removed successively at first.
  - VM instance with the minimum memory utilization: When an auto scaling group starts performing scale-in activities, the VM instance with the minimum memory utilization will be removed successively at first.
- A minimum number of 1 VM instance can be removed from an auto scaling group during each scale-in. If the value is too large, the scale-in activity might fail.

Notice

- In terms of elastic scale-out, the number of VM instances in the auto scaling group must not be greater than that of the specified minimum number of the VM instances. In terms of elastic scale-in, the number of VM instances in the auto scaling group must not be smaller than that of the specified minimum number of the VM instances. If you create an auto scaling group for the first time, the number of VM instances in the auto scaling group is equal to the desired capacity of VM instances.
- A minimum number of 1 VM instance can be added to an auto scaling group during each scale-out. If the value is too large, the scale-out activity might fail. A minimum number of 1 VM instance can be removed from an auto scaling group during each scale-in. If the value is too large, the scale-in activity might fail.
- You can configure load balancing for an scaling group to realize the auto scaling of VM instances based on load balancing. At this time, we recommend that you choose the health check mechanism that comes with the load balancer.
- After you select a load balancer, you must select a listener. If multiple listeners are selected, they will monitor VM instances of the same group through different ports or port groups.
- Currently, auto scaling of VM instances in vRouter network and VPC network scenarios is supported.

- Auto scaling within an auto scaling group can be triggered by configuring ZWatch monitoring alarm mechanism. You can select an endpoint type as needed, including system, email, DingTalk, HTTP application, short message service (SMS), and Microsoft Teams.
- Currently, two types of VM image can be added: qcow2 and raw.
- If you delete resources (such as instance offerings, images, and networks) in the template configurations, you might fail to create an auto scaling group. Please exercise caution.
- Assume that the scaling activity of an auto scaling group is triggered. If you disable the auto scaling group, the ongoing scaling activity will not be affected. After the scaling activity is completed, a new scaling activity will be rejected.
- Assume that the auto scaling group is being inspected. If you disable the auto scaling group, ZWatch or the health check mechanism will stop inspecting the auto scaling group immediately , and will reject a new scaling activity.

More Information

- Business applications running on the VM instances of an auto scaling group must be stateless and can be extensible horizontally.
- The auto scaling service will automatically release VM instances. We recommend that you do not manually attach volumes, NICs, or security groups to the VM instances in the auto scaling group. If the VM instances in the auto scaling group contain stateful information, associated data will be lost.
- The auto scaling group cannot be extended vertically. That is, instance offerings, network bandwidth, and other resources cannot be automatically scaled in or out.
- If you want to change an external monitoring metric to an internal monitoring metric, delete the corresponding auto scaling group and create a new one.
- The auto scaling service can be set in the global settings as follows:
  - When the auto scaling group uses the health check mechanism of a load balancer, you can configure the health check interval of the VM instances in the load balancer.

    Method: Go to **Settings** > **Global Settings** > **Advanced**, locate **Health checking interval of loadBalancing VM instance**, and set a value as needed. Default value: 10. Unit: Second. Minimum value: 10 seconds. Maximum value: 1000 seconds.
  - When the auto scaling group uses the health check mechanism of a load balancer, you can configure the thread count of the VM health check in the load balancer.

Method: Go to **Settings** > **Global Settings** > **Advanced**, locate **Health checking threads of loadBalancing VM instance**, and set a value as needed. Default value: 10. Minimum thread count: 10. Maximum thread count: 1000.

- When the auto scaling group uses the health check mechanism of a VM instance, you can make configurations to delete the health check interval of unhealthy VM instances in the auto scaling group.

  Method: Go to **Settings** > **Global Settings** > **Advanced**, locate **Interval for remove unhealthy instance in group**, and set a value as needed. Default value: 30. Unit: Second. Minimum value: 10 seconds. Maximum value: 1000 seconds.

- When the auto scaling group uses the health check mechanism of a VM instance, you can make configurations to delete the thread count of unhealthy VM instances in the auto scaling group.

  Method: Go to **Settings** > **Global Settings** > **Advanced**, locate **Threads limitation for Unhealthy thread instance**, and set a value as needed. Default value: 10. Minimum thread count: 10. Maximum thread count: 1000.

- The health check interval of the VM count in the auto scaling group can be set.

  Method: Go to **Settings** > **Global Settings** > **Advanced**, locate **Checking interval for instance count in group**, and set a value as needed. Default value: 20. Unit: Second. Minimum value: 10 seconds. Maximum value: 1000 seconds.

7.9 Snapshot

A snapshot is a point-in-time capture of data status in a disk. Before you perform mission-critical operations, you can take snapshots for the data volume or root volume of a VM instance so that you can immediately roll back on failure. For long-term backup, we recommend that you use disaster recovery related services.

Notice

- You can create snapshots for running or stopped VM instances.
- You cannot create batch snapshot for VM instances that have a shared volume attached.
- In a production environment, we recommended that you limit the number of snapshots per disk within 5. Excessive snapshots might affect the I/O performance, data security, and primary storage capacity of the corresponding VM instances and volumes. For long-term backup, we recommend that you use disaster recovery related services.

- To ensure data integrity in a production environment, we recommend that you do not take snapshots for VM instances with high I/O. When a high I/O operation is performed in a VM instance, some data in the VM memory might fail to be saved to the disk. In this case, these data will not be saved to the snapshot you created for the VM instance.
- The snapshot of the VM instance on the Ceph primary storage does not occupy capacity. Therefore, the displayed snapshot capacity is the actual capacity of the VM root volume when the snapshot was created.
- For Ceph primary storages, the VM snapshot capacity might fail to be obtained. Here are some statements:
  - Open source Ceph (version H) and enterprise-level Ceph (earlier than 3.2.0) cannot obtain VM snapshot capacity.
  - Due to the RBD format, enterprise-level Ceph (3.2.0 and later versions) may fail to obtain VM snapshot capacity.
- By restoring a VM snapshot, you will restore the VM data to the time of point when the snapshot was taken. Before you restore a VM snapshot, stop the VM instance.
- By restoring a volume snapshot, you will restore the volume data to the time of point when the snapshot was taken. Before you restore a volume snapshot, stop the VM instance that has the volume attached or detach the volume from the associated VM instance.

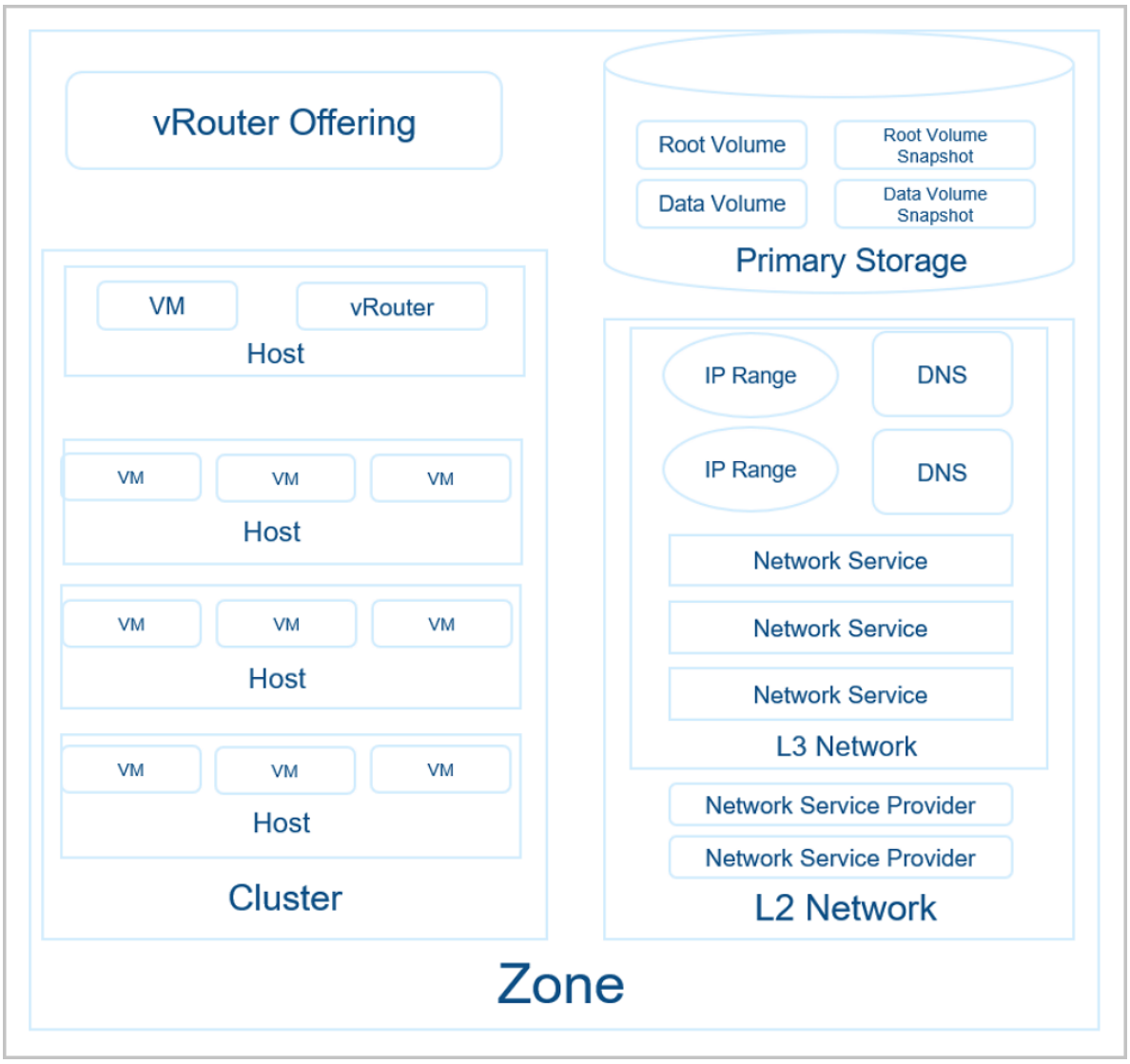
8 Hardware

8.1 Zone

Zone is the largest resource definition in ZStack, including cluster, L2 network, primary storage, and other resources.

- In a data center, a zone corresponds to an equipment room.
- A zone defines a visible boundary. Subresources within the same zone can be visible mutually and can form a certain relationship. However, subresources within different zones are invisible mutually and cannot form mutual relationships.
- Resources in a zone is organized as follows, as shown in *Zone Resource Structure*.

Figure 8-1: Zone Resource Structure



When you organize 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 should be mapped as the 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 storage that is attached to the zone.
   - A backup storage can be detached from a zone. After the backup storage is detached, 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.

Notice

When you use a zone, note that:

- After you disable a zone, all clusters in the zone and hosts in these clusters will also be disabled. At this time, new resources in all clusters in this zone can no longer be applied for. To apply for new resources, you need to enable the zone again.
- After you enable a zone, all clusters in the zone and hosts in these clusters will also be enabled .
- After you delete a zone, all resources and subresources in this zone will also be deleted. Resources include clusters, L2 networks, and primary storages. Subresources include hosts, VM instances, volumes, snapshots, L3 networks, and various network services. Please

exercise caution. Note that this delete operation only removes information about these resources recorded in ZStack. The actual data will not be deleted.

- To help you better manage the relationship between backup storages and zones, the UI specifies that one backup storage corresponds to only one zone. When you delete a zone, you will also delete the backup storage attached to this zone.

8.2 Cluster

A cluster is a logical group of hosts (compute nodes). In a real data center, a cluster usually maps to a rack.

A cluster can be used to achieve the following goals:

- Improve the computing and I/O capabilities of the overall system.
- Improve the service reliability.
- Improve the scale expansion capability of the system and reduce the system O&M costs.

When you organize a cluster, note that:

1. All hosts in the same cluster must be installed with the same operating system.
2. All hosts in the same cluster must have the same network configuration.
3. All hosts in the same cluster must be able to access the same primary storage.
4. To provide VM services, a cluster must have a primary storage and an L2 network attached.
5. The size of a cluster, which is the maximum number of hosts that each cluster can contain, is not enforced.

Relationship Between Cluster and Associated Resources

1. Cluster | Zone

   Operations on **multiple clusters** are supported. That is, you can create more than one cluster in a zone, and allocate newly created hosts to different clusters as needed.

2. 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 Shared Block primary storages attached.

- A cluster can have one Shared Mount Point primary storages attached.
- A cluster can have only one Ceph 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 a Shared Mount Point primary storage attached.
- A cluster can have both a LocalStorage and a Shared Block primary storage attached.
- A cluster can have both a Ceph and a Shared Block primary storage attached.
- A cluster can have both a Ceph and more than one Shared Block primary storage attached.

The following table lists the relationship between primary storages and a cluster, as shown in *Table 8-1: Relationship Between Primary Storage and Cluster*.

Table 8-1: Relationship Between Primary Storage and Cluster

Primary Storage	Cluster
LocalStorage	A cluster can have one or more LocalStorage attached.
NFS	A cluster can have one or more NFS primary storages attached.
Shared Block	A cluster can have one or more Shared Block primary storages attached.
Share Mount Point	A cluster can have one Share Mount Point primary storage attached.
Ceph	A cluster can have only one Ceph primary storage attached.
LocalStorage + NFS	A cluster can have one LocalStorage + one NFS attached.
LocalStorage + SMP	A cluster can have one LocalStorage + one Shared Mount Point attached.
LocalStorage + Shared Block	A cluster can have one LocalStorage + one Shared Block attached.
Ceph + Shared Block	• A cluster can have one Ceph + one Shared Block attached.

Primary Storage	Cluster
	• A cluster can have one Ceph + multiple Shared Block 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.
- After you delete a cluster that uses LocalStorage, all hosts and VM instances in the cluster will be deleted. However, volumes and actual snapshot data of these hosts will not be deleted.
- After you delete a cluster that uses a shared storage, the corresponding VM instances will be stopped. If you add high availability tags to these stopped VM instances, you can restart these VM instances on the hosts in other available clusters.
- If different clusters have the same network and primary storage attached, you can migrate VM instances across these clusters.
- After you detach a primary storage from a cluster, ZStack will stop all VM instances in the cluster. You can start these VM instances only when you attach this primary storage to this cluster again.
- After you put the primary storage where the data disk of a VM instance is located into maintenance mode, the VM instance will be stopped and cannot be started.

3. Customizing the CPU mode of a cluster

- To make the setting take effect, go to **Settings** > **Global Settings** > **Advanced**, locate **Host CPU Model checking**, and set the value to **true**.
- After you specify the CPU mode of a cluster, you can add hosts of the specified CPU mode only to this cluster.
- For clusters created in the previous versions, after you upgrade the cloud to 2.3.2, the CPU mode of the cluster is None, which cannot be changed.

4. 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 VxlanNetworks.
- One NIC can have only one NoVlanNetwork created.
- For VlanNetwork, 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.
- In addition, when you detach a network from a cluster, ZStack will detach the NICs of all VM instances in the cluster. At this time, the VM instances do not have a NIC. Once a running VM instance is stopped, it cannot be started again. To start the VM instance again, you need to attach a network to the cluster again and attach a NIC to the VM instance.
- You can add a migration network to perform migration operations. If no migration network is set, the management network will be used for migration by default.

5. Cluster | Backup Storage

No direct dependency exists between a cluster and a backup storage. A backup storage can provide services for multiple clusters.

Note:

- The primary storage and backup storage attached to the same cluster are associated with each other.
- A Ceph primary storage can work with backup storages of the ImageStore type.
- The following table lists the relationship between primary storages (PS) and backup storages (BS), as shown in *Table 8-2: Relations Between Primary Storage and Backup Storage*.

Table 8-2: Relations Between Primary Storage and Backup Storage

PS/BS	ImageStore	SFTP	Ceph
LocalStorage	○	○	×
NFS	○	○	×
Shared Mount Point	○	○	×

Ceph	○	×	○
Shared Block	○	×	×

6. Cluster | Host

   - After you disable a cluster, you cannot use this cluster to apply for new resources. In addition, all hosts in the cluster will also be disabled. However, the running VM instances are not affected. Note that after these running VM instances are stopped, they will not be started in the cluster again.
   - After you enable a cluster, you will also enable all hosts in the cluster at the same time.

7. Cluster | Global Settings

   - On the **Advanced Settings** tab of the details page of a cluster, you can set the memory overcommitting rate, CPU overcommitting rate, and host reserved memory for the cluster. This setting only takes effect for the resources in the cluster. If not set, values set in the global settings will be used by default.

     Note:
     The values of the advanced setting must be configured according to the needs of different systems and applications. Excessive large values might seriously affect the performance. Please exercise caution.

8. Cluster | DRS

   Dynamic Resource Scheduling (DRS) monitors the load of hosts by cluster, and gives scheduling suggestions according to the configured scheduling strategy. You can migrate VM instances according to the scheduling suggestions to balance the cluster load while effectively improving the cloud stability.

   To make RDS work properly, make sure that:

   - The cluster has only Ceph or Shared Block primary storage.
   - The CPU modes of the hosts in the cluster are consistent.
   - The cluster does not have VM instances that are attached to affinity groups.

   If all the above requirements are met, you can turn on the **Switch for RDS** on the **Advanced Settings** tab of the cluster details page. After the switch is turned on, you can configure the scheduling policy on the **RDS** page. The RDS functionality takes effect after the configurations are completed.

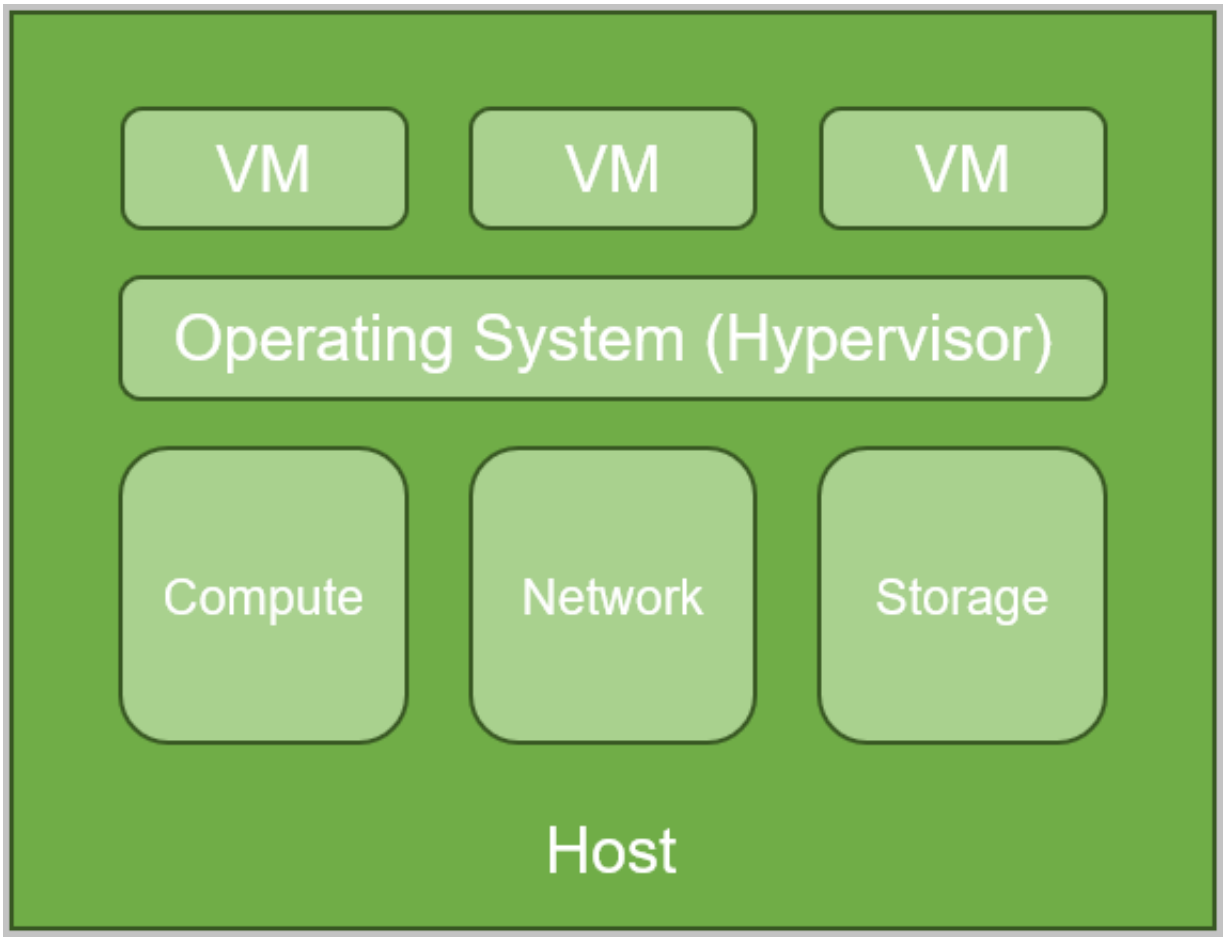
8.3 Host

A host, also known as a compute node, is a physical server that provides VM instances with compute, network, and storage resources.

- Hosts are core assets in ZStack. VM instances run on hosts.

As shown in *Figure 8-2: Host*.

Figure 8-2: Host



Notice on Adding Hosts

When you add hosts, note that:

- The management IP address of the management node must have access to the SSH port of the hosts to deploy agents.
- The user name of the hosts must have the sudo permission.
- The firewall must be enabled or iptables must be allowed for the SSH port.
- The hardware virtualization features of Intel VMX and AMD SVM must be supported.

- When you add or modify host information, make sure that the information matches the actual environment.
- Hosts have a `managementIp` field, which indicates that when a host has multiple IP addresses, the newly added IP addresses are used by the management node to connect and deploy agents.
- The management node periodically sends a **`ping`** command to hosts to check the health status of the channel. Once a host fails to respond, or once the **`ping`** command times out, the status of the host will become disconnected. After a host is disconnected, the status of VM instances running on the host will become unknown. After the host is reconnected, the status of VM instances on the host will be synchronized again.
- The management node will provide a NTP time server to synchronize the time of each host.

Host Operations

- Add host: Add a new host.
- Enable: Enable the host that you selected.
- Disable: Disable the host that you selected.

> **Note:**
> After you disabled a host successfully, the existing resources on the host will not be affected, but the host cannot serve as a candidate host to apply for new resources.

- Reconnect: Reconnect the host that you selected.

> **Note:**
> - Generally, the reconnect operation is performed after you update the configurations of the host.
> - For example, after you update the memory or hard disk of the host, you can reconnect the host to update your database.

- Bind tag: Bind a tag to the host.

> **Note:**
> - Hosts can only bind admin tags.
> - One resource can bind 50 tags at most, while a single tag can bind the unlimited number of resources.

- Many-to-many bindings between tags and resources are supported. That is, you can bind multiple tags to multiple resources.
- Tags that were created by a tenant can only be bound to resources owned by the tenant, while admin tags can be bound to all resources.
- An administrator can unbind or delete tenant tags.
- Resource tags can be sorted in order according to the creation time or tag names (priority: characters > numbers > Chinese characters > English characters). To change the sort order, choose **Settings** > **Global Settings** > **Advanced**, locate **Tag sorting field**, and click the Edit icon. By default, the tags are sorted in order by the tag name.

- Unbind tag: Unbind a tag from the host.

Note:

- Multiple tags on a single resource can be unbound simultaneously. In addition, multiple resources on a single tag can also be unbound simultaneously.
- A tenant can only unbind tags from the resources owned by the tenant itself, while an administrator can unbind tags from all resources.

- Enter maintenance mode: Place the host in maintenance mode. In this mode, you can stop and repair the host.
  - If a host is running on a local storage primary storage, VM instances that are running on the host will be stopped after the host enters maintenance mode.
  - If a host is running on a shared storage, VM instances that are running on the host will be migrated automatically after the host enters maintenance mode.

Note:

- Under the shared storage scenario, after the host enters maintenance mode, you can set the VM migration policy in case of migration failure.
- Method:

  Go to **Settings** > **Global Settings** > **Advanced**, locate **host.maintenance.policy**, and click the Edit icon.

  - If you select **Stop Vm On Migration Failure**, VM instances that are running on a shared storage will be automatically migrated to other hosts after the host where the

VM instances reside enters maintenance mode. In addition, VM instances that fail to be migrated will be forced to stop.

- If you select **Just Migrate**, VM instances that are running on a shared storage will be automatically migrated to other hosts after the host where the VM instances reside enters maintenance mode. If some VM instances are still running on the host, the host will fail to enter maintenance mode.

- Delete: Delete the host that you selected.

Note:

- If you delete a host, all VM instances that are running on the host will be stopped.
- Local storage primary storage scenario:
  - If the cluster where the host belongs is attached to a LocalStorage primary storage, all VM instances and volumes on this host will be deleted as well. Please exercise caution.
  - Even if you add a deleted host to the cloud again, the system will deploy this host again . If the previous database resource is not backed up, associated business data will not be recovered.
- Shared storage scenario:
  - Assume that the **HA Level** on VM instances is set to **None**.

    After you delete the host where the VM instances belong, the corresponding VM instances will be stopped.
  - Assume that the **HA Level** on VM instances is set to **NeverStop**.

    If resources of other hosts permit, the VM instances with the **NeverStop** HA level and running on this host will be stopped firstly after you delete the host. Next, these VM instances will be migrated to other hosts and then automatically start without affecting your data security. If resources on these hosts are insufficient, the corresponding VM instances will be stopped.

    Note:

    Under this circumstance, a portion of VM instances might be migrated to other hosts with sufficient resources, while another portion of VM instances might be stopped due to a shortage of host resources.
  - If you delete the host, data volumes on the shared storage will not be affected.

- Assume that you have installed the Migration Service module license. If the host is specified as a conversion host, the corresponding conversion host will be deleted as well after the host is deleted. In addition, an on-going V2V migration job on this conversion host will be automatically canceled. Please exercise caution.

Notice on Using Hosts

When you use hosts, note that:

- The host maintenance mode is mainly used by the administrator to perform planned shutdown for host maintenance, such as adding memory, adding hard disk, and replacing NICs.
- Assume that a host is in maintenance mode. If the primary storage is local storage, all VM instances on the host will be stopped. If the primary storage is shared storage, VM instances on the host will be automatically migrated to available hosts. If other hosts do not have sufficient resources, these VM instances will be stopped.
- The standard procedure to add memory to a host is as follows:
  1. Put the host into maintenance mode.
  2. Wait for the automatic migration of all VM instances on the host or stop the VM instances on the host, and then perform the **`shutdown`** operation on the host.
  3. Power off the host and add memory to the host.
  4. After the host is powered on, start the host manually or through IPMI to boot the operating system.
  5. Set the status of the host to enabled.
- After a host is disabled, the existing running VM instances will remain running. If these VM instances are stopped, they cannot be started by using the host.
- After a host is disabled or enters maintenance mode, this host can no longer be used as a candidate to apply for new resources. It can be used only after it is enabled again.
- A host can be deleted only after it is disconnected or enters maintenance mode.
- After you delete a host on a local storage, all VM instances or volumes on this host will also be deleted. Note that this delete operation only removes the information about the host, VM instances, and volumes recorded in ZStack. The actual data will not be deleted.
- When you delete a host on a shared storage, the VM instances or volumes on the host will not be directly deleted. Note that these resources can be enabled or used on other hosts.
- After you delete a host, even if you add it back again, the system will not recognize the deleted VM instances. Please exercise caution.

- If you want to use the GPU passthrough functionality, make sure that VT-d is enabled for the host BIOS. When you add a host, check the IOMMU option to scan IOMMU devices. The GPU passthrough functionality can be used only when IOMMU is enabled and ready.

Host Maintenance Troubleshooting Items

If an exception occurs during the host maintenance, troubleshot the following items:

- **Management node logs:**

  In the management node, check whether *`/usr/local/zstack/apache-tomcat/logs/management-server.log`* is abnormal.

- **Host agent process:**

  On a host, check `ps -ef|grep kvmagent` to determine whether the KVM agent is working properly.

- **Host logs:**

  On a host, check whether *`/var/log/zstack/zstack-kvmagent.log`* is abnormal.

- **Host libvirt status:**

  On a host, check whether `service libvirtd status` is abnormal.

- **Host system logs:**

  On a host, check whether *`/var/log/messages`* is abnormal.

- **Connection between hosts and primary storages:**

  Check whether the connection between hosts and primary storages is abnormal.

8.3.1 Host Maintenance (Advanced)

8.3.1.1 Single Host Maintenance

Change Host Password

- Via UI:

  1. Log in to the Cloud, go to the details page of a host, and click the edit icon next to the **Password** field to change the host password.
  2. Reconnect the host manually for the new password to take effect.

- Via CLI:

  1. Run the following command to log in to the Cloud as an administrator:

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

```
admin>> LogInByAccount accountName=admin password=PASSWORD   #
Here, PASSWORD is the login password.
```

2. Run the following command to change the host password:

```
admin>> UpdateKVMHost uuid=HOST_UUID password=NEW_PASSWORD   #
Here, HOST_UUID is the host UUID, and NEW_PASSWORD is the new
password.
```

Enable Host IOMMU

To make the IOMMU take effect, you need to enable Intel VT-d or AMD IOMMU for a host. The method is as follows:

- Log in to the Cloud via the UI. On the **Basic Attributes** tab of the host details page, set **IOMMU State** to **Enable**. Then, restart the system and specify a host to enable IOMMU.

8.3.1.2 Bulk Host Maintenance

Add Hosts in Bulk

ZStack Enterprise allows you to add hosts in bulk via UI or CLI. The methods are as follows:

- Via UI

  1. Log in to ZStack via the UI. On the **Add Host** page, select **Use Import** to add hosts.
  2. Click **Download Template** to download the template and fill in the template according to your needs.
  3. After you fill in the template, add it to ZStack and click **OK**.

  For more information, see *Add Host* in the User Guide.

Configure Password-Free Access on Hosts in Bulk

To configure password-free access, time synchronization, and hostname, follow these steps:

1. Run the following commands to prepare a password-free package:

```
[root@localhost ~]# wget http://cdn.zstack.io/tools/zstack_tools.tar
.gz  #Download the tool package.
[root@localhost ~]# tar zxvf zstack_tools.tar.gz   #Decompress the
tool package.
[root@localhost ~]# cd zstack_tools/   #Go to the directory where
the tool package is stored.
```

2. Modify the configurations in `ansible/hosts.example`.

Note:

- The management IP addresses of all nodes are listed under *[nodes]*.

- **ansible_user** indicates the SSH user name.
- **ansible_pass** indicates the SSH password.
- The initial password of each host must be the same. After you list the time synchronization servers to be configured under *[chrony]*, the script will automatically configure this node as a time synchronization server.

```
[root@localhost zstack_tools]# vim ansible/hosts.example
#Make the modifications as follows:
#Node IP
[nodes]
10.10.0.11
10.10.0.12
10.10.0.13
#Node user/password
[nodes:vars]
ansible_user=root
ansible_ssh_pass=password
#Time synchronization server
[chrony]
10.10.0.13
#Save and exit.
Edit the hostname prefix.
Modify the hostname prefix under ansible/group_vars/nodes.
vim ansible/group_vars/nodes
#Make the modifications as follows:
hostname_prefix: ceph-
#Save and exit. Then, the prefix of each hostname will be configured
 in a specified format, such as ceph-1 and ceph-2.
```

3. Run the following command to prepare the environment in one click. The following script will configure password-free SSH access between different nodes, time synchronization, and `/etc/hosts`. This script will also disable the firewall.

```
[root@localhost ~]# ./prepare.sh -i ./ansible/hosts.example
```

Change System Password and Platform Password in Bulk

This section describes how to change the system password and platform password of hosts in bulk. Note that this operation applies to KVM hosts only. To perform this operation, make sure that hosts added to the Cloud use the root user.

- **Method 1:**

1. Run the following command to log in to the Cloud as an administrator:

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

```
admin>> LogInByAccount accountName=admin password=PASSWORD   #
Here, PASSWORD is the login password.
```

2. In the management node, run the following commands to change the root password of hosts in bulk:

```
admin>> QueryHost fields=managementIp, "hypervisorType"=KVM
admin>>  for i in $(zstack-cli QueryHost fields=managementIp,
hypervisorType=KVM|awk -F "\"" '/managementIp/ {print $4}');
do \
ssh $i -i \
/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/
ansible/rsaKeys/id_rsa 'echo "NEW_PSAAWORD" | passwd --stdin root
';
done    #Here, NEW_PSAAWORD is the new password.
```

- **Method 2:**

1. In the management node, run the following commands to change the platform password of hosts in bulk:

```
[root@localhost ~]# for i in $(zstack-cli QueryHost fields=uuid,
hypervisorType=KVM|awk -F "\"" '/uuid/ {print $4}')
[root@localhost ~]# do zstack-cli UpdateKVMHost uuid=$i password=
NEW_PSAAWORD   #Here, NEW_PSAAWORD is the new password.
[root@localhost ~]# done
```

Create Sudo Users for Hosts and Change User Names and Passwords in Bulk

This section describes how to create sudo users for hosts and change user names and passwords in bulk. Note that this operation applies to KVM hosts only. To perform this operation, make sure that hosts added to the Cloud use the root user.

- **Method 1:** In the management node, run the following command to create test users in bulk, and change the password of the test users with the sudo permission to NEW_PSAAWORD.

```
[root@localhost ~]# zstack-cli LogInByAccount accountName=admin
password=password
admin>>  for i in $(zstack-cli QueryHost fields=managementIp,
hypervisorType=KVM|awk -F "\"" '/managementIp/ {print $4}');
do \
ssh $i -i \
/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/
ansible/rsaKeys/id_rsa \
'adduser test;echo "NEW_PSAAWORD" | passwd --stdin test;echo "
test   ALL=(ALL)       NOPASSWD: ALL" >>/etc/sudoers;'   #Here,
NEW_PSAAWORD is the new password.
admin>>  done
```

- **Method 2:** In the management node, run the `zstack-cli` commands to change the user name and password of hosts in bulk to NEW_NAME and NEW_PSAAWORD, respectively.

```
[root@localhost ~]# for i in $(zstack-cli QueryHost fields=uuid,
hypervisorType=KVM|awk -F "\"" '/uuid/ {print $4}')
```

```
[root@localhost ~]# do
[root@localhost ~]# zstack-cli UpdateKVMHost uuid=$i password=
password123 username=test
[root@localhost ~]# done
```

8.3.1.3 Planned Shutdown of Hosts

Shut Down Hosts for Maintenance

Before you shut down hosts for maintenance, make sure that the Cloud is working properly, and both the hosts and primary storages are in the connected status. To perform planned shutdown of hosts for maintenance, follows these steps:

- **Normal Scenario**
  1. Place all primary storages into maintenance mode. After all primary storages enter maintenance mode, make sure that all VM instances are shut down.
  2. Place all hosts into maintenance mode.
  3. In the management node, run the `zstack-ctl stop` command to stop the management node service.
  4. Power off all servers.
- **MN (Host) HA Scenario**
  1. Place all primary storages into maintenance mode. After all primary storages enter maintenance mode, make sure that all VM instances are shut down.
  2. Place all hosts into maintenance mode.
  3. Run the `zsha2 stop-node` command in each management node to stop the management node service.
  4. Power off all servers.

Power on Hosts After Maintenance

- **Normal Scenario**
  1. Power on all servers.
  2. Log in to the management node, run the `zstack-ctl status` command to view the management node status, and wait for the ZStack service to start successfully.
  3. Log in to ZStack, enable all primary storages and hosts, and make sure that all hosts and primary storages are in the connected status.
- **MN HA Scenario**
  1. Power on all servers.

2. In the HA scenario where VM instances act as management nodes, run the **`zsha status`** command in any host to check the HA service status, and wait for the service to start successfully.
3. In the HA scenario where hosts act as management nodes, run the **`zsha2 status`** command in each management node to check the HA service status, and wait for the service to start successfully.
4. Log in to ZStack, enable all primary storages and hosts, and make sure that all hosts and primary storages are in the connected status.

8.3.1.4 Host Capacity Expansion

Add Hosts to Expand Compute Resources

To expand compute resources by adding hosts, follow these steps:

1. Add new hosts.
2. Install and deploy the server and configure the network according to the User Guide.
3. Log in to the UI. On the **Add Host** page, add hosts to expand the compute servers. For more information, see the *Add Host* topic in the User Guide.

Note:

- In the scenario of separated or converged deployment of Ceph Enterprise, you need to add the compute nodes to storages as a gateway. Note that you need to configure the hostname, hosts files, password free, firewall, SELinux, and time synchronization in advance.
- In the scenario where the Cloud connects to SAN storage, you need to configure LUN of the SAN device in advance and then map the LUN to the host.

Add Hosts to Expand Storage Resources

- **Expand Storage of Ceph Enterprise**

  1. Separated or converged deployment scenario.
  2. Prepare the ISO published on the official website to install the server, and set the hard disk to passthrough mode.
  3. Install and deploy the server and configure the network according to the User Guide. Configure password free, time synchronization, and hostname.
  4. On the storage management page of Ceph Enterprise, add your server as a storage server, add a cache disk (optional), add hard disks in server, add a topology, and add the hard

disks to the storage pool. Then, wait for the server to balance the data automatically, and reconnect ZStack primary storage to complete storage expansion.

- **Expand Storage of SAN Device**

  1. Contact SAN vendors to expand LUN.
  2. In ZStack, reconnect the SAN primary storage that works with Shared Block to complete the storage expansion.

8.3.1.5 Host Replacement

To replace a host, follow these steps:

1. Log in to the UI, and place the target host into maintenance mode.

   Note:
   Before you place a host into maintenance mode, you need to migrate the appliance VM instances on the host.

2. Make sure that no appliance VM instances exist on the host, and then delete the host.
3. Install the custom ZStack operating system for the new host and configure the basic networks. Note that the host is installed as a compute node.
4. On the **Add Host** page, add new hosts. For more information, see the *Add Host* topic in the User Guide.

8.3.1.6 Host Reconnection

Reconnecting a host will redeploy the agent to perform related checks.

Factors to be checked if a host fails to be reconnected:

1. As shown in the following example, if the management node could not access port 22 of the host, troubleshoot the management node to ensure that the management node can SSH to the host.

   ```
   ssh: connect to host 192.168.0.65 port 22: Network is unreachable
   ```

2. The host must have access to the management node to return the result of the agent to the management node.

3. As shown in the following example, if the upgrade fails because you did not use the custom ZStack ISO to install the compute node, you need to solve this issue by using the custom ZStack ISO to install the system again.

```
ERROR: command pkg_list=`rpm -q openssh-clients qemu-kvm bridge-
utils wget qemu-img libvirt-python libvirt nfs-utils vconfig libvirt
-client net-tools iscsi-initiator-utils lighttpd dnsmasq iproute
sshpass rsync nmap | grep \"not installed\" | awk '{ print $2 }'`
 && for pkg in $pkg_list; do yum --disablerepo=* --enablerepo=zstack
-local install -y $pkg; done;failed!
```

4. The libvirt service status of the host must be normal.

   You can use `systemctl status/start/stop/restart libvirtd` to check the service status, or enable, disable, or restart the service.

5. Reconnecting the host will check the networks attached to the cluster to which the host belongs . If the specified device of the L2 network attached to the cluster is eth1, but no eth1 exists after the NIC No. of the host changes, this host will fail to be reconnected.

6. If the storage capacity of the system disk of the host runs out, the host will fail to be reconnecte d.

7. For the host that must have an NFS primary storage attached, if the attach fails, the host will fail to be reconnected. At this time, you need to check the link between the host and the NFS primary storage. For example, if the following error occurs, you need to check the connection from the host to the NFS primary storage.

```
failed to execute shell command: mount 192.168.18.242:/home/Storage
/zhu /opt/zstack/nfsprimarystorage/prim-751565713a6340da884c
33a8668a8916
```

8. For hosts that use distributed block storage, if a storage network exists, the host must have direct access to the storage network.

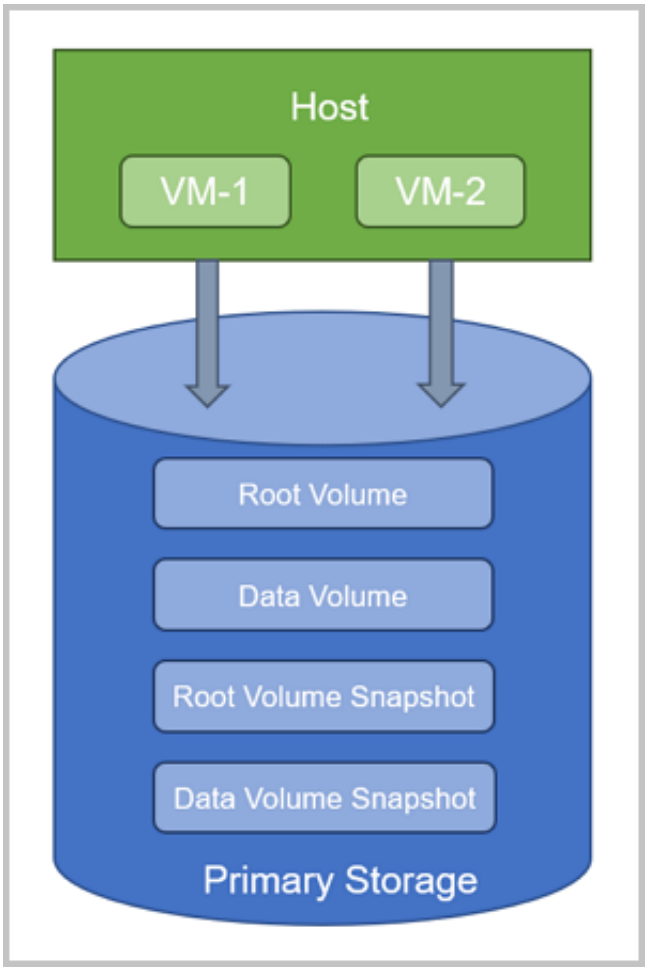
9. If a VXLAN network is used, the VTEP IP specified when you attach the network to the cluster must exist. If the IP does not exist, the host will fail to be reconnected.

8.4 Primary Storage

A primary storage is a storage server used to store disk files, such as root volumes, data volumes , root volume snapshots, data volume snapshots, and image caches, for VM instances.

As shown in *Primary Storage*.

Figure 8-3: Primary Storage



A primary storage can either be a local storage or a shared storage.

- **Local Storage:** Use the hard disks of a host to store disk files.
- **Network Shared Storage:** Support NFS, Shared Mount Point, Ceph, and Shared Block.
  - NFS is a network file system storage.
  - Shared Mount Point supports network shared storages provided by commonly used distributed file systems such as MooseFS, GlusterFS, OCFS2, and GFS2.
  - Ceph uses distributed block storages.
  - Shared Block uses shared block storages.

Scenario: Attaching Primary Storages to Clusters

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 Shared Block primary storages attached.
- A cluster can have one Shared Mount Point primary storages attached.
- A cluster can have only one Ceph 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 a Shared Mount Point primary storage attached.
- A cluster can have both a LocalStorage and a Shared Block primary storage attached.
- A cluster can have both a Ceph and a Shared Block primary storage attached.
- A cluster can have both a Ceph and more than one Shared Block primary storage attached.

Notice

When you use primary storages, note that:

- LocalStorage, NFS, and Shared Mount Point primary storages are based on qcow2.
- The consumption of the root volume and data volume of a VM instance is calculated by virtual capacity.
- After a primary storage is disabled, the primary storage cannot be used to apply for new resources or create VM instances and data volumes. However, running VM instances will not be affected.
- After a primary storage is maintained, the primary storage cannot be used to apply for new resources. In addition, existing running VM instances will also be stopped.
- Relationship between primary storage and backup storage:
  - LocalStorage, NFS, Shared Mount Point, Ceph, and Shared Block primary storages can work with ImageStore backup storages.
  - LocalStorage, NFS, and Shared Mount Point primary storages can work with SFTP backup storages.
  - Ceph primary storages can work with either ImageStore or Ceph backup storages.
- Primary storages are used based on the thin provisioning mode. In addition, primary storages support overcommitting. When the overcommitment ratio is excessive large, pay attention to the usage of the actual physical capacity.
- ZStack uses the virtual size to create volumes. If the virtual size is not enough to provide the required capacity, the volume will fail to be created.

- Deleting a primary storage will also delete all the VM instances, volumes, and snapshots in the primary storage. Please exercise caution. The delete operation only removes the information about the primary storage, VM instances, volumes, and snapshots recorded in ZStack. Actual data will not be deleted.
- You can set independent storage network and management network for shared storages. The management node judges the health status of VM instances based on the storage network. If no independent storage network exists, you can leave it unspecified, which means that the management network is used to judge the health status of VM instances.

8.4.1 Shared Block

Shared Block is a block-level data storage service that features simple deployment, flexible expansion, and high performance in comparison with SMP primary storage. Shared Block allows you to use a LUN device that you segmented on a SAN storage as a storage pool. This storage pool can be used by your appliance VM instances.

- Shared Block adopts the shared block storage method to match ImageStore.
- Shared Block allows you to add LUN devices online.
- A cluster can have multiple Shared Block primary storages attached.
- A cluster can have both one LocalStorage and one Shared Block primary storage attached.
- Stopped VM instances can be migrated with volumes, except for shared volumes, across storages.
- Primary storages support thin provision and thick provision modes.
  - Thick provision: Allocate the required storage space in advance to provide sufficient storage capacities and to ensure storage performances.
  - Thin provision: Allocate storage spaces as needed to achieve a higher storage utilization.
- Live migrations can be performed on VM instances in Windows failover clusters.

> **Note:**
> ZStack 3.9.0 and later versions provide specific support for Windows failover clusters. Due to this support, the live migration of VM instances will not have any adverse effects.

Notice

- When you add a Shared Block primary storage, the **Clear SharedBlock** checkbox is not selected by default.

- If selected, the residual data in LUN devices will be forced to clean, including file systems, RAID, or signatures of partition tables.
- If your LUN devices store data, and you do not clean the devices, you will fail to add LUN devices or attach primary storages.
- When you add LUN devices, the devices must not include partitions. Or otherwise, you will fail to add the devices.

8.4.2 Primary Storage Maintenance (Advanced)

8.4.2.1 Shared Block Maintenance

Shared Block Capacity Expansion

To expand the capacity of the underlay FC SAN, follow these steps:

1. Before capacity expansion, confirm the best expansion plan with the storage vendor.
2. Make sure that the storage expansion does not affect the business, and then perform storage expansion.
3. After the storage expansion is finished, log in to the Cloud via the UI and refresh the capacity on the primary storage details page. The proper display of the capacity indicates that the storage expansion is completed.

Shared Block Maintenance

The planned maintenance of a primary storage will stop all VM instances on the primary storage. The administrator needs to migrate important VM instances in advance. The steps for planned maintenance of a primary storage are as follows:

1. Log in to ZStack via the UI. On the **Primary Storage** page, click **Enter Maintenance** to place the primary storage into maintenance mode.
2. Go to the backend of the primary storage to perform maintenance operations.
3. After the maintenance is completed, go to the **Primary Storage** page via the UI and click **Start** to start the maintenance of the primary storage.

8.4.2.2 Primary Storage Reconnection

Reconnecting a primary storage will redeploy the agent to perform related checks.

Factors to be checked if a primary storage fails to be reconnected:

1. Generally, the state of a local storage is connectable.

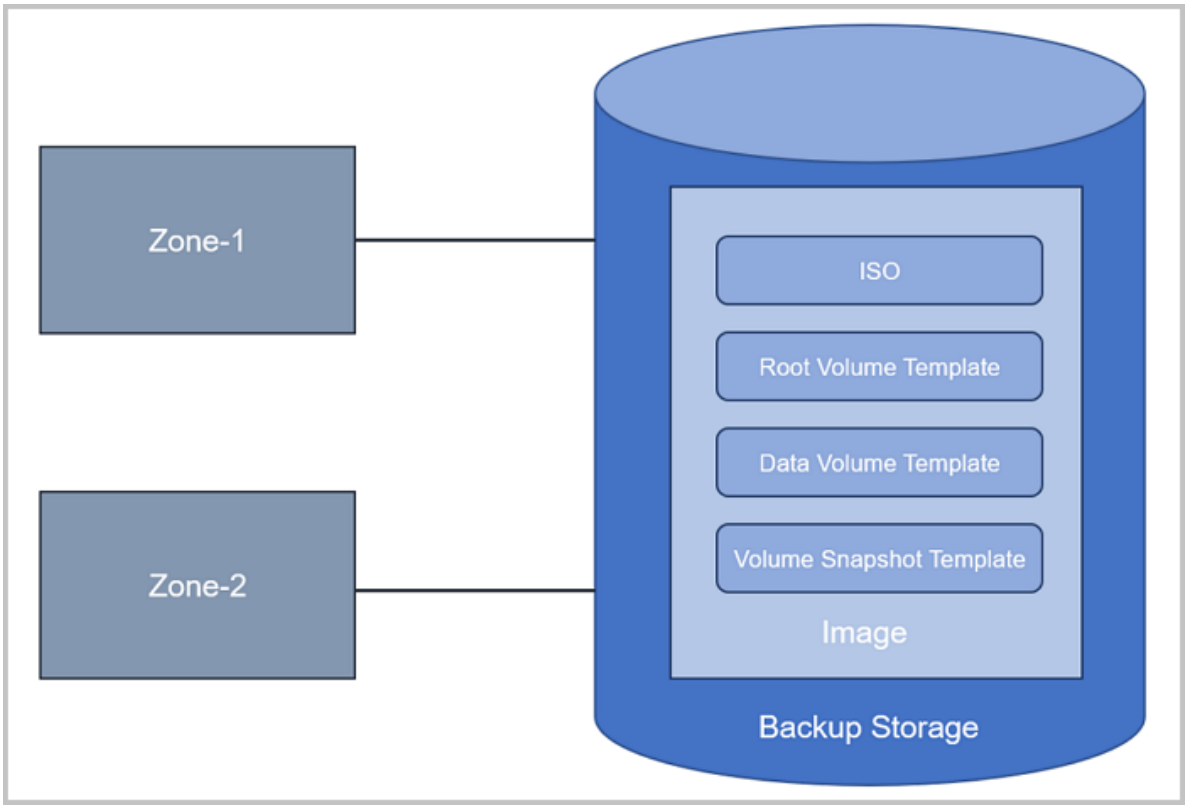
2. If the primary storage is NFS, make sure that a host is available to connect the primary storage . If the reconnection fails, check whether the IP address of the NFS server, the NFS shared directory, and NFS mount parameters are correct.
3. If the primary storage is Ceph, check whether the distributed block storage is normal. If the reconnection fails, check whether the Ceph IP address, Ceph SSH port, user name, and password are correct, whether the user name has the sudo permission, and whether the Ceph cluster status is normal.
4. If the primary storage is Shared Mount Point (SMP), manually mount the SMP directory on the host. We recommend that you make some configurations in `/etc/rc.local` so that the SMP directory can be mounted automatically after the host is started.

8.5 Backup Storage

A backup storage is a storage server used to store image templates including ISO.

- A backup storage must be attached to a zone before the resources on the zone can access it. Note that you can share images across multiple zones by using the backup storage, as shown in *Backup Storage*.

Figure 8-4: 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 | Primary Storage

The types of both primary storage and backup storage are strongly associated, as shown in *Relations Between Backup Storage and Primary Storage*.

Table 8-3: Relations Between Primary Storage and Backup Storage

PS/BS	ImageStore	SFTP	Ceph
LocalStorage	○	○	×
NFS	○	○	×
Shared Mount Point	○	○	×
Ceph	○	×	○
Shared Block	○	×	×

- When primary storages are LocalStorage, NFS, or Shared Mount Point, the default type for backup storages is ImageStore, or SFTP.
- When primary storages are NFS or Shared Mount Point, the corresponding shared directories can be manually attached 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, backup storages can use the primary storages in the same Ceph cluster as backup storages. In addition, backup storages can use the primary storages with the ImageStore type as backup storages.
- When primary storages are Shared Block, the default type for backup storages is ImageStore.

Notice

When you use backup storages, note that:

- The following types of backup storage are supported:

  1. **ImageStore**

     - Image files are stored by means of image segmentation. Incremental storage is supported.
     - Snapshots and images can be created when VM instances are running or stopped.

- When VM instances are cloned without data volumes, the VM instances that are running , paused, or stopped can be cloned.
- When VM instances are cloned with data volumes, the VM instances that are running, paused, or stopped, and with storage types of LocalStorage, NFS, Shared Mount Point, Ceph, or Shared Block can be cloned.
- Images can be synchronized across ImageStore backup storages within the same management network.
- The existing images can be obtained. In addition, you can obtain the existing image files under the URL path in the backup storage.

2. **SFTP**

- Only the SFTP Community edition is supported.
- Image files are stored by means of files.
- Snapshots and images can be created when VM instances are stopped.
- On the backup storage, the images that you created can be accessed according to the corresponding backup storage path, and can be copied to other cloud environments for direct use.

3. **Ceph**

- Image files are stored by means of Ceph distributed block storages.
- Snapshots and images can be created when VM instances are running or stopped.
- When VM instances are cloned without data volumes, the VM instances that are running , paused, or stopped can be cloned.
- VM instances cannot be cloned with data volumes.
- Images can only be exported on backup storages.

  Assume that the image path you use is *ceph://bak-t-c9923f9821bf45498fdf9cdfa1749943/61ece0adc7244b0cbd12dafbc5494f0c*.

  Then, run the following commands 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 image name.
```

```
# /root/export-test.image is the name of the exported target
file.
```

- After you delete a backup storage, all image files will also be deleted and cannot be restored. Please exercise caution. The delete operation only removes the information about the backup storage and images recorded in ZStack. Actual data will not be deleted.
- The following are some details about backup storage cloning and snapshot:
  - Online cloning: ImageStore backup storages can be cloned with or without volumes. Ceph backup storages can be cloned without volumes.
  - Offline cloning: ImageStore backup storages can be cloned with or without volumes. Ceph backup storages can be cloned without volumes.
  - Online snapshot: You can create snapshots for ImageStore and Ceph backup storages online.
  - Offline snapshot: You can create snapshots for ImageStore, SFTP, and Ceph backup storages when VM instances are shut down.
  - Online image creation: You can create images for ImageStore and Ceph backup storages online.
  - Offline image creation: You can create images for ImageStore, SFTP, and Ceph backup storages when VM instances are shut down.
- You can clean up the invalid data that was completely deleted in a backup storage to release the storage space.

Note:

- For example, after you completely delete an image file as well as the VM instances that use the image, you can perform data cleaning to release the storage space of the backup storage.
- Only ImageStore backup storages support the data cleaning operation.

8.5.1 ImageStore

ImageStore stores image files in the form of image segmentation. When the type of a primary storages is LocalStorage, NFS, Shared Mount Point, Ceph, and Shared Block, you can use the primary storage with ImageStore backup storages.

- Image files are stored by means of image segmentation. Incremental storage is supported.
- Snapshots and images can be created when VM instances are running or stopped.

- When VM instances are cloned without data volumes, the VM instances that are running, paused, or stopped can be cloned.
- When VM instances are cloned with data volumes, the VM instances that are running, paused , or stopped, and with storage types of LocalStorage, NFS, Shared Mount Point, Ceph, or Shared Block can be cloned.
- Images can be synchronized across ImageStore backup storages within the same management network.
- The existing images can be obtained. In addition, you can obtain the existing image files under the URL path in the backup storage.

8.5.2 Backup Storage Maintenance (Advanced)

8.5.2.1 ImageStore Maintenance

ImageStore Capacity Expansion

To expand the capacity of an ImageStore backup storage, follow these steps:

1. Disable your local backup storage.
2. Add a new large-capacity disk to a host, and format the partition. Assume the device name is */dev/sdc*.
3. Create a new directory */new_volume*, and run the command `mount /dev/sdc1 /new_volume` to mount this disk.
4. Run the command `rsync -a /zstack_bs /new_volume/` to copy the existing disk files to the new disk.
5. Add content to */etc/fstab* and bind the mount point of the physical disk to the */zstack_ps* directory.
6. Restart the host, and use `df -h /zstack_bs` to check the space increment after expansion.
7. Restart the ZStack management node service.
8. Reconnect the host and continue to use ZStack.

ImageStore Maintenance

The steps for planned maintenance of an ImageStore backup storage are as follows:

1. Disable the ImageStore backup storage.
2. On the **Backup Storage** page, select the ImageStore backup storage, and select **Clear Data** from the **Actions** drop-down list to clean up the invalid data that was completely deleted in the backup storage to release the storage space.

3. After you clean up the data, enable the ImageStore backup storage to continue to use it.

8.5.2.2 Backup Storage Reconnection

Reconnecting a backup storage will redeploy the agent to perform related checks.

Factors to be checked if a backup storage fails to be reconnected:

1. If the backup storage is SFTP or ImageStore, check whether the SSH port, user name, and password are correct, and whether the user name has the sudo permission.
2. If the backup storage is Ceph, check whether the distributed block storage is normal. If the reconnection fails, check whether the Ceph IP address, Ceph SSH port, user name, and password are correct, whether the user name has the sudo permission, and whether the Ceph cluster status is normal.

8.6 SAN Storage

ZStack supports SAN storages and allows you to add iSCSI servers.

iSCSI Server

ZStack allows you to add iSCSI storages. Without reaching to each host for making further configurations, ZStack automatically logs in to iSCSI, automatically scans and discovers disks, and automatically configures iSCSI connections. The entire process is convenient and quick. Specifically, iSCSI disks that can be correctly identified support the following usages:

- iSCSI disks can be passed through directly to VM instances.
- iSCSI disks can be added as Shared Block primary storages in shared block.

FC Storage

ZStack supports FC storage passthroughs, automatically scans and discovers FC storages that you preconfigured, and provides a direct display of FC storage details. Specifically, FC LUN devices that can be correctly detected support the following usages:

- LUN devices of a FC storage can be passed through to VM instances.
- LUN devices of a FC storage can be added as Shared Block primary storages in shared block.

8.6.1 SAN Storage Maintenance (Advanced)

iSCSI Storage Maintenance

The steps for planned maintenance of an iSCSI storage are as follows:

1. Add a new iSCSI device to ZStack.

2. On the iSCSI server side, configure the server IP address and other information that can be accessed. Make sure that the iSCSI service side can access the iSCSI server properly.
3. Log in to the Cloud via the UI, choose **Hardware** > **SAN Storage** > **iSCSI Storage**, and add an iSCSI server.
4. Enter the login information and log in to the iSCSI storage.
5. Synchronize data from the iSCSI storage.

FC SAN Storage Maintenance

The steps for planned maintenance of a FC SAN storage are as follows:

1. Add a FC SAN storage to ZStack.
2. Contact the storage vendor to map the FC SAN storage to a host and make sure that the storage LUN partitioned by the FC SAN storage can be recognized properly on the server.
3. Log in to the Cloud via the UI, choose **Hardware** > **SAN Storage** > **FC Storage**, and view the mapped FC SAN storage.
4. After the scanning is finished, click **Sync Device Info** to synchronize the storage data.

9 Network Resource

9.1 Network Diagram

ZStack supports the network diagram feature. Notice that the Cloud not only supports the global diagram (All), but also allows you to generate your own diagram (Custom) by selecting resources where you can quickly locate the resource states.

Global Diagram Operations

You can perform the following operations on a global diagram:

- Check: Allow you to directly check the network diagram of the entire cloud.
- Refresh: Click the refresh button at the upper left on the UI to display the latest global diagram.
- Export: Click the **Export** button at the upper left on the UI to export the current global diagram as the **png** format.
- Search: Click the **Search** button at the upper right on the UI to display the **Search** box. You can conduct searches by resource types and resource properties.
  - Supported resource types: VM instance, router (vRouter or VPC vRouter), private network, and public network.
  - Supported resource properties: resource name, resource UUID, IP address, and EIP.
- Zoom in/out: Click the **Zoom In** or **Zoom Out** button at the lower right on the UI to zoom in or out the current network diagram.
- Default: Click the **Default** button at the lower right on the UI to recover the network diagram that you have zoomed in or out to the default size.
- Highlighted display via resource selection: Select the resource to be highlighted. When you select a resource, you can highlight that resource and its associated resources.
- Floated display of resource information: Provide a floating display of a resource to which you hover over. The related information of the resource will be automatically floated on the UI.
- Open console: Open the console of the resource to which you hover over. The related information of the resource will be automatically floated on the UI. Then, click the console button at the upper right of the floating page to open the console of the resource.
- State display of router or VM instance: Manipulate real-time states of routers or VM instances by the dot colors at the upper right of the resources. For more information, see *State Display Definition for Router or VM Instance*.

Table 9-1: State Display Definition for Router or VM Instance

Router/VM State	Dot Color
Starting	Blue
Running	Green
Stopping	Blue
Stopped	Red
Rebooting	Blue
Deleting	Blue
Deleted	Grey
Migrating	Blue
Expunging	Blue
Pausing	Blue
Paused	Grey
Recovering	Blue
Unknown	Yellow

Custom Diagram Operations

You can perform the following operations on a custom diagram:

- Generate and check diagram by specifying resource: Generate and check a corresponding network diagram by specifying resources. Currently, these resources include VM instance, router (vRouter or VPC vRouter), private network, and public network.
- Refresh: Click the refresh button at the upper left on the UI to display the latest diagram.
- Export: Click the **Export** button at the upper left on the UI to export the current diagram as the **png** format.
- Search: Click the **Search** button at the upper right on the UI to display the **Search** box. You can conduct searches by resource types and resource properties.
  - Generate the custom network diagram in advance. By using the **Search** button, you can conduct searches for the resources on the custom diagram.
  - Supported resource types: VM instance, router (vRouter or VPC vRouter), private network, and public network.
  - Supported resource properties: resource name, resource UUID, IP address, and EIP.

- Zoom in/out: Click the **Zoom In** or **Zoom Out** button at the lower right on the UI to zoom in or out the current network diagram.
- Default: Click the **Default** button at the lower right on the UI to recover the network diagram that you have zoomed in or out to the default size.
- Highlighted display via resource selection: Select the resource to be highlighted. When you select a resource, you can highlight that resource and its associated resources.
- Floated display of resource information: Provide a floating display of a resource to which you hover over. The related information of the resource will be automatically floated on the UI.
- Open console: Open the console of the resource to which you hover over. The related information of the resource will be automatically floated on the UI. Then, click the console button at the upper right of the floating page to open the console of the resource.
- State display of router or VM instance: Manipulate real-time states of routers or VM instances by the dot colors at the upper right of the resources. For more information, see *Table 1*.

9.2 L2 Network Resource

9.2.1 VXLAN Pool

A VXLAN Pool is a collection of VXLAN types that encapsulate packets with UDP. It is a large layer 2 network established over an IP network for a large-scale cloud computing center.

- To use a VXLAN network, create a VXLAN Pool first.
- A VXLAN Pool cannot be used to create an L3 network, and is only a collection of VXLAN networks.
- A VXLAN Pool supports two types of SDN: software SDN and hardware SDN.
  - Software SDN:
    - The VNI range of a software SDN VXLAN Pool supports 1-16777214.
    - The CIDR IP address of a host that is attached to a cluster can serve as a VTEP (VXLAN tunnel endpoint).
      - Generally, a VTEP corresponds to an NIC IP address of a compute node within a cluster. On the Cloud, you can configure a VTEP according to its corresponding CIDR. For example,
        - Assume that the NIC IP address of a compute node is *10.12.0.8*, the subnet mask 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 of the compute node is *172.20.12.13*, the subnet mask 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 looked up without checking physical L2 devices.
- Hardware SDN:
  - An SDN controller needs to be added to the Cloud in advance.
  - The VNI range of a hardware SDN VXLAN Pool depends on a virtually distributed switch to which an SDN controller corresponds.
  - The NIC of a host that is attached to a cluster must connect to a switch managed by the SDN controller.
  - If you use VCFC to configure hardware SDN, verify that you configure the mapping between VLAN and VXLAN on VCFC in advance.

VXLAN Pool Operations

You can perform the following operations on a VXLAN Pool:

- Change name: Change the name of the VXLAN Pool.
- Change description: Change the description of the VXLAN Pool.
- Attach cluster: Attach the VXLAN Pool to a cluster.
  - Software SDN VXLAN Pool: Specify a CIDR to which a VTEP corresponds. Make sure that the CIDR of each host in the cluster has the corresponding IP address. Or otherwise, you will fail to attach the VXLAN Pool to the cluster.
  - Hardware SDN VXLAN Pool: The NIC of a host that is attached to a cluster must connect to a switch managed by an SDN controller.
- Detach cluster: Detach a cluster from the VXLAN Pool.
- Delete: Delete the VXLAN Pool. If you delete the VXLAN Pool, its corresponding subresource VXLAN networks, associated L3 network, and VM NICs will be deleted as well.
- Share: Share the VXLAN Pool to the specified regular account.
- Recall: Recall the VXLAN Pool from the regular account. You can make this account invisible.
- Share to all: Share the VXLAN Pool to all regular accounts.
- Recall from all: Recall the VXLAN Pool from all regular accounts. You can make these accounts invisible.
- Create VNI range: Create a VNI range to the VXLAN Pool.

- Delete VNI range: Delete a VNI range from the VXLAN Pool.
- Change VNI range name: Change the VNI range name of the current VXLAN Pool. Only a single operation is supported.

  Note:

  - Changing a VNI range name supports up to 255 characters. You can use special characters as needed.
  - Under one VXALN Pool, different VNI ranges can use the same VNI range name.
- Create VXLAN network: Create a VXLAN network according to a VXLAN Pool. Each VXLAN network corresponds to a VNI in a VXLAN Pool.
- Delete VXLAN network: Delete the VXLAN network. If you delete the VXLAN network, its corresponding subresource L3 network and VM NICs of the L3 network will be deleted as well.
- Audit: Check the related operations of the VXLAN Pool.

Notice

- VXLAN Pool and VxlanNetwork are a logical grouping of L2 network overlaid over L3 networks , and are specifically used by VxlanNetwork. Before you use VxlanNetwork, create a VXLAN Pool. Clusters are associated to VTEP of L3 networks. Encapsulation and de-encapsulation of VTEP messages are based on VTEP. After you complete creating VXLAN Pools, you can create VxlanNetwork by specifying or randomly selecting VNIs. Finally, create L3 networks based on VxlanNetwork, and then use them to create VM instances.
- When you attach a cluster to a VXLAN Pool, check whether the corresponding IP range of all hosts within the cluster have available IP addresses to match VTEP. If no IP addresses of the hosts are available, you cannot attach the cluster to this VXLAN Pool correctly.
- A VXLAN Pool can only attach or detach a cluster. VxlanNetwork is the subresource of the VXLAN Pool, and cannot attach or detach any cluster.

9.2.2 L2 Network

Four Major Types of L2 Network

An L2 network supports mainly four types.

1. **L2NoVlanNetwork**

   L2NoVlanNetwork indicates that VLAN settings are not used for connecting the corresponding host.

- If you set VLAN for a switch port, make sure that the switch port is in Access mode.
- If you do not set VLAN for the switch port, do not make any operation.
- If you create an L2 network, note that a bridge will be created according to the network device that you have entered.

2. **L2VlanNetwork**

   L2VlanNetwork indicates that VLAN settings are used for connecting the corresponding host.

   - The switch port connected by the host must be in Trunk mode.
   - The virtual LAN can be divided logically. Notice that it can support 1-4094 subnets.
   - If you create an L2 network, notice that a VLAN device will be created according to the network device that you have entered. In addition, a bridge will be created according to the VLAN device.

3. **VxlanNetwork**

   VxlanNetwork indicates that the VXLAN network is created by using the VNI specialized by VxlanNetworkPool of the **Software SDN** type.

   - VxlanNetwork is created according to VxlanNetworkPool of the **Software SDN** type.
   - Each VxlanNetwork corresponds to a VNI specialized by VxlanNetworkPool of the **Software SDN** type.
   - VxlanNetwork can be used for creating an L3 network.

4. **HardwareVxlanNetwork**

   HardwareVxlanNetwork indicates that the VXLAN network is created by using the VNI specialized by VxlanNetworkPool of the **Hardware SDN** type.

   - HardwareVxlanNetwork is created according to VxlanNetworkPool of the **Hardware SDN** type.
   - Each HardwareVxlanNetwork corresponds to a VNI specialized by VxlanNetworkPool of the **Hardware SDN** type.
   - HardwareVxlanNetwork can be used for creating an L3 network.

Note:

- When you add NoVlanNetWork or VlanNetwork, enter the NIC name.
- 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.

L2NoVlanNetwork and L2VlanNetwork Types

L2 networks with L2NoVlanNetwork and L2VlanNetwork types support the following operations:

- Change name: Change the name of the L2 networks.
- Change description: Change the description of the L2 networks.
- Attach cluster: Attach the L2 networks to a cluster.
- Detach cluster: Detach the L2 networks from a cluster.
- Share: Share the L2 networks to the specified regular accounts or projects.
- Recall: Recall the L2 networks from the specified regular accounts or projects. You can make these accounts or projects invisible.
- Share to all: Share the L2 networks to all regular accounts or projects.
- Recall from all: Recall the L2 networks from all regular accounts or projects. You can make these accounts or projects invisible.
- Delete: Delete the L2 networks. If you delete the L2 networks, subresource L3 networks and VM NICs of the L3 networks will be deleted as well.
- Audit: Check the related operations of the L2NoVlanNetwork and L2VlanNetwork types.

HardwareVxlanNetwork Type

The L2 network with the HardwareVxlanNetwork type supports the following operations:

- Change name: Change the name of the L2 network with the HardwareVxlanNetwork type.
- Change description: Change the description of the L2 network with the HardwareVxlanNetwork type.
- Delete: Delete the L2 network with the HardwareVxlanNetwork type. If you delete the L2 network with the HardwareVxlanNetwork type, its subresource L3 networks and VM NICs of the L3 networks will be deleted as well.
- Audit: Check the related operations of the HardwareVxlanNetwork type.

Notice

When you use an L2 network, note the following:

- NovlanNetWork and VlanNetwork are a logical grouping of L2 network. Their differences mainly depend on whether VLAN is supported. When you add NovlanNetWork and VlanNetwork,

specify an NIC device number whose configurations are identical to those of a switch side of NIC ports of hosts.

- NoVlanNetWork, VlanNetwork, and VXLAN Pool can attach clusters, while VxlanNetwork is only a subset of a VNI range so that VxlanNetwork cannot attach clusters.
- When you use VLAN devices, do not need to create NICs with VLAN ID on hosts. Take eth0.2016 as an example. Only enter eth0 for the device names, and enter 2016 for the VLAN ID. Then, ZStack will automatically create eth0.2016. If you have the eth0.2016 network device and then still choose to enter 2016 in the VLAN ID field, ZStack will create a new network device with the name at eth0.2016.2016.
- ZStack Private Cloud allows you to create multiple L3 networks by using an L2 network. However, we do not recommend doing so unless you have special business requirements.

9.3 L3 Network

An L3 network is a collection of network configurations for VM instances, including the IP range, gateway, DNS, and network services.

- An IP range includes the start IP address, end IP address, netmask, and gateway. For example, 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 an IP range, such as *192.168.1.0/24*.
- DNS provides DNS resolution services used for configuring VM networks.

Public Network

Generally, a public network is a type of network wherein anyone has access and through it can directly connect to the Internet. Due to a fact that the public network is a logical concept, you can also customize the public network when you cannot access the Internet. In addition, the public network can provide the network service in a vRouter network and a VPC network.

- The public network can be used in the flat network environment to create VM instances.
- The public network can be used in the vRouter network environment to create vRouters.
- The public network can be used in the VPC network environment to create VPC vRouters.

System Network

A system network is a specific network used by a management node.

- The system network can be used as a management network to deploy and set related resources, such as a host, primary storage, backup storage, and vRouter.

- The system network can be used as a migration network to migrate VM instances.
- Assume that your network resources are insufficient, and that you cannot use a management network separately. Then, the public network will act as the management network.
- An independent system network can be used in a specific manner, such as managing the vRouter network.
- The system network cannot be used to create regular VM instances.

Private Network

A private network is known as a business network or an access network. Generally, VM instances use the private network. The private network is specified as the network used by VM instances, and supports three network architecture models: flat network, vRouter network, and VPC network.

Specific Network Scenarios

- Management Network

  A management network is a type of a system network, which can be used for managing and controlling the corresponding physical resources.

  - For example, when you access a host, a backup storage, a primary storage, and other resources that require an IP address, use the management network.
  - When you create vRouters or VPC vRouters, you need an IP address that can be interconnected between management networks in vRouters or VPC vRouters. With this IP address, you can deploy an agent and obtain messages returned by the agent.
- Storage Network

  A storage network is the network specified by the shared storage. You can use the 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 clusters, you can specify CIDR for the VDI network. In the VDI scenario, the network traffics generated by the protocol communication between 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 clusters, you can specify CIDR for the migration network, which can be used for VM migrations. 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 the network that images can be synchronized among backup storages with the ImageStore type in the same management node.

  - If you have deployed an independent network for synchronizing images, you can specify CIDR for the image synchronization network.
  - If you do not make any configuration to the image synchronization network, the management network will be used by default.
  - If you set both source image store and target image store as the image synchronization network, only the target image store can take effect.

- Data Network

  A data network is the network where data can transfer between a compute node and a backup storage.

  - If you use an independent data network, you can avoid network congestion, and improve the data transfer rate.
  - If you do not make any configuration to the data network, the management network will be used by default.

- Backup Network

  ZStack provides backup services, which are add-on licensed features. A backup network is the network where you can back up your local VM instances, volumes, or databases to the local backup storage. Also, the backup network is the network where you can restore the local backup data from the local backup storage.

  - If you deploy an independent network for local backups, you can specify CIDR for the backup network.
  - If you use an independent network, you can avoid network congestion and improve the data transfer rate.
  - If you do not make any configuration to the backup network, note that the management network will be used for local backup by default.

Note:

Backup Service is a separate feature module. To use this feature, purchase both the Base License and the Plus License of Backup Service. The Plus License cannot be used independently.

- Traffic Network

  A traffic network is the specified network of a port mirroring, which can be used to mirror the network traffic in the NIC to remote access. In addition, the traffic network cannot act as other networks, and cannot be used to create VM instances.

Notice

- When you create VM instances, you can specify multiple networks. That is, you can specify multiple flat networks, vRouter networks, VPC networks, or a combination of flat networks, vRouter networks, and VPC networks.
- We support 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. If the L2 network is the HarewareVxlanNetwork type, the private network that you created can only support the flat network and other corresponding network services rather than vRouter network.

Considerations for Creating L3 Network

When you create a public network or L3 network, you can specify a DHCP IP address. Based on the selected network range (IP range or CIDR), note the following:

- **IP Range**:

  Note:

  - If you create an L3 network and enable the DHCP service for the first time, or if you add the first IP range for the L3 network that has enabled the DHCP service, you can customize the DHCP IP address.
  - If the L3 network has a DHCP IP address, you cannot customize the DHCP IP address when you add an IP range.
  - The DHCP IP address can be included or excluded in or from the added IP range. However , the DHCP IP address must be within the CIDR to which the added IP range belongs, and must not be occupied.

- The IP range specified within the start IP address and end IP address cannot contain IP addresses of the link-local address (169.254.0.0/16).
- If not specified, the system will randomly specify an IP address within the IP range that you added.

- **CIDR**:

Note:

- If you create an L3 network and enable the DHCP service for the first time, or if you add the first network range for the L3 network of the enabled DHCP service, you can customize the DHCP IP address.
- If the L3 network has a DHCP IP address, you cannot customize the DHCP IP address when you add the IP range.
- The DHCP IP address can be included or excluded on the IP range that you added. However, the DHCP IP address must not be in conflict with the current CIDR.
- If not specified, the system will randomly specify an IP address within the added IP range.
- The first IP address in a CIDR is deemed as a gateway by default, and cannot serve as a DHCP IP address.

Considerations for Using IPv6 Network

If an L3 network uses the IPv6 protocol, note the following:

- If the IP address type of the L3 network (including public network, flat network, and VPC network) is changed, restart the VM instances that use this network for the configurations to take effect. For example, the IP address type of the network changes from IPv4 to IPv4+IPv6.
- If you add a new type of IP range to a VPC network that has a VPC vRouter attached, restart the VPC vRouter. Otherwise, the network might not be accessible. For example, you might want to add a new IPv6 IP range to the VPC network that already has an IPv4 IP range.
- If the L3 public network in the vRouter offering has an IPv6 IP range, when you create a VPC vRouter, make sure that you use the vRouter image of version 3.10.0 or later.
- If you want to create VM instances by using a network with the IPv6 type or IPv4+IPv6 type, run the dhclient -6 NIC_NAME command to manually obtain an IP address.
- We recommend that you use only one IPv6 IP address for a VM instance to avoid potential risks.

9.4 Flat Network

A flat network is a network that does not offer any segmentation options. Any VM instance that is attached to this network can see the same broadcast traffic and can communicate with each other without requiring a router. A flat network has the following attributes:

- Hosts and VM instances reside on the same layer 2 broadcast domain.
- Services such as User Data, EIP, DHCP, and security group are provided.
- Both the distributed EIP and the distributed DHCP can avoid a single point of failure (SPOF). Hence, when high concurrency occurs, the entire concurrency of the system can be improved effectively.

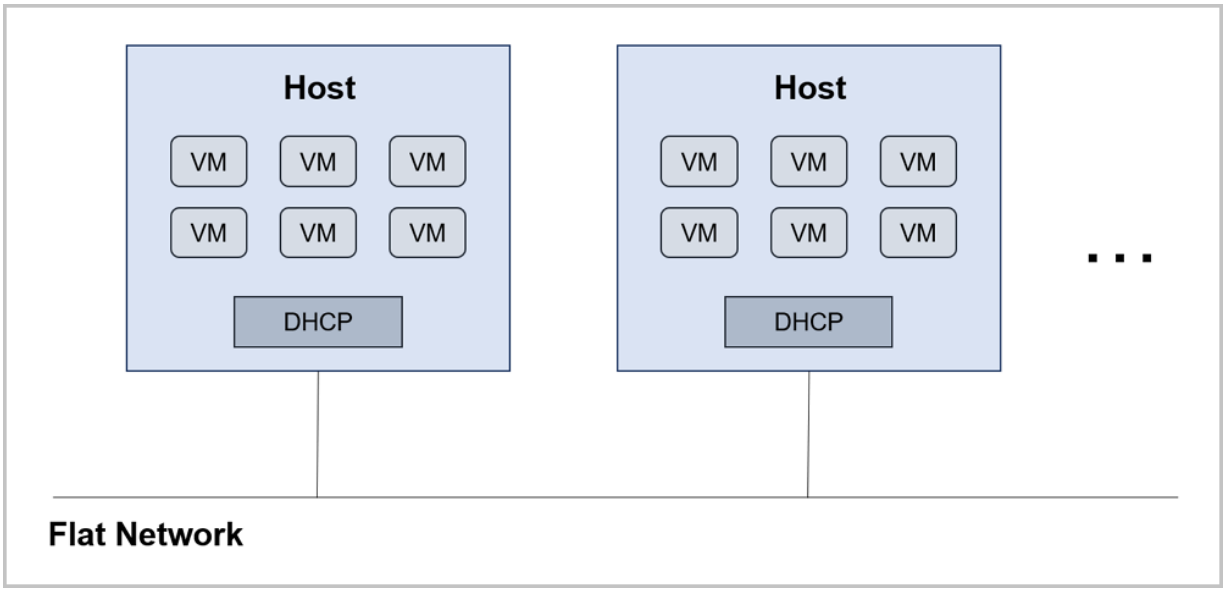
A flat network provides the following network services:

- User Data: Enable you to start, attach or perform specific operations for a VM instance by using `cloud-init`, such as injecting `ssh-key`.
- EIP: Refer to elastic IP addresses that can be used to reach internal, private networks via public networks.
- DHCP: Obtain IP addresses dynamically, which is achieved by the distributed DHCP.

  Note:
  The DHCP service includes the DNS feature.
- Security group:
  - The security group network module provides the security group service.
  - VM firewalls can be securely controlled with iptables.

The flat network topology is shown in *Flat Network Topology*.

Figure 9-1: Flat Network Topology



Notice

When you use a flat network, note the following:

- The flat network runs DHCP servers independently on each host, and then these DHCP servers will assign IP addresses for VM instances.
- The flat network provides the DHCP service by using dnsmasq.
- If all VM instances on a host cannot obtain IP addresses, verify that you check the dnsmasq progress on the host and dnsmasq.log under `/var/lib/zstack/dnsmasq/` that corresponds to your NIC directory of the L2 network.
- The flat network can forward elastic IP addresses by using namespace and iptables of Linux.
- The elastic IP addresses of the flat network require that VM instances must have default routers accessible to gateways of private networks.
- When you add IPv4 network range, note the following:
  - Gateways, broadcast addresses, and network addresses cannot be contained in the IP range that you added.
  - The network ranges of a private network cannot overlap public networks or management networks attached by vRouter offerings.
- When you add an IPv6 network range, note the following:
  - When you use Stateless-DHCP or SLAAC, manually change the generation method of the VM IP addresses to EUI64.

— Prefix length is 64~126. If you set a value less than 64, VM instances will fail to be created.

— Gateways cannot be included in the added IP range.

9.5 VPC

Virtual Private Cloud (VPC) is a custom network environment that consists of VPC vRouters and VPC networks. With VPC, enterprise users can build a logically isolated private cloud.

VPC vRouter and VPC Network

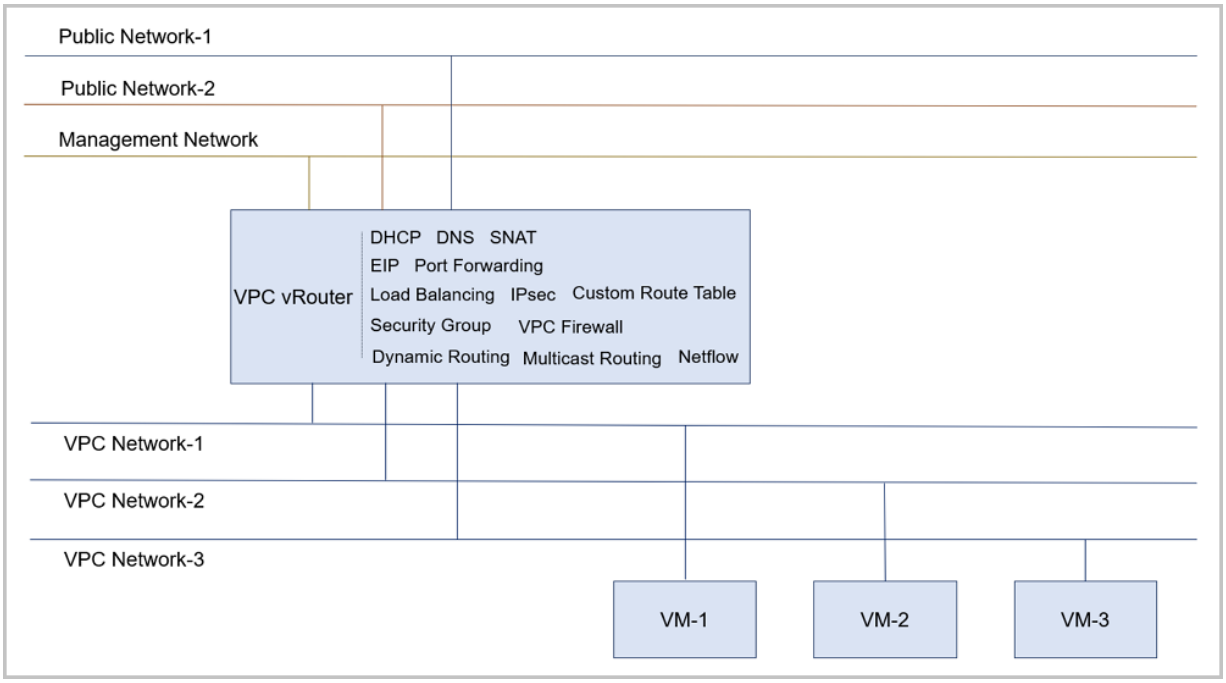
VPC consists of VPC vRouter and VPC network.

1. VPC vRouter: a vRouter that is created based on a vRouter offering. A VPC vRouter has two types of network: public network and management network.
   - VPC vRouters are the core of VPC. A VPC vRouter can be created by specifying a vRouter offering.
   - To create a vRouter offering, create the required public network, management network, and vRouter image in advance.
   - A VPC vRouter can be attached to or detached from VPC networks or other public networks .
   - The public network and the management network that are defined by a vRouter offering cannot be detached.
   - The same vRouter offering can be used to create multiple VPC vRouters. These VPC vRouters share both the public IP range and the management IP range defined by the same vRouter offering.
   - The public network is the default network used to provide network services.
   - VPC vRouters have higher resource priorities than VM instances. When the host workload rates are extremely high, and then resources contend with each other, the resource priority sequence from low to high is as follows: VM instances with **Normal** priorities < VM instances with **High** priorities < VPC vRouters. For example, when CPU resources contend with each other on hosts, VPC vRouters have higher CPU resource grabbing capability.
2. VPC network: a private network that can be attached to a VPC vRouter.
   - You need to create an L2 network before you can create an L3 VPC network.
   - When you create a VPC network, you can specify a vRouter. Or you can attach a vRouter to the VPC network after you create the VPC network.

- If your VM instances use a VPC network, you cannot detach the VPC network from the VPC vRouter.
- The newly created IP range must not overlap any IP range in the VPC vRouter.

The VPC network topology is shown in *VPC Network Topology*.

Figure 9-2: VPC Network Topology



HA Group of VPC vRouter

High availability (HA) group: You can deploy two VPC vRouters according to the active-backup policy. When the active VPC vRouter is abnormal, the backup VPC vRouter will automatically take over to work properly, thus ensuring your business continuity.

Note:

The VPC vRouters in an HA group will be only displayed on the details page of the HA group, but will not be displayed independently in the vRouter table.

VPC Features

VPC has the following feature benefits:

- Flexible network configuration: Different VPC networks can be flexibly attached to the VPC vRouters. You can customize an independent IP range and an independent gateway for each

VPC network. VPC vRouters allow you to attach or detach gateways, and also to dynamically configure your route tables and route entries.

- Secure and reliable isolation: Different VPC networks in different VPCs are logically isolated. That is, the VPC networks support VLAN and VXLAN for logical layer 2 isolation, and different VPCs of different accounts will not affect each other.
- Multi-subnet interconnection: Multiple VPC networks under the same VPC can communicate privately and securely with one another.
- Network traffic optimization: VPC supports distributed route features, indicating that VPC can optimize the east-west network traffic, and reduce the network latency effectively.
- VPC vRouter HA: In a VPC vRouter HA group, you can deploy two VPC vRouters according to the active-standby policy. When the active VPC vRouter is abnormal, the standby VPC vRouter will automatically take over to work properly, thus ensuring your business continuity.

VPC Network Service

The VPC network, which acts as a private network, provides a group of network services by using VPC vRouters.

- DHCP: By default, the VPC network provides distributed DHCP services by using the flat network service module.
- DNS: A VPC vRouter can act as a DNS server to provide DNS services. The DNS address in a VPC vRouter VM instance is the IP address of the VPC vRouter. Note that the DNS address that you set is forwarded by the VPC vRouter.
- SNAT: A VPC vRouter can provide the source network address translation (SNAT) services for VM instances. Then, the VM instances can directly access the Internet by using SNAT.
- Route table: Through the route table, you can manage and customize routes.
- Security group: The security group service is provided by the security group network service module. You can configure and manage firewalls for VM instances by using iptables.
- Elastic IP address (EIP): You can bind an EIP to a VPC network. Then, the public network can interconnect with the private network of the VM instance.
- Port forwarding: The port forwarding service allows a public IP address to interconnect with the private IP address of a VM instance. To be more specific, you can create port forwarding rules to allow external networks to reach specific ports of your VM instances.
- Load balancing: The load balancing service distributes your inbound traffics from a public IP address to a group of backend VM instances. Then, this service will automatically check and isolate the VM instances that are unavailable.

- IPsec tunnel: The IPsec tunnel can be used to achieve interconnection between different virtual private networks (VPNs).
- Dynamic routing: The VPC vRouter supports the Open Shortest Path First (OSPF) routing protocol, which is used to distribute routing information within a single autonomous system.
- Multicast routing: The VPC vRouter 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.
- VPC firewall: The VPC firewall filters the south-north traffic on the VPC vRouter ports, effectivel y protecting the VPC communication security and VPC vRouter security.
- Netflow: The Netflow service monitors and analyzes the inbound and outbound traffics of the VPC vRouter NICs. Currently, the following two types of data-flow output format are supported: Netflow V5 and Netflow V9.

9.5.1 VPC vRouter

The VPC vRouter page displays VPC vRouters and high availability groups on the ZStack Private Cloud.

- VPC vRouter: A virtual router that can be directly created from a vRouter offering. By default, a VPC vRouter has two types of network: public network and management network.

Note:

- VPC vRouters are the core of VPC. A VPC vRouter can be created by specifying a vRouter offering.
- To create a vRouter offering, create the required public network, management network, and vRouter image in advance.
- A VPC vRouter can be attached to or detached from VPC networks or other public networks.
- The public network and the management network that are defined by a vRouter offering cannot be detached.
- The same vRouter offering can be used to create multiple VPC vRouters. These VPC vRouters share both the public IP range and the management IP range defined by the same vRouter offering.
- The public network is the default network used to provide network services.

- VPC vRouters have higher resource priorities than VM instances. When the host workload rates are extremely high, and then resources contend with each other, the resource priority sequence from low to high is as follows: VM instances with **Normal** priorities < VM instances with **High** priorities < VPC vRouters. For example, when CPU resources contend with each other on hosts, VPC vRouters have higher CPU resource grabbing capability.

- VPC vRouter HA group: Deploy a pair of VPC vRouters with the active-standby mode. When the active VPC vRouter is abnormal, the standby VPC vRouter will be used to ensure your business continuity.

Note:

VPC vRouters within high availability groups will only be displayed on the details page of the high availability groups rather than be displayed separately on vRouter lists.

Comparison between VPC vRouter and Regular vRouter

Similarities	Differences
• Are substantially identical and use Linux VM instances achieved by VyOS to act as routing devices. • Must create public networks, management networks, and vRouter image three of which are defined by vRouter offerings. • Support DHCP, DNS, SNAT, security group , EIP, port forwarding, load balancing, IPsec tunnel, Netflow, and other network services. • Cannot detach the public networks and management networks both of which are defined by the vRouter offerings. • Let you configure vRouter route tables and vRouter route entries. • Support high availabilities. By using shared storages, VPC vRouters and regular vRouters will never stop with sufficient resources. • Let you attach and detach new public networks. • Regular vRouter networks can be an exception for VPCs. That is, only a private network under a VPC cannot be detached.	• VPC vRouters can be manually created, while regular vRouters only can be created simultaneously when VM instances are created with vRouter private networks. In other words, regular vRouters cannot be created manually. • The running VPC vRouters that you manually created can only attach public networks and management networks, but regular vRouters must attach public networks, management networks, and private networks. • VPC vRouters let you attach and detach VPC networks, while regular vRouters disallow you to attach and detach private networks. • VPC vRouters let you stop the SNAT network service, while regular vRouters default to enable but cannot stop the SNAT network service. • VPC vRouters support static routing and the OSPF routing protocol, while regular vRouters only support static routing.

VPC vRouter High Availability Group

VPC vRouter HA group: Deploy a pair of VPC vRouters with the active standby bonding mode. When the active VPC vRouter is abnormal, the standby VPC vRouter will be used to ensure your business continuity.

Note:

- VPC vRouters within high availability groups will only be displayed on the details page of the high availability groups rather than be displayed separately on vRouter lists.
- You can import VPC vRouters into high availability groups. The imported VPC vRouters must be in the stopped state.
- Importing the VPC vRouters will synchronize all configurations of the VPC vRouters. Exercise caution. After you import the VPC vRouters, you cannot use them as independent VPC vRouters.
- If the existing VPC vRouters use the same network as the public network and system network , these VPC vRouters cannot be imported into the high availability groups.
- After you create high availability groups, under the high availability groups details page, set DNS for the active-standby VPC vRouters to ensure that the VPC vRouters can work properly.

Notice

When you use a VPV vRouter, note the following:

- To create a vRouter offering, create the required L2 public network, L3 public network, L2 management network, and L3 management network in advance.
- The VPC networks under different VPC vRouters defaults to be isolated within the L2 networks.
- The IP ranges of different VPC networks under the same VPC vRouter cannot be overlapped. Similarly, the gateway of any two VPC vRouters cannot be identical.
- Before regular accounts create VPC vRouters, admins must share vRouter offerings to them. Otherwise, these regular accounts cannot create VPCs.
- To provide network services, VPC vRouters must be in the running state and connected status . If the VPC vRouters are in other states or statuses, check whether related resources are abnormal.
- To avoid malicious attacks, VPC vRouters defaults to disable the SSH password login. The SSH password login can be enabled in the Global Settings.

9.5.2 VPC Network

A VPC network is a virtual version of a physical network. On the Cloud, the VPC network can act as a private network that can be attached to a VPC vRouter. When you create or use a VPC network, note that:

- You need to create an L2 network before you can create an L3 VPC network.
- When you create a VPC network, you can specify a vRouter. Or you can attach a vRouter to the VPC network after you create the VPC network.
- If your VM instances use a VPC network, you cannot detach the VPC network from the VPC vRouter.
- The newly created IP range must not overlap any IP range in the VPC vRouter.

Comparison between VPC Network and Regular Private Network

Similarities	Differences
• Let you flexibly attach multiple public networks. The public networks defined by a vRouter offering cannot be detached. The default IP address of VPC vRouters or vRouters is the IP address of public networks defined by the vRouter offering. This IP address can be selected from the network range of the public network to provide a diversity of network services. • When you create a vRouter offering, a management network can be selected from a system network or public network. If you combine the public network and management network as one, make sure that the public network acts as the management network. If you have independent management networks, ensure that system networks are selected. **Note:** • If your condition does not permit, the management network and the public network can share the same network. • In consideration of security and stability concerns, we recommend that you	• A VPC network can act as the private network of a VPC. A VPC vRouter can be used to provide various network services, while a regular private network supports two types of network structure: flat network and vRouter network. • A VPC vRouter can flexibly attach multiple VPC networks. If the network range of a VPC network attached by the VPC vRouter is similarly *192.168.0.0/24*. Then, the private network IP address of the VPC network corresponded by the VPC vRouter defaults to *192.168.0.1* . Also, this IP address is the default gateway of the regular VM instances that use this VPC network. By using the gateway, the regular VM instances are routed and forwarded to access the Internet in the VPC vRouter. • A vRouter can attach only one regular private network.

Similarities	Differences
deploy the management network independently, and isolate it from the public network. • In terms of the network range, CIDR of public networks, management networks, vRouters or other networks in the vRouters must not be overlapped. For example, assume that the network range of a private network is *10.0.0.0/8*. When a vRouter attaches a network, a new network range cannot be *10.20.0.0/16*. The latter network range is the subset of the former, which is being at risk of IP conflicts Similarly, the network range of any network within the VPC vRouter cannot overlap each other. The network range of a new VPC network cannot overlap that of any network within this VPC vRouter.	If the private network range of a vRouter is similarly *192.168.0.0/24*, the private network IP address of the vRouter defaults to *192.168.0.1*. Also, this IP address is the default gateway of the regular VM instances that use this vRouter network. By using the gateway, the regular VM instances are routed and forwarded to access the internet in the vRouter.

Notice

A VPC vRouter can attach multiple NICs, and support vRouter tables and vRouter route entries. When you use the VPC vRouter, note the following:

- Attaching multiple NICs is generally used in multi-network interconnections, such as hybrid cloud intercommunications.
- The VPC vRouter can attach a vRouter table. After the vRouter table is attached, vRouter route entries within the vRouter table will be added to the VPC vRouter. Hence, the VPC networks of the VPC vRouter can provide corresponding routing features.
- When you add a vRouter table, specify a target network range, and enter the next hop address . Ensure that the next hop is reachable. Generally, the routing type is User Static. To avoid loops, set also User Black Hole, indicating the matched data packages are discarded. The greater the number of the routing priority is, the lower the priority stay.

VPC vRouter Fails to Be Created

When you fail to create a VPC vRouter, note the following:

- Images defined by the vRouter offering:
  - If the images are stored on an ImageStore backup storage, the cluster must be attached to a local storage, NFS, SharedMountPoint, or Ceph primary storage.
  - If the images are stored on an SFTP backup storage, the cluster must be attached to a local storage, NFS, or SharedMountPoint primary storage.
  - If the images are stored on a Ceph backup storage, the cluster must be attached to the corresponding primary storages corresponded by this Ceph backup storage.
- The cluster that is available must attach public networks, management networks, and private networks. Besides, the cluster must have available hosts to meet the requirements of CPU and memory size defined by the vRouter offering.

9.5.3 Routing Protocol Resource

A routing protocol specifies routers to automatically learn the routing information of other available routers, to build routing tables, and to make routing decisions. Compared to a static route, a dynamic routing, which can be applied to a large-scale network environment, supports automatic topology change, route recalculation, and unattended interference. A VPC vRouter supports the OSPF dynamic routing protocol.

Open Shortest Path First (OSPF): An OSPF is an interior gateway protocol of link states and is used to distribute routing information within a single autonomous system (AS). An OSPF is widely used in a data center network and a campus network.

Compared to other routing protocols, the OSPF protocol has the following feature benefits:

- The number of router hops (hop counts) are unlimited.
- Routing information and network information that are updated and changed by a multicast are used.
- The routing convergence speed is faster.
- A cost is served as a metric.
- An SPF algorithm is adopted to effectively avoid loops and minimize the length of the path.

OSPF Area Operations

You can perform the following operations on an OSPF area:

- **Create**: Create an OSPF area.

- **Delete**: Delete an OSPF area that you created. Exercise caution. After you delete the OSPF area, the corresponding routers will delete OSPF configurations and router information. VM instances on these routers will not interconnect to the external network through OSPF.

Notice

- From ZStack 3.5.0 and later versions, VPC vRouters use the OSPF protocol used for intercommunications without disabling the SNAT service.

10 Network Service

ZStack provides VM instances with multiple network resources, including VPC firewall, security group, virtual IP address (VIP), elastic IP address (EIP), port forwarding, IPsec tunnel, load balancing, and flow monitoring.

ZStack supports the following three network models:

- Flat network
- vRouter network
- VPC

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: 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.
   - 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. 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 DHCP service is enabled.
- VIP QoS: Adjusts the upstream bandwidth and downstream bandwidth.
- DNS: Uses vRouters to provide the DNS service.
- SNAT: Enables VM instances to access directly the Internet.
- 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 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: 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.
  - 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.

vRouter 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: 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.
- 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

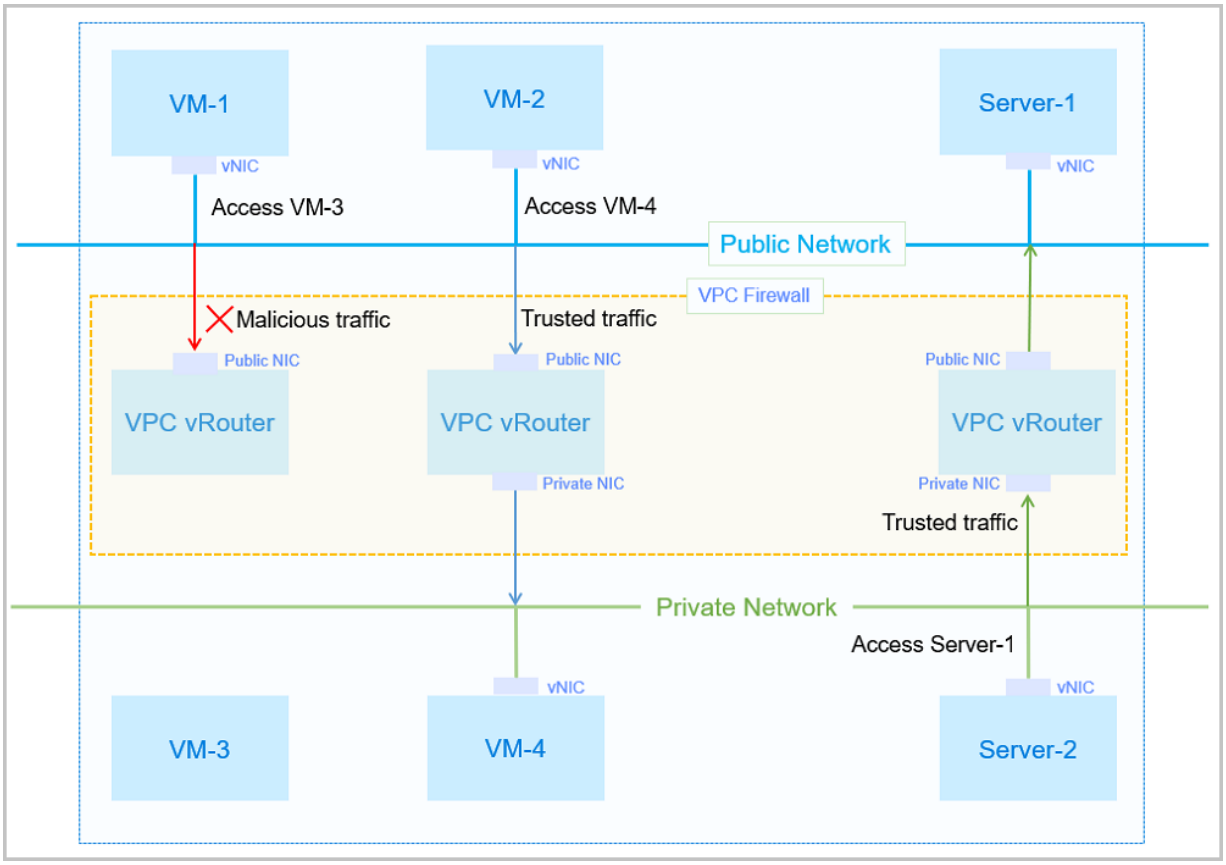
- Dynamic routing: Uses the Open Shortest Path First (OSPF) routing protocol to distribute routing information within a single autonomous system. This service applies to VPC network scenarios.
- Multicast routing: Forwards the multicast information sent by the multicast source to VM instances, achieving 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.

10.1 Security

10.1.1 VPC Firewall

The VPC firewall topology is shown in *VPC Firewall*.

Figure 10-1: VPC Firewall



- Assume that VM-1 attempts to access VM-3: The traffic from VM-1 will match the inbound rule set of the public NIC on the VPC vRouter. If malicious traffics are detected, the access is denied.
- Assume that VM-2 attempts to access VM-4: The traffic from VM-2 will match the inbound rule set of the public NIC on the VPC vRouter, and then will match the outbound rule set of the private NIC on the VPC vRouter. If trusted traffics are detected, the access is allowed.
- Assume that Server-2 attempts to access Server-1: The traffic from Sever-2 will match the inbound rule set of the private NIC on the VPC vRouter, and then will match the outbound rule set of the public NIC on the VPC vRouter. If trusted traffics are detected, the access is allowed.

VPC Firewall Operations

You can perform the following operations on a VPC firewall:

- Create VPC firewall: Create a VPC firewall.
- Update configuration: Modify the configurations of the VPC firewall.

Note:

When you add a new network service, such as OSPF, to a VPC vRouter, some firewall rules will be created at the same time. However, these rules will not be displayed in the UI. To display the rules in the UI, click the update configuration button, and then the rules will be synchronized from the VPC vRouter to the database of the Cloud.

- Add rule set: Add a rule set to the VPC firewall.
- Add rule: Select a rule set and add a rule to it.
- Delete: Delete the VPC firewall.

Rule Set Operations

You can perform the following operations on a rule set:

- Add rule set: Add the rule set to your current VPC firewall.
- Add rule: Add a rule to the rule set.
- Bind network: Bind a network to the rule set.
- Delete: Delete the rule set.

Note:
Inbound rule sets cannot be deleted.

Notice

When you use a VPC firewall, note the following:

- One VPC vRouter can be used to create only one VPC firewall.
- One NIC includes an inbound direction and an outbound direction. You can configure only one rule set for each direction.
- The control mechanism of a VPC vRouter will restrict external access to VM instances without an EIP. If you are using static routing or OSPF, note that the static routing and OSPF will not be available when the firewall with the priority 9999 is disabled. If you still want to use static routing and OSPF, add an inbound rule to the public network NIC.

When you use a rule set, note the following:

- One rule set can have up to 9999 rules attached.
- Only outbound rule sets can be created. Outbound rule sets apply to the outbound direction of the NIC.
- Exercise caution. The inbound and outbound directions of a rule set are designed for VPC vRouters.

- The inbound rule sets are created by the system by default. You can customize your rules in an inbound rule set, but you cannot delete inbound rule sets.
- The rule sets of the same outbound direction can be reused on multiple NICs.

When you use a rule, note the following:

- A rule is a part of a rule set, and cannot be reused on multiple rule sets.
- A system rule is a preconfigured rule that supports system services. The system rule has two priority ranges: 1-1000 and 4000-9999. The priority range of a custom rule is 1001-2999. The system reserved priority range is 3000-3999. Lower integers indicate higher priorities.
- System rules cannot be added, modified, or deleted.

10.1.2 Security Group

A security group serves as a virtual firewall for your VM instances to allow or deny incoming network traffic to, or outgoing network traffic from, multiple types of cloud resources. L3 network security controls are provided over your VM instances, and TCP, UDP, or ICMP data packets are managed for effective filtering. With the security group, you can effectively control specified VM instances on specified networks according to specified security rules.

- Flat networks, vRouter networks, and VPC support the security group service. The security group service is provided by the security group network service module. By using iptables, you can perform security controls over VM instances. This method also applies to flat networks, vRouter networks, and VPC.
- A security group is actually a distributed firewall. When you modify a rule, or when you add or delete a NIC, note that firewall rules in VM instances are updated as well.

Security group rule:

- A security group rule has the following two types of traffics according the direction of data packets:
  - Ingress: Represents inbound data packets that access a VM instance.
  - Egress: Represents outbound data packets that are sent from a VM instance.
- A security group rule supports the following protocol types:
  - ALL: Includes all protocol types, indicating that you cannot specify a port.
  - TCP: Supports ports 1-65535.
  - UDP: Supports ports 1-65535.

— ICMP: By default, both the start port and end port are all -1, indicating that all ICMP protocols are supported.

- A security group rule can limit data sources that comes either from inside or outside of VM instances. Currently, sources can be set as source CIDR or source security group.

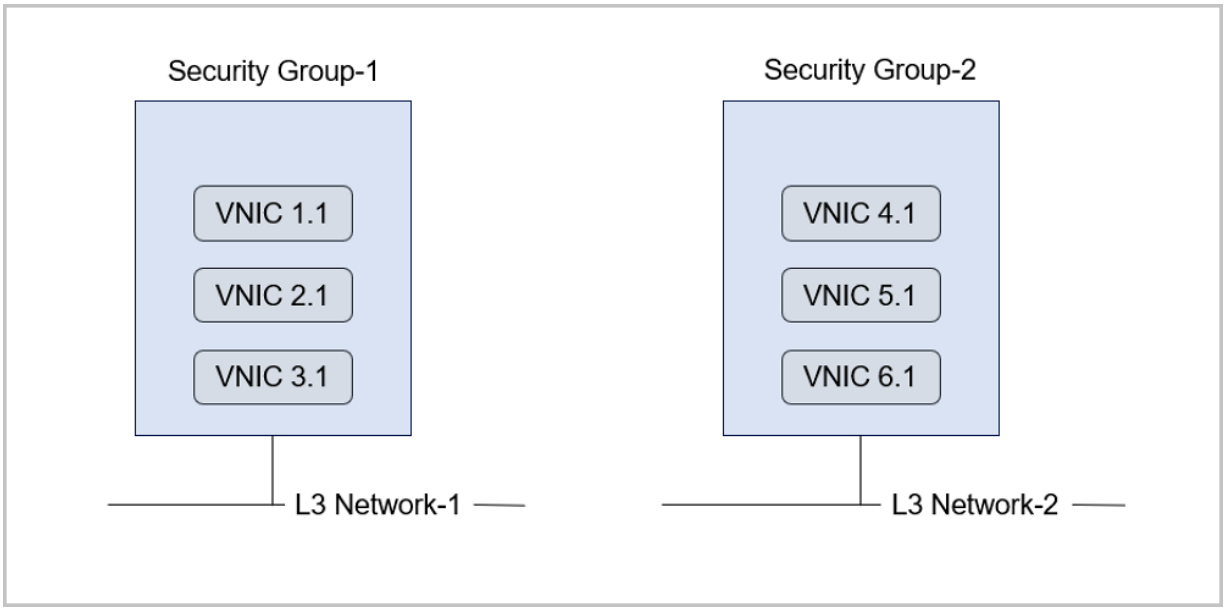
  — Source CIDR: Allows only the specified CIDR.

  — Source security group: Allows only the VM instances in a specified security group.

> **Note:**
> If you set both CIDR and the security group, note that only the intersection of them can take effect.

A security group topology is shown in *Figure 10-2: Security Group*.

Figure 10-2: Security Group



Constraints

The constraints of a security group are as follows:

- A security group can be attached to more than one VM instance. These VM instances will share the same security group rules.
- A security group can be attached to more than one L3 network. These L3 networks will share the same security group rules.
- A security group supports whitelists. That is, you can set all security group rules to Allow. Once you set an allow rule for a port, other ports will not be allowed.

- When you create a security group, the system automatically configures two rules (an inbound rule and an outbound rule whose protocol types are both ALL) for communications 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 did not set any rule, incoming traffics are not allowed to access VM instances in the security group. However, outgoing traffics from VM instances in the security group are allowed.
- If you are using simultaneously the security group with other network services, such as load balancing and vRouter table, make sure that the corresponding rules required by these network services are added to the security group.

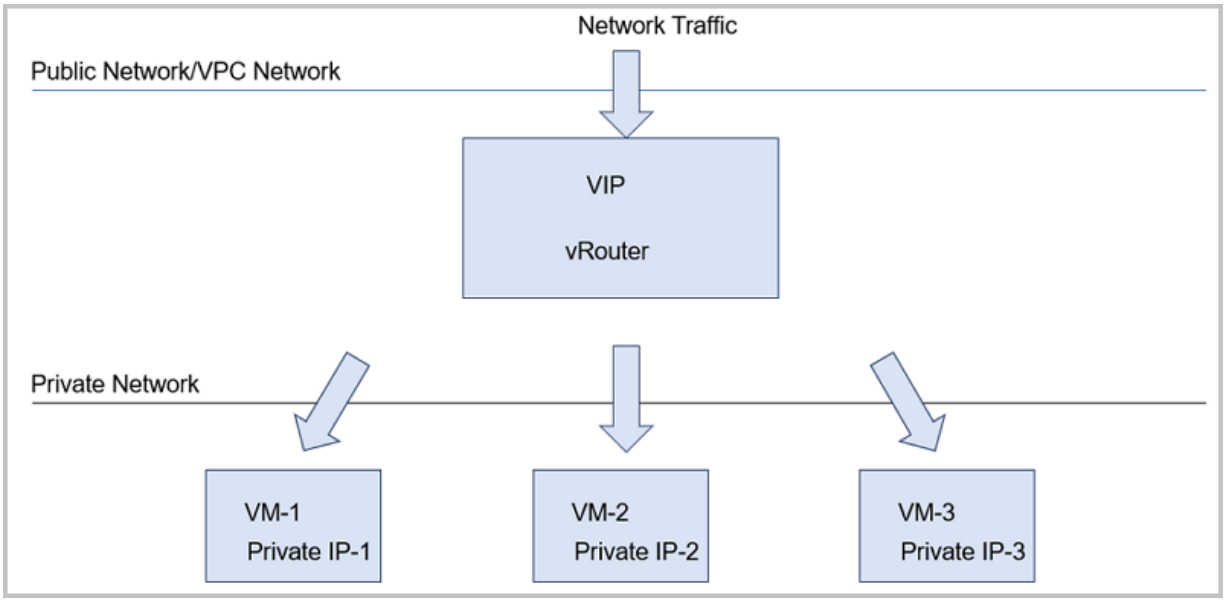
10.2 VIP

In a bridged networking environment, virtual IP addresses (VIPs) are used to provide a group of network services such as elastic IP address (EIP), port forwarding, load balancing, and IPsec tunnel. Packets will be sent to VIPs and then routed to the VM networks.

- The VIP created from a public network can be used to provide network services such as EIP and load balancing for flat networks.
- The VIP created from a public network can be used to provide network services, such as EIP, port forwarding, load balancing, and IPsec tunnel, for vRouter networks and VPC networks.
- The VIP created from a VPC network can be used to provide load balancing services for VPC networks.
- The VIP created from a flat network can be used to provide network services, such as EIP and load balancing, for flat networks.

The following is an example of providing the load balancing service by using a VIP, as shown in *Provide Load Balancing by Using VIP*.

Figure 10-3: Provide Load Balancing by Using VIP



VIP Operations

You can perform the following operations on a VIP:

- Create VIP: Create a custom VIP. Note that system VIPs are created automatically by the Cloud.
- Change name and description: Change the name and description of the VIP.
- Change owner: Change the owner of the VIP.
- Delete:
  - Custom VIP:
    - Deleting a custom VIP will also delete the services associated with the VIP.
    - Deleting a service of a custom VIP does not affect other services associated with the VIP .
  - System VIP:
    - Deleting a service of a system VIP does not affect other services associated with the VIP .
    - Deleting a normal vRouter or VPC vRouter will also delete all services associated with the corresponding system VIPs.
- Add/Delete QoS: Add QoS to or delete QoS from a public VIP or private VIP to control the port traffic of the corresponding VIP. This operation can be performed on the QoS tab of the VIP details page.

Note:

- In a flat network scenario, a custom VIP can be used for EIP and load balancing services. Therefore, the QoS feature of a VIP can be applied to EIP and load balancing services.
- In a vRouter network or VPC network scenario, a custom VIP can be used for EIP, port forwarding, load balancing, and IPsec tunnel services. Therefore, you can set QoS for custom VIPs that provide these four services.
- A system VIP can be used for port forwarding, load balancing, and IPsec tunnel services. Therefore, you can set QoS for system VIPs that provide these three services.
- Multiple QoS rules can be set for the same VIP. Note that the QoS rules without port configurations have the lowest priority.
- Currently, both VPC private VIPs and IPv6 VIPs do not support QoS configurations. If you create a vRouter network by using a vRouter image with the VirtualRouter type, you cannot configure the VIP QoS.

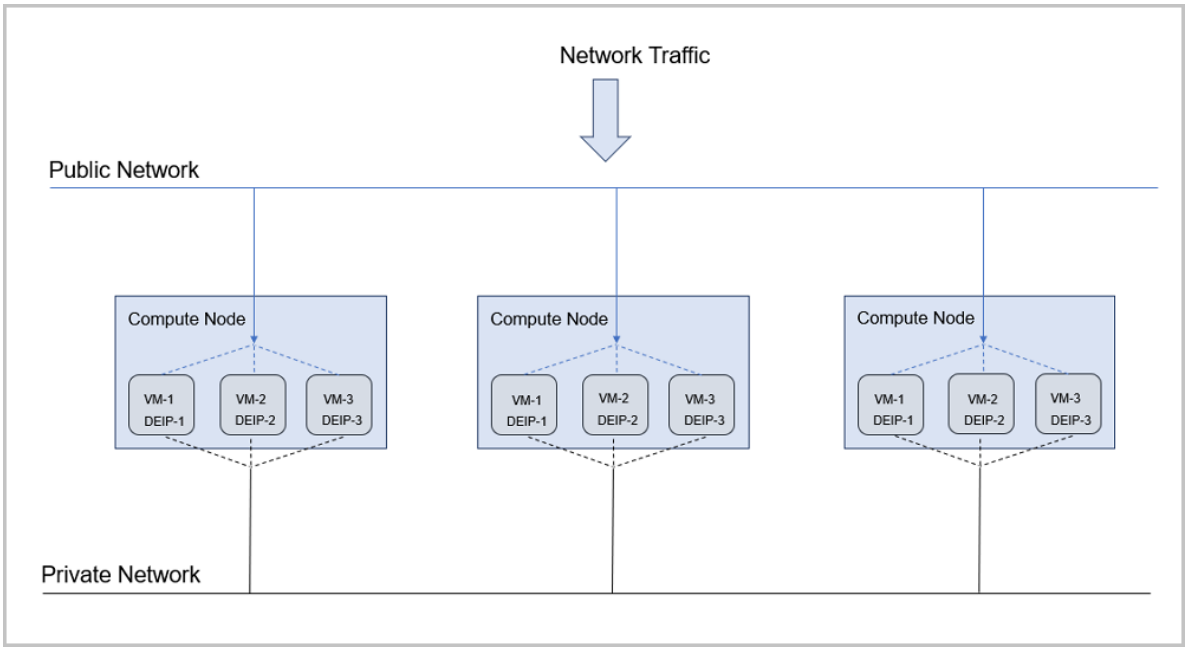
- Monitoring alarm: ZStack supports VIP alarms. After you create an alarm and add the corresponding metric items, the Cloud will automatically monitor multiple metric items associated with the VIP and send alarm messages via email, DingTalk, HTTP application, short message service, or Microsoft Teams.
- Monitoring data: Provide real-time display of the network traffics and packets of the public VIP.
- Audit: View related operations of the VIP.

10.3 EIP

An elastic IP address (EIP) is a method to access a private network through other networks. An EIP converts the IP address of a network into the IP address of another network based on the network address translation (NAT) function.

- The following is an example of a public EIP usage scenario in flat networks, as shown in *EIP Usage Scenario in Flat Network*.

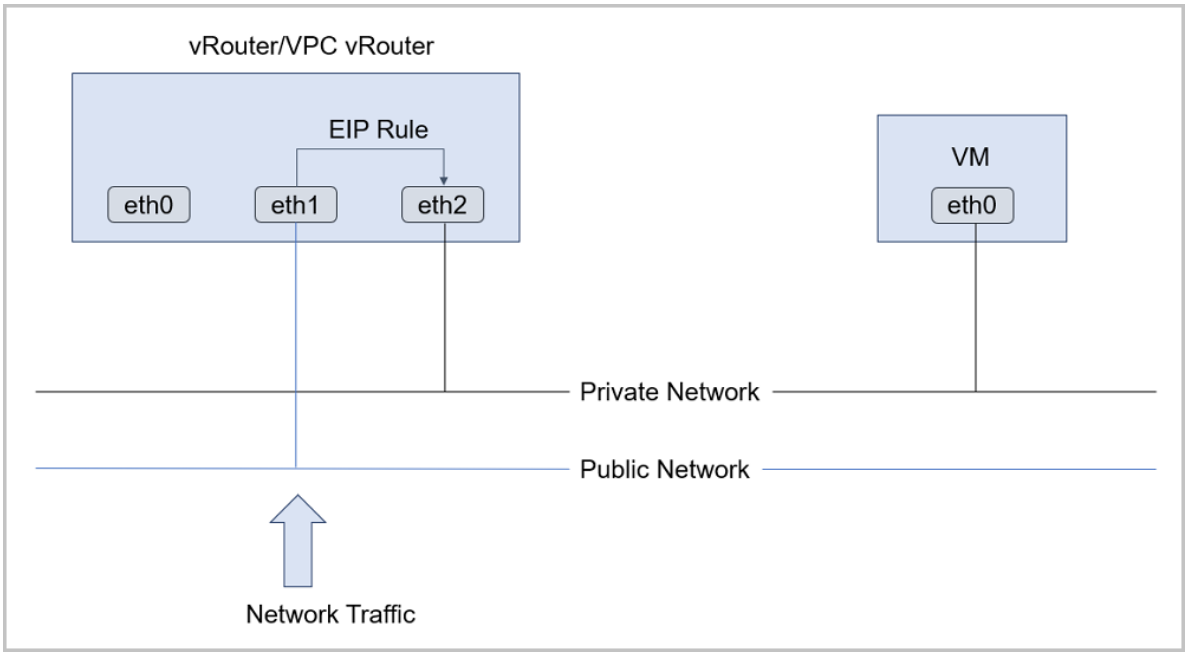
Figure 10-4: EIP Usage Scenario in Flat Network



- Public networks can connect to the Internet through firewalls.
- Private networks (flat networks) provide IP addresses for each VM instance in each compute node. Notice that these IP addresses cannot connect to the Internet by default.
- Distributed EIP is deployed on each compute node, and can be bound to public networks or private networks separately.

• The following is an example of an EIP usage scenario in vRouter networks or VPC networks, as shown in *EIP Usage Scenario in vRouter/VPC Network*.

Figure 10-5: EIP Usage Scenario in vRouter/VPC Network



EIP Operations

You can perform the following operations on an EIP:

- Change name and description: Change the name and description of the EIP.
- Associate: Associate the EIP with a VM NIC.
- Disassociate: Disassociate the EIP from a VM NIC.
- Change owner: Change the owner of the EIP.
- Delete: Delete the EIP. Note that the IP services provided by the EIP will also be deleted. To delete its associated VIP as well, select **Delete VIP**.
- Audit: View related operations of the EIP.

10.4 Port Forwarding

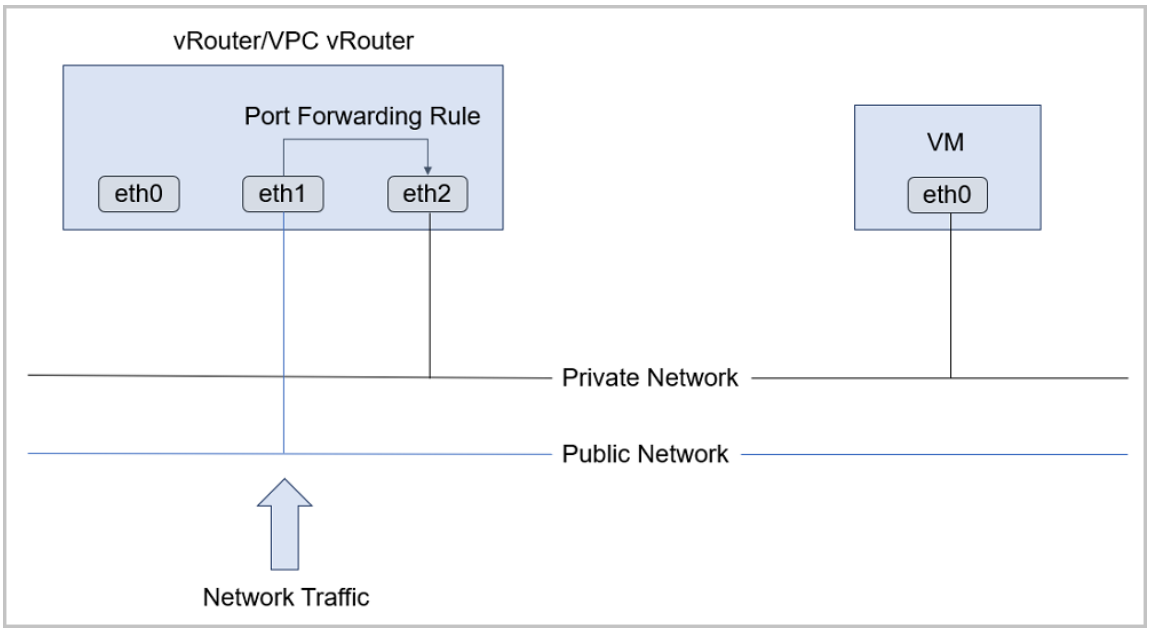
Port forwarding (PF) is a layer 3 forwarding service based on vRouters or VPC vRouters. It can forward the port traffics of specified public IP addresses to the ports of corresponding VM IP addresses. If your public IP addresses are insufficient, port forwarding can provide multiple external services for VM instances to save public IP resources.

- In private networks that enable the source network address translation (SNAT) service, VM instances can access the external network, but cannot be accessed by the external network. A

port forwarding rule can be used to allow the external network to access some specified ports of VM instances behind SNAT.

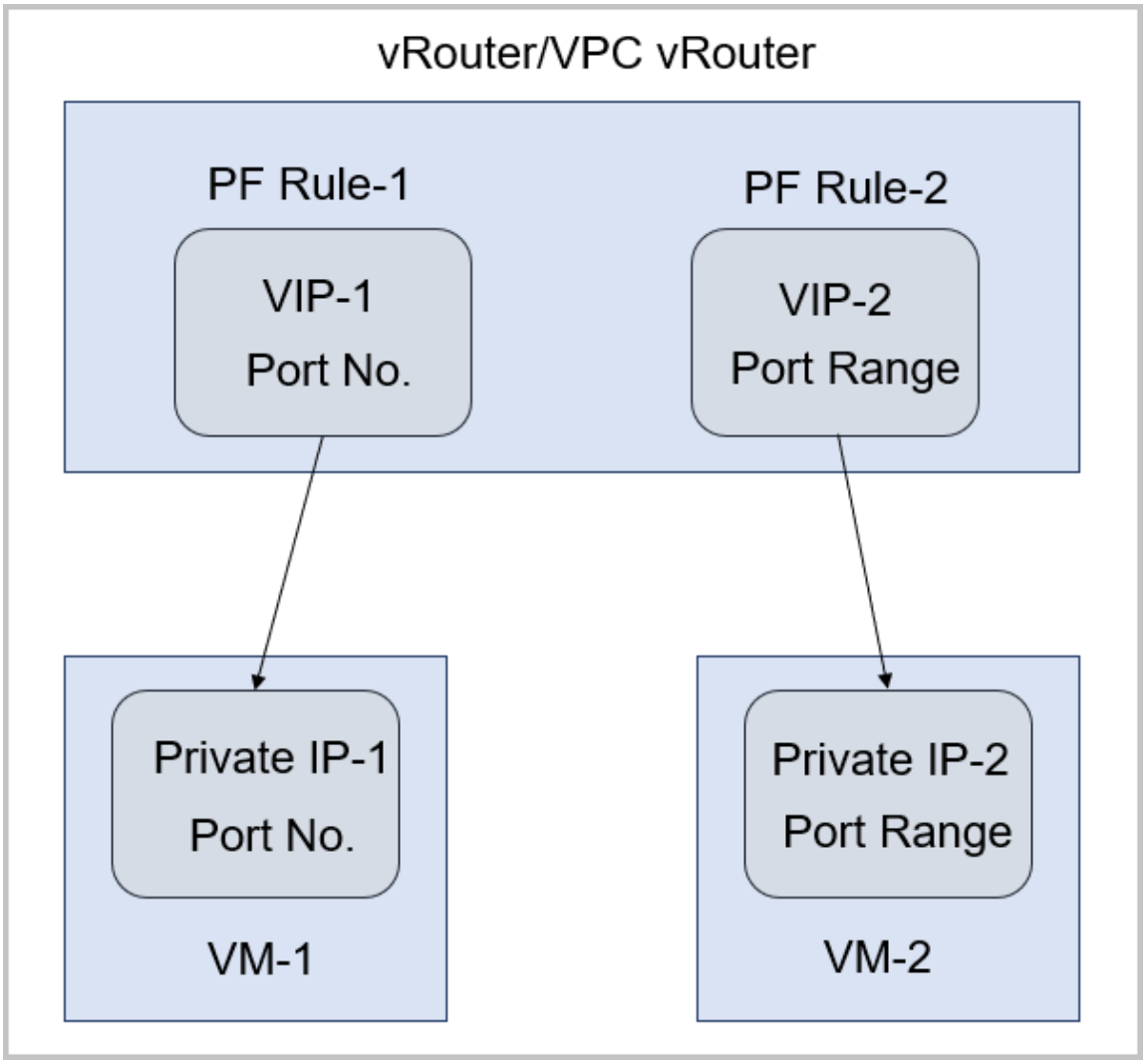
- An elastic port forwarding rule can be dynamically attached to or detached from VM instances.
- The port forwarding service can only be provided by vRouters or VPC vRouters.
  - A port forwarding rule can be created between public networks of a vRouter or VPC vRouter and private networks of VM instances, as shown in *Port Forwarding*.

Figure 10-6: Port Forwarding



- The port forwarding service is provided by VIP.
  - A VIP corresponds to an available IP address in a public IP resource pool.
  - To create port forwarding by using a VIP, either create a new VIP or use an existing VIP.
  - To specify port mappings for port forwarding, choose one-to-one port mapping or range-to-range port mapping, as shown in *VIP - Port Forwarding*.

— Figure 10-7: VIP - Port Forwarding



Constraints

The constraints of a port forwarding rule are as follows:

- To use port forwarding, make sure that the firewall policy in the VM instances can be accessed by the specified ports.
- When you use a VIP to provide the port forwarding service, make sure that the ports used by the VIP are not duplicated.
- A VIP can provide the port forwarding service to different ports of multiple VM NICs on the same L3 network.
- A VM instance can only use one VIP to provide the port forwarding service.

- When you disassociate a VIP from a VM instance and associate a VM instance again, you can only select the VM NIC on the same L3 network of the VM instance that you disassociated before.
- If you select port range for port forwarding, make sure that the source port range and the VM port range are the same. For example, if you set the range of the source port to 22-80, the port range of the VM instance is also 22-80.

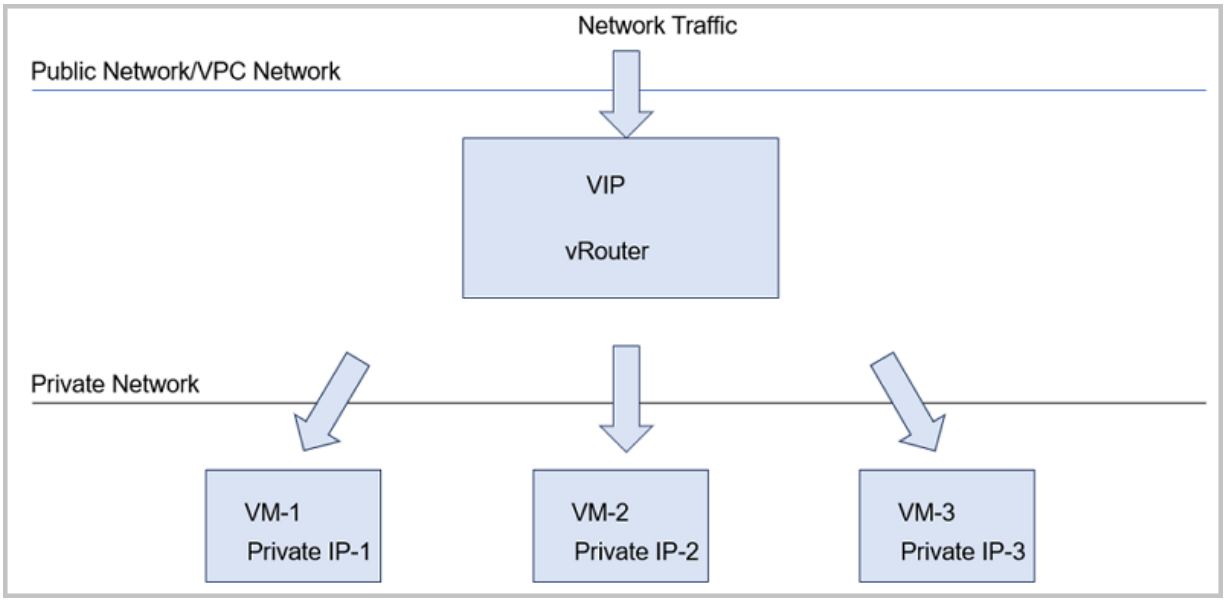
10.5 Load Balancing

Load balancing (LB) distributes inbound traffics from a VIP to a group of backend VM instances, and then automatically detects and isolates unavailable VM instances, whereby enhancing the service capability and availability of your businesses.

- Load balancing automatically distributes your inbound application traffics to the preconfigured backend VM instances, thereby providing highly concurrent and highly reliable access services.
- In your practice, you can adjust the VM instances in load balancing listeners to improve your service capability, which will not affect your normal business access.
- A load balancing listener supports four types of protocols: TCP, HTTP, HTTPS, and UDP.
- If the listener protocol is HTTPS, you need to bind a certificate. Note that you can upload a certificate or a certificate link.
- A load balancer allows you to flexibly configure multiple forwarding policies to achieve advanced forwarding controlling.
- Load balancing allows you to display real-time SLB business traffics and connections in monitoring data.

The following is an example of providing the load balancing service by using a VIP in a flat network, vRouter network, or VPC network scenario, as shown in *VIP - Load Balancing*.

Figure 10-8: VIP - Load Balancing



Load Balancer Operations

You can perform the following operations on a load balancer:

- Change name and description: Change the name and description of the load balancer.
- Create listener: Create a listener for the load balancer.
- Delete: Delete the load balancer. Note that the associated listeners and load balancing service will also be deleted. However, the related VIP and services associated with the VIP will not be affected.
- Audit: View related operations supported by the load balancer.

You can perform the following operations on a listener:

- Change name and description: Change the name and description of the listener.
- Bind VM NIC: Bind a VM NIC to the listener of a load balancer. Then, the VM instance becomes a load balancing resource that works according to the listener rule.
- Unbind VM NIC: Unbind a VM NIC from the listener. Note that the VM NIC will be removed from the load balancing pool.
- Set weight value: When the load balancing algorithm uses weighted round robin, set the weight value for the corresponding VM instances as needed. Value range: 0-100.
- Bind certificate: If the protocol of your listener is HTTPS, bind a certificate or a certificate link to your listener. Note that this operation is not supported if the listener type is TCP, HTTP, or UDP .

- Unbind certificate: If the protocol of your listener is HTTPS, you can unbind a certificate from the listener. Note that this operation is not supported if the listener type is TCP, HTTP, or UDP.
- Display the number of healthy VM instances: Display the number of healthy VM instances attached to the listener on the listener page. For example, healthy backend/total backend number.
- Monitoring data: Display the monitoring data, such as the sessions and inbound/outbound traffics, of the listener.
- Delete: Delete the listener. Note that the load balancing service provided by the listener will be automatically deleted.
- Audit: View related operations supported by the listener.

Constraints

The constraints of the load balancing service are as follows:

- You can create more than one listener for a load balancer.
- The VM NICs bound to the listener of a load balancer must share the same L3 network.
- If the protocol of your listener is HTTPS, you can bind only one certificate to your listener at a time. To change your certificate, unbind the current one first.

Notice

- System virtual IP addresses provided by normal vRouters or VPC vRouters support the load balancing service.
- A listener of a load balancer supports the HTTPS protocol. To use the HTTPS protocol, bind a certificate. The HTTPS lets you upload a certificate and a certificate chain.

10.6 IPsec Tunnel

An IPsec tunnel encrypts and authenticates IP addresses by groups to protect the network transfer data of IP protocols. It provides site-to-site VPN connections.

The following are the attributes of an IPsec tunnel:

- **IPsec connection mode**

  For security reasons, we only support Main Mode and the Encapsulating Security Payload (ESP) protocol, while Aggressive Mode is not supported.
- **IPsec transfer mode**

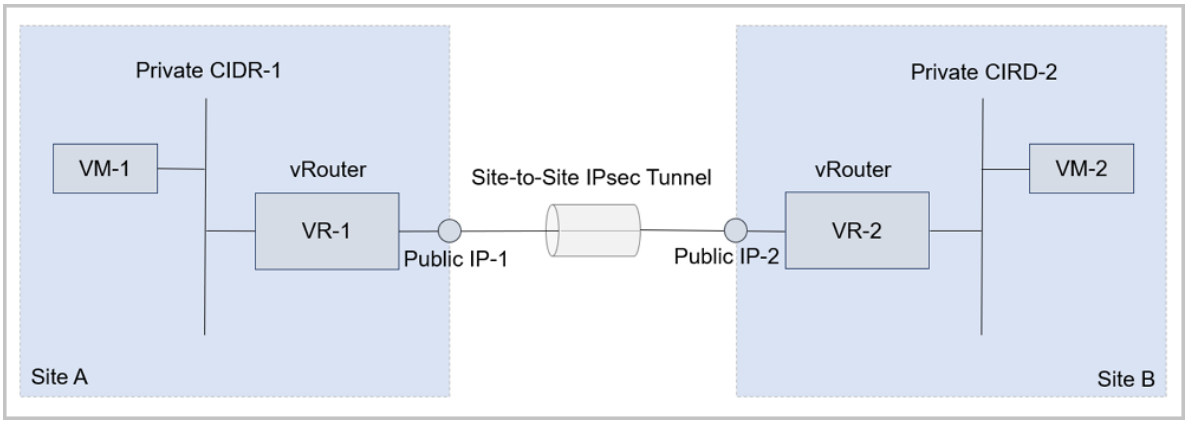
Considering the cloud network model, we only support the site-to-site tunnel mode. The point-to-point PC mode is not supported.

- **IPsec routing model**

  We only support the IPsec routing model that is based on the source-to-destination IP range matching model. The routing forwarding mode is not supported. Notice that OSPF and BGP dynamic routing protocols are not supported.

The typical usage scenario of an IPsec tunnel in vRouter networks is as follows:

- vRouter networks can be used in two isolated ZStack Private Cloud environments. In these two environments, the private networks of VM instances cannot be intercommunicated directly. An IPsec tunnel can be used to realize intercommunication between private networks of the VM instances, as shown in *IPsec Tunnel Usage Scenarios in vRouter Networks*.
- **Figure 10-9: IPsec Tunnel Usage Scenarios in vRouter Networks**



The typical usage scenario of an IPsec tunnel in VPC networks is as follows:

- You can build two separate VPC environments in two isolated ZStack Private Cloud environments. In these two VPC environments, you can create two separate VPC networks (VPC subnets). Notice that these two subnets in these two VPC environments cannot communicate directly with each other. After you use an IPsec tunnel, you can realize intercommunication between subnets within these two VPC environments.

IPsec Tunnel Operations

In the vRouter network scenario, you can perform the following operations on an IPsec tunnel:

- Change name and description: Change the name and description of the IPsec tunnel.

- Delete: Delete the IPsec tunnel. Note that the services provided by the IPsec tunnel will also be deleted. However, the corresponding VIP and services associated with the VIP are not affected.
- Audit: View the related operations supported by the IPsec tunnel.

In the VPC network scenario, you can perform the following operations on an IPsec tunnel:

- Change name and description: Change the name and description of the IPsec tunnel.
- Attach local subnet: Attach more than one local private network to the IPsec tunnel in the VPC network scenario.
- Detach local subnet: Detach a local private network from the IPsec tunnel.
- Add peer CIDR: You can add more than one peer CIDR to the IPsec tunnel in the VPC network scenario.
- Delete peer CIDR: Delete a peer CIDR from the IPsec tunnel.
- Delete: Delete the IPsec tunnel. Note that the services provided by the IPsec tunnel will also be deleted. However, the corresponding VIP and services associated with the VIP are not affected.
- Audit: View the related operations supported by the IPsec tunnel.

10.7 Flow Monitoring

10.7.1 Flow Network

A flow network is a dedicated network for port mirroring, and can be used to mirror the network traffic of a NIC remotely. A flow network cannot be used as other networks and cannot be used to create VM instances.

Note:

- A flow network is a dedicated network for port mirroring, and can be used to mirror the network traffic of a NIC to the remote end.
- A flow network applies to only port mirroring and cannot be used as other networks.
- One port mirroring occupies one flow network.
- Make sure that the VM instances monitored by port mirroring is in the cluster to which the flow network is attached.

Flow Network Operations

You can perform the following operations on a flow network:

- Create flow network: Create a new flow network.
- Add IP range: Add a new IP range to the flow network.
- Delete: Delete the flow network.

> **Note:**
> Deleting a flow network will also delete the port mirroring that is using this network.

10.7.2 Port Mirroring

Port mirroring is used to send a copy of network traffics of a VM NIC from a port to another port, and analyze the business packets on the ports. With port mirroring, network data can be monitored and managed. In addition, problems can be quickly located when network failures occur .

Port Mirroring Operations

You can perform the following operations on a port mirroring:

- Change name and description: Change the name and description of the port mirroring.
- Enable: Enable the port mirroring.
- Disable: Disable the port mirroring.
- Delete: Delete the port mirroring.
- Add session: Add a session to the port mirroring.
- Delete session: Delete a session from the port mirroring.
- Audit: View related operations supported by the port mirroring.

10.7.3 Netflow

Netflow is a network protocol used for analyzing and monitoring inbound and outbound traffics for VPC vRouter NICs. Currently, two types of data stream output format are supported: Netflow V5 and Netflow V9.

Notice

- One Netflow can monitor the traffics of multiple networks on multiple VPC vRouters. All networks of a VPC vRouter can only attach the same Netflow.
- Both IP and port of the collector must be configured correctly. Otherwise, the collected data might be lost.

- A Netflow can collect the north-south traffics of a VPC vRouter and the east-west traffics across the network. In the distributed routing mode, data collected from the east-west traffics across the network might be distorted to performance optimization.
- When a Netflow monitors the routers in a VPC high availability group, it will continuously monitor the network traffics of the primary router to ensure data integrity.
- When a Netflow monitors the network traffics of a VPC vRouter, it will consume the performance of the VPC vRouter. Please select an appropriate monitoring solution to reduce the impact on the performance of the VPC vRouter. The associations between Netflow monitoring and impact on the VPC vRouter performance are as follows:
  - The greater the number of VPC networks monitored by a Netflow reach, the greater the impact on the performance of the VPC vRouter has.
  - The smaller the export interval is, the greater the impact on the performance of the VPC vRouter exerts, and the greater the pressure on the service network bandwidth has.
  - You need to use a stable network, so that the public network of the VPC vRouter can access the collector, ensuring that the Netflow service works properly.

11 Platform O&M

11.1 Performance TOP5

Performance TOP5 is a visual performance monitoring page. This page provides a direct and simple display of the top 5 monitoring metrics of various resources, such as VM instances, routers , hosts, L3 networks, and VIPs. With Performance TOP5, you can directly manage the real-time health state of resources on the Cloud, and improve the O&M efficiency.

- Host tab page:

  On the host tab page, the Cloud analyzes utilizations of CPUs, memories, disks, and network resources of all hosts under the current zone. In addition, the Cloud provides a real-time monitoring display of top 5 resources by taking average CPU utilization, memory utilization, disk read/write IPOS, used disk capacity in percent, disk read/write speed, NIC out/in speed, NIC out/in package rate, and NIC out/in error rate as performance metrics. Different colors of real-time percentage ranks and progress bars will directly indicate resource utilizations or performance bottlenecks, as shown in *Host Performance TOP5*.

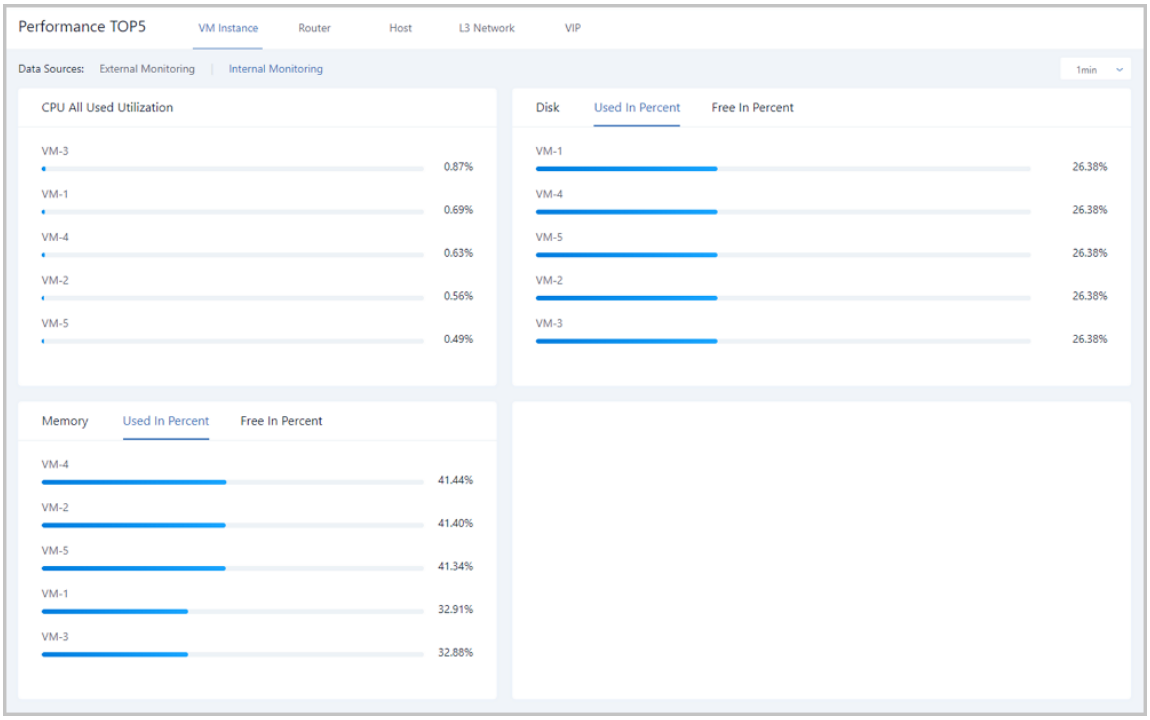
- VM tab page:

  The VM instance page includes external monitoring and internal monitoring.

  - Similar to the host tab page, the external monitoring page provides a utilization analysis of CPUs, memories, disks, and network resources of all VM instances under the current zone. In addition, the external monitoring page provides a real-time monitoring display of top 5 resources by taking average CPU utilization, memory utilization, memory free (idle) in percent, disk read/write IPOS, disk read/write speed, NIC out/in speed, NIC out/in package rate, and NIC out/in error rate as performance metrics. Different colors of real-time percentage ranks and progress bars will directly indicate resource utilizations or performanc e bottlenecks.
  - To check the internal monitoring of VM instances, install an agent. On the internal monitoring page, the Cloud analyzes utilizations of CPUs, memories, and disks of all VM instances under the current zone. In addition, the Cloud provides a real-time monitoring display of top 5 resources by taking average CPU utilization, memory utilization, memory free in percent, used disk capacity in percent, and disk free in percent as performance metrics. Different colors of real-time percentage ranks and progress bars will directly

indicate resource utilizations or performance bottlenecks, as shown in *VM Internal Monitoring TOP5*.

Figure 11-1: VM Internal Monitoring TOP5



Note:

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

- Router tab page:

  The router tab page includes external monitoring and internal monitoring.

  - Similar to the VM instance tab page, the external monitoring page provides a utilization analysis of CPUs, memories, disks, and network resources of all routers (including vRouters and VPC vRouters) under the current zone. In addition, the external monitoring page provides a real-time monitoring display of top 5 resources by taking average CPU utilizatio n, memory utilization, memory free (idle) in percent, disk read/write IPOS, disk read/write speed, NIC out/in speed, NIC out/in package rate, and NIC out/in error rate as performanc e metrics. Different colors of real-time percentage ranks and progress bars will directly indicate resource utilizations or performance bottlenecks.
  - To check the internal monitoring of routers, install an agent. On the internal monitoring page , the Cloud analyzes utilizations of CPUs, memories, and disks of all VM instances under

the current zone. In addition, the Cloud provides a real-time monitoring display of top 5 resources by taking average CPU utilization, memory utilization, memory free in percent , used disk capacity in percent, and disk free in percent as performance metrics. Different colors of real-time percentage ranks and progress bars will directly indicate resource utilizations or performance bottlenecks.

- VIP tab page:

  On the VIP tab page, the Cloud analyzes network transmission performances of all VIPs under the current zone. In addition, the Cloud provides a real-time monitoring display of top 5 resources by taking network in (bytes), network out (bytes), network packets in (count), and network packets out (count) as performance metrics. Different colors of real-time percentage ranks and progress bars will directly indicate performance bottlenecks of some VIPs, as shown in *VIP Performance TOP5*.

- L3 network tab page:

  On the L3 network tab page, the Cloud analyzes IP resource utilizations of all L3 networks under the current zone. In addition, the Cloud provides a real-time monitoring display of top 5 resources by taking used IP in percent, used IP count, available IP in percent, and available IP count as performance metrics. Different colors of real-time percentage ranks and progress bars will directly indicate IP resource utilizations of L3 networks, as shown in *L3 Network Performance TOP5*.

More Information

- On the performance top 5 page at the upper right, select the time drop-down box to set data collection periods for host, VM instance, router, and VIP. Optional period: 1 minute | 1 hour | 24 hours | 1 week, and 1 month. The L3 network tab page does not have data collection period settings.
- A regular account can check the performance top 5. Similar to an admin, the regular account can directly and easily check top 5 information of various monitoring metrics such as VM instances, routers, VIPs, and L3 networks on the performance top 5 page. In this regard, you can directly manage the real-time health state of resources on the Cloud, and can quickly locate problems.
- A project member can also check the performance top 5. Similar to an admin, the project member can directly and easily check top 5 information of various monitoring metrics such as VM instances, routers, L3 networks, and VIPs on the performance top 5 page. In this regard,

project member can directly manipulate the real-time health state of resources on the Cloud, and can quickly locate problems.

11.2 Performance Analysis

ZStack provides real-time performance analysis of the running VM instances, vRouters, and hosts. Specifically,

- **VM Instance, vRouter, and Host**: Display the name, average CPU utilization, memory utilization, disk read or write speed, and NIC in or out speed.
- **L3 Network**: Display the name, used IP count, used IP percentage, available IP count, and available IP percentage.
- **VIP**: Display the name, inbound traffic in bytes, inbound traffic in packages, outbound traffic in bytes, and outbound traffic in packages.
- **Backup Storage**: Display the name and the available backup storage capacity in percent.
- You can customize data ranges (defaults to 1 minute). By clicking the time range button at the upper right, you can specify the start time and end time to check data of performance analysis within different time ranges.
- The left-side filter allows you to check custom performance analysis list according to the resource range and the filter entry. Specifically, a VM instance, router, and VIP allow you to display a custom performance analysis list according to owners.
- By default, each page displays 20 pieces of information. You can choose to display resource counts on a single page. Options: 10 | 20 | 50 | 100. In addition, you can turn your pages by clicking the left arrow button and the right arrow button.
- By clicking the download button at the upper right, you can export a CVS file of resource information.
- A regular account or project member can check performance analysis. Similar to an admin, the regular account or project member can directly and easily check real-time utilizations of VM instances, routers, L3 networks, and VIPs on the performance analysis page.
- A time range can be selected to check performance analysis data. Note that these data are average values collected within the selected time range. To obtain the currently detailed resource data, go to the resource details page.

11.3 Capacity Management

Capacity Management provides a direct display of core resource capacity statistics on the cloud. With Capacity Management, various storage metrics on the Cloud are analyzed and rearranged to

display detailed capacities of core resources in card. In addition, Top 10 resource capacities are displayed so that you can directly manage resource utilizations on the cloud.

The **Capacity Management** page mainly includes the following two sections:

- Upper section: Display detailed capacities of various core resources in card, including primary storages, backup storages, compute nodes, VM instances, volumes, images, snapshots, and management nodes.
- Lower section: Sort top 10 capacities of various core resources, including hosts, primary storages, backup storages, VM instances, images, VM instances, volumes, and snapshots.

Note:

- The resource capacities displayed in this page are all actual physical capacities of your resources.
- The data on this page are all static. To obtain the latest data, refresh this page each time when you go to this page.
- Currently, capacity statistics of primary storages can be analyzed and provided, such as LocalStorage, Shared Block, and Ceph.
- Currently, capacity statistics of backup storages can be analyzed and provided, such as ImageStore and Ceph.

Notice

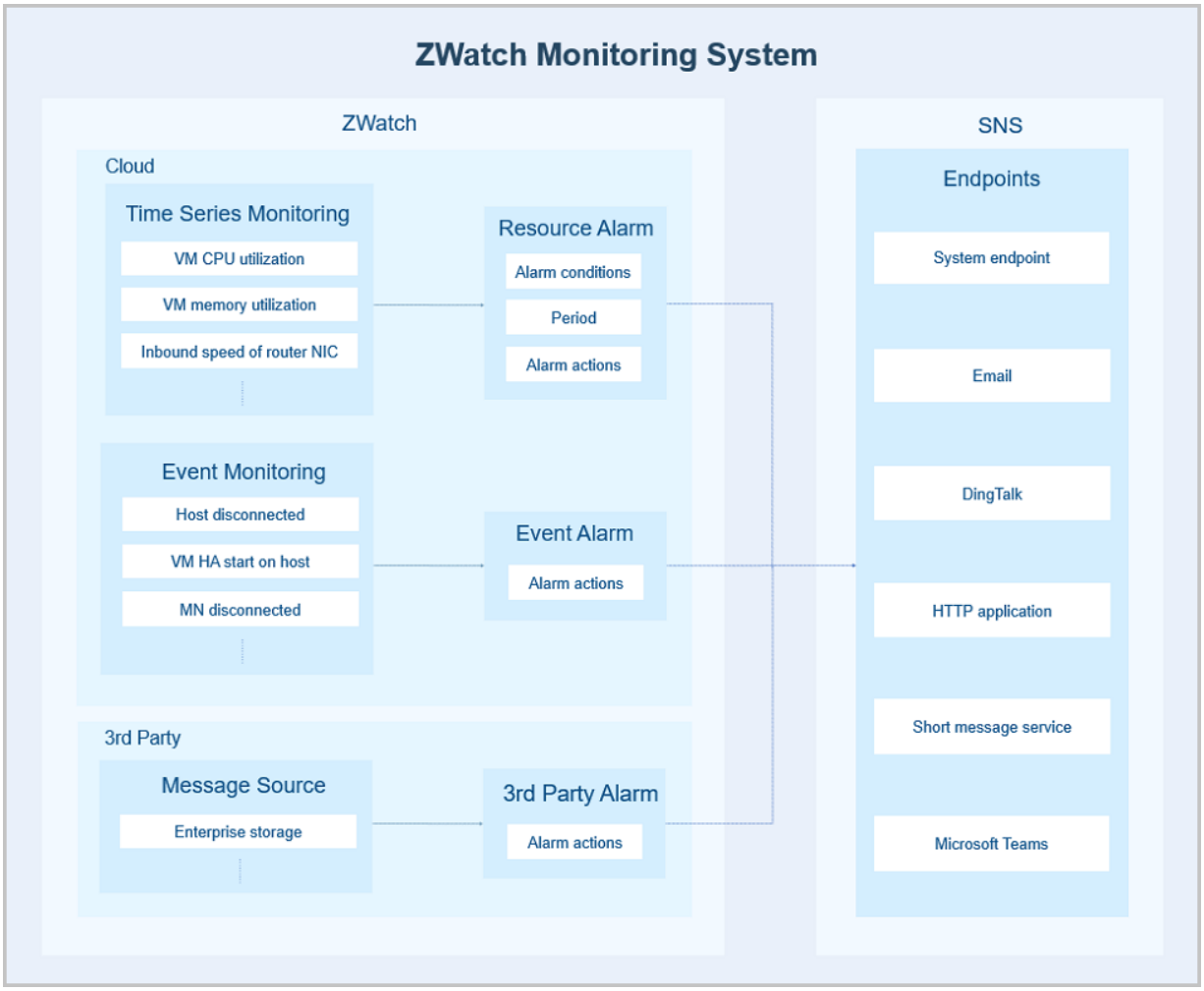
- If your primary storages or backup storages are disconnected, statistics accuracies of associated resource capacity cards and top 10 resource capacities will be affected.
- After you delete or reconnect primary storages and backup storages, wait a while and refresh the capacity management page to obtain the latest capacity data.

11.4 ZWatch

ZWatch, known as ZWatch monitoring system, allows you to monitor time series data and events . With ZWatch, alarm messages are pushed to the specified endpoints via SNS. ZWatch provides three types of alarm: resource alarm, event alarm, and third-party alarm, and supports the following types of endpoint: system endpoint, email, DingTalk, HTTP application, short message service, and Microsoft Teams. To use some specific resource alarms, install an agent.

The ZWatch workflow is shown in *ZWatch Monitoring System*.

Figure 11-2: ZWatch Monitoring System



Alarm

ZWatch allows you to set an alarm for time series data and events, and to receive 3rd-party alarm messages.

- A resource alarm mainly monitors time series data of the Cloud, such as VM memory utilization and host CPU utilization. You can customize a resource alarm.
- An event alarm mainly monitors system events, such as the VM state change event, and the host disconnected event. You can customize an event alarm.

SNS Text Template

An SNS text template is a text template that is used when an alarm or event sends messages to an SNS topic.

- The Cloud contains a default template of an alarm message and a recovered message. If you do not create a template, the Cloud will use the default template.

- You can create multiple message templates, but can only default one template. Specifically, when messages are sent, the default formatted message will be used.
- With `${}`, you can use variables provided by an alarm or event in the template.
- Currently, an SNS text template supports four types of endpoint platform: email, DingTalk, Microsoft Teams, and short message service. If you use an SNS text template, formatted alarm messages will be sent to you via email, DingTalk, Microsoft Teams, or short messages.

Notice

- By default, a resource alarm (except for **License Enabled Days Alarm**) allows you to change the emergency level, alarm condition (if you have set), period, alarm period type, repeat interval, and whether to receive recover message.
- A resource alarm allows you to add an endpoint and remove a newly added endpoint.
- A resource alarm does not allow you to remove the system alarm endpoint and delete default resource alarms.
- If you upgrade the Cloud from an earlier version to 3.8.0, the emergency level of the default resource alarms is **Emergent**. If you customize a resource alarm, the emergency level is **Major** .
- Some metric items need to install agents before you can use these items. Set these items as needed.
- By default, an event alarm allows you to change only the emergency level.
- An event alarm allows you to add an endpoint and remove a newly added endpoint.
- An event alarm does not allow you to remove system alarm endpoints and delete default event alarms.
- If you upgrade the Cloud from an earlier version to 3.8.0, the emergency level of the default event alarms is **Emergent**. If you customize an event alarm, the emergent level is **Major**.

11.5 Notification Service

You can use different endpoints to subscribe to topics. Currently, the supported endpoint types include system endpoint, email, DingTalk, HTTP application, short message service, and Microsoft Teams.

- By default, the Cloud provides a system endpoint. If an alarm binds a system endpoint, you are prompted for alarm notifications displayed near the **Messages** button at the upper right in the UI.

- You can also create an email, DingTalk, HTTP application, short message service, or Microsoft Teams endpoint as needed.

Email Endpoint

- Messages that send to topics will be sent to a specified email address via an email server.
- You can either create an SNS text template in advance or use a system template. Alarm messages will be sent to your email with a unified format.
- You need to add an email server in advance under the current zone, and test whether the email server can work properly.

DingTalk Endpoint

- Messages that send to topics will be sent to a specified DingTalk robot address via DingTalk. If you appoint members, alarm notifications will be sent to corresponding DingTalk members via phone numbers.
- You can either create an SNS text template in advance or use a system template. Alarm messages will be sent to your DingTalk group with a unified format.
- If you set an SNS text template in DingTalk, follow the Markdown syntax. Currently, DingTalk only supports a subset of Markdown syntax.

HTTP Application Endpoint

- Messages that send to topics will be sent to a specified HTTP address via HTTP POST.
- If the specified HTTP application cannot be accessed without a user name and password, enter accurately the user name and the password.

Short Message Endpoint

- Messages that send to topics will be sent to a specified phone number via short message service.
- You can create an SNS text template in advance and set it as the default template. Alarm short messages will be sent to your phone according to the template that you set.

Microsoft Teams Endpoint

- Messages that send to topics will be sent to a specified Microsoft Teams group via Webhook.
- You can either create an SNS text template in advance or use a system template. Alarm messages will be sent to your Microsoft Teams group with a unified format.

Endpoint Operations

You can perform the following operations on an endpoint:

- Create: Create an endpoint.
- Enable: Enable an endpoint that has been stopped.
- Disable: Disable a running endpoint.
- Add alarm: Add an alarm to the endpoint that you selected.
- Remove alarm: Remove an alarm from the endpoint.
- Delete: Delete an endpoint.
- Change name and description: Change a name and description for the endpoint.
- Receive message: Set a time range to check message logs of the endpoint within the time range.
- Audit: Check related operations of this endpoint.

11.6 Notification Center

Notification Center provides notifications and view features of resource alarms or event alarms on ZStack. Shortcut operations are supported, such as converging alarm messages and jumping to alarms or resource details page from alarm message details. With Notification Center, you can quickly locate problems.

Notice

- Subjects of read and unread messages are any role who has the operation permission for the messages. If a role reads alarm messages for the first time or mark alarm messages as read, the read and unread states of these alarm messages will be synchronized to other roles.
- An admin or platform admin can check all alarm messages. The admin or platform admin can perform **Mark All Message As Read** operation for alarm messages that are generated by an admin, regular account, or project. After the marking, the read and unread states of these alarm messages will be synchronized to the admin, regular account, and the project.
- The markings of alarm messages among regular accounts are independent, indicating that these alarm messages are invisible mutually among different accounts. Different accounts can only mark their corresponding alarm messages generated by the alarms of the accounts.
- In the Enterprise Management, alarm messages take projects as units. After a project member , project operator, or project admin reads or marks alarm messages as read, the read and unread states of these alarm messages will be synchronized to other members of this project.

- To use the third-party alarm feature, make sure that the Cloud is connected to a third party.
- The third-party alarm feature can be used by administrators only.

11.7 Operation Log

Operation Log is the user operation records on ZStack, and includes three tab pages: Completed, Ongoing, and Audit.

On the **Ongoing** tab page, check logs of ongoing operations. Specifically, you can check the description, task result, and creation time for the operation. In addition, you can cancel the ongoing tasks.

- The progress bar displays real-time task progresses. To cancel the ongoing tasks, click **Cancel Task**.

  Note:
  Only a portion of tasks support cancellation operations.
- You can search logs of ongoing operations via the operation description.
- You can choose to display log counts of ongoing operations for each page. Optional value: 10 | 20 | 50 | 100. In addition, you can turn pages by clicking the left arrow button and the right arrow button.
- The creation time and completion time are added on the information details page to directly display information details.

On the **Completed** tab page, check logs of completed operations. Specifically, you can check the description, task result, operator, login IP, creation time, completion time, and information details returned by operations to achieve more granular managements.

- You can set a time range to check logs of completed operations within the time range.
- You can search logs of completed operations via the operation description or login IP.
- You can export operation logs in the CSV format.
- You can display log counts of completed operations for each page. Optional value: 10 | 20 | 50 | 100. In addition, you can turn pages by clicking the left arrow button and the right arrow button .
- The creation time and completion time are added on the information details page to directly display information details.

The **Audit** tab page allows you to view resource operation audits and login operation audits.

- Resource operation audit:
  - You can set a time range to check audit information of call APIs within the time range.

    Note:
    The UI can display up to 300 pieces of audit information. Make sure that you adjust an appropriate time range before searching target audit information.
  - You can search the audit information of call APIs via the resource type, resource UUID, API name, and operator.
  - You can export audit information in the CSV format.
  - You can choose to display audit information counts for each page. Optional value: 10 | 20 | 50 | 100. In addition, you can turn pages by clicking the left arrow button and the right arrow button.
- Login operation audit:
  - You can set a time range to check audit information of call APIs within the time range.

    Note:
    The UI can display up to 300 pieces of audit information. Make sure that you adjust an appropriate time range before searching target audit information.
  - You can search the audit information of call APIs via the operator, API name, login IP, or browser.
  - You can export audit information in the CSV format.
  - You can choose to display audit information counts for each page. Optional value: 10 | 20 | 50 | 100. In addition, you can turn pages by clicking the left arrow button and the right arrow button.

Notice

- By default, an operation log is reserved for 90 days. To set log reservation days, choose **Global Settings** > **Advanced**.

  Note:
  Exercise caution when you change log reservation days. If a value that you entered is smaller than the preconfigured log reservation days, logs that exceed the current reservation days will be deleted after the value takes effect.

11.8 CloudFormation

ZStack CloudFormation is a service that helps you simplify the cloud computing resource management and automate the deployment and O&M. With a resource stack template, you can define what cloud resources you need, the dependency between the resources, and the resource configuration. With the CloudFormation engine, CloudFormation can provide automatic batch deployment and resource configuration, as well as easy lifecycle management of cloud resources. You can also use API and SDK to integrate the automatic O&M capabilities.

The advantages of CloudFormation are as follows:

1. You only need to create a stack template or modify an existing one to define what cloud resources you need, the dependency between the resources, and the resource configuration. With the CloudFormation engine, CloudFormation will automatically complete the creation and configuration of all resources.
2. The Cloud provides sample templates and a designer to create stack templates quickly.
3. You can dynamically update a stack template based on your business needs, and then you can update the related resource stack to flexibly meet the needs of business development.
4. If you no longer need a resource stack, you can simply one-click delete it, which also deletes all of the resources in the stack.
5. You can reuse an existing stack template to quickly duplicate all stack resources without repeated configuration.
6. You can flexibly combine cloud services based on different scenarios to meet the needs of automatic maintenance.

11.8.1 Resource Stack

CloudFormation allows you to quickly create and configure a group of resources by using a stack template. This group of resources is defined as a resource stack. You can manage resources in a stack by creating, updating, or deleting the stack.

Supported operations on resource stack are as follows:

- Create a resource stack
- Get the details of a resource stack
- Delete a resource stack

11.8.2 Stack Template

A stack template is a template used to create resource stacks. Creating resource stacks must satisfy the template syntax.

Supported operations on stack template are as follows:

- Create a stack template
- Get the details of a stack template
- Enable a stack template
- Disable a stack template
- Generate a resource stack
- Modify a stack template
- Delete a stack template

Constraints

- The maximum size of a template is 4 MB.
- If you use the CLI or API to create a stack, you can upload a template with a maximum size of 64 KB.

11.8.3 Sample Template

The Cloud provides some commonly used sample templates for you to quickly create resource stacks in CloudFormation.

Supported operations on sample template are as follows:

- Get the details of a sample template
- Generate a resource stack by using a sample template

12 Platform Management

12.1 Billing Management

Billing Management includes bills and pricing list.

Bills of different resources under different projects, departments, and accounts are calculated and displayed in real time based on the unit price and time of usage defined in a pricing list. The time is accurate to seconds.

Pricing list, also known as price table, defines the unit price of different resources based on the resource specification and time of usage. After you attach a pricing list to a project or an account, the corresponding bills of resources will be generated accordingly.

Bills Notice

- Resource bills are generated at a specified time, not in real time. By default, the system generates bills at 00:00 on a daily basis. You can set the bill generation time as needed. The method is as follows:

  Go to **Settings** > **Global Settings** > **Advanced**, locate **The time point of billing generation**, and click the Edit icon. Default value: 0.
- If you change the pricing list of a project or an account, bills of the associated resources will be generated immediately.
- If you delete a up-to-date historical price in a pricing list, bills of the associated resources will be generated immediately.
- The billing details, such as the bills of VM instances, root volumes, data volumes, GPU devices , and public IP addresses, in an account can be viewed by regular accounts and project members.
- To view the project bills, obtain and install the license of the Enterprise Management Module in advance.
- After you attach a pricing list to a project and set the unit price for each resource to be billed, the billing starts, and project bills will be generated accordingly.
- Project bills can be viewed by the administrators, platform members, and project members.
- To view the department bills, obtain and install the license of the Enterprise Management Module in advance.

- After you add a project to a department, you can obtain the project-related billing data, including the historical data, and generate bills by department.
- The billing data is directly related to projects. After you remove a project from a department, all relevant billing data (including the historical data) will be removed from the department bills.
- Department bills can be viewed by the administrators, platform members, and head of departments.
- After you attach a pricing list to an account and set the unit price for each resource to be billed, the billing starts, and account bills will be generated accordingly.
- Account bills can be viewed by the administrators, platform members, and account owners.
- Resource bills are generated at a specified time, not in real time. By default, the system generates bills at 00:00 on a daily basis. You can set the bill generation time as needed. The method is as follows:

  Go to **Settings** > **Global Settings** > **Advanced**, locate **The time point of billing generation**, and click the Edit icon. Default value: 0.
- The resource bills of VM instances and routers (including vRouters and VPC vRouters) are displayed on the VM instance tab page.
- The resource bill of a VM instance includes the total billed amount of the compute resources, such as the memory and CPU.
- The public IP resource bill includes two bill lists: public IP (flat network) and public IP (virtual IP).
- The billing details, such as the bills of VM instances, root volumes, data volumes, GPU devices , and public IP addresses, in an account can be viewed by regular accounts and project members.
- If you turn off the **Switch for Billing** in global settings, the Cloud will stop billing the resources, and no new bills will be generated.
- When a VM instance is deleted but not expunged (completely deleted), compute resources, such as the CPU and memory, and IP resources, such as the public IP (flat network), will be released immediately. Therefore, the CPU, memory, and public IP resources are no longer billed.
- When a VM instance or volume is deleted but not expunged, the VM instance or volume still occupies the physical storage resources (root volume and data volume). Therefore, the root volume and data volume continue to be billed until the corresponding VM instance or volume is completely deleted.

- A VM instance in the Stopped state still occupies storage resources and IP resources. Therefore, the root volumes, data volumes, and public IP (flat network) will continue to be billed .
- An uninstantiated VM instance is not billed. However, the VM instance will be immediately billed once instantiated. For example, a project or an account has an instantiated data volume , and does not attach the data volume to a VM instance. In this case, the data volume is still billed.
- Change the resource owner: The fees generated before the resource owner changed are retained in the old accounts and projects, and new fees will be charged for the new accounts and project after the resource owner changed.

Pricing List Notice

- A pricing list can be attached to more than one project or account. A project or an account can have only one pricing list attached.
- The Cloud provides a default pricing list, which cannot be deleted. When you upgrade the Cloud, a default pricing list will be automatically created and attached to all projects or accounts according to the previous billing setting.
- The default pricing list cannot be deleted.
- The pricing list that is being used by a project or an account cannot be deleted. To delete such a pricing list, change a pricing list for the associated project or account, and then delete the pricing list.
- Changes of public IP addresses are incurred only after QoS is set.
- Currently, virtual IP addresses of the IPv6 type cannot be billed.
- Pricing List lets you bill root volumes or data volumes according to disk performances via advanced parameters. The configuration metrics rely on **`priceUserConfig`** in the advanced parameters of an instance offering or disk offering. Make sure all configurations are strictly consistent. Otherwise, a pricing list cannot be generated.
- When you delete a pricing history whose end date is the current date, the pricing records will also be deleted. Meanwhile, the corresponding bills will be generated immediately, and no more fees will be incurred any longer.
- When you delete a pricing history whose end date is not the current date, only the pricing records will be deleted. The billing and bills are not affected.

12.2 Tag

With Tag, you can create tags for resources as needed, and quickly locate the required resources according to the tag type and tag name.

- You can create tags with different colors, simple style, and brief language. You can also bind 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 (admins or platform admins), and can be bound to VM instances, volumes, hosts, and bare metal instances.
  - Tenant tags are created and owned by tenants (regular accounts or projects), and can be bound to VM instances and volumes.
- Currently, you can bind tags to or unbind tags from VM instances, volumes, hosts, and bare metal instances.

Notice

- Admin tags are created and owned by administrators (admins or platform admins), while tenant tags are created and owned by tenants (regular accounts or projects).
- Tags created by tenants can only be bound to resources of the corresponding tenants, while admin tags can be bound to all of your resources.
- Administrators can unbind or delete tenant tags.
- Tags in a project are owned by the project. Therefore, all members, including the head of project, 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 bound to the resource will be unbound. 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.
- When you create a tag, the naming convention must satisfy the following rules:
  - The length of the tag name cannot exceed 20 characters.
  - The tag name is case-sensitive.
  - Tags are unique. The same roles can have only one tag with the same name and color.
- When you attach a tag, note the following:

- One resource can bind 50 tags at most, while a single tag can bind the unlimited number of resources.
- Many-to-many bindings between tags and resources are supported. That is, you can bind multiple tags to multiple resources.
- Tags that were created by a tenant can only be bound to resources owned by the tenant, while admin tags can be bound to all resources.
- An administrator can unbind or delete tenant tags.
- Resource tags can be sorted in order according to the creation time or tag names (priority: characters > numbers > Chinese characters > English characters). To change the sort order, choose **Settings** > **Global Settings** > **Advanced**, locate **Tag sorting field**, and click the Edit icon. By default, the tags are sorted in order by the tag name.

- When you detach a tag, note the following:
  - Multiple tags on a single resource can be unbound simultaneously. In addition, multiple resources on a single tag can also be unbound simultaneously.
  - A tenant can only unbind tags from the resources owned by the tenant itself, while an administrator can unbind tags from all resources.

12.3 Application Center

Application Center provides enhanced functionality and fast access to various third-party applications. You can add the URLs of different third-party applications for centralized management and quick access.

12.4 Email Server

ZStack provides the ZWatch feature. If you select an email as the endpoint when you use ZWatch, you need to set the email server to receive alarm emails.

Notice

- From ZStack 3.3.0, you can set the AD/LDAP or email server connection timeout as needed. Method:

  Go to `/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`, and set the following parameters in the **zstack.properties** configuration file:

  - ```
    Ldap.addServer.connectTimeout = XX
    ```
    ```

```
# Set the AD/LDAP connection timeout.
```

- ```
  SNS.addEmailPlatform.connectTimeout = XX
  # Set the email server connection timeout.
  ```
- ```
  SNS.addEmailPlatform.readTimeout = XX
  # Set the data read timeout for an email server.
  ```

Note:

- By default, the timeout value of the preceding three parameters is 5000. Unit: ms.
- If you need to modify the timeout, run the **`zstack-ctl configure`** command. For example,

  ```
  [root@localhost ~]# zstack-ctl configure Ldap.addServer.
  connectTimeout = 10000
  [root@localhost ~]# zstack-ctl configure SNS.addEmailPlatform.
  connectTimeout = 10000
  [root@localhost ~]# zstack-ctl configure SNS.addEmailPlatform.
  readTimeout = 10000
  ```

  After the settings are completed, restart the management node by running the `zstack-ctl restart_node` command to take effect.

12.5 Log Server

ZStack allows you to add a log server to the cloud. With the log server, you can collect management node logs and quickly locate problems, thereby improving the cloud O&M efficiency.

Notice

- To normally receive log information, ensure that the configurations between the log level and the log server are completely consistent.
- Enter related information as needed. If you have any problem, contact related log service providers.

12.6 Console Proxy

The Platform Management feature of ZStack displays the current console proxy information, that is, the information about the proxy you use when you open the console of your VM instance.

- You need to modify the console proxy address only in the management node.
- The default proxy address is the IP address of the management node.
- The displayed type is ManagementServerConsoleProxy.

- You can open the console of a VM instance only when the state of the console proxy is **Enabled** and the status is **Connected**.

You can perform the following operations on a console proxy:

- **Reconnect:** You can reconnect the console proxy if the console of a VM instance fails to be opened. After reconnection, you can open the console again when the proxy state is Enabled and the proxy status is Connected.
- **Set the console proxy address:** ZStack allows you to set the console proxy address on the UI.
  - The console proxy address can either be the public IP address, the NAT address, or the domain name of a management node. Port settings are not supported.
  - The setting takes effect immediately without a need to restart the management node.

12.7 IP Blacklist/Whitelist

ZStack allows you to configure a blacklist or whitelist for login IP addresses to protect your cloud. You can configure a blacklist or whitelist as needed to identify and filter the identities of those who access your cloud, thereby enhancing the access control and security of your cloud.

To use the IP Blacklist/Whitelist feature, go to **Settings** > **Global Settings** > **Advanced**, locate **IP Blacklist/Whitelist**, and change the value to **true**.

Notice

The implementation mechanism of IP blacklist and whitelist is as follows:

- By default, if no IP blacklist or whitelist is added, the access requests from all IP addresses are allowed.
- If only an IP blacklist is added, the access requests from all IP addresses in the blacklist are denied, while the access requests from IP addresses outside of the blacklist are allowed.
- If only an IP whitelist is added, the access requests from both IP addresses in and outside of the whitelist are allowed.
- If both an IP blacklist and an IP whitelist are added, the whitelist takes precedence over the blacklist. For example, if an IP address is added to a blacklist and a whitelist at the same time, the access requests from the IP address will be allowed.

12.8 MN Monitoring

The Management Node Monitoring (MN Monitoring) feature allows you to view the health status of each management node in a multi-management node environment.

The MN Monitoring feature displays the management IP address, node status, VIP, and management service status of different management nodes. The management service includes:

- Whether monitor IP is reachable

  Checks whether the monitor IP address of the active and standby management nodes is reachable. If unreachable, the high availability feature of the management node might be invalid.
- Whether peer management node is reachable

  Checks whether the standby management node is reachable. If unreachable, the standby management node cannot be communicated.
- Whether VIP is reachable

  Checks whether the VIP is reachable. If unreachable, the active management node cannot access the UI through the VIP.
- Database status

  Monitors the status of the database. If the database is abnormal or the databases of multiple management nodes are not synchronized, the data might be lost. We recommend that you troubleshot this issue as soon as possible.

Notice

- The management node area includes three colors: green, red, and gray. Green indicates that the management node or related information is normal. Red and gray indicate that the management node or the related information is abnormal. If red or gray is displayed, perform troubleshooting as soon as possible.
- The multi-management node environment uses the active-standby mode, and the environmen t has only one active management node. The active management node displays its VIP, while standby management nodes do not display their VIPs.
- If all standby management nodes are abnormal, after the active management node fails, services in the active management node cannot be switched to standby management nodes and the active management node is down. Therefore, if you find an exception in a management node, perform troubleshooting as soon as possible.

12.9 Certificate

The Certificate feature complies with the digital certificate protocol. Trusted certificate authorities (CAs) issue digital certificates after verifying the identity of a server. The issued certificates can verify server identities and encrypt data transmission.

Currently, the Certificate feature is only applied to load balancing services. If you use HTTPS for your load balancing listener, you need to bind a certificate.

- Prepare a certificate in advance. You can use relevant tools to generate a self-signed certificat e or purchase a certificate issued by a CA.
- Upload the prepared certificate to the Cloud. Note that both certificates and certificate chains can be uploaded.
- Note that the load balancing service supports only PEM certificates. Before you upload a certificate, make sure that the certificate, private key, and certificate chain meet the format requirements.

Certificate Operations

- Change name and description: Change the name and description of a certificate.
- Delete: Delete a certificate. If the certificate is bound with one or more listeners, deleting the certificate will also unbind it from the listeners.
- Unbind certificate: Unbind a certificate from a listener.

12.10 Access Key Management

An AccessKey can either be a local AccessKey or a third-party AccessKey.

- In ZStack Private Cloud , a local AccessKey (which contains an AccessKey ID and an AccessKey Secret) is a security credential authorized by the Cloud to third-party users. With the authorized AccessKey, third-party users can access cloud resources by calling ZStack Private Cloud APIs. We recommend that you keep your AccessKey confidential to maintain securities.
- A third-party AccessKey (which contains an AccessKey ID and an AccessKey Secret) is a security credential authorized by third-party users to the Cloud. With the authorized AccessKey , the Cloud can access cloud resources of the third-party users by calling APIs. Third-party AccessKey must also be kept confidential to maintain security.

AccessKey is a key factor for ZStack Private Cloud to perform security authentication on API requests. We recommend that you keep your AccessKey confidential to maintain securities. If your AccessKey is at risk of leakage, we recommend that you delete it in time and create a new one.

Notice

- Admins and platform admins can create multiple AccessKeys, while the tenants (normal accounts and project members) can create only two AccessKeys.
- Admins and platform admins can enable, disable, or delete AccessKeys created by themselves and those created by tenants at any time.
- Tenants can enable, disable, or delete AccessKeys created by themselves at any time.
- An AccessKey has all permissions of the person who created it.

13 Advanced Function (Plus)

ZStack provides the following advanced functions:

- Enterprise Management
- BareMetal Management
- Backup Service
- Migration Service

Advanced functions are provided as separate feature modules. To use an advanced function, purchase both the Base License and the corresponding Plus License. The Plus License cannot be used independently

13.1 Enterprise Management

Enterprise Management mainly provides enterprise users with organization structure management s and project-based resource access control, ticket management, and independent zone management. Enterprise Management is a separate feature module. To use this feature, purchase both the Base License and the Plus License of Enterprise Management. The Plus License cannot be used independently.

Enterprise Management Account System

The following are the related definitions:

- **Admin**

  A super administrator who owns all permissions. Usually, IT system administrators obtain the permissions.
- **User**

  A virtual ID, simply a natural person who is the most basic unit in Enterprise Management . A user has multiple attributes, such as a platform admin, project admin, and head of a department.
- **Local User**

  A user that is created in the Cloud. A local user can be added to an organization, added to a project, bound with a role.
- **3rd Party User**

A user is that is synchronized to the Cloud through 3rd party authentication. A 3rd party user can be added to an organization, added to a project, and bound with a role.

- **Platform User**

  A user that is not added to a project yet, including platform admin and the regular platform member.

- **Platform Admin**

  A user that has the platform admin role attached. A platform admin who has been allocated a specified zone or all zones manages the data center of the allocated zone or zones.

- **Head of Department**

  A user that is responsible for managing departments in an organizational structure. A head of a department has the permission to check department bills.

- **Project Member**

  A user who has joined a project, including project admin, project operator, and normal project member.

- **Project Admin**

  A user that has the project admin role attached. A project admin is responsible for managing users in a project, and has the highest permission in a project.

- **Project Operator**

  A user that has the project operator role attached. A project operator assists project admins to manage projects. One or more project members in the same project can be specified to act as project operators.

- **Member Group**

  A virtual ID group that has a group of project members. You can organize project members in groups for better management, and perform permission control by member group.

- **Organization**

  The basic unit of an organizational structure in Enterprise Management. You can create an organization or synchronize an organization through 3rd party authentication. An organization can be divided into a top-level department and a normal department. The top-level department is the first-level department in the organization, and can have multi-level subsidiary department s.

- **Project**

The task that related members will be specified to accomplish specified targets with a specified time, resource, and budget. Enterprise Management organizes resources based on projects and allows you to create an independent resource pool for a specific project.

- **Role**

  A collection of permissions. You can grant permissions to a user by attaching a role to the user , so that the user can operate on the related resources by calling related APIs.

- **System Role**

  A special role preconfigured by the Cloud. As the Cloud upgrades, the permission contents of a system role will be updated, and new permissions will be added automatically. The system role cannot be configured manually.

- **Custom Role**

  A custom role that you created in the Cloud. Similar to the system role, the permission contents of a custom role will be updated as the Cloud upgrades. Notice that you need to manually configure the additional permissions after the upgrade.

- **Quota**

  A measurement standard that determines the total quantity of resources for a project. A quota mainly includes the VM instance count, CPU count, memory capacity, maximum number of data volumes, and maximum capacity of all volumes.

- **Project Collection Policy**

  When you create a project, specify a project collection policy. The project collection policy includes the unlimited collection, specified time collection, and specified spending collection.

  - Unlimited Collection

    After you create a project, resources within the project will be in the enabled state by default .

  - Specified Time Collection

    - When the expiration date for a project is less than 14 days, the smart operation assistant will prompt you for **The license will be expired** after a project member logs in to the Cloud.
    - After the project expired, resources within the project will be collected according to the specified policy. The policy includes disabling login, stopping resources, and deleting projects.

- Specified Spending Collection

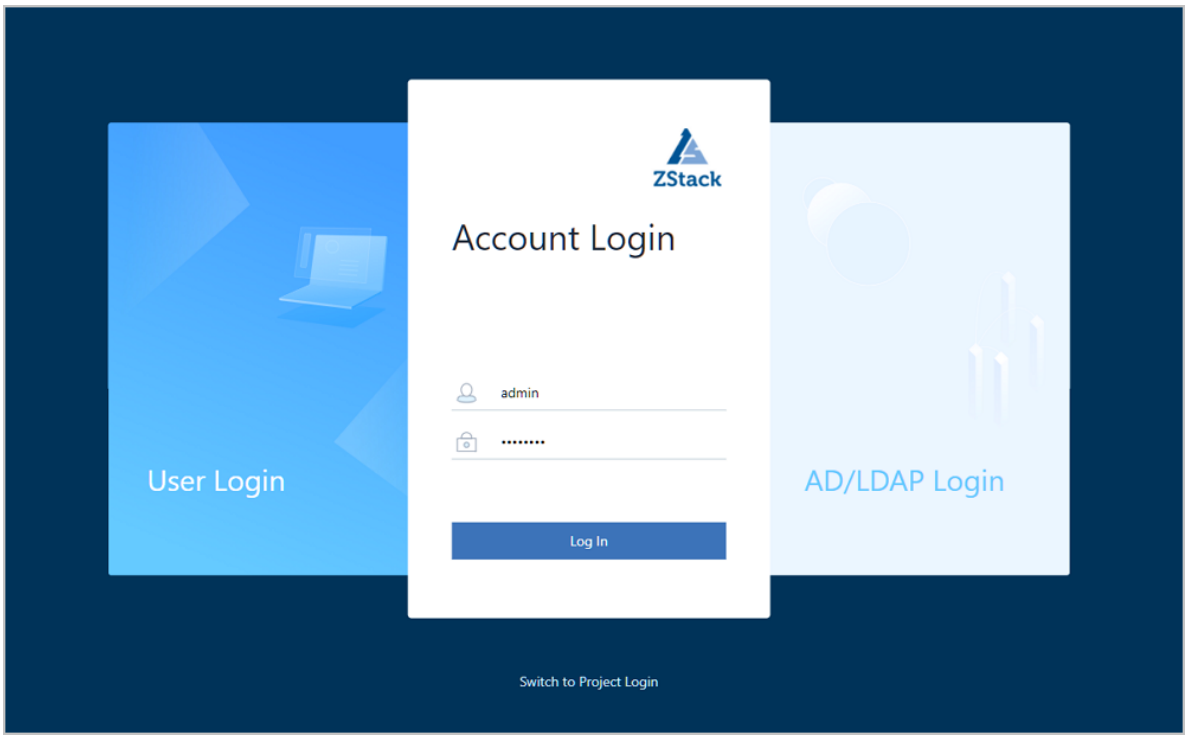
  When the project spending reaches the maximum limit, resources within the project will be collected according to the specified policy. The policy includes disabling login, stopping resources, and deleting projects.

Account Login in Enterprise Management

- Admins can log in to the Cloud via Main Login.

  By using Chrome or Firefox, go to the Main Login page via *http://your_machine_ip:5000/#/login* . To log in to the Cloud, the admin must enter the corresponding user name and password, as shown in *Main Login Page*.

  Figure 13-1: Main Login Page



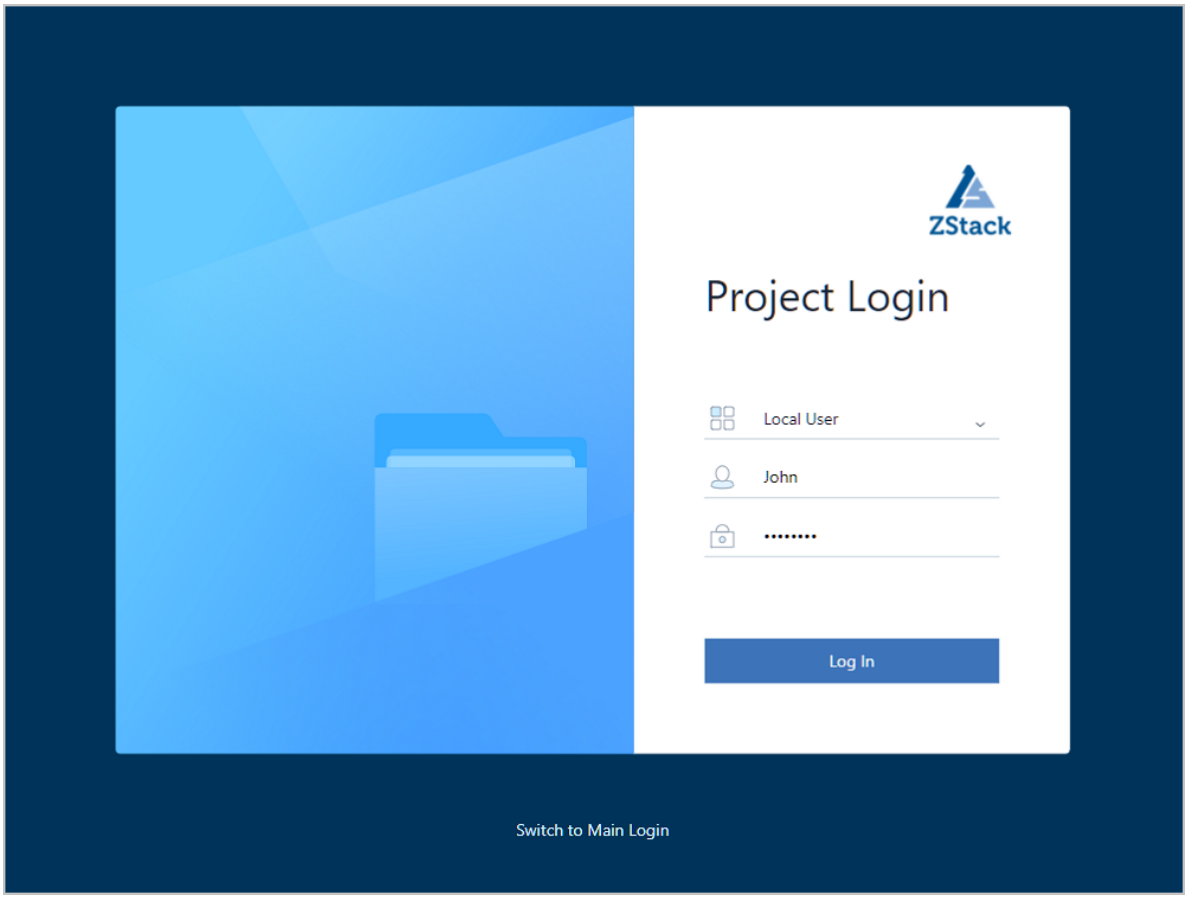
- For users (platform admin, platform user, project admin, project operator, or regular project member), log in to the Cloud via Project Login.

  By using Chrome or Firefox, go to the Project Login page via *http://your_machine_ip:5000/#/project*. To log in to the Cloud, enter the corresponding user name and password. Specifically, the Cloud has two login entrances for Project Login as follows:

  - Local user: the user created on the Cloud. Log in to the Cloud via Local User.

- AD/LDAP user: the 3rd party user synchronized to the Cloud via the 3rd party authentication. Log in to the Cloud via AD/LDAP User, as shown in *Project Login Page*.

Figure 13-2: Project Login Page



Three Subfeatures of Enterprise Management

The Enterprise Management mainly includes four subfeatures, including **project management**, **ticket management**, **independent zone management**, and **third-party authentication**

- **Project Management**:

  The project management is project-oriented to plan for resources. Specifically, you can create an independent resource pool for a specific project. Project lifecycles can be managed (including determining time, quotas, and permissions) to improve cloud resource utilizations at granular, automatic level and strengthen mutual collaborations between project members.

  For more information, see *Project Management*.

- **Ticket Management**:

To better provide basic resources efficiently for each project, project members (project admins , project operators, or regular project members) can apply for tickets to obtain cloud resources . Tickets are reviewed and approved according to custom ticket review processes of each project. Finally, admins or project admins approve the tickets. Currently, five types of ticket are available, including applying for VM instances, deleting VM instances, modifying VM configurat ions, modifying project cycles, and modifying project quotas.

For more information, see *Ticket Management*.

- **Platform Management**:

  To effectively manage the Cloud, the platform user (platform admin/regular platform member) can cooperate with the super administrator to manage and operate the Cloud together. ZStack provides various system roles such as Platform Admin Role and Dashboard Role. Also, you can satisfy various usage scenarios by creating custom roles at the API level.

  For more information, see *Platform Management*.

- **Independent Zone Management**:

  Usually, a zone corresponds to an actual data center in a place. If you isolated resources for zones, you can specify the corresponding zone admins for each zone to achieve independen t managements of various machine rooms. In addition, admins can inspect and manage all zones.

  For more information, see *Independent Zone Management*.

- **3rd Party Authentication**:

  The 3rd party authentication is a third-party authentication service provided by ZStack. ZStack lets you seamlessly access the third-party login authentication system. The corresponding account system can directly log in to the Cloud to conveniently use cloud resources. Currently, you can add an AD/LDAP server.

  For more information, see *3rd Party Authentication*.

13.1.1 Organization

Enterprise Management provides an organization management feature for enterprise users, where an organizational structure tree is displayed in cascade and you can directly get a complete picture of the enterprise organization structure. Enterprise Management mainly includes the following concepts:

- **Organization**

The basic unit of an organizational structure in Enterprise Management. You can create an organization or synchronize an organization through 3rd party authentication. An organization can be divided into a top-level department and a normal department. The top-level department is the first-level department in the organization, and can have multi-level subsidiary department s.

- **User**

  A virtual ID, simply a natural person who is the most basic unit in Enterprise Management . A user has multiple attributes, such as a platform admin, project admin, and head of a department.

- **Head of Department**

  A user that is responsible for managing departments in an organizational structure. A head of a department has the permission to check department bills.

Organization Tree

- The organization tree is displayed in hierarchy and allows you to view the whole picture of the enterprise structure.
- The organization can be divided into top-level department and department. Specifically, the top -level department, the first level department, can have multi-level departments.
- In the organization tree, the head of department for the top-level department or department has a red star icon at the lower right.
- The organization synchronized via the 3rd authentication lets you create an organization tree independently.
- You can add multiple organization trees. Notice that the users under the different organization trees are invisible from each other.
- The admin or platform admin can view all the organization trees, while the platform users can only view their own organization trees.

Organization Operations

An organization includes two types of add method: manual addition and 3rd party authentication. Organizations of different add methods support different operations.

Operations Supported by Cloud Organization

An admin, platform admin, or regular platform user can perform the following operations for an organization in the Cloud:

- Add organization: Create an organization tree.
- Change parent department: Change the parent department for the organization. Notice that the top-level department does not support this operation.
- Change department head: Respecify the head of department.
- Create subsidiary department: Create a subsidiary department under the organization.
- Delete subsidiary department: Delete the subsidiary department under the organization. Notice that the organization without any subsidiary department does not support this operation.
- Add user: Add a new user to the organization.
- Remove user: Remove a user from the organization.

> **Note:**
> If the user is the head of department, removing this user will also remove its identification as the head of department.

- Delete: Delete the specified organization.

> **Note:**
> Exercise caution. Deleting an organization will also delete all its subsidiary departments.

3rd Party Authentication Synchronization Operations

An admin, platform admin, or regular platform user can perform the following operations for the synchronized 3rd party organization:

- Add user: Add a new user to the organization.
- Remove user: Remove a user from the organization.

> **Note:**
> If the user is the head of department, removing this user will also remove its identification as the head of department.

- Delete: Delete the specified organization. Deleting the specified organization will also delete the 3rd party server. Notice that this organization cannot be deleted independently.

Notice

The visibility of the organization tree is different from different angles as follows:

- An admin or platform admin can view all organization trees.

- A regular palindrome user, project admin, or project operator can only view its own organization tree.
- A regular project member cannot view the organization tree.

13.1.2 User

A user (virtual ID) is simply a natural person who is the most basic unit in Enterprise Management . A user has multiple attributes, such as a platform admin, project admin, and head of a department.

ZStack provides the following two types of user classification:

- Classification by source

  — **Local User**

  A user that is created in the Cloud. A local user can be added to an organization, added to a project, bound with a role.

  — **3rd Party User**

  A user is that is synchronized to the Cloud through 3rd party authentication. A 3rd party user can be added to an organization, added to a project, and bound with a role.

  Note:
  Users in Enterprise Management can log in to the Cloud via Project Login, while local users can log in to the Cloud via User Login. Besides, third-party users can log in to the Cloud via AD/LDAP User.

- Classification by project

  — **Platform User**

  A user that is not added to a project yet, including platform admin and the regular platform member.

  — **Project Member**

  A user who has joined a project, including project admin, project operator, and normal project member.

Notice

- An admin or platform admin can view a list of all users.

- If an organization tree is created in the Cloud, a platform user can only view the user list of its own organization. If no organization tree is created in the Cloud, a platform user can view all users.
- If an organization tree is created in the Cloud, a project admin or project operator can only view the users under its own organization tree.
- If no organization tree is created in the Cloud, a project admin or project operator can view all users.
- To create users with a template, note the following:
  - Existing organizations are required. Notice that these organizations must be separated by **"/"**, such as *Company/Dev*.
  - If the organization path duplicates, attach the UUID of a top-level department, such as *Company(f11444d42701483791370e9f8b9300b9)/Dev*.
  - If a user is added to multiple organizations simultaneously, separate these organizations by "&&", such as *Company/Dev&&Company/QA*.
  - A project is required. When a single project is added, enter the project name directly, such as *project-01*.
  - If a user is added to multiple projects simultaneously, separate these projects by "&&", such as *project-01&&project-02*.

User Operations

Operations between a local user and a 3rd party user are little bit different.

Local User Operations

An admin, platform admin, or regular platform user supports the following operations for a local user:

- Create user: Create a local user based on the basic employee information.
- Change user name: Change the user name. The user name that is the login name must be unique.
- Change password: Change the login password for the local user.
- Change personal information: Change the full name, phone number, email address, and identifier.
- Join department: Add the local user to one or more departments.
- Remove from department: Remove the local user from the department.

Note:

If the local user is the head of department, removing this local user from the department will also remove its identification as the head of department.

- Join project: Add the local user to one or more projects.
- Remove from project: Remove the local user from the project.

Note:

- If the local user is the project admin or project operator, removing the local user from the project will also remove its identification as the project admin or project operator.
- If the local user is part of a ticket process, the ticket process will be unavailable after you remove the local user from the project. Also, the tickets related to the process will be all recalled.

- Delete: Delete the local user.

Note:

- If you delete the local user that acts as the head of department, project admin, or project operator, deleting the local user will also delete its identification as the head of department, project admin, or project operator
- If you delete the local user that is part of ticker process, the ticket process will be unavailabl e after you remove the local user from the project. Also, the tickets related to the ticket process will be all recalled.

- Audit: Check the related operations of the local user. These operations are performed by the admin or platform admin.

3rd Party User Operations

An admin, platform admin, or regular platform user support the following operations for a 3rd party user:

- Join department: Add the 3rd party user to one or more departments.
- Remove from department: Remove the 3rd party user from the department to be selected.

Note:

If the 3rd party user is the head of department, removing the 3rd party user from the project will also remove its identification as the head of department.

- Join project: Add the 3rd party user to one or more projects.
- Remove from project: Remove the 3rd party user from the project.

Note:

- If the 3rd party user is the project admin or project operator, removing the 3rd party user from the project will also remove its identification as the project admin or project operator.
- If the 3rd party user is part of ticket process, the ticket process will be unavailable after you remove the 3rd party user from the project. Also, the tickets related to the ticket process will be all recalled.

- Delete: Delete the 3rd party user.

Note:

- If you delete the 3rd party user that acts as the head of department, project admin, or project operator, removing the 3rd party user will also remove its identification as the head of department, project admin, or project operator.
- If you delete the 3rd party user that is part of a ticket process, the ticket process will be unavailable after you remove the 3rd party user from the project. Also, the tickets related to the ticket process will be all recalled.

- Convert to local user: After you synchronize an AD server, the non-existent 3rd party user will be changed to the deleted state and cannot log to the Cloud. At this time, the 3rd party user can be converted to a local user, while the AD user that is in the deleted state can be changed to the local user in the Cloud.

Note:

- After you convert a 3rd party user to a local user, the original data of the 3rd party user will be inherited, such as the belonged project and the acquired permissions.
- After you convert a 3rd party user to a local user, verify that you perform **Change Password**. Then, the converted local user can log in to the Cloud normally.

13.1.3 Role

A role is a collection of permissions used for entitling users to manage resources by calling associated APIs. A role has two types, including system role and custom role.

- **System Role**

A special role preconfigured by the Cloud. As the Cloud upgrades, the permission contents of a system role will be updated, and new permissions will be added automatically. The system role cannot be configured manually.

- **Custom Role**

  A custom role that you created in the Cloud. Similar to the system role, the permission contents of a custom role will be updated as the Cloud upgrades. Notice that you need to manually configure the additional permissions after the upgrade.

The role page includes two tab pages: system role and custom role. Specifically, the system role includes the following:

- Dashboard role:

  After you bind the dashboard role, the dashboard user can only have the permission of the monitoring dashboard. Once you log in to the Cloud, you will go to the dashboard page.

  - The dashboard user does not have the user home page. This user cannot change the password by its own. Notice that only the admin, platform admin, or regular platform user can change the password for the dashboard user.
  - The default language and the theme of the dashboard are consistent with the current configurations of the Cloud. Notice that only the admin, platform admin, or regular platform user can change these configurations for the dashboard user.
  - After the dashboard user logs in to the Cloud, closing the Web browser will still keep the user logging in. If the user wants to log out, access *http://management node_ip:port/#/login* and then perform the logout operation, such as http://172.20.11.50:5000/#/login.
- Platform admin role:

  After you bind the platform admin role, the platform admin can act as the platform administrator. The platform admin has the zone attribute, and manipulates the data center of the zone that is allocated to the platform admin.

  - The newly created platform admin defaults to manipulate all zones before zones are allocated.
  - After one or more zones are assigned to the platform admin, this platform admin can only manipulate the assigned zones.
  - One platform admin can manipulate multiple zones while one zone can be manipulated by multiple platform admins.

  - The platform admin needs to log in to the Cloud via Project Login.
- Project admin role:

  After you bind the project admin role, the project admin can act as the project administrator. The same project can only be assigned to one project admin. Notice that the project admin role can be changed.
- Project operator role:

  After you bind the project operator role, the project operator can act as the project manager who can assist the project admin to manage projects. One or more project members can act as the project operator within the same project.

Role Operations

An admin, platform admin, or regular platform user can perform the following operations for a role:

- Bind user: Bind a role to a user. By doing so, the user can own permissions of the related operations.
- Unbind user: Unbind the user from a role. By doing so, the related permissions owned by the user will be removed.
- Clone: Clone the role.
- Delete: Delete the role.

Note:

- Exercise caution. After you delete a role, the related user will automatically unbind this role , which will affect directly the normal usage of the related project members.
- The system role cannot be deleted.

Notice

- A role has two types: platform and project. The platform role can only be bound to the platform user, while the project role can only be bound to the project member of the project where the project role belongs.
  - The same user can only be bound to one type of role.
  - The same user can be bound to multiple same types of custom role.
  - The project member can only be bound to the custom role of the project where the project member belongs.

- The role is a collection of permissions base on resources. Dependencies exist among different types of role. We recommend that you use the predefined system role in the Cloud or select all roles.
- To remove roles, note the following:
  - After a role is removed, the user that binds this role can no longer own the related permissions.
  - Exercise caution. Dependencies exist among different types of role.

13.1.4 Project Management

Enterprise Management provides the project management feature for enterprise users.

Project management:

The project management is project-oriented to plan for resources. Specifically, you can create an independent resource pool for a specific project. Project lifecycles can be managed (including determining time, quotas, and permissions) to improve cloud resource utilizations at granular, automatic level and strengthen mutual collaborations between project members.

The project management mainly includes the following concepts:

- **Project**

  The task that related members will be specified to accomplish specified targets with a specified time, resource, and budget. Enterprise Management organizes resources based on projects and allows you to create an independent resource pool for a specific project.
- **Project Member**

  A user who has joined a project, including project admin, project operator, and normal project member.
- **Project Admin**

  A user that has the project admin role attached. A project admin is responsible for managing users in a project, and has the highest permission in a project.
- **Project Operator**

  A user that has the project operator role attached. A project operator assists project admins to manage projects. One or more project members in the same project can be specified to act as project operators.
- **Member Group**

A virtual ID group that has a group of project members. You can organize project members in groups for better management, and perform permission control by member group.

- **Role**

  A collection of permissions. You can grant permissions to a user by attaching a role to the user , so that the user can operate on the related resources by calling related APIs.

- **Quota**

  A measurement standard that determines the total quantity of resources for a project. A quota mainly includes the VM instance count, CPU count, memory capacity, maximum number of data volumes, and maximum capacity of all volumes.

- **Project Collection Policy**

  When you create a project, specify a project collection policy. The project collection policy includes the unlimited collection, specified time collection, and specified spending collection.

  - Unlimited Collection

    After you create a project, resources within the project will be in the enabled state by default .

  - Specified Time Collection

    - When the expiration date for a project is less than 14 days, the smart operation assistant will prompt you for **The license will be expired** after a project member logs in to the Cloud.
    - After the project expired, resources within the project will be collected according to the specified policy. The policy includes disabling login, stopping resources, and deleting projects.

  - Specified Spending Collection

    When the project spending reaches the maximum limit, resources within the project will be collected according to the specified policy. The policy includes disabling login, stopping resources, and deleting projects.

Project Operations

An admin, platform admin, or regular platform user can perform the following operations for a project:

- Create project: Create a project.
- Change project cycle: Change the project cycle of the project via the project details page.

Note:

- The project cycle can be changed to Unlimited, Job Scheduling Recovery, or Billing Recovery.
- If the project is specified as Billing Recovery, the billing quota must be larger than the total of the currently real-time billing.

- Change project quota: Change the project quota via the quota tab page.
- Change project admin: Change the project admin.
- Enable project: Enable the project that is in the stopped state. By doing so, you can log in to the project normally.
- Disable project: Disable the project that is in the enabled state. The project will disable any login. However, the related resources within the project can still work normally.
- Change pricing list: Change the pricing list for the project, and use this pricing list to bill your resources.
- Generate project template: Generate a project template by using an existing project. When you create the project, you can configure your project by using the quota defined by the project template.
- Add member: Add members to the project.
- Remove member: Remove project members from the project.

Note:

- If the project member is the project admin or project operator, removing the project member from the project will also remove its identification as the project admin or project operator.
- If the project member is part of a ticket process, the ticket process will be unavailable after you remove the project member from the project. Also, the tickets related to the process will be all recalled.

- Stop project resource: Exercise caution. Stopping the project resources will stop all VM instances and routers within the project, but the project can still work normally.
- Recover expired project: Recover an expired project. After you recover the expired project, you can still log in to the project, and the related resources within the project work normally.
- Attach organization: After the project is attached to a department, you can view the department bills.

- Detach organization: Detach the project from the department. Besides, the project bills will be removed from the department bills.
- Delete: Delete the project. After the project is deleted, the project will be placed in the deleted state and will disable any login. Besides, the related resources within the project will be stopped.
- Restore: Restore the project that is in the deleted state to the available state. Make sure that you specify the project cycle.
- Expunge: Expunge the project that is in the deleted state. Besides, the related resources within the project will be placed in the deleted state and belong to the admin.

Project Template Operations

An admin, platform admin, or regular platform user can perform the following operations for a project template:

- Create project template: Create either a project template by customizing quotas or generate a project template by using the existing project.
- Change name and description: Change the name and description for the project template.
- Change quota: Change the project template quota via the quota details page.
- Delete: Delete the project template.
- Audit: Check the related operations of the project template. These operations are performed by the admin or platform admin.

For more information, see .

13.1.5 Ticket Management

The Enterprise Management provides the ticket management feature for enterprise users.

Ticket Management:

To better provide basic resources efficiently for each project, project members (project admins , project operators, or regular project members) can apply for tickets to obtain cloud resources. Tickets are reviewed and approved according to custom ticket review processes of each project. Finally, admins or project admins approve the tickets. Currently, five types of ticket are available , including applying for VM instances, deleting VM instances, modifying VM configurations, modifying project cycles, and modifying project quotas.

Ticket Process Management

ZStack lets you customize ticket processes. With Process Management, an admin, platform admin, or regular platform user can create different types of ticket process for different projects.

ZStack mainly includes the following several types of ticket process:

- Default process: Project member submits a ticket>admin approves the ticket. This process applies to the following scenarios:
  - The tickets that are not configured with a ticket process will use the default ticket process.
  - The tickets whose project cycle has been modified will use the default ticket process.
  - The tickets whose project quota has been modified will use the default ticket process.
  - If the custom ticket process is deleted, the tickets will be resubmitted automatically via the default ticket process.
- Custom process: Project member submits a ticket>the ticket is approved with your customization>admin or project admin approves the ticket. This process applies to the following scenarios:
  - The tickets with the types of applying for VM instances, deleting VM instances, and changing VM configurations will be prioritized to be submitted via the configured, custom ticket process.
  - If you modify the valid ticket process, the tickets will be automatically resubmitted via this modified, custom ticket process.
  - If you modify the invalid ticket process, resubmit the tickets manually by using this modified, custom ticket process.

Note:

- The same ticket process can use multiple ticket types, including applying for VM instances, deleting VM instances, and changing VM configurations.
- The ticket process with the same type can only correspond to one ticket process.
- In terms of the deployment, the differences among different responsible persons are as follows:
  - When an admin is responsible for the Publish flow, add an additional flow in your custom ticket process. When a project admin is responsible for the Publish flow, you can choose not to add an additional flow in your custom ticket process.

- For the tickets with the type of applying for VM instances, the admin will approve the tickets, and then deploy the VM instances. The admin can make advanced settings by selecting **Advanced Deploy**. When the project admin approves the tickets and deploy the VM instances, the project admin cannot make the advanced settings.

- To change the ticket process, note the following:
  - If you modify the valid ticket process, the tickets will be automatically resubmitted via this modified, custom ticket process.
  - If you modify the invalid ticket process, resubmit the tickets manually by using this modified , custom ticket process.
  - Deleting a ticket type in the ticket process will delete the custom ticket process for this ticket type. After you modify the ticket process, the tickets will be automatically resubmitted via the default ticket process.
  - Adding ticket types for the ticket process will create a custom ticket process for this ticket type. After you modify the ticket process, the tickets will be resubmitted via this custom ticket process.

13.1.6 3rd Party Authentication

The 3rd party authentication is a third-party authentication service provided by ZStack. ZStack lets you seamlessly access the third-party login authentication system. With 3rd Party Authentication, the corresponding account system can directly log in to the Cloud to conveniently use cloud resources. Currently, you can add an AD/LDAP server.

- AD authentication:

  AD (Active Directory) is a directory service designed for Windows Standard Server, Windows Enterprise Server, and Windows Datacenter Server. AD provides an independent, standard login authentication system for increasingly diverse enterprise office applications.

  AD users or organizations can be synchronized to the ZStack user list or organization via an AD server, while specified AD login attributes can be used to directly log in to ZStack.

- LDAP authentication:

  LDAP (Lightweight Directory Access Protocol) can provide a standard directory service that offers an independent, standard login authentication system for increasingly diverse enterprise office applications.

LDAP users can be synchronized to the ZStack user list via an LDAP server, while specified LDAP login attributes can be used to directly log in to ZStack.

AD Server Operations

An admin, platform admin, or regular platform user can perform the following operations for an AD server and 3rd party users:

- On the 3rd party authentication page, you can perform the following operations:
  - **Test Connection**:

    Test the connection between the AD server and the Cloud. If the connection fails, troubleshoot this issue according to the following possible reasons:

    - The AD server IP or port authentication failed. Check whether the AD server is available, and whether the IP or port is changed.
    - The user DN or password connection failed. Use the latest authenticated user DN and password within the base DN.
  - **Modify Mapping Rule**:

    Modify the synchronized user mapping rule and the organization mapping rule.

    > **Note:**
    > The modified mapping rule will take effect when the AD server is synchronized next time. Verify that you manually select Synchronize or set Auto Synch for the next synchronization.
  - **Synchronize**:

    Synchronizing the AD server will obtain the latest user list and organizations.

    > **Note:**
    > After synchronization, the non-existent users will be placed in the deleted state and can no longer log in to the Cloud.
  - **Delete**:

    Delete the AD server.

    > **Note:**
    > If you delete an AD server, the users and organizations synchronized to the Cloud will also be deleted. However, the users and organizations in the source AD server are not affected.

- On the AD server details page, you can perform the following operations:
  - **Configuration**:

    Select the Configuration button. Afterwards, you can modify the base DN, user DN, password, and filter rule.

    Note:

    - Exercise caution. After the configuration information is modified, the AD server will be synchronized.
    - Modifying the configurations will take effect at the next synchronization for the AD server . Verify that you manually select Synchronize or set Auto Synch for the next synchroniz ation.
    - After synchronization, the non-existent users will be in the deleted state and can no longer log in to the Cloud.
  - **Auto Sync**:

    Select Auto Sync. After synchronization, you can specify the synchronization cycle and enable the auto synchronization.

    Note:

    - After you enable Auto Sync, you will obtain the latest user list and the organizations at schedule based on the synchronization cycle.
    - After synchronization, the non-existent users can be placed in the deleted state and can no longer log in to the Cloud.

LDAP Server Operations

An admin, platform admin, or regular platform user can perform the following operations for an LDAP server and 3rd party users:

- On the 3rd authentication page, you can perform the following operations:
  - **Test Connection**:

    Test the connection between the LDAP server and the Cloud. If the connection fails, troubleshoot this issue according to the following possible reasons:

    - The LDAP server IP or port authentication failed. Check whether the LDAP server is available, and whether the IP or port is changed.

- The user DN or password connection failed. Use the latest authenticated user DN and password within the base DN.

- **Modify Mapping Rule**:

  Modify the synchronized user mapping rule and the organization mapping rule.

  Note:
  The modified mapping rule will take effect when the LDAP server is synchronized next time. Verify that you manually select Synchronize or set Auto Synch for the next synchronization.

- **Synchronize**:

  Synchronizing the LDAD server will obtain the latest user list and organizations.

  Note:
  After synchronization, the non-existent users will be placed in the deleted state and can no longer log in to the Cloud.

- **Delete**:

  Delete the LDAD server.

  Note:
  If you delete an LDAD server, the users and organizations synchronized to the Cloud will also be deleted. However, the users and organizations in the source LDAD server are not affected.

- On the LDAD server details page, you can perform the following operations:

  - **Configuration**:

    Select the Configuration button. After configuration, you can modify the base DN, user DN, password, and filter rule.

    Note:

    - Exercise caution. After the configuration information is modified, the LDAD server will be synchronized.
    - Modifying the configurations will take effect at the next synchronization for the LDAD server. Verify that you manually select Synchronize or set Auto Synch for the next synchronization.

- After synchronization, the non-existent users will be in the deleted state and can no longer log in to the Cloud.

- **Auto Sync**:

  Select Auto Sync. After synchronization, you can specify the synchronization cycle and enable the auto synchronization.

  Note:

  - After you enable Auto Sync, you will obtain the latest user list and the organizations at schedule based on the synchronization cycle.
  - After synchronization, the non-existent users can be placed in the deleted state and can no longer log in to the Cloud.

13.2 Bare Metal Management

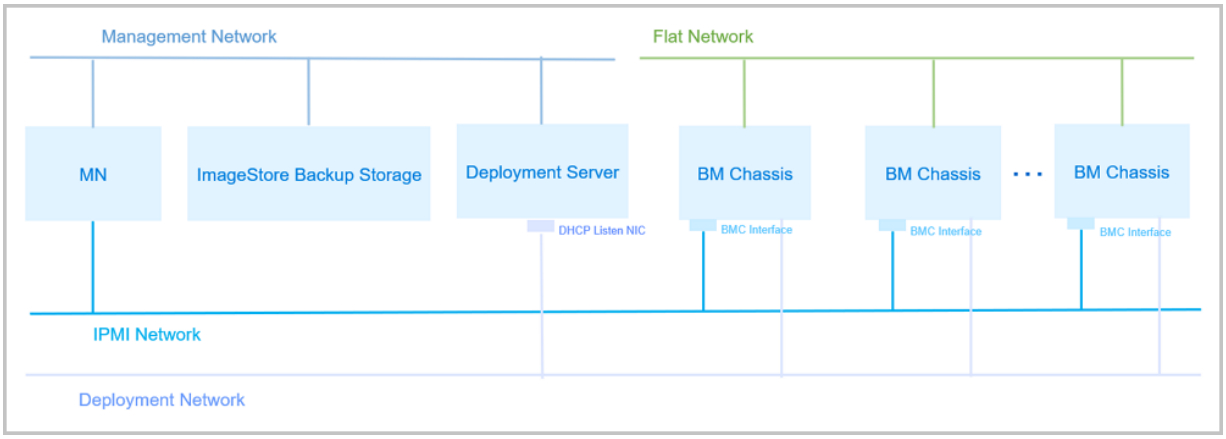
ZStack offers the BareMetal Management service that provides your applications with dedicated physical servers, ensuring the high performance and stability of your key applications. After your servers are configured well and the related preparations are completed, you can deploy Bare Metal (BM) chassis in bulk on the UI. After the deployment succeeds, you can use these BM chassis to create BM instances. With preconfigured templates, you can achieve unattended batch installation for BM instance operating systems. In addition, you can configure a business network for BM instances and easily manage the entire lifecycle of these BM instances.

The BareMetal Management service is a separate feature module. To use this service, purchase both the Base License and the Plus License of BareMetal Management. The Plus License cannot be used independently.

Basic Workflow

How does the BareMetal Management service work? A deployment server provides two types of service: DHCP and FTP. Specifically, the deployment server can instruct multiple BM chassis to be started through a PXE NIC, and can allocate dynamic IP addresses with the DHCP service. In addition, BM chassis can download related software packages from the deployment server with the FTP service, of whose packages can be applied to the operating system installation of the BM instance, as shown in *BareMetal Management Network Topology*.

Figure 13-3: BareMetal Management Network Topology



Key Features and Benefits

The BareMetal Management service provides the following features and benefits:

- Provides applications with dedicated physical servers to ensure the high performance and stability of your key applications.
- Deploy deployment servers independently as recommended, which can meet the requirements for the host high availability scenario of multiple management nodes. This also simplifies the network environment and helps to avoid DHCP conflicts. In addition, you can attach an independent deployment server to each BM cluster, which helps to avoid a single point of failure and improve greatly the deployment rate.
- Helps create BM chassis in bulk on the UI via either the manual creation or template file import. You can also add IPMI addresses in bulk to deploy efficiently BM clusters, which increases O&M efficiencies.
- Helps to quickly generate configuration files by using preconfigured templates to achieve unattended batch installation for BM instance operating systems.
- Enables you to customize the installation of your operating system. Supported operating systems: custom operating system of the Cloud and the mainstream Linux distributions (RHEL/CentOS, Debian/Ubuntu, and SUSE/openSUSE).
- Supports flat network. Specifically, BM instances and VM instances on the same L2 network can reach each other without routing to each other by gateways.

Typical Usage Scenarios

The BareMetal Management service can be applied to the following typical scenarios:

- High-Security and Strict Management Scenario

Financial industry, security industry, and others have rigorous standards for the business compliance and business data security. With the BareMetal Management service, they can ensure their exclusive use of resources, data isolation, strict supervision and control, and effective tracking.

- High-Performance Computing Scenario

  In high-performance computing scenarios, supercomputing centers, gene sequencing companies, and other entities require high computing performance, high stability, and accurate real-time update for servers. Sometime later, business performances will be affected by the performance loss and hyper-threading brought by visualization. In this regard, to deploy BM cluster to a certain scale, meet the strict requirements for the high performance computing.

- Key Database Scenario

  In some entities, some key database businesses cannot be deployed on normal VM instances, and must be loaded on the physical servers that can protect their exclusive resources, network isolation, and performances. To meet this requirements, use the BareMetal Management service that provides exclusive, high-performance physical servers for one or more appliances.

13.2.1 Bare Metal Cluster

A Bare Metal cluster provides independent cluster managements for Bare Metal chassis.

- To provide PXE services for Bare Metal instances on a Bare Metal cluster, the Bare Metal cluster must attach a deployment server.
- One Bare Metal cluster can only attach one deployment server, while one deployment server can attach multiple Bare Metal clusters simultaneously.
- To provide network services for Bare Metal instances on a Bare Metal cluster, the Bare Metal cluster must attach L2 networks.
- Flat networks are supported. Specifically, both Bare Metal instances and VM instances on the same L2 network can reach each other without routing via a gateway.

You can perform the following operations on a Bare Metal cluster:

- Create a Bare Metal cluster.
- View the details of the Bare Metal cluster.
- Enable or disable the Bare Metal cluster.
- Attach or detach an L2 network to the Bare Metal cluster.
- Attach or detach a deployment server from the Bare Metal cluster.

- Delete the Bare Metal cluster.

Notice

- One Bare Metal cluster can only attach one deployment server, while one deployment server can attach multiple Bare Metal clusters simultaneously.
- Flat networks are supported. Specifically, BM instances and VM instances on the same L2 network can reach each other without routing to each other by gateways.
- Exercise caution. Disabling a Bare Metal cluster will disable all Bare Metal devices on this Bare Metal cluster.
- Exercise caution. Detaching a deployment server from a Bare Metal cluster will cause the deploying Bare Metal instances to be expunged. In addition, after these Bare Metal instances are deployed, their consoles cannot be reached.
- Exercise caution. Deleting a Bare Metal cluster will delete all Bare Metal devices and Bare Metal instances on the Bare Metal cluster.

13.2.2 Deployment Server

A deployment server, known as PXE server, is an independently specified server used for providing PXE services and console proxy services for Bare Metal chassis.

- We recommend that you deploy PXE servers independently, thus satisfying the need of the multi-MN host HA scenario and avoiding a single point of failure (SPOF) to greatly improve deployment efficiencies.
- A deployment server must be attached to a BareMetal cluster.
- One Bare Metal cluster can only attach one deployment server, while one deployment server can attach multiple Bare Metal clusters simultaneously.
- A deployment server must have sufficient storage space to save images used for PXE deployments.
- A deployment server must connect to a management network for reaching management nodes.
- A deployment server must connect to a deployment network for reaching Bare Metal chassis.
- A DHCP listening NIC on a deployment server must connect to a deployment network. In addition, make sure that this deployment network does not contain other DHCP services for avoiding IP conflicts.
- A deployment server must install the latest ZStack Custom ISO with the recommended c76 version. Otherwise, this deployment server cannot provide software packages for Bare Metal chassis via the FTP service.

You can perform the following operations on a deployment server:

- Create a deployment server.
- View the details of the deployment server.
- Enable or disable the deployment server.
- Reconnect the deployment server.
- Attach or detach a Bare Metal cluster from the deployment server.
- Delete the deployment server.

Notice

- DHCP listening NICs must connect to the deployment network of Bare Metal chassis and have been configured with IP addresses.
- A DHCP listening NIC is an independent NIC with an IP address and provides a stable DHCP service.
- The deployment network where a DHCP listening NIC resides cannot contain any other DHCP services for avoiding IP conflicts.
- A deployment server must have sufficient storage space used for storing images to deploy PXE services.
- If a deployment server is disabled, the Bare Metal chassis on the corresponding cluster cannot obtain hardware information and cannot be used to create Bare Metal instances.
- One Bare Metal cluster can only attach one deployment server, while one deployment server can attach multiple Bare Metal clusters simultaneously.
- Exercise caution. Detaching a Bare Metal cluster from a deployment server will cause the deploying Bare Metal instances to be expunged. In addition, after these Bare Metal instances are deployed, their consoles cannot be reached.
- Exercise caution. Deleting a deployment server will cause the deploying Bare Metal instances to be expunged. In addition, after these Bare Metal instances are deployed, their consoles cannot be reached.

13.2.3 Bare Metal Chassis

A Bare Metal chassis can be used to create Bare Metal instances and can be universally identified via a BMC interface and IPMI configurations. With an IPMI network, a management node can control remotely powers of Bare Metal chassis, start networks, and enable disks. An administrator can complete deploying all Bare Metal chassis in bulk on the UI.

- A management node must connect to an IPMI network and control remotely Bare Metal chassis via IPMI.
- A Bare Metal chassis must contain a BMC interface, and configures an IPMI address, port, user name, and password, to connect to an IPMI network.
- A deployment server-enabled NIC on a Bare Metal chassis must connect to a deployment network.
- Other NICs of Bare Metal chassis can connect to the corresponding L2 networks as needed.

You can perform the following operations on a Bare Metal chassis:

- Add a Bare Metal chassis.
- View the details of the Bare Metal chassis.
- Enable or disable the Bare Metal chassis.
- Power on, power off, or power reset (reboot).
- Obtain hardware information.
- Open the console.
- Delete the Bare Metal chassis.

More Information

A Bare Metal chassis has three types of states or statuses: **Provision Status**, **State**, and **Power Status**.

Provision Status	Remarks
Unknown hardware information	The Bare Metal chassis cannot obtain the hardware information. **Note:** • Possible cause: When the Bare Metal chassis was added, you deselected **Reboot Bare Metal Chassis**. After completing adding the Bare Metal chassis, its provision status is unknown hardware information. • Solution: Manually **Power Reset** the Bare Metal chassis, or manually **Get Hardware Info**.

Provision Status	Remarks
PXE is rebooting	PXE servers instruct the Bare Metal chassis remotely to be enabled and assign IP addresses dynamically from PXE NICs.
Rebooting PXE failed	The Bare Metal chassis fails to be enabled from PXE NICs. **Note:** To address this problem, note the following: • Ensure that deployment servers cannot contain any other DHCP services in a deployment network. • Ensure that the NICs where the Bare Metal chassis connects to deployment networks have enabled PXE in BIOS. **Note:** • For a portion of Bare Metal chassis, ensure that this PXE NIC will be firstly booted. Or, ensure that (boot order) all NICs before this PXE NIC disable PXE. • Ensure that the boot mode for the Bare Metal chassis is Legacy.
Available	The Bare Metal chassis can be used to create Bare Metal instances, and enables you to install operating systems for the Bare Metal instances in a custom manner.
Provisioned	The Bare Metal chassis has been used to create Bare Metal instances.
Rebooting	The Bare Metal chassis is rebooting.

State	Power Status
• Enable	• Powered On

State	Power Status
• Disable	• Rebooting • Powered Off

13.2.4 Preconfigured Template

A preconfigured template can be used to quickly generate a preconfigured file to install Bare Metal instance operating systems in bulk without attended interferences.

- Make sure that you prepare well the preconfigured template in advance on the Cloud.
- A preconfigured template includes the following two types of templates:
  - System template: Is defaulted by the Cloud, including basic system variables, thereby satisfying a simple, unattended deployment scenario.
  - Custom template: Enable you to upload custom template files with the UTF8 format. Apart from basic system variables, you can customize other variables as needed to satisfy a complex, unattended deployment scenario.

You can perform the following operations on a preconfigured template:

- View the details of the preconfigured template.
- Download the preconfigured template.

You can perform the following operations on a custom template:

- Add a custom template.
- View the details of the custom template.
- Enable or disable the custom template.
- Download the custom template.
- Delete the custom template.

Notice

- To use a system template, note the following:
  - A system template keeps being in the enable state and disallows you to make any modificati on.
  - A system template includes basic system variables and is applied to a simple, unattended deployment scenario.

- Take system variables as an example. We recommend that you capitalize all variables and use underscore instead of hyphen. For example,

```
REPO_URL
# Use the installation source path created from the selected
 ISO image.
# Create comments as needed, and manually specify --url to
 other sources.
USERNAME
# Refer to the system user name.
# If the operating system is RHEL/CentOS or SUSE/openSUSE, the
 system user name defaults to root. You only need to specify a
 password.
# If the operating system is Debian or Ubuntu, enter a user
 name and a password as needed.

PASSWORD
# Refer to the password corresponding to the system user name.

NETWORK_CFGS
# Refer to both the NIC UUID and the network UUID that you
 entered on the UI.
# Replace the NIC UUID and the network UUID after executing
 distribution algorithms or specifying an IP address.

FORCE_INSTALL
# Whether to automatically overwrite the original data of the
 disk during deployment.

PRE_SCRIPTS
# Execute the script before deployment.

POST_SCRIPTS
# Execute the script after deployment.
```

— Different types of templates correspond to different syntax rules.

- For **kickstart** templates, for more information about the **kickstart** syntax rules, see *Red Hat Official Documentation*.
- For **preseed** template, for more information about the **preseed** syntax rules, see *Ubuntu Official Documentation*.
- For **autoyast** templates, for more information about the **autoyast** syntax rules, see *SUSE Official Documentation*.

• To use a custom template, note the following:

— Supported mainstream Linux distributions: RHEL/CentOS, Debian/Ubuntu, and SUSE/openSUSE.

— The template type must match the operating system that you selected. Otherwise, you cannot add the preconfigured template.

— The matching between template types and operating systems is recommended as follows:

- If you select a ZStack custom operating system, we recommend that you select the **kickstart** template.
- If you select the RHEL or CentOS operating system, we recommend that you select the **kickstart** template.
- If you select the Debian or Ubuntu operating system, we recommend that you select the **preseed** template.
- If you select the SUSE or openSUSE operating system, we recommend that you select the **autoyast** template.

— The custom template not only includes the basic system variables, but also enables you to customize your own variables, which is applied to a complex, unattended deployment scenario.

- Take system variables as an example. We recommend that you capitalize all variables and use underscore instead of hyphen. For example,

```
REPO_URL
# Use the installation source path created from the selected
 ISO image.
# Create comments as needed, and manually specify --url to
 other sources.
USERNAME
# Refer to the system user name.
# If the operating system is RHEL/CentOS or SUSE/openSUSE, the
 system user name defaults to root. You only need to specify a
 password.
# If the operating system is Debian or Ubuntu, enter a user
 name and a password as needed.

PASSWORD
# Refer to the password corresponding to the system user name.

NETWORK_CFGS
# Refer to both the NIC UUID and the network UUID that you
 entered on the UI.
# Replace the NIC UUID and the network UUID after executing
 distribution algorithms or specifying an IP address.

FORCE_INSTALL
# Whether to automatically overwrite the original data of the
 disk during deployment.

PRE_SCRIPTS
# Execute the script before deployment.

POST_SCRIPTS
```

```
# Execute the script after deployment.
```

- Take custom variables as an example. We recommend that you capitalize all variables and use underscore instead of hyphen. For example,

```
hostname
# Refer to the host name.

keyboard
# Refer to the keyboard.

timezone
# Refer to the time zone.
```

— Different types of templates correspond to different syntax rules.

- For **kickstart** templates, for more information about the **kickstart** syntax rules, see *Red Hat Official Documentation*.
- For **preseed** template, for more information about the **preseed** syntax rules, see *Ubuntu Official Documentation*.
- For **autoyast** templates, for more information about the **autoyast** syntax rules, see *SUSE Official Documentation*.

- The disabled custom templates cannot be used to install the operating system for Bare Metal instances in bulk in an unattended manner.

13.2.5 Bare Metal Instance

A Bare Metal instance is a VM instance created by a Bare Metal chassis. After you add a Bare Metal chassis, you can use the Bare Metal chassis to create Bare Metal instances.

- A preconfigured template can be used to quickly generate a preconfigured file to install Bare Metal instance operating systems in bulk without attended interferences.
- Operating system installations can be customized. Currently, the supported versions of operating systems include custom operating systems of the Cloud and mainstream Linux distributions (RHEL/CentOS, Debian/Ubuntu, and SUSE/openSUSE). These versions must be ISO and non-live CD.
- A business network can be configured for Bare Metal instances. Currently, flat networks are supported. Specifically, both Bare Metal instances and VM instances on the same L2 network can reach each other without routing via gateways. Make sure that a Bare Metal cluster where the Bare Metal chassis resides attaches the corresponding L2 network in advance.

You can perform the following operations on a Bare Metal instance:

- Create Bare Metal instance: Create a Bare Metal instance.

- Start: Start the Bare Metal instance that you selected.
- Stop: Stop the Bare Metal instance that you selected.
- Power reset (reboot): Power reset the Bare Metal instance that you selected.
- Bind tag: Bind tags to the Bare Metal instance.

Note:

- A Bare Metal instance only enables administrators to bind tags.

Note:

- One resource can bind 50 tags at most, while a single tag can bind the unlimited number of resources.
- Many-to-many bindings between tags and resources are supported. That is, you can bind multiple tags to multiple resources.
- Tags that were created by a tenant can only be bound to resources owned by the tenant, while admin tags can be bound to all resources.
- An administrator can unbind or delete tenant tags.
- Resource tags can be sorted in order according to the creation time or tag names (priority: characters > numbers > Chinese characters > English characters). To change the sort order, choose **Settings** > **Global Settings** > **Advanced**, locate **Tag sorting field**, and click the Edit icon. By default, the tags are sorted in order by the tag name.

- Unbind tag: Unbind tags from the Bare Metal instance.

Note:

- Multiple tags on a single resource can be unbound simultaneously. In addition, multiple resources on a single tag can also be unbound simultaneously.
- A tenant can only unbind tags from the resources owned by the tenant itself, while an administrator can unbind tags from all resources.

- Open console: Open the console of the current Bare Metal instance.
  - If the deployment is time-consuming, reach the console to view the installation details.
  - After deployment, you can perform various operations on the Bare Metal instance via the console.

Note:

- Ensure that the cluster where the Bare Metal instance corresponds to the Bare Metal chassis has attached one or more deployment servers. Otherwise, you fail to open the console of the Bare Metal instance.
- If the operating system is Debian or Ubuntu, opening a console is not supported. However, you can view the installation details by connecting an external display (monitor).
- If the operating system is SUSE or openSUSE, opening a console will enforce you to enter a password. Preconfigured console password: **password**.

- Delete: Delete the Bare Metal instance that you selected.

Note:

- Deleting a Bare Metal instance supports three types of delete policies: immediate delete (Direct), deferred delete (Delay), and never delete (Never). Default type: Delay.
  - Direct: When set to Direct, if you delete Bare Metal instances, these Bare Metal instances will be deleted immediately.
  - Delay: When set to Delay, if you delete Bare Metal instances, these Bare Metal instances will be marked as deleted and display on the delete tab page of the corresponding Bare Metal instances. After Delay completely times out (Default Delay: 24 hours or 86400 seconds.), or when you manually enforce to delete these Bare Metal instances, these Bare Metal instances will be expunged.
  - Never: When set to Never, if you delete Bare Metal instances, these Bare Metal instances will never be deleted automatically by the system.
- Set a delete policy for a Bare Metal instance as needed.

  Method: Choose **Settings** > **Global Settings** > **Advanced**, and set **Deletion Policy**.

- Restore: Restore the deleted Bare Metal instance.

Note:

- After restoring the Bare Metal instance, go back to **Available** tab page. At this time, its state is displayed as **Stopped**. You can manually reboot this Bare Metal instance.
- After the Bare Metal instance is deleted, its IP address will be reclaimed back into the IP address pool. After the Bare Metal instance is restored, the DHCP service of PXE servers will reassign a new IP address for the Bare Metal instance.

- Expunge: Expunge the deleted Bare Metal instance.

Note:

Exercise caution. This operation cannot be reversed.

Notice

- Create Bare Metal instance:
  - One Bare Metal chassis can only be used to create one Bare Metal instance.
  - Up to 50 Bare Metal instances can be created in bulk at one time.
  - Obtain hardware information in advance for a Bare Metal chassis. Otherwise, the candidate list will not display this Bare Metal chassis.
  - Prepare well images in your backup storage in advance. ImageStore backup storages are supported. These images must be ISO and non-live CD.
  - Currently, the supported operating systems include:
    - Operating systems customized through the Cloud.
    - Supported mainstream Linux distributions: RHEL/CentOS, Debian/Ubuntu, and SUSE/openSUSE.
  - Prepare well the preconfigured templates on the Cloud in advance.
    - The operating system of the selected preconfigured template must match the selected image.
    - If the operating system is SUSE or openSUSE, opening a console for the Bare Metal instance will enforce you to enter a password. Preconfigured console password: **password**.
  - If the operating system is RHEL/CentOS or SUSE/openSUSE, the system user name defaults to root. You only need to specify a password.
  - If the operating system is Debian or Ubuntu, enter a user name and a password as needed.
  - Bare Metal instances must have available NICs. Then, these NICs can be used to configure business networks.
  - If you want to use the same configurations, ensure that the NIC count and NIC name between Bare Metal instances are the same.
  - Currently, both flat networks and VLAN layer 2 isolations are supported.
  - Make sure that the corresponding L2 network is attached to the Bare Metal cluster where the Bare Metal chassis resides.

- Bare Metal instances will be automatically rebooted after creation. Based on the preconfigured template, the operating system will be installed in bulk on these Bare Metal instances without attended interferences.
- If the deployment is time-consuming, reach the console to view the installation details.
- After the deployment completes, the Bare Metal instance automatically reboots, and then its status is **Provisioned**.

- Open console:
  - Ensure that a deployment server has been attached to the cluster where the Bare Metal instance corresponds the Bare Metal chassis. Otherwise, you fail to open the console of the Bare Metal instance.
  - If the operating system is Debian or Ubuntu, opening a console is not supported. However, you can view the installation details by connecting an external display (monitor).
  - If the operating system is SUSE or openSUSE, opening a console will enforce you to enter a password. Preconfigured console password: **password**.
- Delete Bare Metal instance:
  - Deleting a Bare Metal instance supports three types of delete policies: immediate delete (Direct), deferred delete (Delay), and never delete (Never). Default type: Delay.
    - Direct: When set to Direct, if you delete Bare Metal instances, these Bare Metal instances will be deleted immediately.
    - Delay: When set to Delay, if you delete Bare Metal instances, these Bare Metal instances will be marked as deleted and display on the delete tab page of the corresponding Bare Metal instances. After Delay completely times out (Default Delay: 24 hours or 86400 seconds.), or when you manually enforce to delete these Bare Metal instances, these Bare Metal instances will be expunged.
    - Never: When set to Never, if you delete Bare Metal instances, these Bare Metal instances will never be deleted automatically by the system.
  - Set a delete policy for a Bare Metal instance as needed.

    Method: Choose **Settings** > **Global Settings** > **Advanced**, and set **Deletion Policy**.
- Restore or expunge Bare Metal instance:
  - After restoring the Bare Metal instance, go back to **Available** tab page. At this time, the state is displayed as **Stopped**. You can manually reboot this Bare Metal instance.

  - After the Bare Metal instance is deleted, its IP address will be reclaimed back into the IP address pool. After the Bare Metal instance is restored, the DHCP service of PXE servers will reassign a new IP address for the Bare Metal instance.
  - Exercise caution. Expunging the Bare Metal instance cannot be reversed.
- ZStack enables you to monitor the real-time performance of Bare Metal instances. The monitor method is internal. Specifically, the internal monitoring data will be obtained from these Bare Metal instances via agents, and performance indicators of various loads are displayed on the UI, including, CPU, memory, disk capacity, disk IO, and NIC.

> **Note:**
> To view the monitoring data of these Bare Metal instances, ensure that agents are pre-installed. For more information, see *Install Agent*.

More Information

A Bare Metal instance has two types of states or statuses: **State** and **Status**:

State	Status
• Created • Starting • Running • Stopped • Rebooting • Deleted • Error	• Unprovisioned • Provisioning • Provisioned

13.3 Backup Service

Backup Service, which is business-centered, integrates the scheduled incremental backup, scheduled full backup, and other backup technologies to ZStack Private Cloud. With Backup Service, multiple backup solutions are supported, such as local backup, remote backup, and Public Cloud backup solutions. Select an appropriate backup solution according to your own business needs.

Backup Service is a separate feature module. To use this service, purchase both the Base License and the Plus License of BareMetal Management. The Plus License cannot be used independently.

Typical Backup Scenarios

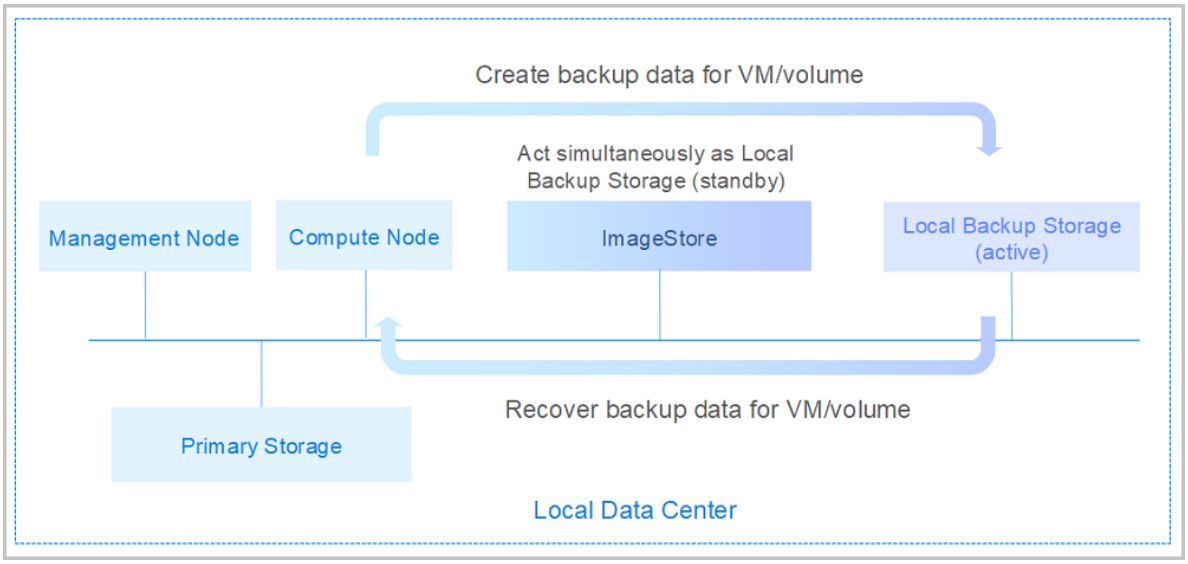
Backup Service can be applied to the following three typical scenarios: local backup, remote backup, and Public Cloud backup.

- **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.

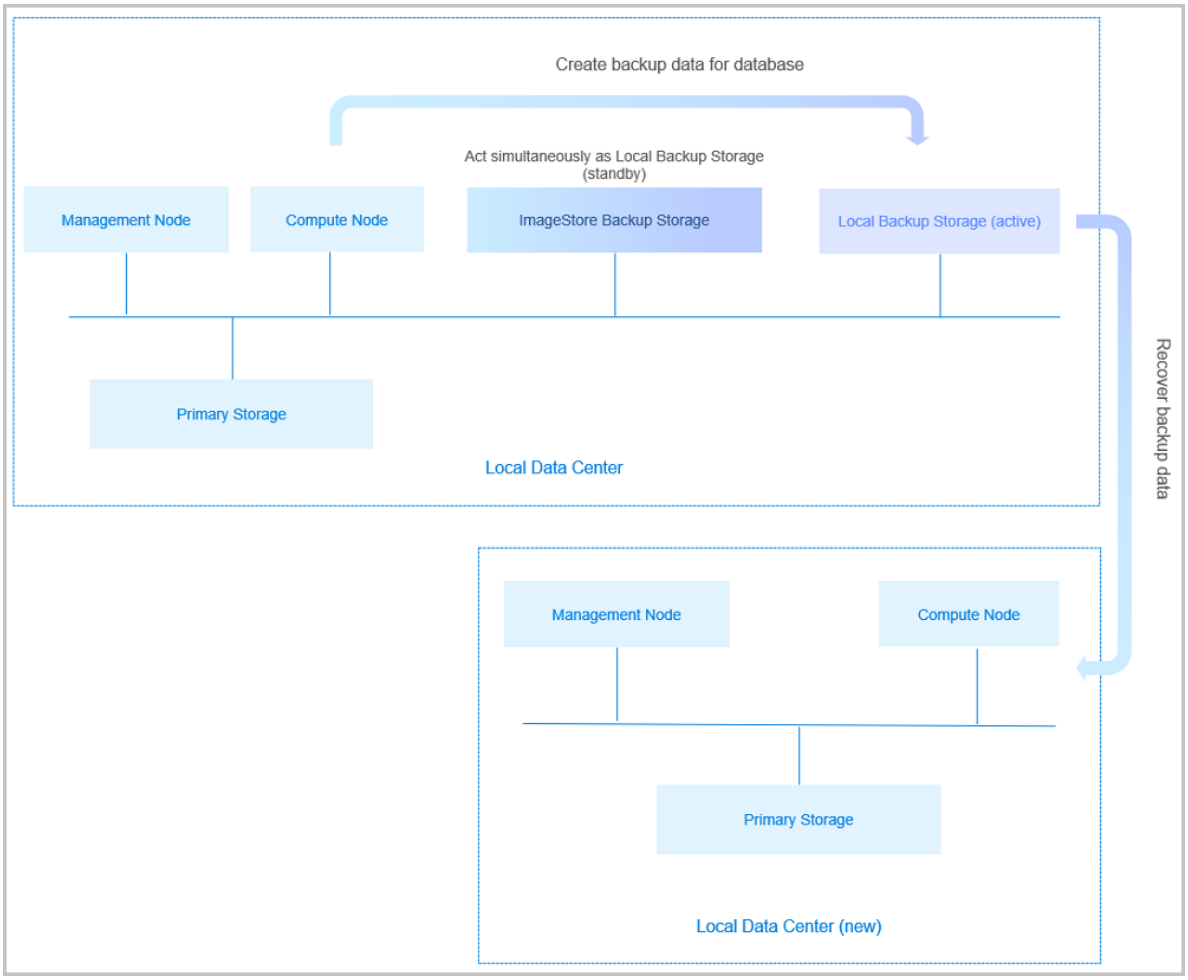
  If your local data is mistakenly deleted, or data in the local primary storage is damaged, you can recover the backup data from the local backup storage, as shown in *Local Backup Scenario-1*

  Figure 13-4: 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 13-5: Local Backup Scenario-2

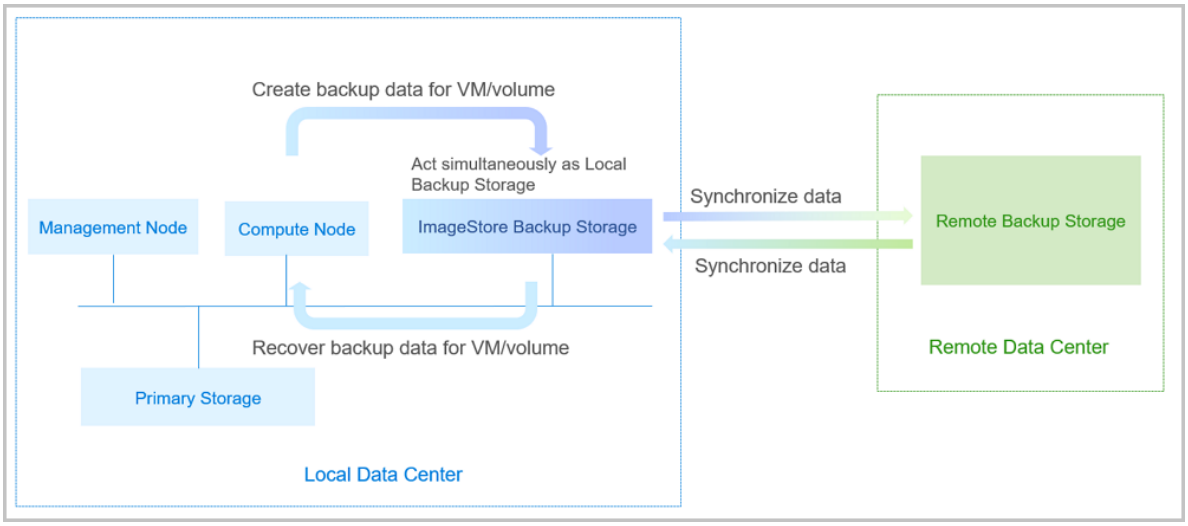


- **Remote Backup**

  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.

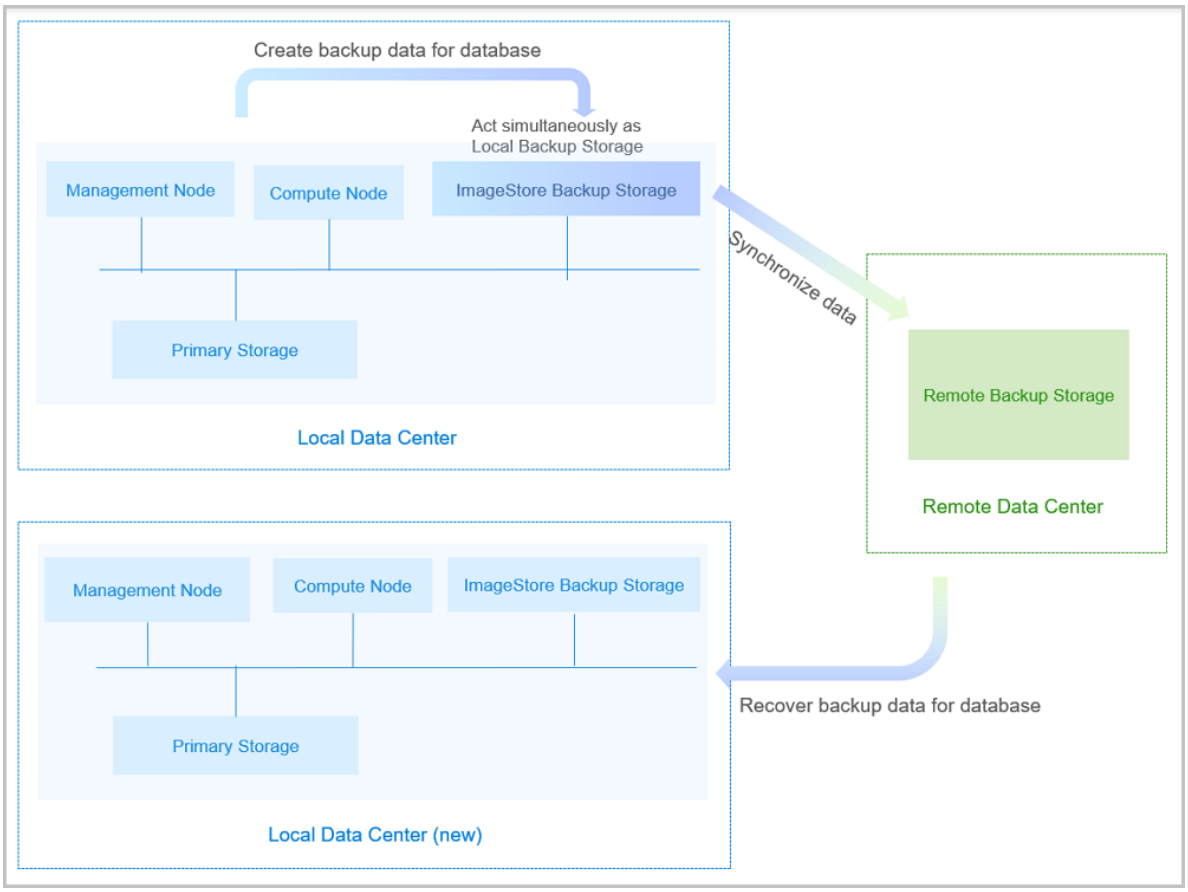
  If your local data is mistakenly deleted, or data in the local primary storage is damaged, you can recover the backup data from the remote backup storage, as shown in *Remote Backup Scenario-1*

Figure 13-6: 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 13-7: Remote Backup Scenario-2

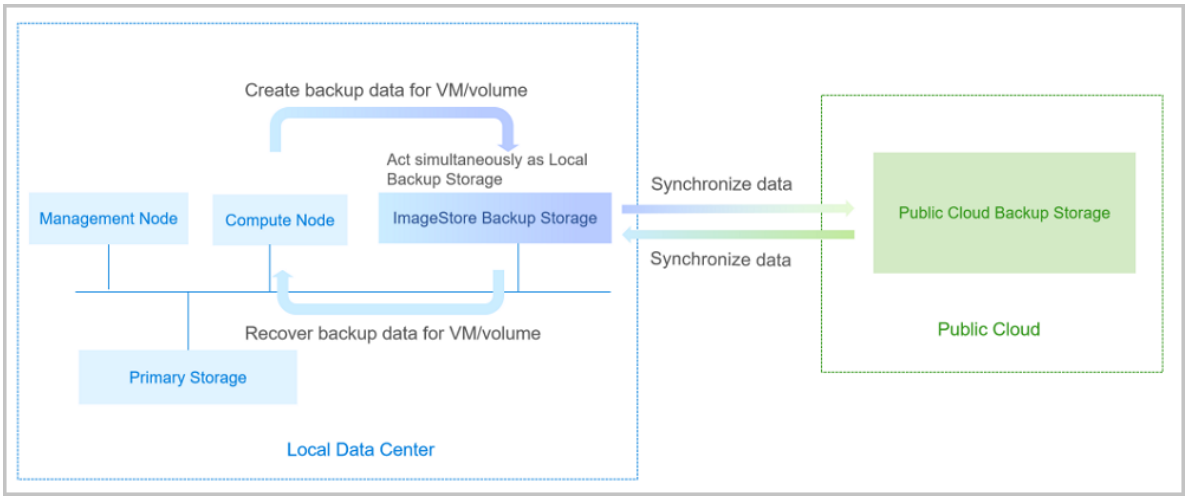


- **Public Cloud Backup**

  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.

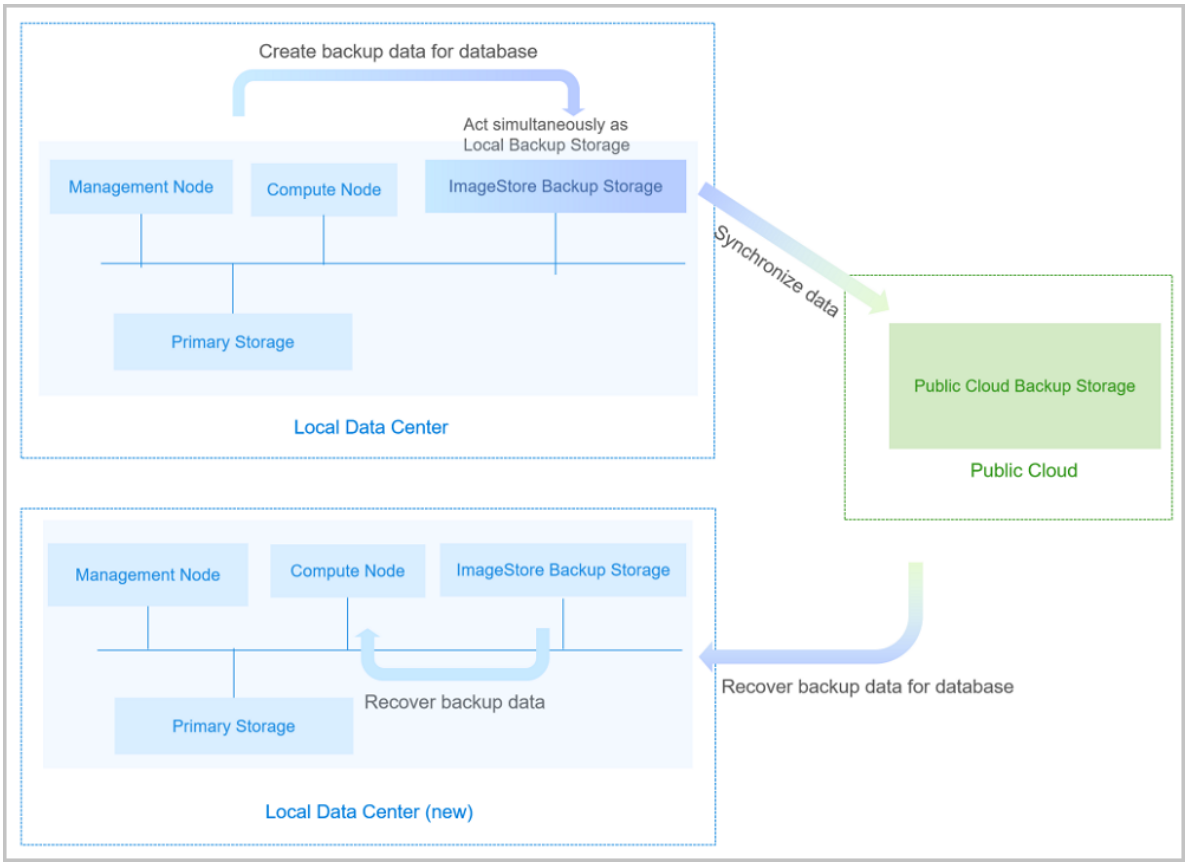
  If your local data is mistakenly deleted, or data in the local primary storage is damaged, you can recover the backup data from the Public Cloud backup storage, as shown in *Public Cloud Backup Scenario-1*.

  Figure 13-8: 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 13-9: Public Cloud Backup Scenario-2



13.3.1 Backup Task

A backup task enables you to back up local VM instances, local volumes, or local MN database (database) on schedule to a specified local backup storage, and also to synchronize backup data to a specified remote backup storage (offsite backup storage or Public Cloud backup storage.

The backup task overview page displays backup task executions of VM instances, volumes, and database, where backup tasks within a time range are calculated and analyzed in visual graph. As a result, you can directly get a whole picture of all backup tasks.

- A backup task enables you to back up local VM resources or local volume resources on schedule to a specified local backup storage, and also to synchronize backup data to a specified remote backup storage (offsite backup storage or Public Cloud backup storage).
  - Make sure that you add a local backup storage to the Cloud in advance. If you specify two local backup storages, the active-standby seamless switchover between these two backup storages are supported.

- If you want to back up your data remotely, make sure that you add a remote backup storage to the Cloud in advance. Notice that you are only allowed to add one remote backup storage to the Cloud.
- Backup tasks of local VM instances or volumes:
  - A single backup task supports multiple resources.
  - Set the incremental backup strategy and the full backup strategy as needed.
  - Backup progress bars are provided to let you view resource backup states at any time.
  - Update a backup policy for a backup task as needed.
  - You can perform a one-time backup task immediately.
  - Set a network QoS or disk QoS for a backup task as needed.
  - When you create a backup task, the rich text mode is provided. Obtain help information at any time in the process.
  - After you create a backup task, you can perform a backup once immediately.
  - If the stopped VM instances skip backups, a one-time backup (technical preview) will be automatically performed after these VM instances start.
  - Currently, you are not allowed to perform a scheduled backup for shared volumes.
- A single VM instance or volume can be backed up immediately, where important businesses can be backed up at any time.

- A backup task enables you to back up an MN database (database) on schedule to a specified local backup storage, and also to synchronize backup data to a specified remote backup storage (offsite backup storage or Public Cloud backup storage.
  - Make sure that you add a local backup storage to the cloud in advance. If you specify two local backup storages, the active-standby seamless switching between these two backup storages are supported.
  - If you want to back up your data remotely, make sure that you add a remote backup storage to the Cloud in advance. Note that you are only allowed to add one remote backup storage to the cloud.

  The following are two types of backup policies:

  - Incremental + default full policy:
    - With a backup task, you can perform incremental backups for your resources by defining the incremental policy.

- After you perform 63 times of incremental backups (you can modify the incremental backup count on the terminal), the system defaults to execute a full backup once.

- Incremental + custom full policy:
  - With a backup task, incremental backups and full backups will be performed based on the user-defined incremental policy and full backup policy.
  - After you perform 63 times of incremental backups (you can modify the incremental backup count on the terminal), the system defaults to execute a full backup once.
- If an incremental backup and a full backup task are triggered simultaneously at a time, a backup sequence will be used.
- The corresponding incremental backups and full backups are all displayed on the list of the local backup data. If you have chosen to synchronize your local backup data to a remote backup storage, you can view the synchronized backup data on the list of the remote backup storage.

Notice

- A backup task can be performed for the running VM instances.
- To create the backup task for volumes, these volumes must be attached to the running VM instances.
- If VM instances have attached shared volumes, these shared volumes cannot be not backed up when a backup task is performed for these VM instances.
- One backup task can be specified to two local backup storages at most. When two local backup storages are specified, which of these two backup storages will be master or standby depends on their add sequence. The first to be added to the Cloud will be master, while the second or later will be standby.
- When a local backup storage (Master) fails over, another local backup storage (Standby) will be automatically started to ensure your business continuity.
  - When the local backup storage (Master) works properly, backup tasks will be performed directly on this local backup storage.
  - When the local backup storage (Master) is stopped, deleted, or disconnected, backup tasks will be automatically performed on another local backup storage (Standby).
  - When the local backup storage (Master) is restored to a normal working condition, the backup tasks will be automatically performed on this local backup storage (Master) again.

- When backups are calculated by count, the retention count for backup data must be integer. The minimum allowed retention is one.
- When backups are calculated by time, follow the rules below:
  - The retention count for backup data must be integer. Unit: Day | Week | Month. The minimum allowed retention is one day.
  - Retain X day (s), indicating that since backup tasks are performed for the first time, the backup data will be retained for 24 hours * day (s).
  - Retain X week (s), indicating that since backup tasks are performed for the first time, the backup data will be retained for 7 days*week (s).
  - Retain X month (s), indicating that since backup tasks are performed for the first time, the backup data will be retained for 30 days * month (s).
- Run `incrementalBackup.maxNum` to set the default value to 64 globally, an indication that after 63 times of backup tasks are performed, a full backup will be performed once.
- Run **`zstack-cli`** to update this global configuration value. For example,

```
[root@localhost ~]# zstack-cli  #Run CLI.

admin>>> LogInByAccount accountName=admin password=password #Log in
to CLI. Default user name/password: admin/password.

admin >>>UpdateGlobalConfig category=volumeBackup name=incrementa
lBackup.maxNum value=10 #Modify the maximum incremental backups.
{
    "inventory": {
        "category": "volumeBackup",
        "defaultValue": "64",
        "description": "the maximum numbers of continuous incrementa
l backup",
        "name": "incrementalBackup.maxNum",
        "value": "10"
    },
    "success": true
}
```

- The updated backup policy will not affect the triggered backup tasks.
- A new backup task will no longer be performed for the resource that has been backed up.
- After deleting the backup task of this resource, you can create a new backup task for it.

13.3.2 Local Backup Data

A local backup data is the backup data (local VM instances, local volumes, or database) that are backed up on a local backup storage. On the **Local Backup Data** page, you can manage your local backup data.

- Backup data can either be recovered to the local backup storage or synchronized to the remote backup storage.
- When you recover database, the UI page will not work properly if you refresh your browser, which does not affect the database recovery process.
- This feature module enables you to back up and recover the data that are saved on an MN database, while data of operation logs and monitoring information are not available for this operation.

You can perform the following operations on local backup data:

- View details of the local backup data.
- Restore the local backup data.
- Synchronize the local backup data to a remote backup storage.
- Delete the local backup data.
- Scan the database backup.
- Export the backup data of the local database.

Notice

- When overwriting the original resources, ensure that VM instances are placed into the stopped state.
- When synchronizing the local backup data remotely, ensure that you add a remote backup storage to ZStack Private Cloud in advance. Only one remote backup storage can be added.
- When the local backup storage is deleted, only the local backup data will be deleted by default. To delete the backup data on the remote backup storage, select **Sync Delete Remote Backup Data**.
- If the remote backup data is deleted simultaneously, its local records will be deleted, but the actual data are not affected.
- Assume that you restore the backup data for a volume. If the volume resides on a SharedBlock primary storage, ensure that you select a provisioning method, including thin provisioning and thick provisioning.
  - Thin provisioning: Allocate storage space to data volumes based on the actual usage to achieve higher storage utilization.
  - Thick provisioning: Preallocate required storage space to provide sufficient storage capacity for data volumes, ensuring the storage performance.

- After the database is restored, all resources on the Cloud will be changed to the state at a time when the backup task is created. Ensure that, in the local backup storage, select **Scan Backup** to obtain the information of the currently actual backup data.

13.3.3 Local Backup Storage

A local backup storage is a storage server located at your local data center for storing backup data of local VM instances, local volumes, or database.

- An ImageStore backup storage that has been deployed in your local data center can serve as a local backup storage.
- You can also deploy a new local backup storage on the Cloud.
- The Cloud enables you to add multiple local backup storages.
- When a backup task specifies multiple local backup storages, the active-standby seamless switchover between these local backup storages are supported.
- Both the expunged, invalid backup data and expired, temporary data that have been expunged can be cleared up to release more storage spaces.
- The backup data that have been backed up to a local backup storage can be viewed at the local backup storage details page.

You can perform the following operations on a local backup storage:

- Add a local backup storage.
- Enable the local backup storage.
- Disable the local backup storage.
- Reconnect the local backup storage.
- Scan the backup data.
- Clean up the data of the local backup storage.
- Delete the local backup storage.
- Modify the basic attributes of the local backup storage.
- Manage the local backup storage.

Notice

- Add an existing ImageStore backup storage to act as a local backup storage. The **Name** option will automatically detect and use the name of this ImageStore backup storage. Also, after addition, you can modify the name by going to the details page of the local backup storage.

- Assume that you specify a local backup storage for a backup task. If you disable this local backup storage, the backup task will fail.
- Assume that you specify multiple local backup storages for a backup task. If you disable one of these local backup storages, the backup task will be automatically switched to another local backup storage (Standby).
- If the local backup storage is an existing ImageStore backup storage, deleting the local backup storage will not delete the local records (of the backup data) and the actual data on this local backup storage. When you add this local backup storage again, the local records of the backup data will be restored in real time.
- If the local backup storage is a newly added storage server, deleting this local backup storage will delete the local records of the backup data on the local backup storage, but the actual data is not affected. Exercise caution when you add this local backup storage again, the local records of the backup data cannot be automatically restored.
- Data can be cleaned. If you clean both the expunged, valid backup data and the expired, temporary data on the local backup storage, you can release more storage spaces.

Note:

For example, assume that you expunge the local backup data of a VM instance or volume , and expunge this VM instance or volume restored from this backup data. At this time, performing the clear data button will release the storage space for this local backup storage.

13.3.4 Remote Backup Storage

A remote backup storage is a storage server located at your offsite data center or Public Cloud for storing backup data of local VM instances, local volumes, or database.

- Backup data can only be synchronized to a remote backup storage from a local backup storage .
- The Cloud enables you to add only one remote backup storage.
- The backup data that have been backed up to a remote backup storage can be viewed at the details page of the remote backup storage.
- To recover the remote backup data of local VM instances or local volumes locally, the remote backup data must firstly be synchronized to a local backup storage.
- The remote backup data of a database can directly be recovered to the local backup storage.

You can perform the operations on a remote backup storage:

- Add a remote backup storage.
- Enable the remote backup storage.
- Disable the remote backup storage.
- Reconnect the remote backup storage.
- Clear data for the remote backup storage.
- Delete the remote backup storage.
- Modify the basic attributes of the remote backup storage.
- Attach or detach a zone from the remote backup storage.
- Manage the remote backup storage.

Notice

- Assume that you specify a remote backup storage for a backup task. If you disable the remote backup storage, the backup task will continue to work normally on a local backup storage, but stops synchronizing to the remote backup storage.
- Deleting a remote backup storage will delete the local records of the backup data on this remote backup storage, but the actual data is not affected. Exercise caution when you add the remote backup storage again, the local records of the backup data will not be automatically restored.
- To restore remote backup data locally, synchronize it to a local backup storage in advance.
- Data can be cleaned. If you clean both the expunged, valid backup data and the expired, temporary data on a local backup storage, you can release more storage spaces.

> **Note:**
>
> For example, assume that you expunge the local backup data of a VM instance or volume , and expunge this VM instance or volume restored from this backup data. At this time, performing the Clear Data button will release the storage space for this local backup storage.

13.4 Migration Service

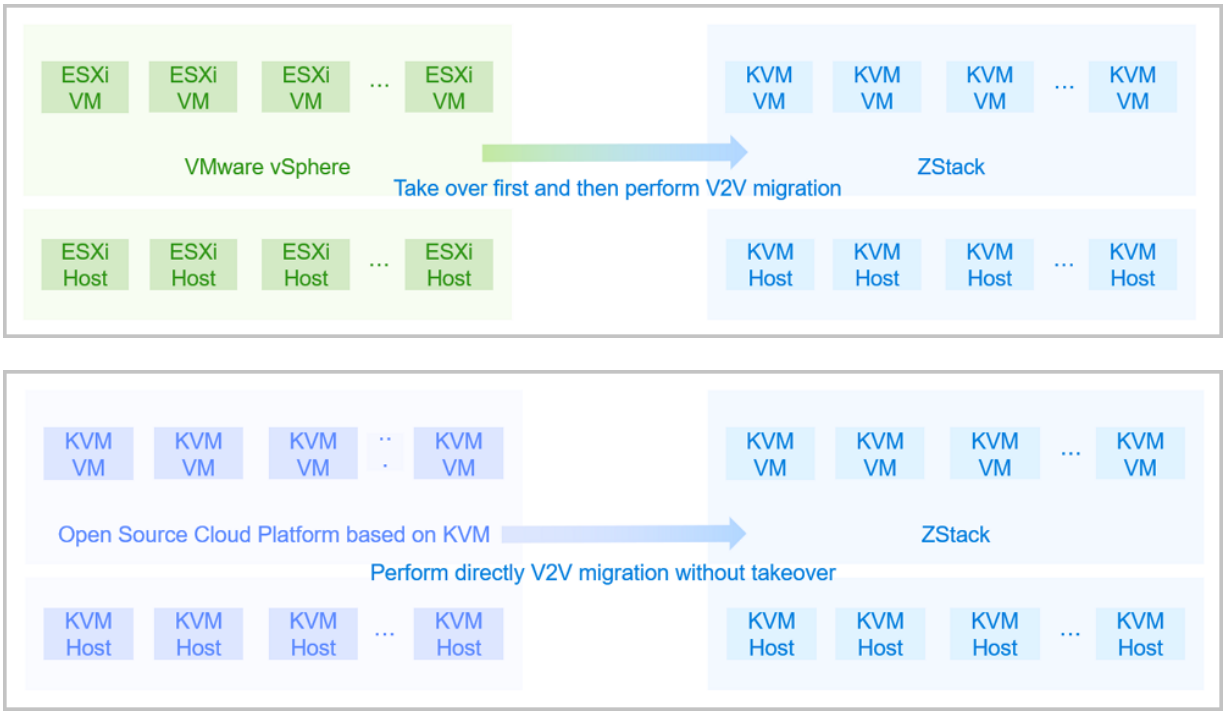
ZStack provides the V2V Migration Service, allowing you to migrate VM systems and data from other virtualization platforms to the current cloud. Currently, with the V2V Migration Service, you can:

- Migrate VM instances from the vCenter that you took over to the current cloud. The supported versions of the source vCenter platform include 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7. Note that the version of vCenter Server must be consistent with that of ESXi Host.

- Migrate VM instances from a KVM cloud platform to the current cloud.

As shown in *V2V Migration*.

Figure 13-10: V2V Migration



The V2V Migration Service is a separate feature module. To use this feature, you need to purchase both the Base License and the Plus License of the V2V Migration Service. The Plus License cannot be used independently.

With the V2V Migration Service, you can:

- Perform one-click V2V migrations in bulk for VM instances.
- Only need to add a conversion host and create a V2V job. The cloud will do the rest of your work.
- Configure an independent migration network and a network QoS for a conversion host to control transmission bottlenecks and to improve migration efficiencies.
- Customize configurations for destination VM instances when you create a V2V job.
- Monitor and manage the entire migration process in the visualized, well-designed UI.

13.4.1 V2V Migration

Currently, the V2V Migration Service allows you to migrate VM instances from a VMware cloud platform or a KVM cloud platform to the current cloud.

Source Cloud Platform: VMware

By creating V2V migration jobs, you can migrate VM instances from the vCenter that you took over to the current Cloud.

- Before migrations, perform **data synchronization** on the vCenter that you took over to manually synchronize the latest status of vCenter resources.
- You can perform bulk V2V migrations for VM instances, and customize configurations of the destination VM instances to be migrated.
- The supported versions of the source vCenter platform include 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7. Note that the version of vCenter Server must be consistent with that of ESXi Host.
- The supported systems of source vCenter VM instances include RHEL/CentOS 4.x, 5.x, 6.x, 7.x, SLES 11, 12, 15, Ubuntu 12, 14, 16, 18, and Windows 7, 2003, 2008, 2012, 2016.
- The VM instances will be forced to shut down during the V2V migration process. Therefore, pay attention to the business impact.

  Note:
  The system firstly attempts to shut down the VM instances softly. If the shutdown fails, the system will shut down the VM instances forcibly.
- The type of the source primary storage is not enforced. The type of the destination primary storage can be LocalStorage, NFS, Ceph, and Shared Block.
- For Windows VM instances, the Windows VirtIO driver is automatically installed during the migrations, which improves the NIC and disk efficiencies.
- You can perform V2V migration for VM instances booted by UEFI. After migrations, these VM instances are also booted by UEFI.

When you migrate VM instances from the vCenter that you took over to the current Cloud, note that:

- During the V2V migration process, do not power on the source vCenter VM instances that were stopped. Otherwise, the migration might fail.
- During the V2V migration process, do not restart the V2V conversion host. Otherwise, the migration might fail.
- After the V2V migration is completed, the number of drivers from which the destination VM instances are started will be set according to the number of source VM drivers. Currently, up to three drivers can be set.

- Assume that you enabled the switch for automatically starting VMs after migration. If the physical resources in your destination cluster are insufficient, the destination VM instances will fail to start and enter the stopped state. At this time, the status of the V2V job is displayed as **Succeeded**.
- For Windows VM instances, the Windows VirtIO driver is automatically installed during the migration process. You need to manually update the driver after migration. Note that the Windows VirtIO driver will be installed in the local directory, and you can search for it and then update it.
- For Windows VM instances that have volumes, the volumes are in offline mode after migration. You need to manually change the mode to online.
- For Linux and Windows VM instances that have volumes, the drive letter of the volumes might be modified after migration. You need to manually modify the drive letter according to the drive letter order of the source VM instances. We recommend that you record the drive letter order of the source VM instances before migration.
- For Linux and Windows VM instances whose volumes are in SCSI mode, the volume mode can be automatically recognized during the migration process. You can set the volume mode for the destination VM instances after migration.
  - For Windows VM instances, the volume mode defaults to non-VirtioSCSI after migration.
  - For Linux VM instances, the volume mode defaults to VirtioSCSI after migration.

  Note:

  If the kernel version is relatively old, such as RHEL5 (kernel 2.x), the volumes cannot be in VirtioSCSI mode. You need to manually change the volume mode to non-VirtioSCSI after migration.

  For example, if a destination VM instance fails to start after migration, and an error "Cannot find hard disk" is reported, and the kernel version is relatively old (such as kernel 2.x), the reason may be that the old version of the Virtio driver does not support SCSI. In this case, you need to manually change the volume mode to non-VirtioSCSI. Then, the VM instance can enter the system after restart.
- For Linux VM instances, if these VM instances were started in GUI mode before migration, you might need to update the display configuration of the VM instances for the first startup after migration.

- For Linux VM instances that are booted by UEFI and whose system version is RHEL/CentOS 5.x, 6.x, or 7.x, you need to delete the **rhgb** parameter in the startup option for the VM instances to start successfully after migration.
- For Linux VM instances that are booted by UEFI and whose version is CentOS 7.4 or later, the VM instances will enter the UEFI Shell if you start them after migration. To enter the operating system, run the following commands:

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

  If you want the VM instances to automatically enter the operating system instead of the UEFI Shell upon restart, run the `vim /boot/efi/startup.nsh` command to create a script and save the following content:

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

- You can set the maximum number of V2V jobs that can run at a time. The method is as follows:

  Go to **Settings** > **Global Settings** > **Advanced**, locate **ParallelismDegree**, and click the Edit icon. The default value is 10.
- You can set the host allocator strategy for starting the destination VM instances after migration. The method is as follows:

  Go to **Settings** > **Global Settings** > **Advanced**, locate **HostAllocatorStrategy**, and click the Edit icon. The default option is Host with min. running VMs.

Source Cloud Platform: KVM

By creating V2V migration jobs, you can migrate VM instances from a KVM cloud platform to the current cloud.

- You can perform bulk V2V migrations for VM instances, and customize configurations of the destination VM instances to be migrated.
- You can migrate the VM instances that are running or paused. Do not power off the VM instances that need to be migrated.
- You can perform V2V migrations for VM instances booted by UEFI. After migrations, these VM instances are also booted by UEFI.

- The type of the source primary storage is not enforced. The type of the destination primary storage can be LocalStorage, NFS, Ceph, and Shared Block.
- For different types of source primary storage or destination primary storage, the libvirt version and QEMU version must meet the following requirements:
  - If either the source primary or destination primary storage is Ceph, use libvirt 1.2.16 and QEMU 1.1 or their later versions.
  - If neither the source primary storage nor destination primary storage is Ceph, use libvirt 1.2.9 and QEMU 1.1 or their later versions.

When you migrate VM instances from a KVM cloud platform to the current cloud, note that:

- For VM instances with high I/O, we recommend that you pause them before migration to ensure the data integrity. When you perform V2V migrations for VM instances that undergoing high I/O operations, a portion of data in the memory might not be saved to hard disks. In this case, this portion of data might be lost after V2V migration.
- During the V2V migration process, do not power the source VM instances.
- During the V2V migration process, do not restart the V2V conversion host. Otherwise, the migration might fail.
- After the V2V migration is completed, you need to manually start the source VM instances that were paused.
- Assume that you enabled the switch for automatically starting VMs after migration. If the physical resources in your destination cluster are insufficient, the destination VM instances will fail to start and enter the Stopped state. At this time, the status of the V2v job is displayed as **Succeeded**.
- You can set the maximum number of V2V jobs that can run at a time. The method is as follows:

  Go to **Settings** > **Global Settings** > **Advanced**, locate **ParallelismDegree**, and click the Edit icon. The default value is 10.
- You can set the host allocator strategy for starting the destination VM instances after migration. The method is as follows:

  Go to **Settings** > **Global Settings** > **Advanced**, locate **HostAllocatorStrategy**, and click the Edit icon. The default option is Host with min. running VMs.

13.4.2 V2V Conversion Host

To perform V2V migrations, specify a host in a destination cluster as the V2V conversion host.

- A V2V conversion host must have sufficient hardware resources, such as network bandwidth and disk space. The following table lists the minimum configuration requirements.

Table 13-1: Minimum Configuration Requirements for V2V Conversion Host

Hardware	Configuration Requirements
CPU	Minimum 8 cores
Memory	Minimum 16 GB
Network	Minimum 1 Gigabyte NIC
Storage	Minimum 50 GB for the rest of storage spaces **Note:** You can modify the storage configuration according to the number of VM instances to be migrated.

- The type of the V2V conversion host must be consistent with that of the source cloud platform.
- You can set an independent migration network and a network QoS for a V2V conversion host to control transmission bottlenecks and to improve migration efficiencies.

Notice

- Before you create a V2V job, you need to add a V2V conversion host to the cloud.
- The V2V conversion host is a host in a target cluster. Make sure that the host has sufficient hardware resources for V2V migration.
- The type of the V2V conversion host must be consistent with that of the source cloud platform.
- A host cannot be used as both a VMware V2V conversion host and a KVM V2V conversion host.
- If multiple source VM instances were selected, the V2V jobs created accordingly will use the same V2V conversion host.
- During the V2V migration, the VM system and data are first cached in the V2V migration host, and then imported into the target primary storage.
- If a V2V conversion host is disabled when the V2V jobs are being performed, the migration will not be affected.
- Deleting a V2V conversion host will automatically cancel the ongoing V2V jobs. However, the resources that have been migrated will not be affected.

14 MN Maintenance

This chapter describes how to perform maintenance on ZStack management nodes (MNs).

Considerations

When you perform maintenance on a MN, note that:

- Before you perform maintenance on a MN, such as upgrading or restarting the MN, go to **Settings** > **Global Settings** > **Advanced**, locate **VM HA**, and set the value to **false**. After the maintenance is finished, set the value to **true**.

14.1 MN High Availability

14.1.1 Multi-MN High Availability

Overview

ZStack provides high availability (HA) for multiple management nodes (MNs, also known as hosts) by using separate HA suites. When any one of the MNs is disconnected, the HA will be triggered in seconds to ensure the business continuity.

HA mechanism: In a multi-MN model, each MN runs a **zsha2** HA process. This process monitors the key services, including the MN service, UI service, and database service, in each MN in real time. When any key service is down, the system immediately triggers virtual IP (VIP) migration through Keepalived, and then attempts to restore the downtime service.

This topic provides an example of a dual-MN HA scenario to describe the procedures for installation, deployment, and upgrade. This topic also provides some considerations for using multi-MN HA. For more information, see the *Multi-MN HA Tutorial*.

Installation and Deployment

- Assume that you have a single-MN environment and want to upgrade it to a dual-MN HA environment.

  1. Download the latest ZStack Custom ISO, bin package, and multi-MN HA suite from the official website.
  2. Upgrade your existing MN to the latest version of ZStack.
  3. Install the latest version of ZStack in the newly added MN.
  4. Install a license for the newly added MN. Make sure that the license type of these two MNs is exactly the same.

5. Import the HA suite into the previous MN. Then, decompress and install the suite.

- Assume that you have a newly installed dual-MN environment and want to deploy it as an HA environment.

  1. Download the latest ZStack Custom ISO, bin package, and multi-MN HA suite from the official website.
  2. Install the latest version of ZStack in these two MNs.
  3. Install a license for these two MNs. Make sure that the license type of these two MNs is exactly the same.
  4. Import the HA suite into one of the MNs. Then, decompress and install the suite.

Upgrade

- HA suite upgrade

  After you obtain the new version of the HA suite, you can use it to upgrade the current **`zsha2`** service.

  After the databases of the active and standby MNs are automatically synchronized, import the new version of the HA suite into the active MN and decompress the suite. Then, run the following command in the active MN to finish the HA suite upgrade:

  ```
  [root@localhost ~]# ./zsha2 upgrade-ha
  ```

- MN upgrade

  In the dual-MN HA scenario, you need to upgrade the HA suite before you can upgrade a MN.

  You only need to run the following commands in one MN. Then, both MNs can be upgraded.

  - If you perform upgrade from the bin package, run the following command:

    ```
    [root@localhost ~]# zsha2 upgrade-mn -peerpass password ./ZStack-installer-3.10.0.bin
    ```

  - If you perform upgrade from ISO, run the following command:

    ```
    [root@localhost ~]# zsha2 upgrade-mn -peerpass password ./ZStack-x86_64-DVD-3.10.0-c76.iso
    ```

    Note:

    In the command above, the `-peerpass` parameter is optional. You can set a password for SSH login to the peer MN.

Considerations

- We recommend that you configure at least 8 CPUs and 12 GB memory for the host (MN).
- We recommend that you use a 10-Gigabit bandwidth or above for the management network. If the management network is deployed independently, a 1-Gigabit bandwidth is allowed.
- We recommend that you use **`zs-network-setting`** to create static network bridges as needed.
- The multi-MN HA suite depends on ZStack 2.6.0 and later versions. Note that the version of the HA suite and ZStack must be the same. For example, if the version of the HA suite is 2.6.0, the version of ZStack must also be 2.6.0.
- The ZStack version of these two MNs must be the same. In addition, the license type of these two MNs must also be the same.
- To install an HA suite, you need to put **zsha2** and **zstack-hamon** to the same directory. During the installation, **zsha2** will automatically deploy **zstack-hamon** and related configuration files.
- During the installation, the database of the standby MN will be overwritten by the database of the active MN. Please exercise caution.
- To ensure real-time synchronization of monitoring data between these two MNs, we recommend that you perform password-free SSH login between these two MNs.
- The version of the Chrome browser used to access the MN must be 49 or later.

14.2 MN Disaster Recovery

When you use ZStack, you might fail to access the system via the MN due to hardware or system failure. In this case, you need to prepare two servers, install an HA environment by using two hosts as MNs, and restore ZStack MN service by using a remote database backup file. Then, you can perform disaster recovery on ZStack.

Note:

- We recommend that the newly prepared server use the same model and configurations as the existing MN.
- If the existing MN has only an operating system failure, you can also use the existing MN server to reinstall ZStack.

14.2.1 Preparations

Local Database Backup

After the Cloud is installed for the first time, the Cloud automatically backs up databases at 00:30 and 12:30 on a daily basis. By default, the backup data is stored in the `/var/lib/zstack/mysql-backup/` directory of the MN, and up to 14 latest backups can be reserved. You can view the backup data by using `crontab -l`.

```
30 0,12 * * * zstack-ctl dump_mysql --keep-amount 14
```

If the MN is running in a high load state for a long time, we recommend that you adjust the backup frequency and the number of reserved backups by using `crontab -e`. The following example indicates that the database is backed up at half-past the hour on an hourly basis and the latest 200 backups are reserved.

```
30 * * * * zstack-ctl dump_mysql --keep-amount 200
```

Remote Database Backup

We recommend that you configure a remote database backup to avoid the scenario where you could not access the system via the MN due to MN failure.

Assume that the IP address of the MN and the remote backup server is *172.20.12.16* and *172.20.12.75*, respectively. To perform remote backup, run the following commands in the MN whose IP address is *172.20.12.16*:

```
ssh-keygen
#Generate an SSH public key in the MN.
ssh-copy-id root@172.20.12.75
#Copy the SSH public key to the remote backup server. Note that you
need to manually enter yes and the root password.
```

Redundant Backup of Remote Database

If you have multiple servers for redundant backup, you can perform remote database backup on the remote backup servers to increase database backups.

On the remote backup server *172.20.12.75*, you can use `crontab -e` to modify **`crontab`**, and use **`rsync`** to remotely copy the database directory stored by the MN to perform regular remote backups.

```
0 0,12 * * * zstack-ctl dump_mysql --host root@172.20.12.75 --d --
keepamount 24
```

```
#Back up the MN database directly to the /var/lib/zstack/from-zstack-
remote-backup/ directory of the remote backup server at 00:00 and 12:
00 every day, and reserve up to 24 latest backups.
```

14.2.2 MN Disaster Recovery

Context

If you could not access the system via a MN due to hardware or software failure, you can perform disaster recovery by following these steps:

Procedure

1. Install the MN operating system.

   Install the operating system by referring to the ISO on the ZStack official website. You can install the operating system in the existing MN or select a new server as a MN.

2. Install ZStack.

   Install ZStack by referring to the installation documentation on the *ZStack Official Website*.

   Note:
   Please install the version where the system failure occurred. For example, if the system failure occurred on ZStack 3.8.0, we recommend that you install ZStack 3.8.0.

3. Update the license.

   After you install ZStack, update the license before you proceed with other operations.

4. Restore the database.

   On the remote backup server, select the latest database backup file. The format of the file name is as follows:

   ```
   zstack-backup-db-2016-12-07_14-43-43.gz
   #Indicates that the database is backed up at 14:43:43 on December 7
   , 2016.
   ```

   Copy this file to the newly installed ZStack. Assume that the file is saved to the `/root/` directory. Run the following command to restore the database. Note that ZStack will back up the current database again before restoring the database. During the recovery process, the related MN services will be stopped.

   ```
   zstack-ctl restore_mysql -f /root/zstack-backup-db-2016-12-07_14-43-
   43.gz --mysql-root-password zstack.mysql.password
   #The -f parameter indicates that /root/zstack-backup-db-2016-12-
   07_14-43-43.gz is selected for database recovery.
   ```

```
#The --mysql-root-password zstack.mysql.password parameter indicates
 that zstack.mysql.password is used as the root password of mysql
for database recovery.
```

Note:

- Before the database recovery, if the MN is added to the host list as a compute node at the same time, the compute node could not be recovered and needs to be deleted manually.
- Before the database recovery, if the value of consoleProxyOverriddenIp of the MN is modified, the consoleProxyOverriddenIp configuration of the following file needs to be modified in the new MN to restore the original settings.

  ```
  /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/
  zstack.properties
  ```

- If a failure occurred before the database backup of the MN is synchronized to a remote backup server, the failure cannot be repaired.
- According to the recovery method described in this document, for VM instances created from the time when database backup is performed to the time when a failure occurred in a MN, these VM instances might become uncontrollable after data is recovered. However , the status of other VM instances will directly synchronize with the status of the original hosts.

14.3 Change MN IP Address

When you use ZStack, if the IP address of the server where the MN is located changes, you need to change the IP address of the MN manually. This involves two scenarios: single MN scenario and multi-MN HA scenario.

14.3.1 Single-MN Scenario

If the IP address of the server where the MN is located changes, change the IP address of the MN by following these steps:

1. In the MN, run the following command to back up the database:

```
[root@localhost ~]# zstack-ctl dump_mysql
```

2. Run the following command in sequence to manually change the NIC address of all servers. (Here, assume that bond0 is the management network.)

```
[root@localhost ~]# zs-network-setting -i br_bond0  172.31.250.100
255.255.255.0 172.31.250.1  #Enter the addresses according to your
actual needs.
```

3. Run the following commands in sequence to change the IP address of the MN:

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110   #Here
, 172.31.250.110 is the new IP address of the MN.
[root@localhost ~]# zstack-ctl restart_node    #Restart the MN for
the configuration to take effect.
```

More Information

If the server where the MN is located is added as another node at the same time, update the IP address of the corresponding node in the UI by following these steps:

Note:
Changing the IP address of a host may cause the host to be disconnected. Please exercise caution.

- Scenario 1: The management node, compute node, and backup storage (ImageStore) share the same server.

  1. Log in to the UI. On the **Hardware** page, place the target host into maintenance mode and disable the target backup storage.
  2. In the MN, run the following command to back up the database:

```
[root@localhost ~]# zstack-ctl dump_mysql
```

  3. Run the following command in sequence to manually change the NIC address of all servers. (Here, assume that bond0 is the management network.)

```
[root@localhost ~]# zs-restore-network-setting -i br_bond0  #Clear
 the IP address of the bridge.
[root@localhost ~]# zs-show-network     #Check whether the IP
address is successfully cleared.
```

```
[root@localhost ~]# zs-network-setting -i br_bond0  172.31.250.100
  255.255.255.0 172.31.250.1  #Enter the addresses according to
your actual needs.
```

4. Run the following commands in sequence to change the IP address of the MN:

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110   #
Here, 172.31.250.110 is the new IP address of the MN.
[root@localhost ~]# zstack-ctl restart_node    #Restart the MN for
 the configuration to take effect.
```

5. Log in to the UI, and change the IP address of the host and backup storage, respectively.

Note:

- Changing the IP address of a host may cause the host to be disconnected. Please exercise caution.
- After you change the IP address of a backup storage, you cannot perform operations on resources on the backup storage during the reconnection.

- Scenario 2: The management node and storage node share the same server. Here, the storage node uses the Ceph distributed deployment method.

1. In the MN, run the following command to back up the database:

```
[root@localhost ~]# zstack-ctl dump_mysql
```

2. Change the management IP address of the Ceph storage.
3. Run the following commands in sequence to change the IP address of the MN:

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110   #
Here, 172.31.250.110 is the new IP address of the MN.
[root@localhost ~]# zstack-ctl restart_node    #Restart the MN for
 the configuration to take effect.
```

- Scenario 3:

The management node, compute node, storage node, and backup storage share the same server. Here, the storage node uses the Ceph distributed deployment method.

1. In the MN, run the following command to back up the database:

```
[root@localhost ~]# zstack-ctl dump_mysql
```

2. Log in to the UI. On the **Hardware** page, place the target host into maintenance mode and disable the target backup storage.
3. Change the management IP address of the Ceph storage.

4. Run the following commands in sequence to change the IP address of the MN:

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110   #
Here, 172.31.250.110 is the new IP address of the MN.
[root@localhost ~]# zstack-ctl restart_node    #Restart the MN for
 the configuration to take effect.
```

5. Log in to the UI, and change the host IP address, backup storage IP address, and monitor IP address of the Ceph primary storage in sequence.

Note:

- Changing the IP address of a host may cause the host to be disconnected. Please exercise caution.
- After you change the IP address of a backup storage, you cannot perform operations on resources on the backup storage during the reconnection.
- The monitor IP address of a Ceph primary storage or backup storage cannot be changed. For more information, contact the official technical support.

14.3.2 Multi-MN HA Scenario

If the IP address of the server where a MN is located changes, change the IP address of the MN by following these steps:

1. In a MN, run the following command to back up the database:

```
[root@localhost ~]# zstack-ctl dump_mysql
```

2. Run the following commands in each MN to manually change the NIC addresses of all servers. (Here, assume that bond0 is the management network.)

```
[root@localhost ~]# zs-restore-network-setting -i br_bond0  #Clear
the IP address of the bridge.
[root@localhost ~]# zs-show-network     #Check whether the IP
address is successfully cleared.
[root@localhost ~]# zs-network-setting -i br_bond0  172.31.250.100
255.255.255.0 172.31.250.1  #Enter the addresses according to your
actual needs.
```

3. In each MN, run the following commands in sequence to change the IP address of each MN:

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110  #Here
, 172.31.250.110 is the new IP address of the MN.
[root@localhost ~]# zstack-ctl restart_node    #Restart the MN for
the configuration to take effect.
```

4. In the MN of the backup database, run the **`install_ha`** command to reinstall the HA suite. For more information, see *Specify Command Line*.

More Information

If the server where a MN is located is added as another node at the same time, update the IP address of the corresponding node by following these steps:

- Scenario 1: The management node, compute node, and backup storage share the same server.

  1. Log in to the UI. On the **Hardware** page, place the target host into maintenance mode and disable the target backup storage.
  2. In a MN, run the following command to back up the database:

     ```
     [root@localhost ~]# zstack-ctl dump_mysql
     ```

  3. Run the following command in each MN to manually change the NIC address of all servers. (Here, assume that bond0 is the management network.)

     ```
     [root@localhost ~]# zs-restore-network-setting -i br_bond0  #Clear
      the IP address of the bridge.
     [root@localhost ~]# zs-show-network     #Check whether the IP
     address is successfully cleared.
     [root@localhost ~]# zs-network-setting -i br_bond0  172.31.250.100
       255.255.255.0 172.31.250.1  #Enter the addresses according to
     your actual needs.
     ```

  4. In each MN, run the following commands in sequence to change the IP address of each MN:

     ```
     [root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110  #
     Here, 172.31.250.110 is the new IP address of the MN.
     [root@localhost ~]# zstack-ctl restart_node    #Restart the MN for
      the configuration to take effect.
     ```

  5. Log in to the UI by using the MN IP address of the backup database, and change the IP address of the corresponding host and backup storage, respectively.
  6. In the MN of the backup database, run the **`install_ha`** command to reinstall the HA suite. For more information, see *Specify Command Line*.

- Scenario 2: The management node and storage node share the same server. Here, the storage node uses the Ceph distributed deployment method.

  1. In a MN, run the following command to back up the database:

     ```
     [root@localhost ~]# zstack-ctl dump_mysql
     ```

  2. Log in to the UI by using a VIP. On the **Hardware** page, place the target host into maintenance mode, and disable the target primary storage and backup storage. On the **Resource Pool** page, disable the VM instance.

3. Change the management IP address of the Ceph storage.
4. In each MN, run the following commands in sequence to change the IP address of each MN:

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110  #
Here, 172.31.250.110 is the new IP address of the MN.
[root@localhost ~]# zstack-ctl restart_node    #Restart the MN for
 the configuration to take effect.
```

5. In the MN of the backup database, run the **`install_ha`** command to reinstall the HA suite. For more information, see *Specify Command Line*.

> **Note:**
> Modifying an IP address in Ceph scenarios is a heavy operation. Please contact the official technical support for help.

- Scenario 3:

The management node, compute node, storage node, and backup storage share the same server. Here, the storage node uses the Ceph distributed deployment method.

1. In a MN, run the following command to back up the database:

```
[root@localhost ~]# zstack-ctl dump_mysql
```

2. Log in to the UI by using a VIP. On the **Hardware** page, place the target host into maintenance mode, and disable the target primary storage and backup storage. On the **Resource Pool** page, disable the VM instance.
3. Change the management IP address of the Ceph storage.

> **Note:**
> Modifying an IP address in Ceph scenarios is a heavy operation. Please contact the official technical support for help.

4. In each MN, run the following commands in sequence to change the IP address of each MN:

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110  #
Here, 172.31.250.110 is the new IP address of the MN.
[root@localhost ~]# zstack-ctl restart_node    #Restart the MN for
 the configuration to take effect.
```

5. Log in to the UI by using the MN IP address of the backup database, and change the corresponding host IP address, backup storage IP address, and the monitor IP address of the Ceph primary storage.

> **Note:**
> If the type of the backup storage is Ceph, change the monitor IP address of the Ceph backup storage. For more information, contact the official technical support.

6. In the MN of the backup database, run the **`install_ha`** command to reinstall the HA suite. For more information, see *Specify Command Line*.
7. Log in to the UI by using a VIP. On the **Hardware** page, enable the backup storage, primary storage, and host. On the **Resource Pool** page, enable the VM instance.

14.4 Switch MN

To switch MNs, follow these steps:

1. Log in to the original MN, and run the following command to copy the database of the original MN to the `/root/` directory:

```
[root@localhost ~]# zstack-ctl dump_mysql #Back up the database.
Assume that the database backup file is /var/lib/zstack/mysql-backup
/zstack-backup-db-2018-12-13_17-57-52.gz.
[root@localhost ~]# cp /var/lib/zstack/mysql-backup/zstack-backup-db
-2018-12-13_17-57-52.gz /root #Copy the backup file to the /root/
directory.
```

2. In the new MN, install ZStack with the same version as the original MN and add a license to the new MN.

3. In the original MN, run the following command to stop the MN service:

```
[root@localhost ~]# zstack-ctl stop
```

4. In the original MN, run the following command to copy the database backup file of the original MN to the new MN:

```
[root@localhost ~]# scp /root/zstack-backup-db-2018-12-13_17-57-52.
gz root@new MN IP address:/root
```

5. In the new MN, run the following command to restore the database:

```
[root@localhost ~]# zstack-ctl restore_mysql -f /root/zstack-backup
-db-2018-12-13_17-57-52.gz --mysql-root-password zstack.mysql.
password   #zstack.mysql.password is the password of the database.
```

6. In the new MN, run the following command to start the MN:

```
[root@localhost ~]# zstack-ctl start
```

7. Optional. Verify that the services in the new MN are running properly. Then, run the following command to delete directories in the original MN to ensure data security:

```
[root@localhost ~]#  rm –rf /user/local/zstack
```

14.5 Upgrade Compute Node to MN

To upgrade a compute node to a management node (MN), follow these steps:

1. In the target compute node, run the following commands in sequence to check whether the processes are idle:

```
[root@localhost ~]# lsof +d /usr/local/zstack/     #Check the
resource usage in the processes.
[root@localhost ~]# ps aux|grep usr.local.zstack     #Check whether
the folder is used by a process.
```

2. Stop the host to be upgraded as a MN.
3. In the original MN, run the following command to stop the MN:

```
[root@localhost ~]# zstack-ctl stop
```

4. In the target compute node, run the following commands in sequence to stop the agent service:

```
[root@localhost ~]# systemctl stop zstack-sharedblock-agent;
[root@localhost ~]# /etc/init.d/zstack-network-agent stop;
```

```
[root@localhost ~]# kill -15 `pgrep dnsmasq`
```

5. In the target compute node, run the following commands in sequence to upgrade the compute node to a MN:

```
[root@localhost ~]# mv /usr/local/zstack/ /mnt/    # mv /usr/local/
zstack/ /mnt/
[root@localhost ~]# bash ZStack-install.bin -E     #Upgrade the
compute node to a MN.
[root@localhost ~]# cp -r /mnt/zstack/* /usr/local/zstack/     #Copy
 the original file to usr/local/zstack/.
```

6. Start the host and perform subsequent optional operations, for example, replace this MN with the original MN, or deploy multiple MNs.

15 Basic Maintenance

This chapter mainly describes how to troubleshoot ZStack abnormal basic operations.

15.1 Installation and Deployment

If you fail to install, deploy, and upgrade ZStack, troubleshoot the following:

1. When installing an operating system, you select ZStack Enterprise Management Node. However, after installation, you have not installed ZStack.

   Cause

   - The minimum hardware requirement is not met (4-core CPU or 8-G memory).
   - When installing the operating system, you have not configured a proper IP address. This is because the ZStack management node must have available IP addresses.

   Solution

   - At this time, run `bash /opt/zstack*installer.bin -E` to install ZStack Enterprise.
   - Or, run `bash /opt/zstack*installer.bin` to install ZStack Community.

2. When you install ZStack, the following error is reported:

   Symptom

   ```
   Fail Reason: /usr/local/zstack is existing. Please delete it
   manually before installing a new ZStack
   ```

   Cause

   At this time, the system has ZStack installed without allowing you to reinstall the Cloud.

   Solution

   - If you want to upgrade the Cloud, use **`-u`** directly.
   - If you want to reinstall the Cloud, run `rm -rf /usr/local/zstack; bash zstack-installer.bin -D`.

3. After you fail to install and deploy the Cloud, the failure information will be displayed on the screen.

   Solution

   Check *`/tmp/zstack_installation.log`*. Based on the error tips, try to address this problem by yourself.

4. During upgrade, ZStack ISO versions are incompatible and, then, the following error will be reported:

   Cause:

   ```
   mount: /dev/loop0 is write-protected, mounting read-only
   /root
   Current release c76 not matched the new ISO c74,
   Use zstack-upgrade -r xxx.iso to update current repo,
   Use zstack-upgrade -a/--add_repo xxx.iso to add a new repo
   ```

   Solution

   To solve this problem

   1. Download the latest ISO image on your management node. For example, run the following command on the management node:

      ```
      wget http://cdn.zstack.io/product_downloads/iso/ZStack-x86_64-DVD-
      3.10.0-c76.iso
      ```

   2. Run the following command to upgrade the Cloud. Yum repositories that are upgraded in the ISO image will be synchronized locally, and then the management node can be upgraded directly.

      ```
      zstack-upgrade ZStack-x86_64-DVD-3.10.0-c76.iso
      ```

5. When you upgrade ZStack, custom developments or database modifications will cause upgrade failure. Hence, you want to restore the original ZStack.

   Prerequisites

   When you upgrade ZStack, the currently core files and the database default to be backed up to a corresponding directory.

   1. ZStack core files will be backed up to the *`/usr/local/zstack/upgrade/`* directory, and their file name will be named after the time when the Cloud is upgraded. Assume that the file name is **2017-11-09-15-41-52**.
   2. The database defaults to be backed up to the *`/usr/local/zstack/db_backup/`* directory, and their file name will be named after the time when the Cloud is upgraded. Assume that the file name is **2017-11-09-15-42-43**, while the backup file is **backup.sql**.

   Procedure

1. Back up the former version of the ZStack core files, and run the following command:

```
cp /usr/local/zstack/upgrade/2017-11-09-15-41-52 /root -r
```

2. Back up the former version of the database, and run the following command:

```
cp /usr/local/zstack/db_backup/2017-11-09-15-42-43/backup.sql /
root
```

3. Back up the current database again, and run the following command:

```
zstack-ctl dump_mysql
```

4. Delete the current ZStack environment, and run the following command:

```
zstack-ctl stop
rm -rf /usr/local/zstack
```

5. Use the former installation package to install ZStack directly:

```
bash ZStack-enterprise-installer.bin -D
```

6. Restore the ZStack core files backed up in the step 1:

```
zstack-ctl stop
mv /usr/local/zstack/apache-tomcat/webapps/zstack /usr/local/
zstack/apache-tomcat/webapps/zstack-bk
cp /root/2017-11-09-15-41-52/zstack /usr/local/zstack/apache-
tomcat/webapps  -r
chown zstack:zstack /usr/local/zstack/apache-tomcat/webapps/zstack
 -R
```

7. Restore the database backed up in the step 2:

```
cat /root/backup.sql |mysql -u root -pzstack.mysql.password zstack
```

8. Start the ZStack management node. At this time, ZStack has restored successfully to the version before the original version failed.

```
zstack-ctl start
```

6. If you install ZStack via the All-in-One method, we recommend that you set **ReservedMemory**. The following are three types of granular methods to set the reserved memory for a host:

- **Global Settings**

  Navigate to **Settings** > **Global Settings** > **Basic Settings**, and set **ReservedMemory**. Default value: 1G.

  Note:

If your cluster or host has been configured with this option, this global setting will not take effect for this cluster or host.

- **Cluster**

  Navigate to **Hardware** > **Cluster**, and select a cluster to go to the cluster details page. On the **Global Settings** tab page, set **ReservedMemory**. Default value: 1G.

  Note:
  If your host has been configured with this option independently, the global setting for this cluster will not take effect for this host.

- **Host**

  Currently, you can set the reserved memory for a single host via CLI. For example,

```
UpdateResourceConfig category=kvm name=reservedMemory resourceUuid
=e2f4836723a2490095768fe611c540b1 value=10G
# resourceUuid is the UUID of the host, while the value is the
reserved memory of the host.
```

15.2 Start Service

After the related ZStack services are rebooted on your management node, these services will be started automatically.

If you fail to start the ZStack service, troubleshoot the following:

1. The database works properly.

   Run `systemctl status/start/stop/restart mariadb` to check the status of, or start, stop, and reboot the database.

2. The following error is reported:

   Symptom

```
ERROR: failed to connect to the mysql server[hostname:10.0.0.18,
port:3306, user:zstack, password:zstack.password]
```

   Solution

   - Ensure that the IP addresses, user name, and password related to the database under the *`/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`* file path are all correct, and the database can be accessed via the **`mysql`** command.

- For example, run `mysql -u zstack -pzstack.password -h 10.0.0.18` to access the database directly.

3. The following error is reported:

   Symptom

   ```
   8080 is occupied by some process. Please use netstat to find out and
    stop it
   ```

   Solution

   Run `netstat -anp|grep 8080` to find the program that is occupied by port 8080 and then to stop port 8080 before starting ZStack.

4. The following error is reported:

   Symptom

   ```
   MN status: Unknown, the management node seems to become zombie as it
    stops responding APIs
   ```

   Cause and **Solution**

   Generally, memories are out of capacity, so the message bus is not correctly handled. Expand the memories. At this time, we recommend that you not use the management node to act as a compute node and add this compute node to ZStack.

15.3 zstack-ctl Commands

ZStack lets you manipulate services or resources via **`zstack-ctl`**.

The following are common **`zstack-ctl`** commands:

- Check status: `zstack-ctl status`
- Manipulate service: `zstack-ctl stop/start/stop_ui/start_ui/start_node/stop_node/restart_node/`
- Collect log: `zstack-ctl configured_collect_log`
- Back up database: `zstack-ctl dump_mysql`
- Restore database: `zstack-ctl restore_mysql -f back.gz --mysql-root-password password`
- Change IP address for management node: `zstack-ctl change_ip`
- Check configuration: `zstack-ctl show_configuration`
- Check UI configuration: `zstack-ctl show_ui_configuration`

- Install license: `zstack-ctl install_license -f license_key.txt`
- Reset admin password: `zstack-ctl reset_password`
- Change database password: `zstack-ctl change_mysql_password --root-password zstack.mysql.password --user-name zstack --new-password password`

Note:

For more information about **`zstack-ctl`** commands, see zstack-ctl Command Manual in *ZStack Documentation*.

15.4 zstack-cli Commands

ZStack lets you manipulate its various internal resources via **`zstack-cli`**.

1. **Log in to `zstack-cli`:**

   ```
   LogInByAccount accountName=admin password=password
   ```

   The original password is **password**. If you have modified the password, enter the correct password.

2. **`zstack-cli` supports the following two types of keywords:**

   - Resource:

     ```
     zone cluster host vm primarystorage image L2 L3 backupstorage volume offering
     ```

   - Operation:

     ```
     add reconnect start stop destroy delete create get set update attach detach
     ```

3. **Manipulate resources via `zstack-cli`:**

   - Enter a resource keyword and an operation keyword.
   - Use the **Tab** key wisely. For example, enter the keyword cluster for a cluster, and press the **Tab** key twice. Then, all operations supported by this cluster will be displayed as follows:

     ```
     AttachL2NetworkToCluster
     AttachPrimaryStorageToCluster
     ChangeClusterState
     CreateCluster
     DeleteCluster
     DetachL2NetworkFromCluster
     DetachPrimaryStorageFromCluster
     GetCandidateZonesClustersHostsForCreatingVm
     GetVmStartingCandidateClustersHosts
     QueryCluster
     QueryVCenterCluster
     UpdateCluster
     ```

Assume that you want to create a cluster. Based on the supported operations, after you enter `CreateCluster`, press the **Tab** key again. Then, the CreateCluster parameter will be displayed.

4. **Create a VM instance via `zstack-cli`:**

```
CreateVmInstance name=ceph instanceOfferingUuid=$instanceofferUuid
l3NetworkUuids=$L3Uuid imageUuid=$imageUuid
```

5. **Query the running VM instances via `zstack-cli`:**

```
QueryVmInstance state="Running" name~=test limit=3 fields=uuid
```

The name of VM instances includes test, and three pieces of records and the corresponding UUIDs will be displayed.

Note:

For more information about **`zstack-cli`** commands, see zstack-cli Command Manual in *ZStack Documentation*.

15.5 VM Instance Abnormality

Workflow for Creating VM Instance and Analysis of Creation Failure

The following is the basic workflow for creating a VM instance:

1. If you select an image, you can associate the backup storage where the image resides. Make sure that this backup storage is connected.
2. After you select the backup storage, you can choose an available cluster. Additionally, based on the corresponding cluster and instance offering, you can select an available host. Make sure that this host is connected.
3. Based on the virtual size of this image, you can select an available primary storage and decide whether the capacity of this primary storage is sufficient. Make sure that this primary storage is available, connected, and sufficient.
4. If you select a network, you can configure the corresponding an IP address and an MAC address. Make sure that this network works normally, and your IP address pool has sufficient IP addresses.
5. Images are downloaded to the LocalStorage primary storage from the backup storage. These images that are stored to the primary storage as image caches can be used to create root volumes.

6. Assign an IP address for a VM instance.
7. Start the VM instance on the host.

When you fail to create the VM instance, troubleshoot the following:

1. The backup storage is disconnected. Check whether the backup storage is available and connected.
2. The primary storage does not attach any cluster, so no available hosts are found. Make sure that the primary storage attaches a cluster.
3. No hosts are available on the cluster to meet the requirements of the instance offering. Make sure that hosts are available and have the required resources.
4. The primary storage is out of capacity so that this primary storage cannot provide the required virtual capacity for these images. Make sure that the primary storage has sufficient resources.
5. The cluster does not attach the corresponding network. Make sure that the cluster attaches the corresponding network.
6. The IP address pool does not have sufficient IP addresses. Make sure that IP ranges are sufficient.
7. When images are downloaded to the backup storage from the primary storage, this downloaded link is abnormal. Make sure that this link is normal.
8. Make sure that the distributed DHCP service and the dnsmasq service work properly to provide normal IP assignment services.
9. Make sure that the libvirtd service works normally to provide the virtualization service.

Solutions

Abnormal Information	Cause and Solution
`“code”:”HOST.1005”,”description”:”Failed to start vm on hypervisor”, “details”:”failed to start …., Libvirt error: internal error no supported architecture for os type ‘hvm’”or "details": "failed to start vm on kvm host, because unable to start vm, libvirt error: invalid argument: could not find capabilities for domaintype=kvm "`	• **Cause** The host must support and enable hardware virtualization such as VMX or SVM. The possible cause is that CPU virtualization is not enabled on BIOS. • **Solution** Reboot the system, and enable the CPU related virtualization on BIOS.

Abnormal Information	Cause and Solution
`“details”: "cannot find either 'vmx' or 'svm' in /proc/cpuinfo, please make sure you have enabled virtualization in your BIOS setting"`	• **Cause** The host must support and enable hardware virtualization such as VMX or SVM. The possible cause is that the CPU of the added host does not support the hardware virtualization feature. The added host is a VM instance. Ensure that you enable nested virtualization corresponding to the VM instance. • **Solution** For more information, contact the provider of the VM instance.
`"details": "the local primary storage has no hosts with enough disk capacity[xxx bytes] required by the vm[uuid:xxx]"`	• **Cause** The current system (or any single host) does not have sufficient capacities of the primary storage (disk space). When ZStack allocates VM instances and volumes, thin clones are used. That is, the system will allocate the corresponding capacity based on what the VM instance requires. However, when you create a VM instance, the capacity of the system primary storage will be deducted based on the maximum applied space defined by the VM instance. In that case, the space finally used by the VM instance will not exceed the system available space. Besides, assume that the primary storage is LocalStorage. Disks of the VM instance cannot be migrated across hosts, so if no sufficient space is left on each host to create a new VM instance, this error will still be reported. • **Solution**

Abnormal Information	Cause and Solution
	Delete some unnecessary VM instances and volumes. Or, modify the image size used by the VM instance. If you have grasped both the overprovisioning workflow and usage of a primary storage, you can also expand the overprovisioning ratio of the primary storage to obtain more overprovisioning spaces.
`"details": "unable to allocate hosts; due to pagination is enabled, there might be several allocation failures happened before; the error list is [{no host having cpu[x HZ], memory [xxx bytes] found}]"`	• **Cause** The current system (or any single host) does not have sufficient capacities of CPU or memory. • **Solution** Delete some unnecessary VM instances. Or, modify the size of the instance offering used by the VM instance. If you have grasped both the overprovisioning workflow and usage of a primary storage, you can also expand the overprovisioning ratio of the primary storage to obtain more overprovisioning spaces.
`"details": "failed to start vm[uuid:xxx name:xxx] on kvm host[uuid:xxx, ip:x.x.x.x], because unable to start vm[uuid:xxx, name:xxx], libvirt error: internal error: early end of file from monitor: possible problem: Cannot set up guest memory 'pc.ram': Cannot allocate memory" set up guest memory 'pc.ram':Cannot allocate memory"`	• **Cause** In the current system, the actual, available and physical memory is out of capacity so that this memory cannot be used to create a VM instance. When you encounter this error, if you expand the overprovisioning ratio, you still cannot create a larger capacity of memory. • **Solution** Downsize the instance offering of a VM instance and expand the memory size of the host. Or,

Abnormal Information	Cause and Solution
	increase the swap partition of the host, which will lower the system performance.
`"failed to migrate vm[uuid:xxx] from kvm host[uuid:xxx, ip:xxx] to dest host[ip:xxx], unable to migrate vm[uuid:xxx] to qemu+tcp://xxx/system, Unsafe migration: Migration may lead to data corruption if disks use cache != none"`	• **Cause** On the current Basic Settings, the disk cache mode of the VM instance is set to other modes, such as writethrough or writeback. The system decides that migrations with the cache mode is insecure. • **Solution** Ensure that the cache mode on the Basic Settings is set to none before migrations are performed.
`"description": "Failed to start vm on hypervisor",libvirt error: Unable to create tap device vnic15.0: Device or resource busy`	• **Cause** This compute node may be added repeatedly and has attached the VM instance that uses vnic15.0, so devices are in conflict. • **Solution** We recommend that when you add a host, ensure that you keep the host clean and clear. Or, ensure that you detach the running VM instances from the host.
`Permission denied: '/opt/zstack/nfsprimarystorage/prim-cd8075752a0b4c669afa79acfc433ca5/dataVolumes'`	• **Cause** When you create a VM instance or volume, the directory of the NFS primary storage does not have the read and write permission. • **Solution** Enable the read and write permission on the NFS primary storage.
`internal error: unable to execute QEMU agent command`	• **Cause**

Abnormal Information	Cause and Solution
`'guest-set-user-password': failed to set password: The user name could not be found.`	When you modify the password for the VM instance, the specified user name is not found. • **Solution** Ensure that you specify an existing user name.
`internal error: unable to execute QEMU agent command 'guest-set-user-password': The command guest-set-user-password has not been found`	• **Cause** When you modify the password for the VM instance, QEMU Guest Agent is not installed to the VM instance, or the version of the proxy agent is low. • **Solution** Run `qemu-ga -V` to check the version of QEMU Guest Agent. • For CentOS 7.2, the minimum required version is 2.3.0. • For Windows Server 2012 R2, the minimum required version is 0.12.1. • For Ubuntu 14.04, the minimum required version is 2.5. Default version: 2.0. You need to manually upgrade the version.
`"libvirt error: error from service: ListActivatableNames: Connection is closed"or " libvirt error: Activation of org.freedesktop.machine1 timed out"`	• **Cause** This error is usually caused by the inactive system DBUS process or abnormal DBUS. • **Solution** — Method 1: Reboot the ZStack host. Then, DBUS will be automatically recovered. — Method 2: Run the following commands on the host: **1.** Run `service systemd-machined restart`. **2.** Run `service libvirtd restart`.

Abnormal Information	Cause and Solution
	3. After running the preceding commands, reconnect the host via UI or CLI.
`{ "error": { "code": "HOST.1009", "description": "Failed to migrate vm on hypervisor", "details": "failed to migrate vm[uuid:90bb61f55e774f5f89c9e1ea46db7661] from kvm host[uuid:e5105c61114a4efe8bcc025f744226bd, ip:10.0.247.244] to dest host[ip:10.0.197.238], unable to migrate vm[uuid:90bb61f55e774f5f89c9e1ea46db7661] to qemu+tcp://10.0.197.238/system, internal error: Attempt to migrate guest to the same host localhost.domain.com" }, "createdTime": 1488170137857, "type": { "_name": "key.event.API.API_EVENT" }, "id": "e6bcd7c33ad9446b919e11cd647fc8dc" }`	• **Cause** Hostnames are identical on two hosts. When you migrate KVMs online, hostnames will be used to identify different hosts. In this case, hostnames can be used to decide which host is used for migrating these KVMs. If hostnames are identical, the system deems that the same host is used. • **Solution** Make sure that the hostnames cannot be identical. Run `hostnamectl set-hostname your_new_hostname` to set the hostnames.
`all mons failed to execute http call[/ceph/primarystorageolume/clone`	• **Solution** Reconnect primary storages (master-standby).
`failed to start vm[uuid:4ef5a9e4ae6441c7b046c384c3ae6f7f name:stack_local] on kvm host[uuid:d0d9800a09c34da4891e0cc624a0d349, ip:192.168.1.166], because Traceback (most recent call last): File "/var/lib/zstack/virtualenv/kvm/lib/python2.7/site-packages/kvmagent/plugins/vm_plugin.py", line 2721, in start_vm self._start_vm(cmd) File "/var/lib/zstack/virtualenv/kvm/lib/python2.7/site-packages/kvmagent/plugins/vm_plugin.`	• **Cause** The host-passthrough option is enabled on the management platform. • **Solution** Disable this option.

Abnormal Information	Cause and Solution
`py", line 2664, in _start_vm 'unable to start vm[uuid:%s, name:%s], libvirt error: %s' % (cmd.vmInstanceUuid, cmd.vmName, str(e))) KvmError: unable to start vm[uuid: 4ef5a9e4ae6441c7b046c384c3ae6f7f, name:stack_local], libvirt error: internal error: early end of file from monitor, possible problem: qemu-kvm: /root/rpmbuild/BUILD/qemu-2.6.0/target-i386/kvm.c:1736: kvm_put_msrs: Assertion `ret == n' failed.`	
`”code”:”SYS.1006”,description:An operation failed, details:failed to check physical network interfaces on lvm`	• **Cause** You fail to check the NIC for the host. • **Solution** Ensure that the cluster where this host resides has attached this L2 network. When this host is added, make sure that this host has attached this NIC.
`description": "A message or an operation timeout","details": "[Async Http Timeout] url: http://10.10.10.253:7272/init, timeout after 300000[MILLISECONDS], command: {\"uuid\":\"78183b0a46094e30bc8a6128b30ee8cb\",\"restartDnsmasqAfterNumberOfSIGUSER1\":0}"`	• **Cause** The IP address of the management node may not reach the external network. Generally, when servers with multiple NICs are installed with management services, you specify the NIC address of the first default route. • **Solution** Go to *`/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`*.

Abnormal Information	Cause and Solution
	Run **`management.server.ip = xxx.xxx.xxx.xxx`** to modify this IP address so that it can reach the external network
`failed: Error in connection establishment: net::ERR_CONNECTION_REFUSED`	• **Cause** The console proxy is not configured yet. • **Solution** Log in to UI. Navigate to **Platform Management** > **Console Proxy**, and set an IP address for the console proxy.
`Could not access KVM kernel module: No such file or directory failed to initialize KVM: No such file or directory.`	• **Cause** This VM instance does not support virtualization. • **Solution** Enable nested virtualization in advance.

15.6 Log Analysis

The following are the related log paths:

Log Type	Log Path	Belonged Server
Management node	*`/usr/local/zstack/apache-tomcat/logs/management-server.log`*	Management node
Management node UI	*`/usr/local/zstack/apache-tomcat/logs/zstack-ui.log`*	Management node
Console proxy	*`/var/log/zstack/zstack-console-proxy.log`*	Management node
management node deployment	*`/var/log/zstack/deploy.log`*	Management node
Shell command	*`/var/log/zstack/zstack.log`*	host
zstack kvmagent	*`/var/log/zstack/zstack-kvmagent.log`*	host
libvirt corresponded by a VM instance	*`/var/log/libvirt/qemu/vm_uuid.log`*	host

Log Type	Log Path	Belonged Server
System-basic	`/var/log/messages`	Management node/ host
ImageStore	`/var/log/zstack/zstack-store/zstore.log`	ImageStore
Ceph primary storage	`/var/log/zstack/ceph-primarystorage.log`	Ceph Mon node
Ceph backup storage	`/var/log/zstack/ceph-backupstorage.log`	Ceph Mon node
vRouter	`/home/vyos/zvr/zvr.log`	vRouter
Flat network	`/var/lib/zstack/dnsmasq/`	host

When you encounter an error during the common maintenance, troubleshoot the following:

1. Simply analyze the error based on the error information displayed on the UI.
   - For example, when you fail to create a VM instance, `no host found` is displayed. At this time, the possible cause is that no available hosts are found after you select the image running on the backup storage and then select the network on the selected cluster.

     Ensure that you check whether the cluster has available hosts, attaches the corresponding network, and attaches the corresponding primary storage.
2. Analyze the `/usr/local/zstack/apache-tomcat/logs/management-server.log` management node log about the error information.
   - Query the error information, and analyze the workflow when the abnormal event occurs according to the error context.
   - Also, you can query and analyze the error via APIs. For example, when you create a VM instance, you can run CreateVmInstance. Search this API on the management node, and then analyze the cause of the error successively.
3. Check the error information of the related agent logs based on the specific information of the error.
   - For example, check the proxy error logs when you manage the lifecycle of the VM instance under `/var/log/zstack/zstack-kvmagent.log`.

15.7 Port Occupation

ZStack occupied ports list as follows:

Port	Daemon	Description
25	master	Email server
53	dnsmasq	DHCP service
80	httpd	Web server
123	ntpd	NTP/Chrony time synchronization service
3306	mysqld	MySQL daemon
4100-4200	usbredirserve	USB redirection service
4369	epmd	Erlang port mapper daemon
4900	consoleproxy	Console proxy
5000	/bin/java	ZStack UI service (HTTP)
5345	lttng-sessiond	kernel tracing framework
5443	/bin/java	ZStack UI service (HTTPS)
5900	qemu-kvm	KVM console service
6080	websockify	Agent service of deployment server
7069	python	Monitoring data collection
7070	kvmagent	KVM Agent service
7171	sftpbackupstorage	SFTP backup storage service
7272	zstack-vyos agent	vRouter agent service
7758	python	Console proxy service
7761	python	Ceph backup storage
7762	python	Ceph primary storage
7770	python	Deployment server
7771	nginx	Agent service of deployment server
7772	nginx	Agent service of deployment server
8000	zstore	zstore ImageStore daemon
8001	zstore	zstore ImageStore daemon
8005	/bin/java	ZStack management service
8080	/bin/java	ZStack management service
8081	/bin/java	ZStack management service
8086	influxd	Monitoring data storage

Port	Daemon	Description
8088	influxd	Monitoring data storage
8090	nginx	ZStack management service (Bare Metal console proxy of management node)
9090	prometheus	Prometheus daemon
9091	pushgateway	Monitoring data cache (management node)
9092	pushgateway	Monitoring data cache (billing node)
9093	pushgateway	Monitoring data cache (Bare Metal deployment server)
9100	node_exporter	Monitoring data collection
9103	collectd_expo	Monitoring data collection
16509	libvirtd	libvirtd service
18081	zstack-hamon	Monitoring service of multi-MN HA

15.8 Network Script

A ZStack Custom ISO provides the following network scripts to let you simply configure networks:

1. Run `zs-show-network` to display the network status without setting additional parameters.

   That is, the network connectivity and the link aggregation status are displayed.

```
[root@localhost ~]# zs-show-network
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: vmnic0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast state UP qlen 1000
    link/ether fa:84:ba:34:92:00 brd ff:ff:ff:ff:ff:ff
    inet 172.20.54.194/16 brd 172.20.255.255 scope global vmnic0
       valid_lft forever preferred_lft forever
    inet6 fe80::f884:baff:fe34:9200/64 scope link
       valid_lft forever preferred_lft forever

-------------------------------------------------------------------
| Bond Name  | SLAVE         | BONDING_OPTS                      |
-------------------------------------------------------------------
```

2. Run `zs-network-setting` to configure the physical network. The following are two methods to configure the physical network:

a. Method 1:

```
# -i enables you to configure the network address for the
 interface.

zs-network-setting -i [interface] [ipaddress] [netmask] [gateway]
                       interface   IP address  netmask   gateway

# Example 1: zs-network-setting -i eth0 192.168.1.10 255.255.255.0
 192.168.1.1
# Example 2: zs-network-setting -i eth0.10 192.168.1.10
 255.255.255.0 192.168.1.1
```

b. Method 2:

```
# -b enables you to create a bridge and configure the network
 address based on the interface.

zs-network-setting -b [interface] [ipaddress] [netmask] [gateway]
                       interface   IP address  netmask   gateway

# Example 1: zs-network-setting -b eth0 192.168.1.10 255.255.255.0
 192.168.1.1
# Example 2: zs-network-setting -b eth0.10 192.168.1.10
 255.255.255.0 192.168.1.1
```

3. Run `zs-change-nic` to change the NIC name. After the change, the script will be configured to *`/etc/udev/rules.d/70-persistent-net.rules`*. After the host reboots, the NIC will be changed to the new name.

```
# -c enables you to change the physical interface name.

zs-change-nic -c [old-nic-name] [new-nic-name]
                  old NIC name  new NIC name

# Example: zs-change-nic -c eth0 em01
```

4. Run `zs-vlan` to configure a VLAN interface. The following are two methods to configure a VLAN interface.

a. Method 1: Create a VLAN.

```
# -c enables you to create a VLAN ID.

zs-vlan -c [nic-name] [vlan]
        specified NIC VLAN interface

# Example: zs-vlan -c zsnic0 10
```

b. Method 2: Delete a VLAN.

```
# -d enables you to delete a VLAN interface.

zs-vlan -d [nic-name] [vlan]
        specified NIC VLAN interface
```

```
# Example 1: zs-vlan -d zsnic0 10
# Example 2: zs-change-nic -c eth0 em01
```

Note:

- After you create the VLAN interface, the corresponding network configuration files will be created in `/etc/sysconfig/network-scripts/`. After the host reboots, the VLAN interface will still take effect. Deleting the VLAN interface will delete the corresponding network configurations.
- After you create the VLAN interface, if other devices communicate with each other via this port, refer to the VLAN configuration manual of the corresponding network device vendor. Then, allow this VLAN interface to transfer traffics.
- The following are several references for configuring common VLAN network device:
  - Huawei: Click *here*.
  - H3C: Click *here*.
  - Cisco: Click *here*.
  - Juniper Networks: Click *here*.

5. Run `zs-bond-lacp` to create or delete the link aggregation (network bonding). The following are two types of methods to configure a link aggregation:

   a. Method 1: Create a link aggregation.

   ```
   #-c enables you to create a bond interface.

   zs-bond-lacp -c [bond-name]
                 bond interface

   # Example: zs-bond-lacp -c bond0
   ```

   b. Method 2: Delete a link aggregation.

   ```
   #-d enables you to delete a bond interface.

   zs-bond-lacp -d [bond-name]
                bond interface

   # Example: zs-bond-lacp -d bond0
   ```

   Note:

   This command is used to create an interface based on IEEE 802.3ad LACP. This interface requires administrators to configure the port group of multiple switch ports on hosts.

6. Run `zs-nic-to-bond` to configure the link aggregation.

   a.
   ```
   #-a enables you to attacch a physical interfaec to the bond
    interface.

   zs-nic-to-bond -a [bond-name] [nic-name]
                 bond interface physcial interface

   # Example: zs-nic-to-bond -a bond0 em1
   ```

   b.
   ```
   #-d enables you to detach the physical interface from the bond
    interface.

   zs-nic-to-bond -d [bond-name] [nic-name]
                 bond interface  physcial interface

   # Example: zs-nic-to-bond -d bond0 em1
   ```

   Note:

   After you run this command, the interface is configured, and the relationship between the bond interface and the physical interface are displayed. For example,

   ```
   ---------------------------------------------------------------------------------
    | Bond Name | SLAVE(s) | BONDING_OPTS |

   ---------------------------------------------------------------------------------
    | bond0 | enp1s0f1 | miimon=100 mode=4 xmit_hash_policy=layer2+3
   |
    |       | enp1s0f0 |
   |

   ---------------------------------------------------------------------------------
   ```

   - Specifically, bond0 is the bond interface, while enp1s0f0 and enp1s0f1 are the physical interfaces. Also, the bonding relationship will be displayed.
   - Additionally, the physical port of the network devices corresponded by both enp1s0f0 and enp1s0f1 is composed of the port group. Administrators must configure the port group according to the network device model.
   - The following are several references for setting common port groups:
     - Huawei: Click *here*.
     - H3C: Click *here*.
     - Cisco: Click *here*.
     - Juniper Networks: Click *here*.

15.9 Delete Resource

Delete operations are highly risky on ZStack. Performing delete operations affects your data plane directly. In addition, mistaken delete operations may put you at risk of a great data loss. This topic mainly provides a summary of high-risk delete operations.

Table 15-1: Delete Scenarios

Operation	Description
Delete zone	Exercise caution. Deleting a zone will also delete all he subresources on the zone, including cluster, host, network, primary storage, and vCenter .
Delete cluster	• Deleting a cluster will also delete all the hosts residing on the cluster. • Exercise caution. If the cluster has attached a LocalStorage primary storage, deleting the cluster will also delete all the VM instances and volumes residing on the related hosts.
Delete host	• Deleting a host will stop all the VM instances residing on the host. • Exercise caution. If the cluster has attached a LocalStorage primary storage, deleting the cluster will also delete all the VM instances and volumes residing on the related hosts. • Exercise caution. If the host is specified as a conversion host, deleting the host will also delete the corresponding conversion host. Additionally, the running V2V job will be automatically cancelled on this conversion host.
Delete primary storage	Deleting a primary storage will also delete all the resources on the primary storage, including VM instance, volume, and snapshot.
Delete backup storage	Exercise caution. Deleting a backup storage will also delete all the images residing on the backup storage.
Delete VXLAN Pool	Deleting a VXLAN Pool will also delete all the VxlanNetwork networks and related L3 networks on the Pool.
Delete L2 network	Deleting an L2 network will also delete all the L3 networks and related routers on the L2 network and detach the corresponding VM NICs.
Delete public network	Exercise caution. Deleting an L3 network will also detach VM NICs that are using this network and will delete the corresponding vRouters, network services, and vRouter offerings.
Delete system network	Deleting a system network will also delete the related routers.
Delete private network	Deleting a private network will also detach the VM NICs that are using this network.

Operation	Description
Delete vCenter	Exercise caution. Deleting a vCenter will delete the related resources related to the vCenter.
Delete deployment server	Deleting a deployment server will expunge both the deploying Bare Metal instances and the deployed Bare Metal instances.
Delete vRouter	Exercise caution. Deleting a vRouter will place the related network services of VM instances into the unavailable status. To recover these network services, reboot the VM instances.
Delete vRouter image	Exercise caution. Deleting a vRouter image will disallow you to create routers.
Delete vRouter offering	Exercise caution. Deleting a vRouter offering will disallow you to create routers.
Delete VM instance	• After you delete a VM instance, the resources related to the VM instance will be deleted immediately. • After you delete the VM instance, its enable state will be marked as Deleted and moved to the Deleted tab page. The system defaults to delete this VM instance after 24 hours. • Exercise caution. If you choose to expunge this VM instance, the resources related to this VM instance will be expunged. This operation cannot be reversed. • When you delete the VM instance and select the added volumes, all the regular volumes attached by this VM instance will be deleted as well. Notice that shared volumes will not be deleted.
Delete volume snapshot	• Exercise caution. Assume that snapshots are created on primary storages such as LocalStorage, NFS, Shared Mount Point, and SharedBlock. These snapshots are stored as a tree structure. Deleting the root snapshot will also delete the snapshots on the branch of the tree structure. • The snapshots that are created on a Ceph primary storage are independent. Deleting a snapshot will not affect other snapshots. • The shared volumes that are created on a SharedBlock primary storage disallow you to create snapshots.
Delete drive	Deleting a drive will also detach the existing ISO on this drive.
Delete auto-scaling group	Exercise caution. Deleting an auto-scaling group will delete all the VM instances on the group.

Operation	Description
Delete security group	Deleting a security group will automatically delete all the security group rules and related security group services.
Delete VIP	Deleting a VIP will delete the network services related to this VIP.
Delete EIP	Deleting an EIP will automatically delete the EIP services. An EIP is created based on a VIP. If you want to delete the related VIPs, choose to delete the VIPs.
Delete port forwarding	Deleting a port forwarding rule will automatically delete the port forwarding services. The related VIP and other services on the VIP are not affected.
Delete load balancer	Deleting a load balancer will automatically delete all the listeners and the services related to the load balancer. The related VIP and other services on the VIP are not affected.
Delete listener	Deleting a listener will automatically delete the load balancing service provided by the listener.
Delete IPsec tunnel	Deleting an IPsec tunnel will automatically delete the IPsec tunnel service. The related VIP and other services on the VIP are not affected.
Delete alarm	Exercise caution. Deleting an alarm will also remove all the resources on the alarm and delete the alarming service of the alarm.
Delete scheduler	Deleting a scheduler will also detach the scheduled jobs on this scheduler. These scheduled jobs can be reattached to other running schedulers.
Delete resource stack	Exercise caution. Deleting a resource stack defaults to expunge all the resources created on the resource stack, including VM instance or volume.
Delete billing settings	• Deleting historical billing settings will not affect the corresponding billings. • After you delete the currently used billing settings, the corresponding bills will be generated once. Then, the bill is suspended. The billing time period: the time when the last bill is generated-the time when the delete operation takes effect.
Delete AccessKey	After the AccessKey is deleted, the API access permission authorized by the AccessKey will be invalid. Also, the console is not accessible.
Delete account	Exercise caution. When the delete policy is Delete (immediate delete), the VM instances and volumes owned by an account will be expunged . If the delete policy is Delay (deferred delete), the state of the VM instances and volumes on an account will be placed into Deleted

Operation	Description
	. Additionally, the owner of all the resources will be changed to an administrator.
Delete user in Enterprise Management	Exercise caution. If you delete a user, its ticket process will be unavailable.

15.10 Detach Resource

Detach operations are also highly risky on ZStack. This topic mainly provides a summary of high-risk detach operations.

Table 15-2: Detach Scenario

Operation	Description
Detach cluster from primary storage	Exercise caution. To detach a cluster from a primary storage, note the following: • All the VM instances, vRouters, and VPC vRouters residing on this primary storage will be stopped. • All the volumes residing on this primary storage cannot work properly .
Detach L2 network from cluster	After you detach an L2 network from a cluster, the NIC corresponded by a VM instance will be detached.
Detach primary storage from cluster	To detach a primary storage from a cluster, note the following: • All the VM instances, vRouters, and VPC vRouters residing on this primary storage will be stopped. • All the volumes residing on this primary storage cannot work properly .
Detach Bare Metal cluster	Exercise caution. Detaching a Bare Metal cluster will expunge the deploying Bare Metal instances. Additionally, the consoles of the deployed Bare Metal instances are not accessible.
Detach cluster from VXLAN Pool	Exercise caution. After you detach a cluster from a VXLAN Pool, the NIC corresponded by a VM instance will be detached.
Detach cluster from L2 network	Exercise caution. After you detach a cluster from an L2 network, the NIC corresponded by a VM instance will be detached.
Detach VPC vRouter from VPC network	To detach a VPC vRouter from a VPC network, ensure that no VM instance uses this VPC network.

Operation	Description
Detach volume	• Detach the added volumes from a VM instance. You can detach volumes from a running or stopped VM instance. • Exercise caution. Detaching volumes from a running VM instance will affect your business continuity.
Detach NIC from VM instance	• You can detach NICs or networks dynamically from a VM instance. • Exercise caution. Detaching NICs will unbind the related network services.
Detach ISO	• Detach the added ISO image from a VM instance. You can detach an ISO image from a running or stopped VM instance. Batch detaching is supported. • Exercise caution. Detaching an ISO image from a running VM instance may affect your business continuity.
Detach LUN	Detach the added LUN from a VM instance. You can detach an LUN device from a running or stopped VM instance.
Detach physical GPU	• When you detach a physical GPU device, hot swapping is supported. • Detaching a physical GPU from a running VM instance may result in a blue screen and system hang. We recommend that you detach the physical GPU after stopping the VM instance.
Detach vGPU	Detach a vGPU device from a VM instance. **Note:** To attach or detach a vGPU from a VM instance, place the VM instance into the Stopped state first.
Detach USB device	Detach a USB device from a VM instance. You can detach a USB device from a running or stopped VM instance.

16 Other Maintenance Scenarios in the Cloud

16.1 Configuration Maintenance

This chapter provides advanced users with guidance on configuration maintenance in some scenarios.

16.1.1 Upgrading Prometheus

ZStack uses Prometheus to provide data monitoring features. Currently, the following two Prometheus versions are supported by ZStack:

- Prometheus 1.8.2: This version is supported by all versions of ZStack.
- Prometheus 2.9.2: This version is supported by ZStack 3.5.0 and later versions. Compared with its earlier versions, Prometheus 2.9.2 greatly improves the system stability, resource usage, and functionality.

Version Upgrade Mechanism

When you upgrade ZStack, note that:

- If you upgrade ZStack from a version earlier than 3.5.0 to ZStack 3.5.0 or a later version, Prometheus 1.8.2 is used by default.
- If you upgrade ZStack from 3.5.0 or a later version, the existing Prometheus version does not change.
- If you install ZStack 3.5.0 or a later version for the first time, Prometheus 2.9.2 is used by default.

Switching Prometheus Versions

ZStack 3.5.0 and later versions support both Prometheus 1.8.2 and Prometheus 2.9.2. You can switch between these two versions by using the following methods:

- Run the following commands to switch from Prometheus 1.8.2 to Prometheus 2.9.2:

```
[root@localhost ~]# zstack-ctl configure Prometheus.versionMode=2.x
[root@localhost ~]# zstack-ctl restart_node
```

Note:

After you upgrade ZStack from a version earlier than 3.5.0 to ZStack 3.5.0 or a later version, if you re-enable Prometheus 2.9.2, the existing monitoring data would not be available. To make sure that the existing monitoring data is available when you enable Prometheus 2.9.2, run the following commands:

```
[root@localhost ~]# zstack-ctl configure Prometheus.versionMode=2.x
-compatible
[root@localhost ~]# zstack-ctl restart_node
```

- Run the following commands to switch from Prometheus 2.9.2 to Prometheus 1.8.2:

```
[root@localhost ~]# zstack-ctl configure Prometheus.versionMode=1.8.
2
[root@localhost ~]# zstack-ctl restart_node
```

- Run the following commands to disable Prometheus. Note that the monitoring data is not available after Prometheus is disabled.

```
[root@localhost ~]# zstack-ctl configure Prometheus.versionMode=none
[root@localhost ~]# zstack-ctl restart_node
```

Global Settings

Prometheus supports the following two global settings. You can configure the settings by going to **Settings** > **Global Settings** > **Advanced**.

- **Retention time of Monitoring data**: The number of months that the monitoring data can be retained locally. Maximum value: 12 months. Default value: 6 months.
- **Retention size of Monitoring data**: For Prometheus 2.9.2, you can set this parameter to limit the space used by the monitoring directory. Default value: 50 GB.

16.1.2 zstack.properties Core Configuration File

zstack.properties is a core configuration file of ZStack and is stored in each management node.

The zstack.properties file stores information such as the database URL, the user name and password for database access, and the IP address of the message bus. The content of the zstack.properties file in each management node is basically the same. You can obtain the path of the file by running the `zstack-ctl status` command.

If you use the default installation mode, the file is stored in *`/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`*.

zstack.properties Parameters

The following table lists the parameters in the zstack.properties file.

Table 16-1: zstack.properties

Category	Parameter	Description
Database	• Single-MN environment: DB.url = jdbc:mysql://Actual IP address of the MN:3306 • Dual-MN environment: DB.url = jdbc:mysql://VIP:3306	The URL and port of the database.
	DB.user = zstack	The user name of the database.
	DB.password = REoVaLs+sSFz5WKl8KVzjPQOt0gyL7MpkkIx6PjNB6urlpkp4U1rQsDkHGekirfG	The password of the database. Default password: zstack.password. **Note:** The Cloud encrypts the password of the database to ensure the account security.
SFTP backup storage	SftpBackupStorageFactory.agentPort = 7171	The port of the SFTP backup storage.
Ansible	Ansible.cfg.forks = 100	The forks value of Ansible.
	Ansible.cfg.host_key_checking = False	The host_key_checking value of Ansible.
	Ansible.cfg.pipelining = True	The pipelining value of Ansible.
	Ansible.keepHostsFileInMemory = false	Whether to reserve ansible/hosts in the memory.
	Ansible.cfg.ssh_connection.ssh_args = -C -o ControlMaster=auto -o ControlPersist=1800s	The SSH connection parameters of Ansible.
Message bus	CloudBus.serverIp.0 = 10.0.5.87	The IP address of the CloudBus server.
Log	org.jboss.logging.provider = slf4j	The log service provider.
Console	consoleProxyCertFile = /usr/local/zstack/zstack-ui/ui.keystore.pem	The console certificate.

Category	Parameter	Description
	consoleProxyOverriddenIp = 172.20.11.50	The external IP address of the console proxy.
	consoleProxyPort = 4900	The port of the console proxy.
ZWatch/SNS	• Single-MN environment: sns.systemTopic.endpoints.http.url = http://localhost:5000/zwatch/webhook • Dual-MN environment: sns.systemTopic.endpoints.http.url = http://VIP:5000/zwatch/webhook • Dual-MN environment: ticket.sns.topic.http.url = http://VIP:5000/zwatch/webhook	The system endpoint for receiving ZWatch notifications.
ZStack YUM	Ansible.var.zstack_repo = " zstack-mn,qemu-kvm-ev-mn"	The name of the YUM repository used by ZStack.
Management node (MN) service	• Single/Dual-MN environment: management.server.ip = Actual IP address of the MN • Dual-MN environment: management.server.vip = VIP	The IP address of the MN server.
chrony	chrony.serverIp.0 = 10.0.5.87	The IP address of the chrony server.
Default iptables rules of a KVM host	KvmHost.iptables.rule.0 = '-I INPUT -p tcp -m tcp --dport 1234 -j ACCEPT'	The preset iptables rules of the KVM compute node.
	KvmHost.iptables.rule.1 = '-I INPUT -p tcp -m tcp --dport 2345 -j ACCEPT'	The preset iptables rules of the KVM compute node.
ImageStore server	imagestore.backupstorage.primary.storage.priority = [{\"PS\":\"Ceph\"\, \"priority\":\"5\"}\, {\"PS\":\"LocalStorage\"\, \"priority\":\"10\"}]	Specifies the primary storage allocation priority for backup storages with the ImageStore type. The smaller the number, the higher the priority.

Notice

- For versions earlier than 3.2.0, you can configure the default API timeout in the zstack.properties file. For example,

  ```
  ApiTimeout.org.zstack.header.image.APIAddImageMsg = timeout::3h
  ```

  The above method also applies to 3.2.0. If you upgrade the Cloud to 3.2.0 or a later version, when you set the timeout for corresponding APIs in the global settings, you can use the API timeout configured in zstack.properties as the default value.

  Note:
  After you upgrade the Cloud to 3.2.0 or a later version, you can configure the API timeout in global settings instead of by using zstack.properties.

- From ZStack 3.3.0, you can set the AD/LDAP or email server connection timeout as needed. Method:

  Go to `/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`, and set the following parameters in the **zstack.properties** configuration file:

  - ```
    Ldap.addServer.connectTimeout = XX
    # Set the AD/LDAP connection timeout.
    ```
  - ```
    SNS.addEmailPlatform.connectTimeout = XX
    # Set the email server connection timeout.
    ```
  - ```
    SNS.addEmailPlatform.readTimeout = XX
    # Set the data read timeout for an email server.
    ```

  Note:

  - By default, the timeout value of the preceding three parameters is 5000. Unit: ms.
  - If you need to modify the timeout, run the **`zstack-ctl configure`** command. For example,

    ```
    [root@localhost ~]# zstack-ctl configure Ldap.addServer.
    connectTimeout = 10000
    [root@localhost ~]# zstack-ctl configure SNS.addEmailPlatform.
    connectTimeout = 10000
    [root@localhost ~]# zstack-ctl configure SNS.addEmailPlatform.
    readTimeout = 10000
    ```

    After the settings are completed, restart the management node by running the `zstack-ctl restart_node` command to take effect.
    ```

- From ZStack 3.3.0, you can set the memory name for ivshmem devices (also known as virtual PCI devices that implement memory sharing between VM instances and hosts). Method:

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

  ```
  Kvm.ivshmem.dev.prefix = nu_fsec-$prefix$VMUUID
  # Set a name for the shared memory.
  ```

- From ZStack 3.3.0, you can set the maximum number of concurrent threads for querying the total count of alarm messages. Method:

  Go to `/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`, and set the following parameters in the **zstack.properties** configuration file:

  - ```
    InfluxDB.query.alarmData.count.maxThreadNum = 30
    # Set the maximum number of concurrent threads for querying the
     total count of alarm messages triggered by the resource alarm.
    Default value: 30.
    ```
  - ```
    InfluxDB.query.eventData.count.maxThreadNum = 30
    # Set the maximum number of concurrent threads for querying the
     total count of alarm messages triggered by the resource alarm.
    Default value: 30.
    ```

- From ZStack 3.7.1, you can set the `zstack-hamon` port for the monitoring service in the multi-MN HA scenario. Method:

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

  ```
  Prometheus.zsha2ExporterPort = 18081
  # Set the zstack-hamon port for the monitoring service in the multi-
  MN HA scenario.
  # By default, port 18081 is the exporter of Prometheus.
  ```

- From ZStack 3.9.0, you can set the primary storage priority when the backup storage type is local storage. Method:

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

  ```
  imagestore.backupstorage.primary.storage.priority = [\{\"PS\":\"Ceph
  \"\, \"priority\":\"10\"}\, \{\"PS\":\"LocalStorage\"\, \"priority
  \":\"1\"}]
  ```

```
# With this configuration, the primary storage of the local storage
type is used for VM instances.
```

- From ZStack 3.10.0, you can set the log language as needed. Method:

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

  ```
  locale = en
  ```

16.1.3 zstack.ui.properties Core Configuration File

zstack.ui.properties is a core configuration file of ZStack UI and is stored in each management node.

The zstack.ui.properties file stores information such as the UI database URL, the user name and password for UI database access, and the port of the UI server. The content of the zstack.ui.properties file in each management node is basically the same.

If you use the default installation mode, the file is stored in *`/usr/local/zstack/zstack-ui/zstack.ui.properties`*.

The following table lists the parameters in the zstack.ui.properties file.

Table 16-2: zstack.ui.properties

Category	Parameter	Description
Management node (MN)	• Single-MN environment: mn_host = 127.0.0.1 • Dual-MN environment : mn_host = Actual IP address of the MN	The IP address of the MN. • In a single-MN environment, the default IP address is 127.0.0.1. • In a dual-MN environment, the default IP address is the actual IP address of a MN.
	mn_port = 8080	The port of the MN. Default port: 8080.
Webhook host	• Single-MN environment: webhook_host = 127.0.0.1 • Dual-MN environment: webhook_host = VIP	The IP address of the webhook host. • In a single-MN environment, the default IP address is 127.0.0.1.

Category	Parameter	Description
		• In a dual-MN environment, the default IP address is the VIP.
	webhook_port = 5000	The port of the webhook host. Default port: 5000.
UI server	server_port = 5000	The port of the UI server. Default port: 5000.
UI log	log = /usr/local/zstack/apache-tomcat/logs	The UI log folder. Default folder: *`/usr/local/zstack/apache-tomcat/logs`*.
UI HTTPS	enable_ssl = false	Enables/Disables the HTTPS method for UI login.
	ssl_keyalias = zstackui	The alias of the UI certificate. Default alias: zstackui.
	ssl_keystore = /usr/local/zstack/zstack-ui/ui.keystore.p12	The path of the UI certificate. Default path: *`/usr/local/zstack/zstack-ui/ui.keystore.p12`*.
	ssl_keystore_type = PKCS12	The type of the UI certificate. Default type: PKCS12.
	ssl_keystore_password = password	The private key password of the UI certificate. Default password: password.
Database	db_url = jdbc:mysql://10.0.5.87:3306	The URL of the UI database. Default URL: *`jdbc:mysql://10.0.46.243:3306`*.
	db_username = zstack_ui	The user name of the UI database. Default user name: zstack_ui.
	db_password = zstack.ui.password	The password of the UI database. Default password: zstack.ui.password.
UI server process	catalina_opts = -Xmx4096m	The maximum available memory of the UI service process.

16.1.4 Changing Password for Hardware Resources in the Cloud

ZStack has different hardware resources, such as hosts, Ceph primary storages, and backup storages. If a password changes in the operating system of these nodes, you need to change the corresponding password of the hardware resource in the ZStack UI. This ensures the Cloud use the correct password to connect corresponding hardware resources. Otherwise, the resources might be disconnected and unavailable, and an SSH connection error will be reported during the reconnection.

Method to change the password: In the ZStack UI, click on the corresponding node to expand the details page, and click the edit button next to the IP address of the node to change the IP address. Then, reconnect the node for the change to take effect.

16.1.5 Changing Physical Environment in Management Node

The authorization of ZStack matches the environment of your physical host. If you update the hardware configuration of your host in the management node, the authorization of ZStack might become invalid and the startup might fail. In this case, contact ZStack sales and technical support for help.

16.1.6 Database Backup and Recovery

The Cloud supports active and regular database backup to ensure the data security and prevent data loss.

- You can use the `zstack-ctl dump_mysql` command to back up the database.
- You can use the `zstack-ctl restore_mysql -f back.gz --mysql-root-password password` command to restore the database.
- By default, the **`crontab`** command is used to manage the backup and recovery jobs.
  - You can use the **`crontab -l`** command to view the automatic, scheduled backup jobs related to a management node.
  - You can use the **`crontab -e`** command to modify the backup policy. By default, the backup job is performed at 00:00 and 12:30 every day, and up to 14 latest backups are saved.
- By default, the backup file of the database is stored in *`/var/lib/zstack/mysql-backup/`*.

- We recommend that you use a remote backup policy to improve the security. As long as the database file exists, even if the related server of ZStack is down, the database file can be used for recovery.
- Note that the database backup might affect the fluency of management node operations.

16.1.7 Expanding Local Storage Capacity

Prerequisites

During the use of ZStack, if the local storage capacity is insufficient, you can expand the capacity by using the following method.

Context

The following is an example of how to expand the system primary storage `/zstack_ps`.

Procedure

1. Place the target host into maintenance mode.
2. Insert a new large-capacity disk into the host and format the partition. Assume that the device name is `/dev/sdc`.
3. Create a new directory `/new_volume` and run the following command to mount the disk you inserted in the preceding step:

   ```
   mount /dev/sdc1 /new_volume
   ```

4. Run the following command to copy the original disk files to the new disk:

   ```
   rsync -a /zstack_ps /new_volume/
   ```

5. Run the following command to unmount the `/zstack_ps` and `/new_volume` mount directories:

   ```
   umount /zstack_ps
   ```

```
umount /new_volume
```

6. Run the following command to mount the new large-capacity disk to the original primary storage directory:

```
mount /dev/sdc1 /zstack_ps
```

7. Modify `/etc/rc.d/rc.local` and add the following content:

```
mount /dev/sdc1 /zstack_ps
```

8. For `/etc/rc.d/rc.local`, grant the execute permission.

```
chmod +x /etc/rc.d/rc.local
```

9. In the Cloud UI, enable and reconnect the host, start the VM instances on the host, and verify that the data is still available after disk expansion.
10. After the storage is successfully expanded, you can remove the original disk and its internal data for other purposes.

16.1.8 Resizing Root Volume

ZStack allows you to resize the root volume of a VM instance that is in the running or stopped state to expand the storage capacity.

Resize Root Volume for VM

You can resize the root volume for a VM instance to extend the storage capacity 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 click **Actions** > **Resize Root Volume**. Then, you can resize the root volume as needed. Note that the new size takes effect immediately.
2. Click on a VM instance that is in the running or stopped state and go to the details page of the VM instance. On the **Configurations** tab page, click **Volume**, select the target root volume, and click **Actions** > **Resize Volume** to resize the root volume. Note that the new size takes effect immediately.
3. Click on a VM instance that is in the running or stopped state and go to the details page of the VM instance. On the **Configurations** tab page, click the target root volume. On the details page of the root volume, click the edit icon next to **Size**. Note that the new size takes effect immediately.

Note:

- The new size must be greater than the current size, and the increment must be equal to or greater than 4 MB.
- The new size must be a multiple of 4 MB. For example, if you set the new size to 37 MB, the actual size would be 40 MB.

The above steps only resize the root volume of a VM instance. You need to partition and resize the hard disk in the operating system of the VM instance for the VM instance to recognize the resized partition.

Partition and Resize Hard Disk in VM Operating System

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

Note:

- Before you resize a root volume, a snapshot is created for the current system by default to enhance the data security.
- Resizing a disk or volume has potential risks. For security reasons, we recommend that you plan a new partition for the increase.
- Resizing a disk or volume can only increase the capacity, not reduce the capacity.
- The increase 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 increase.
  - If the last partition is a swap partition, you can delete the swap partition first, add the increase to the last partition, and then rebuild a swap partition.

Here, we will introduce the resizing methods in different application scenarios:

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

   Note:

   - To use this method, you need to re-plan the current partition by using Live CD.
   - When you adjust partitions, exercise caution to prevent data loss.

Assume that your VM instance uses both an ext4 root partition (35 GB) and a swap partition (5 GB), and the total size is 40 GB. After the system is resized from 40 GB to 50 GB, you want to add the increase to the ext4 root partition.

Procedure:

1. Add a GParted ISO, which can be downloaded from the GPared official website *https://gparted.org/download.php*. We recommend that you download amd64.iso, which supports the 64-bit operating system.
2. After you add the ISO, set the boot sequence to CdRom > HardDisk, which means that the system boots from CdRom next time.
3. Use GParted Live CD to boot the system and open the VM console. After GParted boots, follow the instructions and press the Enter key until the graphical interface is displayed.
4. On the GParted interface, right-click the original swap partition to delete it. Then, resize the ext4 partition from 35 GB to 46 GB, and create a new swap partition for the unallocated 4 GB.
5. Shut down the VM instance, detach the ISO, and then start the VM instance.
6. Open the VM console and run the `df -h` command. Then, you will find that the root partition of the VM instance is resized 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
#Here, 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 the
 swap partition can be enabled automatically after the VM instance
 is started.
```

8. After you power off and restart the VM instance, the ext4 partition of the VM root volume is resized successfully, and the swap partition has 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 is suitable for 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 system from 100 GB to 120 GB, you want to add the increase 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 resizing, run the `fdisk /dev/vda` command to partition the increase, 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 capacity 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 restart the VM instance, the XFS system of the VM LVM partition is resized successfully, and the swap partition has 4 GB.

3. Resizing a Windows partition.

You can resize a Windows partition directly on the disk management page.

Note:

After you resize a Windows partition online, you need to scan the disk again.

16.2 Upgrading Shared Block Shared Volumes

To upgrade shared volumes of the Shared Block type, follow these steps:

1. Run the following command to query the detached Shared Block shared volumes that need to be upgraded, and make sure that these volumes need to be formatted.

```
[root@localhost ~]# zstack-ctl fix_sharedvolume --operation
convert_volume --admin-password password
```

2. Run the following command to convert the queried Shared Block shared volumes from the qcow2 format to the raw format:

```
[root@localhost ~]# zstack-ctl fix_sharedvolume --operation
convert_volume --admin-password password --dryrun False
```

3. Run the following command to query the original Shared Block shared volumes with the qcow2 format that can be deleted:

```
[root@localhost ~]# zstack-ctl fix_sharedvolume --operation
delete_qcow2_volume --admin-password password
```

4. Ensure the data integrity after format conversion, and then run the following command to delete the original Shared Block shared volumes with the qcow2 format:

```
[root@localhost ~]# zstack-ctl fix_sharedvolume --operation
delete_qcow2_volume --admin-password password --dryrun False
```

5. Run the following command to create image files from the snapshots in the Shared Block shared volumes and save the files as a backup:

```
[root@localhost ~]# zstack-ctl fix_sharedvolume --operation
commit_snapshot_to_image --admin-password password --backup-storage-
uuid  XXXXX  --dryrun False
```

6. Run the following command to delete the original snapshots with the qcow2 format:

```
[root@localhost ~]# zstack-ctl fix_sharedvolume --operation
delete_shared_volume_snapshots --admin-password password --dryrun
False
```

16.3 Changing Time in Ceph Enterprise

The method to change the time in Ceph Enterprise varies according to the versions of Ceph Enterprise. To change the time in Ceph Enterprise, **contact the official technical support**. The recommended method is as follows:

- For Ceph Enterprise 3.1.9 and later versions, follow these steps:

> **Note:**
> Before you change the time in Ceph Enterprise, make the following preparations:
>
> - Make sure that the Ceph status is **ok** and the UI server status is healthy.
> - Properly plan the time server roles to avoid secondary changes.

1. In all client nodes, use the following command to view the time synchronization status in the Ceph cluster to make sure that the time is synchronized:

```
[root@ Ceph ~]# chronyc sources -v   #The asterisk (*) in the
output indicates that the time is synchronized.
```

2. Manually change the time of the time service node, and then run the following command to restart the time service process:

> **Note:**
> Do not point this node client to the IP address of your time server.

```
[root@ Ceph ~]# service chronyd restart
```

3. After the time of the time service node is normal, run the following commands in the other node in the Ceph cluster to restart the chronyd service of the server, and check the time synchronization result.

```
[root@ Ceph-1 ~]# service chronyd restart
[root@ Ceph-1 ~]# chronyc sources -v   #The asterisk (*) in the
output indicates that the time is synchronized.
```

4. Run the following command in each node of the Ceph cluster to restart the xmsd service:

```
[root@ Ceph-1 ~]# systemctl restart xmsd
```

5. Run the following command to write the changed time into the server hardware:

```
[root@ Ceph ~]# hwclock -w
```

6. Verify that the time is successfully changed, specify the time node IP address (**chrony.serverIp.0 = XXX**. Here, XXX is the IP address of the time server node.) in the configuration file (`/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`) of the management node, and then run the `service chronyd restart` command to restart the time service in the management node.

Note:

After the time change operation is completed, you can check the result by using the following method:

- Use the `ceph -s` command to check whether the Ceph status is **ok**.
- Use the `chronyc sources -v` command to check whether the time is synchronized (that is, whether the output is *).
- Verify that the time is changed as expected, the status of each server in the storage UI is healthy, and the storage pool status is healthy.

- For Ceph Enterprise earlier than 3.1.9, follow these steps:

  1. Stop all VM instances, including the management node VM instances.
  2. Perform time synchronization and adjust the time.
  3. Run the `systemctl restart xmsd` command to restart the xmsd service in each node.
  4. Verify that the time is successfully changed, and specify the time node IP address (**chrony.serverIp.0 = XXX**. Here, XXX is the IP address of the time server node.) in the configuration file (`/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`) of the management node.
  5. Run the `service chronyd restart` command to restart the time service in the management node.

17 Physical Infrastructure Maintenance

This chapter provides some methods for physical infrastructure maintenance. In a production environment, you need to perform maintenance operations by referring to the procedures described in this document. Otherwise, uncontrollable risks will be caused.

17.1 Power Maintenance in Equipment Room

Planned Shutdown

To perform planned shutdown in an equipment room, follow these steps:

1. Stop all running businesses.
2. Place all primary storages into maintenance mode. After all primary storages enter maintenance mode, make sure that all VM instances are shut down.
3. Place all hosts into maintenance mode.
4. Stop the management node (MN). The methods to stop the MN in different scenarios are as follows:
   - In a single MN scenario, run the `zstack-ctl stop` command to stop the MN.
   - In a multi-MN (host) HA scenario, run the `zsha2 stop-node` command in each MN to stop the MNs and shut down the zsha2 service.
5. Verify that no I/O operation is performed in the primary storages of the Cloud, and run the `poweroff` command on each host to normally shut down all hosts.
6. Disable the storages, such as the NFS, Ceph, SAN, and SMP storages.
7. Disable the switches and other hardware facilities.

Planned Power-on

To perform planned power-on in an equipment room, follow these steps:

1. Power on the switches.
2. Power on the storages, such as the NFS, Ceph, SAN, and SMP storages.
3. Power on the server.
4. Check the service status of the MN and make sure that the MN service is started successfully. The methods to check the MN status in different scenarios are as follows:
   - In a single MN scenario, run the `zstack-ctl status` command to view the MN status.
   - In a multi-MN (host) HA scenario, run the `zsha2 status` command in one of the MNs to view the HA status and the MN status.

5. Log in to the ZStack Cloud, enable all primary storages and hosts and make sure that all hosts and primary storages are in the connected state.
6. Start the VM instances and resume the businesses.

Recovery from Unexpected Power Outage

The steps to recover from unexpected power outage in an equipment room are the same as those in planned power-on.

1. Power on the switches.
2. Power on the storages, such as the NFS, Ceph, SAN, and SMP storages.
3. Power on the server.
4. Check the service status of the MN and make sure that the MN service is started successfully. The methods to check the MN status in different scenarios are as follows:
   - In a single MN scenario, run the `zstack-ctl status` command to view the MN status.
   - In a multi-MN (host) HA scenario, run the `zsha2 status` command in one of the MNs to view the HA status and the MN status.
5. Log in to the ZStack Cloud, enable all primary storages and hosts and make sure that all hosts and primary storages are in the connected state.
6. Start the VM instances and resume the businesses.

17.2 Equipment Room Relocation

When you relocate an equipment room, perform maintenance by following these steps:

1. Power off all power supplies by referring to *Planned Shutdown*.
2. Mark the access ports of all switch wiring and hosts.
3. Pack the server, move the server to the new equipment room, and connect the server.
4. Power on all power supplies by referring to *Planned Power-on*.
5. Check the recovery status of the network, Cloud, and VM instances.

17.3 Switch Maintenance

Management Network Switch Maintenance

The maintenance on management network switches might affect the proper running of the business. **Please exercise caution.** If this kind of maintenance is necessary, we recommend that you perform this operation during off-peak hours. The maintenance procedure is as follows:

1. Turn off VM high availability in the global settings of the Cloud.

2. Stop the management node (MN). The methods to stop the MN in different scenarios are as follows:
   - In a single MN scenario, run the `zstack-ctl stop` command to stop the MN.
   - In a multi-MN (host) HA scenario, run the `zsha2 stop-node` command in each MN to stop the MN and the zsha2 service.
3. Adjust or restart related management switches.
4. Check the IP connectivity of all hardware resources (such as the host, primary storage, and backup storage) at the access end of the switch to ensure that all the management networks in the access end can communicate with each other properly.

   Note:
   If a node fails to connect to the MN, troubleshot this issue before you proceed with subsequent operations.
5. Start and check the MN service status to ensure that the MN service starts successfully. The methods to check the MN startup in different scenarios are as follows:
   - In a single MN scenario, run the `zstack-ctl start` command to start the MN service, and run the `zstack-ctl status` command to view the MN status.
   - In a multi-MN (host) HA scenario, run the `zsha2 start-node` command in each MN to start the MN service, and run the `zsha2 status` command to view the HA status and the MN status.
6. Make sure that all hosts and primary storages are in the connected state, and VM high availability is enabled in the global settings of the Cloud.

Business Network Switch Maintenance

We recommend that you perform maintenance on business network switches during off-peak hours to avoid affecting important services. The maintenance procedure is as follows:

1. Place the hosts accessed to the switches into maintenance mode.
2. Adjust or restart related service switches.
3. Start a host that is in maintenance mode and check the connectivity. For example, you can use this host to create a test VM instance and check the connectivity between this VM instance and other VM instances. If the connectivity succeeds, the switch interface configuration corresponding to this host is correct and available. If the network is unreachable, continue to check the connectivity.

4. Repeat Step 3 to check the connectivity in turn to ensure that all business networks are available.

Storage Network Switch Maintenance

The maintenance on storage network switches directly affects all the business. You must stop all business before you perform the maintenance. The maintenance procedure is as follows:

1. Place all primary storages associated with the storage switches on the Cloud into maintenance mode.
2. Log in to the UI of Ceph Enterprise and choose **Settings** > **Disable data recovery** > **Ban**.
3. Adjust or restart related storage switches.
4. Make sure that the storage networks of all storage nodes are interconnected and reachable.
5. Log in to the UI of Ceph Enterprise and choose **Settings** > **Enable Data Recovery** > **Enable**.
6. Enable the primary storages that are in the maintenance mode and make sure that the primary storages are in the connected state.
7. Start the stopped VM instances.

18 FAQ

18.1 Quick Start

1. Q: What can I do with ZStack Cloud?

   A:

   In general, the Cloud helps you easily create and manage VM instances and related network storage resources. For example,

   - You can obtain the usage of physical resources, such as processors, memories, storages, and networks in the Cloud in real time. You only need to create VM instances and the Cloud will immediately send alarms if resources are insufficient.
   - The Cloud allows you to copy templates before you create VM instances.
   - After you create a VM instance, the Cloud allows you to set or change the relevant IP address.
   - The Cloud supports flat networks, vRouter networks, and VPC networks. You can quickly set up flexible and diverse network scenarios as needed with simple clicks in the UI.
   - The Cloud can take over vCenter. Specifically, the Cloud can manage both KVM and VMware clusters at the same time. In addition, the Cloud supports the V2V migration of VM instances from vCenter to ZStack.
   - The Cloud allows different accounts to see different VM instances.
   - The Cloud supports advanced features such as billing.
   - You can directly add firewalls to VM instances on the Cloud and set various security policies , which is simple and convenient.
   - The Cloud supports advanced features, such as enterprise management, bare metal management, V2V migration, and backup service.

   In addition, ZStack has a lot of powerful features. Try ZStack Enterprise to find more highlights.

2. Q: What documents does ZStack provide? Which documents should I read?

   A: ZStack provides the following documents:

   - **Release Notes:**

     The release notes briefly describe the new features provided by ZStack during each release and detail the changes or enhancements made to the Cloud.

- **Product Manuals:**

  The product manuals include the **User Guide**, **Maintenance Manual**, **Technical Whitepaper**, **CLI Command Manual**, and **CTL Command Manual**. These manuals describe the functional architecture, functional advantages, installation and deployment, how to use the Cloud, and solutions to common problems during the O&M of ZStack. You will find a new world if you explore ZStack by using CLI.

- **Tutorials:**

  We provide you with many tutorials that cover various application scenarios, for example, Quick Start Installation Tutorial, Upgrade Tutorial, Multi-MN HA Tutorial, and V2V Migration Tutorial. With these tutorials, you can get started quickly and easily.

- **API Reference:**

  The API Reference, as the core of ZStack, helps you gain in-depth insight of ZStack from the API level.

- **FAQ:**

  The FAQ provides answers to a list of frequently asked questions during the use of the Cloud.

- **Blogs:**

  The blogs provide a place where you can voice your ideas and share your thoughts on ZStack as well as the cloud computing industry. Here, you can expand your horizon and have a more thorough understanding of IaaS.

Different users can find the most suitable documents here.

- **For beginners:**

  - First of all, we recommend that you learn some basic concepts of IaaS, and understand what ZStack is and what can it do.
  - Then, you can refer to the Quick Start Installation Tutorial to install the Cloud quickly.
  - After you installed the Cloud successfully, you can use it by referring to our tutorials. For example, you can try to deploy a flat network without virtual routing.
  - If you successfully created the first VM instance, you succeeded in taking the first step and could perform further operations.
  - Next, you can try some deployment scenarios according to the tutorials. Then, you will have a new understanding of various features and nouns in the UI.

- If you read the blogs carefully, you will find something new and more interesting.

- **For developers:**
  - If you are interested only in some features, refer to the **API Reference** to learn more about the APIs for secondary development.
  - You can also refer to the **CLI Command Manual** to deploy a ZStack environment by using CLI.
  - The **API Reference** and **CLI Command Manual** are necessary for developers. You can also find answers to some questions in the tutorials and blogs.
- **For experts:**
  - You can take a quick glance at the installation tutorial and then select an appropriate solution.
  - Maybe you have more interests in the **API Reference** and **Blogs**.
  - If you have any questions during the use of the Cloud, refer to the **FAQ**. If you did not find your answers, feel free to raise your questions in the ZStack community (QQ group numbers: 1046295840, 741300236, 443027683, and 410185063).

18.2 Installation and Deployment

1.
Q: What hardware environments does ZStack support?

A: ZStack supports x86 and ARM servers with hardware virtualization features, workstations or desktops, and mainstream Intel or AMD processors.

2.
Q: What operating systems does ZStack support?

A: ZStack supports ZStack Custom ISO that is deeply customized based on CentOS 7.4 or CentOS 7.6.

3.
Q: Can I install ZStack by using the standard CentOS 7.4 or CentOS 7.6 operating system?

A: Currently this is not supported. However, ZStack supports ZStack Custom ISO that is deeply customized based on CentOS 7.4 or CentOS 7.6.

4.
Q: How many servers are needed to install and deploy ZStack?

A: A minimum of one server is required. This server can act as the management node and compute node at the same time. In a production environment, we recommend that you install

the management node and compute node separately. ZStack can manage all hardware resources by using only one management node.

5. Q: What is the minimum server configuration requirement for installing and deploying ZStack?

   A: 4 CPUs, 8 GB memory, 200 GB primary storage, and 200 GB backup storage. Note that the minimum configuration is only applicable to test environments.

6. Q: What installation modes does ZStack Custom ISO support? What are the differences?

   A: ZStack Custom ISO supports the following installation modes:

   1. ZStack Enterprise Management Node

      Install the ZStack Custom ISO that is deeply customized based on CentOS 7.4 or CentOS 7.6 as well as the ZStack Enterprise management node.

   2. ZStack Community Management Node

      Install the ZStack Custom ISO that is deeply customized based on CentOS 7.4 or CentOS 7.6 as well as the ZStack Community management node.

   3. ZStack Compute Node

      Install the ZStack Custom ISO that is deeply customized based on CentOS 7.4 or CentOS 7.6 as well as the essential software package of ZStack compute node.

   4. ZStack Expert Node

      Install the ZStack Custom ISO that is deeply customized based on CentOS 7.4 or CentOS 7.6 and configure the local repo. You can customize the system usage as needed.

7. Q: How do I install ZStack Enterprise?

   A: Download the latest *ZStack Custom ISO*. If you are installing the system for the first time, we recommend that you select the Enterprise management node. After the operating system is installed, you can restart the operating system to automatically install the Enterprise management node.

8. Q: How do I upgrade ZStack Enterprise?

   A: To upgrade ZStack that you already deployed to the latest version, use one of the following methods. Here we take c76 as an example.

   - **Incremental upgrade:**

1. Obtain the latest bin installation package from *ZStack Official Website*: ZStack-installer-3.10.0.bin.
2. If the root password of the database is the default password, run the following command to upgrade the Cloud:

```
[root@localhost ~]# bash ZStack-installer-3.10.0.bin -u
```

If the root password of the database is a custom non-blank password, run the following command to upgrade the Cloud:

```
[root@localhost ~]# bash ZStack-installer-3.10.0.bin -u -P
 MYSQL_ROOT_PASSWORD
```

- **Offline upgrade:**

1. Obtain the latest ISO installation package from *ZStack Official Website*: ZStack-x86_64-DVD-3.10.0-c76.iso.
2. Obtain the latest upgrade script: *Upgrade script*.
3. Run the following command to upgrade the Cloud:

```
[root@localhost ~]# bash zstack-upgrade ZStack-x86_64-DVD-3.10.
0-c76.iso
```

Note:

The method to upgrade the c74 version is the same as that of the c76 version. Please obtain the installation package corresponding to the c74 version to upgrade.

9.

Q: How do I upgrade from an expert node to a management node?

A: Run the following commands:

```
[root@localhost ~]# yum --disablerepo=* --enablerepo=zstack-local
 install zstack-manager
[root@localhost ~]# bash ZStack-installer-3.10.0.bin -E
```

10.

Q: How do I upgrade from an expert node to a compute node?

A: Run the following command:

```
[root@localhost ~]# yum --disablerepo=* --enablerepo=zstack-local,
qemu-kvm-ev groupinstall zstack-host
```

11.

Q: How do I upgrade from a compute node to a management node?

A: Run the following commands:

```
[root@localhost ~]# rpm -e zstack-host
[root@localhost ~]# yum --disablerepo=* --enablerepo=zstack-local
 install zstack-manager
[root@localhost ~]# bash ZStack-installer-3.10.0.bin -E
```

12. Q: How do I upgrade a management node from ZStack Community to ZStack Enterprise?

    A: Obtain and use the latest Enterprise license.

13. Q: How do I reinstall ZStack?

    A:

    1. Run the following command to delete the original database:

       ```
       [root@localhost ~]# rm -rf /usr/local/zstack
       ```

       Note:
       This command will delete all the data under this directory. You can use this command only when you want to completely reinstall ZStack.

    2. Then, run the following command to reinstall the management node:

       ```
       [root@localhost ~]# bash ZStack-installer-3.10.0.bin -D #Install
        ZStack Enterprise.
       ```

14. Q: I installed ZStack as a root user. However, when I start the service, the system reports that I am not a root user. Why?

    A:

    - **Symptom:**

      When you install ZStack, you use root for login. However, when you start the service, the system reports that you are not a root user and `sudo` is required.

      ```
      ERROR: please use sudo or root user FAIL
       Reason: failed to start zstack
      ```

      When you run the following command in a Python CLI environment, you find that Python determined that you are not a root user.

      ```
      import getpass
       user = getpass.getuser()
      ```

```
print user
```

- **Cause:**

  When you switch from a regular user to a root user, you used `su` instead of `sudo su`. In this case, only the root user is switched but relevant environment variables are not switched.

- **Description:**

  - The `sudo` command can be used by the current user with the root super permission.
  - The `su` command can be used to switch to a root user. However, the relevant environment variables are not switched to the root directory.
  - The `sudo su` command is used to switch to a root user with the root permission.

15.

Q: In a multi-node deployment environment, can I use a VM instance as a node?

A: Yes, you can. Make sure that the network is connected. We recommend that you bridge the VM node with other nodes. In addition, the VM node is more suitable to act as a management node with a minimum of 4 CPUs and 8 GB memory.

16.

Q: Can I install ZStack on a ZStack VM instance?

A: Yes, you can. Method: Go to **Settings** > **Global Settings** > **Basic Settings**, locate **Vm.cpuMode**, and set the value to **host-passthrough**. Then, the virtualization feature of a host can be passed through.

17.

Q: After I perform one-click installation of ZStack, what should I do if the Cloud takes a long time to start up?

A:

- **Cause:**

  The startup time of the management node is related to the configuration resources of the node. The startup takes a long time only when you install ZStack on a VM instance.

- **Solution:**

  We recommend that you use more than 4 CPUs and 16 GB memory in a virtualization environment.

  Note:

The startup takes a long time does not indicate that the installation or startup fails. If a time out error is reported, use `zstack-ctl status` to check the status. If the status is **stopped**, use `zstack-ctl start` to start the service. If the status is **unknown**, use `zstack-ctl stop` to stop the service, and then use `zstack-ctl start` to start the service.

18.

Q: How do I change the installation directory of ZStack?

A: When you install ZStack, add **`-r destination directory`**. For example,

```
[root@localhost ~]# bash zstack-installer.bin -r /home/zstack
```

19.

Q: When I upgrade the Cloud, what should I do if the new version of ZStack Custom ISO does not match the old one?

A:

- **Symptom:**

  If the new version of ZStack Custom ISO does not match the old one during the upgrade, the following error message will be reported:

  ```
  mount: /dev/loop0 is write-protected, mounting read-only
  /root
  Current release c76 not matched the new ISO c74,
  Use zstack-upgrade -r xxx.iso to update current repo,
  Use zstack-upgrade -a/--add_repo xxx.iso to add a new repo
  ```

- **Cause:**

  The current ISO version used by the system is not suitable for upgrading the installation package. You need to upgrade the corresponding ISO and then upgrade ZStack.

- **Solution:**

  Follow these steps to perform the deployment. Here, we take c76 as an example.

1. Run the following command to download the latest upgrade script:

```
wget http://cdn.zstack.io/product_downloads/scripts/zstack-upgrade
```

2. Run the following command to download the latest ISO in the management node:

```
wget http://cdn.zstack.io/product_downloads/iso/ZStack-x86_64-DVD-3.10.0-c76.iso
```

3. Perform the upgrade. That is, upgrade the yum repo in the ISO and synchronize it to your local server. Then, directly upgrade the management node.

```
bash zstack-upgrade ZStack-x86_64-DVD-3.10.0-c76.iso
```

20.

Q: When I upgrade ZStack, the following error is reported: `The Operating System version is not suitable for zstack-enterprise installation.`. What should I do?

A: Use the latest *ZStack Custom ISO* for installation and upgrade.

21.

Q: During the upgrade of ZStack, if the upgrade fails due to secondary development or database adjustment, how can I restore the original ZStack?

A:

- **Prerequisite:**

  During the upgrade of ZStack, the core files and database of the current ZStack are backed up to the corresponding directory by default.

- **Procedure:**

  1. Back up the core files in ZStack of the previous version.

```
cp /usr/local/zstack/upgrade/2017-11-09-15-41-52 /root -r
```

  2. Back up the database of the previous version.

```
cp /usr/local/zstack/db_backup/2017-11-09-15-42-43/backup.sql /root
```

  3. Back up the database again.

```
zstack-ctl dump_mysql
```

  4. Delete the current ZStack environment.

```
zstack-ctl stop
```

```
rm -rf /usr/local/zstack
```

5. Use the previous installation package to directly install ZStack.

```
bash ZStack-installer-3.10.0.bin -D
```

6. Perform recovery by using the core files backed up in Step 1.

```
zstack-ctl stop
mv /usr/local/zstack/apache-tomcat/webapps/zstack /usr/local/
zstack/apache-tomcat/webapps/zstack-bk
cp /root/2017-11-09-15-41-52/zstack /usr/local/zstack/apache-
tomcat/webapps  -r
chown zstack:zstack /usr/local/zstack/apache-tomcat/webapps/
zstack -R
```

7. Restore the database backed up in Step 2.

```
cat /root/backup.sql |mysql -u root -p zstack.mysql.password
zstack
```

8. Start the ZStack management node service. Then, ZStack is successfully restored to the previous version.

```
zstack-ctl start
```

22.

Q: When I restart a management node, the management node fails to be started, and the system reports that no space is available. What should I do?

A:

- **Cause:** The versions earlier than ZStack 3.5.0 use Prometheus 1.8.2, which might cause the monitoring data to occupy the root space.

> **Note:**
> ZStack 3.5.0 and later versions use Prometheus 2.9.2, which allow you to set the retention policy. (By default, 50 GB monitoring data can be saved.)

- **Solution:** If the monitoring data is no longer needed, permanently delete the Prometheus monitoring data to release the space.

  — In a single management node environment, run the following commands in sequence to delete the Prometheus monitoring data:

```
[root@hostname ~]# du -sh /var/lib/zstack/prometheus/data/
  //View the monitoring data size.
[root@hostname ~]# zstack-ctl stop
[root@hostname ~]# kill -9 `ps -ef |grep prometheus|awk '{print
 $2}'`
[root@hostname ~]# rm -rf /var/lib/zstack/prometheus/data
```

```
[root@hostname ~]# zstack-ctl start
```

- In a dual-MN environment, run the following commands in each management node to delete the Prometheus monitoring data:

```
[root@mn-1 ~]# du -sh /var/lib/zstack/prometheus/data/    //
View the monitoring data size.
[root@mn-1 ~]# zsha2 stop-node
[root@mn-1 ~]# kill -9 `ps -ef |grep prometheus|awk '{print $2
}'
[root@mn-1 ~]# rm -rf /var/lib/zstack/prometheus/data
[root@mn-1 ~]# zsha2 start-node
```

23.

Q: I tried to install a compute node by using an unofficial ZStack but failed. Why?

A: Unofficial ISO cannot be used to install a compute node. Please use the official ZStack custom ISO.

24.

Q: I successfully installed a ZStack Cloud in a nested virtualization environment. However, when I add a host in the Cloud, the following error is reported: `ERROR:could not insert 'kvm_intel':Operation not supported stdout`. What should I do?

A: When you set up ZStack in nested virtualization environments such as KVM, VMware, VirtualBox, Hyper-V, and Xen, enable Intel VT-x/EPT or AMD-V/RVI(V) in the virtualization engine settings of the corresponding virtualization platform.

18.3 System Login

1.

Q: Which browsers are recommended to log in to ZStack?

A: Chrome 49, Firefox 52, or their later versions are recommended for a better experience.

2.

Q: What should I do if I could not log in to the UI?

A: Check the following information:

1. If the system reports that the user name or password is incorrect, enter the correct user name and password.
2. If the system reports that you could not connect to the management node, run the `zstack-ctl status` command to check whether the management node service is running properly.
3. If you still could not connect to the management node, perform login via **`cli`**.

```
[root@localhost ~]# zstack-cli  #Go to the CLI mode.
```

```
admin>>> LogInByAccount accountName=admin password=password #Log
in to the CLI. Default user name/password: admin/password.
```

4. Check whether the related Java process cannot run due to zombies in the process. If yes, restart the management node service.

3. Q: How do I change the admin password of the UI?

   A: Three methods are available:

   - **UI method:**

     On the **Homepage** of ZStack, click the admin icon, and then click **Change Password**.

   - **CTL method:**

     Run the following command:

     ```
     [root@localhost ~]# zstack-ctl reset_password --password
     NEW_PASSWORD #Change the password. (NEW_PASSWORD is the new
     password.)
     ```

   - **CLI method:**

     Run the following commands in sequence:

     ```
     [root@localhost ~]# zstack-cli  #Go to the CLI mode.
     admin>>> LogInByAccount accountName=admin password=password #Log
     in to the CLI. Default user name/password: admin/password.
     admin>>> UpdateAccount uuid=36c27e8ff05c4780bf6d2fa65700f22e
     password=NEW_PASSWORD #Change the password. (NEW_PASSWORD is the
     new password.)
     ```

4. Q: How do I change the default port (5000) of the UI?

   A: Run the following commands in sequence:

   ```
   [root@localhost ~]# zstack-ctl config_ui --server-port 8888  #Change
    the UI port to 8888.
   [root@localhost ~]# zstack-ctl config_ui --webhook-port 8888  #
   Change the webhook host port to 8888.
   [root@localhost ~]# zstack-ctl stop_ui  #Stop the UI service.
   [root@localhost ~]# zstack-ctl start_ui  #Start the UI service.
   ```

5. Q: How do I extend the session timeout?

   A:

   - **UI method:**

     Go to **Settings** > **Global Settings** > **Basic Settings**, locate **Session.timeout**, and set a value as needed.

- **CLI method:**

  Run the following commands in sequence:

```
[root@localhost ~]# zstack-cli  #Go to the CLI mode.
admin>>> LogInByAccount accountName=admin password=password #Log
in to the CLI. Default user name/password: admin/password.
admin>>> UpdateGlobalConfig name=session.timeout category=identity
 value=720000 #Change the session timeout to 200 hours.
```

6.

Q: How do I change the number of concurrent logins in ZStack?

A:

- **UI method:**

  Go to **Settings** > **Global Settings** > **Advanced**, locate **Session.maxConcurrent**, and set a value as needed.

- **CLI method:**

  1. Run the `QueryGlobalConfig name~=session` command. Then, you will find that the maximum number of allowed concurrent sessions is 500.

```
{
            "category": "identity",
            "defaultValue": "500",
            "description": "Max number of sessions management
server accepts. \
When this limit met, new session will be rejected",
            "name": "session.maxConcurrent",
            "value": "500"
 }
```

  2. If you want to change the value to 1000, run the following command:

```
UpdateGlobalConfig category=identity name="session.maxConcurr
ent" value=1000
```

7.

Q: How do I switch the language of the backend environment?

A: The UI language and backend language of ZStack are independent of each other. The default backend language is Chinese. You can run the following commands in sequence to switch the language:

```
[root@localhost ~]# zstack-ctl configure locale=en_US   #Switch the
 language. Note that en_US indicates English, and zh_CN indicates
Chinese.
[root@localhost ~]# zstack-ctl restart_node   #Restart the
management node for the configuration to take effect.
```

8.

Q: Can I log in to the UI via HTTPS?

A: ZStack allows you to log in to the UI via HTTPS or HTTP.

18.4 Resource Pool

VM Instance

1. Q: How can I check whether one VM instance supports hardware virtualization?

   A: To check whether one VM instance supports hardware virtualization, run `egrep "vmx|svm" /proc/cpuinfo` in your terminal. If there are outputs, the VM instance supports hardware virtualization.

2. Q: How do I know whether DHCP services of ZStack are in conflict with those of the current data center?

   A: If ZStack DHCP services conflict with those of the current data center, the network range used by VM instances in ZStack must not duplicate the used IP range in the current environment. If both ranges duplicate, IP addresses are in conflict.

3. Q: I create a VM instance by selecting a flat network, but do not set hostname for the VM instance. What is the default hostname?

   A: If the original hostname is localhost in the image used by the VM instance, the DHCP service will associate hostname with the IP address of the VM instance. For example, if the IP address of the VM instance is *192.168.12.3*, then hostname for the VM instance is **192-168-12-3**.

4. Q: Why doesn't hostname of a flat network take effect when **`zstack-cli`** is performed?

   A: If the original hostname is not localhost in the image used by the VM instance, the DHCP service will use the original hostname rather than assign a new hostname.

5. Q: How can I change an IP address for a console proxy?

   A: The following are two methods on how to change the IP address for a console proxy:

   - **UI**:

Go to **Platform Management** > **Console Proxy**, and set an IP address for a console proxy. Changes to this setting will take effect immediately without the need to restart your management node.

- **Command Line**:

  Run the following commands successively (MANAGEMENT_NODE_PUBLIC_IP_ADDRESS is the IP address of the console proxy):

```
[root@localhost ~]# zstack-ctl configure consoleProxyOverriddenIp=
MANAGEMENT_NODE_PUBLIC_IP_ADDRESS
[root@localhost ~]# zstack-ctl restart_node
```

6.

Q: How can I connect the console of a VM instance with an internal IP address via the public IP address of my management node?

A: Similar to Q5, change the IP address for the console proxy.

7.

Q: Can I reserve one IP address in an IP range without allowing ZStack to assign IP addresses for a VM instance?

A:

- Currently, the `ReserverIpRange` API is not available. If you want ZStack to reserve several specific IP addresses from the configured IP range, create a specified VIP on the UI to reserve IP addresses.
- Use the `CreateVip` API.

  For example, use *a.b.c.d* to act as a VIP to do the IP reservation from a specified L3 network by running the following commands:

```
[root@localhost ~]# zstack-cli  #Run CLI.
admin>>> LogInByAccount accountName=admin password=password #Log
in to CLI. Default user name/password: admin/password
admin>>> CreateVip l3NetworkUuid=YOU_L3_NETWORK_UUID name=
for_reserver requiredIp=a.b.c.d
```

8.

Q: How can I modify instance offerings for multiple VM instances in bulk?

A: Go to **Resource Pool** > **VM Instance**, select multiple VM instances, choose **Actions** > **Change Instance Offering**, and select an appropriate instance offering.

9.

Q: How can I address the incompatibility issue of qemu versions?

A:

- **Symptom**:

  When you start a VM instance, you may encounter the following similar errors:

  ```
  uses a qcow2 feature which is not supported by this qemu version:
  QCOW version 3
  ```

- **Cause**:

  The main reason is that qcow versions are inconsistent. The original qcow2 uses the newer version of qemu-img, while the current qcow2 uses the older version of qemu-img. The older version of qemu-img is inconsistent with the newer version of qemu-img.

- **Solution**:

  Perform compatibility transformation for the newer version of qemu-img. For example, run the following command to do the transformation. After transformation, add the image again.

  ```
  qemu-img convert -o compat=0.10 -f qcow2 -O qcow2 centos6-cloud-
  init.qcow2 centos-st-ssh-key.qcow2
  ```

10.
Q: Can I manually modify the MAC address assigned by ZStack?

A: Yes. ZStack lets you modify MAC addresses for the stopped VM instances.

11.
Q: How can I modify the MAC address for the VM NIC in ZStack?

A: When you create a VM instance, you can specify an MAC address. After you stop the VM instance, in the **Configurations** page, choose **Actions** > **Set MAC** on the left of the **vNIC** tab page to set or modify the MAC address.

12.
Q: I power off the data center to perform maintenance. After the data center is powered on, how can businesses of VM instances be resumed automatically?

A: For more information about powering off or on data centers as planned and resuming data centers due to the accidental power outage, see *Data Center Power Maintenance*.

13.
Q: After I detach and then reattach an L3 network from a VM instance, will the IP address of the VM instance be changed?

A: Yes. With the DHCP service, an IP address will be randomly reassigned.

14.
Q: How can I modify the delete latency for a VM instance?

A: The following are two methods on how to modify the delete latency for a VM instance:

- **UI**:

  Go to **Settings** > **Global Settings** > **Basic Settings**, and set **ExpungePeriod**.

- **Command Line**:

  Run the following commands successively:

```
[root@localhost ~]# zstack-cli  #Run CLI.
admin>>> LogInByAccount accountName=admin password=password #Log
in to CLI. Default user name/password: admin/password.
admin>>> UpdateGlobalConfig category=vm name=expungePeriod value=
3600  #Set the delete latency to 3600 seconds.
```

15.
Q: Can I attach or detach an ISO for a running VM instance in ZStack?

A: Yes. In the **VM Instance** page, select one VM instance that is in the running state. Then, click **Actions**, and select attach or detach ISOs.

16.
Q: How can I attach multiple NICs to a VM instance?

A:

- **Symptom**:

  When you create a VM instance, you may discover that one VM instance has attached multiple networks. At this time, you can see multiple NICs on the VM instance via the console, but no IP addresses are found.

- **Cause**:

  For a VM instance, each network is exactly one NIC. Attaching a network to a VM instance is equal to connecting a physical NIC to a server. By running **`ifconfig`**, you can see the eth device. If no IP addresses are found, this NIC has been actually connected but is not configured properly.

- **Solution**:

  Ensure that you create a configuration file for this new NIC by incurring through the eth configuration file as follows:

  1. Make a copy of eth0: (The following is an example of a CentOS 7.2 environment. Notice that other versions of Linux path and file may be slightly different.)

```
# Replace eth0 to eth1 in your configuration file, and delete
the UUID.
cp /etc/sysconfig/network-scripts/ifcfg-eth0 /etc/sysconfig/
network-scripts/ifcfg-eth1
sed -i 's/eth0/eth1/g' ifcfg-eth0
```

```
sed -i '/UUID*/d' /etc/sysconfig/network-scripts/ifcfg-eth1
```

2. Restart the network to take effect:

```
/etc/init.d/network restart
```

3. By running `ifconfig`, you will see the IP addresses of the second NIC. If you attach multiple NICs to one VM instance, run the preceding commands.

17.

Q: How can I migrate VM instances on KVM to ZStack?

A: ZStack provides the V2V migration service, and allows you to migrate the VM instances and data completely on a KVM-based cloud to ZStack. For more information, see *V2V Migration Tutorial*.

18.

Q: How can I set the boot order for a VM instance in ZStack?

A: Go to **Resource Pool** > **VM Instance**, select the name of the VM instance. Then, click **Actions** > **Set Boot Order**, and select the required boot order.

19.

Q: How can I specify an IP address when creating a VM instance?

A: In most circumstances, the DHCP service will assign an IP address for a VM instance. If you want to specify an IP address by yourself, refer to the following steps:

Stop the VM instance, and enter its details page. In the **Configurations** tab page, select a NIC attached by the VM instance, and click **Actions** > **Set Fixed IP**.

20.

Q: What can I do when an error report occurs after changing the password for a Windows VM instance?

A:

- **Symptom**:

  When the password for a Windows VM instance is modified, an error may be reported:

  ```
  return code: 1 stdout: stderr: error: internal error: unable to
  execute QEMU agent command 'guest-set-user-password':
  The command guest-set-user-password has not been found
  ```

- **Cause**:

  The possible reason is that you use the wrong Windows Virtio driver.

  Solution:

Currently, ZStack Custom ISO has integrated an available Windows Virtio driver. Decompress this ISO image, and add this Windows Virtio driver as an ISO image to a backup storage. Then, attach this ISO image to the Windows VM instance, and install the corresponding QEMU guest agent.

21.

Q: How can I resume my SSH key after accidentally deleting it?

A: By default, an SSH key is stored in the *`/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/ansible/rsaKeys`* directory. If you happen to delete the SSH key, you can resume it via the following method:

1. Firstly, generate an SSH key by running the following command:

```
ssh-keygen -f /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-
INF/classes/ansible/rsaKeys/id_rsa -N ""    //In the command, ""
is the double quotation marks.
```

2. After generation, ensure that you have access permission to the SSH key by running the following command:

```
chown -R zstack.zstack /usr/local/zstack/apache-tomcat/webapps/
zstack/WEB-INF/classes/ansible/rsaKeys
```

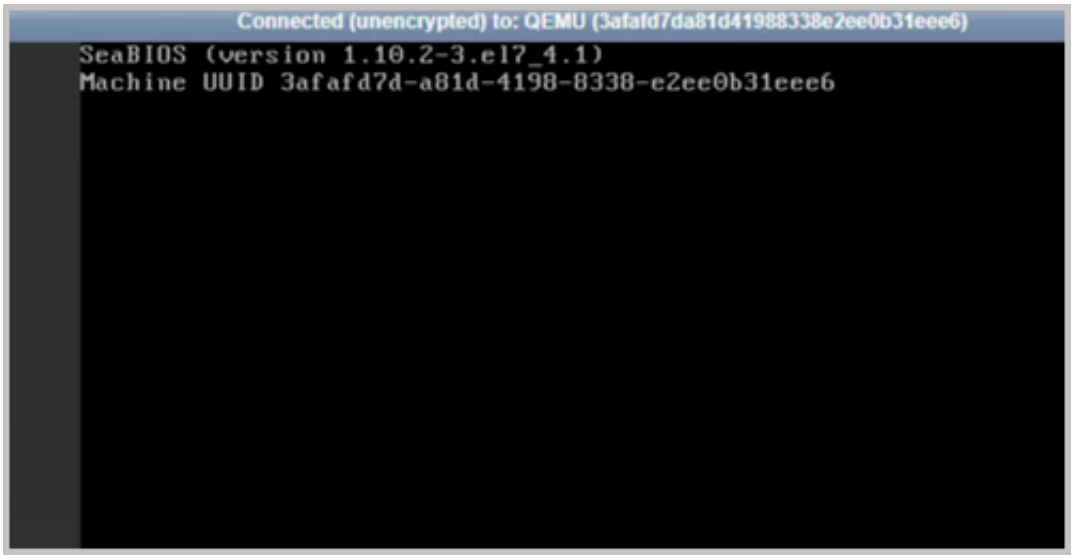
22.

Q: What happens to **Guest has not initialized the display (yet).** displayed in the console of a VM instance?

A:

- **Symptom and Cause**:

  If you use an old server as your compute node, you may fail to create a VM instance or cannot log in to the console of the VM instance due to the earlier CPU model. The following figure shows this symptom and cause.



- **Solution**:

  If this situation reproduces, try the following:

  1. Add `ept=0` to the first line in kvm-nested.conf. For example,

     ```
     options kvm_intel nested=1 ept=0
     #vim /etc/modprobe.d/kvm-nested.conf
     ```

  2. Stop the VM instance that is in the running state, and remove kvm_intel:

     ```
     #rmmod kvm_intel
     ```

  3. Reattach kvm_intel:

     ```
     #modprobe kvm-intel ept=0 unrestricted_guest=0
     ```

23.

Q: What are a CPU model and passthrough (supports nested virtualization)?

A: You can set the CPU mode for a VM instance via the following methods. Go to **Settings** > **Global Settings** > **Advanced**, and set **Vm.cpuMode** to **host-model**.

The following are three methods to set the CPU mode for a VM instance:

- **none**: The VM CPU model is QEMU emulator.
- **host-model**: The type of VM CPU model is host CPU.
- **host-passthrough**: The VM CPU model is identical with the host CPU model.

Note:

- When the CPU mode is **host-model** and **host-passthrough**, the VM instance can get nested virtualization.
- Using the virtualization may influence hot migrations for the VM instance. When host migrations are performed, the VM CPU model will be checked. If CPU models of two hosts are different, hot migrations for the VM instance are failed.

24.
Q: Under what circumstance will a VM instance enter **Paused** state?

A: When a VM instance is out of memory, creating or migrating the VM instance will place the VM instance into the **Paused** state.

25.
Q: What can I do when an IO error is reported on the console proxy?

A:

- **Symptom**:

```
"description": "Cannot do an IO operation(e.g. network IO error,
file IO error)", "details": "I/O error on POST request for \"http
://127.0.0.1:7758/console/establish\": Connect to 127.0.0.1:7758
 [/127.0.0.1] failed: Connection refused; nested exception is org
.apache.http.conn.HttpHostConnectException: Connect to 127.0.0.1:
7758 [/127.0.0.1] failed: Connection refused","$$hashKey": "object
:1344"
```

- **Solution**:

  Delete the **`consoleProxy`** file under the *`/var/lib/zstack/pickledb/`* directory, and reconnect the console proxy.

26.
Q: Why can't VM instances with the same network range **`ping`** each other?

A: Assume that VM instances on a host can ping each other. Also, hosts whose NICs are attached to VM instances can also ping each other, but the VM instances residing across hosts cannot ping each other. In that case, your switch probably goes wrong.

27.

Q: If I do not have a DNS server in my network, how can VM instances use the IP addresses assigned by the DNS server of a telecommunication corporation to reach the external network?

A: Make sure that when you create a network, specify a DNS address.

28.

Q: What is the possible cause for migration failures of a VM instance?

A:

- **Symptom**:

```
{
  "error": {
    "code": "HOST.1009",
    "description": "Failed to migrate vm on hypervisor",
    "details": "failed to migrate vm[uuid:90bb61f55e774f5f89c9
e1ea46db7661] from kvm host[uuid:e5105c61114a4efe8bcc025f744226
bd, ip:10.0.247.244] to dest host[ip:10.0.197.238], unable to
migrate vm[uuid:90bb61f55e774f5f89c9e1ea46db7661] to qemu+tcp://10
.0.197.238/system, internal error: Attempt to migrate guest to the
 same host localhost.domain.com"
  },
  "createdTime": 1488170137857,
  "type": {
    "_name": "key.event.API.API_EVENT"
  },
  "id": "e6bcd7c33ad9446b919e11cd647fc8dc"
}
```

- **Cause**:

  Two hosts have the identical hostname. Migrating a KVM VM instance depends on a hostname for confirming hosts. If the hostnames duplicate, ZStack deems that the same host is used.

- **Solution**:

  We recommend that you set different hostnames for different hosts. If the preceding errors are reproduced, contact our official technical support.

29.

Q: Why does stopping some VM instances be time-consuming?

A:

- **Symptom**:

Generally, VM instances whose Guest OS is Linux take a long time to be stopped for lack of the ACPID service (a daemon designed to process power-related events). By default, KVM VM instances with Linux do not have the ACPID service. Therefore, this service is unavailable. In other words, ZStack will force to kill the progresses of these VM instances after these VM instances are stopped for one minute.

- **Solution**:

  In this case, only ensure that you have installed and enabled the ACPID service in these VM instances. Run the following commands:

```
[root@kvm_client_00 ~]# yum install acpid -y
# Reenable the ACPID service. That is, after ACPID installation,
the service defaults to be enabled when the VM instance starts.
[root@kvm_client_00 ~]# /etc/init.d/acpid restart
```

30.

Q: How many phases does the high availability of a VM instance have?

A: If a VM instance with the high availability fails to reboot, this VM instance will enter the following phases:

- Detect the state of the VM instance via the mechanisms such as round robin and trigger. If the VM instance is confirmed to stop, the VM instance configured with NeverStop will reboot immediately.
- Detect the state of the VM instance via the mechanisms such as round robin and trigger. If the VM instance is not confirmed to stop, the following procedures will be applied:
  1. Based on the existing network configurations, the most accurate method will be selected to detect the state of the host where the VM instance resides.
  2. If the host is abnormal, the VM instance configured with NeverStop will try to automatica lly reboot.

31.

Q: I install QEMU Guest Agent for Ubuntu VM instances online by running `apt-get install qemu-guest`. After installation, the version of QEMU Guest Agent is 2.0 which is too old. How can I resolve this issue?

A:

1. On the official Ubuntu dependency library website, search the QEMU Guest Agent with Ubuntu 16.04, and download the offline deb package of QEMU Guest Agent at version 2.5.

https://ubuntu.pkgs.org/16.04/ubuntu-universe-amd64/qemu-guest-agent_2.5+dfsg-5ubuntu10_amd64.deb.html

2. Install this offline deb package.

```
dpkg -i <package.deb>    //<package.deb> represents the offline
deb package of QEMU Guest Agent at version 2.5.
```

3. Modify the password on the UI. If no errors are reported, the modification is completed.

32.

Q: What are the possible causes for failing to create VM instances in ZStack?

A:

- Backup storages are disconnected. Verify that these backup storages are available and normally connected.
- Primary storages have not attached any cluster. Therefore, available hosts are not found. Verify that these primary storages have attached clusters.
- No available hosts in clusters satisfy instance offerings. Verify that hosts are available and have sufficient resources.
- Capacities for primary storages are insufficient to provide virtual capacities required by images. Verify that these capacities of these primary storages are sufficient.
- Clusters have not attached the corresponding networks. Verify that these clusters have attached the corresponding networks.
- Resources of an IP address pool are insufficient. Verify that IP ranges are sufficient.
- The links between backup storages and primary storages are abnormal. Verify that the links where images are downloaded to these primary storages from these backup storages are normal.
- The dnsmasq service of the distributed DHCP service in hosts are abnormal. Verify that the DHCP service can automatically assign IP addresses to VM instances.
- The libvirtd service of hosts are abnormal. Verify that the libvirtd service is normal so that it can provide virtualization.
- If a VM instance keep enabling, check whether the image of this VM instance is huge and whether downloading image caches is time-consuming. If these image caches exist, continue to check `/var/log/zstack/zstack-kvmagent.log` of the host where the VM instance resides.

33.

Q: What is the relationship between the system time of VM instances and the system time of hosts?

A: To ensure the correct time synchronization for VM instances, we strongly recommend that you set an independent time synchronization server for these VM instances. If you have not configured any time synchronization server, the time synchronization mechanism for VM instances with different operating systems are as follows:

- The internal system time of Linux VM instances will use the host time as clock followed by the operations such as creating, enabling, and rebooting the VM instances. Whether the time of the VM instances either lags behind or goes ahead will take effect.
- Creating Windows VM instances will automatically read the time of hosts as clock.
- When the internal system time for Windows VM instances lags behind compared to that of hosts, the internal system time for these Windows VM instances will use the time of these hosts as clock followed by the operations such as enabling and starting the VM instances.
- When the internal system time of Windows VM instances is ahead of that of hosts, the operations such as enabling and rebooting these VM instances will not read the time of these hosts. The possible cause is related to the Windows licensing policy. For example , after a 180-day trial expires, Windows VM instances will stop every one hour. Time regression will skip off the Microsoft licensing policy.

Note:

- Generally, the time source of the underlying hosts is defined by the `chrony.serverIp.0 = 172.20.0.10` option under the *`/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`* directory (Assume that the time synchronization server is *172.20.0.10*).
- Management nodes will synchronize all hosts to use the same time source. When VM instances are created or enabled, these VM instances will follow the time source of their hosts.

34.

Q: Can I resize the system disk for a VM instance?

A: Yes. For more information, see *System Disk Resizing* in User Guide.

35.

Q: My GPU devices are inserted to a host that has added to the Cloud but are not found on the UI. In that case, I cannot pass through these GPU devices to VM instances. What should I do?

A:

- Run `lspci -s xx:xx -v` to check the GPU driver information. That is, check whether this host has used these GPU devices.
- Enable IOMMU for hosts, and enable the Intel VT-d/AMD IOMMU option in BIOS.

36.

Q: How can I set my account or password when creating a VM instance?

A:

- Method 1: Go to **Create VM Instance** > **SSH Login Method**, and select **Password**. Options for setting a password for a VM instance include:
  - Linux image: Default user name is root. Both SSH key and password are supported.
  - Windows image: Default user name is administrator. Only password is supported.
- Method 2: Go to **Create VM Instance** > **Advanced** > **User Data**, and set your account or password via the User Data injection.

For more information, see *Create VM Instance* in User Guide.

37.

Q: How can I settle the slow SSH access to a VM instance?

A:

1. On your SSH server, modify the configurations in the *`/etc/ssh/sshd_config`* file as follows:

```
UseDNS no
#GSSAPI options
GSSAPIAuthentication no
```

2. Run `/etc/init.d/sshd restart` to restart the sshd (OpenSSH Daemon) service.

38.

Q: When I can use SSH to remotely log in to a Windows Server VM instance, it prompts me for **This could be due to CredSSP encryption oracle remediation.**. What should I do?

A: **To enable the encryption Oracle remediation**

1. In the Windows enterprise OS, press windows+R, enter `gpedit.msc`, and click **OK** to go to the **Local Group Policy Editor** page.
2. Navigate to **Computer Configuration** > **Administrative Templates** > **System** > **Credentials Delegation** > **Encryption Oracle Remediation**, and go to the **Encryption Oracle Remediation** page.

3. Set **Encryption Oracle Remediation** to **Enabled**, and click **Apply** to enable the encryption Oracle remediation.

> **Note:**
> After the remediation is applied, if the configurations do not take effect, restart the operating system.

39.

Q: When I create Windows VM instances and Linux VM instances both with an L3 network, only the network of these Windows VM instances are unavailable, but intercommunications among these Linux VM instances are normal. What are the possible causes for this event?

A: You must install the corresponding version of Virtio NIC driver and then restart these Windows VM instances.

40.

Q: My VM instances use shared storages, and the CPU mode is set to host-passthrough. I attempt to migrate these VM instances online within the same cluster, but failed. What should I do?

A:

- **Symptom**:

  When migrations are performed, the following error is reported:

  ```
  Assertion `ret == cpu >kvm_msr_buf->nmsrs`failed
  ```

- **Cause**:

  The CPU model of the target host is inconsistent with that of the current server.

- **Solution**:

  Either migrate these VM instances to the host with the same CPU model or stop these VM instances before migrations are performed.

41.

Q: My VM instance is booted via the UEFI mode. After I install the operating system for the VM instance, this VM instance restarts and automatically goes to the **UEFI shell** page. What should I do?

A: Run **`vim /boot/efi/startup.nsh`** to write and save the following settings. Restart the VM instance to start normally.

```
FS0:
CD EFI
```

```
CD centos
shimx64-centos.efi
```

Image

1. Q: How does the occupied space for creating an image work?

   A:

   - **Prerequisites**: A primary storage is not overprovisioned or uses the thick provisioning. This primary storage must be ImageStore.
   - **Example**: Assume that you create a VM instance (A) that occupies 400 G by using a 800 G primary storage. Encapsulate A as an image (B). The actual size for B is less than 400 G. Presumably, B only holds 10 G. Then, use B to create a new VM instance (C). Now, B will be downloaded from a backup storage to the cache directory of this primary storage. 10 G of this primary storage will be consumed. After download, the virtually available capacity for this primary storage holds only 390 G. However, creating C requires the 400 G capacity. Hence, C fails to be created.

2. Q: When I create an image, errors related to the URL will be displayed. What are the general resolutions?

   A:

   - ZStack supports the following URL formats:
     - *HTTP/HTTPS*:
       - Format: *http://path/file* or *https://path/file*
       - Example: *http://cdn.zstack.io/product_downloads/images/zstack-image.qcow2*
     - *FTP*:
       - Anonymous mode: *ftp://hostname[:port]/path/file*

         Example: *ftp://172.20.0.10/pub/zstack-image.qcow2*
       - Non-anonymous mode: *ftp://user:password@hostname[:port]/path/file*

         Example: *ftp://zstack:password@172.20.0.10/pub/zstack-image.qcow2*
     - *SFTP*:
       - Specified password mode: *sftp://user:password@hostname[:port]/path/file*

         Example: *sftp://root:password@172.20.0.10/pub/zstack-image.qcow2*

- Password-free mode: *sftp://user@hostname[:port]/path/file*

  Example: *sftp://root@172.20.0.10/pub/zstack-image.qcow2*

— The absolute path on backup storages such as SFTP and ImageStore:

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

Note:

- We recommend that you download images by creating a HTTP server.
- If local images are used, make sure that image URLs must be absolute paths.

3.

Q: What should I do when adding an image times out?

A:

- **Cause**:

  When I download an image, the timeout error is reported due to the low download speed. This is because sometimes the image is too large, or the network goes wrong.

- **Solution**:

  If I download the image, the HTTP service will be enabled on the backup storage. When the timeout error is displayed on the UI, or even the management node stops (Notice that the backup storage is not running on the host where the management node resides), your business will not be affected.

  Hence, there is no need to worry about the time-consuming download. The image will be automatically downloaded in the terminal. When you continue to add this image next time, the progress will take shorter.

4.

Q: What should I do if the Windows internal monitoring does not display any data?

A: After a PCI device driver is installed, the memory information cannot be obtained via QEMU . After installation, this PCI device driver is called VirtIO Balloon Driver.

To solve this problem

1. Load windows-virtio-driver ISO image.
2. Take 64-bit Windows Server 2012 as an example. Copy the **BLNSVR.EXE** file under the *`X:\Balloon\2k12R2\amd64`* directory to the *`C:\Windows\System32`* directory.
3. Select Administrator: Windows PowerShell and run `BLNSVR -I`.

5.

Q: When I encapsulate a Windows template, the Virtio driver cannot be correctly identified. What should I do?

A:

- **Symptom**:

  During installation, the loaded Virtio driver cannot be correctly identified so that you are not able to see the loaded system volume.

- **Cause**:

  The Windows ISO image that you used is possibly not downloaded from the official Microsoft website, which means that this ISO image has been customized via other tools.

- **Solution**:

  Download the corresponding ISO file from the official Microsoft website.

6.

Q: Where can I find the Windows Virtio ISO image?

A: Take C76 as an example. Under the `/opt/zstack-dvd/x86_64/c76/` directory of the management node, you can find the native *zstack-windows-virtio-driver.iso* image.

7.

Q: How can I set the write cache for a single VM instance?

A: The write cache mode belongs to the parameters of the global settings. After the write mode is modified, restart the VM instance to take effect. If you need to set a write cache for a single VM instance, modify the cache mode before creating the VM instance, and then restore the original cache mode.

8.

Q: What are the differences between a raw image and a qcow2 image?

A:

- raw: Raw format. When you create a raw image, specify a storage capacity. The raw image can occupy all capacities. However, this image does not support dynamic resizing and snapshots. Hence, its performance is great.
- qcow2: Quick copy on write 2. At the beginning, a qcow2 image will only occupy a small portion of capacity, and supports dynamic resizing, compression, AES encryption, and snapshot. Hence, its performance is relatively great.

9.

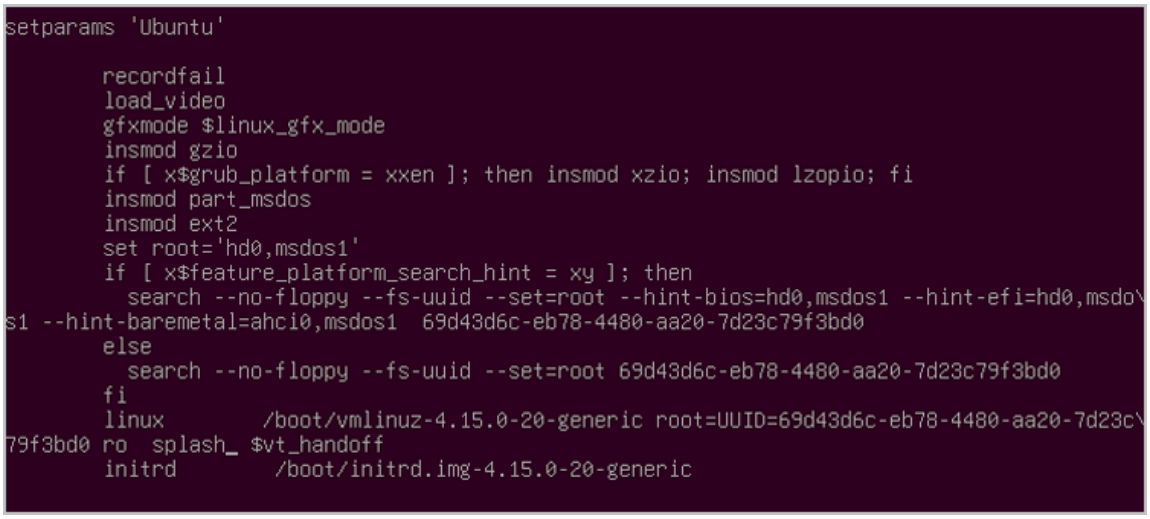
Q: For a VM instance installed with the Ubuntu 18 operating system, if GRUB configures the Splash option, this VM instance cannot be started. What should I do?

A:

- **Symptom**:

  For a VM instance installed with the Ubuntu 18 operating system, if GRUB configures the Splash option, this VM instance cannot be started and its start page turns blurry or fuzzy, as shown in *GRUB Configures the Splash Option* and *Blurry Start Page*.

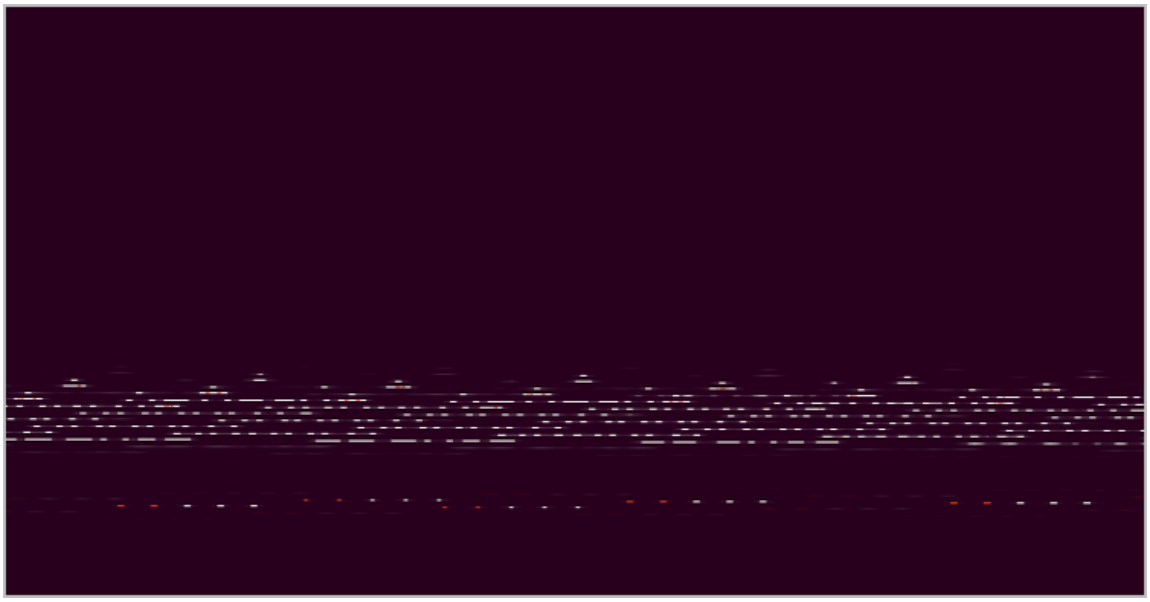
Figure 18-1: GRUB Configures the Splash Option



```
setparams 'Ubuntu'

        recordfail
        load_video
        gfxmode $linux_gfx_mode
        insmod gzio
        if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; fi
        insmod part_msdos
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hint-efi=hd0,msdo\
s1 --hint-baremetal=ahci0,msdos1  69d43d6c-eb78-4480-aa20-7d23c79f3bd0
        else
          search --no-floppy --fs-uuid --set=root 69d43d6c-eb78-4480-aa20-7d23c79f3bd0
        fi
        linux        /boot/vmlinuz-4.15.0-20-generic root=UUID=69d43d6c-eb78-4480-aa20-7d23c\
79f3bd0 ro  splash_ $vt_handoff
        initrd        /boot/initrd.img-4.15.0-20-generic
```

Figure 18-2: Blurry Start Page



- **Solution**:

  Navigate to **Settings** > **Global Settings** > **Basic Settings**, and set **VideoType** to VGA before the VM instance can work properly.

  > **Note:**
  > This issue only reproduces in the Ubuntu 18 version, excluding the earlier Ubuntu versions.

10.

Q: What should I do if I cannot set the resolution ratio for a Windows VM instance?

A: On the ZStack UI page, choose **Settings** > **Global Settings** > **Advanced**, set **VideoType** to **vga**, and restart the VM instance.

11.

Q: When I create an image for a VM instance that uses a Ceph primary storage to an ImageStore backup storage, it takes a long time. Why?

A: The Ceph storage volume uses the raw format, indicating that creating an image requires you to make a full data copy. After the VM image is created, it can be exported. Then, the image type will be automatically converted to the qcow2 format. Finally, this image will be reimported to the ImageStore backup storage.

Volume

1.

Q: Volumes can be created on shared storages. Can these volumes be randomly attached to any VM instance?

A: ZStack lets you add different clusters to different primary storages within a zone, while these primary storages can either be LocalStorage or shared storages.

- If primary storages are shared storages, volumes are created on these shared storages but are irrelevant to hosts. These volumes can be attached to the VM instances of any host. Specifically, these volumes are not constrained by the hosts, and cannot be migrated.
- If primary storages are LocalStorage and attached one volume before, ensure that both this volume and the target VM instance reside on the same host. If both this volume and the target VM instance reside on the same host, migrate the volume and the target VM instance to the same host. You can either choose to migrate the VM instance (Make sure that you stop the VM instance in advance) or the volume.

2.

Q: When I attach a new L3 network for a VM instance, why does only one NIC be displayed?

A: When you add a new NIC to a VM instance, QEMU only presents this NIC to the system, but this NIC cannot correctly be identified. To view this new NIC, run `lspci`. The following are the two methods to correctly identify the NIC when you run the operating system of the VM instance:

- Method 1: Restart the VM instance. After restarting the VM instance, you will automatically obtain the NIC information.
- Method 2: Manually configure the NIC without the need to restart the VM instance.

  Procedure

  1. Reference *`/etc/sysconfig/network-scripts/ifcfg-eth0`* in the VM instance, and add the **ifcfg-eth1** configuration file to the new eth1 NIC.
  2. Go to the *`ifcfg-eth1`* configuration file of eth1, and set the required parameters. For example:

     ```
     [root@VM-web ~]# cd /etc/sysconfig/network-scripts/
     [root@VM-web network-scripts]# vim ifcfg-eth1
     ...
     TYPE=Ethernet
     BOOTPROTO=dhcp
     NAME=eth1
     DEVICE=eth1
     ONBOOT=yes
     ...
     ```

     After setting, run `:wq` to save and exit this setting.
  3. Run `systemctl restart network` to restart the network to take effect. Hence, this NIC can be correctly identified.

3.

Q: Why is `QueryVolume actualSize` inconsistent with the actual file size?

A: When you use disks, **`actualsize`** will continue to increase. Navigate to **Resource Pool** > **Volume**, expand the details page of a volume, and click the refresh button behind the **Actual Size** field to synchronize data.

4.

Q: When the disk of a VM instance is completely written, the VM instance cannot be started. What should I do?

A: Before starting the VM instance, expand the disk. We recommend that you back up the VM instance as an image.

5.

Q: How can I migrate a volume to the target primary storage?

A: **To migrate a volume to the target primary storage**

Navigate to **Resource Pool** > **Volume**, select the volume to be migrated. Then, click **Actions** > **Storage Migration**, and select the target primary storage.

6. Q: When I install Virtio drivers in Windows, which types of driver should I install for the disk?

   A: Install the VioStor storage controller and vioscsi disk controller.

7. Q: Which storage should the data volume be created on, primary storage or backup storage? Why can't the created data volume be found on Windows?

   A: The data volume is created on the primary storage. Hence, you must install a Virtio driver to your VM instances.

8. Q: Can the VM instance that is created based on a template in ZStack use the **Master Disk+ Incremental Disk** mode?

   A: ZStack adopts the incremental disk mode. An image will be downloaded to a primary storage as an image cache from a backup storage. This image cache will be used as a base image. VM instances can be created by using this base image. Hence, these VM instances use the same base image.

9. Q: After attaching a volume to a Linux VM instance, modify the `/etc/fstab` file of the VM instance. When encapsulating the VM instance as an image online and using this image to create other VM instances, the created VM instances will be hung and cannot be started. What should I do?

   A:

   - **Cause**:

     Attaching a volume to a VM instance is a dynamic operation, while the `/etc/fstab` configuration file for the VM instance is static. After attaching the volume to the VM instance, you modify the fstab file of the VM instance, encapsulate the VM instance as an image online, and use this image to create another new VM instances. The fstab file does not contain the corresponding mount information so that the created VM instances are hung and cannot be started,

   - **Solution**:

- After the Linux VM instance attaches the volume, we recommend that you do not modify the */etc/fstab* file.
- Recommended method:
  - Go to */etc/rc.d/rc.local*, and run **mount** to mount the volume:

```
# chmod +x /etc/rc.d/rc.local
# mount -U <the file system UUID> <the target mount path>
```

> **Note:**
> We recommend that you use the file system UUID of the volume to mount the VM instance rather than use the drive letter similar to */dev/vdb*.

10. Q: Why is the actual capacity for a volume larger than the allocated capacity?

    A: When the volume is qcow2, the actual capacity for the volume will accumulate the snapshot capacity.

18.5 Hardware

1. Q: How can I check whether one host supports hardware virtualization?

   A: Run `egrep "vmx|svm" /proc/cpuinfo` in the terminal. If there are outputs, the host supports hardware virtualization.

2. Q: How do I enable the support for hardware virtualization in BIOS?

   A: By default, the support for hardware virtualization is enabled in BIOS. If the support is modified, enable the **Intel Virtual Technology** or **Secure Virtual Machine** option, and save and exit the setting.

3. Q: Which versions of QEMU and libvirt are supported by a ZStack compute node?

   A: Run `virsh version` on the host to check the qemu version and libvirt version.

4. Q: Why does a host keep connecting for a long time after the management node restarts?

   A: After the management node or service restarts, it will reconnect to various hardware resources. Also, the related agents will take a long time to be redeployed.

5.

Q: What should I quickly do if IP addresses of a management node, database, and message bus are modified?

A: For more information, see *Change MN IP Address*.

6. Q: What should I quickly do if the IP address of a compute node is modified?

   A: If the IP address of a compute node is modified, use the following method: Navigate to **Hardware** > **Host**, expand the host details page, and click **Edit** behind the **Host IP** field to modify the host IP. After modification, the host will automatically reconnect.

7. Q: What should I quickly do if the IP address of a backup storage is modified?

   A: If the IP address of a backup storage is modified, use the following method: Navigate to **Hardware** > **Backup Storage**, expand the host details page, and click **Edit** behind the **Backup Storage IP** field. After modification, the backup storage will automatically reconnect.

8. Q: How can I manually extend the boot time for a ZStack management node?

   A:

   - **Symptom**:

     If you run ZStack in a VM instance, you will probably find that the Cloud fails to start due to the boot timeout. However, after you run `zstack-ctl status`, the Cloud displays Running. The following is an example of the system notification:

     ```
     no management-node-ready message received within 120 seconds, \
     please check error in log file /tmp/zstack_installation.log
     ```

   - **Solution**:

     Run the following command to change the timeout (Take 300s as an example):

     ```
     [root@localhost ~]# zstack-ctl start_node --timeout 300
     ```

9. Q: How can I migrate a ZStack management node from a host to another host?

   A: For more information, see *Switch MN*.

10. Q: How can I resume the original configurations after reinstalling the management node?

    A: For more information, see *Upgrade Compute Node to Management Node*.

11. Q: How can I set the reserved memory for a host?

A: The following are two methods to set the reversed memory for a host:

- Method 1: Navigate to **Settings** > **Global Settings** > **Basic Settings**, select **ReservedMemory** to set the reserved memory for hosts globally.
- Method 2: In the **Advanced Settings** tab page under the cluster details page, select **ReservedMemory** to set the reserved memory for hosts within a cluster. Regard a cluster as a unit.

12.

Q: How can I modify the MySQL password after ZStack is installed?

A: Run the following command to modify the MySQL password:

```
[root@localhost ~]# zstack-ctl change_mysql_password --root-password
 zstack.mysql.password --user-name zstack --new-password password
```

13.

Q: What are the differences between entering maintenance mode and disable operation?

A:

- **Enter Maintenance Mode**:

  Place a host into maintenance mode. Afterwards, you can disable or repair the host. After the host is confirmed to enter maintenance mode, if your primary storage where the host is running is LocalStorage, ZStack will disable all running VM instances residing on the host. If your primary storage where the host is running is a shared storage, VM instances will automatically be migrated to other hosts.

  Note:

  - Under the shared storage scenario, after the host enters maintenance mode, you can set the VM migration policy in case of migration failure.
  - Method:

    Go to **Settings** > **Global Settings** > **Advanced**, locate **host.maintenance.policy**, and click the Edit icon.

    - If you select **Stop Vm On Migration Failure**, VM instances that are running on a shared storage will be automatically migrated to other hosts after the host where the VM instances reside enters maintenance mode. In addition, VM instances that fail to be migrated will be forced to stop.

- If you select **Just Migrate**, VM instances that are running on a shared storage will be automatically migrated to other hosts after the host where the VM instances reside enters maintenance mode. If some VM instances are still running on the host, the host will fail to enter maintenance mode.

- **Disable**:

  Stop a host. Afterwards, new VM instances cannot be created on the host, and the stopped VM instances on the host cannot be started. Currently, the running VM instances are not affected.

14.

Q: What are the possible causes that a host is disconnected?

A: The following are the possible causes that a host is disconnected. Make sure that you check whether:

- The management node can normally access port 22 of the host.
- *ZStack Custom ISO* can be used to install the system properly.
- The libvirt service of the host works normally.
- The network attached to the cluster where the host is running can be mounted normally.

  If eth1 is specified to be the physical NIC of the L2 network that is attach to the cluster, but the NIC device number of the host has been changed, which means that eth1 is no longer existed, the host cannot be reconnected.
- The system disk of the host is out of storage capacity.
- Assume that you must attach the host to the NFS primary storage. If you fail to attach it to this primary storage, check the link from the host to this primary storage.
- Assume that the host uses a distributed storage. If this distributed storage has a storage network, the host can access the storage network directly.
- If you use a VXLAN network, when you attach it to the cluster, the specified VTEP IP should be existed. If this IP is not existed, the host cannot be reconnected.

15.

Q: What if I cannot add a backup storage when using ZStack Enterprise?

A: The following are the possible causes that a backup storage cannot be added. Make sure that you check whether:

- For SFTP backup storages and ImageStore backup storages, the SSH port number, user name, and password have the sudo permission.

- For Ceph backup storages, the distributed storages work properly. Check whether the Ceph IP address, Ceph SSH port, user name, and password have the sudo permission, and Ceph clusters can work properly.

16.

Q: How can I do with the SSH connection timeout?

A:

- **Symptom**:

  Many services in ZStack require the SSH connection, including host, storage, and creating HA for a management node. As the user networks may be faulty, performing the preceding operations will prompt you for the timeout error because of the SSH connection timeout.

- **Cause**:

  It is primarily because you perform the DNS authentication for the IP address, and then the timeout appears.

- **Solution**:

  Take creating HA for a management node as an example.

  To solve this problem

  1. Modify the configurations on the *`/etc/ssh/sshd_config`* file of the SSH server as follows:

     ```
     UseDNS no
     #GSSAPI options
     GSSAPIAuthentication no
     ```

  2. Run `/etc/init.d/sshd restart` to restart the sshd service.

17.

Q: When I start ZStack, it prompts me for `MySQL is not running`. What should I do?

A:

- **Symptom**:

  After you run `zstack-ctl start` to start ZStack, the error is displayed as follows:

  When I run `zstack-ctl status`, the system prompts me for `MySQL is not running`.

- **Solution**:

  First, attempt to check the configurations of *`/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`*.

For example:

```
DB.url = jdbc:mysql://10.0.0.18:3306
DB.user = zstack
DB.password = zstack.password
```

Run `mysql -u zstack -pzstack.password -h 10.0.0.18 -P 3306` to check whether the MySQL database can be accessed.

18.

Q: What is stateless ZStack?

A: Under the circumstance of the stateless service, the requester will no longer ask for where to send requests. When a new service instance is added or an old service instance is disintegrated, services will also no longer exchange states.

If you delete br_eth0 (the NIC of the L2 network that is connected to a host) of a host, reconnect these hosts, for all hosts in ZStack are stateless. Actually, no fixed configuration file is existed on the hardware of the host, but on the memory. After reconnection, regenerate the configuration file.

19.

Q: Which data does a ZStack backup require?

A: The ZStack backup only requires a backup database.

20.

Q: How can I back up my database in ZStack?

A:

- Run `zstack-ctl dump_mysql` to back up the database once.
- Run `crontab -l`. Then, the database will be backed up once every 00:00 and 12: 30. The latest 14 copies of databases will be reserved. You can make some adjustments for the setting as needed. In consideration of your data security, we recommend that you back up your database to a remote server.

```
30 0,12 * * * zstack-ctl dump_mysql --keep-amount 14
```

21.

Q: When a host is added to the Cloud, the following error is displayed. What should I do?

A:

- **Symptom**:

When a new host is added to the Cloud, the following error is displayed:

```
{"org.zstack.header.host.APIAddHostEvent":{"success":false,"apiId
":"75b0774fc7b94007ac1ba274e6ed5eb3","headers":{"schema":{}},"
error":{"code":"HOST.1000","cause":{"code":"HOST.1003","cause":
{"code":"SYS.1006","description":"An operation failed","details
":", failed to check physical network interfaces[names : enp2s0
] on kvm host[uuid:fab977f38e024e6e86f048a4090845f8, ip:192.168
.10.11]"},"description":"An error happened when connecting to
host","details":"connection error for KVM host[uuid:fab977f38e
024e6e86f048a4090845f8, ip:192.168.10.11]"},"description":"Unable
 to add host","details":"connection error for KVM host[uuid:
fab977f38e024e6e86f048a4090845f8, ip:192.168.10.11]"},"createdTim
e":1489036864392,"type":{"_name":"key.event.API.API_EVENT"},"id":"
8f1d551677c44788953eae7255eda54b"}}
```

- **Cause and Solution**:

  This host does not have the enp2s0 NIC. Ensure that you enter the correct NIC name.

22.

Q: Virtualization is enabled on my CPUs. When a host is added to the Cloud, the following error is displayed. What should I do?

A:

1. After ZStack is installed, the following error is displayed when a host is added:

```
ERROR:could not insert 'kvm_intel':Operation not supportedn
nstdout
```

2. Run `cat /proc/cpuinfo | grep "vmx|svx"` to check whether virtualization is enabled.

   - If a return value is displayed, virtualization is enabled.
   - If no return value is displayed, virtualization is not enabled. Verify that the virtualization option is enabled in BIOS.

23.

Q: What are the requirements for a file system to deploy a Shared Mount Point primary storage ?

A: A Shared Mount Point primary storage requires that your compute node attaches the same NFS primary storage, and the NFS primary storage attaches the same directory of the compute node.

24.

Q: If I use a Ceph primary storage, I create three snapshots: 1, 2, and 3, for a VM instance. Then, I delete the snapshot 1, but not the snapshot 2 and snapshot 3. Is it right to perform this operation? When I create an image template for the VM instance, a new snapshot will be

automatically generated. Can I use this new snapshot to restore a new VM instance when creating the new VM instance?

A: The Ceph type is non-tree. Specifically, no dependency exists between snapshot points. Restoring snapshots will lose the current state of the new VM instance. It is because Snap Clone of Ceph is used.

25.

Q: What should I do when a Ceph compute node prompts me for `could not get value of the secret for username zstack`?

A:

- **Symptom**:

  If your compute node uses a Ceph primary storage, the following error is displayed when you create, enable, or migrate a VM instance:

  ```
  Internal error: could not get value of the secret for username '
  zstack' using uuid 'ee5b6375-4564-446b-ac53-c94ea4e13904'
  ```

- **Cause**:

  Generally, when your compute node connects to the Ceph primary storage, the private key for the Ceph primary storage is lost, so you need to delete this private key and reconnect the host.

- **Solution**:

  To solve this problem

  1. Run `virsh secret-list` to obtain the UUID of this Ceph primary storage on the faulty compute node.

     For example: Obtain the 03b5ee0d-df21-46d2-9927-7c930333cb70 UUID.

     ```
     root@ceph-host ~]# virsh secret-list
      UUID                                   Usage
     ------------------------------------------------------------------------------
      03b5ee0d-df21-46d2-9927-7c930333cb70  ceph 03b5ee0d-df21-46d2-
     9927-7c930333cb70
     ```

  2. Run `virsh secret-undefine 03b5ee0d-df21-46d2-9927-7c930333cb70` to delete the private key of this Ceph primary storage.

     ```
     [root@ceph-host ~]# virsh secret-undefine 03b5ee0d-df21-46d2-
     9927-7c930333cb70
     ```

```
secret 03b5ee0d-df21-46d2-9927-7c930333cb70 deleted
```

3. Run `/etc/init.d/zstack-kvmagent stop` to stop the agent of the compute node.

```
[root@ceph-host ~]# /etc/init.d/zstack-kvmagent stop
2017-05-08 10:07:57,590 DEBUG [zstacklib.utils.shell] /sbin/
iptables-save
2017-05-08 10:07:57,596 DEBUG [zstacklib.utils.iptables]
removed empty chains:[]
2017-05-08 10:07:57,598 DEBUG [zstacklib.utils.shell] /sbin/
iptables-restore < /tmp/tmpBW4mWX
Stop Daemon...
Stop Daemon Successfully
stop zstack kvm agent .... SUCCESS
```

4. Reconnect this compute node on the UI. After this compute node is reconnected successfully, you can normally create, enable, or migrate VM instances.

> **Note:**
> Currently, ZStack has supported the option to disable the CephX private key authentication.

26.

Q: Should system versions between VM instances be consistent?

A: We recommend that system versions between management nodes and hosts are consistent .

27.

Q: What information should I back up for a management node?

A: Back up only the database. Run `zstack-ctl dump_mysql` to manually back up the database of the management node.

28.

Q: How do I allocate volumes when one cluster attaches two primary storages?

A:

ZStack let one cluster attach two primary storages, while the types of primary storage are different, such as LocalStorage and NFS. When you create a new VM instance again, the root volume defaults to be created on the LocalStorage primary storage, while the data volume defaults to be created on the NFS primary storage.

29.

Q: I install ZStack on a Dell server, and I find an error reported as **dracut-initqueue timeout**. After installation, the system cannot be started. What should I do?

A: In the Boot Settings page of BIOS, set the BIOS mode to UEFI.

30.

Q: A management node has multiple NICs and IP addresses. How can I specify which IP address should be listened by the ZStack service?

A: When the system has many NICs and IP addresses (such as an internal network and an external network), ZStack defaults to select the NIC IP address used by the system default route.

Also, you can run the following command to manually specify the IP address listened by the ZStack service:

```
[root@ceph-host ~]# zstack-ctl configure management.server.ip=${
MANAGEMENT_IP}    //${MANAGEMENT_IP} is the IP address specified by
the user.
[root@ceph-host ~]# zstack-ctl restart_node   //Restart the
management node.
```

31.

Q: How can I troubleshoot if networks of VM instances on two hosts are not interconnected?

A: Based on different types of networks, troubleshoot this problem by following the steps below:

- For the VLAN network, if the NIC of the network is eth0, VLAN ID is 25.
  1. Run `ifconfig br_eth0_25 the configured IP address` to configure one IP address for different network bridges on both hosts respectively.
  2. Run `arping -I br_eth0_25 the configured IP address` on one of the hosts to decide whether the IP address is connected. If not connected, check whether your switch is configured properly.
  3. Check whether the switch is configured with a trunk port, all VLAN IDs are allowed, and VLAN 25 is included in the VLAN database.
  4. Run `ip addr del the configured IP dev br_eth0_25` to delete the IP configurations on both hosts after intercommunications between these hosts are tested.
- For the VXLAN network, we recommend that you check whether the VTEP IP addresses corresponded by the VXLAN network can be intercommunicated properly.

32.

Q: Can one cluster attach multiple primary storages in ZStack? Can I couple with different types of primary storage?

A: ZStack lets one primary storage add multiple clusters, while one cluster can attach multiple primary storages. Currently, the supported scenarios are as follows:

- 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 Shared Block primary storages attached.
- A cluster can have one Shared Mount Point primary storages attached.
- A cluster can have only one Ceph primary storage attached.

33.
Q: What should I do when my compute node keeps reconnecting?

A: Log in to the compute node, and run the following commands successively. After settings, reconnect the compute node on the UI.

```
[root@10-0-5-87 ~]# kill -HUP `pgrep collectdmon
[root@10-0-5-87 ~]# service virtlogd restart
[root@10-0-5-87 ~]# service libvirtd restart
[root@10-0-5-87 ~]# service zstack-kvmagent restart
```

34.
Q: How can I restore the image that is accidentally deleted on a backup storage?

A: For the ImageStore backup storage, add this image to the backup storage again via UI. In the **Add Backup Storage** page, select **Import existing images**.

35.
Q: What are the differences between the available capacity and the available physical capacity in a host?

A:

- Available capacity: After the overprovisioned capacity of a primary storage is deducted, the equation for the rest of the virtual capacity on the host is: Available capacity = Total capacity - Volume (Root volume + data volume) / Overprovisioning ratio - Snapshot - Image cache - Used capacity of the system.
- Available physical capacity: Refer to the availably actual total capacity under the partitioned directory specified by the URL of each LocalStorage primary storage. The host is attached to the primary storage. Run the following command to check the capacity: df / The URL mounted by the primary storage, such as df /zstack_ps.

36.
Q: What should I do when kvm_zap_rmapp appeared in a host causes the host to shut down due to the kernel panic?

A:

- **Cause**:

  Run kvm_zap_rmapp. Then, the kernel crashes.

  The scope of impact: the versions earlier than kernel-3.10.0-327.53.1.el7.x86_64

> **Note:**
> The kernel version of ZStack CentOS 7.2 is 3.10.0-327.36.1.el7.x86_64.

For more information, see *Red Hat*.

- **Solution**:
  - You can upgrade the kernel of the compute node from the original CentOS 7.2 to the latest CentOS 7.4 of ZStack.
  - Also, you can reference the following method to temporarily address the problem:
    1. Add `options kvm_intel pml=0` to the KVM module configuration file of the compute node.
    2. Run the following command:

       ```
       echo "options kvm_intel pml=0" >>/etc/modprobe.d/kvm.conf
       ```
    3. Restart the host.

37.

Q: How can I disable the Prometheus service when using the ZStack community edition?

A:

1. Add the following parameters in the properties configuration file of your management node to disable the Prometheus service:

   ```
   Prometheus.versionMode=none
   ```
2. Run `zstack-ctl restart` to restart the management node.

38.

Q: How can I release more spaces when an ImageStore backup storage is out of capacity?

A: Delete the unavailable images. Navigate to **Hardware** > **Backup Storage** > **Actions** > **Clear Data**, and clear up the invalid data.

39.

Q: When I virtually split an AMD GPU, an error is reported. What should I do?

A:

- **Symptom**:

  When you virtually split an AMD GPU, an error is reported as follows:

  ```
  failed to remove gim.ko, , modprobe: FATAL: Module gim not found
  ```
- **Solution**:

Run the following commands:

```
[root@localhost ~]# wget https://github.com/GPUOpen-LibrariesA
ndSDKs/MxGPU-Virtualization/archive/master.zip    #Download the
dependency package.
[root@localhost ~]# unzip master.zip   #Decompress the file.
[root@localhost ~]# cd MxGPU-Virtualization-master
[root@localhost MxGPU-Virtualization-master]# make
[root@localhost MxGPU-Virtualization-master]# cp gim.ko /lib/
modules/3.10.0-693.11.1.el7.x86_64/
[root@localhost MxGPU-Virtualization-master]# depmod
[root@localhost MxGPU-Virtualization-master]# modprobe gim
```

18.6 Network

1. Q: What rates of NICs does ZStack support?

   A: ZStack supports 40G, Gigabit, and 10-Gigabit NICs. Gigabit NICs or above is recommended.

2. Q: Can I set different netmasks and gateways in the same L3 network?

   A: No, you cannot. This kind of configuration might cause network exceptions.

3. Q: How do I release the IP address occupied by the flat network service provider?

   A:

   - **Cause:**

     The flat network service provider provides DHCP services and therefore occupies an IP address.

   - **Solution:**

     If you do not want to use the DHCP service, you can delete the corresponding L3 network. However, the IP address occupied by the flat network service provider will not be released . You can use the following method to reclaim the IP address and eliminate the correspond ing impact.

     Run the following commands in all hosts:

     1. Run the `ip netns` command.
     2. Run the `ip netns delete xxxx` command for all output namespace. Note that xxxx is the namespace in the output of Step 1.
     3. Run the `ebtables -F` command.

4. Run the `pkill dnsmasq` command to kill all DHCP servers.

4.

Q: Is it true that ZStack supports only eth0? If yes, why em01 is not supported?

A: ZStack identifies NIC names according to your configuration. The NIC No. of all compute nodes in the same cluster must be the same.

- If you already added an eth0 L2 network, but the NIC of the new compute node is em01, not eth0, you will fail to add a host.
- If you chose eth0 when you add an L2 network, you must configure the eth0 network for all compute nodes.
- You can also set em01 as an L2 network. In this case, you must configure the em01 network for all compute nodes.
- You can delete an L2 network and configure it again.

5.

Q: Can I deploy the management network and business network together?

A: We recommend that you separate these two networks for security reasons and more reasonable network load balancing. You can deploy them together if network resources are insufficient.

6.

Q: Why an IP address is missing from the IP range? What is the IP address of the DHCP service?

A:

- For the first question, this IP address is assigned to the vRouter or DHCP server. You can see the IP address of the vRouter directly.
- For the second question, the IP address occupied by the DHCP server is used to provide the DHCP service and cannot be released. The IP address of the DHCP service can be viewed on the details page of the corresponding L3 network.

7.

Q: How can I modify the IP range of an L3 network in ZStack?

A: ZStack only allows you to add or delete IP ranges. To modify the IP range of an L3 network, add a new IP range and then delete the previous one. Next, restart the VM instance. Then, you can re-allocate IP addresses from the newly added IP range.

Note:

When you delete an IP range, note that:

- Deleting an IP range will cause the VM NIC that uses the IP range to be uninstalled. Please exercise caution.
- If the L3 network already has an IP address for the DHCP service and the IP address is within the chosen IP range, after the IP range is deleted, the IP address of the DHCP service will be retained. If all the IP ranges in the L3 network are deleted, the IP address of the DHCP service will be released.

8.

Q: How do I set a fixed IP address for VM instances in ZStack?

A: On the details page of a VM instance, click on the **Configurations** tab. On the **vNIC** tab page, select a network and click **Actions** > **Fixed IP** to set a fixed IP address for the VM instance.

Note:

Before you set a fixed IP address for a VM instance, stop the VM instance.

9.

Q: Why a 10 Gigabit NIC can recognize only one module?

A: The 10 Gigabit NIC added to your server has two optical modules. You must ensure that the brand models of these two optical modules are the same and match the NIC so that the modules can be recognized at the same time.

10.

Q: What should I do if the following error is reported when I create a vRouter network?

A:

- **Symptom:**

  The following error is displayed when you create a vRouter network:

```
"description": "A message or an operation timeout",
     "details": "[Async Http Timeout] url: http://10.10.10.253:
7272/init, timeout after 300000[MILLISECONDS], command: {\"uuid
\":\"78183b0a46094e30bc8a6128b30ee8cb\",\"restartDnsmasqAfterN
umberOfSIGUSER1\":0}"
   }
```

- **Cause:** The management network in the vRouter offering and the management node cannot ping each other.
- **Solution:** When you create a vRouter offering, select the correct management network.

11.

Q: Who provides the DHCP service for ZStack?

A: The flat network service provider provides the distributed DHCP service for the flat network, vRouter network, and VPC network of ZStack.

12.

Q: How do a host and VM instance ping each other?

A: A host and VM instance can ping each other as long as they belong to the same L2 network and share the same IP range. Note that the L2 network can be either a flat network or public network.

13.

Q: How load balancing is planned in ZStack? Does the Cloud support business plans such as NetScaler?

A: ZStack provides the load balancing service by using VPC vRouters or regular vRouters. The load balancing service mainly uses VIPs to distribute traffics to backend VM instances. That is, in load balancing scenarios, services are mainly provided by backend VM instances.

14.

Q: When I create an L2 network in ZStack, can I assign multiple VLANs to a physical NIC? Should I configure the corresponding switch to the trunk mode?

A: Yes, you can. Ports **1- 4094** are available. ZStack allows you to create multiple L2 VLAN networks on a NIC. After you connect to a switch, configure it to the trunk mode and allow VLAN.

15.

Q: I completed the VLAN settings, but the VLANs cannot communicate with each other. After the system enables iptables, do I need to add some other configurations to ensure VLAN communication?

A: The VLAN communication needs to be configured on the corresponding switch.

16.

Q: How do I log in to a VPC vRouter or regular vRouter?

A: The user name and password are required to log in to a vRouter. You can set the login password of a vRouter by going to **Settings** > **Global Settings** > **Basic Settings**.

- The administrator account of a vRouter is vyos, and the default login password is **vrouter12#**.
- After you set a password, you need to restart the vRouter via the UI for the password to take effect.
- This operation applies to all vRouter devices.

17.

Q: How do I troubleshoot if an elastic IP address is not available?

A:

- Check whether the default gateway inside the VM instance is configured and reachable.
- Check whether the physical link is reachable. Make sure that the corresponding L2 network wiring on each host is exactly the same.

18.

Q: When I create an L2 network, I failed to attach a cluster. Why?

A: Check whether the NIC name is filled in correctly. Before you can create an L2 network, make sure that hosts in the same cluster have the same NIC name.

19.

Q: If the NIC bonding is set incorrectly, how can I modify the setting?

A: Take bond0 as an example. Run the following commands in sequence to delete the incorrect bond:

```
[root@host ~]# ip link set br_XXX down   //Stop the bridge you
created before.
[root@host ~]# brctl delbr br_XXX    //Delete the bridge.
[root@host ~]# rm -f /etc/sysconfig/network-scripts/ifcfg-br_XXX
 //Delete the bridge configuration file.
[root@host ~]# zs-vlan -d bond0 XX    //Delete the VLAN sub
interface.
[root@host ~]# zs-bond-ab -d bond0    //Delete the incorrect bond.
```

Then, you can configure the network and add a bond from the beginning.

20.

Q: Does ZStack support IPv6?

A: ZStack 3.1.0 and later versions support IPv6. When you create a VM instance, you can select different types of IP addresses, such as IPv4, IPv6, and IPv4+IPv6.

21.

Q: What are the mechanism and default rules of a security group?

A: The security group is based on the allowlist mechanism. By default, if no rules are set for a newly created security group, all inbound traffics to access VM instances in the security group are not allowed, while outbound traffics from VM instances in the security group are not restricted.

22.

Q: Can I set QoS for networks and disks in ZStack? If yes, where can I set it? And what is the QoS range?

A: Yes, you can. You can set QoS when you create an instance offering or disk offering. You can also modify it on the configurations page of a VM instance. QoS range of a disk: 1 MB/s–100 GB/s. QoS of a NIC: 8 Kbps–30 Gbps.

23.
Q: Can I bind multiple elastic IP addresses to the same IP address of a VM instance?

A: Yes, you can set multiple elastic IP addresses for the same VM instance to meet different access requirements. Note that these elastic IP addresses can be used to access the same VM instance.

24.
Q: What should I do if I could not create virtual functions for physical NICs by using the SR-IOV feature?

A: To use the SR-IOV feature, make sure that your Cloud meets the following requirements:

- Virtual functions can be created for the NICs at the hardware level.
- The Intel VT-d and SR-IOV are enabled in the BIOS settings.
- In the Cloud, the **IOMMU State** of the corresponding host is enabled.

> **Note:**
> After you change the **IOMMU State** of a host, you need to restart the host for the change to take effect. You can check the state via the **IOMMU Status**.

25.
Q: I configured a bond for the server and set the bond to LACP mode. However, the network between the VM instances fluctuates greatly. How do I troubleshoot this issue?

A: You can troubleshoot this issue as follows:

1. Verify that the LACP is successfully aggregated and the switch is configured properly.
2. Verify that the same bond has the same NIC model.

> **Note:**
> You can check the NIC model by using `lspci |grep -i net`.

18.7 Platform Management O&M

1.
Q: Does ZStack support SPICE protocol?

A: Yes, it does. You can change the VM console mode by using the following method:

Go to **Settings** > **Global Settings** > **Basic Settings**, locate **Vm.consoleMode**, and change the mode from VNC to SPICE.

2. Q: Can ZStack connect to AD/LDAP? If yes, is it true that I can manage users by using API only?

   A: Yes, ZStack can connect to AD/LDAP and provides RESTful API documentation for your reference. For more information, see the *3rd Party Authentication Operations* chapter in the *API Reference*.

3. Q: How do I set the retention time for Prometheus data of a management node?

   A: Go to **Settings** > **Global Settings** > **Advanced**, locate **Retention time of Monitoring data** and **Retention size of Monitoring data**, and set their values as needed.

4. Q: What should I do if the monitoring data on the homepage of the Cloud UI is not displayed properly?

   A: Restart the Prometheus service to obtain the monitoring data. The restart method is as follows:

   - For versions earlier than 3.1.0, kill the Prometheus process in the management node and wait for the management node to pull up the monitoring service again (about 30 seconds).
   - For 3.1.0 and later versions, run the `systemctl restart prometheus` command in the management node to restart the monitoring service.

5. Q: In the global settings, how is the CPU overcommitment ratio calculated?

   A: CPU overcommitment is used to control the number of virtual CPUs (vCPUs) allocated to VM instances. The calculation formula is as follows: Number of vCPUs can be allocated = Total number of physical CPU threads x CPU overcommitment ratio.

   - Assume that the physical CPU you use has 12 cores and 24 threads. If the CPU overcommitment ratio in the global settings is set to 10, the number of vCPUs that can be allocated to VM instances is 240 cores.
   - Excessively large CPU overcommitment ratio might seriously affect the host performance and cause the business performance to freeze.

6. Q: In the global settings, how is the memory overcommitment ratio calculated?

A: Memory overcommitment is used to control the virtual memory capacity allocated to VM instances. The calculation formula is as follows: Virtual memory capacity can be allocated = Physical memory capacity x Memory overcommitment ratio.

- Assume that the physical memory is 128 GB. If the memory overcommitment ratio in the global settings is set to 2, the memory that can be allocated to VM instances is 256 GB.
- Excessively large memory overcommitment ratio might seriously affect the host memory performance and cause the out of memory (OOM) condition. Therefore, memory overcommitting is not recommended. If you do need to perform memory overcommitting, make sure that the overcommitment ratio does not exceed 1.2.

7.

Q: In the global settings, how is the primary storage overcommitment ratio calculated?

A: Primary storage overcommitment is used to control the available virtual primary storage space that can be allocated to VM instances. The calculation formula is as follows: Virtual primary storage space can be allocated = Physical primary storage space x Primary storage overcommitment ratio.

- Assume that the primary storage capacity is 2 TB. If the primary storage overcommitment ratio in the global settings is set to 2, the primary storage capacity is not changed after overcommitting. However, the primary storage capacity occupied by the volumes and snapshots is half of the actual capacity. For example, when you create a 100 GB volume (raw format), only 50 GB is occupied in the primary storage.
- Excessively large primary storage overcommitment ratio might seriously affect the storage pressure or cause the disk capacity to be fully occupied quickly and thus lead to system I/O errors. Therefore, primary storage overcommitting is not recommended. If you do need to perform primary storage overcommitting, make sure that the overcommitment ratio does not exceed 1.2.

8.

Q: If the Enterprise license expires, will the VM instances be stopped automatically?

A: No, the VM instances will not be stopped automatically after a license expires. However, you can no longer perform operations in the Cloud. To continue to use the Cloud, apply for a license again.

9.

Q: If I forget the Cloud UI login password, how can I reset it?

A: Run the **`zstack-ctl reset_password --password NEW_PASSWORD`** command in the management node and change **`NEW_PASSWORD`** to a new password.

10. Q: How do I change the management IP address in a compute node?

    A:

    1. Place the target compute node into maintenance mode.

       > **Note:**
       > Make sure that the VM instances in this node are migrated to other hosts or are in the shutdown state.

    2. Log in to the compute node by accessing the display or using IPMI.
    3. Change the static IP address in the configuration file of the management NIC.
    4. Restart the network service.
    5. Log in to the Cloud, choose **Hardware** > **Host**, and change the host IP address on the details page of the target host.
    6. Wait for the host to reconnect.

18.8 Advanced Function

1. Q: What should I do if a Bare Metal chassis cannot obtain the hardware information?

   A: **To solve this problem, ensure that:**

   - Other DHCP services are not included in the deployment network except for the deployment server.
   - The NIC where the Bare Metal chassis connects to the deployment network has enabled PXE.

     > **Note:**
     > - For part of Bare Metal model, ensure that this PXE NIC is firstly booted. Or, ensure that (boot sequence) all NICs before the PXE NIC must disable PXE.

   - The boot mode of the Bare Metal chassis is Legacy.

Glossary

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 ZStack.

Cluster

A cluster is a logical group of analogy hosts (compute nodes). Hosts in the same cluster must be installed with the same operating system, have the same network configuration, and be able to access the same primary storage. In a real data center, a cluster usually maps to a rack.

Management Node

A management node is a host with operating system installed to provide UI management and Cloud deployment.

Compute Node

A compute node is a physical server (also known as a host) that provides VM instances with compute, network, and storage resources.

Primary Storage

A primary storage is a storage server used to store disk files in VM instances. Local storage, NFS, Ceph, Shared Mount Point, and Shared Block are supported.

Backup Storage

A backup storage is a storage server used to store image template files. ImageStore, SFTP (Community Edition), and Ceph are supported. We recommend that you deploy backup storage separately.

ImageStore

ImageStore is a type of backup storage. You can use ImageStore to create images for VM instances that are in the running state and manage image version updates and release. ImageStore allows you quickly upload, download, export images, and create image snapshots as needed.

VM Instance

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

Image

An image is an image template used by a VM instance or volume. Image templates include system volume images and data volume images.

Volume

A volume can either be a data volume or a root volume. A volume provides storage to a VM instance. A shared volume can be attached to one or more VM instances.

Instance Offering

An instance offering is a specification of the VM instance CPU and memory, and defines the host allocator strategy, disk bandwidth, and network bandwidth.

Disk Offering

A disk offering is a specification of a volume, which defines the size of a volume and how the volume will be created.

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.

L3 Network

An L3 network is a collection of network configurations for VM instances, including the IP range, gateway, and DNS.

Public Network

A public network is generally allocated with a public IP address by Network Information Center (NIC) and can be connected to IP addresses on the Internet.

Private Network

A private network is the internal network that can be connected and accessed by VM instances.

L2NoVlanNetwork

L2NoVlanNetwork is a network type for creating an L2 network. If L2NoVlanNetwork is selected, VLAN settings are not used for host connection.

L2VlanNetwork

L2VlanNetwork is a network type for creating an L2 network. If L2VlanNetwork is selected, VLAN settings are used for host connection and need to be configured on the corresponding switches in advance.

VXLAN Pool

A VXLAN pool is an underlay network in VXLAN. You can create multiple VXLAN overlay networks (VXLAN) in a VXLAN pool. The overlay networks can operate on the same underlay network device.

VXLAN

A VXLAN network is a L2 network encapsulated by using the VXLAN protocol. A VXLAN network belongs to a VXLAN pool. Different VXLAN networks are isolated from each other on the L2 network.

vRouter

A vRouter is a custom Linux VM instance that provides various network services.

Security Group

A security group provides L3 network firewall control over the VM instances. It can be used to set different security rules to filter IP addresses, network packet types, and the traffic flow of network packets.

EIP

An elastic IP address (EIP) is a method to access a private network through a public network.

Snapshot

A snapshot is a point-in-time capture of data status in a disk. A snapshot can be either an automatic snapshot or a manual snapshot.