



Technical Whitepaper

Version: ZStack 3.9.0

Issue: V3.9.0

Copyright Statement

Copyright © 2020 Shanghai Yunzhou Information and Technology Ltd. All rights reserved.

Without its written consent, any organization and any individual do not have the right to extract, copy any part or all of, and are prohibited to disseminate the contents of this documentation 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 documentation 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 documentation may not be in the scope of your purchase or use. Unless there are additional conventions, Shanghai Yunzhou Information and Technology Ltd. will not claim any implicit or explicit statement or warranty on the contents of this documentation.

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

Contents

Copyright Statement.....	I
1 Product Overview.....	1
2 Product Profiles.....	2
2.1 ZStack Functional Architecture.....	2
2.2 ZStack Resource Model.....	5
2.2.1 Resource Pool.....	9
2.2.1.1 VM Instance.....	9
2.2.1.2 Volume.....	9
2.2.1.3 Image.....	9
2.2.1.4 Affinity Group.....	11
2.2.1.5 Instance Offering.....	13
2.2.1.6 Disk Offering.....	13
2.2.1.7 GPU Specification.....	13
2.2.1.8 Auto Scaling Group.....	13
2.2.1.9 Snapshot.....	15
2.2.2 Hardware.....	15
2.2.2.1 Zone.....	15
2.2.2.2 Cluster.....	16
2.2.2.3 Host.....	20
2.2.2.4 Primary Storage.....	21
2.2.2.5 Backup Storage.....	22
2.2.2.6 SAN Storage.....	25
2.2.3 Network Resource.....	26
2.2.3.1 Network Diagram.....	26
2.2.3.2 SDN Controller.....	27
2.2.3.3 L2 Network Resource.....	27
2.2.3.4 L3 Network.....	30
2.2.3.5 Route Resource.....	33
2.2.3.6 VPC.....	35
2.2.4 Network Service.....	38
2.2.4.1 Security.....	42
2.2.4.1.1 VPC Firewall.....	42
2.2.4.1.2 Security Group.....	44
2.2.4.2 VIP.....	45
2.2.4.3 EIP.....	47
2.2.4.4 Port Forwarding.....	50
2.2.4.5 Load Balancing.....	51
2.2.4.6 IPsec Tunnel.....	53
2.2.4.7 Flow Monitoring.....	54
2.2.4.7.1 Flow Network.....	54
2.2.4.7.2 Port Mirroring.....	54

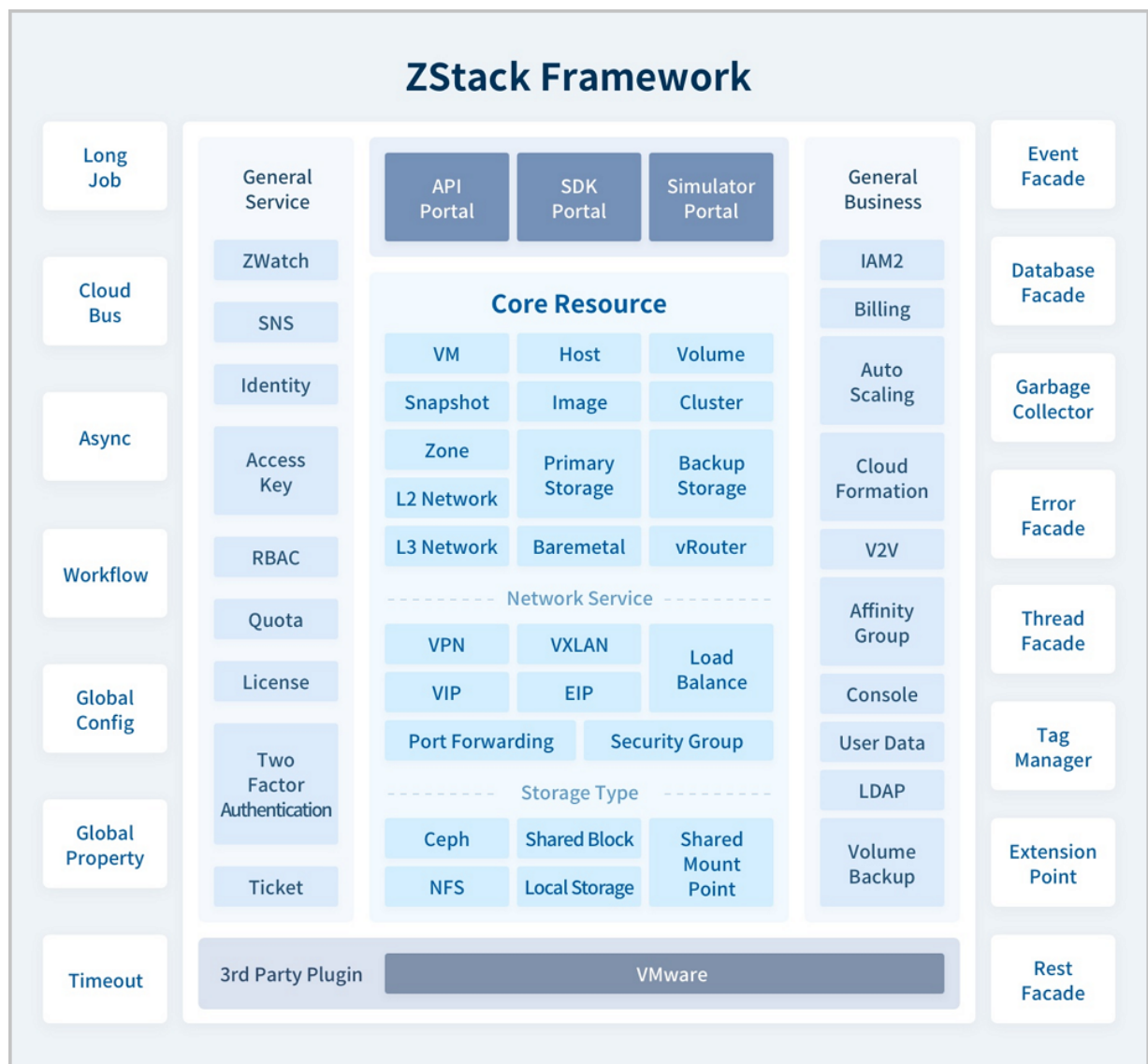
2.2.4.7.3 Netflow.....	54
2.2.5 vCenter Manipulation.....	55
2.2.6 Platform O&M.....	58
2.2.6.1 Performance TOP5.....	58
2.2.6.2 Performance Analysis.....	60
2.2.6.3 Capacity Management.....	61
2.2.6.4 ZWatch.....	61
2.2.6.5 Notification Service.....	64
2.2.6.6 Notification Center.....	65
2.2.6.7 Operation Log.....	65
2.2.6.8 CloudFormation.....	67
2.2.7 Platform Management.....	68
2.2.7.1 User Management.....	68
2.2.7.2 Billing Management.....	69
2.2.7.2.1 Bills.....	69
2.2.7.2.2 Pricing List.....	69
2.2.7.3 Job Scheduling.....	70
2.2.7.3.1 Scheduler.....	70
2.2.7.3.2 Scheduled Job.....	70
2.2.7.4 Tag.....	70
2.2.7.5 Application Center.....	71
2.2.7.6 Email Server.....	71
2.2.7.7 Log Server.....	71
2.2.7.8 AD/LDAP.....	72
2.2.7.9 Console Proxy.....	72
2.2.7.10 MN Monitoring.....	73
2.2.7.11 IP Blacklist/Whitelist.....	73
2.2.7.12 Certificate.....	73
2.2.7.13 AccessKey Management.....	73
2.2.8 Advanced Function (Plus).....	74
2.2.8.1 Enterprise Management.....	74
2.2.8.1.1 Organization.....	78
2.2.8.1.2 User.....	79
2.2.8.1.3 Role.....	80
2.2.8.1.4 3rd Party Authentication.....	80
2.2.8.1.5 Project Management.....	81
2.2.8.1.6 Ticket Management.....	83
2.2.8.2 BareMetal Management.....	84
2.2.8.2.1 Bare Metal Cluster.....	86
2.2.8.2.2 Deployment Server.....	86
2.2.8.2.3 Bare Metal Chassis.....	87
2.2.8.2.4 Preconfigured Template.....	87
2.2.8.2.5 Bare Metal Instance.....	88
2.2.8.3 Backup Service.....	88

2.2.8.3.1 Backup Task.....	93
2.2.8.3.2 Local Backup Data.....	94
2.2.8.3.3 Local Backup Storage.....	95
2.2.8.3.4 Remote Backup Storage.....	95
2.2.8.4 Migration Service.....	96
2.2.8.4.1 V2V Migration.....	97
2.2.8.4.2 Conversion Host.....	99
3 Product Features.....	100
4 Product Highlights.....	144
Glossary.....	146

1 Product Overview

ZStack is the next-generation, open-source IaaS software designed mainly for future-oriented, smart data centers. Additionally, 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 application scenarios, such as VDI, PaaS, and SaaS, on the stable ZStack.

Figure 1-1: ZStack Framework

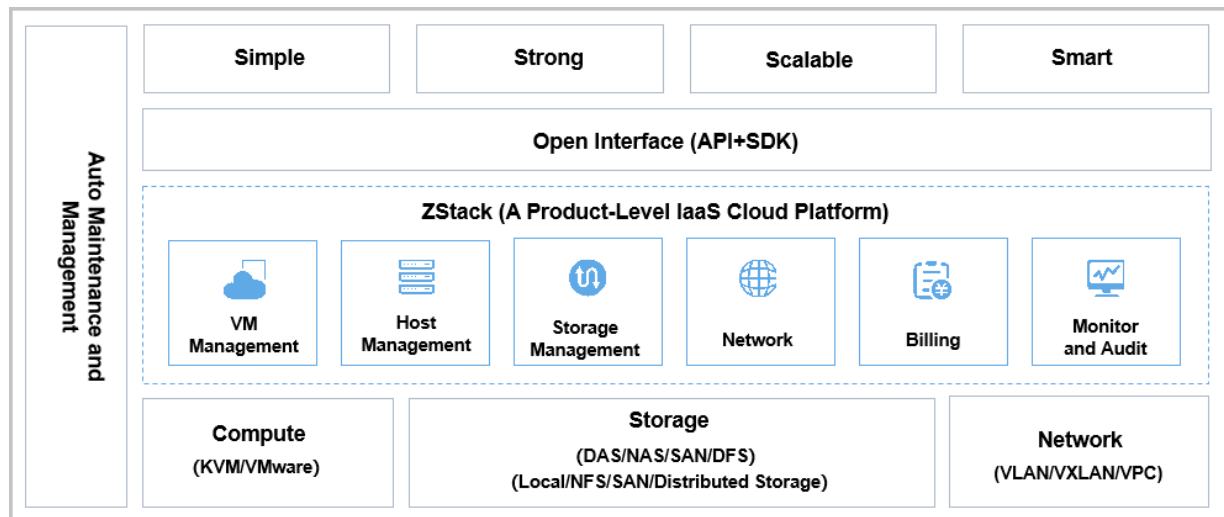


2 Product Profiles

2.1 ZStack Functional Architecture

The functional architecture of ZStack is shown in [Figure 2-1: ZStack Functional Architecture](#).

Figure 2-1: 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 centralized 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

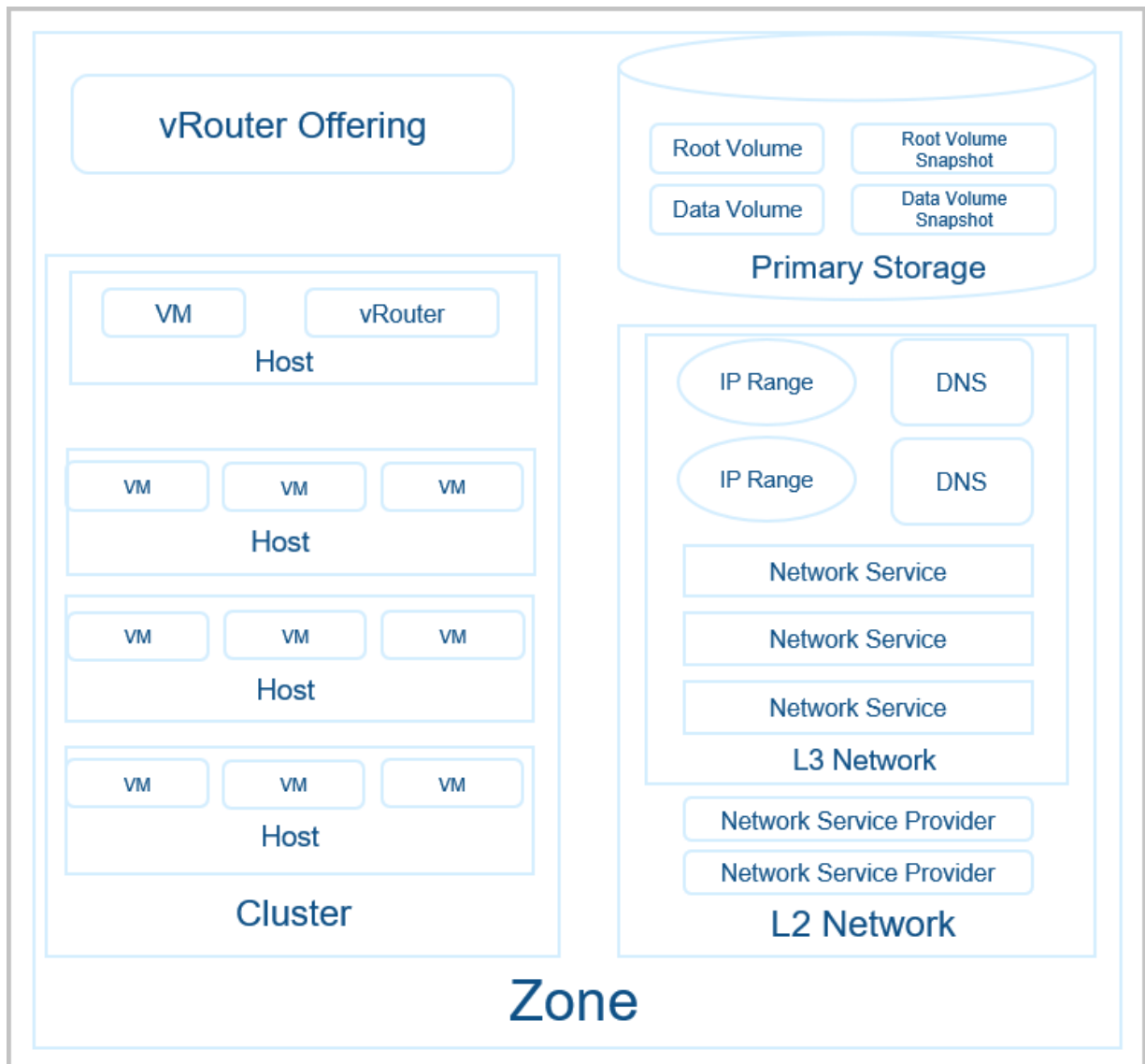
- Being seamlessly integrated with Ansible (which is agentless), ZStack can automatically install dependencies, configure physical resources, and deploy agents. This whole process is transparent to users and requires no additional intervention. You can upgrade your agents simply by reconnecting the agents.

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.

2.2 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 2-2: ZStack Resource Model](#).

Figure 2-2: 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.

2.2.1 Resource Pool

2.2.1.1 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.

2.2.1.2 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.

2.2.1.3 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.

2.2.1.4 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):

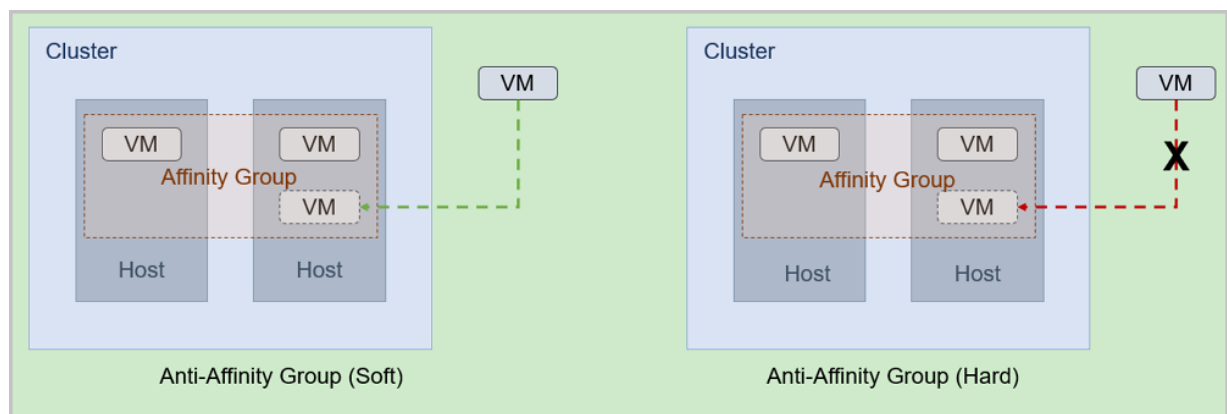
Allocates VM instances in the affinity group to different hosts as much as possible. If no more hosts are available, the VM instances will be allocated randomly.

- Anti-affinity group (hard):

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

As shown in [Figure 2-3: Anti-Affinity Group \(Soft\) and Anti-Affinity Group \(Hard\)](#).

Figure 2-3: Anti-Affinity Group (Soft) and Anti-Affinity Group (Hard)



Usage Scenario

The following are application examples of anti-affinity group (soft) and anti-affinity group (hard) policies.

- Application scenario of 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.

- Application scenario of anti-affinity group (hard):

You might want to deploy two VM instances that run an active and a standby databases on different hosts to ensure high availability of services.

- For example, you deploy two appliance VM instances to run an active and a standby MySQL databases 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 in advance which hosts have 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 of services.

2.2.1.5 Instance Offering

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

2.2.1.6 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.

2.2.1.7 GPU Specification

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) specification or a virtual GPU (vGPU) specification.

- pGPU specification: Display a list of physical GPU specifications detected on all hosts within the cloud and associated basic information of the physical GPU specifications.
- vGPU specification: Display a list of available virtual GPU specifications that have been virtually split and associated basic information of the virtual GPU specifications.

2.2.1.8 Auto Scaling Group

ZStack provides the auto scaling feature based on load balancing to better manage VM instances. With the auto scaling feature, the number of VM instances in an auto scaling group is automatically adjusted according to your business load changes and predefined policies. This

helps to better leverage the cloud resources, reduce the O&M costs, and ensure smooth business operations. Currently, the auto scaling feature is applicable to KVM-type VM instances.

Scaling Mode

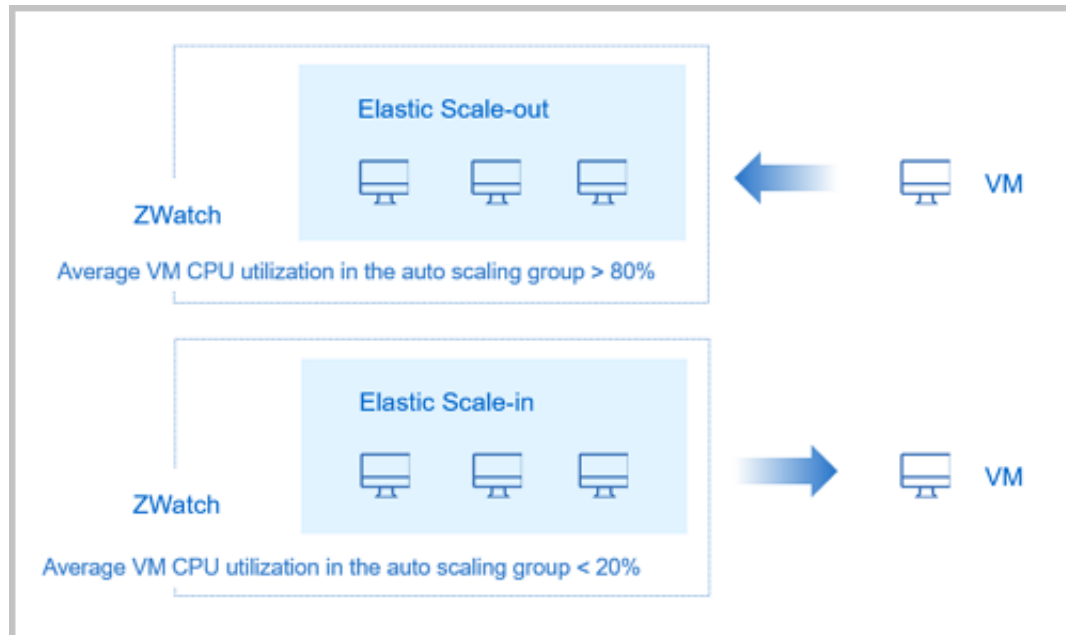
Two types of scaling mode are supported on the cloud as follows:

1. Auto Scaling

- Auto scaling includes elastic scale-in and elastic scale-out. For the elastic scale-in, when your business is growing, VM instances will be automatically added to ensure your business continuity. For the elastic scale-out, when your business decreases, VM instances will be automatically reduced.
- With the ZWatch monitoring alarm, the auto scaling mode can be triggered. You can customize endpoint types, including email, DingTalk, HTTP application, and short message service.

The auto scaling is shown in [Auto Scaling](#).

Figure 2-4: Auto Scaling



2. Elastic Self-Health

- In the elastic self-health mode, an auto scaling group monitors the health state of the VM instances within the auto scaling group, and automatically replaces the unhealthy VM instances with new VM instances. In this regard, healthy VM instances within the auto

scaling group will be ensured to be adjusted not lower than the minimum specified VM count

- Two types of health check are provided to trigger the elastic self-health, including load balancing health check and VM health check. If an auto group configures the load balancing feature, 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 2-5: Elastic Self-Health



2.2.1.9 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.

2.2.2 Hardware

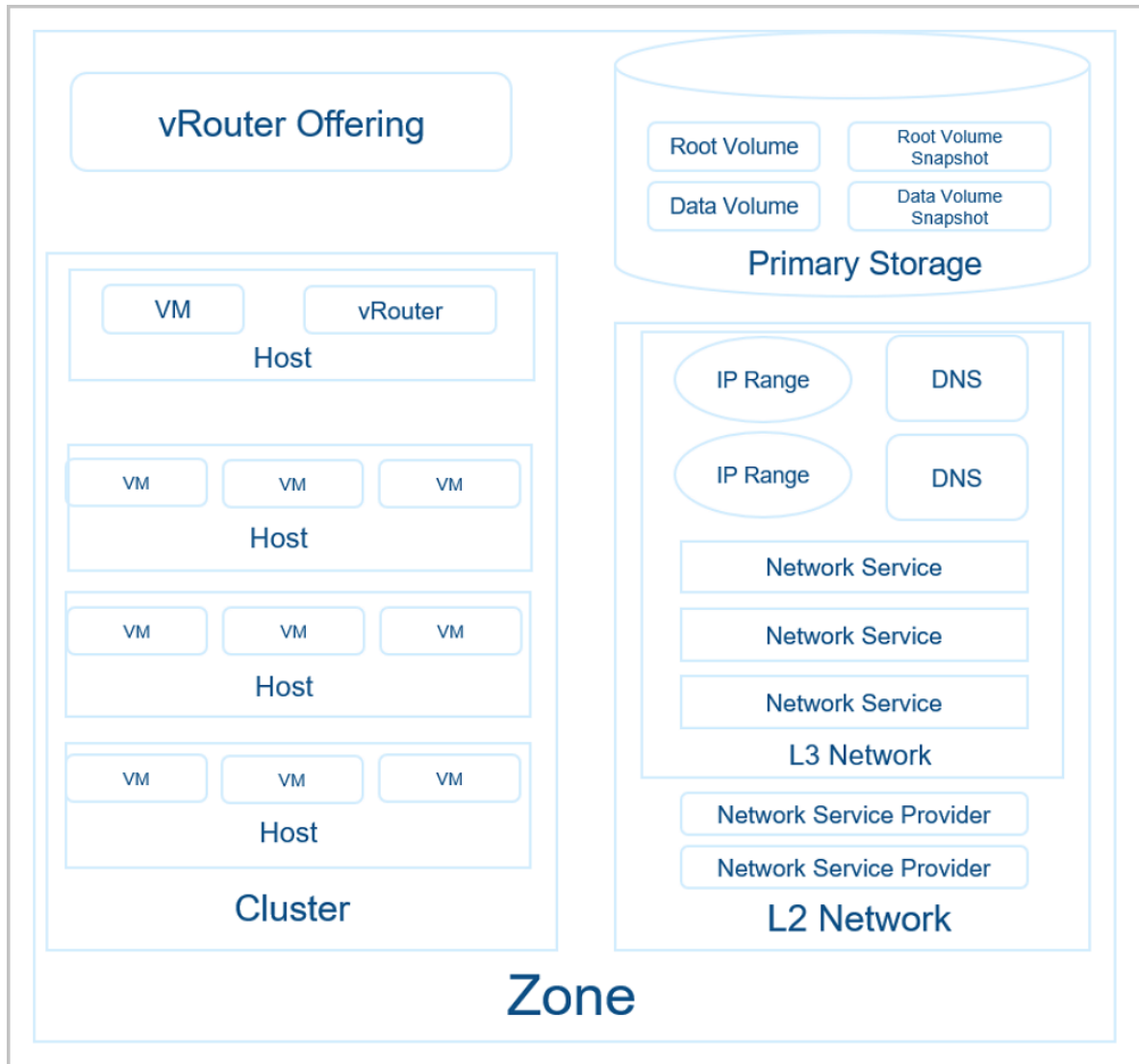
2.2.2.1 Zone

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 2-6: Zone Resource Structure



2.2.2.2 Cluster

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

When you organize a cluster, make sure 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.

The relationship between a typical cluster and its associated resources is as follows.

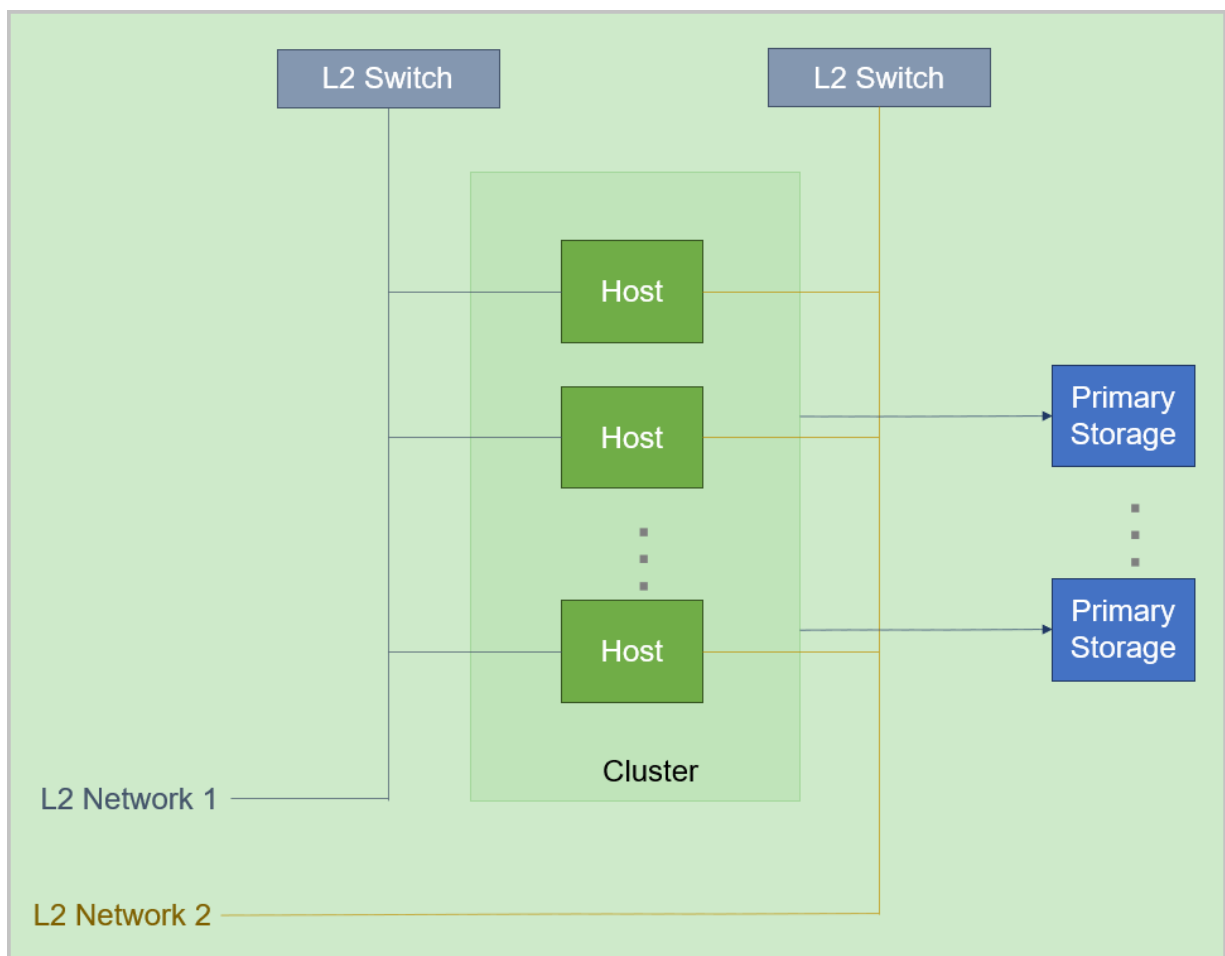
Cluster | Zone

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.

Cluster | Primary Storage and L2 Network

Primary storage and L2 network can be attached to or detached from a cluster. The following diagram shows the relationship between cluster and primary storage, L2 network, as shown in [Figure 2-7: Relationship Between Cluster and Primary Storage, L2 Network](#).

Figure 2-7: Relationship Between Cluster and Primary Storage, L2 Network



Note:

When you attach a primary storage and an L2 network to a cluster, make sure that:

1. Cluster | Primary Storage

- A primary storage can be attached to one or more clusters.
- A cluster can have one or more primary storages attached.

The following are primary storages of the same type that a cluster can have:

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

The following table lists the relationship between primary storages and a cluster, as shown in [Table 2-1: Relationship Between Primary Storage and Cluster](#).

Table 2-1: 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.

Primary Storage	Cluster
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 Share Mount Point attached.
LocalStorage + Shared Block	A cluster can have one LocalStorage + one Shared Block attached.
Ceph + Shared Block	<ul style="list-style-type: none"> • A cluster can have one Ceph + one Shared Block attached. • 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.

2. Cluster | L2 Network

- A cluster can have one or more L2 networks attached. Also, an L2 network can be attached to one or more clusters.
- A cluster can have a VXLAN pool attached. The VNIs in the VXLAN pool can be used to create different 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.

Cluster | Backup Storage

No direct dependency exists between cluster and 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 2-2: Relations Between Primary Storage and Backup Storage](#).

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

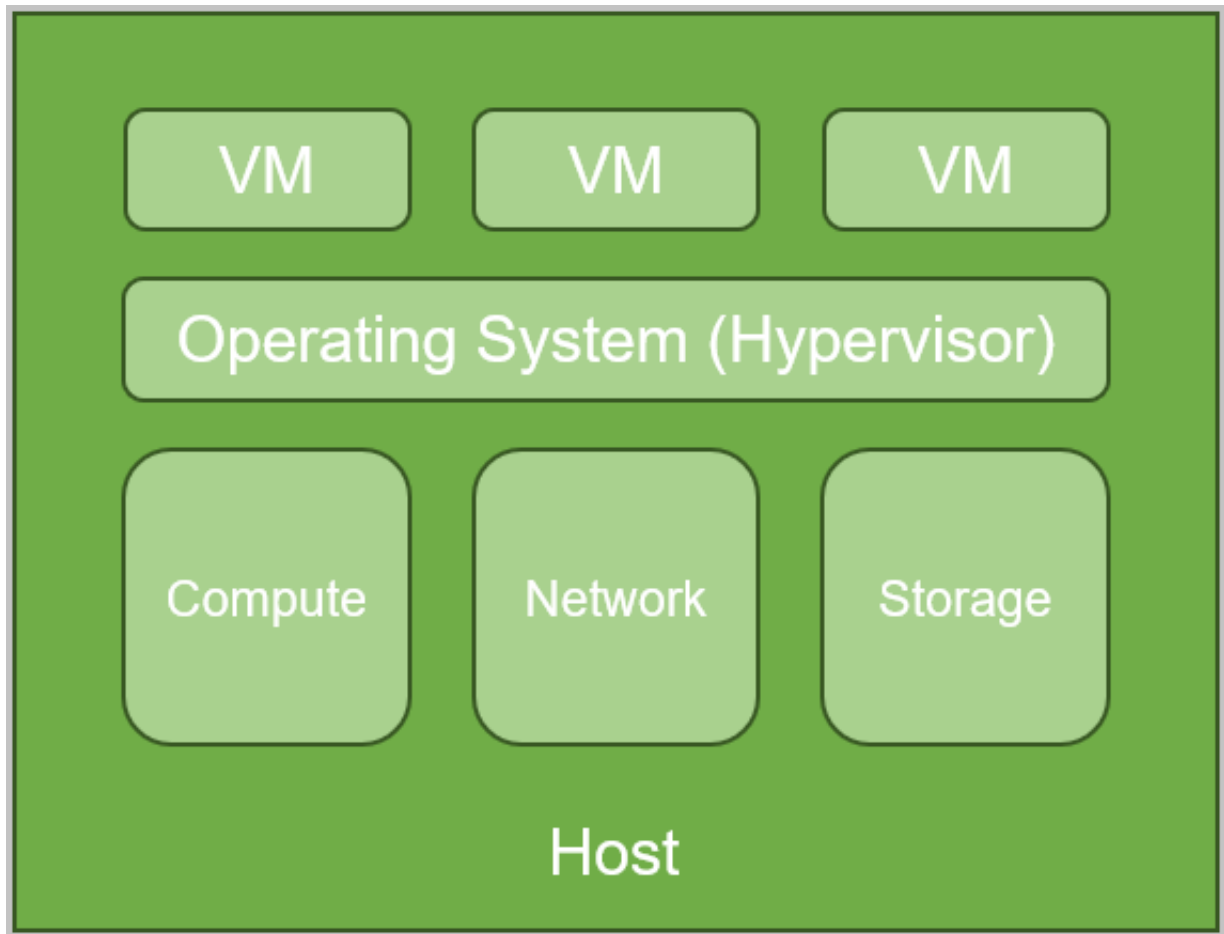
PS/BS	ImageStore	SFTP	Ceph
LocalStorage	○	○	×
NFS	○	○	×
Shared Mount Point	○	○	×
Ceph	○	×	○
Shared Block	○	×	×

2.2.2.3 Host

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

- Host is the core asset in ZStack. VM instances run on hosts.

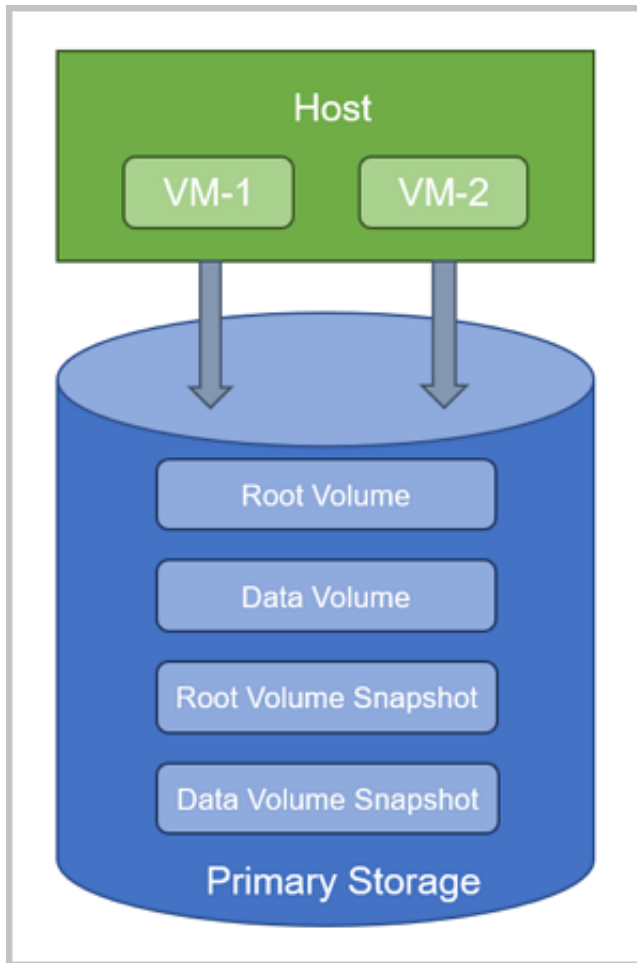
As shown in [Figure 2-8: Host](#).

Figure 2-8: Host

2.2.2.4 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 2-9: Primary Storage

A primary storage can either be a local storage or a shared storage.

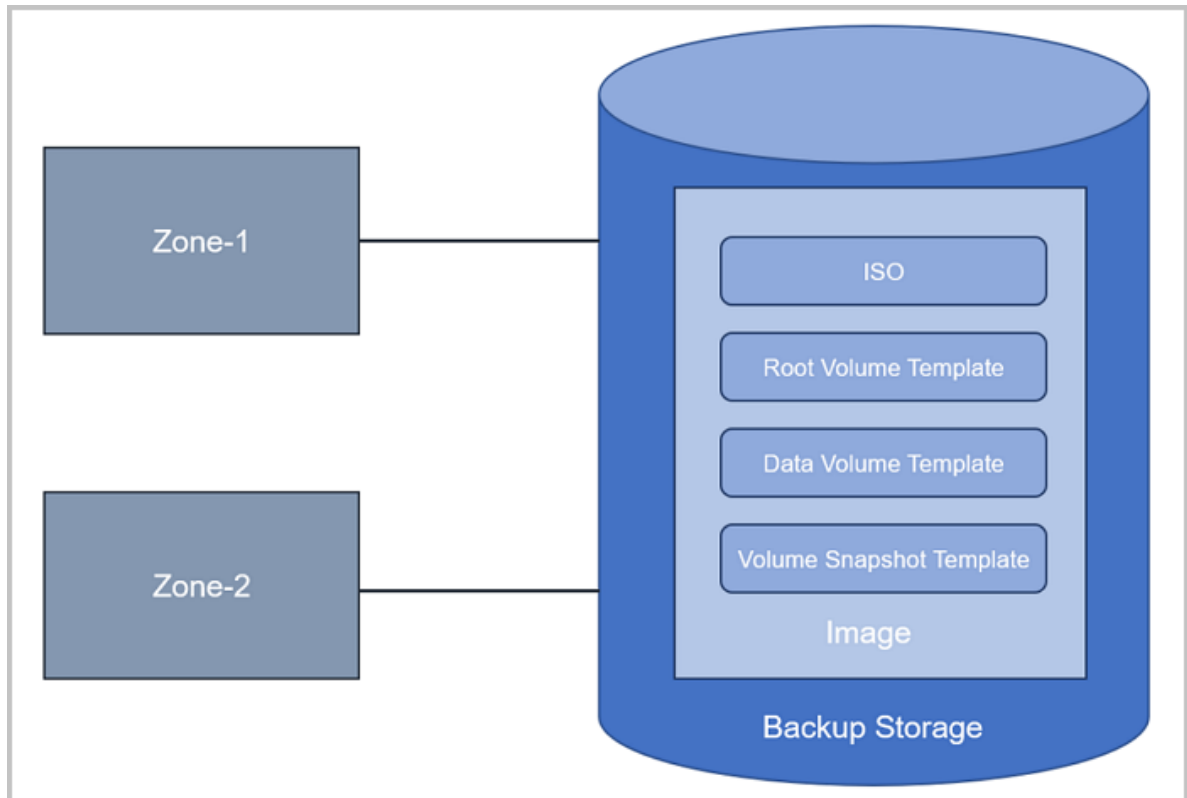
- **Local Storage:** Use the hard disks of a host to store disk files.
- **Network Shared Storage:** Support NFS, Shared Mount Point, Ceph, and Shared Block, .
 - NFS is a network file system storage.
 - Shared Mount Point supports network shared storages provided by commonly used distributed file systems such as MooseFS, GlusterFS, OCFS2, and GFS2.
 - Ceph uses distributed block storages.
 - Shared Block uses shared block storages.

2.2.2.5 Backup Storage

A backup storage is a storage server used to store image template files.

- A backup storage must be attached to a zone before the resources on the zone can reach it. Note that you can share images across multiple zones by using the backup storage, as shown in [Backup Storage](#).

Figure 2-10: 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 that attaches the zone will also be deleted.

Backup Storage Type

A backup storage supports the following types:

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 SharedBlock 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 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 disk volumes, the VM instances that are running, paused, or stopped can be cloned.
- VM instances cannot be cloned with data volumes.
- Images must 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 /root/export-test.image

# bak-t-c9923f9821bf45498fdf9cdfa1749943 is the pool name where
the image belongs to.
# 61ece0adc7244b0cbd12dafbc5494f0c is the image name.
# /root/export-test.image is the exported target file name.
```

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 2-3: 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 SharedBlock, the default type for backup storages is ImageStore.

2.2.2.6 SAN Storage

ZStack lets you to take over LUN devices segmented from iSCSI-SAN or FC-SAN storages. Specifically, these LUN devices can be either passed through directly to VM instances or added as SharedBlock primary storages. With the cloud, you can manipulate SAN storages, including iSCSI storage and FC storage.

iSCSI Storage

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.

2.2.3 Network Resource

2.2.3.1 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 diagram (Custom) for your custom resources where you can quickly locate the resource states.

Figure 2-11: All

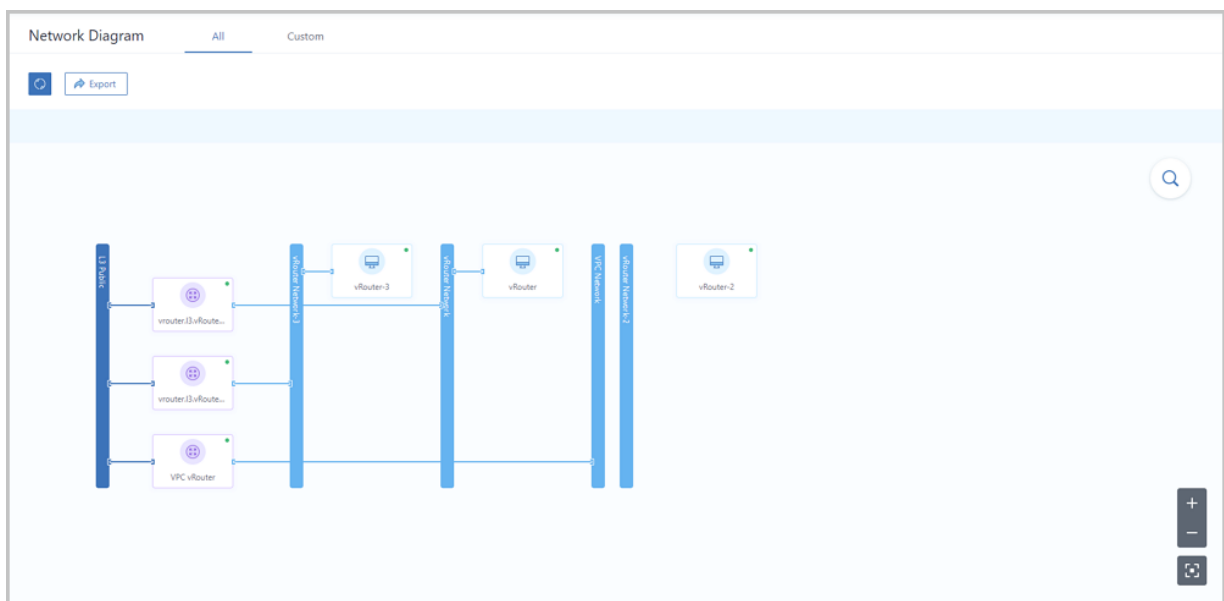
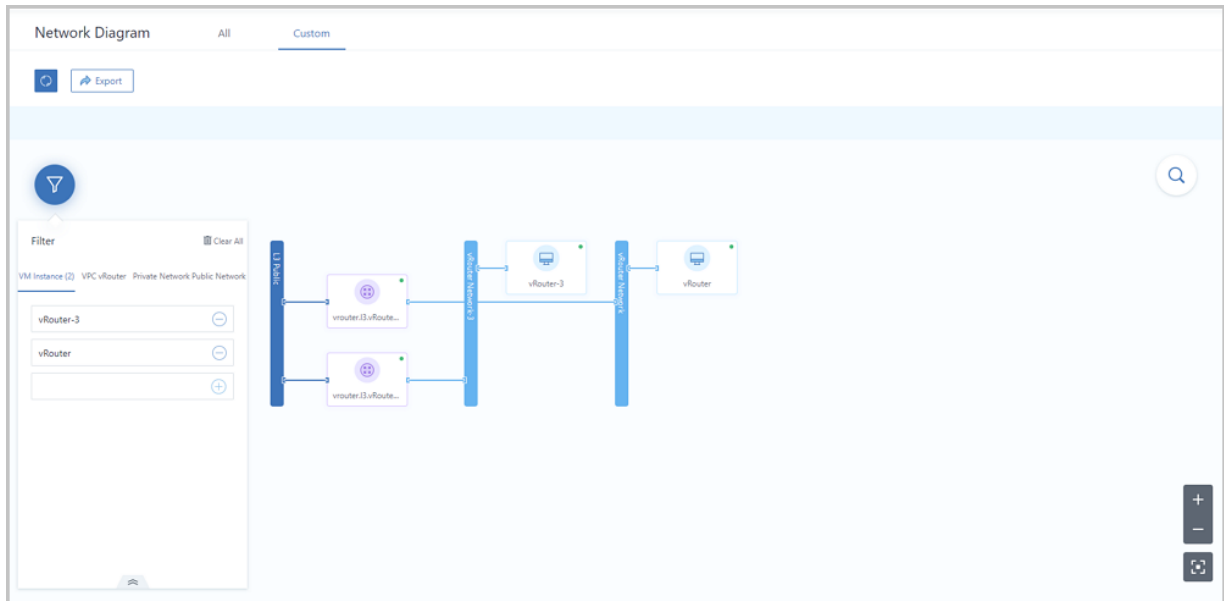


Figure 2-12: Custom

2.2.3.2 SDN Controller

By adding an SDN controller, you can take over SDN networks of hardware switches to reduce network latencies and improve VXLAN network performances.

- To add an SDN controller to the cloud, plan for management networks in advance, and complete preparing the basic configurations for the SDN controller.
- Currently, the cloud only allows you to add an H3C SDN controller: VCFC.

2.2.3.3 L2 Network Resource

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.

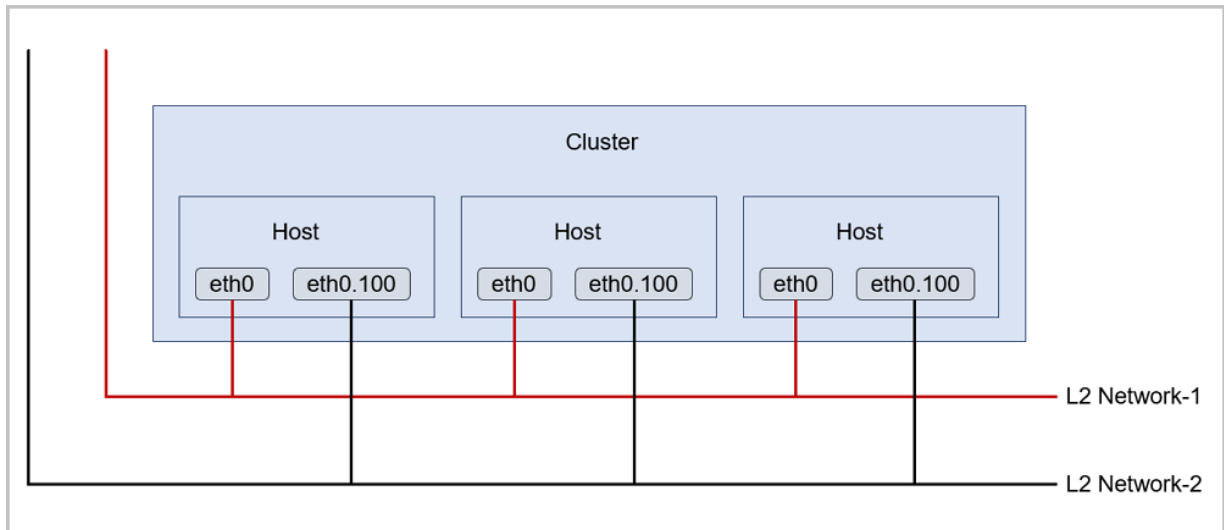
— Hardware SDN:

- 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.

L2 Network

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

- VLAN, VXLAN, or SDN can be used as an L2 network and can provide layer 2 isolation.
- An L2 network is used to provide layer 2 isolation for an L3 network, as shown in [L2 Network](#).

Figure 2-13: 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.

2.2.3.4 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, you can specify the IP range from *172.20.12.2* to *172.20.12.255*, set the netmask to *255.255.0.0*, and set the gateway to *172.20.0.1*. In addition, you can use a CIDR to specify 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 can specify 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, you need to 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.

2.2.3.5 Route Resource

A virtual router network (vRouter network) mainly uses custom Linux VM instances as route devices. The vRouter VM instances provide many network services, such as DHCP, DNS, SNAT, vRouter table, elastic IP (EIP), port forwarding, load balancing, IPsec tunnel, and security group.

A vRouter network mainly includes a vRouter image, vRouter offering, and vRouter.

- vRouter image: Encapsulates many network services, and is used only to create vRouters.
- vRouter offering: Defines the resources used by a vRouter, including the CPU, memory, vRouter image, public network, and management network.
- vRouter: Acts as a custom Linux VM instance and provides network services such as DHCP, DNS, SNAT, route table, EIP, port forwarding, load balancing, IPsec tunnel, and security group.

vRouter Network Topology

A vRouter VM instance mainly includes the following three basic networks:

- Public network

Provides virtual IPs for user VM instances that use EIP, port forwarding, load balancing, and IPsec tunnel. Generally, the public network must be accessible to the Internet.

- Management network

Manages and controls the corresponding physical resources, such as a host, backup storage, and primary storage, of whose resources can be reached by using an IP address.

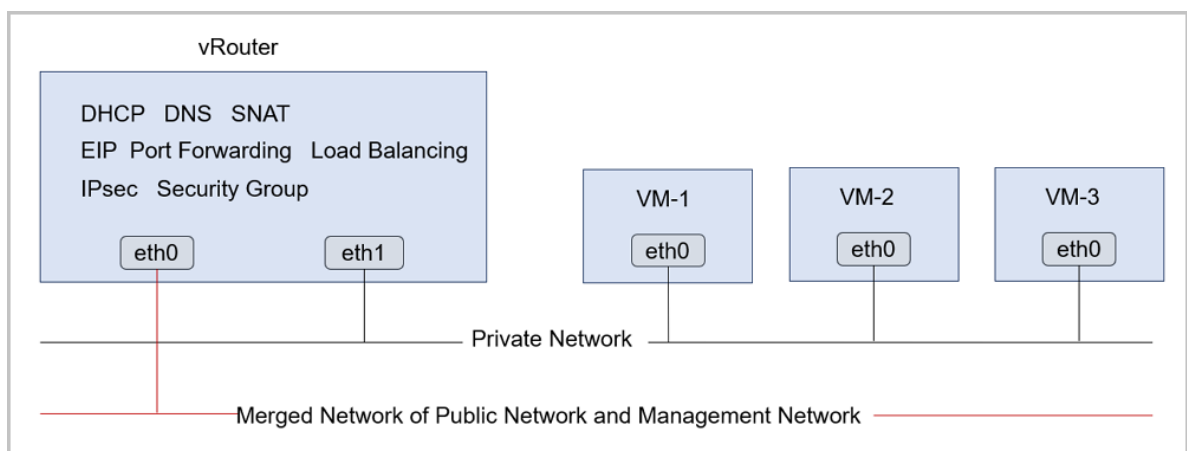
- Private network

Also known as the business network or the access network and is the internal network used by VM instances.

Here is the deployment mode of the vRouter network.

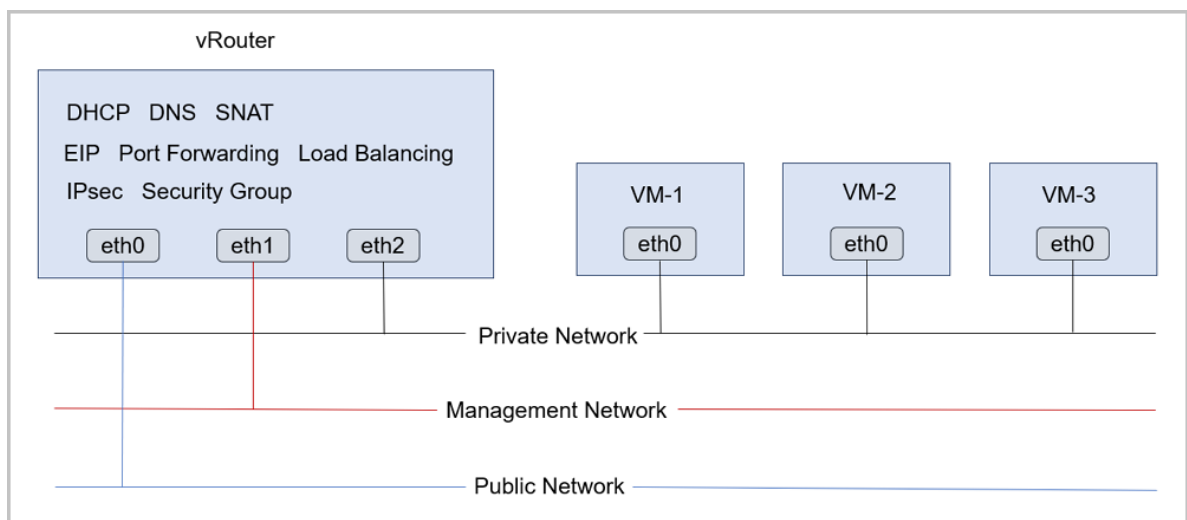
- You can combine the public network and the management network, while deploying the private network independently, as shown in [Deployment Mode-1](#).

Figure 2-14: Deployment Mode-1



- You can deploy the public network, management network, and private network separately, as shown in [Deployment Mode-2](#).

Figure 2-15: Deployment Mode-2



vRouter Network Service

The vRouter VM instances provide a collection of network services, including the DHCP, DNS, SNAT, route table, EIP, port forwarding, load balancing, IPsec tunnel, and security group.

- DHCP
 - In a vRouter, the DHCP service is provided by the flat network by default.
- DNS
 - A vRouter can act as a DNS server to provide the DNS service.
 - The DNS address in a vRouter VM instance is the vRouter IP address. Note that the DNS address that you set is forwarded by the vRouter.
- SNAT
 - A vRouter can act as a router to translate the source network address for VM instances.
 - VM instances can directly access the Internet by using SNAT.
- We will introduce the vRouter table, security group, EIP, port forwarding, load balancing, and IPsec in specific sections.
- 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:
 - The security group network service module provides security group services.
 - You can manipulate securities of VM instance firewalls by using iptables.

2.2.3.6 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

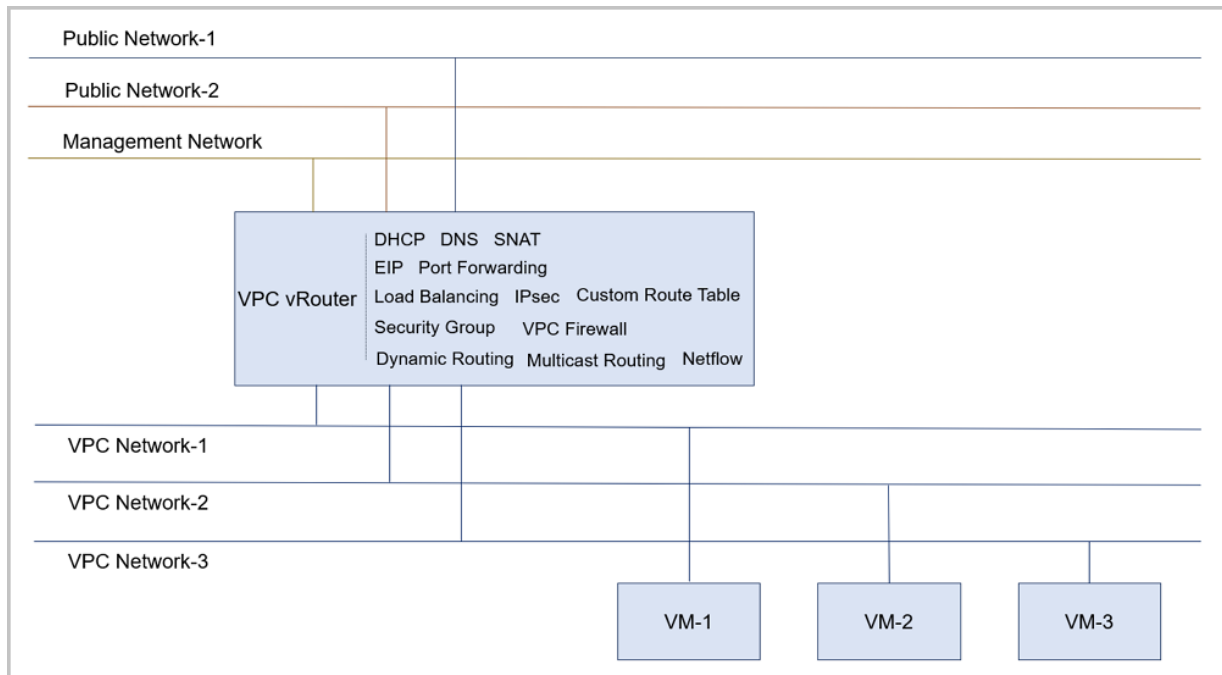
VPC consists of VPC vRouters and VPC networks.

- A VPC vRouter is a virtual router that you can directly create by attaching a vRouter offering.
By default, a VPC vRouter has two types of network: public network and management network.

- A VPC network can be used as a VPC private network, and can be attached to a VPC vRouter.

The VPC network topology is shown in [VPC Network Topology](#).

Figure 2-16: VPC Network Topology



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, effectively 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.

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.

2.2.4 Network Service

ZStack provides VM instances with multiple network resources, including the security group, virtual IP address (VIP), elastic IP address (EIP), port forwarding, load balancing, and IPsec tunnel.

ZStack supports the following three network models:

- Flat network
- vRouter network
- VPC

Network Service Module

Network Service Module provides 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)

This module provides the following network services: DNS, SNAT, load balancing, port forwarding, EIP, and DHCP.

2. Flat Network Service Module (Flat Network Service Provider)

This module provides the following network services:

- Userdata: Customizes some operations, such as `ssh-key` injection, by using the userdata service. Then, the `cloud-init` plugin in your VM instance will load and perform these operations 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 covers the DNS feature.

- VIP QoS: Adjusts the upstream bandwidth and downstream bandwidth, and can only be applied to EIPs.

3. vRouter Network Service Module

This 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

This 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
 - Userdata: Customizes some operations, such as `ssh-key` injection, by using the userdata service. Then, the `cloud-init` plugin in your VM instance will load and perform these operations 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 covers 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
 - Userdata: Customizes some operations, such as `ssh-key` injection, by using the userdata service. Then, the `cloud-init` plugin in your VM instance will load and perform these operations 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

- Userdata: Customizes some operations, such as `ssh-key` injection, by using the userdata service. Then, the `cloud-init` plugin in your VM instance will load and perform these operations 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.
- 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.

- 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.

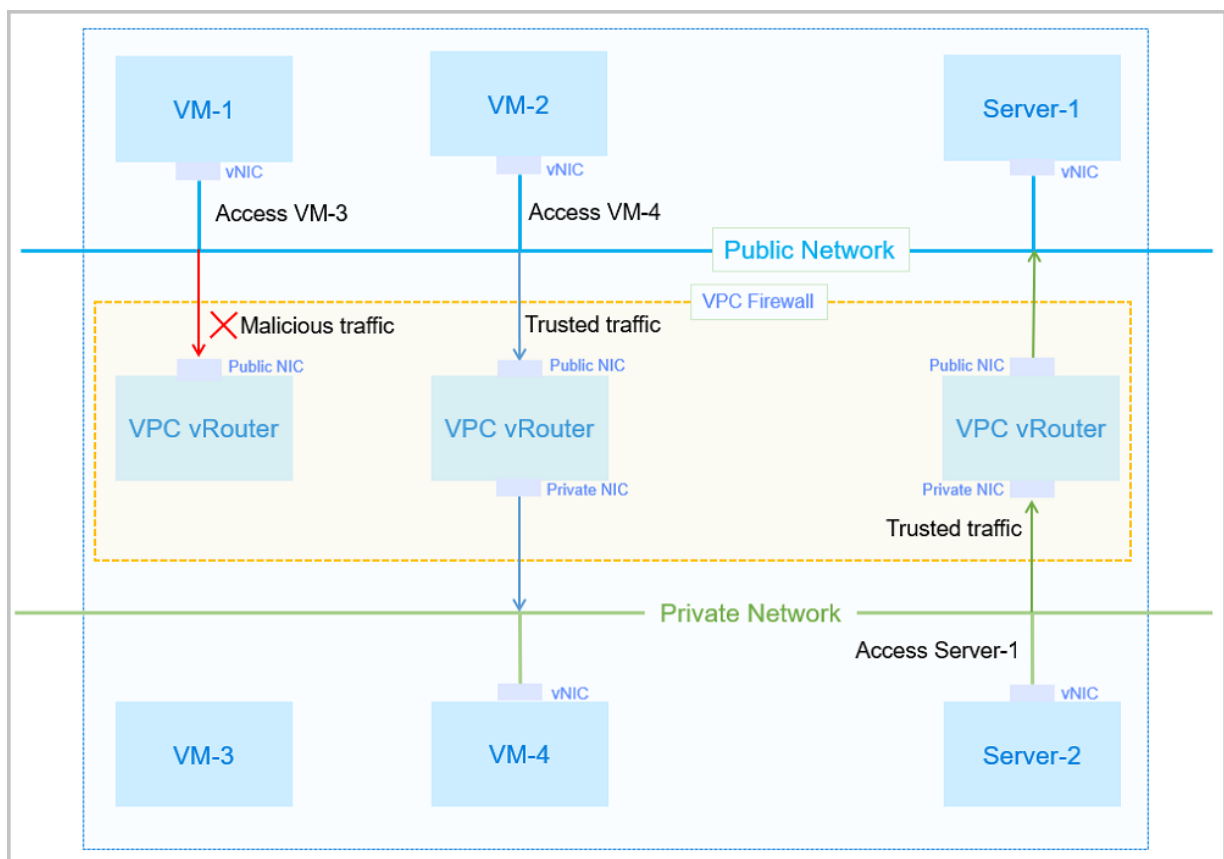
2.2.4.1 Security

2.2.4.1.1 VPC Firewall

A VPC firewall manages the south-north traffics of VPC networks, and allows you to manage the access control policies by configuring rule sets and rules.

As shown in [VPC Firewall](#).

Figure 2-17: 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 Server-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.

Difference between a VPC firewall and a security group: A VPC firewall manages the south-north traffic, and can be applied to the entire VPC. On the contrary, a security group mainly manages the east-west traffic, and can be applied to VM NICs. They can complement each other. The detailed differences are as follows.

Comparison	Security Group	VPC Firewall
Application scope	VM NIC	The entire VPC network
Deployment mode	Distributed	Centralized
Deployment location	VM instance	VPC vRouter
Configuration policy	Supports only allowed policies	Enables you to customize the accept policy, drop policy, or reject policy as needed
Priority	Takes effect according to the configuration sequence	Enables you to customize priorities
Matching rules	Source IP address, source port, and source protocol	Source IP address, source port, destination IP address, destination port, protocol, and packet status

Notice

When you use a VPC firewall, make sure that:

- 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.
- **After you create a VPC firewall, public networks can only access VM instances through EIPs.** 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, make sure that:

- 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, make sure that:

- 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.

2.2.4.1.2 Security Group

A security group provides L3 network firewall controls 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.

- Flat networks, vRouter networks, and VPC all support the security group service. The security group service is provided by the security group network service module. By using iptables, you can perform firewall security controls over VM instances. This method 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 traffic 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.

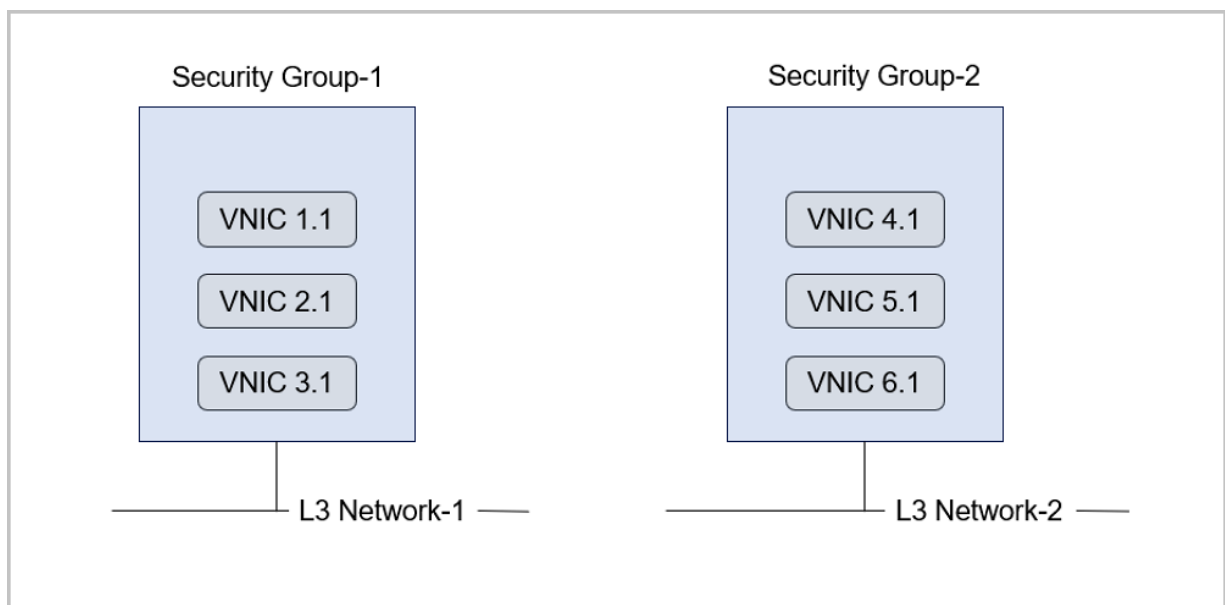
- UDP: Supports ports 1-65535.
- ICMP: Supports all ICMP protocols. By default, both the start port and end port are all -1.
- A security group rule can limit data sources that comes either from inside or outside of VM instances. Currently, sources can be set as source CIDR or source security group.
 - 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 2-18: Security Group](#).

Figure 2-18: Security Group



2.2.4.2 VIP

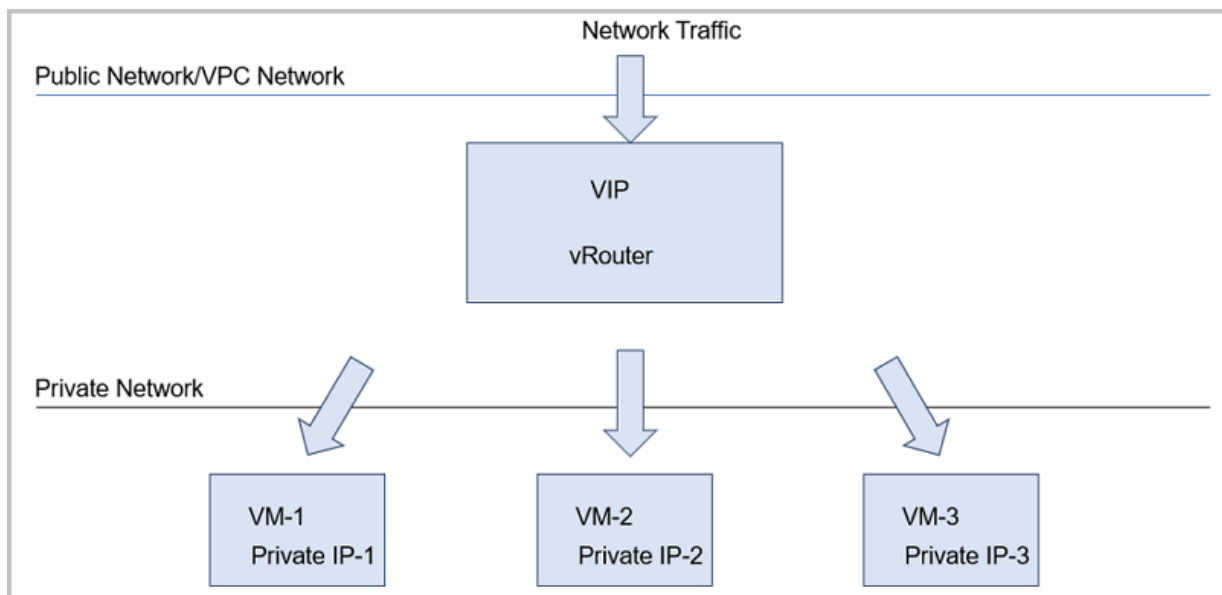
In a bridged networking environment, virtual IP addresses (VIPs) are used to provide network services such as elastic IP address (EIP), port forwarding, load balancing, and IPsec tunnel. Packets are sent to VIPs and then routed to the VM networks.

- 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 2-19: Provide Load Balancing by Using VIP



Definitions related to VIP:

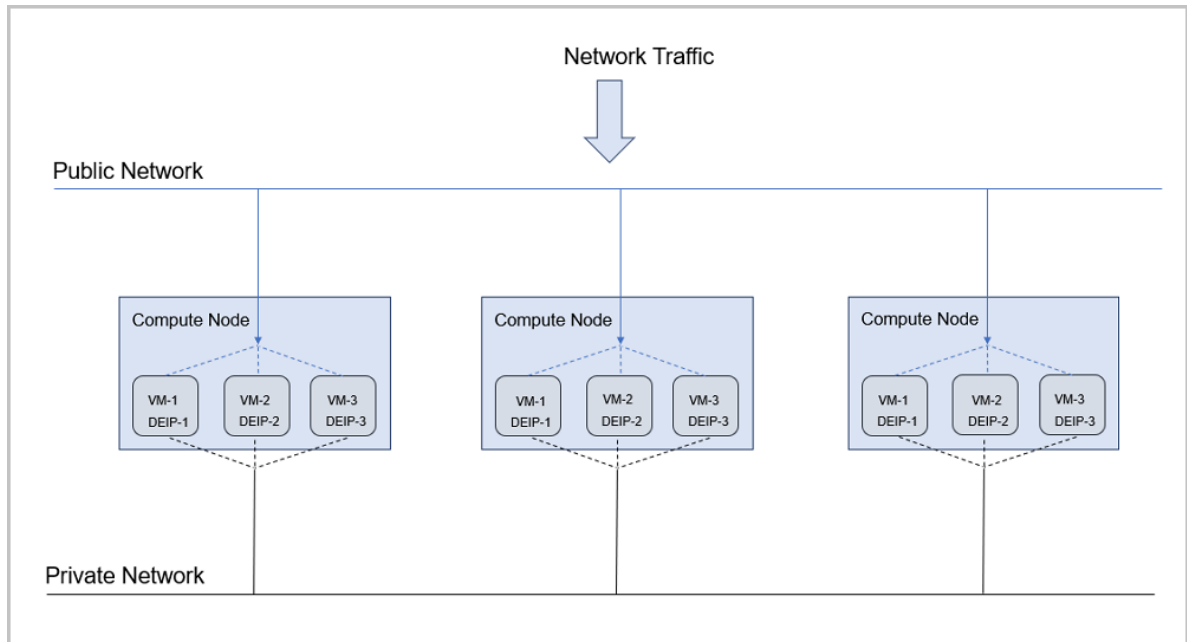
- Public VIP: The VIP created from a public network. A public VIP can be created manually, or created automatically by the system after a vRouter is created.
 - A public VIP can provide network services, such as EIP and load balancing, for flat networks . A public VIP can also provide network services, such as EIP, port forwarding, load balancing, and IPsec tunnel, for vRouter networks and VPC networks.
 - A public VIP can be simultaneously applied to services such as port forwarding, load balancing, and IPsec tunnel, and supports multiple instances of the same service type. Note that different types of services cannot use the same port No.
 - A public VIP supports QoS, monitoring data, performance TOP 5, performance analysis, alarm, and other features.
- VPC VIP: The VIP created from a VPC network. A VPC VIP can only be created manually.
 - A private VPC VIP can provide load balancing services for VPC networks.

- Currently, private VPC VIPs do not support QoS, monitoring data, performance TOP 5, performance analysis, and alarm features.
- Flat VIP: The VIP created from a flat network. A flat VIP can be created manually, or created automatically by the system after a vRouter is created.
 - A flat VIP provides network services, such as EIP and load balancing, for flat networks.
 - A flat VIP supports QoS, monitoring data, performance TOP 5, performance analysis, alarm , and other features.
- Custom VIP: The VIP manually created by a user. Public VIPs, VPC VIPs, and flat VIPs can be created manually.
 - One custom public VIP is only applied to one EIP service instance.
 - Custom VIPs cannot be used across normal vRouters or VPC vRouters.
 - When you use the EIP, port forwarding, load balancing, or IPsec tunnel services, you can select **Create new IP** to create a new VIP, or you can select **Use existing IP** to provide corresponding services.
- System VIP: The VIP automatically created by the system by using the L3 network attached by a vRouter (a normal vRouter or VPC vRouter) after the vRouter is successfully created. Both public VIPs and flat VIPs can be created automatically by the system after a vRouter is created.
 - A system VIP has a one-to-one relationship with a vRouter or VPC vRouter. Each time a vRouter attaches a public network, the system will automatically create a system VIP. In addition, the system VIP is the same as the default IP address of the vRouter or VPC vRouter.
 - By default, the system VIPs created from public networks are used to provide the source network address translation service.
 - When you use the EIP, port forwarding, load balancing, or IPsec tunnel service, you can select **Use existing IP** to provide corresponding services.

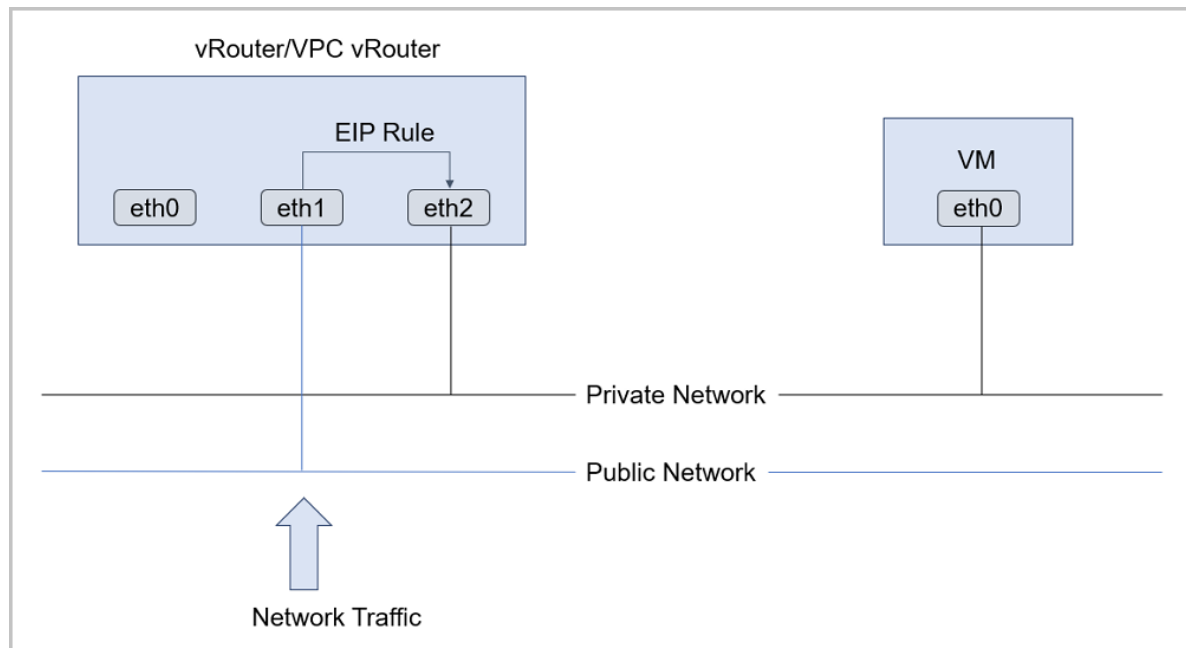
2.2.4.3 EIP

An elastic IP address (EIP) is a method to access a private network through a public network. 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 an EIP usage scenario in flat networks, as shown in [EIP Usage Scenario in Flat Network](#).

Figure 2-20: 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. Note that these IP addresses cannot connect to the Internet by default.
- Distributed EIP is deployed on each compute node. The EIP 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 2-21: EIP Usage Scenario in vRouter/VPC Network

Definitions related to EIP:

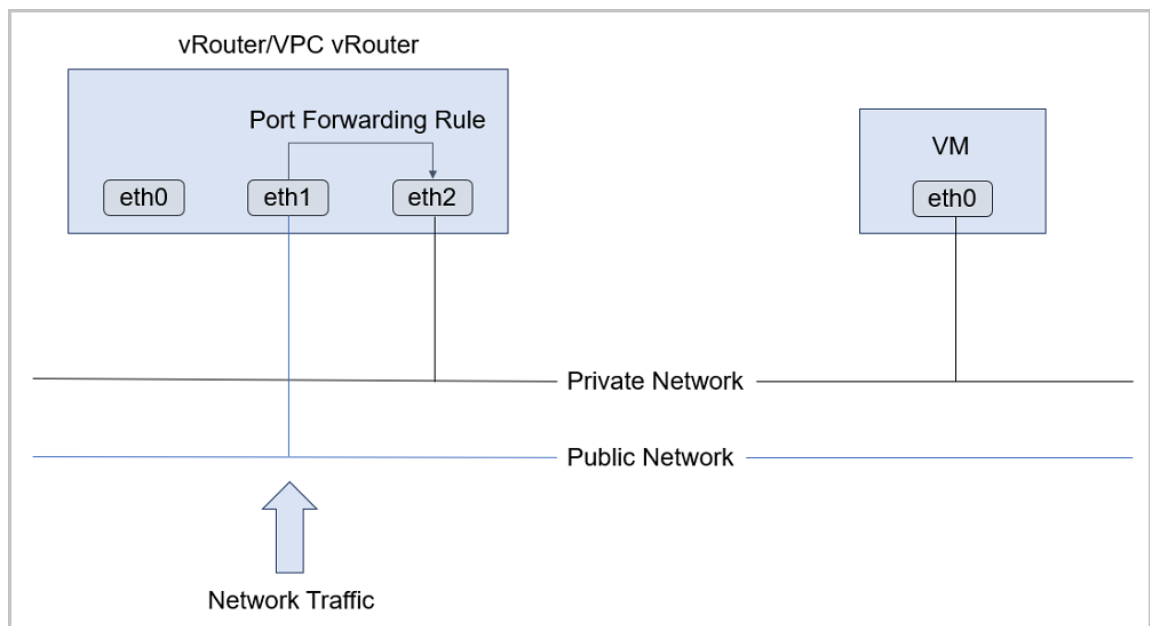
- Public EIP: The EIP service provided by a public VIP created from a public network.
 - An internal private network is an isolated network space, which cannot be directly accessed by the external network. A public EIP can directly associate the access to a public network with the VM IP of an internal private network.
 - A public EIP can be attached to or detached from a VM instance dynamically.
 - A public EIP can be attached to VM instances created from private networks, such as flat networks, vRouter networks, and VPC networks.
 - The EIP realized by distributed EIP can access flat networks through public networks.
 - vRouters or VPC vRouters can be used to access vRouter networks or VPC networks through public networks.
- Flat EIP: The EIP service provided by a flat VIP created from a flat network.
 - L3 isolations exist between flat networks of different IP ranges. Therefore, these flat networks cannot be accessed directly. A flat EIP can be used to associate the access to one flat network with the VM IP created from another flat network.
 - A flat EIP can be attached to or detached from a VM instance dynamically.
 - A flat EIP can be attached to VM instances created from other flat networks.

2.2.4.4 Port Forwarding

Port forwarding 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.

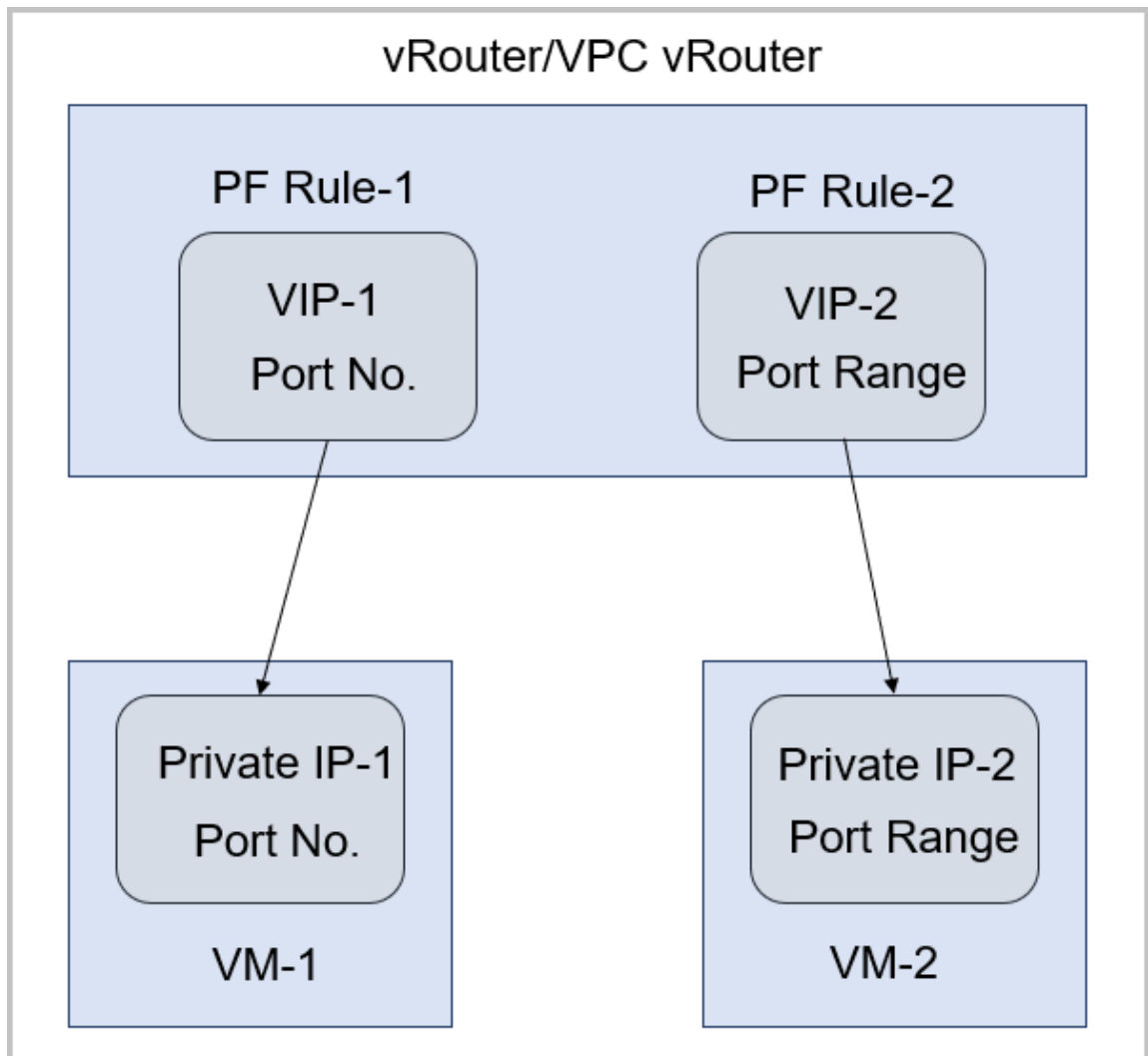
- In private networks that enable the source network address translation (SNAT) service, VM instances can access the external network, but cannot be accessed by the external network. A port forwarding rule can be used to allow the external network to access some specified ports of VM instances behind 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 2-22: 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 2-23: VIP - Port Forwarding



2.2.4.5 Load Balancing

Load balancing distributes inbound traffics from a VIP to a group of backend VM instances, and then automatically detects and isolates unavailable VM instances. This improves 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.

Definitions related to load balancing:

- Frontend network: In load balancing network services, a frontend network is used to provide VIP networks. Public networks, flat networks, and VPC networks can be used as frontend networks.
- Backend network: In load balancing network services, a backend network is used to create a private network for backend VM instances. Flat networks, vRouter networks, and VPC networks can be used as backend networks.
- Internet load balancing: A public network is used as the frontend network to provide Internet-facing load balancing services through routers (VPC vRouters or vRouters).
 - A VPC network can be used as a backend network to provide Internet load balancing services based on a VPC network. In this scenario, multiple backend networks can be used . However, these backend networks must be attached to the same VPC vRouter.
 - A vRouter network can be used as a backend network to provide Internet-facing load balancing services based on a vRouter network. In this scenario, make sure that the frontend network and the L3 network attached to the vRouter are the same.
 - A flat network can be used as a backend network to provide Internet-facing load balancing services based on a flat network. In this scenario, the frontend network and the L3 network attached to the vRouter must be the same.
- Intranet load balancing (VPC private network): A VPC network is used as the frontend network to provide intranet load balancing services through VPC vRouters.
 - A VPC network that shares the same VPC vRouter with a frontend network can be used as a backend network to provide intranet load balancing services based on VPC networks.
 - In this scenario, multiple backend networks can be used. However, these backend networks must be attached to the same VPC vRouter.
- Intranet load balancing (flat network): A flat network is used as the frontend network to provide intranet load balancing services through vRouters.
 - A frontend network can be also used as a backend network to provide intranet load balancing services based on flat networks. In this scenario, the L3 network specified in the

vRouter offering that is attached to the frontend network can be either a public network or a flat network.

- Other flat networks can be also used as a backend network to provide intranet load balancing services based on flat networks. In this scenario, the frontend network and the L3 network attached to the vRouter must be the same.



Note:

To use intranet load balancing (flat network) services, attach a vRouter offering to the flat network in advance.

2.2.4.6 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 features of an IPsec tunnel are as follows:

- **IPsec connection mode**

For security reasons, we only support Main Mode and the Encapsulating Security Payload (ESP) protocol. 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.

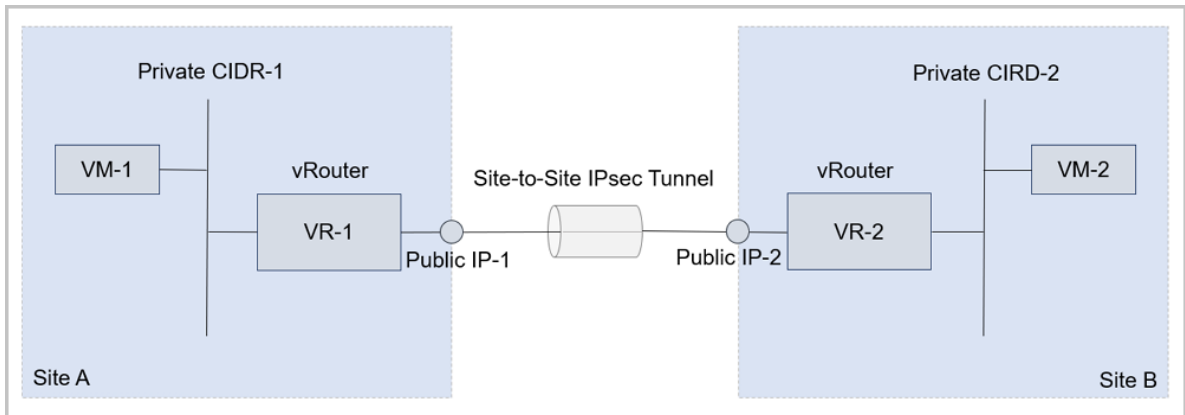
- **IPsec routing model**

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. Note 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 2-24: 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). Note 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.

2.2.4.7 Flow Monitoring

2.2.4.7.1 Flow Network

A flow network is a dedicated network for port mirroring, and can be used to mirror the network traffic of a NIC to the remote end. A flow network cannot be used as other networks and cannot be used to create VM instances.

2.2.4.7.2 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.

2.2.4.7.3 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.

2.2.5 vCenter Manipulation

Introduction

VMware vCenter Server is a centralized management platform of a VMware vCenter.

If you deployed VMware vCenter Server, ZStack would allow you to manipulate the VMware vCenter via public API interfaces provided by VMware. In addition, ZStack can be highly compatible with and manipulate a portion of features of VMware vCenter Server to achieve a unified management of multiple virtualization platforms.

With ZStack, you can manage VMware virtualization environments in an existing data center, and view vSphere server resources and VM resources managed by VMware vCenter Server. In addition, you can use VMware vSphere resources in a virtual data center, and perform common operations on VM instances in your VMware vCenter cluster.

Currently, ZStack supports multiple vCenter versions, including 5.5, 6.0, 6.5, and 6.7.

Basic Resource

ZStack can manage vCenter basic resources, namely vCenter virtual resources, in a unified manner, including adding a vCenter, synchronizing data for a vCenter, and deleting a vCenter.

After you add a vCenter for the first time, ZStack will automatically synchronize the clusters, hosts, VM instances, templates, storages, networks, and other resources in the vCenter. To use a managed vCenter, click **Sync Data** to synchronize vCenter resources to your current cloud. Then, you can view the associated resources in the UI.

- You can add and manage multiple vCenters.
- You can filter resources before you import vCenter resources to ZStack.

— dvSwitch scenario:

Only resources of the hosts added to a dvSwitch can be imported to ZStack. If you do not add a host to a dvSwitch, the associated resources cannot be imported to ZStack.

— vSwitch scenario:

Only resources of the hosts in the same cluster, added to at least one same vSwitch, and have at least one same port group attribute (including the same network labels and the same VLAN ID) can be imported to ZStack.



Note:

ZStack can only take over VM networks rather than VMkernels or management networks.

VM Instance

After you add a vCenter, the vCenter VM instances will be automatically synchronized to ZStack. In addition, you can create vCenter VM instances on your cloud.

Network

Before you create new VM instances in the vCenter managed by ZStack, you need to create a vRouter network or a flat network in the vCenter in advance.

vCenter network services currently support the vRouter network architecture model.

A vCenter vRouter network provides network services such as DNS, SNAT, Elastic IP (EIP), port forwarding, load balancing, IPsec tunnel, and Netflow.

- DNS:
 - A vCenter vRouter can act as a DNS server to provide DNS services.
 - By default, the DNS address that you see in a vCenter VM instance is the IP address of the corresponding vCenter vRouter. The DNS address set by a user is forwarded and configured by the vCenter vRouter.
- SNAT:
 - A vCenter vRouter provides the source network address translation (SNAT) service to vCenter VM instances.
 - vCenter VM instances can directly access the Internet by using SNAT.
- EIP: Allows a vCenter vRouter to access the private network of a vCenter VM instance through a public network.
- Port forwarding: Forwards the port traffics of a specified public IP address to the port of a corresponding vCenter VM IP address.
- Load balancing: Distributes inbound traffics from a public IP address to a group of backend vCenter VM instances, and then automatically detects and isolates unavailable vCenter VM instances.
- IPsec tunnel: Uses the IPsec tunnel protocol to provide site-to-site VPN connections.

Network Service

A vCenter vRouter network provides network services such as DNS, SNAT, Elastic IP (EIP), port forwarding, load balancing, IPsec tunnel, and Netflow.

- DNS:

- A vCenter vRouter can act as a DNS server to provide DNS services.
- By default, the DNS address that you see in a vCenter VM instance is the IP address of the corresponding vCenter vRouter. The DNS address set by a user is forwarded and configured by the vCenter vRouter.
- SNAT:
 - A vCenter vRouter provides the source network address translation (SNAT) service to vCenter VM instances.
 - vCenter VM instances can directly access the Internet by using SNAT.
- EIP: Allows a vCenter vRouter to access the private network of a vCenter VM instance through a public network.
- Port forwarding: Forwards the port traffics of a specified public IP address to the port of a corresponding vCenter VM IP address.
- Load balancing: Distributes inbound traffics from a public IP address to a group of backend vCenter VM instances, and then automatically detects and isolates unavailable vCenter VM instances.
- IPsec tunnel: Uses the IPsec tunnel protocol to provide site-to-site VPN connections.

ZStack supports multi-tenant management in a managed vCenter. Normal accounts and project members can use vCenter network services, including EIP, port forwarding, and load balancing.

Volume

In vCenter, a volume provides storages for vCenter 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.

In vCenter, data volumes are mainly involved in volume management.

Image

In ZStack, you can add a local image of the VMDK format to a vCenter. Then, you can synchronize the vCenter image between the local client and the remote client by synchronizing data. Both system images and volume images can be added.

Event Message

The Event Message feature allows you to check vCenter alarm messages, such as the message description, type, the vCenter from which the event message is sent, triggered user, target, and date.

- The UI can display up to 300 event messages. You can set a time range to check alarm messages within the time range via the time adjustment button at the upper left.
- You can choose to display alarm message count for each page via the display count button at the upper right. Optional value: 10 | 20 | 50 | 100. In addition, you can turn pages by clicking the left arrow button and the right arrow button.

2.2.6 Platform O&M

2.2.6.1 Performance TOP5

Performance TOP5 is a visual performance monitoring page designed for O&M personnel. 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, the O&M personnel can directly manage the real-time healthy 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 IOPS, 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:

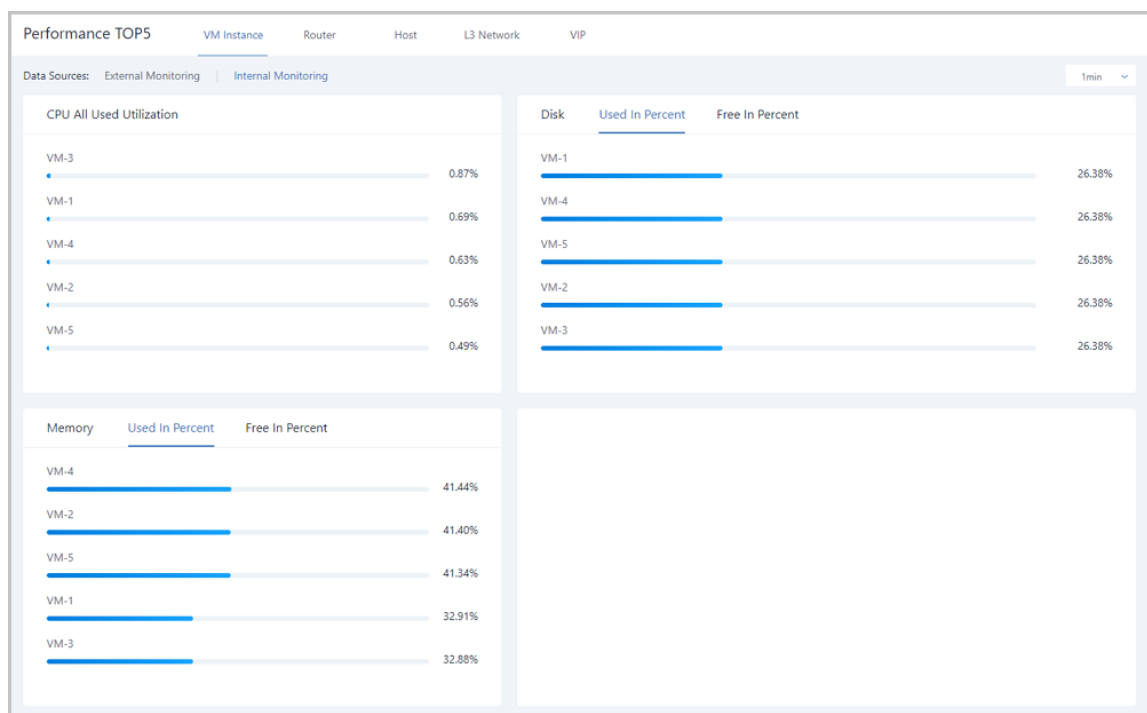
The VM instance page includes external monitoring and internal monitoring.

- 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 IOPS, 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.

- 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 [Internal Monitoring TOP5](#).

Figure 2-25: 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 utilization, memory utilization, memory free (idle) in percent, disk read/write IOPS, 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.
- 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](#).

2.2.6.2 Performance Analysis

Performance Analysis is a performance statistics page designed for O&M personnel. This page takes resources as a unit to directly and simply display monitoring metrics of various resources, such as VM instances, routers, hosts, L3 networks, VIPs, and backup storages at different time

ranges. With Performance Analysis, the O&M personnel can directly manipulate the healthy states of resources on the cloud.

Specifically,

- **VM instances, router, and physical hosts:** Display names, average CPU utilizations, memory utilizations, disk read and write speeds, and NIC in or out speeds.
- **L3 network:** Display names, used IP counts, used IP percentages, available IP counts, and available IP percentages.
- **VIP:** Display names, downstream network traffics (network in), downstream network in packet rates (network packets in), upstream network traffics (network out), and upstream network in packet rates (network packets out).
- **Backup storage:** Display names and available capacity percentages of backup storages.

2.2.6.3 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.

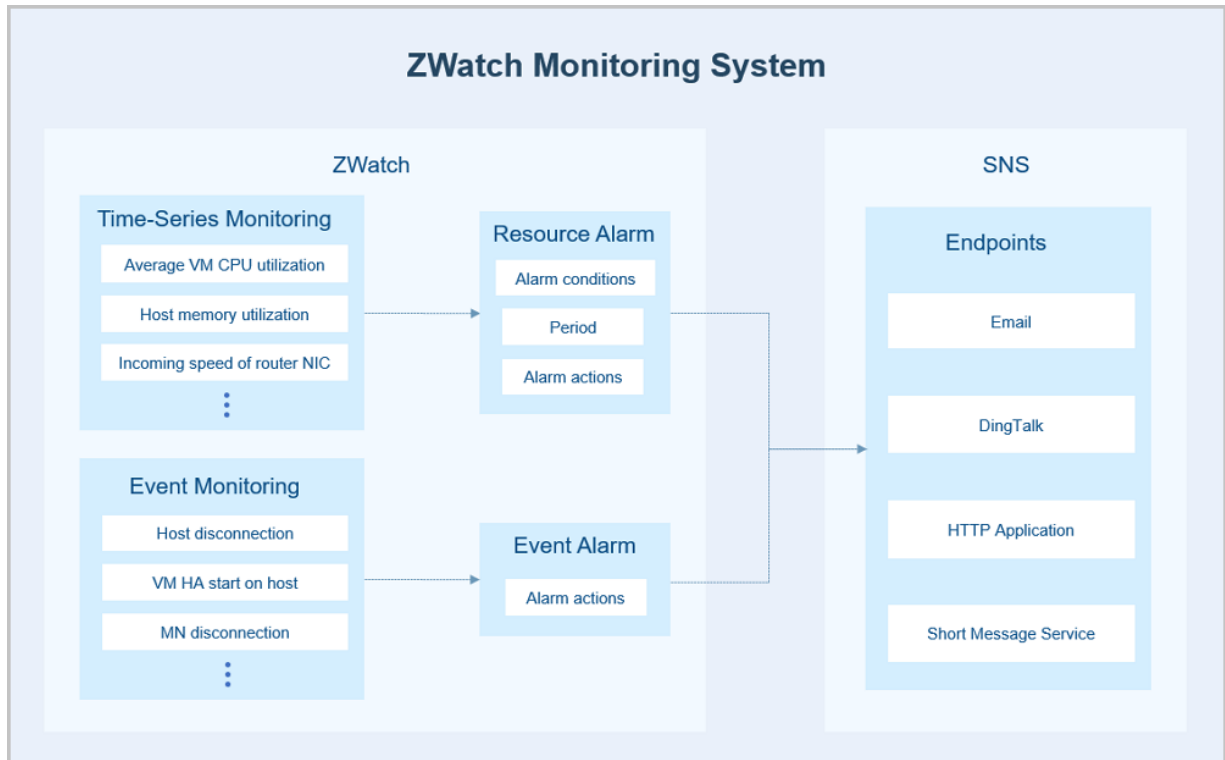
Notice

- 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.

2.2.6.4 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 two types of alarm: resource alarm and event alarm, and supports four types of endpoints: email, DingTalk, HTTP application, and short message. To use some specific resource alarms, install an agent.

The ZWatch workflow is shown in [ZWatch Monitoring System](#).

Figure 2-26: ZWatch Monitoring System

Basic Workflow

- **ZWatch**

ZWatch provides the following features:

- Time series monitoring: Currently, monitors the following two types of time series data:
 - Resource load data: Provides a visual display of VM CPU utilizations and host memory utilizations.
 - Resource capacity data: Provides a visual display of used IP counts and the total number of the running VM instances.
- Event collection: Collects predefined events triggered on the cloud, such as the host disconnection and enabling the VM HA feature.
- Alarming: Triggers alarms for time series data or events.
- Audit: Records all operations and lets you to conduct searches for these operations.
- Customization: Customizes alarm settings and alarm SNS text templates.
 - Alarm: Currently supports the following two types of alarm:

- Resource alarm: Triggers alarms for time series data. For example, set an alarm for VM CPU utilizations. Specifically, when the CPU utilization of a VM instance exceeds 80% for consecutive 5 minutes, an alarm notification will be sent to your email.
- Event alarm: Triggers alarms for events, known as event subscriptions. For example, subscribe an event of the host disconnection. And then an alarm notification will be sent to your DingTalk when a host is disconnected.
- An SNS text template is a text template that is used when an alarm or event sends messages to themes of the SNS system.
 - The system contains a default template of an alarm message and a recovered message. If you do not create a template, the system will use this default template.
 - You can create multiple message templates, but can only default a 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 three types of endpoint platform: email, DingTalk, and short message. If you use an SNS text template, formatted alarm messages will be sent to you via email, DingTalk, or short messages.
- **SNS**

Notification services will push alarm messages to an endpoint, including an email, DingTalk, HTTP application, and short message service.

Endpoint setting:

- By default, the cloud provides a system-native endpoint. If an alarm binds the 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, or short message service endpoint as needed.

Feature Benefits

ZWatch provides the following feature benefits:

- Provides a diversity of alarm metric items to monitor core resources and events on the cloud in a comprehensive, fine-grained, and flexible manner.
- Supports five types of subscription theme: email, DingTalk, HTTP application, and short message service. Select an appropriate alarm theme as needed.

- One alarm can monitor multiple resources simultaneously.
- Endpoints such as email, DingTalk, and short message service let you to customize the alarm SNS text template. To quickly locate key information from alarm messages, set the alarm SNS text template as needed.

Typical Usage Scenario

ZWatch monitors core resources and events on the cloud, and sets the alarm receiving mechanism. When core resources are abnormal, ZWatch will initiate real-time responses according to alarm levels, where O&M personnel can quickly locate and then solve problems.

More Information

- Monitoring data retention cycle defaults to 6 months. You can customize your monitoring data retention cycle as needed. Method:

In the UI, choose **Settings > Global Settings > Advanced**, locate **Retention time of Monitoring data**, and click the Edit icon. Default value: 6. Unit: month. Value range: 1-12, integer.

- Monitoring data retention size defaults to 50 GB. You can customize your monitoring data retention size as needed. Method:

In the UI, choose **Settings > Global Settings > Advanced**, locate **Retention size of Monitoring data**, and click the Edit icon. Default value: 50 GB. We recommend that you set your retention size as needed.

2.2.6.5 Notification Service

You can use different endpoint subscription themes. Currently, the supported endpoint types include system, email, DingTalk, HTTP application, and short message service.

- By default, the cloud provides a system-native endpoint. If an alarm binds the 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, or short message service endpoint as needed.

Email Endpoint

- Messages that send to themes will be sent to a specified email address via an email server.
- You can either create an SNS text template in advance or use the system default 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 themes 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 the system default 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 themes will be sent to a specified HTTP address via HTTP POST.
- If the specified HTTP application sets a user name and password, enter accurately the user name and the password.

Short Message Service Endpoint

- Messages that send to themes 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.

2.2.6.6 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.

2.2.6.7 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.

2.2.6.8 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.

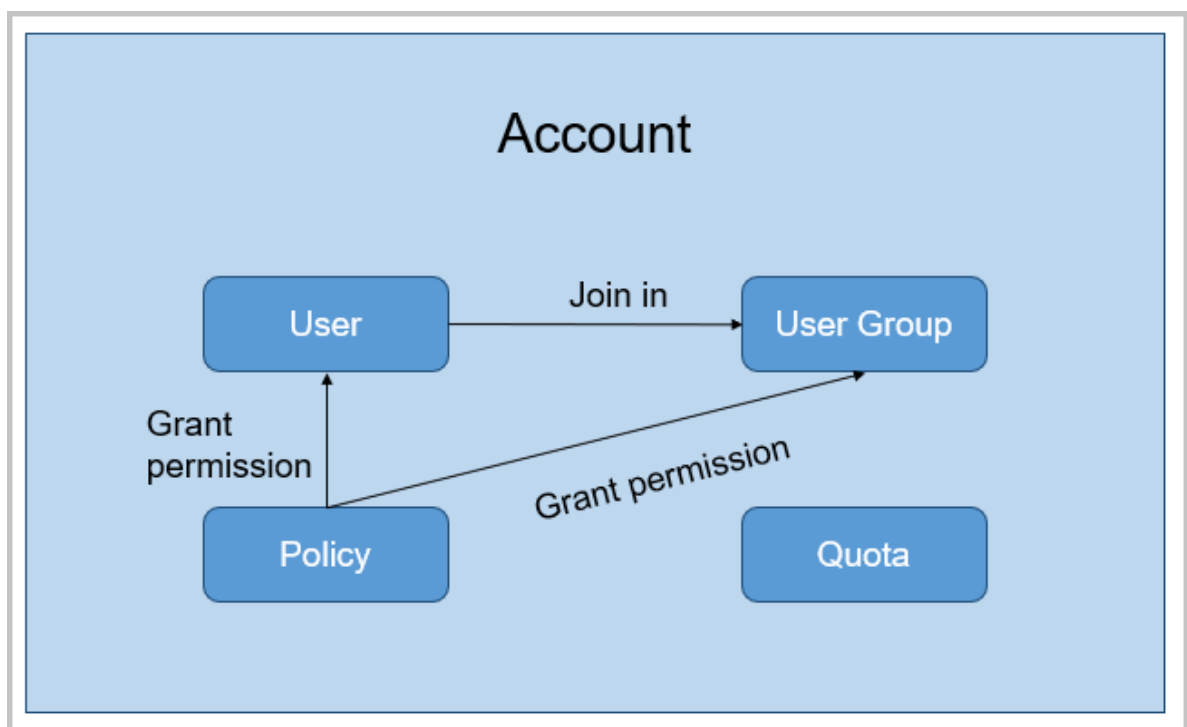
2.2.7 Platform Management

2.2.7.1 User Management

The User Management feature provides you with access control to system resources. With User Management, you can perform fine-grained managements on resource ownership and permission control.

- User Management provides managements of accounts, user groups, and users, and involves concepts such as policy and quota.
- The overall structure of User Management is shown in [Figure 2-27: User Management](#).

Figure 2-27: User Management



Concepts

- **Account**

Account is the root identity that owns all your resources. An account can perform multiple operations, such as create, delete, share, and recall, on resources of its ownership. Account consists of admin account and normal account.

- **User**

User is created by account to achieve fine-grained permission controls. Users created by an admin account are admin users who inherit all permissions of the admin account.

- **User Group**

User group is created by normal account to perform batch permission controls on users in the same group.

- **Resource Quota**

Resource quota, also referred to as quota, is used by admin account to limit the resource amount of a normal account.

- Resource quota involves the following parameters: VM count, CPU count, memory capacity , maximum number of data volumes, and maximum capacity of all volumes.
- The admin account can modify the preceding parameters to adjust the resource quota of each normal account. If a resource is deleted but not expunged, the resource still consumes the primary storage and volume resources.

2.2.7.2 Billing Management

2.2.7.2.1 Bills

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.

2.2.7.2.2 Pricing List

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.

2.2.7.3 Job Scheduling

2.2.7.3.1 Scheduler

A scheduler is a container that carries scheduled jobs. This feature can be better applied to time-consuming operations, such as creating a snapshot for a VM instance. A scheduler and a scheduled job can be completely decoupled. That is, you can create schedulers with different rules and create different scheduled jobs as needed, and flexibly attach or detach the scheduled jobs to or from the schedulers. Operations of the schedulers will be recorded completely to the audit.

Scheduler execution strategy includes repeat and repeat count.

- **Repeat:** Execute the scheduled job repeatedly without limits according to the time cycle.
- **Set Repeat Count:** Execute the scheduled job with limits according to the time cycle. Make sure that you set the repeat count for the scheduled job.



Note:

For the scheduler that is executed with limits within the time cycle, after the scheduled job is performed, the scheduler state will be displayed as **Completed**.

2.2.7.3.2 Scheduled Job

A scheduled job is a job metric that is attached to a scheduler. A scheduler and a scheduled job can be completely decoupled. That is, you can create schedulers with different rules and create different scheduled jobs as needed, and flexibly attach or detach the scheduled jobs to or from the schedulers. Besides, a scheduled job can be selectively disabled, enabled, attached, and detached. Operations of the scheduled jobs will be recorded completely to the audit.

The **Scheduled Job** page displays names of scheduled jobs, task types, resource names, start time, task strategies, states, schedulers, and creation time.

2.2.7.4 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, and hosts.
- Tenant tags are created and owned by tenants (normal 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, and hosts.

Notice

- Admin tags are created and owned by administrators (admins or platform admins), while tenant tags are created and owned by tenants (normal 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.

2.2.7.5 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.

2.2.7.6 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.

2.2.7.7 Log Server

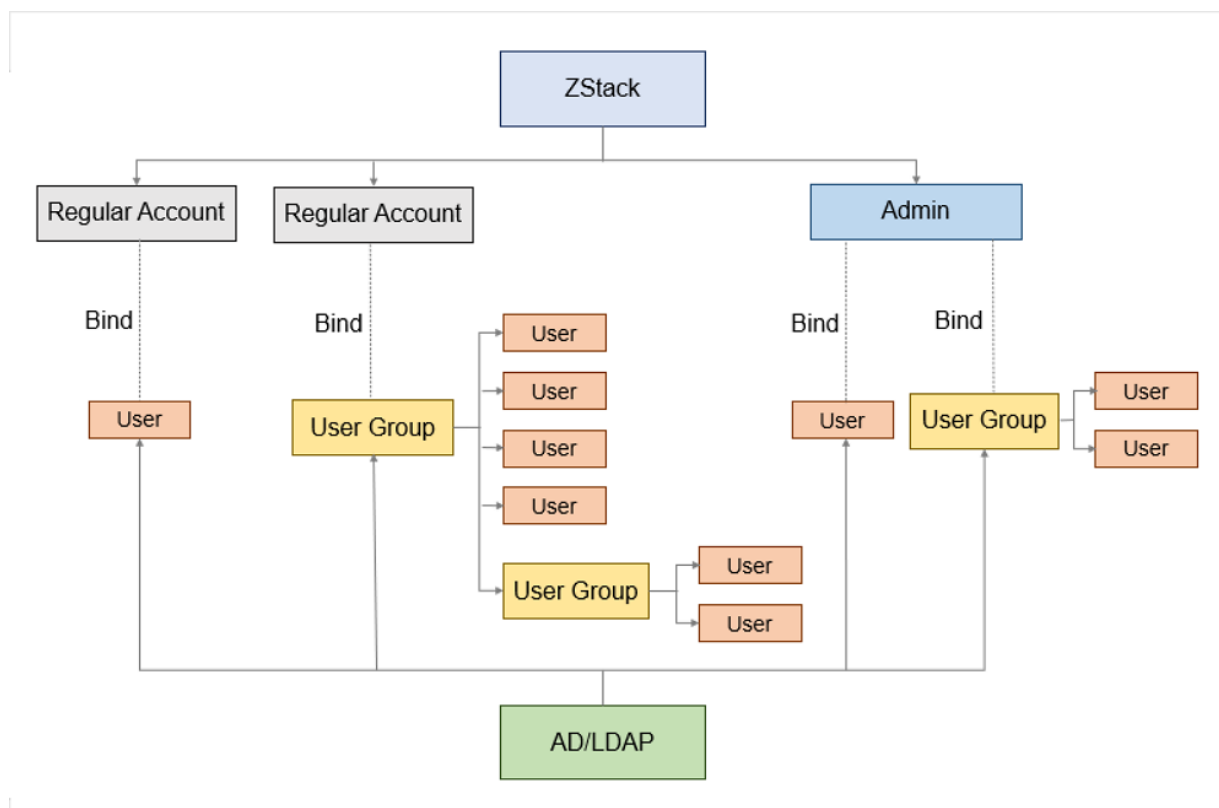
ZStack allows you to add a log server to the cloud. With the log server, you can collect management node logs and quickly locate problems, thereby improving the cloud O&M efficiency.

2.2.7.8 AD/LDAP

LDAP (Lightweight Directory Access Protocol) provides a standard directory service. Both Microsoft Windows AD software (AD) and OpenLDAP software (LDAP) provided in a variety of popular Linux versions are LDAP-based and provide an independent, standard login authentication system for increasingly diverse enterprise office applications.

The binding relationship between ZStack accounts (regular accounts or admins) and AD/LDAP members (regulars account or admins) is shown in [Binding Relationship between ZStack Account and AD/LDAP Member](#).

Figure 2-28: Binding Relationship between ZStack Account and AD/LDAP Account



2.2.7.9 Console Proxy

- 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**.

2.2.7.10 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 troubleshoot this issue as soon as possible.

2.2.7.11 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.

2.2.7.12 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.

2.2.7.13 AccessKey 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.

2.2.8 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

2.2.8.1 Enterprise Management

The Enterprise Management feature mainly provides enterprise users with organization structure managements and project-based resource access control, ticket management, and independent zone management. The Enterprise Management feature 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 related definitions are as follows:

- **Admin**

An admin is a super administrator who owns all permissions. Usually, IT system administrators obtain the permissions.

- **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.

- **Local User**

A local user is the user that is created in the cloud. You can add a local user to an organization or a project, attach a role to the user, and perform other operations on the user.

- **3rd Party User**

A 3rd party user is the user that is synchronized to the cloud through 3rd party authentication. You can add a 3rd party user to an organization or a project, attach a role to the user, change the user to a local user, and perform other operations on the user.

- **Platform User**

A platform user is the user that is not added to a project yet, including the platform admin and the normal platform member.

- **Platform Admin**

A platform admin is the user that has the platform admin role attached. A platform admin is zone specific, and manages the data center of the allocated zone.

- **Head of Department**

A head of a department is the 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 project member is the user who has joined a project, including a project admin, project operator, and normal project member.

- **Project Admin**

A project admin is the 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 project operator is the user that has the project operator role attached. A project operator assists project admins to manage projects. You can specify one or more project members in the same project to act as project operators.

- **Member Group**

A member group (virtual ID group) is a group of project members. You can organize project members into groups for better management, and perform permission control by member group.

- **Organization**

An organization is 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 departments.

- **Project**

A project is the task that related members will be specified to accomplish specified targets with a specified time, resource, and budget. The Enterprise Management feature organizes resources based on projects and allows you to create an independent resource pool for a specific project.

- **Role**

A role is a collection of permissions. You can grant permission 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 system role is 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. System roles cannot be configured manually.

- **Custom Role**

A custom role is the 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 quota is a measurement standard that controls the total 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, you need to 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 the **The license will be expired** notification 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.

Four 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 for resource planning. 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.

- **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 for 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.

- **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 independent managements of various machine rooms. In addition, admins can inspect and manage all zones.

- **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.

2.2.8.1.1 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**

An organization is 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 departments.

- **User**

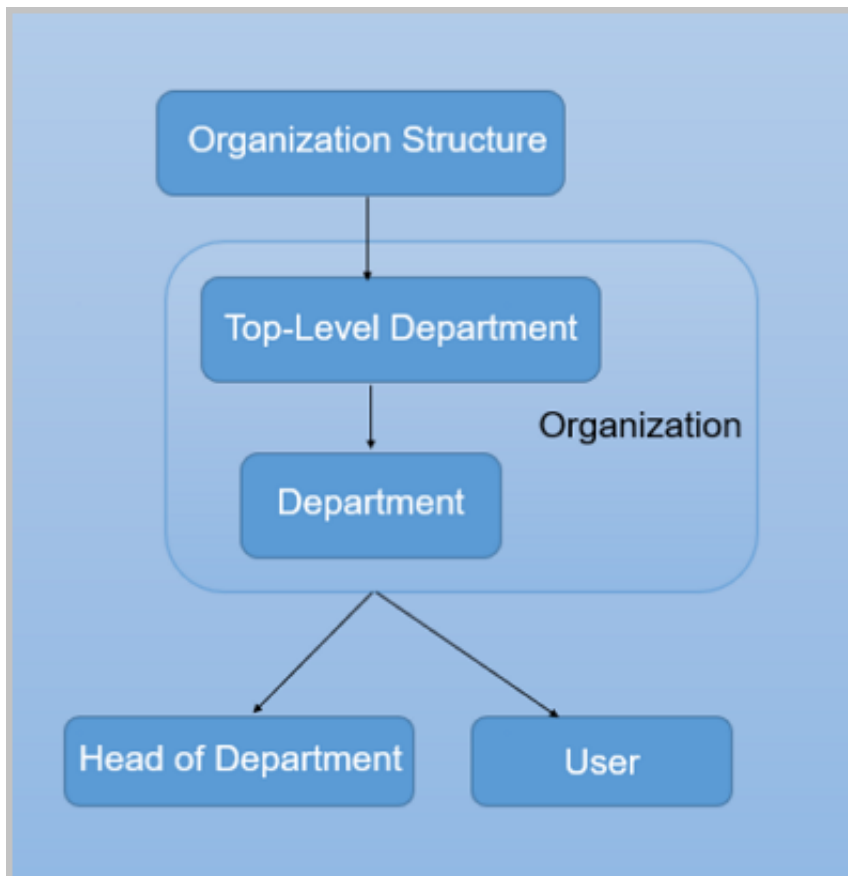
A user (virtual ID) is simply a natural person who is the most basic unit in Enterprise Management. A user has multiple attributes, such as a platform admin, project admin, and head of a department.

- **Head of Department**

A head of a department is the user that is responsible for managing departments in an organizational structure. A head of a department has the permission to check department bills.

Associated concepts of the organization is shown in [Associated Concepts of Organization](#).

Figure 2-29: Associated Concepts of Organization



2.2.8.1.2 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:

- Source classification

— Local User

A local user is the user that is created in the cloud. You can add a local user to an organization or a project, attach a role to the user, and perform other operations on the user.

— 3rd Party User

A 3rd party user is the user that is synchronized to the cloud through 3rd party authentication. You can add a 3rd party user to an organization or a project, attach a role to the user, change the user to a local user, and perform other operations on the user.



Note:

Users in Enterprise Management can log in to the cloud via the project login, while local users can log in to the cloud via the user login. Besides, third-party users can log in to the cloud via the AD/LDAP login.

- Project classification

— Platform User

A platform user is the user that is not added to a project yet, including the platform admin and the normal platform member.

— Project Member

A project member is the user who has joined a project, including a project admin, project operator, and normal project member.

2.2.8.1.3 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 system role is 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. System roles cannot be configured manually.

- **Custom Role**

A custom role is the 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.

2.2.8.1.4 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 directly log in to ZStack.

2.2.8.1.5 Project Management

Enterprise Management provides the project management feature for enterprise users.

Project management:

The project management is project-oriented for resource planning. 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**

A project is the task that related members will be specified to accomplish specified targets with a specified time, resource, and budget. The Enterprise Management feature organizes resources based on projects and allows you to create an independent resource pool for a specific project.

- **Project Member**

A project member is the user who has joined a project, including a project admin, project operator, and normal project member.

- **Project Admin**

A project admin is the 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 project operator is the user that has the project operator role attached. A project operator assists project admins to manage projects. You can specify one or more project members in the same project to act as project operators.

- **Member Group**

A member group (virtual ID group) is a group of project members. You can organize project members into groups for better management, and perform permission control by member group.

- **Role**

A role is a collection of permissions. You can grant permission 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 quota is a measurement standard that controls the total 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, you need to 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

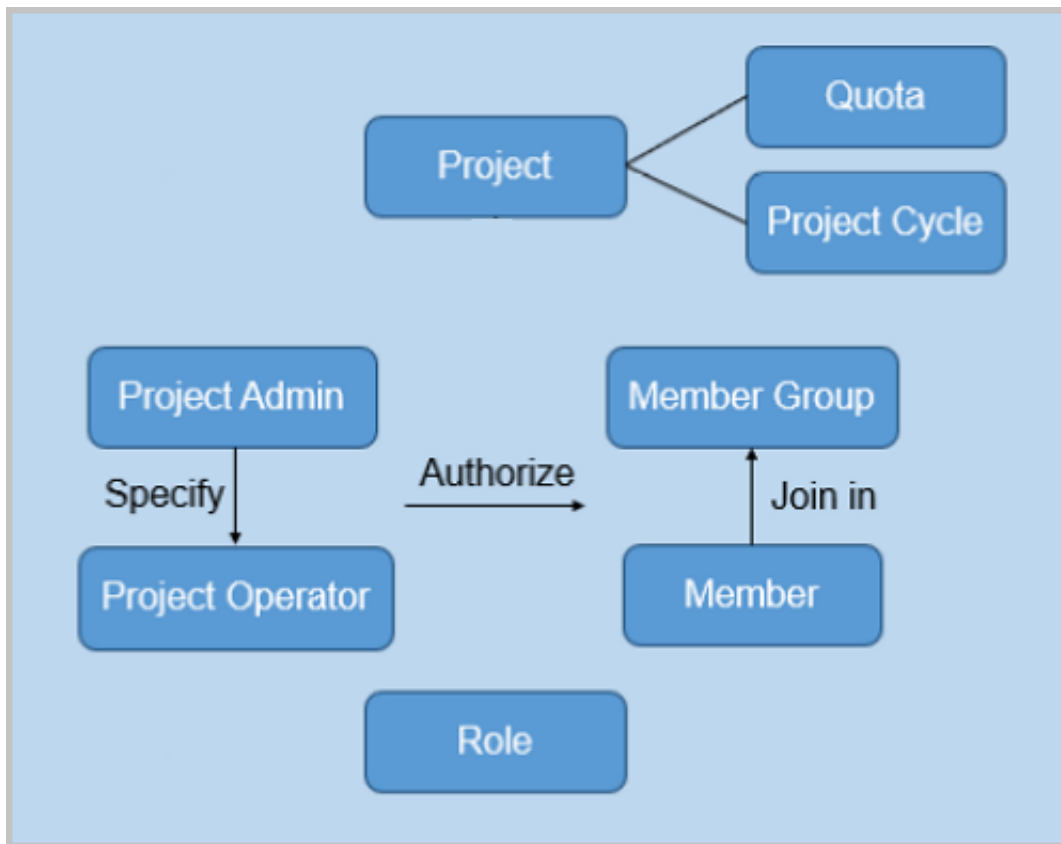
- When the expiration date for a project is less than 14 days, the smart operation assistant will prompt you the **The license will be expired** notification after a project member logs in to the cloud.
 - After the project expired, resources within the project will be collected according to the specified 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.

Associated concepts of the project management is shown in [Associated Concepts of Project Management](#).

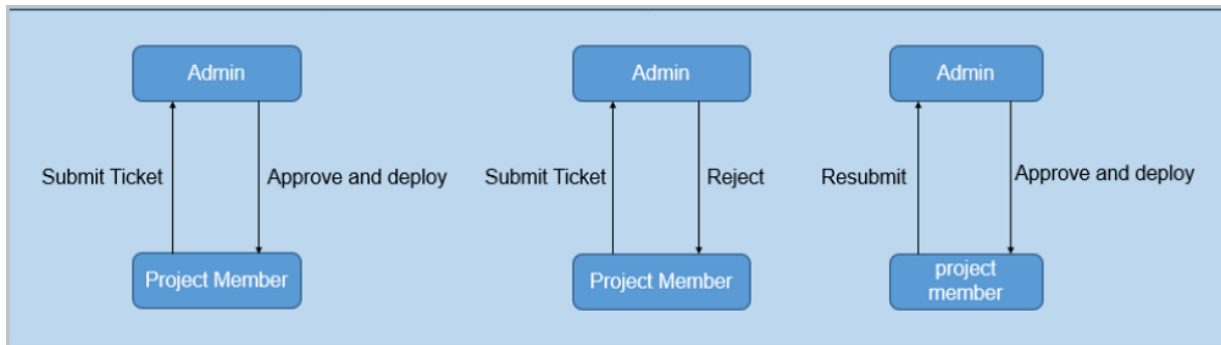
Figure 2-30: Associated Concepts of Project Management



2.2.8.1.6 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 for 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.

The major workflow is shown in [Major Workflow of Ticket Management](#).

Figure 2-31: Major Workflow of Ticket Management

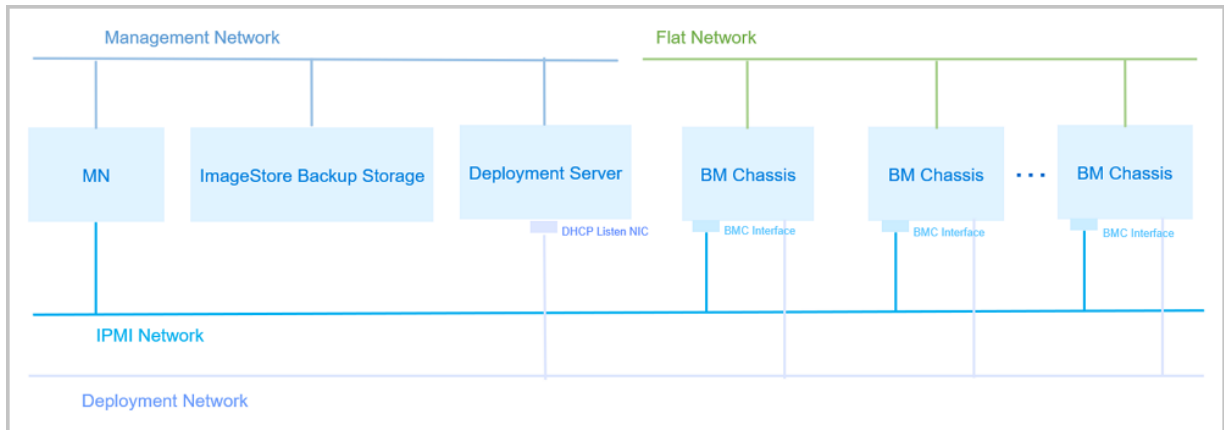
2.2.8.2 BareMetal Management

ZStack provides the BareMetal Management service. Notice that this service provides your applications with dedicated physical servers, ensuring the high performance and stability of your key applications. After your server is ready 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 the 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 Principle

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 2-32: BareMetal Management Network Topology

Key Features and Benefits

The BareMetal Management service provides the following features and benefits:

- This service provides applications with dedicated physical servers to ensure the high performance and stability of your key applications.
- We recommend that you deploy deployment servers independently, 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.
- You can create BM chassis in bulk on the UI by either creating manually BM chassis or importing template files. You can also add IPMI addresses in bulk to deploy efficiently BM clusters, which increases O&M efficiencies.
- You can quickly generate configuration files by using preconfigured templates to achieve unattended batch installation for BM instance operating systems.
- You can customize the installation of your operating system. Currently, the following operating systems are supported: custom operating system of the cloud and the mainstream Linux distribution operating systems (RHEL/CentOS, Debian/Ubuntu, and SUSE/openSUSE).
- This service supports the flat network scenarios. Specifically, BM instances and VM instances on the same L2 network can access 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 updating for servers. Sometime later, business performances will be affected by the performance loss and hyper-threading brought by the visualization. In this regard, if you deploy BM cluster to a certain scale, you can 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 your demand, you can use the BareMetal Management service that provides exclusive, high-performance physical servers for your appliances.

2.2.8.2.1 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 be attached to multiple Bare Metal clusters simultaneously.
- To provide network services for BareMetal instances on a Bare Metal cluster, the Bare Metal cluster must attach L2 networks.
- In the supported flat network scenario, both Bare Metal instances and VM instances on the same L2 network can reach each other without routing via a gateway.

2.2.8.2.2 Deployment Server

A deployment sever, 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 be attached to multiple Bare Metal clusters simultaneously.
- A deployment server must have sufficient storage spaces 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 have 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.

2.2.8.2.3 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 admin 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 have a BMC interface, and configure 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.

2.2.8.2.4 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 template:
 - System template: Defaulted by the cloud, including basic system variables, thereby satisfying a simple, unattended deployment scenario.
 - Custom template: Allow 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.

2.2.8.2.5 Bare Metal Instance

A Bare Metal instance is a VM instance of 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 distribution operating systems (RHEL/CentOS, Debian/Ubuntu, and SUSE/openSUSE). These versions must be the ISO format and non-live CD.
- A business network can be configured for Bare Metal instances. Currently, in the supported flat network scenario, both Bare Metal instances and VM instances on the same L2 network can reach each other without routing via a gateway. Make sure that a Bare Metal cluster where the Bare Metal chassis is running attaches the corresponding L2 network in advance.

2.2.8.3 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. You can 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

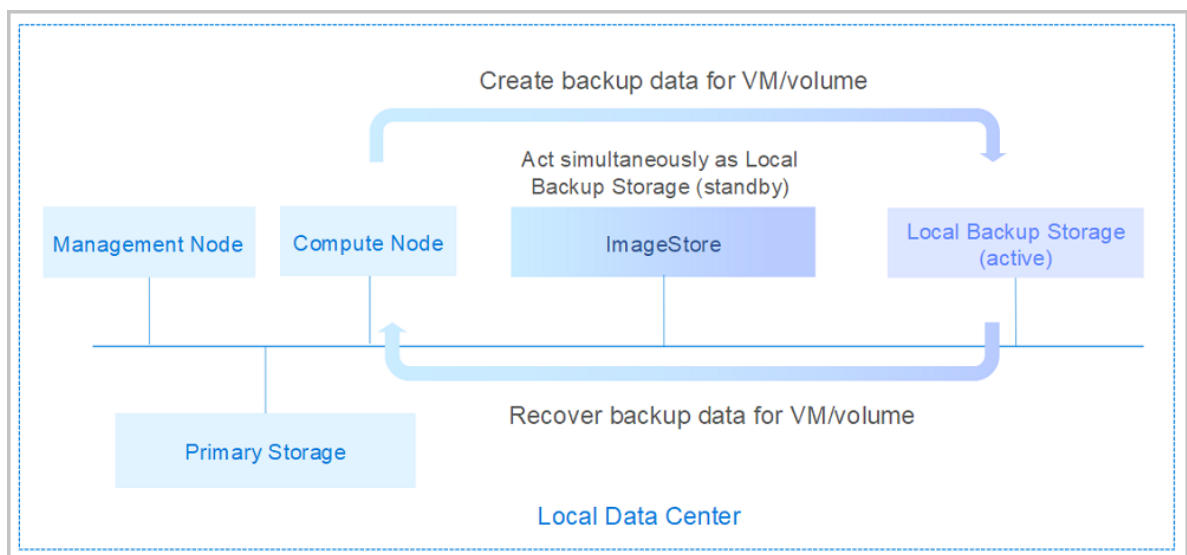
Backup Service can be applied to the following three typical scenarios: local backup, remote backup, and public cloud backup.

- **Local Backup**

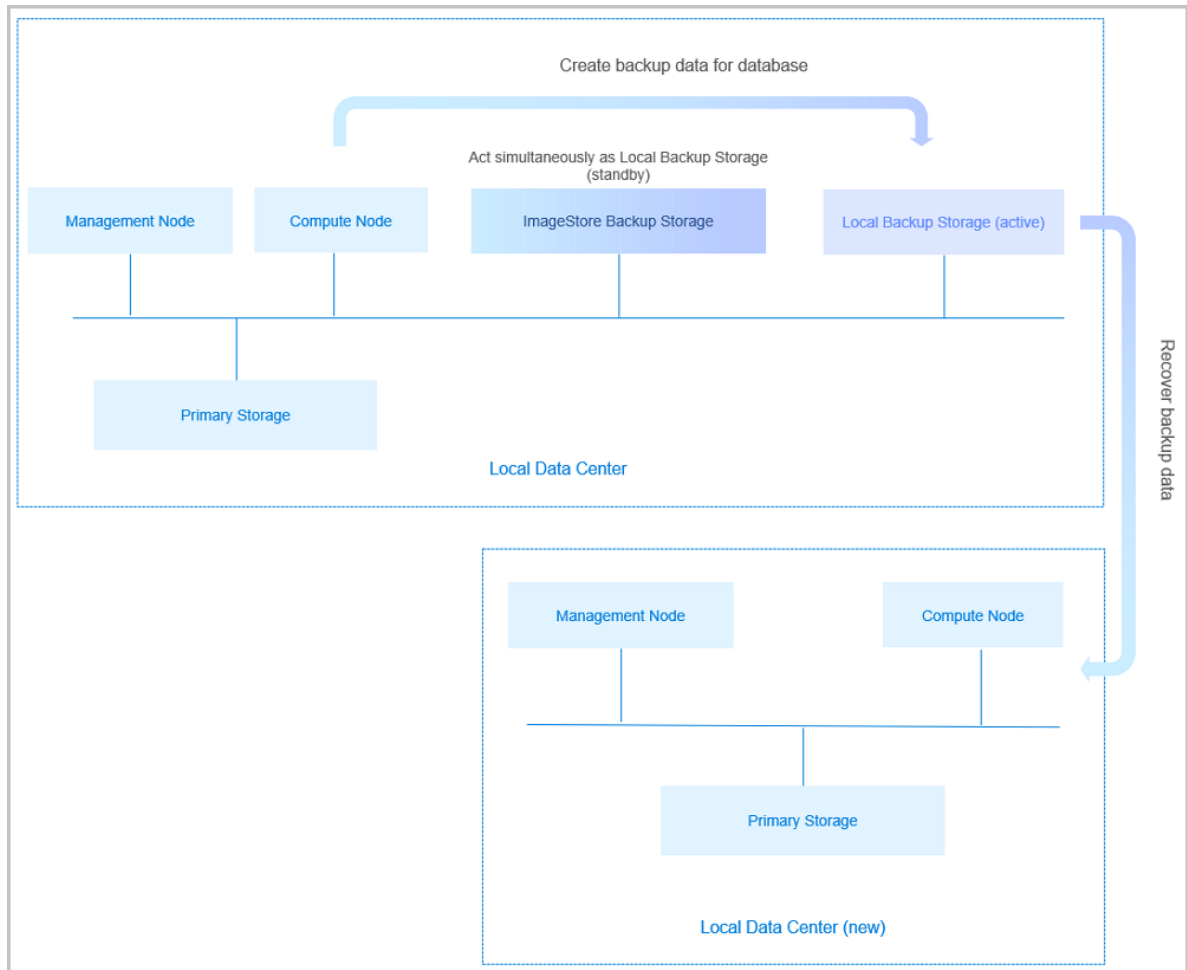
The local ImageStore can act as the **Local Backup Storage** to store scheduled backup data of the local VM instances, volumes, and management node databases. Meanwhile, the seamless switchover between the active local backup storage and the standby local backup storage is supported, which effectively 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 2-33: 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](#).

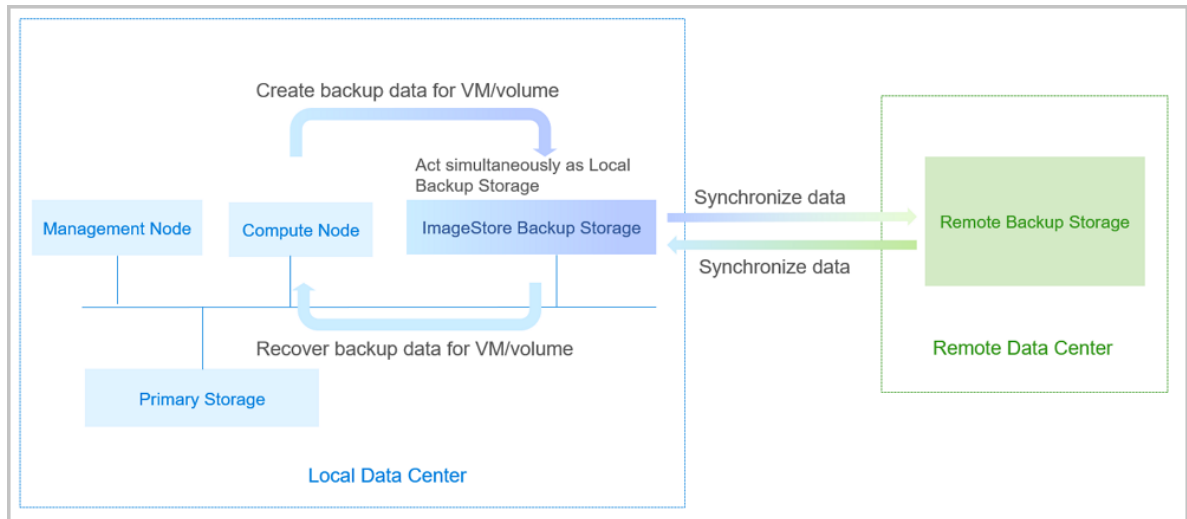
Figure 2-34: Local Backup Scenario-2

- **Remote Backup**

The storage server in the 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.

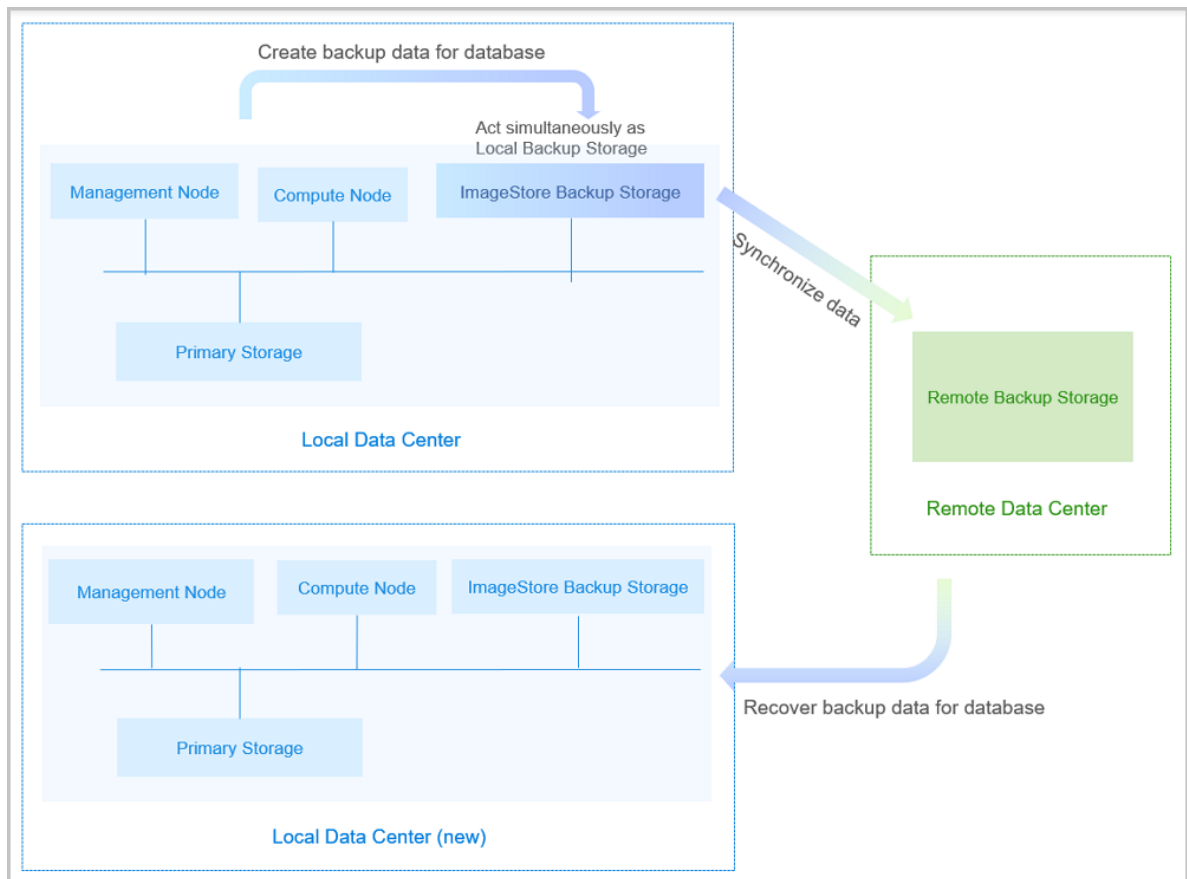
If your local data is mistakenly deleted, or data in the local primary storage is damaged, you can recover the backup data from the remote backup storage, as shown in [Remote Backup Scenario-1](#)

Figure 2-35: 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 2-36: Remote Backup Scenario-2

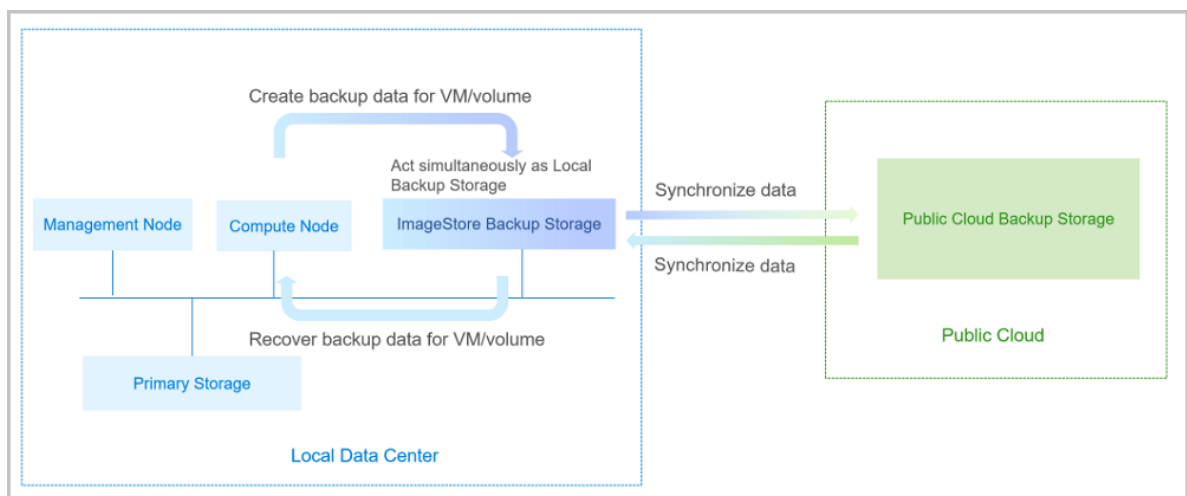


- **Public Cloud Backup**

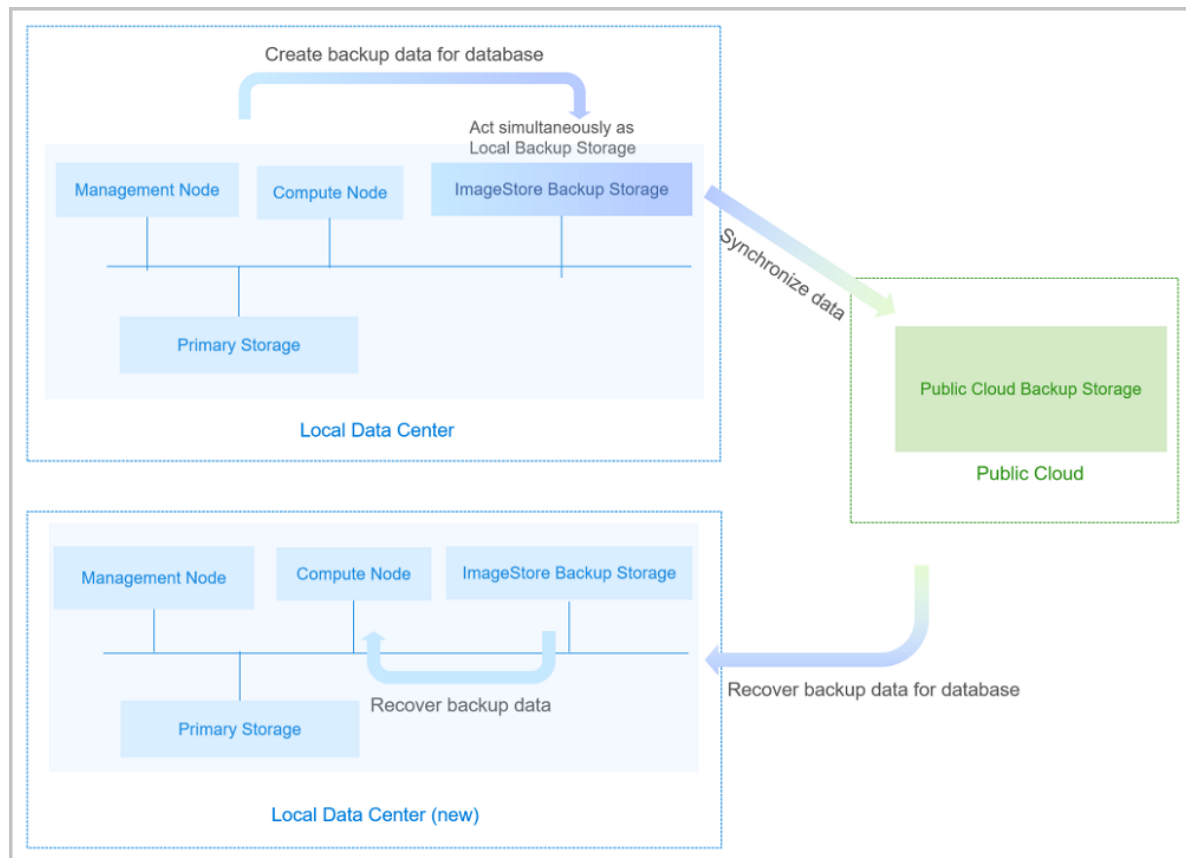
The storage server in the public cloud can act as the **Public Cloud Backup Storage** to store the scheduled backup data of the local VM instances, volumes, and databases. The backup data can be synchronized to the public cloud backup storage from the local backup storage.

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 2-37: 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 2-38: Public Cloud Backup Scenario-2

2.2.8.3.1 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.
 - You can 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.
 - You can update a backup policy for a backup task.
 - You can perform a one-time backup task immediately.
 - You can set a network QoS or disk QoS for a backup task.
 - When you create a backup task, the rich text mode is provided. You can 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 miss backup, 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.

2.2.8.3.2 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 available for this operation.

2.2.8.3.3 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.
- Invalid backup 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.

2.2.8.3.4 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 remote backup storage page.
- To recover 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.

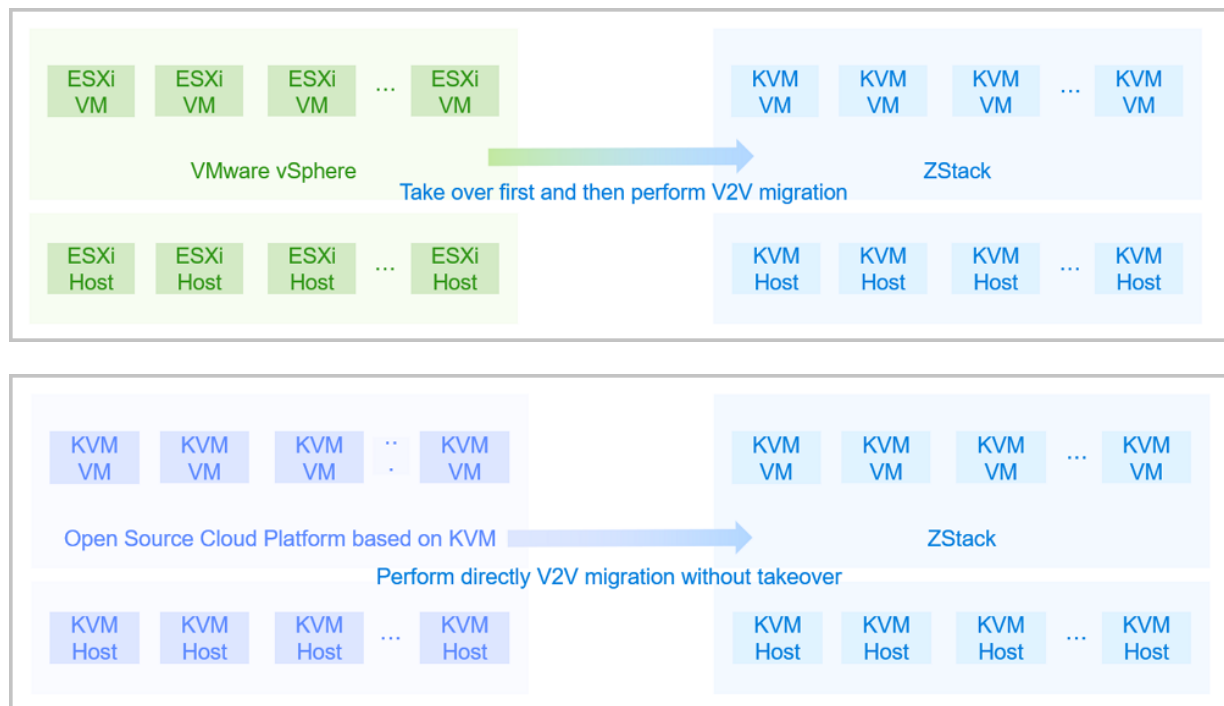
2.2.8.4 Migration Service

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 2-39: 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.

2.2.8.4.1 V2V Migration

Currently, V2V Migration Service allows you to migrate VM instances from a VMware cloud platform or a KVM cloud platform to the current cloud.

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.

Source Cloud Platform: KVM

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.

Source Cloud Platform: KVM

y 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.

2.2.8.4.2 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 2-4: 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.

3 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 automatically configure the networks of the VM instances.

The following table lists the features of ZStack Enterprise.

Type	Feature	ZStack Enterprise
Zone	Multi-zone management	<ul style="list-style-type: none"> • 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	<p>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.</p> <ul style="list-style-type: none"> • 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	<p>Tenants (normal accounts or project members) can manipulate the resources of the vCenter that you took over.</p> <ul style="list-style-type: none"> • Tenants can perform common operations on VM instances and volume resources in the vCenter that you took over.

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 high availability features, and defines cluster properties based on the CPU infrastructure of a host.
	Network service	<ul style="list-style-type: none"> 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 the scheduling suggestions to effectively improve your cloud stability while balancing cluster workloads.
	Advanced settings	Configures parameters for cluster resources by cluster:

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> 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	<p>ZStack Custom ISO has two versions: c76 ISO and c74 ISO.</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Allows you to set host properties for better management. After a host is disabled, you cannot create resources on this host. Note that the existing resources on this host are not affected.

Type	Feature	ZStack Enterprise
	Maintenance mode	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.
	Operation logs	Displays audit information associated with event login operations when you manage and operate hosts.

Type	Feature	ZStack Enterprise
	CSV file exporting	Allows you to export host lists in CSV format to facilitate the statistics analysis of your hosts.
	Zero copy	Allows you to enable the zero copy switch for hosts in a cluster. This helps to reduce the number of data copies between the kernel mode and the user mode, lower the CPU overhead, and improve the Virtio NIC performance of VM instances.
VM instance	Batch operation	Manages VM instances in bulk.
	VM instance creation	Provides multiple strategies to create VM instances to effectively use resources.
	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	<ul style="list-style-type: none"> Allows you to access VM instances through terminals without using remote tools. Supports three console modes: 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.
	VM snapshot	<ul style="list-style-type: none"> 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. Takes snapshots for VM instances that are in the running state (ImageStore and Ceph backup storages are supported).

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Clones both root volumes and data volumes of VM instances. If a VM instance has shared volumes attached, the data volumes of the VM instance cannot be cloned with the VM instance. Supports only ImageStore backup storages.

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<p>Makes a template image based on the current VM instance so that you can create VM instances in bulk in a custom manner.</p> <ul style="list-style-type: none"> 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).
	Custom MAC	<ul style="list-style-type: none"> Allows you to specify an MAC address when you create a VM instance.

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> 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 performance monitoring	<p>Displays VM workloads in real time for popular systems, such as Linux, Windows, and Chinese domestic operating systems.</p> <ul style="list-style-type: none"> 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).
	High availability(HA)	Automatically reboots a VM instance if its host encounters failures, and displays the rebooting process in the UI.

Type	Feature	ZStack Enterprise
	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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. Provides specific support for Windows failover clusters. Hot migration of VM instances will not have any adverse effects.

Type	Feature	ZStack Enterprise
	Storage migration	<ul style="list-style-type: none"> • Supports cold migration of VM instances across primary storages of the same type in the cloud. <ul style="list-style-type: none"> — 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	<ul style="list-style-type: none"> • Provides guest tools for Windows and Windows Virtio operating systems, and supports one-click installation of Virtio drive, agent, and QGA. • 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.

Type	Feature	ZStack Enterprise
	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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 <code>zstack-cli</code> . 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 with the SSH authentication method. When you create a VM instance, you can set a hostname or password in the UI with simple operations. These simple operations can improve user experience.
	Advanced settings	<p>Allows you to configure parameters for VM resources by VM instance.</p> <ul style="list-style-type: none"> Configures VM parameters independently, such as the NUMA and hyper-V switches of VM instances.

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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, automatically 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	<ul style="list-style-type: none"> 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.
	Volume management	<ul style="list-style-type: none"> 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.

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 independent billing or display. The supported types of primary 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	<ul style="list-style-type: none"> Allows you to create, enable, disable, delete an instance offering, share an instance offering

Type	Feature	ZStack Enterprise
		<p>globally, recall an instance offering globally, and set the disk QoS and network QoS for an instance offering.</p> <ul style="list-style-type: none"> 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 independent billing or display. The supported types of primary storages include Ceph, LocalStorage, NFS, and SharedBlock.
GPU specification	GPU specification	<ul style="list-style-type: none"> 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.
	ISO image	Guides a VM instance to install an operating system via an ISO image.
	BIOS mode	<ul style="list-style-type: none"> 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.

Type	Feature	ZStack Enterprise
	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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Supports image transmissions among ImageStores. 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	<p>Supports the following software operating environments:</p> <ul style="list-style-type: none"> 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

Type	Feature	ZStack Enterprise
	Application image preconfiguration	<p>Supports the following application systems:</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.
	Shared Mount Point primary storage	<ul style="list-style-type: none"> 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.

Type	Feature	ZStack Enterprise
	Shared Block primary storage	<ul style="list-style-type: none"> • Allows you to add an iSCSI or FC protocol storage through which hosts can intercommunicate. • Allows you to add an iSCSI storage, to automatically 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 passthrough 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.
	Ceph primary storage	<ul style="list-style-type: none"> • 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.

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Supports VXLAN networks to effectively address the shortage of logical network segments in the 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.

Type	Feature	ZStack Enterprise
	Distributed flat network	<ul style="list-style-type: none"> Allows a VM instance to use a real network IP resource. Provides two types of IP address type: IPv4 and IPv6. Provides the following network services: security group, VIP in flat, private 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Allows you to specify a gateway when you add a network range by using an IP range. 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	<ul style="list-style-type: none"> 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.

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> • 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 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.
	Firewall	<ul style="list-style-type: none"> • 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. • 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.

Type	Feature	ZStack Enterprise
	VPC vRouter HA group	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.
	Public network	<ul style="list-style-type: none"> 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. For a public network of the IPv4 type, you can add an IP pool based on the common IP range. The IP pool can be used to create VIPs and provide various network services.
	System network	Acts as a management network, storage network, and migration network.
	vRouter network	<ul style="list-style-type: none"> 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.

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Supports the following load balancing network services: <ul style="list-style-type: none"> — 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.

Type	Feature	ZStack Enterprise
	Netflow	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.

Type	Feature	ZStack Enterprise
	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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Allows a security group to uniformly manage VM security policies to achieve intercommunication within the security group. Specifically, a security 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.

Type	Feature	ZStack Enterprise
	Router performance analysis	<ul style="list-style-type: none"> 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.
	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	<p>Intuitively displays the capacity information about core resources in the cloud.</p> <ul style="list-style-type: none"> 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

Type	Feature	ZStack Enterprise
		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	<ul style="list-style-type: none"> 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.
	Alarm	<ul style="list-style-type: none"> Provides resourceful metric items so that you can monitor and create alarms for the following resources and events: <ul style="list-style-type: none"> Resources: VM instance, BareMetal instance , router, image, backup storage, system data directory, host, L3 network, volume, VIP, primary storage, and load balancer listener Events: Events related to VM instance, router , backup storage, management node, host, primary storage, vCenter, and backup job. Sets alarms for metric data and event, and receives alarm messages via SNS notification, such as email, DingTalk, HTTP application, and Aliyun short message. 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

Type	Feature	ZStack Enterprise
		<p>for resource alarms. Specifically, you can flexibly configure an alarm policy as needed.</p> <ul style="list-style-type: none"> 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 readability 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 efficiencies.
	Multiple endpoint	<ul style="list-style-type: none"> Supports multiple endpoints, including email, DingTalk, HTTP application, and Aliyun short message. Allows you to add multiple endpoint addresses to email endpoints and Aliyun short message endpoints.
Auditing	Resource auditing	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> Allows you to configure log reservation time as needed. Displays event audits and login audits of performed operations. Global settings allows you to set log reservation 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	<ul style="list-style-type: none"> 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.

Type	Feature	ZStack Enterprise
	Specified allocation of network resource	Allows you to share an L2 network resource and an L3 network resource. Specifically, you can specify whether an account can use the L2 network resource and the L3 network resource.
	Global settings	<p>Allows you to directly perform global settings on various properties in the UI.</p> <ul style="list-style-type: none"> 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 <code>zstack-ctl reset_password</code> to restore the default setting.
Billing	Custom pricing list	<ul style="list-style-type: none"> 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	Supports project-based or account-based billings to calculate expenses of each resource. You can use different pricing lists to customize different pricing strategies for different projects and accounts.
	Disk performance-based pricing	Allows you to set different pricing units independently for different types of disks.
	Billing currency symbol	Allows you to set a billing currency symbol on the global settings. The supported currency unit includes CNY (¥), USD (\$), EUR (€), GBP (£), AUD (A\$), HKD (HK\$), JPY (¥), CHF (CHF), and CAD (C\$).

Type	Feature	ZStack Enterprise
	Bills	<p>Calculates and displays resource expense information of an administrator and all tenants by billing price and time of usage.</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Allows you to authenticate with dynamic authentication 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. 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.

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 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.

Type	Feature	ZStack Enterprise
	In-process display	Adds progress bars of multiple scenarios.
VDI	Solution	<ul style="list-style-type: none"> • 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 information 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	<ul style="list-style-type: none"> • Allows you to create tags of different names or colors, and binds them to VM instances or volumes to manage and search 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)	<ul style="list-style-type: none"> • Includes enterprise edition and hybrid edition. • Allows you to upload Basic License via a local browser. • Supports expiration notifications of Basic License. • Supports all features for Enterprise, standalone version with unlimited trials. • Supports two types of authorization method: CPU and host.
	Module license (Plus License)	<ul style="list-style-type: none"> • Provides additional functionality. • Depends on Basic License.

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 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 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.
Compute node	Batch host addition	<ul style="list-style-type: none"> Allows you to add hosts in bulk according to the network range that you entered.

Type	Feature	ZStack Enterprise
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 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

Type	Feature	Enterprise Management Module
		information of projects where the users belong can be synchronously imported.
	Organization	<ul style="list-style-type: none"> • 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 organization 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 organization, change a parent department, create a subsidiary department, delete a subsidiary department, add a user, and remove a user.
	Role	<ul style="list-style-type: none"> • 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. • 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.

Type	Feature	Enterprise Management Module
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 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	<ul style="list-style-type: none"> Identifies the template of each resource quota. Allows you to directly use the quota defined by the template to quickly create a project.

Type	Feature	Enterprise Management Module
		<ul style="list-style-type: none"> Allows you to create a project template and delete a project template.
	project member	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.
	Ticket approval	<ul style="list-style-type: none"> 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 automatically deployed successfully and distributed to the corresponding project.

Type	Feature	Enterprise Management Module
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.
	Resource isolation	<ul style="list-style-type: none"> 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	BareMetal cluster	<ul style="list-style-type: none"> Manages BareMetal hosts by creating a BareMetal cluster. Allows you to attach a BareMetal cluster to an L2 network.
	Deployment server	<ul style="list-style-type: none"> Automatically installs and deploys the system for newly-created BareMetal chassis via a deployment server. Allows you to deploy a deployment (PXE) server independently.
	BareMetal chassis	<ul style="list-style-type: none"> Deploys BareMetal chassis in bulk via an IPMI network. Allows you to manage powers of BareMetal chassis remotely. Adds BareMetal chassis in bulk according to the network range that you entered. Allows you to add BareMetal chassis in bulk via template importing. Allows you to open the IPMI management page (login page) of BareMetal chassis via a console. You can log in to the BareMetal chassis by entering the configured IPMI user name and the IPMI password.
	BareMetal instance	<ul style="list-style-type: none"> Allows you to install Linux operating system for BareMetal chassis with an ISO image. Allows you to install Ubuntu, CentOS, and SUSE in an unattended manner. Allows you to add network configurations for a BareMetal instance. Provides real-time monitoring of internal workloads . For BareMetal instance monitoring, you need to install an agent. You can check CPU, memory, disk, NIC, and other performance inductors of a BareMetal instance. Provides associated monitoring items of a BareMetal instance, including CPU, memory, disk, and NIC.

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

Type	Feature	Backup Service Module
Backup service	Backup	<ul style="list-style-type: none"> • 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. • 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.

Type	Feature	Backup Service Module
		<ul style="list-style-type: none"> • Cleans invalid backup data that was completely deleted 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	<ul style="list-style-type: none"> • 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. • 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 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.

Type	Feature	Migration Service Module
		<ul style="list-style-type: none"> Provides unlimited types of source primary storage . Currently, the target primary storage supports Ceph, Shared Block, NFS, and LocalStorage.
	V2V migration for KVM	<ul style="list-style-type: none"> 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.

4 Product Highlights

ZStack is the next-generation, private cloud IaaS software featuring Simple, Strong, Scalable and Smart (4S).

1. Simple

- Easy installation and deployment: Allows you to download installation packages from our official website. You can install and deploy the cloud from scratch within just 30 minutes.
- Easily-managed cloud: Supports bulk operations of VM instances, such as creating or deleting VM instances in bulk, and provides list displays and sliding window details.
- Simple, practical operations: Provides a thorough User Guide with ample help information, a productive community, and standard APIs.
- Friendly UI: Provides you with a well-designed, friendly user interface to realize powerful features by performing simple operations.

2. Strong

- Stable, efficient system architecture design: Provides an asynchronous architecture, in-process microservices architecture, lock-free architecture, stateless service architecture, and consistent hashing ring to ensure the system efficiency and stability. Currently, ZStack has achieved various functions. For example, a single management node can manage tens of thousands of hosts, and hundreds of thousands of VM instances. A cluster that contains multiple management nodes can use a database and a set of message buses to manage hundreds of thousands of hosts and millions of VM instances, and handle tens of thousands of concurrent APIs.
- High concurrent API requests: Handles high concurrences of API requests. A single ZStack management node can easily handle tens of thousands of concurrent API call requests per second.
- Stringent HA requirements: Provides stringent HA requirements. When a network or management node is unavailable, appliance VM instances can be automatically switched to another management node that is detected as healthy. The management node virtualization helps to achieve the high availability for a single management node. That is, standby management nodes will be dynamically applied within seconds if any management node is disconnected, thus ensuring your business continuity.

3. Scalable

- **Large scale:** Manipulates a huge scale of VM instances. Technically, a single management node can manage one to tens of thousands of hosts and hundreds of thousands of VM instances.
- **Comprehensive API:** Provides a whole set of IaaS APIs. Hence, you can create brand-new, available zones across multiple geographical locations, modify network configurations, and upgrade physical servers.
- **Resource allocation based on your needs:** Resizes important resources such as VM instances and cloud storages according to your demands. ZStack not only allows you to modify online the CPU, memory, and other resources for a VM instance, but also allows you to dynamically adjust its network bandwidth, disk bandwidth, and other resources for a VM instance.

4. Smart

- **Automatic O&M:** Provides all O&M operations that can be managed by ZStack APIs in the ZStack environment. By using the Ansible inventory, ZStack can realize full-automatic deployment and upgrade as well as automatic detection and reconnection. If network jitters happen or hosts restart, each management node can be automatically reconnected to the networks or the hosts. Note that a ZStack scheduler allows you to start or stop VM instances on schedule, and allows you to take VM snapshots on schedule with the round-robin policy.
- **Online seamless upgrade:** Provides one-click seamless upgrade within 5 minutes. Hence, you only need to upgrade and manipulate management nodes. After the cloud is upgraded successfully and started, the compute node, storage node, and network node will be automatically upgraded as well.
- **Intelligent UI interaction:** Displays compute resources in real time, thereby empowering you to avoid misoperations.
- **Real-time global monitoring:** Manages and controls the current resource consumption of the entire cloud. With the real-time monitoring, you can adjust your resources intelligently to save IT software and hardware resources.

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 platform 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.