Quick Installation and Usage Tutorial

Version: ZStack Cloud 4.3.12

Issue: V4.3.12

ZStack

Copyright Statement

Contents

1 Introduction

ZStack Cloud provides the following two custom ISO editions:

- C76: ZStack-Cloud-x86_64-DVD-4.3.12-c76.iso

- C74: ZStack-Cloud-x86_64-DVD-4.3.12-c74.iso

> **Note:**
>
> - The custom ISO of the c76 edition inherits all features of the c74 edition. In addition, it uses the updated operating system core and supports NVIDIA vGPU.
>
> - **For the first installation of ZStack Cloud, we recommend that you use ISO of the c76 edition.**. If you have deployed ZStack Cloud, you can upgrade the Cloud to the latest version of the same edition. For more information, see Upgrading Tutorial.
>
> - Starting from 3.7.1, ZStack Cloud custom ISO of the c72 edition is no longer available. If you have deployed the ISO of the c72 edition, contact the technical support for upgrading.

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

2 Environment Preparations

2.1 Prepare Software Packages

Before you install ZStack Cloud, prepare the following software packages:

- ZStack Cloud custom ISO:

    — C76: ZStack-Cloud-x86_64-DVD-4.3.12-c76.iso

    — Download address: *Click here*

- ZStack Cloud installation package:

    — Software: ZStack-Cloud-installer-4.3.12.bin

    — Download address: *Click here*

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

2.2 Hardware Requirements

The following table takes a single server deployment (All-in-One) as an example to describe the configuration requirements over the server and other hardware devices for the installation and deployment of ZStack Cloud.

Device	Configuration Requirements
Server	- CPU: support for 64 bit, Intel VT or AMD V virtualization hardware extensions, and with no lower than 4 cores - Memory: no lower than 8 GB for basic demonstration environments and no lower than 64 GB for production environments - At least 1 SATA hard disk with no lower than 1 TB of storage capacity - At least a one-gigabit NIC
Network Switch	- At least a one-gigabit switch, ten-gigabit switch recommended - Several Category 5 jumpers

2.3 Burn Image to U Disk

Context

This topic describes how to use UltraISO to burn the prepared ISO image file to a U disk.

Procedure

1. Use UltraISO to open the ISO image file.

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

   Figure 2-1: Use UltraISO to Open ISO Image File
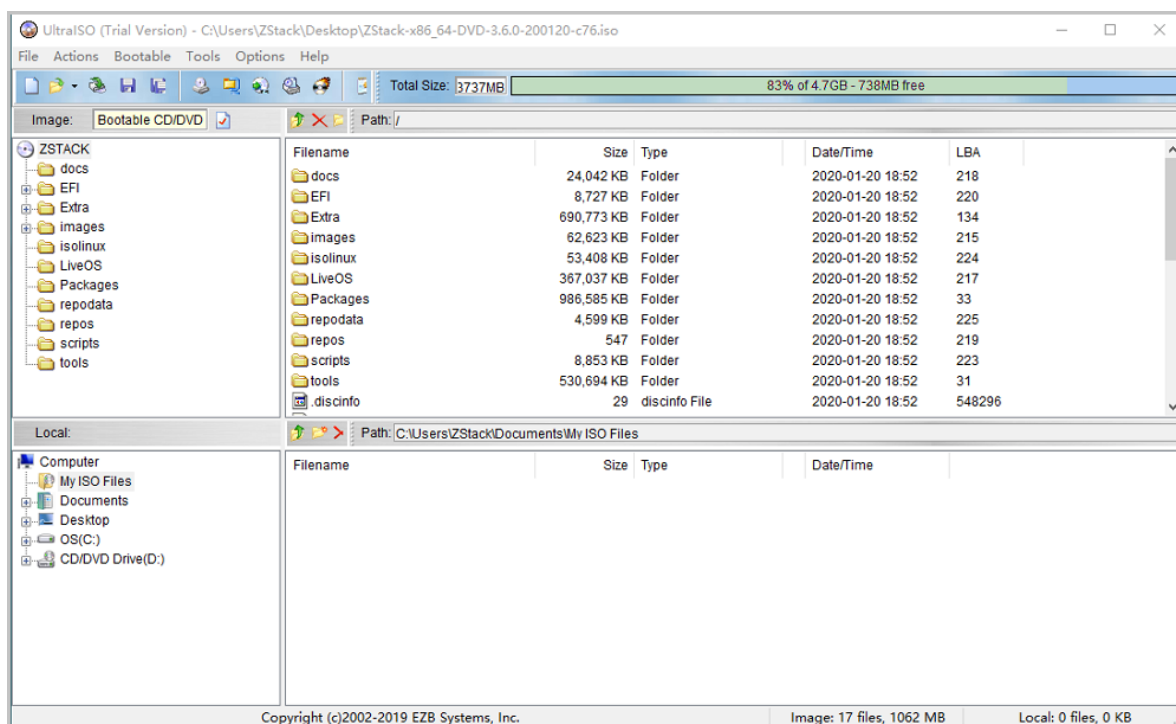
2. Write the Image.

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

Figure 2-2: Write Disk Image on UltraISO
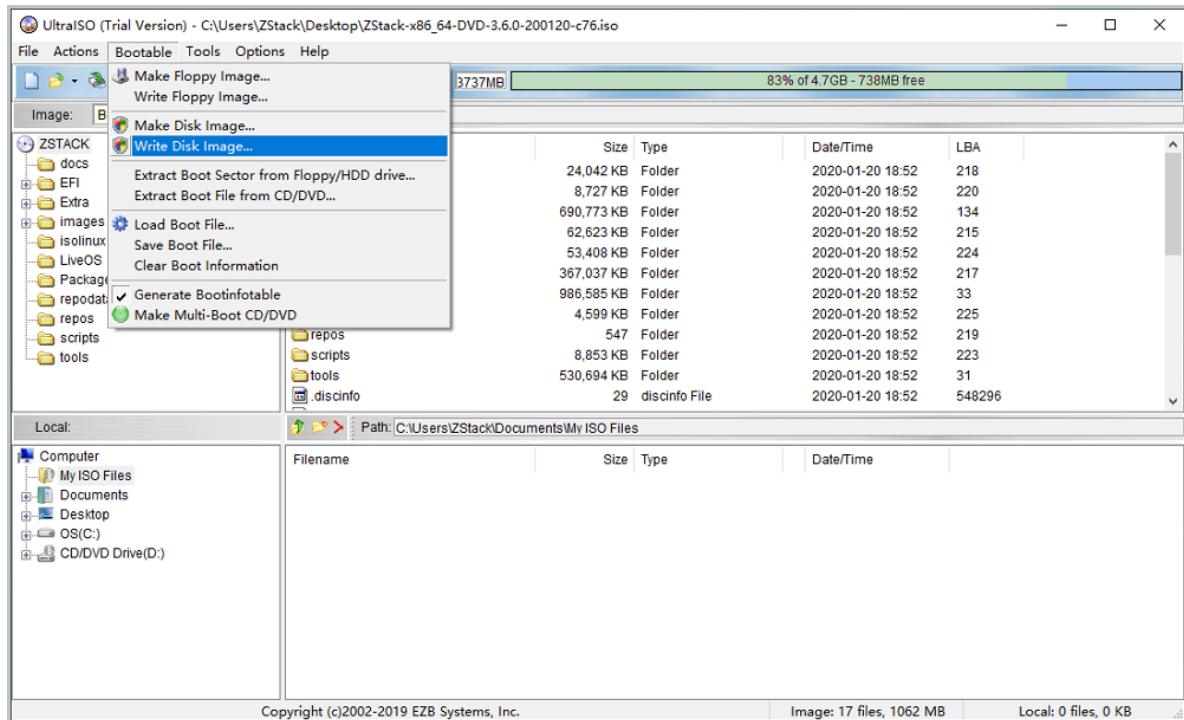
3. Select a U disk from the **Disk Drive** drop list to burn the image file.

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

Figure 2-3: Confirm to Write ISO Image on UltraISO
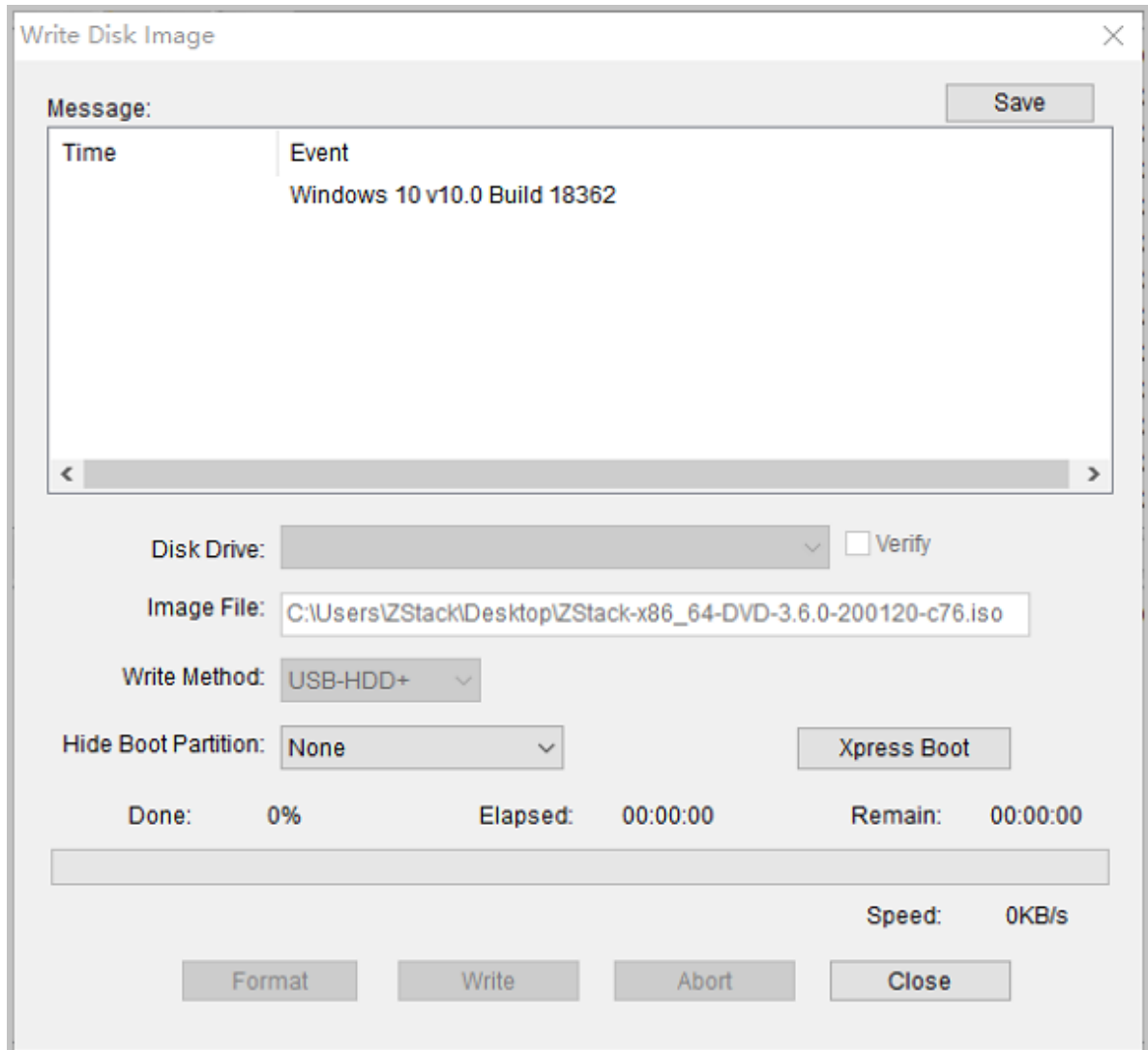
4. On the page that appears, click **Yes**. Then UltraISO burns the ISO image file to the U disk.

5. Then the U disk is used as the startup disk that supports the Legacy and UEFI boot modes.

3 Install Operating System

Procedure

1. Configure the server.

   - Make sure that the data on the disks of the server is backed up. The data will be overwritten during installation.

   - Enter BIOS and enable the virtualization technology and hyper-threading options for CPU.

   - Enter the RAID configuration page and configure the RAID level to provide a data redundancy mechanism that suits your business needs.

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

2. Select the boot item.

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

   Figure 3-1: System Boot
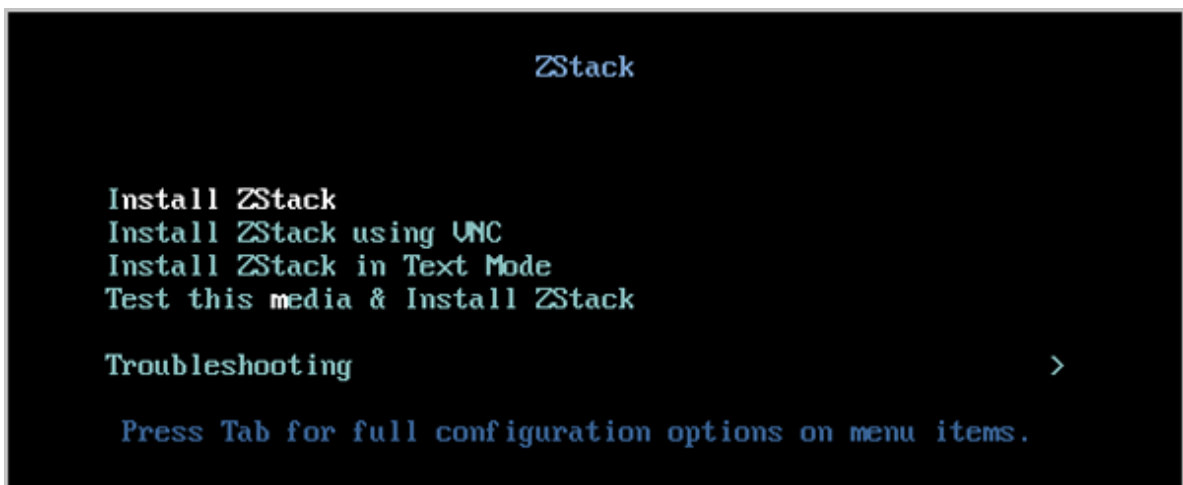
   📋 **Note:**

   - ZStack Cloud provides the following installation methods: (graphic user interface) GUI, virtual network computing (VNC), and character user interface (CUI). We recommend that you use GUI to install the operating system.

   - If the server does not have a VGA connector and only supports serial communication, you can use the VNC or CUI method.

3. Installation configuration summary.

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

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

Figure 3-2: System Installation Interface

4. Select the installation mode.

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

   ZStack Cloud provides the following installation modes:

- ZStack Enterprise Management Node

> **Note:**
>
> We recommend that you select this mode in the initial installation.

- ZStack Community Management Node

- ZStack Compute Node

- ZStack Expert Mode

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

Figure 3-3: Select Installation Mode
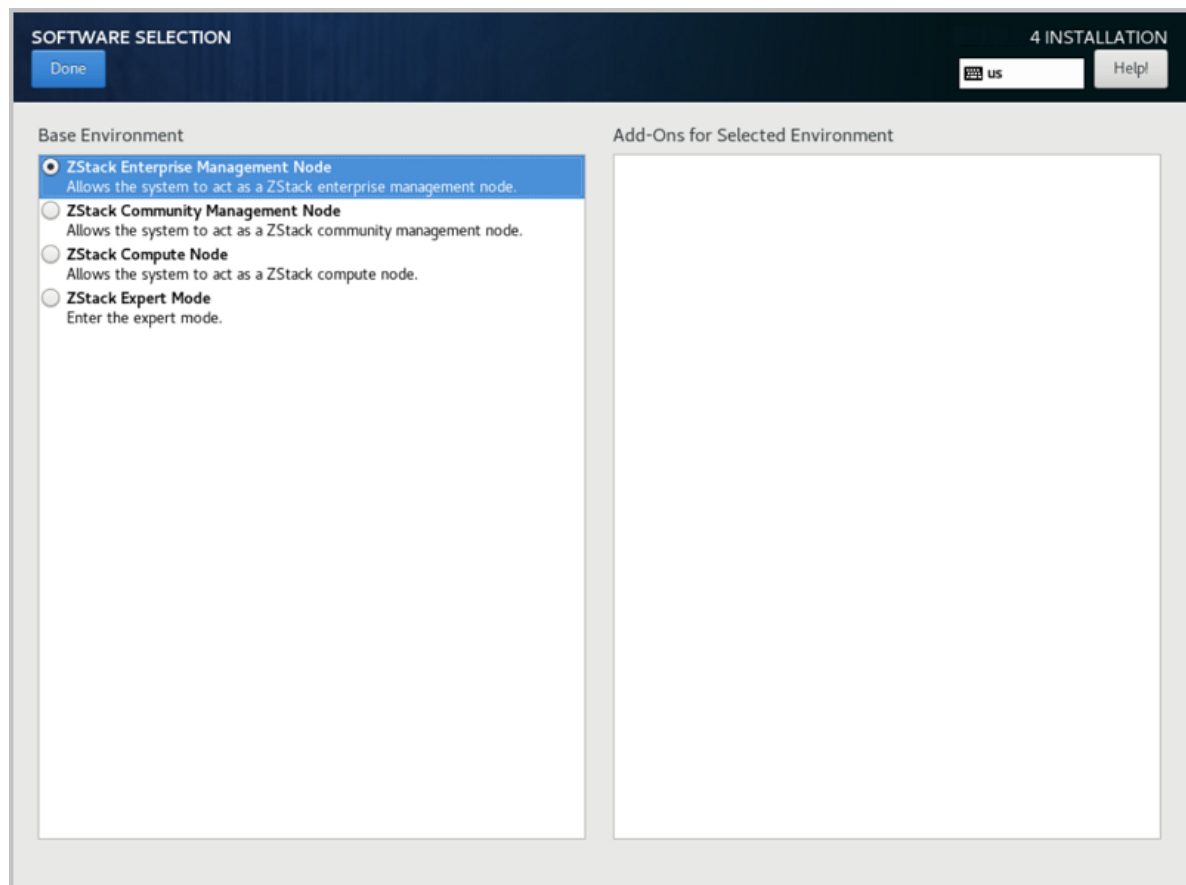
5. Configure disk partitioning.

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

Figure 3-4: Default Disk Partitioning

> 📋 **Note:**
>
> We recommend that you configure only the system disk on the page. After the system is installed, you can configure other disks.

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

- UEFI mode

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

  — */boot/efi*: stores UEFI boot file. We recommend that you distribute 500 MB to the directory.

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

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

- Legacy mode

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

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

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

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

6. Configure the network.

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

1. Configure a static IP address.

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

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

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

Figure 3-5: Configure Static Address

2. Configure NIC auto-activation.

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

Figure 3-6: Configure NIC Auto-Activation
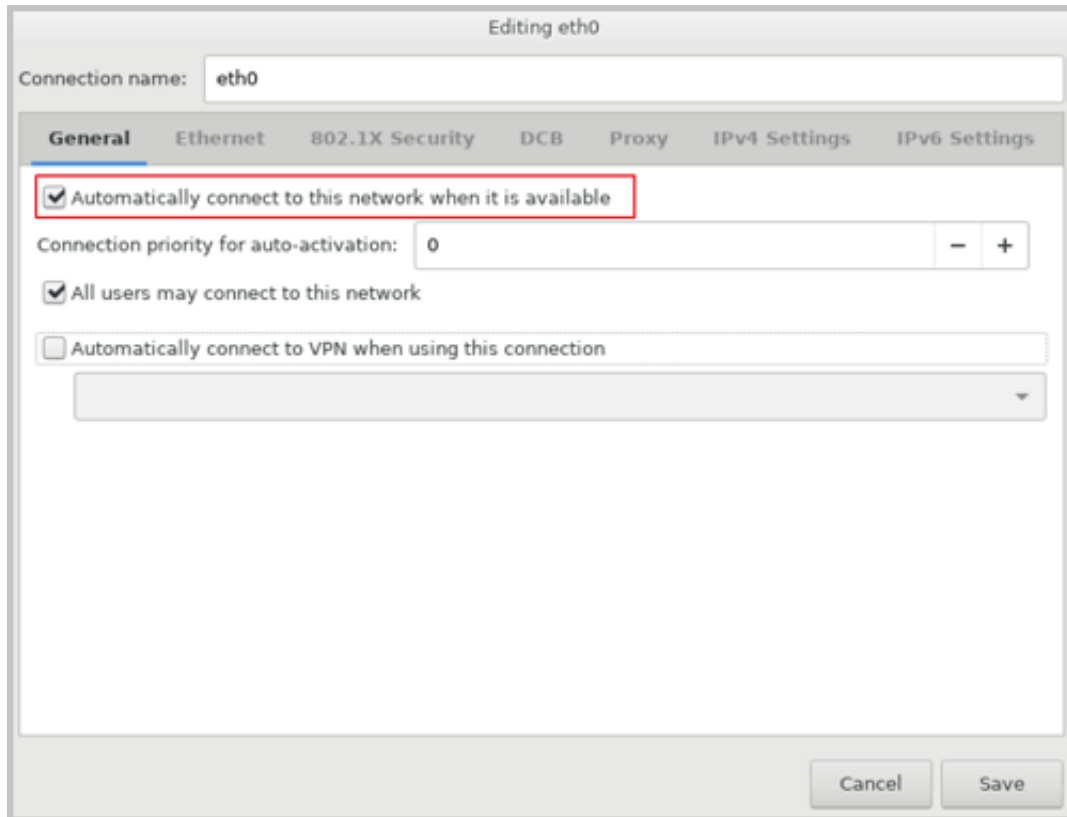
7. Start installation.

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

8. Set a password.

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

Figure 3-7: Set Password
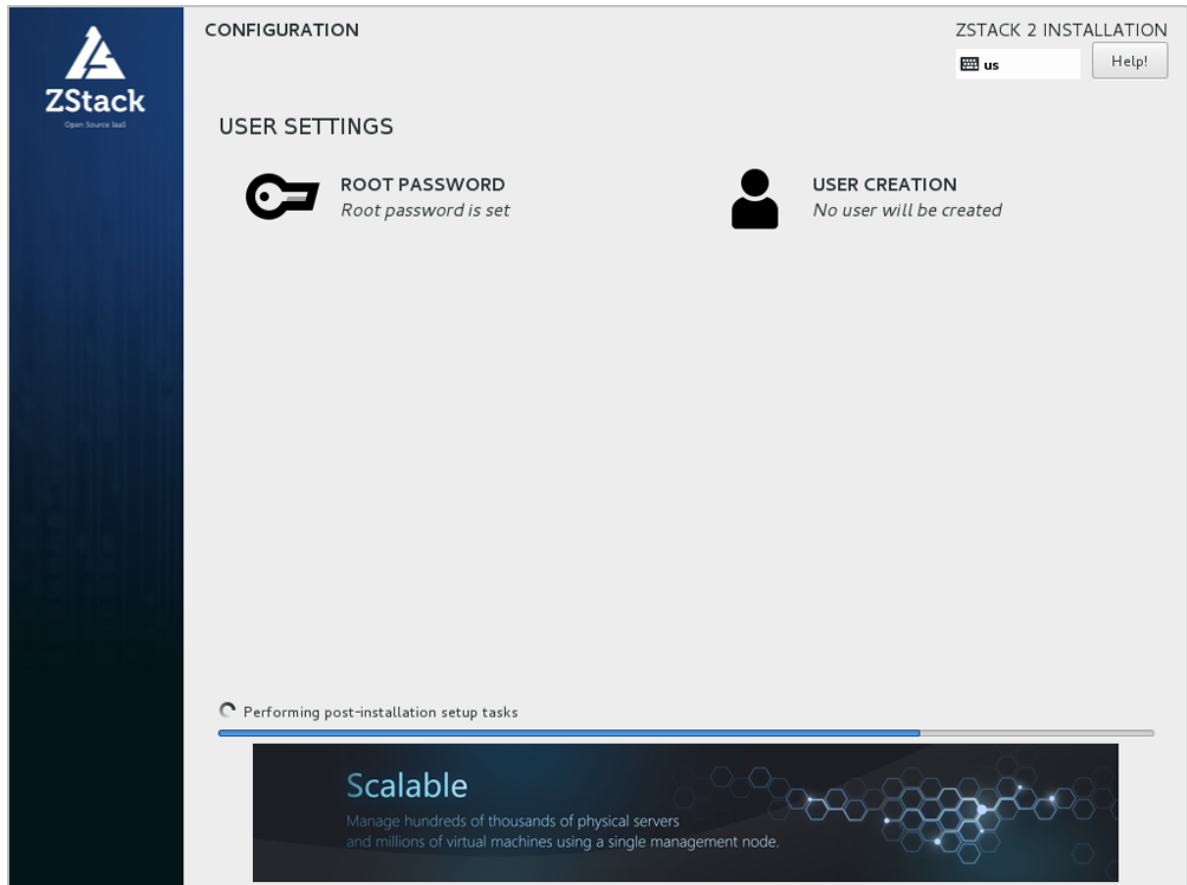
9. Enter the system.

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

4 Getting Started

4.1 Initialization by Wizard

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

- If you stop using the wizard or delete key resources during initial setup, **you are not directed to use the wizard again**.

- We recommend that you use the wizard to complete the basic environment configurations of ZStack Cloud.

4.1.1 Create a Zone

Context

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

Figure 4-1: Create Zone

On the displayed page, set the following parameters:

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

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

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

4.1.2 Create a Cluster

Context

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

Figure 4-2: Create Cluster

On the displayed page, set the following parameters:

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

- **Description**: Optional. Enter a description for the cluster.

- **Type**: Optional. Select a hypervisor type for the server. Valid values: KVM and XDragon.

- **CPU Architecture**: Optional. Set the CPU architecture of the hosts in the cluster. If left blank, when you add the first host to the cluster, the CPU architecture of the hosts that you later add to the cluster must be the same as the architecture of this host. You cannot change the CPU architecture of the cluster any more.

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

4.1.3 Add a Host

Context

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

Figure 4-3: Add Host

On the displayed page, set the following parameters:

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

- **Description**: Optional. Enter a description for the host.

- **Type**: Select a hypervisor type for the server. Valid values: KVM and XDragon.

- **Host IP**: Enter an IP address for the host, for example, *172.20.14.32*.

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

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

  — The separation of the management network and public network can maximize system security and ensure sufficient bandwidth for the management network.

- **SSH Port**: Enter an SSH port for the host. Default: 22. If you do not specify an SSH port for the host, the system uses port 22 as the SSH port.

- **User Name**: Enter a username that has the sudo permission for the host.

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

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

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

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

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

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

- The configuration process may last several minutes.

- Error messages are prompted if errors occur.

What's next

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

4.1.4 Add a Backup Storage

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

You can add the following types of backup storages:

- **ImageStore**: stores images in the format of chips and supports incremental storage.

- **Sftp**: stores images in the format of files.

- **Ceph**: stores images in the format of distributed blocks.

Configure a backup storage based on your business needs.

4.1.4.1 ImageStore

Context

Figure 4-4: Add ImageStore Backup Storage

On the displayed page, set the following parameters:

- **Name**: Enter a name for the backup storage.

- **Description**: Optional. Enter a description for the backup storage.

- **Type**: Select ImageStore.

- **Backup Storage IP**: Enter a backup storage IP.

  — In the production environment, for the concerns of security and stability concerns, we recommend that you separate the management network from the public network.

  — You can assign a management network IP address to the backup storage and save public network bandwidth.

  — If the public network has ten-gigabits of bandwidth, you can assign a public network IP address to the backup storage. This increases the image transmission rate between the backup storage and compute nodes.

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

— You can set a dedicated storage network if necessary.

- **Mount Path**: Specify a path on the backup storage that corresponds to sufficient storage space, for example, */ImageStore_bs*.

- **Retrieve Existing Image**: Choose whether to retrieve images stored in the specified path.

- **SSH Port**: Enter an SSH port for the backup storage. Default: 22. If you do not specify an SSH port for the backup storage, the system uses port 22 as the SSH port.

- **User Name**: Enter a username. By default, root user is used. You can also specify a normal user.

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

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

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

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

4.1.4.2 Ceph

Context

Figure 4-5: Add Ceph Backup Storage

On the displayed page, set the following parameters:

- **Name**: Enter a name for the backup storage.

- **Description**: Optional. Enter a description for the backup storage.

- **Type**: Select Ceph.

- **Monitor Node IP**: Enter the IP address of the Ceph monitor node.

- **SSH Port**: Enter an SSH port for the monitor node. Default: 22. If you do not specify an SSH port for the monitor node, the system uses port 22 as the SSH port.

- **User Name**: Enter a username. By default, root user is used. You can also specify a normal user.

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

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

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

- **Pool UUID**: Optional. Specify a storage pool for the Ceph backup storage.

  — Before you specify a pool, you need to create a pool in the Ceph storage cluster.

  — If left blank, a storage pool is created automatically.

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

4.1.5 Add a Primary Storage

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

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

- **LocalStorage**: uses the disks of the host for storage.

- **Network Sharing Storage**: supports NFS, Shared Mount Point, and Ceph.

  — NFS allows you to store files by using the NFS protocol.

  — Shared Mount Point provides network sharing storage by using popular distributed file systems including MooseFS, GlusterFS, OCFS2, and GFS2.

  — Ceph stores files in the format of distributed blocks.

> **Note:**
>
> The type of primary storage is associated with the type of backup storage:
>
> - If you use ImageStore backup storage, you can use a primary storage of the LocalStorage, NFS, Share Mount Point, or Ceph type.

> • If you use a Ceph backup storage, you can use only Ceph primary storage.
>
> If you need to add a primary storage of the SharedBlock type, exit the wizard and add a primary storage on the primary storage management page.

4.1.5.1 LocalStorage

Context

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

Figure 4-6: Add LocalStorage Primary Storage

On the displayed page, set the following parameters:

- **Name**: Enter a name for the primary storage.

- **Description**: Optional. Enter a description for the primary storage.

- **Type**: Select LocalStorage.

- **Mount Path**: Specify a path on the primary storage

> 📋 **Note:**
>
> - If the specified path does not exist on the primary storage, the system automatically creates the path.
>
> - You cannot specify the following system paths. Otherwise, a host error may occur:
>
>   — /

```
    ━ /dev/

    ━ /proc/

    ━ /sys/

    ━ /usr/bin

    ━ /bin
```

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

4.1.5.2 NFS

Context

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

Figure 4-7: Add NFS Primary Storage

On the displayed page, set the following parameters:

- **Name**: Enter a name for the primary storage.

- **Description**: Optional. Enter a description for the primary storage.

- **Type**: Select NFS.

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

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

- **Mount Option**: To add mount options, make sure that these options are supported by the NFS server.

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

- **Storage Network**: Specify a network for the shared storage. You can use the management network.

> **Note:**

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

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

4.1.5.3 Shared Mount Point

Prerequisites

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

Context

Figure 4-8: Add SMP Primary Storage

On the displayed page, set the following parameters:

- **Name**: Enter a name for the primary storage.

- **Description**: Optional. Enter a description for the primary storage.

- **Type**: Select SharedMountPoint.

- **Mount Path**: Specify the URL of the shared directory mounted on hosts.

- **Storage Network**: Specify a network for the shared storage. You can use the management network.

  > 📋 **Note:**

- If you specify a dedicated storage network, you need to specify the CIDR of the network.

- You can use the storage network to check the health status of VM instances.

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

4.1.5.4 Ceph

Context

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

Figure 4-9: Add Ceph Primary Storage

On the displayed page, set the following parameters:

- **Name**: Enter a name for the primary storage.

- **Description**: Optional. Enter a description for the primary storage.

- **Type**: Select Ceph.

- **Cephx**: Choose whether to use keys for authentication.

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

- **IP Address**: Enter the IP address of the Ceph monitor node.

- **SSH Port**: Enter the SSH port of the Ceph monitor node. Default: 22.

- **User Name**: Enter the username of the Ceph monitor node.

- **Password**: Enter the password for the specified username.

- **Image Cache Pool**: Enter an image cache pool. If left blank, the system automatically creates a pool.

- **Data Volume Pool**: Enter a data volume pool. If left blank, the system automatically creates a pool.

- **Root Volume Pool**: Enter a root volume pool. If left blank, the system automatically creates a pool.

- **Storage Network**: Specify a network for the shared storage. You can use the management network.

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

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

4.1.6 Create an Instance Offering

Context

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

Figure 4-10: Create Instance Offering

On the displayed page, set the following parameters:

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

- **Description**: Optional. Enter a description for the instance offering.

- **CPU**: Enter the number of CPU cores of a VM instance.

- **Memory**: Set the size of the VM memory. Note that this value must be an integer. Unit: MB, GB, and TB.

- **Host Allocation Strategy**: Specify how the Cloud allocates hosts when you create VM instances. Default strategy: **Host with min. running VMs**.

  — **Host with min. running VMs**: Allocates the host with the minimum number of running VM instances to create VM instances.

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

  > **Note:**
  >
  > - The Cloud collects the host CPU loads over a period of time, calculates the CPU average utilization during this period, and then selects the host with the lowest CPU utilization to create VM instances.
  >
  > - By default, the Cloud collects data at an interval of 10 minutes. You can change the collection cycle by using the following method:
  >
  >   Choose **Settings** > **Platform Setting** > **Global Setting** > **Advanced** > **Host** and set **Host CPU Utilization Collection Interval**

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

  > **Note:**
  >
  > - The Cloud collects the host memory loads over a period of time, calculates the memory average utilization during this period, and then selects the host with the lowest memory utilization to create VM instances.
  >
  > - By default, the Cloud collects data at an interval of 10 minutes. You can change the collection cycle by using the following method:
  >
  >   Choose **Settings** > **Platform Setting** > **Global Setting** > **Advanced** > **Host** and set **Host Memory Utilization Collection Interval**.

  — **Host with max. running VMs**: Allocates the host with the maximum number of running VM instances to create VM instances. Before you can use this option, set the maximum number of VM instances that can run on a host. Then, the Cloud selects the host that meets

the requirements to create VM instances. If no host is available, you will fail to create a VM instance.

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

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

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

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

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

• **Total Speed**:

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

• **Read/Write Speed**:

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

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

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

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

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

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

> 📋 **Note:**

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

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

  Sample:

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

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

1. Set the primary storage for root volumes.

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

- `type`: Enter a primary storage type. Valid values: Ceph, LocalStorage, NFS, and
  SharedBlock. If you specify a Ceph primary storage, you can specify a Ceph pool.

- `uuid`: Enter the UUID of a primary storage.

- **poolNames**: Enter the name of a Ceph pool. Delete this parameter if you do not specify a Ceph primary storage.

> 📋 **Note:**
>
> If you do not specify a primary storage, delete the preceding parameter settings.

2. Set the billing type of a root volume.

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

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

> 📋 **Note:**
>
> If you do not need billing settings, delete the preceding parameter settings.

3. Set the display type of a root volume.

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

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

> 📋 **Note:**
>
> If you do not need special display, delete the preceding parameter settings.

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

4.1.7 Add an Image

Context

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

Figure 4-11: Add Image

On the displayed page, set the following parameters:

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

- **Description**: Optional. Enter a description for the image.

- **Image Format**: Select an image format. You can select qcow2, iso, or raw based on the image file property.

- **Platform**: Select an image platform type. Valid values: Linux, Windows, WindowsVirtio, Other, and Paravirtualization.

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

- **Image Path**: Specify an image URL or upload a local file:

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

    ■ A URL that starts with *http* or *https*:

- Syntax: *http://host[:port]/path/file* or *https://host[:port]/path/file*.
  - Example: *http://cdn.zstack.io/product_downloads/images/zstack-image.qcow2*
- A URL that starts with *ftp*:
  - Syntax that does not specifies the user: *ftp://hostname[:port]/path/file*.
    Example: *ftp://172.20.0.10/pub/zstack-image.qcow2*.
  - Syntax that specifies the user: *ftp://user:password@hostname[:port]/path/file*.
    Example: *ftp://zstack:password@172.20.0.10/pub/zstack-image.qcow2*.
- A URL that starts with *sftp*:
  - Syntax that specifies the user identity: *sftp://user:password@hostname[:port]/path/file*.
    Example: *sftp://root:password@172.20.0.10/pub/zstack-image.qcow2*.
  - User-identity-free syntax: *sftp://user@hostname[:port]/path/file*.
    Example: *sftp://root@172.20.0.10/pub/zstack-image.qcow2*.
- The absolute path of an image file that is stored on a backup storage. The backup storage that stores the image file can be an ImageStore backup storage.

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

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

- If you specify a URL with the `file:///` syntax to add an image:

  — Ceph backup storage does not support the *file:///* syntax.

  — The three forward slashes (*/*) in `file:///` represents the absolute path of a file on a backup storage. For example, if you specify the URL `file:///opt/zstack-dvd/image-1.4.qcow2`, you add the image file named *image-1.4.qcow2* in the `/opt/zstack-dvd` path of a backup storage to the Cloud.

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

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

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

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

> **Note:**
>
> Mode mismatch may cause VM instances unable to work as expected. Select a mode based on your business needs:
>
> - If you add an image in qcow2 or raw format, select the mode consistent with the mode used when the image was created.
> - If you add an image in iso format, you can select either of the two modes. OS will be boot based on the selected mode.
> - If you want to boot the OS of a VM instance in UEFI mode, we recommend that you select a VM image that is created from one of the OS listed in the following table.

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

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

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

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

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

  ▬ Manually exit the UEFI Shell.

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

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

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

  Figure 4-12: Press Any Key to Continue

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

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

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

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

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

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

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

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

4.1.8 Create an L2 Network

Context

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

Figure 4-13: Create L2 Network

On the displayed page, set the following parameters:

- **Name**: Enter a name for the L2 network.

- **Description**: Optional. Enter a description for the L2 network.

- **Type**: Valid values: L2NoVlanNetwork and L2VlanNetwork.

  — L2NoVlanNetwork

    ■ If you do not need to use VLAN, select L2NoVlanNetwork.

    ■ If you specify L2NoVlanNetwork, the switch port connected by the specified NIC must be in Access mode.

    ■ **NIC Name**: Enter the NIC name of the corresponding host.

  — L2VlanNetwork

    ■ If you need to use VLAN on ZStack Cloud, select L2VlanNetwork.

    ■ If you specify L2NoVlanNetwork, the switch port connected by the specified NIC must be in Access mode.

    ■ **VLAN ID**: Specify a VLAN ID that matches the actual network configurations. Valid values: 1 to 4094.

    ■ **NIC Name**: Enter the NIC name of the corresponding host.

- **vSwitch Type**: The vSwitch type of the L2 network, including Linux Bridge and OVS-DPDK. Default: Linux Bridge.

- **NIC Name**: Enter a NIC name for the L2 network. For example, em01.

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

4.1.9 Create an L3 Network

Context

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

Figure 4-14: Create L3 Network

On the displayed page, set the following parameters:

- **Name**: Enter a name for the L3 network.

- **Description**: Optional. Enter a description for the L3 network.

- **Network Type**: The wizard supports only flat network.

- **Network Range Method**: Select a method to add a network range for the L3 network. You can select IP Range or CIDR.

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

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

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

- **Netmask**: Set a netmask for the network range, for example, *255.255.0.0*.

- **Gateway**: Set a gateway for the network range, for example, *172.20.0.1*.

- **DNS**: Add a DNS server to provide domain name resolution services for the L3 network. You can specify *223.5.5.5*, *8.8.8.8*, or *114.114.114.114*.

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

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

- **Gateway**: Set a gateway for the L3 network, for example, *192.168.108.1*.

> **Note:**
>
> - You can use the first or last IP address in the specified CIDR block as the gateway.
>
> - If left blank, the first IP address in the specified CIDR block is used as the gateway.

- **DNS**: Add a DNS server to provide domain name resolution services for the L3 network. You can specify *223.5.5.5*, *8.8.8.8*, or *114.114.114.114*.

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

What's next

The wizard is complete.

4.2 Create a VM Instance

Context

After you complete the initialization of ZStack Cloud, you can create a VM instance.

Procedure

1. Create a VM instance.

   On the main menu of ZStack Cloud, choose **Resource Center** > **Resource Pool** > **Virtual Resource** > **VM Instance**. Click the **Fast Creation** button on the right of **Create VM Instance**. Then, the **Fast Creation** page is displayed. On the **Fast Creation** tab page, set the following parameters:

   - **Name**: Enter a name for the VM instance. Note that the VM name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).

- **Quantity**: Enter the number of VM instances to be created. Valid values: 1 to 100. You can change the maximum number by modifying the value of **Maximum VM Creation in Batch on UI** in the global setting.

- **Tag**: Optional. Bind one or more tags to the VM instance as needed.

- Set the VM offering by using one of the following methods:

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

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

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

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

Figure 4-15: Create VM Instance (Fast Creation)

2. Verify the VM instance.

After the VM instance is created, you can go to the console of the VM instance.

Figure 4-16: Open VM Console

What's next

You have completed the quick installation and usage of ZStack Cloud of the c76 edition. For more detailed information, see *User Guide*.

Glossary

VM Instance

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

Volume

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

Root Volume

A root volume provides support for the system operations of a VM instance.

Data Volume

A data volume provides extended storage space for a VM instance.

Image

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

Instance Offering

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

Disk Offering

A disk offering defines the capacity and other configuration settings of volumes.

GPU Specification

A GPU specification defines the frame per second (FPS), video memory, resolution, and other configuration settings of a physical or virtual GPU. GPU specifications are categorized into physical GPU specifications and virtual GPU specifications.

Auto-Scaling Group

An auto-scaling group is a group of VM instances that are used for the same scenarios. An auto-scaling group can automatically scale out or in based on application workloads or health status of VM instances in the group.

Snapshot

A snapshot is a point-in-time capture of data status in a volume.

Affinity Group

An affinity group is an orchestration policy for IaaS resources to ensure the high performance and high availability of businesses...

Zone

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

Cluster

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

Host

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

Primary Storage

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

Backup Storage

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

iSCSI Storage

iSCSI storage is an SAN storage that uses the iSCSI protocol for data transmission. You can add an iSCSI SAN block as a Shared Block primary storage or pass through the block to a VM instance.

FC Storage

FC storage is an SAN storage that uses the FC technology for data transmission. You can add an FC SAN block as a Shared Block primary storage or pass through the block to a VM instance.

L2 Network

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

VXLAN Pool

A VXLAN pool is a collection of VXLAN networks established based on VXLAN Tunnel Endpoints (VTEPs). The VNI of each VXLAN network in a VXLAN pool must be unique.

L3 Network

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

Public Network

Generally, a public network is a logical network that is connected to the Internet. However, in an environment that has no access to the Internet, you can also create a public network.

Flat Network

A flat network is connected to the network where the host is located and has direct access to the Internet. VM instances in a flat network can access public networks by using elastic IP addresses.

VPC Network

A VPC network is a private network where VM instances can be created. A VM instance in a VPC network can access the Internet through a VPC vRouter.

Management Network

A management network is used to manage physical resources in the Cloud. For example, you can create a management network to manage access to hosts, primary storages, backup storages, and VPC vRouters.

Flow Network

A flow network is a dedicated network for port mirror transmission. You can use a flow network to transmit the mirrors of data packets of NIC ports to the target ports.

VPC vRouter

A VPC vRouter is a dedicated VM instance that provides multiple network services.

VPC vRouter HA Group

A VPC vRouter HA group consists of two VPC vRouters. Either VPC vRouter can be a primary or secondary VPC vRouter for the group. If the primary VPC vRouter does not work as expected, the VPC vRouter becomes the secondary VPC vRouter in the group to ensure high availability of business.

vRouter Image

A vRouter image encapsulates network services and can be used to create VPC vRouters and load balancers. vRouter images can be categorized into VPC vRouter images and load balancer (LB) images.

Dedicated-Performance LB Image

A dedicated-performance load balancer (LB) image encapsulates dedicated-performance load -balancing services and can be used to create load balancer instances. However, a dedicated-performance load balancer image cannot be used to create VM instances.

vRouter Offering

A vRouter offering defines the number of vCPU cores, memory size, image, management network , and public network configuration settings of VPC vRouters. You can use a vRouter offering to create VPC vRouters that can provide network services for public networks and VPC networks.

LB Instance Offering

A load balancer (LB) instance offering defines the CPU, memory, image, and management network configuration settings used to create LB instances. LB instances provide load balancing services for the public network, flat network, and VPC network.

SDN Controller

An SDN controller is used to control network devices such as switches. You can add an external SDN controller to the Cloud and use the controller to control external switches and other network devices.

Security Group

A security group provides security control services for VM instances on the L3 network. It filters the ingress or egress TCP, UDP, and ICMP packets of specified VM instances in specified networks based on the specified security rules.

VIP

In bridged network environments, a virtual IP address (VIP) provides network services such as serving as an elastic IP address (EIP), port forwarding, load balancing, IPsec tunneling. When a VIP provides the preceding network services, packets are sent to the VIP and then routed to the destination network where VM instances are located.

EIP

An elastic IP address (EIP) functions based on the NAT technology. IP addresses in a private network are translated into an EIP that is in another network. This way, private networks can be accessed from other networks by using EIPs.

Port Forwarding

Port forwarding functions based on the layer-3 forwarding service of VPC vRouters. This service forwards traffic flows of the specified IP addresses and ports in a public network to specified ports of VM instances by using the specified protocol. If your public IP addresses are insufficient, you can configure port forwarding for multiple VM instances by using one public IP address and port.

Load Balancer

A load balancer distributes traffic flows of a virtual IP address to backend servers. It automatically inspects the availability of backend servers and isolates unavailable servers during traffic distribution. This way, the load balancer improves the availability and service capability of your business.

Listener

A listener monitors the frontend requests of a load balancer and distributes the requests to a backend server based on the specified policy. In addition, the listener performs health checks on backend servers.

Forwarding Rule

A forwarding rule forwards the requests from different domain names or URLs to different backend server groups.

Backend Server Group

A backend server group is a group of backend servers that handles requests distributed by load balancers. It is the basic unit for traffic distribution by load balancer instances.

Backend Server

A backend server handles requests distributed by a load balancer. You can add a VM instance on the Cloud or a server on a third-party cloud as a backend server.

Frontend Network

A frontend network is a type of network that is associated with a load balancer. Requests from the network are distributed by the load balancer to backend servers based on a specified policy.

Backend Network

A backend network is a type of network that is associated with a load balancer. Requests from frontend networks are distributed by the load balancer to servers in the backend network.

Load Balancer Instance

A load balancer instance is a custom VM instance used to provide load balancing services.

Certificate

If you select HTTPS for a listener, associate it with a certificate to make the listener take effect. You can upload either a certificate or certificate chain.

Firewall

A firewall is an access control policy that monitors ingress and egress traffic of VPC vRouters and decides whether to allow or block specific traffic based on a defined set of security rules.

IPsec Tunnel

An IPSec tunnel encrypts and verifies IP packets that transmit over a virtual private network (VPN) from one site to another.

OSPF Area

An OSPF area is split from an autonomous system based on the OSPF protocol. This splitting simplifies the management of vRouters.

NetFlow

An NetFlow monitors the ingress and egress traffic of the NICs of VPC vRouters. The supported versions of data flows are V5 and V9.

Port Mirroring

Port mirroring mirrors the traffic data of VM NICs and sends the traffic data to the target ports. This allows for the analysis of data packets of ports and simplifies the monitoring and management of data traffic and makes it easier to locate network errors and exceptions.

Route Table

A route table contains information about various routes that you configure. Route entries in a route table must include the destination network, next hop, and route priority.

CloudFormation

CloudFormation is a service that simplifies the management of cloud resources and automates deployment and O&S. You can create a stack template to configure cloud resources and their dependencies. This way, resources can be automatically configured and deployed in batches. CloudFormation provides easy management of the lifecycle of cloud resources and integrates automatic O&S into API and SDK.

Resource Stack

A resource stack is a stack of resources that are configured by using a stack template. The resources in the stack have dependencies with each other. You can manage resources in the stack by managing the resource stack.

Stack Template

A stack template is a UTF8-encoded file based on which you can create resource stacks. The stack template defines the resources that you want, the dependencies between the resources , and the configuration settings of the resources. When you use a stack template to create a resource stack, CloudFormation parses the template and the resources are automatically created and configured.

Sample Template

A sample template is a commonly used resource stack. You can use a sample template provide by the Cloud to create resource stacks.

Designer

A designer is a CloudFormation tool that allows you to orchestrate cloud resources. You can drag and drop resources on a canvas and use lines to establish dependencies between the resources.

Baremetal Cluster

A baremetal cluster consists of baremetal chassis. You can manage baremetal chassis by managing a baremetal cluster where the chassis reside.

Deployment Server

A deployment server is a server that provides PXE service and console proxy service for baremetal chassis.

Baremetal Chassis

A baremetal chassis is used to create a baremetal instance and is identified based on the BMC interface and IPMI configuration setting.

Preconfigured Template

A preconfigured template is used to create a preconfigured file that allows for unattended batch installation of an operating system for baremetal instances.

Baremetal Instance

A baremetal instance is an instantiated baremetal chassis.

Elastic Baremetal Management

Elastic Baremetal Management provides dedicated physical servers for your applications to ensure high performance and stability. In addition, this feature allows elastic scaling. You can apply for and scale resources based on your needs.

Provision Network

A provision network is a dedicated network for PXE boot and image downloads while creating elastic baremetal instances.

Elastic Baremetal Cluster

An elastic baremetal cluster consists of elastic baremetal instances. You can manage elastic baremetal instances by managing an elastic baremetal cluster where the instances reside.

Gateway Node

A gateway node is a node where the ingress and egress traffic of the Cloud and elastic baremetal instances is forwarded.

Baremetal Node

A baremetal node is used to create a baremetal instance and is identified based on the BMC interface and IPMI configuration setting.

Elastic Baremetal Instance

An elastic baremetal instance has the same performance as physical servers and allows elastic scaling. You can apply for and scale resources based on your needs.

Elastic Baremetal Offering

An elastic baremetal offering defines the number of vCPU cores, memory size, CPU architecture, CPU model, and other configuration settings of elastic baremetal instances.

vCenter

The Cloud allows you to take over vCenter and manage resources on the vCenter.

VM Instance

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

Network

A vCenter network defines the network settings of VM instances on vCenter, such as IP range, gateway, DNS, and network services.

Volume

A volume provides storage space for a VM instance on vCenter. A volume attached to a VM instance can be used as a root volume or data volume. A root volume provides support for the system operations of a VM instance. A data volume provides extended storage space for a VM instance.

Image

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

Event Message

Event Message displays event alarm messages of vCenter that is took over by the Cloud. This feature allows you to locate errors and exceptions efficiently.

Network Topology

A network topology visualizes the network architecture of the Cloud. It allows for efficient planning , management, and improvement of network architecture. Network topologies can be categorized into global topologies and custom topologies.

Performance Analysis

Performance Analysis displays the performance metrics of key resources under monitoring in the Cloud. Cloud resources can be externally or internally monitored. You can use either method to monitor the performance of resources in the Cloud and improve O&S efficiency.

Capacity Management

Capacity Management visualizes the capacities and usages of key resources in the Cloud. You can use this feature to improve O&S efficiency.

MN Monitoring

MN monitoring allows you to view the health status of each management node when you use multiple management nodes to achieve high availability.

Alarm

An alarm is used to monitor the status of time-series data and events and respond to the status change. Alarms can be categorized into resource alarm, event alarm, and extended alarm.

One-Click Alarm

A one-click alarm integrates multiple metrics of a resource. You can create one-click alarms for multiple resources to monitor these resources.

Alarm Template

An alarm template is a template of alarm rules. If you associate an alarm template with a resource group, an alarm is created to monitor the resources in the group.

Resource Group

A resource group consists of resources grouped based on your business needs. If you associate an alarm template with a resource group, the alarm rules specified by the template take effect on all the resources in the group.

Message Template

A message template specifies the text template of a resource alarm message or event alarm message sent to an SNS system.

Message Source

A message source is used to take over extended alarm messages. If you configure alarms for message sources, extended alarm messages can be sent to various endpoints.

Endpoint

An endpoint is a method that users obtain subscribed messages. Endpoints are categorized into system endpoints, email, DingTalk, HTTP application, short message service, and Microsoft Teams.

Alarm Message

An alarm message is a message sent the time when an alarm is triggered.

Operation Log

An operation log is a chronological record of operations on the specified objects and their operation results.

Audit

Audit monitors and records all activities on the Cloud. You can use this feature to implement operation tracking, cybersecurity classified protection compliance, security analysis, troubleshooting, and automatic O&M.

Backup Management

Backup management integrates multiple disaster recovery technologies such as incremental backup and full backup that are suitable for multiple business scenarios. You can implement local backup and remote backup based on your business needs.

Backup Job

You can create a backup job to back up local VM instances, volumes, or databases to a specified storage server on a regular basis.

Local Backup Data

Local backup data of VM instances, volumes, and databases is stored in the local backup storage.

Local Backup Storage

A local backup storage is located at the local data center and is used to store local backup data.

Remote Backup Storage

A remote backup storage is located at a remote data center or a public cloud and is used to store remote backup data.

Continuous Data Protection (CDP)

Continuous Data Protection (CDP) provides second-level and fine-grained continuous backups for important business systems in VM instances, allowing users to restore VM data to any time state and retrieve files without restoring the system.

CDP Task

You can create a CDP task to continuously back up your VM data to a specified backup storage to achieve continuous data protection and restoration.

CDP Data

The backup data generated from continuous data protection on VM instances is stored in local backup storages.

Scheduled Job

A scheduled job defines that a specific action be implemented at a specified time based on a scheduler.

Scheduler

A scheduler is used to schedule jobs. It is suitable for business scenarios that last for a long time.

Tag

A tag is used to mark resources. You can use a tag to search for and aggregate resources.

Migration Service

The Cloud provides V2V migration service that allows you to migrate VM instances and data from other virtualized platform to the current cloud platform.

V2V Migration

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

V2V Conversion Host

A V2V conversion host is a host in the destination cluster that you need to specify during V2V migration to cache VM instances and data when you implement V2V migration. After the VM instances and data are cached in the V2Vconversion host, they are migrated to the destination primary storage.

User

A user is a natural person that constructs the most basic unit in business management.

Member Group

A member group is a collection of natural persons or a collection of project members. You can use a member group to grant permissions.

Role

A role is a collection of permissions that can be granted to users. A user that assumes a role can call API operations based on the permissions specified by the role. Roles are categorized into system roles and custom roles.

3rd Party Authentication

The 3rd party authentication feature allows you to integrate third-party authentication systems to the Cloud. Then you can use a third-party account to log in to the Cloud and use the resources in the Cloud. You can add an AD or LDAP server to the Cloud.

Project

A project is a task that needs to be accomplished by specific personnel at a specified time. Resources and budgets are also specified for projects. In business management, you can plan resources at the project granularity and allocate an independent resource pool for a project.

Project Member

A project member is a member in a project who is granted permissions on specific project resources and can use the resources to accomplish tasks. Project members include the project admin, project managers, and normal project members.

Process Management

Process management is part of ticket management that manages the processes related to the resources of projects. Processes can be categorized into default processes and custom processes .

My Approvals

In the Cloud, only the administrator and project administrators are granted approval permissions. the administrator and project administrators can approve or reject a ticket. If a ticket is approved, resources are automatically deployed and allocated to the specified project.

Bills

A bill is the expense of resources totaled at a specified time period. Billing is accurate to the second. Bills can be categorized into project bills, department bills, and account bills.

Pricing List

A pricing list is a list of unit prices of different resources. The unit price of a resource is set based on the specification and usage time of the resource.

Console Proxy

Console proxy allows you to log in to a VM instance by using the IP address of a proxy.

AccessKey Management

An AccessKey pair is a security credential that one party authorizes another party to call API operations and access its resources in the Cloud. AccessKey pairs shall be kept confidential.

IP Blocklist/Allowlist

An IP blocklist or allowlist identifies and filters IP addresses that access the Cloud. You can create an IP allowlist or blocklist to improve access control of the Cloud.

Application Center

Application Center allows you to add third-party applications to the Cloud and then access the applications by using the Cloud. It extends the functionality of the Cloud.

Sub-Account Management

A sub-account is created and managed by the admin. Resources created under a sub-account is managed by the sub-account.

Theme and Appearance

You can customize the theme and appearance of the Cloud.

Email Server

If you select Email as the endpoint of an alarm, you need to set an email server. Then alarm messages are sent to the email server.

Log Server

A log server is used to collect logs of the management node. You can add a log server to the cloud and use the collected logs to locate errors and exceptions. This makes your O&M more efficient.

Global Setting

Global Setting allows you to configure settings that take effect on the whole platform.

Scenario Template

Scenario Template provides multiple templates that encapsulate scenario-based global settings . You can apply a template globally with one click based on your business needs. This improves your O&M efficiency.