ZStack ZSphere

Installation and Upgrade Tutorial

Version: ZStack ZSphere 4.10.25

Issue: V4.10.25

Shanghai Yunzhou Technology Co.,Ltd.

Copyright Statement

Trademark

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

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

Notice

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

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

Contents

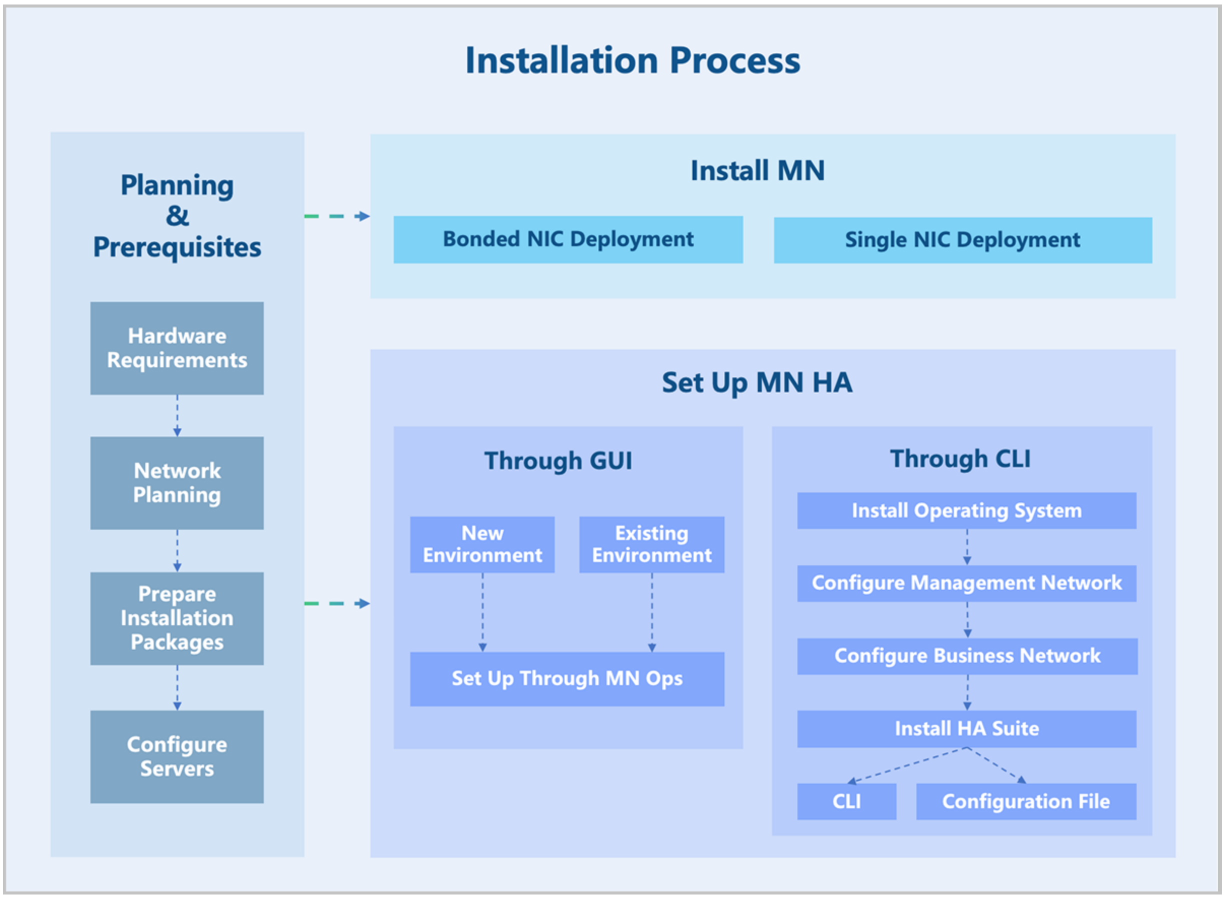
1 ZStack ZSphere Installation

1.1 Introduction

About This Tutorial

This chapter describes how to install ZStack ZSphere management node and how to set up management node HA.

Figure 1-1: Installation Process



Intended Audience

This chapter is intended for experienced administrators who want to install ZStack ZSphere.

Installation Modes

ZStack ZSphere provides three installation modes. Each includes different components and is intended for different scenarios.

Installation Mode	Component	Scenario
Management Node Mode	• Base operating system • Dependencies such as `MariaDB` and `CloudBus` message bus	Suitable for installing the management node.
Compute Node Mode	• Base operating system • Virtualization components such as `libvirt` and `QEMU`	Suitable for installation as nodes other than the management node, for example: • Compute nodes • Standalone image storage, distributed image storage, and monitoring nodes of distributed image storage • Distributed storage nodes and monitoring nodes of distributed storage
Expert Mode	Base operating system	

1.2 Planning and Prerequisites

1.2.1 Hardware Requirements

The server configuration, including CPU, memory, storage capacity and NIC performance, determines the business capacity of ZStack ZSphere.

- For demonstration environment: The server must have at least 4 CPU cores and 8 GB of memory.
- For production environment:
  - Management node configuration: For small-scale scenarios, the server must have at least 8 CPU cores, 16 GB of memory, and 240 GB of storage.

    The actual hardware configuration requirements depend on your business scale. For details , contact official technical support.
  - Compute node configuration: The actual hardware configuration requirements depend on your business scale. For details, contact official technical support.

Recommended Hardware Configuration

The following table shows the recommended hardware configuration for servers in both demonstration and production environments.

Device		Configuration
Server	CPU	• x86 architecture: 64-bit. Supports Intel VT-x or AMD-V hardware virtualization features (such as Intel VMX or AMD/Hygon SVM). • ARM architecture: 64-bit. Supports hardware virtualization features.
	Memory	No special requirements. DDR4 or higher specification memory is recommended.
	Motherboard	Standard dual-socket server motherboard.
	RAID Controller	Supports SAS/SATA RAID 0/1/10 and passthrough mode.
	Disk	No special requirements. Select HDD or SSD based on capacity and performance requirements.
	Network Ports	• Management port: 1 × 1 GbE RJ45 • Business port: 1 × 10 GbE SFP+
Network Switch		• At least one 1 GbE switch. 10 GbE switch is recommended. • Multiple Category 5 or higher network cables.

Hardware Planning

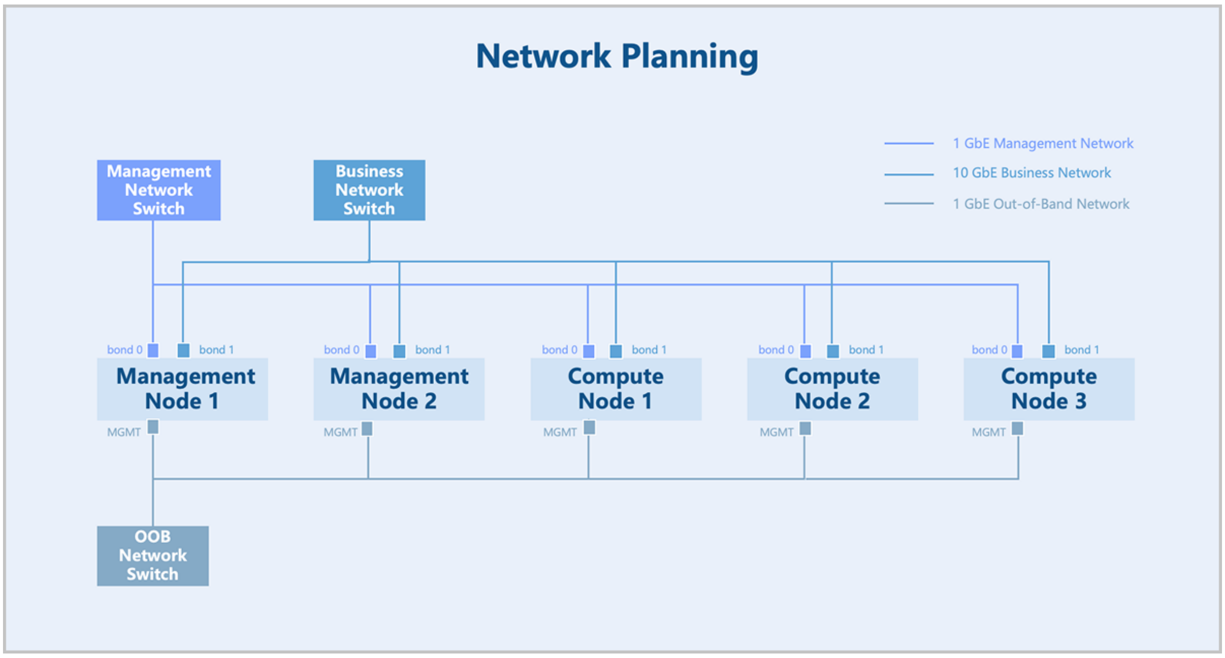
You need to plan your server resources according to your production needs. In a large data center with sufficient resources, we recommend deploying two servers as management nodes to control the entire virtualization platform. These two management nodes provide high availability. If one management node fails, the system automatically triggers a high availability switchover within seconds. This ensures the management service remains continuously available. In a small data center, you can use a single server as the management node.

The remaining servers act as compute nodes. In a large data center, you can select multiple compute nodes to act as image storage. This expands the total image storage capacity and improves throughput. In a small data center, the image storage can share a server with the management node.

1.2.2 Network Planning

Figure 1-2: Network Planning shows a typical data center that consists of several servers with different functions and two independent network environments.

Figure 1-2: Network Planning



- The management network uses dual Gigabit networks for managing hardware resources related to the virtualization platform. The business network uses dual 10-Gigabit networks for virtual machine service traffic. You can configure network speeds based on your actual business requirements.
- If you use network storage such as NFS or distributed storage, you need also plan an additional storage network to handle storage traffic.
- We recommend that you maintain consistent NIC naming across all servers and use NICs with the same name to carry the same type of network traffic. For example, all management network traffic use the `em1` NICs.
- If you use a VLAN network, you need to configure the corresponding VLAN network communication on the switch in advance.
- ZStack ZSphere automatically assigns IP addresses to virtual machines. You need to reserve an IP range that does not conflict with the system and ensure this range does not conflict with any existing DHCP services in your network environment.

1.2.3 Prepare Installation Packages

ZStack ZSphere ISO is built on Helix, a self-made virtualization kernel software that operates between the infrastructure layer and the upper-layer operating systems. It integrates essential components like hardware drivers, macro kernels, and virtual agents, shielding the differences among heterogeneous hardware. This releases operating systems from hardware driver dependencies, ensuring proper access to the heterogeneous hardware on the under layer. By doing so, Helix enhances hardware compatibility, high reliability, high availability, scalability, and performance of your virtual environment.

You can install ZStack ZSphere without connecting to the public network or configuring a yum source, allowing for a completely offline installation.

The following table shows the software packages used for installing ZStack ZSphere.

Sever Architecture	Package Name
x86	ZStack-ZSphere-x86_64-DVD-4.10.25-H84r.iso
	ZStack-ZSphere-x86_64-DVD-4.10.25-KylinV10SP3.iso
ARM	ZStack-ZSphere-aarch64-DVD-4.10.25-H22e.iso
	ZStack-ZSphere-aarch64-DVD-4.10.25-KylinV10SP3.iso

Note:

After obtaining the software package, use an MD5 checksum tool to verify the checksum and ensure the software is complete and intact.

1.2.3.1 Burn ISO Image Using Rufus

After you obtain the ISO package, you can use Rufus to burn the ISO image to a USB drive.

Procedure

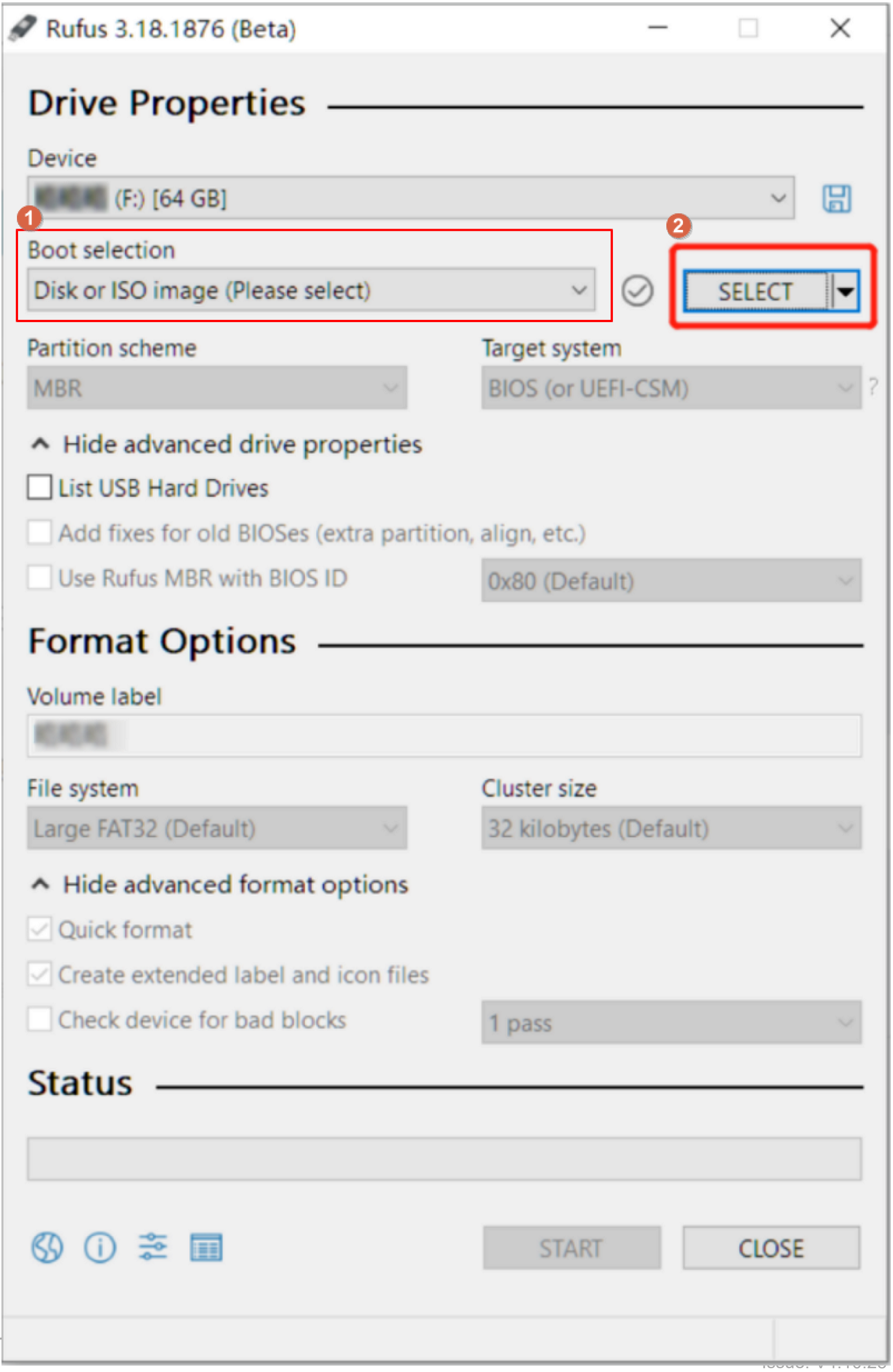
1. Select an ISO image.

   a) Connect your USB drive and open Rufus.

   b) In the **Boot Selection** drop-down list, choose **Disk or ISO image**.

   c) Click **SELECT** to open the ISO image file that you obtained.

Figure 1-3: Select ISO Image



Drive Properties

Device

[redacted] (F:) [64 GB]

Boot selection

Disk or ISO image (Please select)

Partition scheme: MBR

Target system: BIOS (or UEFI-CSM)

□ List USB Hard Drives

□ Add fixes for old BIOSes (extra partition, align, etc.)

□ Use Rufus MBR with BIOS ID: 0x80 (Default)

Format Options

Volume label

[redacted]

File system: Large FAT32 (Default)

Cluster size: 32 kilobytes (Default)

☑ Quick format

☑ Create extended label and icon files

□ Check device for bad blocks: 1 pass

Status

2. Burn the image.

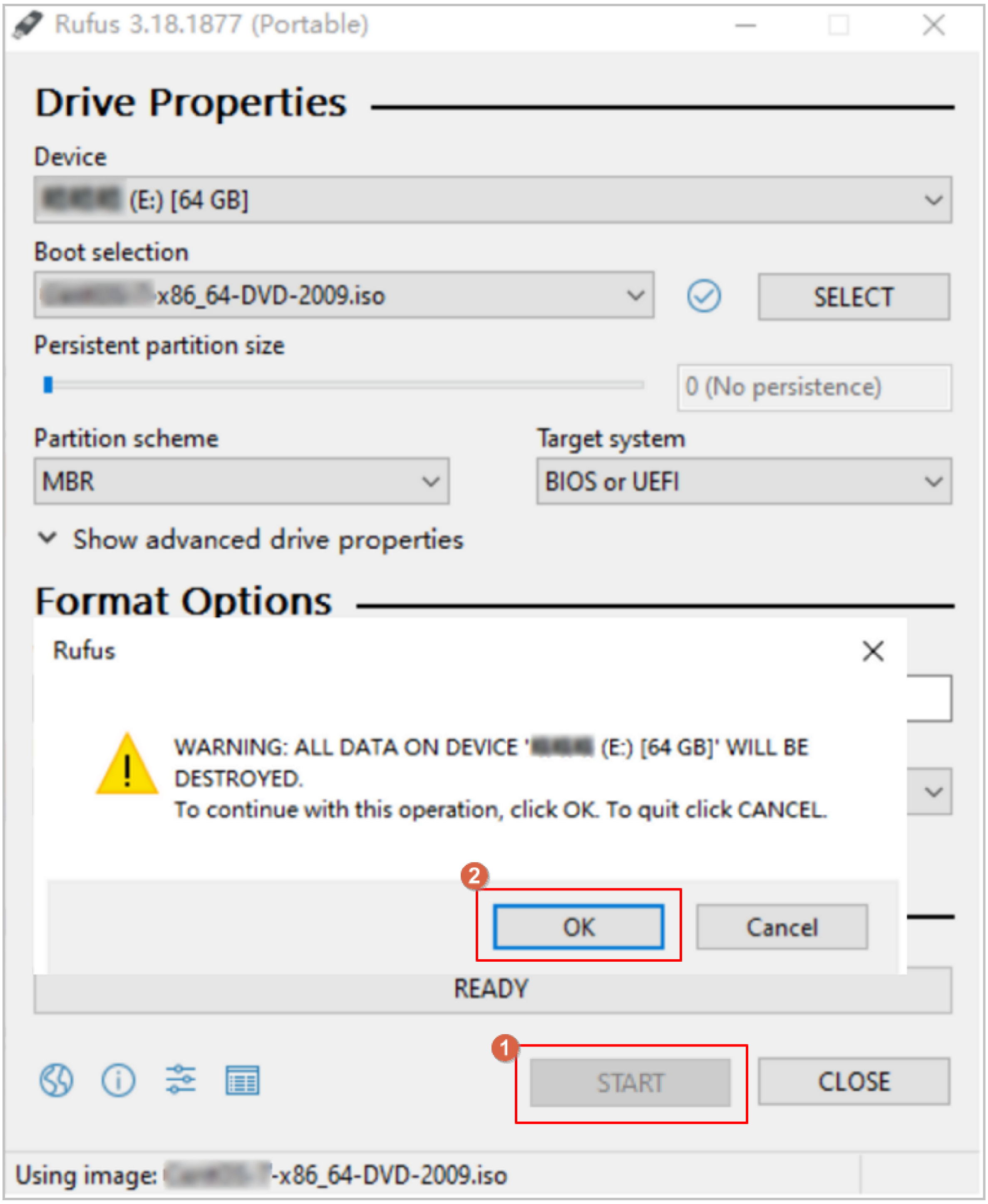
   a) After selecting the ISO image, keep the other options at their default settings and click **START**.

   b) Confirm the warning message.

   > **Note:**
   >
   > Burning the image will format the data on the USB drive. If you have important data on your USB drive, make sure to back it up before formatting.

   c) Click **OK**, and Rufus will burn the ISO image to the USB drive.

Figure 1-4: Burn the Image



Rufus 3.18.1877 (Portable)

Drive Properties

Device: [redacted] (E:) [64 GB]

Boot selection: [redacted]x86_64-DVD-2009.iso

Persistent partition size: 0 (No persistence)

Partition scheme: MBR

Target system: BIOS or UEFI

Show advanced drive properties

Format Options

Rufus

WARNING: ALL DATA ON DEVICE '[redacted] (E:) [64 GB]' WILL BE DESTROYED.
To continue with this operation, click OK. To quit click CANCEL.

READY

Using image: [redacted]-x86_64-DVD-2009.iso

What to do next

After the burning process completes, you can use the USB drive as a boot disk. ZStack-ZSphere supports booting in Legacy mode or UEFI mode.

1.2.3.2 Burn ISO Image Using Fedora Media Writer

After you obtain the ISO package, if you are using the Kylin operating system, we recommend using Fedora Media Writer to burn the ISO image.

Procedure

1. Select an ISO image.
   1. a) Connect your USB drive and open Fedora Media Writer.
   2. b) Click **Custom Image** to open the ISO image file that you obtained.
2. Burn the image.
   1. a) After selecting the ISO image, keep the other options at their default settings and click **Write Disk**.

> **Note:**
>
> Burning the image will format the data on the USB drive. If you have important data on your USB drive, make sure to back it up before formatting.

What to do next

After the burning process completes, you can use the USB drive as a boot disk. ZStack-ZSphere supports booting in Legacy mode or UEFI mode.

1.2.4 Configure Servers

Based on your actual network planning, you need to rack, cable, and power on the servers and network equipment. Then, start the servers and enter BIOS to verify the following:

- The installation process overwrites all data, so confirm that you have backed up all disks in the servers.
- Enter the server BIOS and enable CPU VT and Hyper-Threading (HT) options.
- Configure the appropriate RAID level in the RAID controller to provide data redundancy.
- Set the USB drive as the first boot device.

For information about how to change server configurations, refer to your hardware vendor documentation.

1.3 Install ZStack ZSphere

1.3.1 Install Management Node

1.3.1.1 Bonded NIC Deployment

To meet the requirements for network port bandwidth capacity and high reliability, NIC bonding must be configured in production environments. Since the operating system installation process is identical for both x86 and ARM servers, this chapter uses x86 servers to introduce the detailed installation procedure.

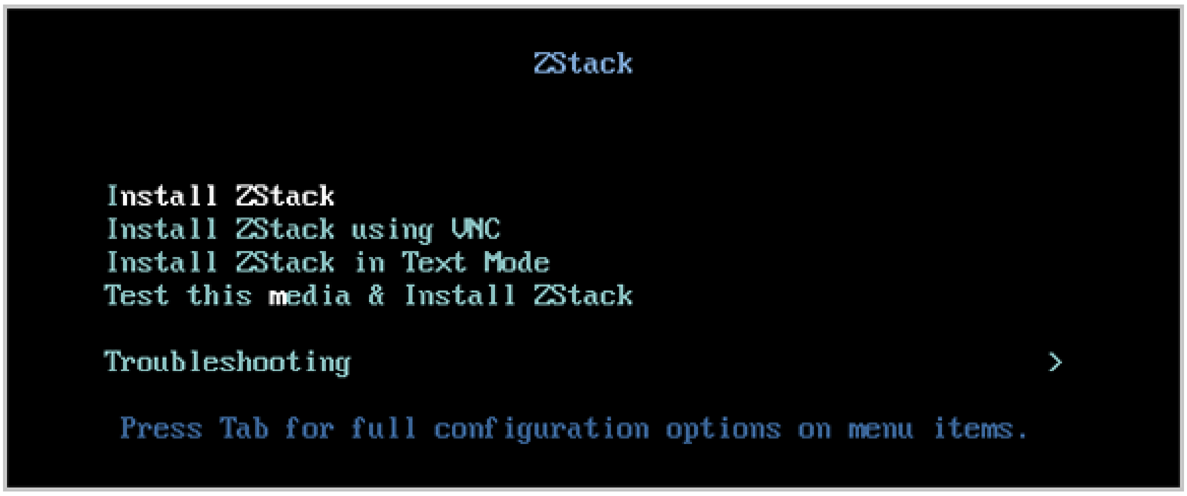
Procedure

1. Select the boot option.

   Enter the ISO boot interface and choose the default option to start the operating system installation. You can select based on your actual situation, but we recommend using the graphical user interface (GUI) for installation. If the server does not have a VGA port and only supports serial connections, you can use either VNC or text mode installation methods.

   - GUI method
   - VNC method
   - Text mode method

   Figure 1-5: System Boot



```
ZStack

Install ZStack
Install ZStack using VNC
Install ZStack in Text Mode
Test this media & Install ZStack

Troubleshooting                                  >

Press Tab for full configuration options on menu items.
```

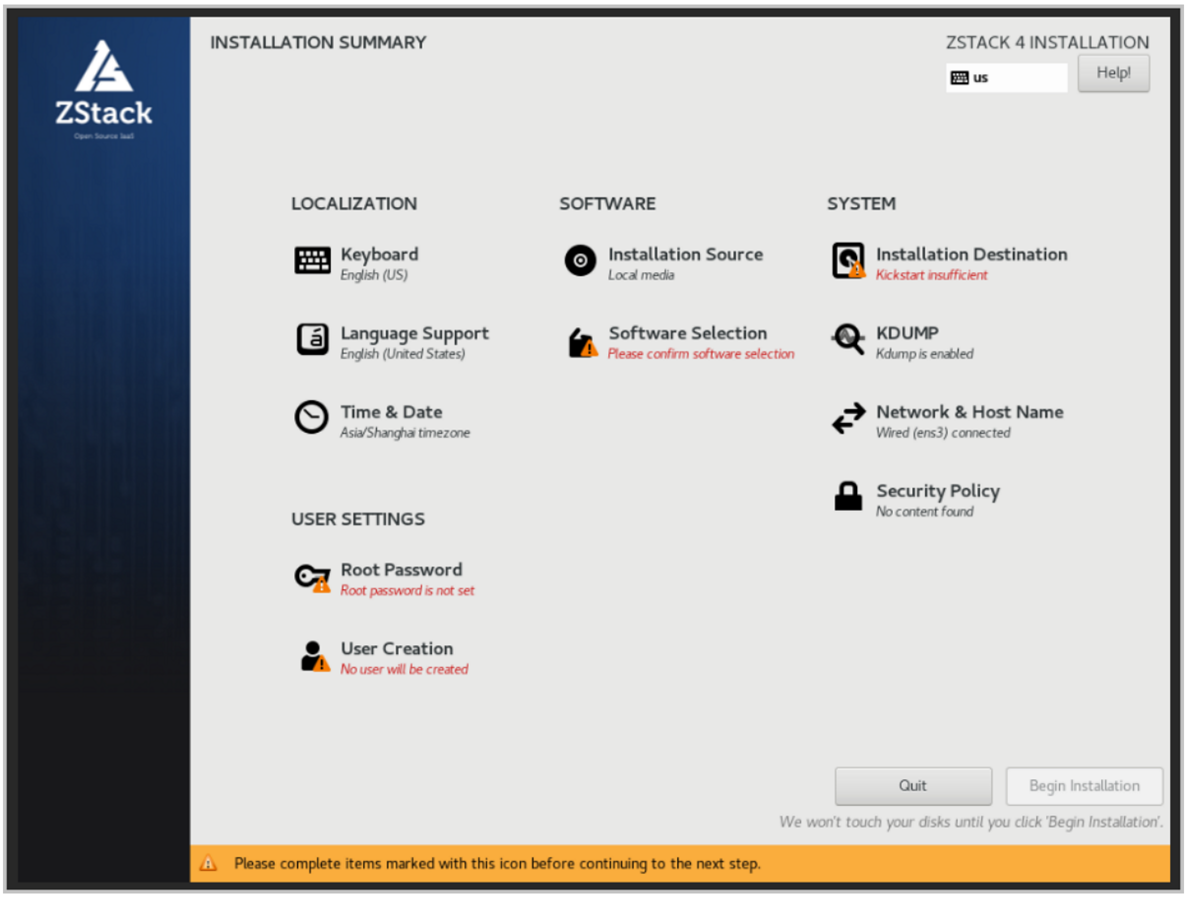
2. Review the installation configuration summary.

   This page displays the system installation configuration. You can modify the configuration as needed. By default, ZStack ZSphere is configured with the following settings:

   - **Keyboard**: English (US)

- **Language Support**: English (United States)
- **Time & Date**: Asia/Shanghai (UTC+8). We recommend that you check the host's time in advance and configure it to the current time and time zone.

Figure 1-6: System Installation Interface



Keyboard: English (US)

Language Support: English (United States)

Time & Date: Asia/Shanghai timezone

Installation Source: Local media

Software Selection: Please confirm software selection

Installation Destination: Kickstart insufficient

KDUMP: Kdump is enabled

Network & Host Name: Wired (ens3) connected

Security Policy: No content found

Root Password: Root password is not set

User Creation: No user will be created

We won't touch your disks until you click 'Begin Installation'.

⚠ Please complete items marked with this icon before continuing to the next step.

3. Select the installation mode.

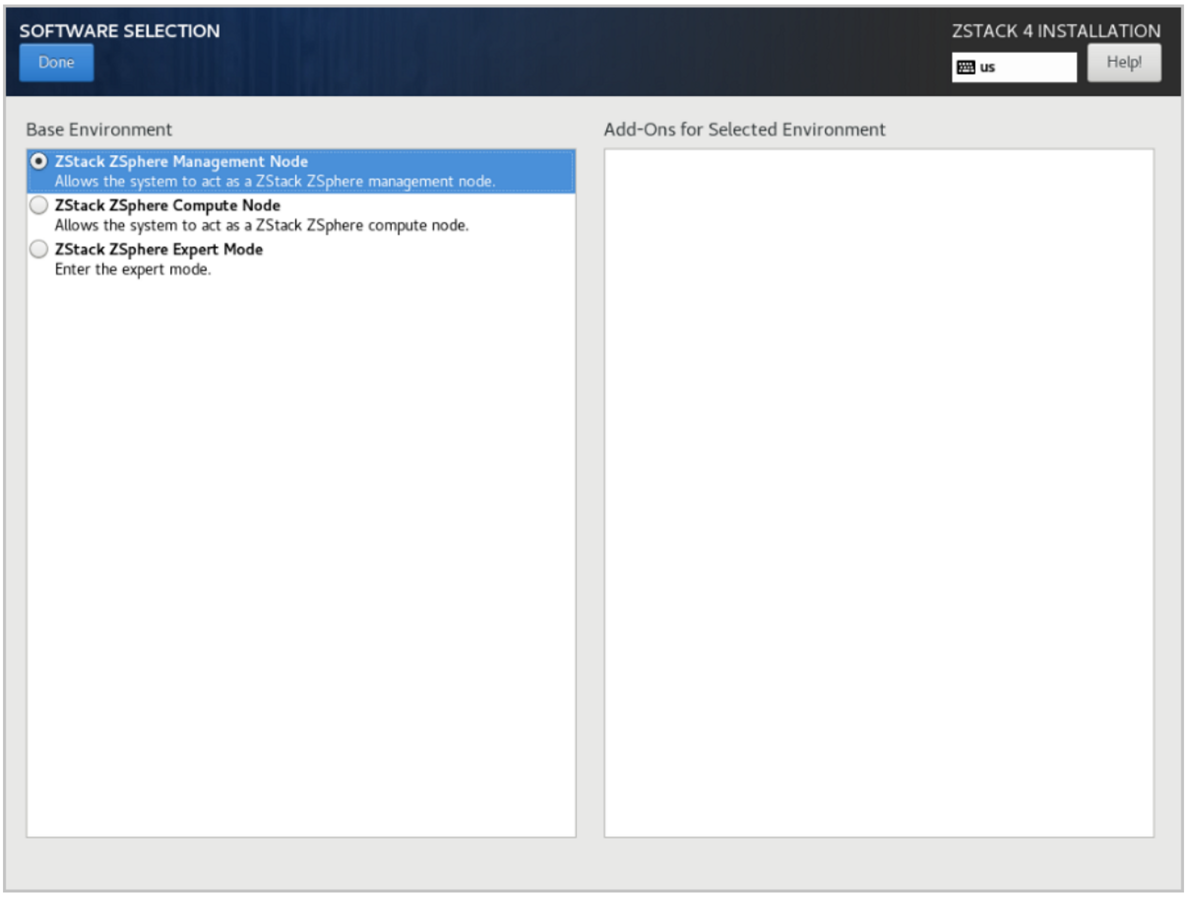
   a) On the **INSTALLATION SUMMARY** page, click **Software Selection**.

   b) On the **SOFTWARE SELECTION** page, choose the installation mode.

      Set the servers for management nodes to **ZStack ZSphere Management Node** mode. Set the other servers to **ZStack ZSphere Compute Node** mode.

   c) After selecting the installation mode, click **Done**.

Figure 1-7: Select Installation Mode



● ZStack ZSphere Management Node
Allows the system to act as a ZStack ZSphere management node.

○ ZStack ZSphere Compute Node
Allows the system to act as a ZStack ZSphere compute node.

○ ZStack ZSphere Expert Mode
Enter the expert mode.

4. Configure the disk partitions.

a) On the **INSTALLATION SUMMARY** page, click **Installation Destination** to enter the **INSTALLATION DESTINATION** page.

b) For **Device Selection**, we recommend that you only configure the system disk. After the system is installed, you can configure other disks.

c) For **Storage Configuration**, we recommend selecting **Automatic** to automatically configure the disk partitions.

If you need to manually configure disk partitions, refer to the following guidelines based on the BIOS boot mode:

- UEFI Mode:
  - `/boot`: This directory stores the core files needed for Linux boot. We recommend allocating 1 GB of space.
  - `/boot/efi`: This directory stores the UEFI boot files. We recommend allocating 500 MB.

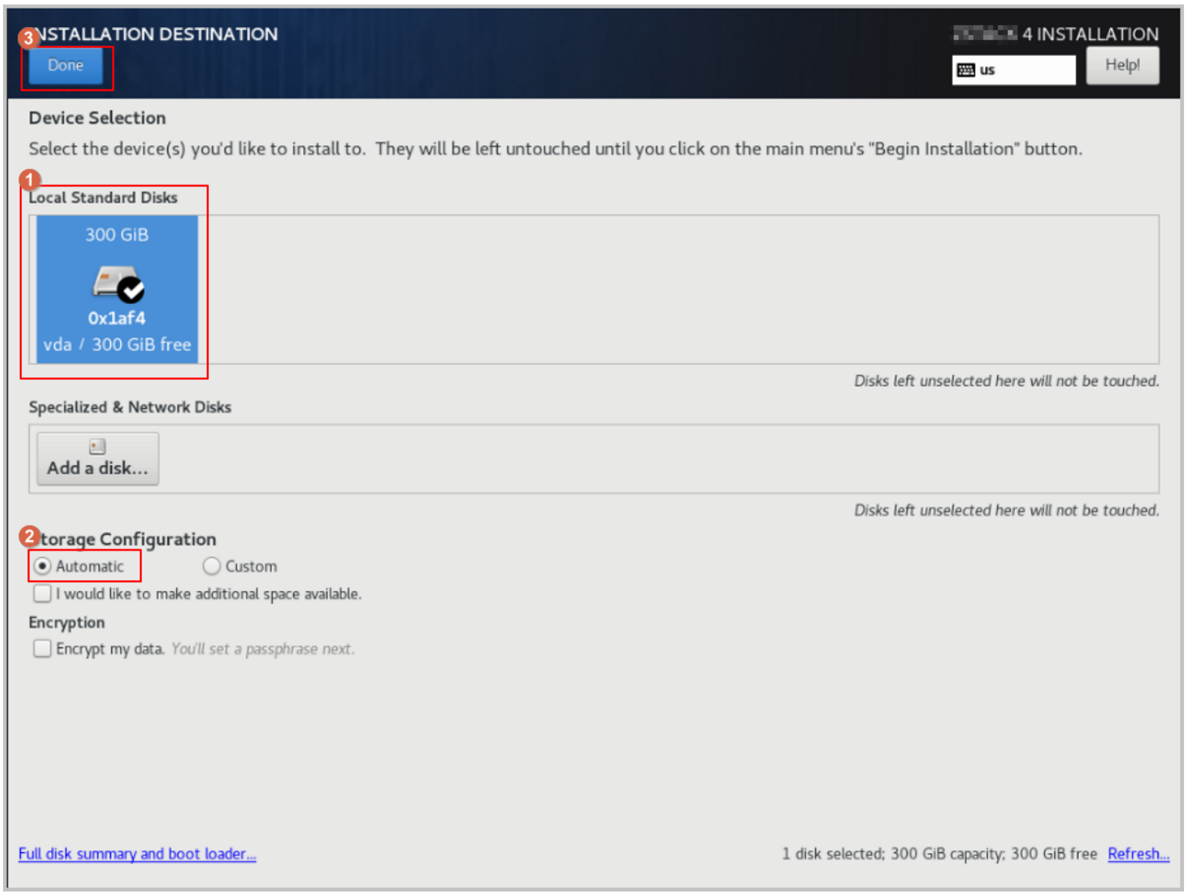
  - `swap`: This is the swap area. We recommend allocating 32 GB.
  - `/`: This is the root directory for the Linux system. We recommend allocating all remaining space.
- Legacy Mode:
  - `/boot`: This directory stores the core files needed for Linux boot. We recommend allocating 1 GB of space.
  - `swap`: This is the swap area. We recommend allocating 32 GB.
  - `/`: This is the root directory for the Linux system. We recommend allocating all remaining space.

Note:

- The above values represent the recommended partition sizes for ZStack ZSphere (total disk capacity should be greater than 300 GB).
- In Legacy mode, if the system disk capacity exceeds 2 TB, you need to configure a BIOS boot partition to support GPT partitioning. UEFI mode does not have this limitation and supports GPT partitioning.

d) Review the configuration and click **Done**.

Figure 1-8: Configure Disk Partitions



INSTALLATION DESTINATION

Done

[redacted] 4 INSTALLATION

us

Help!

Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

300 GiB

0x1af4

vda / 300 GiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

Add a disk...

Disks left unselected here will not be touched.

Storage Configuration

● Automatic ○ Custom

□ I would like to make additional space available.

Encryption

□ Encrypt my data. *You'll set a passphrase next.*

Full disk summary and boot loader...

1 disk selected; 300 GiB capacity; 300 GiB free Refresh...

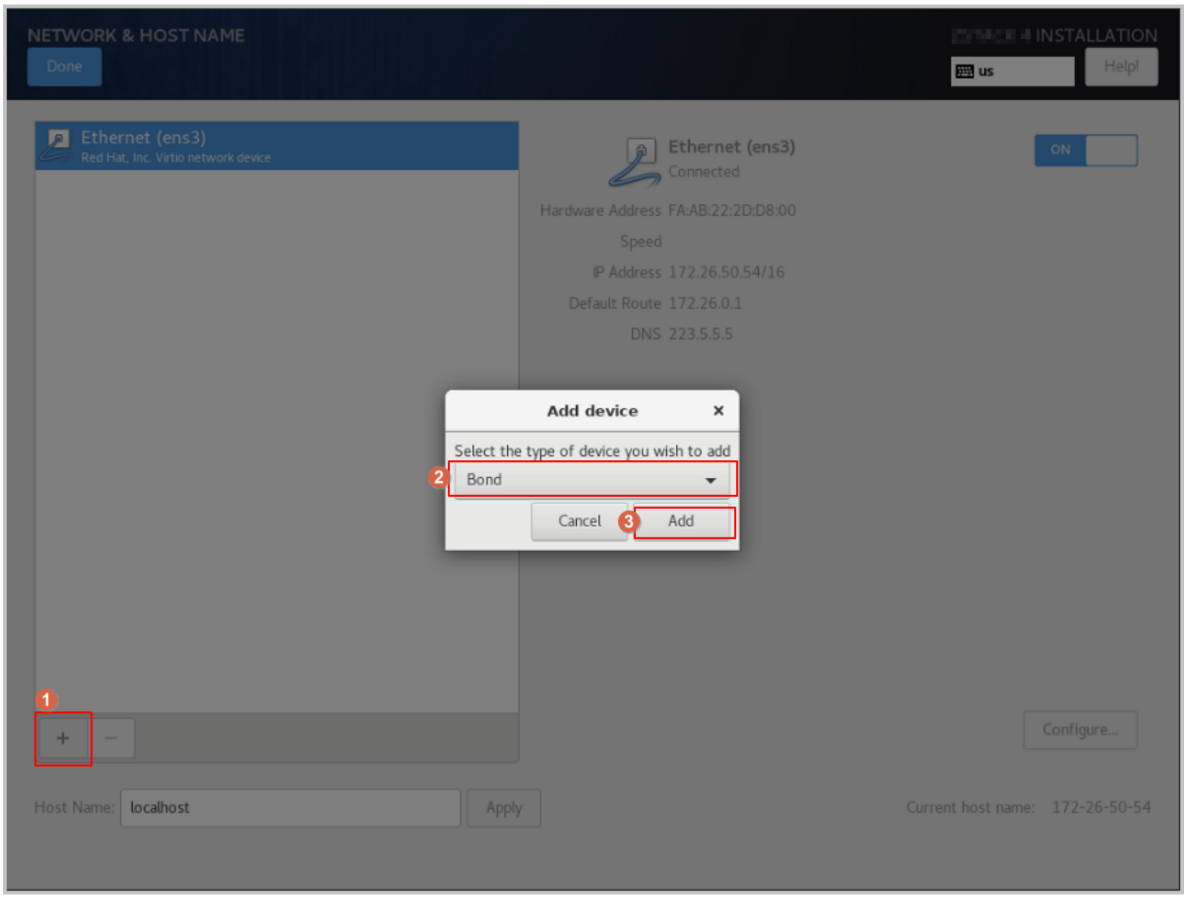
5. Add a bond device.

a) On the **INSTALLATION SUMMARY** page, click **Network & Host Name**.

b) On the **NETWORK & HOST NAME** page, click the **+** button at the bottom left of the page.

This will open the **Add device** dialog. From the drop-down list, choose **Bond**, then click **Add**.

Figure 1-9: Add Bond Device



Hardware Address FA:AB:22:2D:D8:00

Speed

IP Address 172.26.50.54/16

Default Route 172.26.0.1

DNS 223.5.5.5

Select the type of device you wish to add: Bond

Host Name: localhost

Current host name: 172-26-50-54

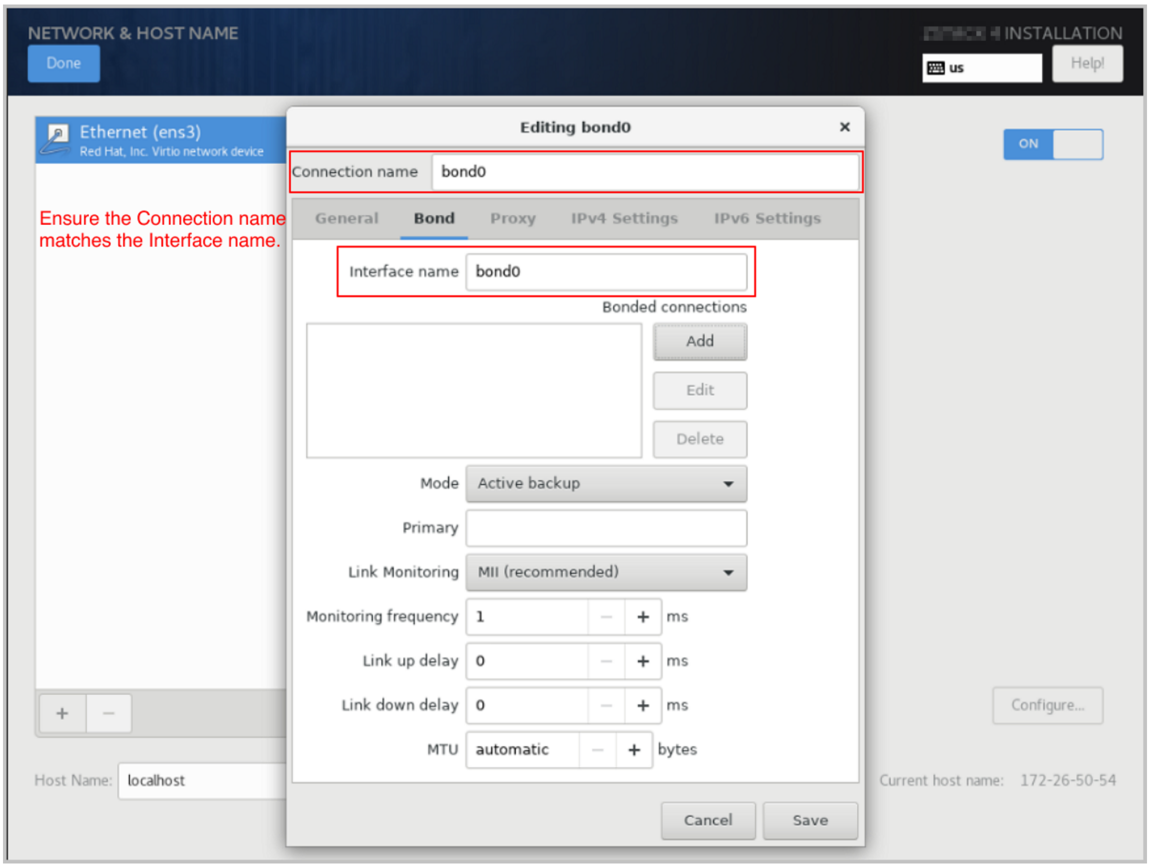
6. Add a Bond Slave.

   a) In the Bond configuration dialog, adjust the Connection name as needed.

   Note:

   Make sure the Connection name matches the Interface name.

Figure 1-10: Adjust Connection Name



Ensure the Connection name matches the Interface name.

Connection name: bond0

Interface name: bond0

Mode: Active backup

Primary:

Link Monitoring: MII (recommended)

Monitoring frequency: 1 ms

Link up delay: 0 ms

Link down delay: 0 ms

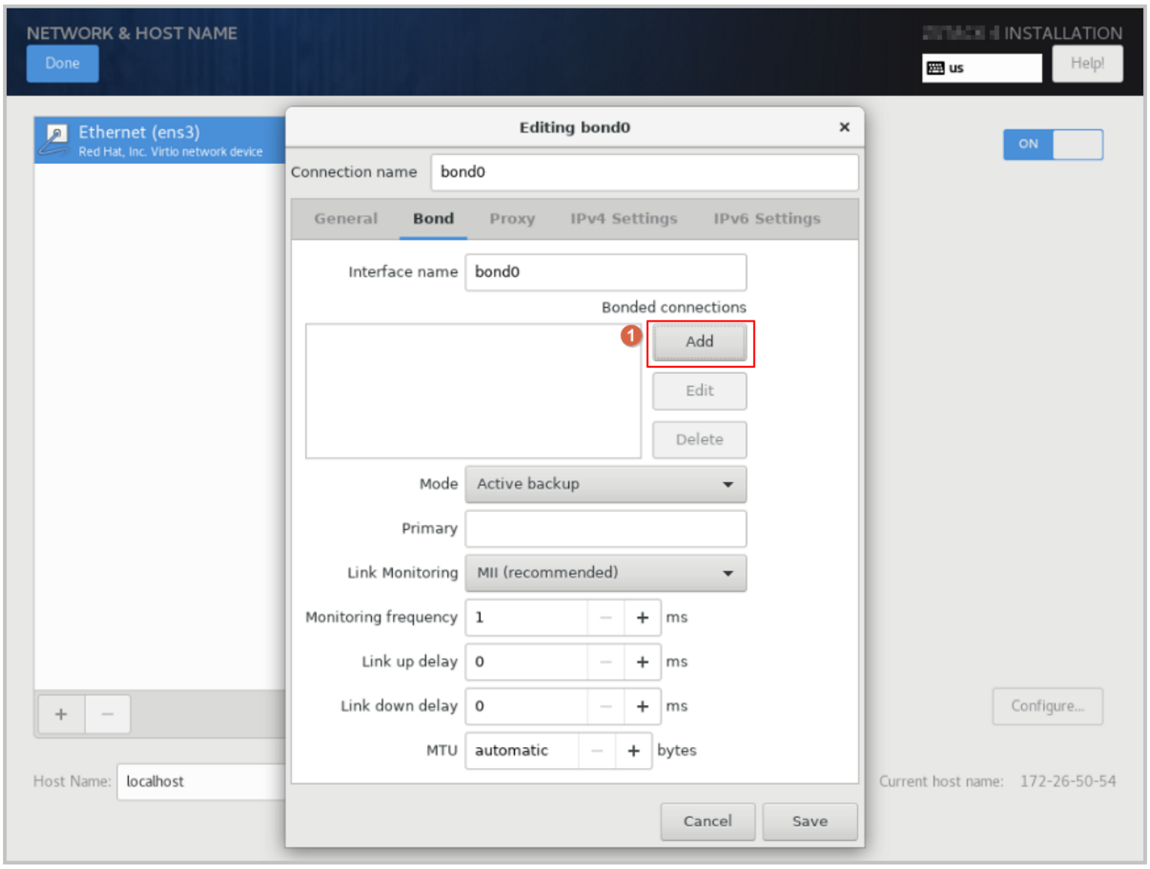
MTU: automatic bytes

Host Name: localhost

Current host name: 172-26-50-54

b) On the Bond configuration window, click **Add** to add a bond slave.

Figure 1-11: Add Bond Slave



Editing bond0

Connection name: bond0

Interface name: bond0

Mode: Active backup

Primary:

Link Monitoring: MII (recommended)

Monitoring frequency: 1 ms

Link up delay: 0 ms

Link down delay: 0 ms

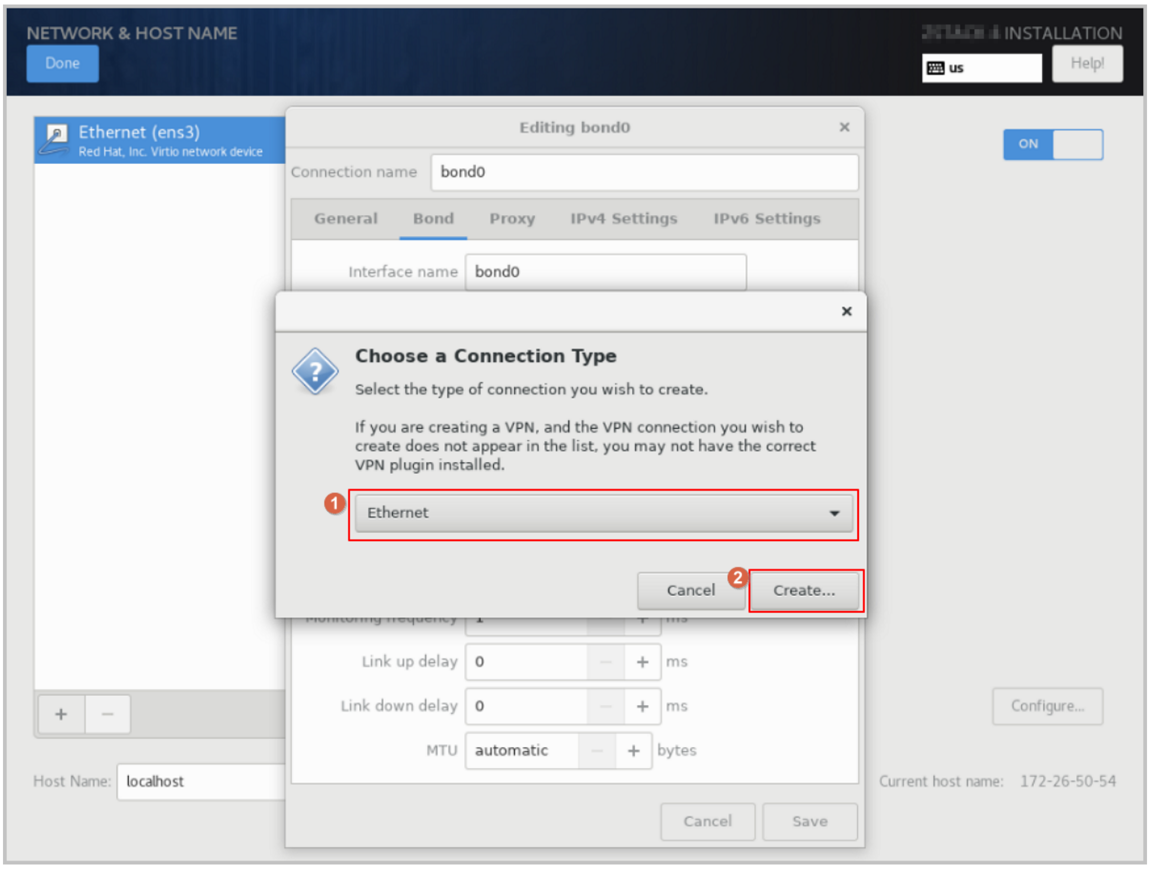
MTU: automatic bytes

Host Name: localhost

Current host name: 172-26-50-54

c) In the **Choose a Connection Type** dialog, choose a connection type from the drop-down list, such as **Ethernet**, and then click **Create...**.

Figure 1-12: Select Bond Slave Connection Type



NETWORK & HOST NAME

Editing bond0

Connection name: bond0

Interface name: bond0

Choose a Connection Type

Select the type of connection you wish to create.

If you are creating a VPN, and the VPN connection you wish to create does not appear in the list, you may not have the correct VPN plugin installed.

1 Ethernet

2 Create...

Link up delay: 0 ms

Link down delay: 0 ms

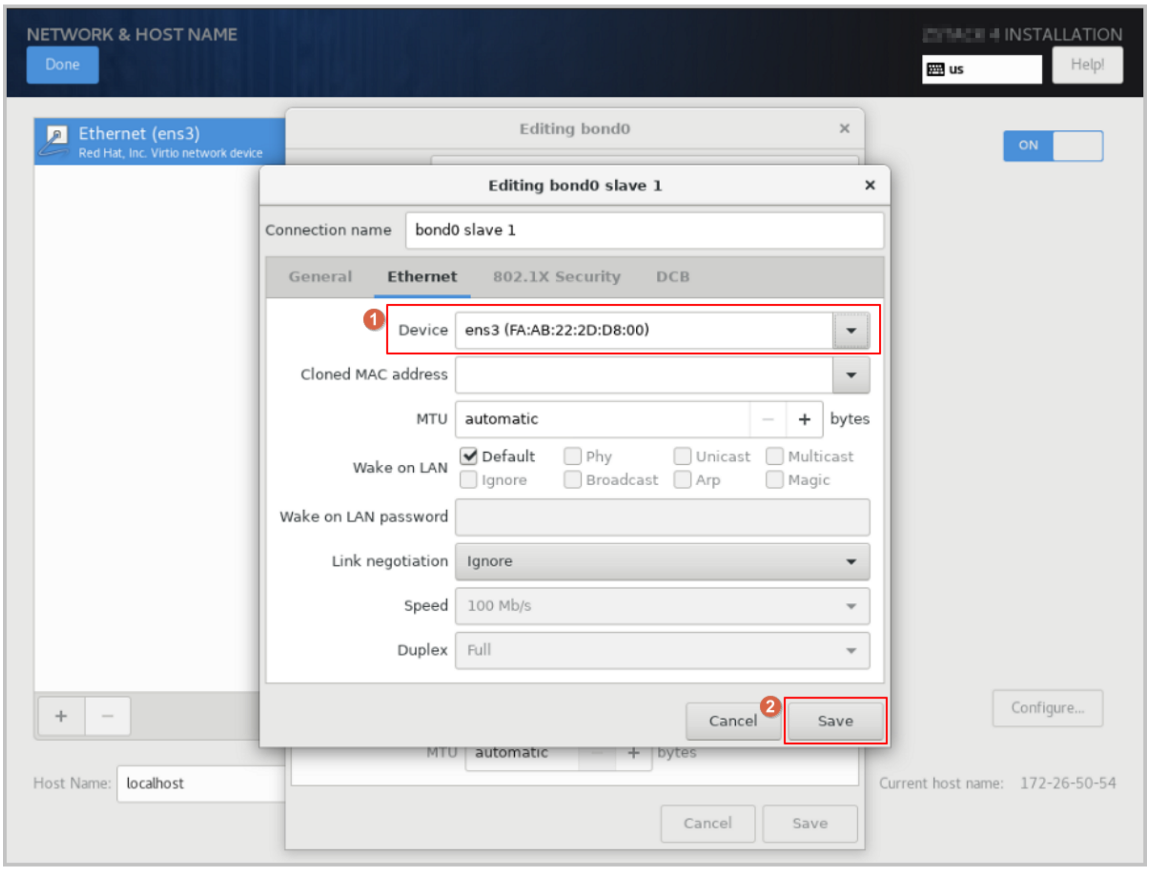
MTU: automatic bytes

Host Name: localhost

Current host name: 172-26-50-54

d) On the **Ethernet** tab of the **Editing bond0 slave1** dialog, click **Device** and select the Slave device you want to bind, such as **ens3 (corresponding MAC address)**. Keep the other options as default or customize them as needed, then click **Save**.

Figure 1-13: Select Bond Slave Device



Editing bond0 slave 1

Connection name: bond0 slave 1

Device: ens3 (FA:AB:22:2D:D8:00)

Cloned MAC address:

MTU: automatic bytes

Wake on LAN: ☑ Default □ Phy □ Unicast □ Multicast □ Ignore □ Broadcast □ Arp □ Magic

Wake on LAN password:

Link negotiation: Ignore

Speed: 100 Mb/s

Duplex: Full

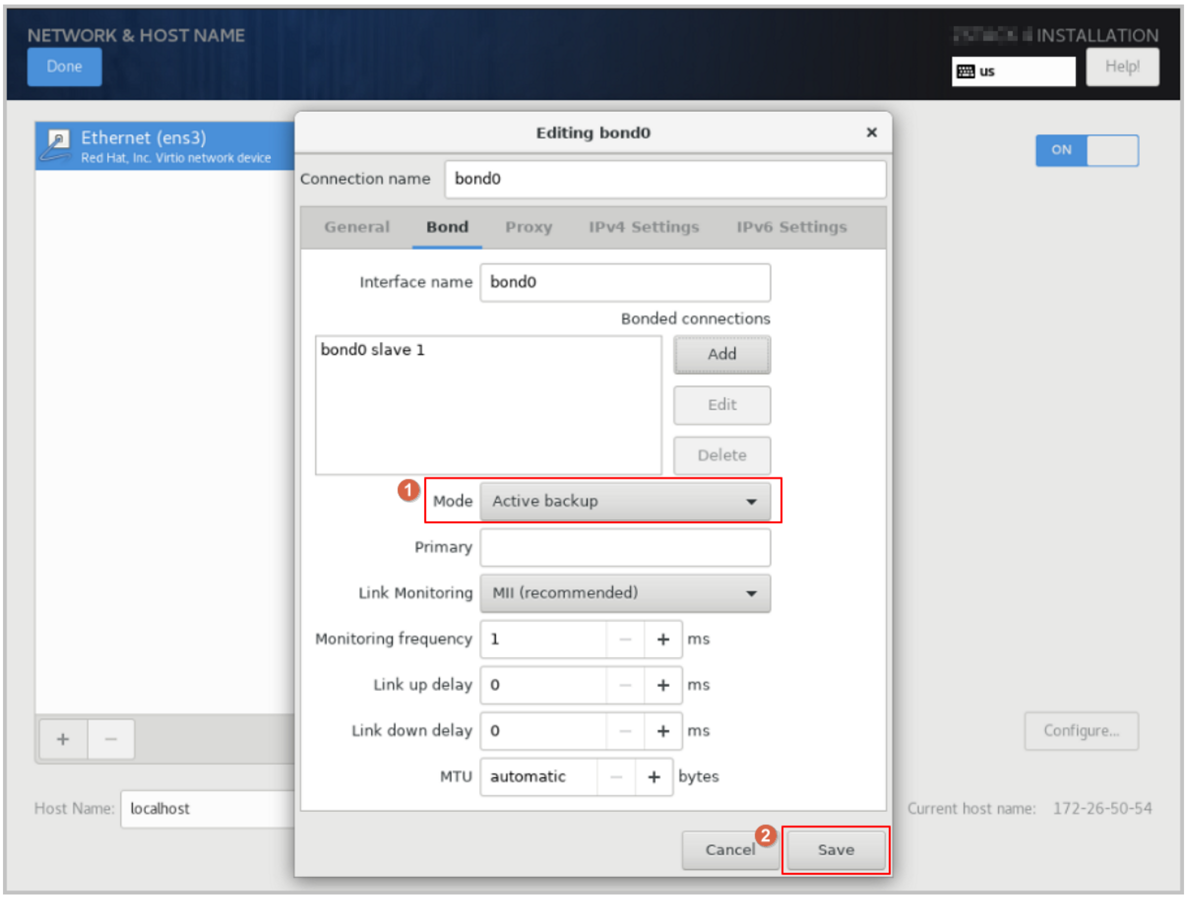
Host Name: localhost

Current host name: 172-26-50-54

7. Select the Bond mode.

   In the Bond configuration dialog, choose the bond mode from the **Mode** drop-down list as needed, such as **Active backup**. Keep the other options as default or customize them as needed, then click **Save**.

Figure 1-14: Select Bond Mode



Connection name: bond0

Interface name: bond0

Bonded connections: bond0 slave 1

Mode: Active backup

Primary:

Link Monitoring: MII (recommended)

Monitoring frequency: 1 ms

Link up delay: 0 ms

Link down delay: 0 ms

MTU: automatic bytes

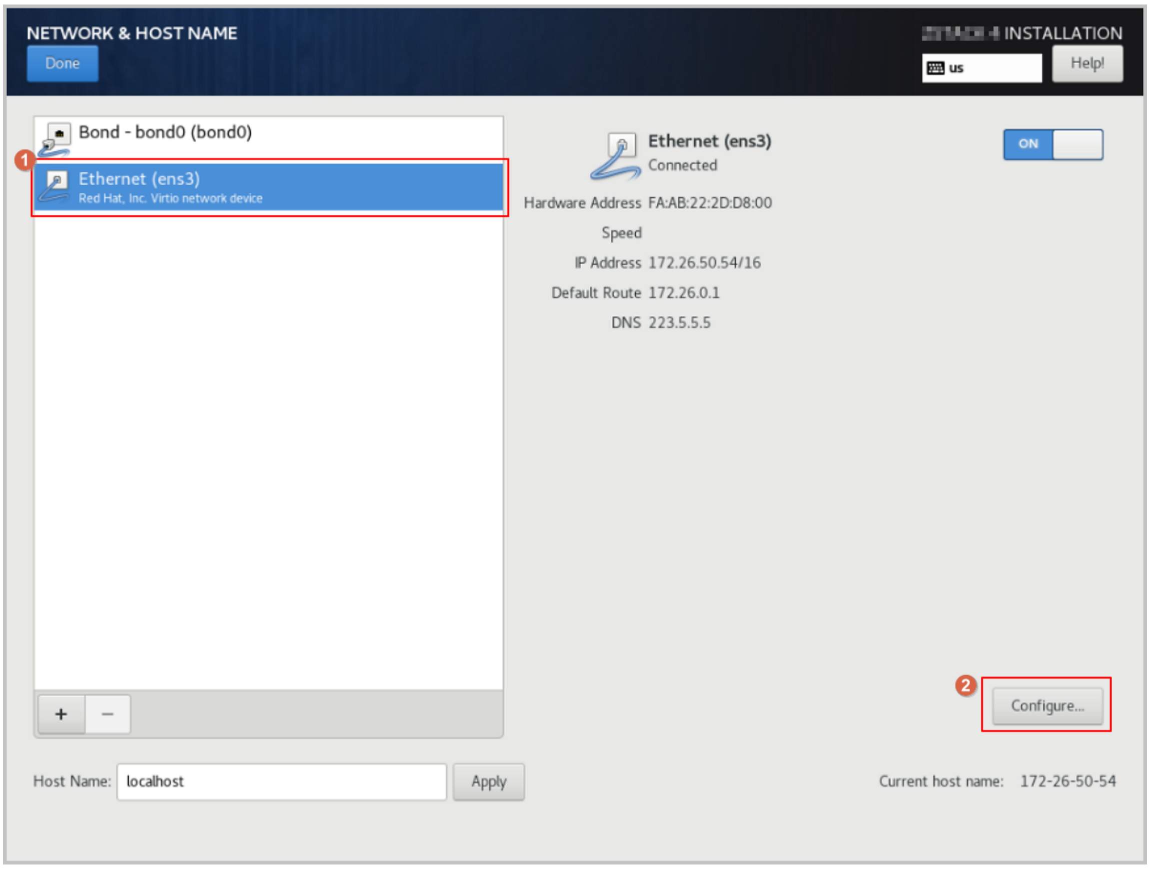
Host Name: localhost

Current host name: 172-26-50-54

8. Disable IPv4 on the original NIC.

   a) Select the original NIC, such as **Ethernet (ens3)**, and click **Configure**.

Figure 1-15: Configure Original NIC



Ethernet (ens3)
Connected

Hardware Address FA:AB:22:2D:D8:00

Speed

IP Address 172.26.50.54/16

Default Route 172.26.0.1

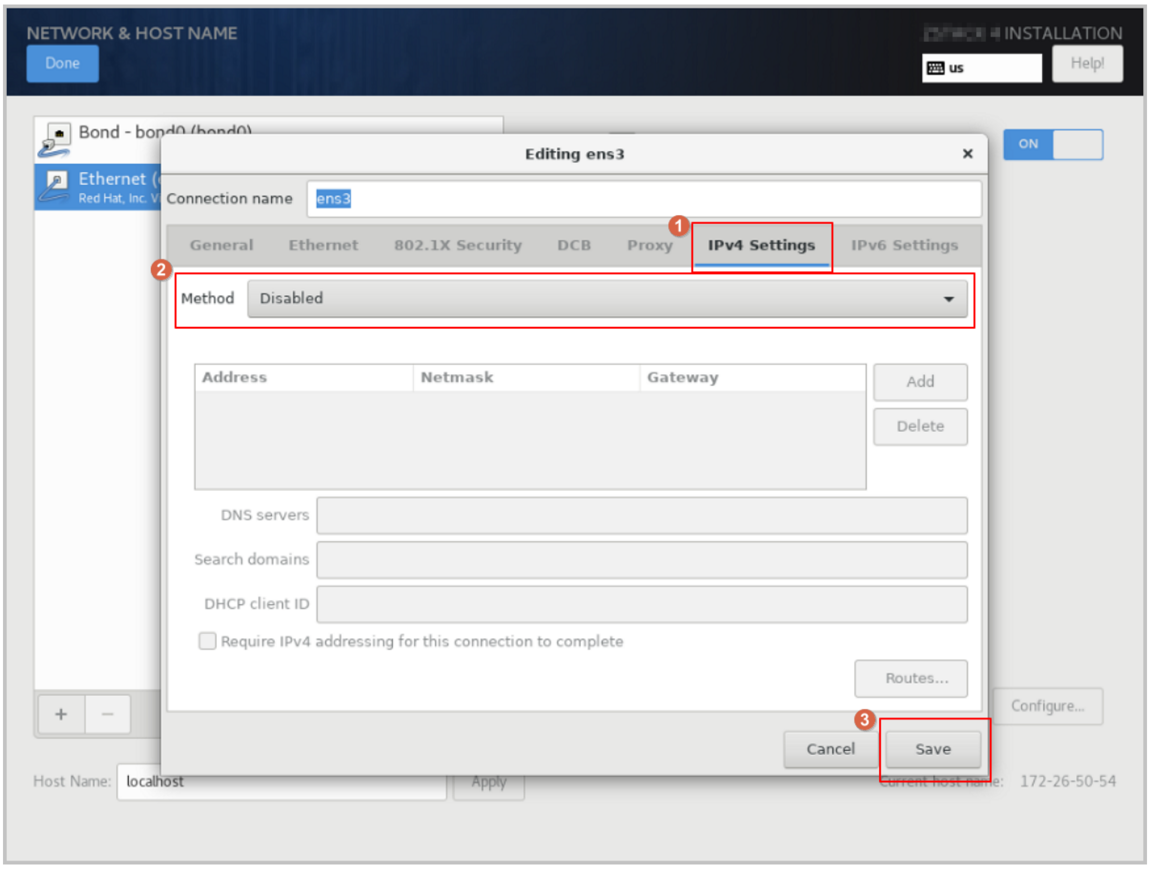
DNS 223.5.5.5

Host Name: localhost

Current host name: 172-26-50-54

b) The **Editing ens3** dialog pops up. Click **IPv4 Settings** to access the **IPv4 Settings** tab. Change the **Method** parameter value to **Disabled**, then click **Save**.

Figure 1-16: Disable IPv4



Editing ens3

Connection name: ens3

Method: Disabled

☐ Require IPv4 addressing for this connection to complete

Host Name: localhost

Current host name: 172-26-50-54

9. Configure a static IP address for Bond.

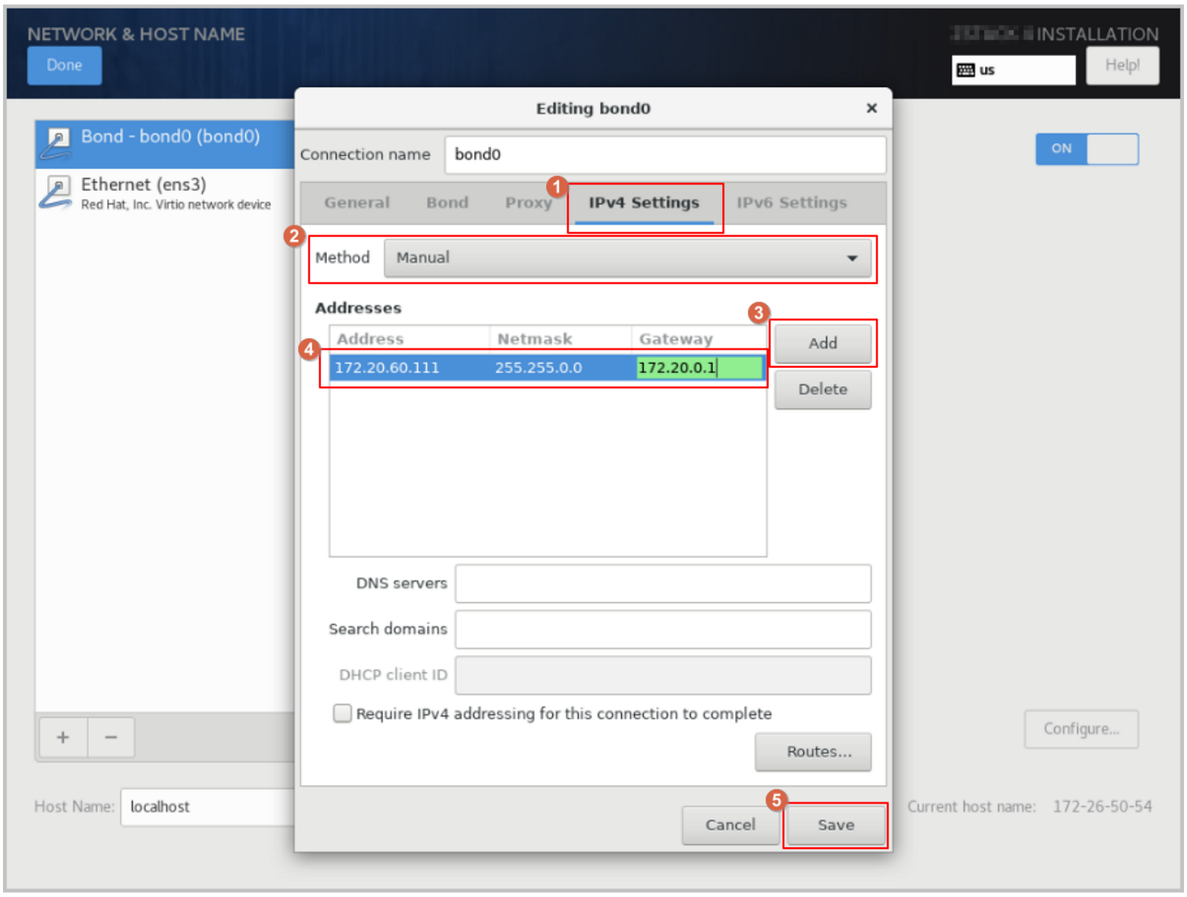
a) On the **NETWORK & HOST NAME** page, choose the bond device, such as **Bond (bond0)**, and then click **Configure**.

b) The **Editing bond0** dialog pops up. click **IPv4 Settings** to access the **IPv4 Settings** tab. Change the **Method** parameter value to **Manual** to switch the IP address acquisition method to manual.

> **Note:**
>
> You can configure the IP address acquisition method as needed, including using DHCP for automatic acquisition or specifying it manually.

c) Click **Add** to add an IP address entry. Configure the IP address, netmask, and gateway as needed, then click **Save** to save the configuration.

Figure 1-17: Configure Bond Static IP Address



Connection name: bond0

Method: Manual

Addresses

Address	Netmask	Gateway
172.20.60.111	255.255.0.0	172.20.0.1

DNS servers:

Search domains:

DHCP client ID:

□ Require IPv4 addressing for this connection to complete

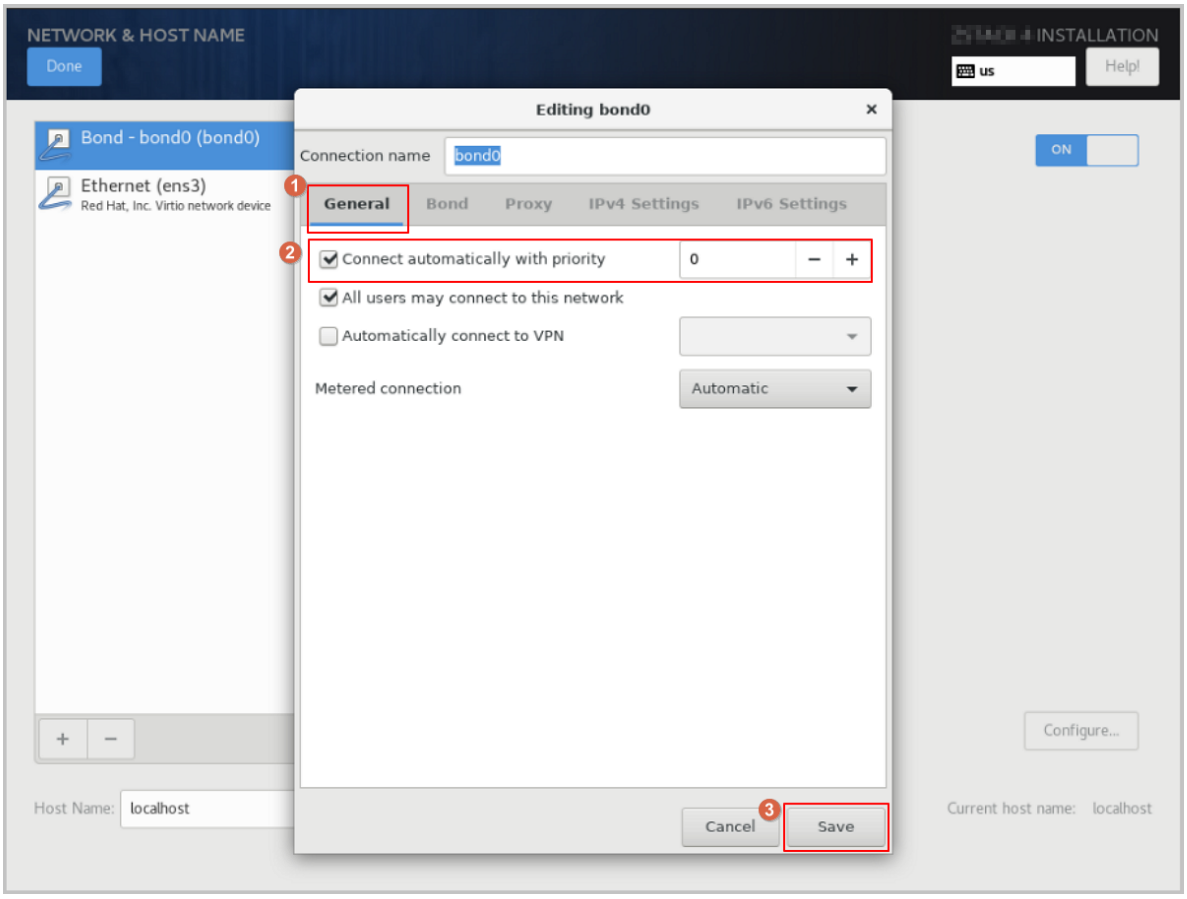
Host Name: localhost

Current host name: 172-26-50-54

10. Configure the NIC to activate automatically.

In the **Editing bond0** dialog, click **General** to access the **General** tab. Select the **Connect automatically with priority** checkbox to set the NIC to activate automatically, then click **Save**.

Figure 1-18: Configure NIC to Activate Automatically



Editing bond0

Connection name: bond0

General | Bond | Proxy | IPv4 Settings | IPv6 Settings

☑ Connect automatically with priority 0 − +

☑ All users may connect to this network

□ Automatically connect to VPN

Metered connection: Automatic

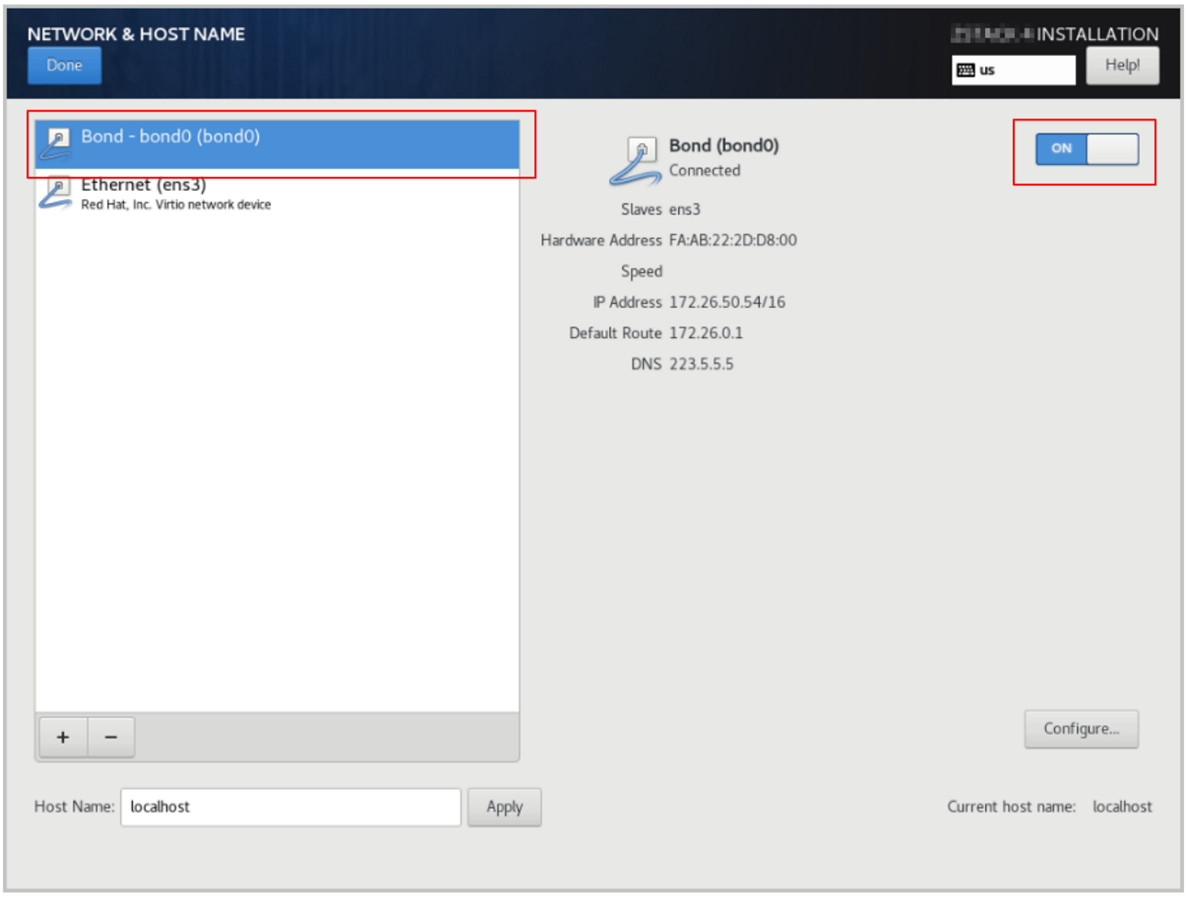
Cancel | Save

11. Complete the Bond configuration.

a) Check the Bond configuration settings. Ensure that **On** is enabled and that you have configured the IP address. Also, make sure the Bond Slave (such as ens3) is set to **On**. Otherwise, ZStack ZSphere will not be installed properly.

b) Review the configuration and click **Done** to return to the **INSTALLATION SUMMARY** page.

Figure 1-19: Check Bond Configuration



NETWORK & HOST NAME

[redacted] INSTALLATION

Bond - bond0 (bond0)

Ethernet (ens3)
Red Hat, Inc. Virtio network device

Bond (bond0)
Connected

Slaves ens3
Hardware Address FA:AB:22:2D:D8:00
Speed
IP Address 172.26.50.54/16
Default Route 172.26.0.1
DNS 223.5.5.5

Host Name: localhost

Current host name: localhost

12. On the **INSTALLATION SUMMARY** page, click **Root Password** to set the root password for the operating system.

13. On the **INSTALLATION SUMMARY** page, click **Begin Installation** to begin installing the operating system.

1.3.1.2 Single NIC Deployment

The operating system installation process is identical for both x86 and ARM servers. This chapter uses x86 servers to introduce the detailed installation procedure.

Procedure

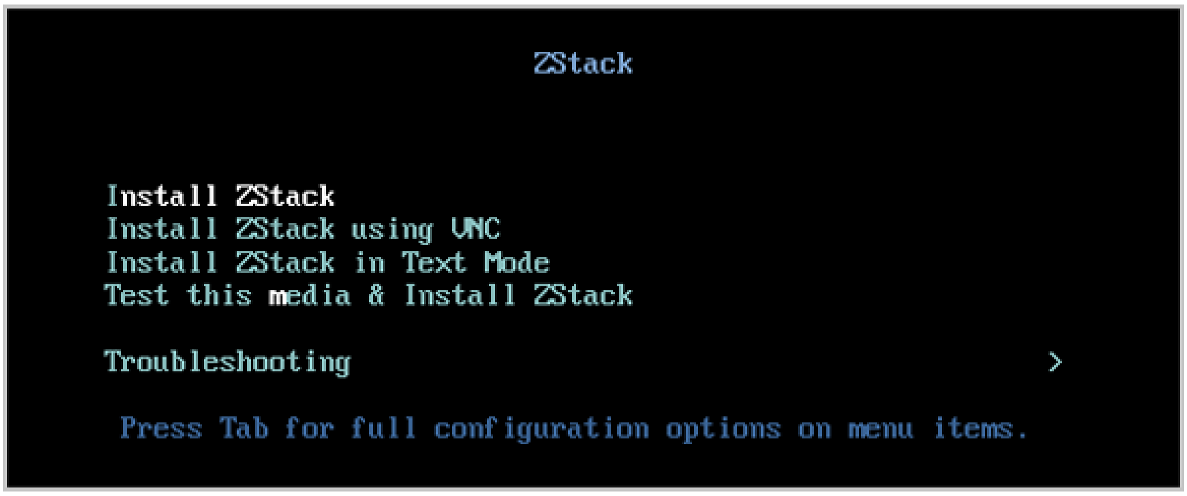
1. Select the boot option.

   Enter the ISO boot interface and choose the default option to start the operating system installation. You can select based on your actual situation, but we recommend using the graphical user interface (GUI) for installation. If the server does not have a VGA port and only supports serial connections, you can use either VNC or text mode installation methods.

   - GUI method

- VNC method
- Text mode method

Figure 1-20: System Boot



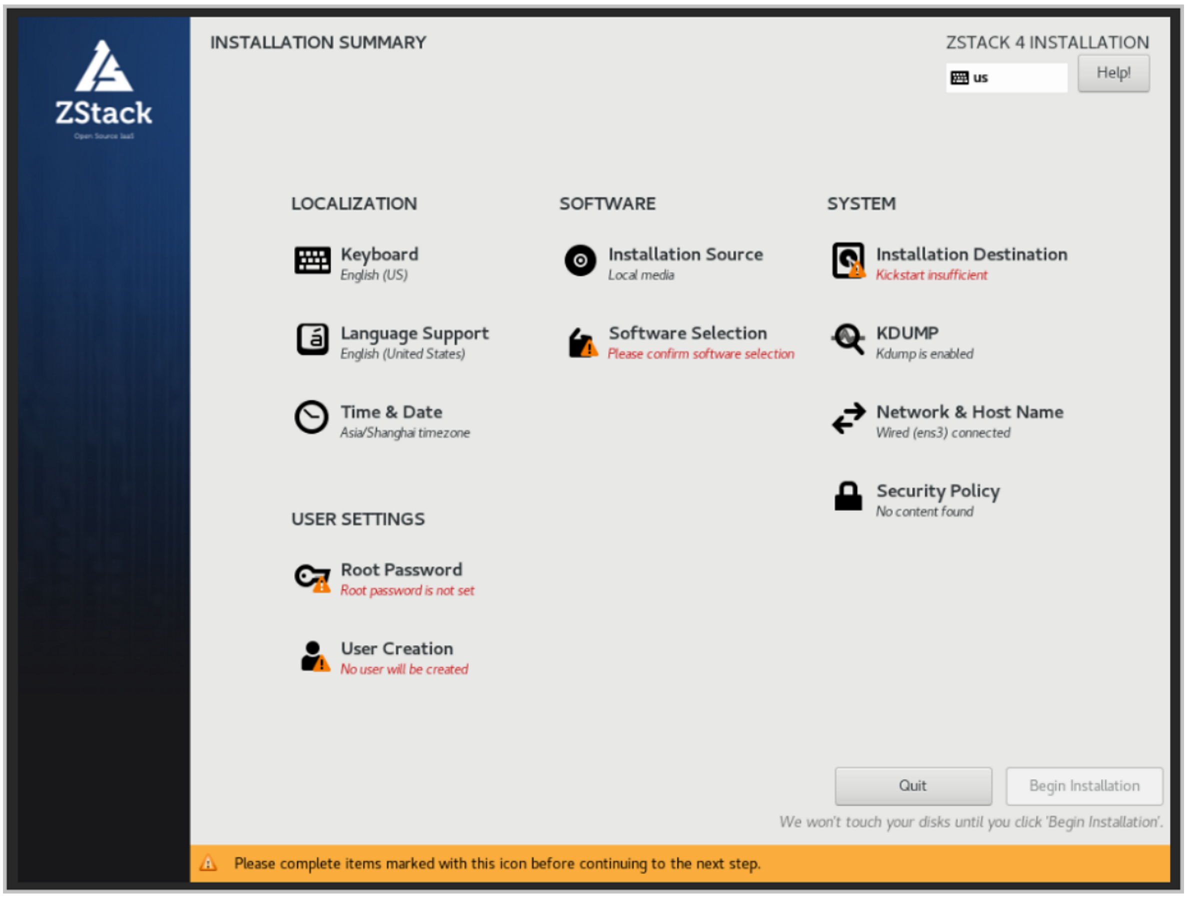
```
                    ZStack


   Install ZStack
   Install ZStack using VNC
   Install ZStack in Text Mode
   Test this media & Install ZStack

   Troubleshooting                              >

    Press Tab for full configuration options on menu items.
```

2. Review the installation configuration summary.

   This page displays the system installation configuration. You can modify the configuration as needed. By default, ZStack ZSphere is configured with the following settings:

   - **Keyboard**: English (US)
   - **Language Support**: English (United States)
   - **Time & Date**: Asia/Shanghai (UTC+8). We recommend that you check the host's time in advance and configure it to the current time and time zone.

Figure 1-21: System Installation Interface



INSTALLATION SUMMARY

ZSTACK 4 INSTALLATION

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Asia/Shanghai timezone

SOFTWARE

Installation Source
Local media

Software Selection
Please confirm software selection

SYSTEM

Installation Destination
Kickstart insufficient

KDUMP
Kdump is enabled

Network & Host Name
Wired (ens3) connected

Security Policy
No content found

USER SETTINGS

Root Password
Root password is not set

User Creation
No user will be created

We won't touch your disks until you click 'Begin Installation'.

⚠ Please complete items marked with this icon before continuing to the next step.

3. Select the installation mode.

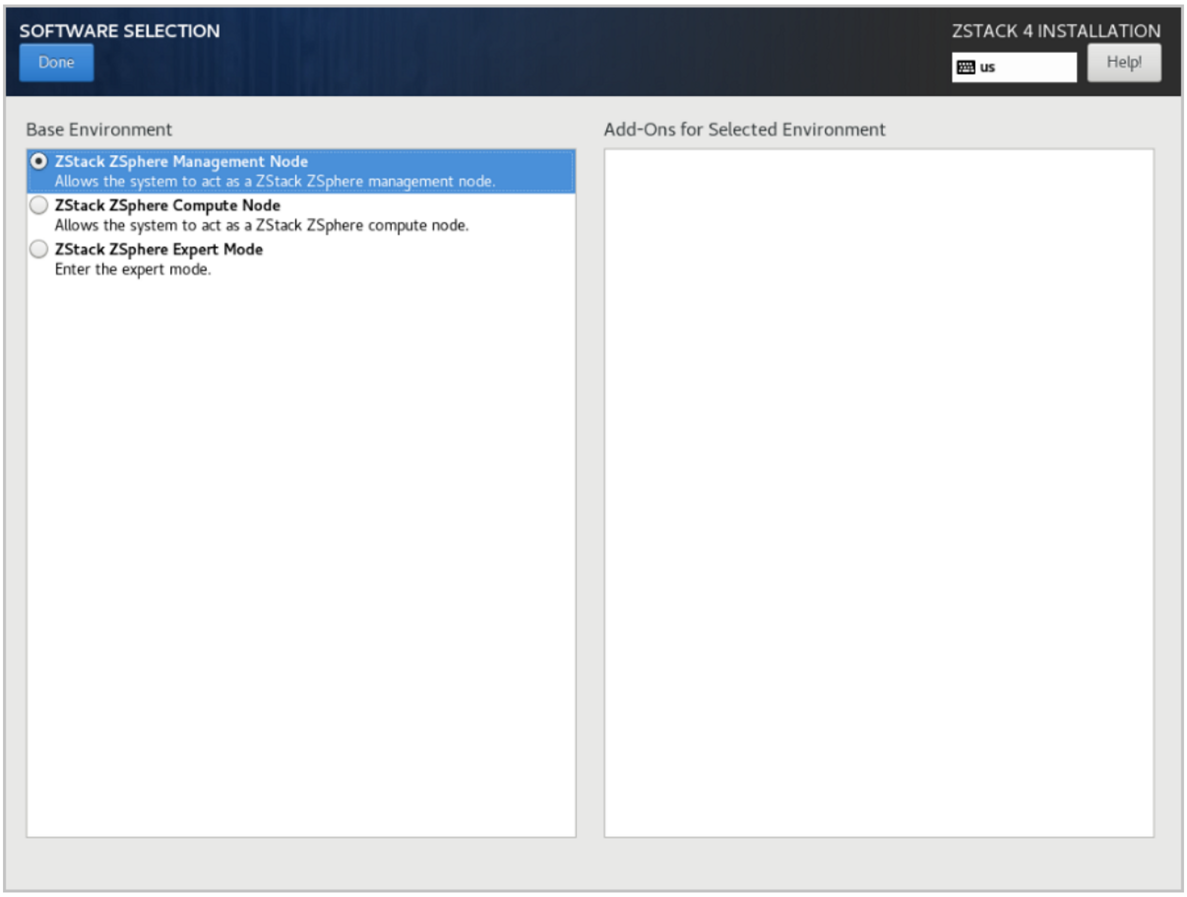
   a) On the **INSTALLATION SUMMARY** page, click **Software Selection**.

   b) On the **SOFTWARE SELECTION** page, choose the installation mode.

      Set the servers for management nodes to **ZStack ZSphere Management Node** mode. Set the other servers to **ZStack ZSphere Compute Node** mode.

   c) After selecting the installation mode, click **Done**.

Figure 1-22: Select Installation Mode



● ZStack ZSphere Management Node
Allows the system to act as a ZStack ZSphere management node.

○ ZStack ZSphere Compute Node
Allows the system to act as a ZStack ZSphere compute node.

○ ZStack ZSphere Expert Mode
Enter the expert mode.

4. Configure the disk partitions.

   a) On the **INSTALLATION SUMMARY** page, click **Installation Destination** to enter the **INSTALLATION DESTINATION** page.

   b) For **Device Selection**, we recommend that you only configure the system disk. After the system is installed, you can configure other disks.

   c) For **Storage Configuration**, we recommend selecting **Automatic** to automatically configure the disk partitions.

   If you need to manually configure disk partitions, refer to the following guidelines based on the BIOS boot mode:

   - UEFI Mode:
     - `/boot`: This directory stores the core files needed for Linux boot. We recommend allocating 1 GB of space.
     - `/boot/efi`: This directory stores the UEFI boot files. We recommend allocating 500 MB.

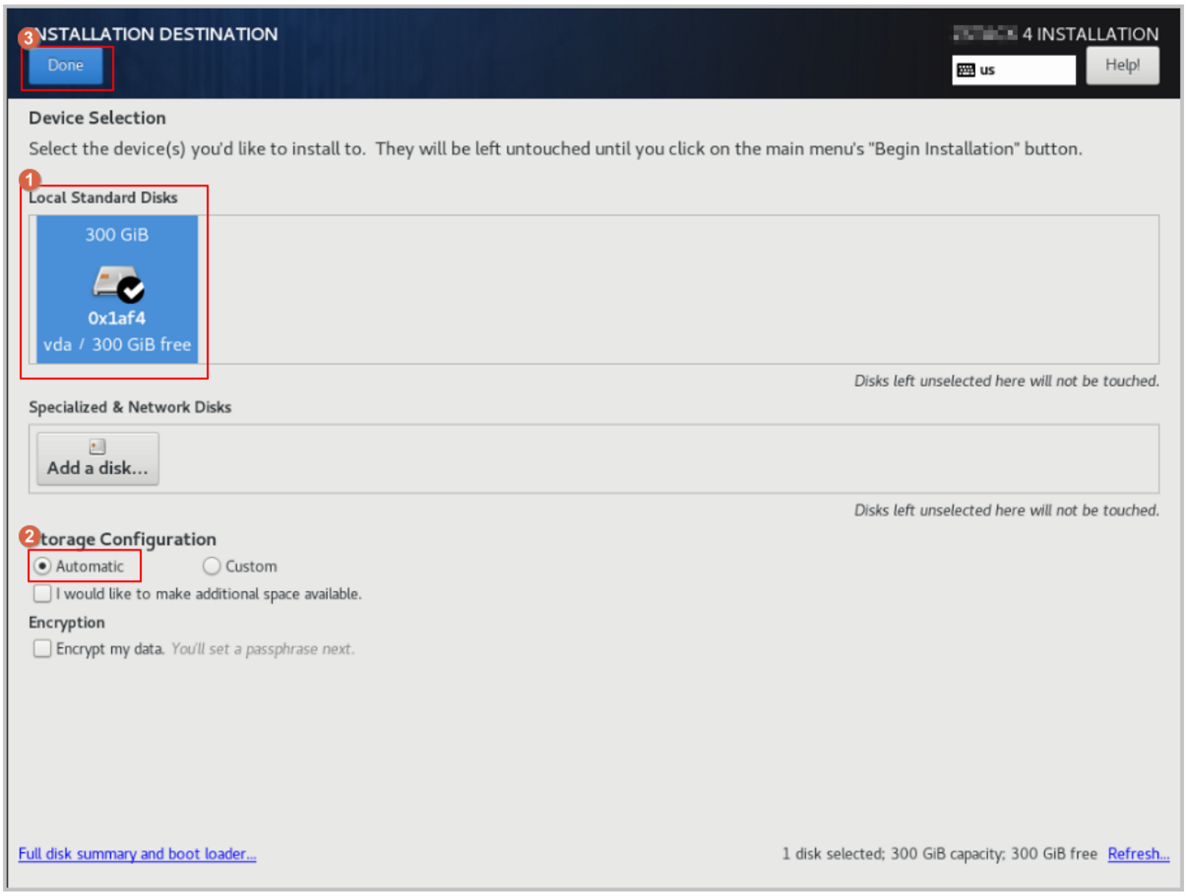
    - `swap`: This is the swap area. We recommend allocating 32 GB.
    - `/`: This is the root directory for the Linux system. We recommend allocating all remaining space.
- Legacy Mode:
    - `/boot`: This directory stores the core files needed for Linux boot. We recommend allocating 1 GB of space.
    - `swap`: This is the swap area. We recommend allocating 32 GB.
    - `/`: This is the root directory for the Linux system. We recommend allocating all remaining space.

Note:

- The above values represent the recommended partition sizes for ZStack ZSphere (total disk capacity should be greater than 300 GB).
- In Legacy mode, if the system disk capacity exceeds 2 TB, you need to configure a BIOS boot partition to support GPT partitioning. UEFI mode does not have this limitation and supports GPT partitioning.

d) Review the configuration and click **Done**.

Figure 1-23: Configure Disk Partitions


3
INSTALLATION DESTINATION
Done
[redacted] 4 INSTALLATION
us
Help!
1
2
Add a disk...
Full disk summary and boot loader...
Refresh...

Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

300 GiB
0x1af4
vda / 300 GiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

Disks left unselected here will not be touched.

Storage Configuration

● Automatic ○ Custom

□ I would like to make additional space available.

Encryption

□ Encrypt my data. *You'll set a passphrase next.*

1 disk selected; 300 GiB capacity; 300 GiB free

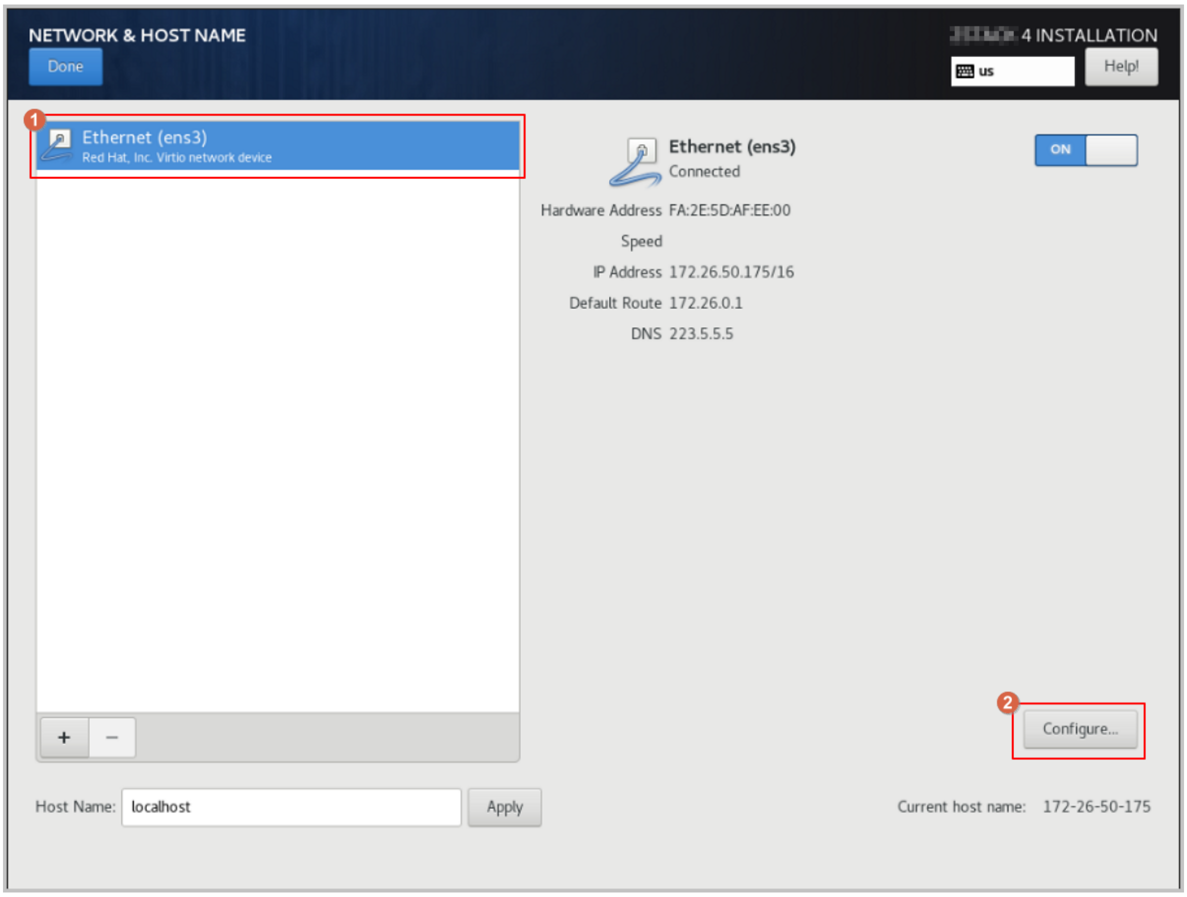
5. Start configuring the NIC.

   a) On the **INSTALLATION SUMMARY** page, click **Network & Host Name** to access the **NETWORK & HOST NAME** page.

   b) Select a NIC from the list on the left, such as **Ethernet (ens3)**.

   c) Click **Configure**.

Figure 1-24: Configure NIC



Ethernet (ens3)
Connected

Hardware Address FA:2E:5D:AF:EE:00
Speed
IP Address 172.26.50.175/16
Default Route 172.26.0.1
DNS 223.5.5.5

Host Name: localhost

Current host name: 172-26-50-175

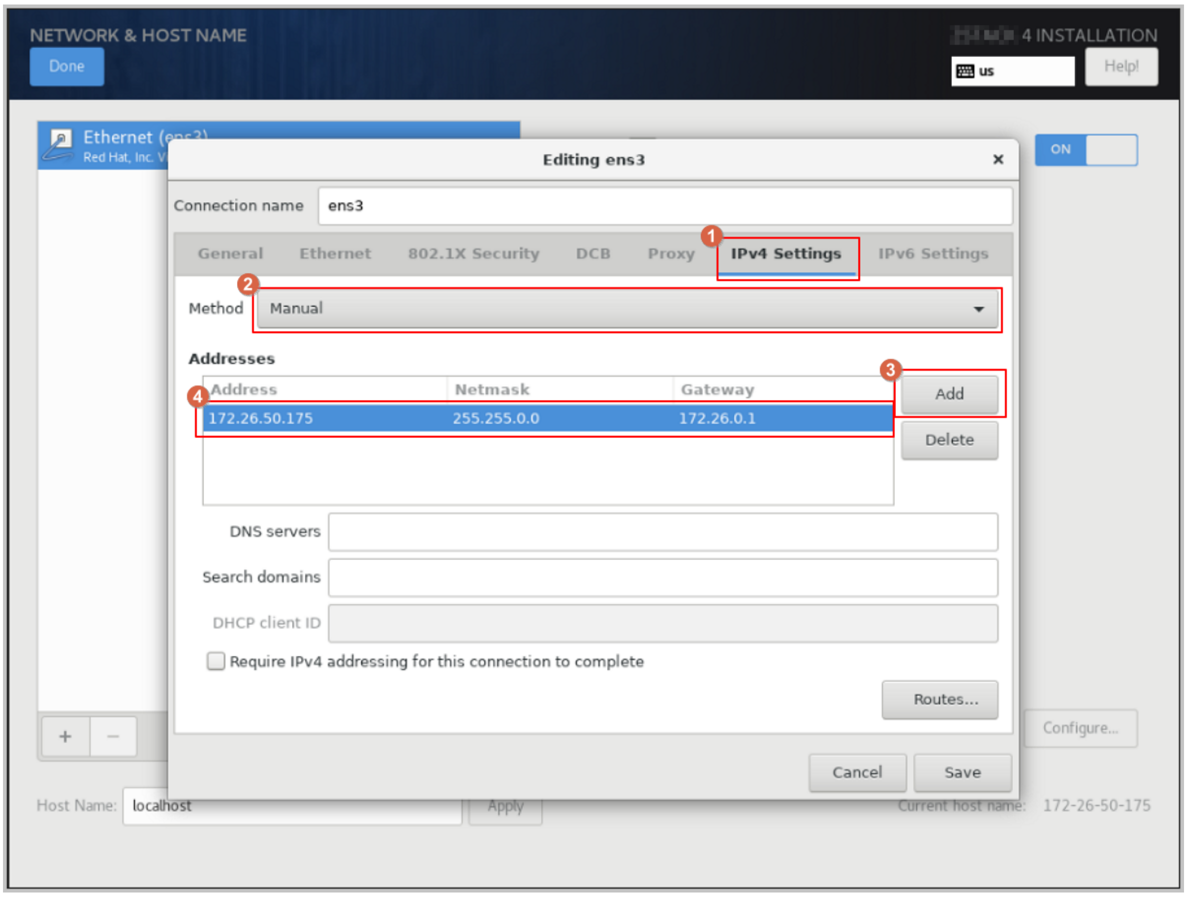
6. Configure a static IP address for the NIC.

   a) In the **Editing ens3** dialog, click **IPv4 Settings**.

   b) For **Method**, choose the IP address acquisition method as needed. For example, select **Manual** to specify the IP address manually.

   c) Click **Add** to add an IP address entry, and configure the IP address, netmask, and gateway as needed.

Figure 1-25: Configure Static IP Address



NETWORK & HOST NAME

Done

[redacted] 4 INSTALLATION

us

Help!

Ethernet (ens3)

Red Hat, Inc. V

ON

Editing ens3

Connection name: ens3

General | Ethernet | 802.1X Security | DCB | Proxy | 1 IPv4 Settings | IPv6 Settings

2 Method: Manual

Addresses

Address	Netmask	Gateway
172.26.50.175	255.255.0.0	172.26.0.1

3 Add

4

Delete

DNS servers:

Search domains:

DHCP client ID:

□ Require IPv4 addressing for this connection to complete

Routes...

Cancel | Save

Configure...

Host Name: localhost

Apply

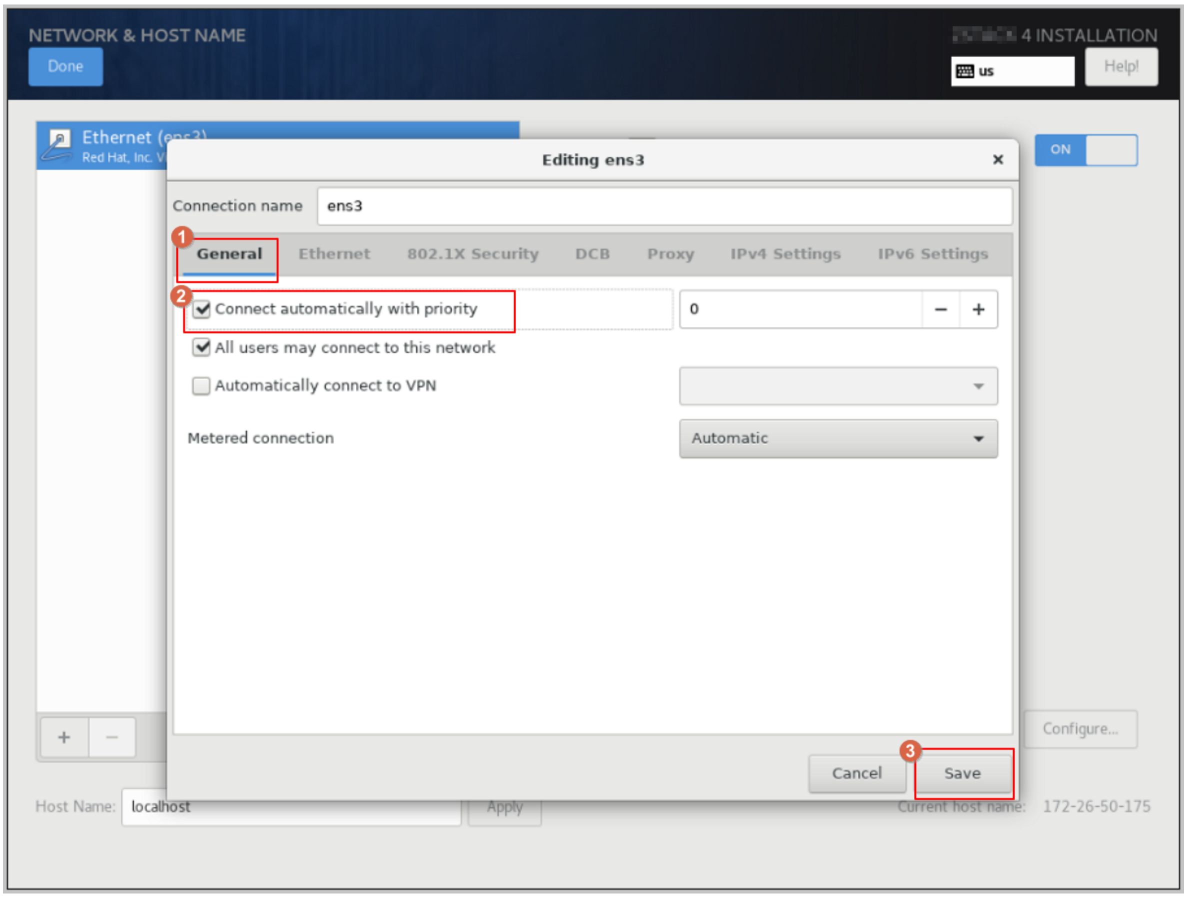
Current host name: 172-26-50-175

7. Configure the NIC to activate automatically.

   a) In the **Editing ens3** dialog, click **General**, then select the **Connect automatically with priority** checkbox to set the NIC for automatic activation.

   b) Review the configuration and click **Save**.

Figure 1-26: Configure NIC to Activate Automatically



Editing ens3

Connection name: ens3

☑ Connect automatically with priority 0

☑ All users may connect to this network

□ Automatically connect to VPN

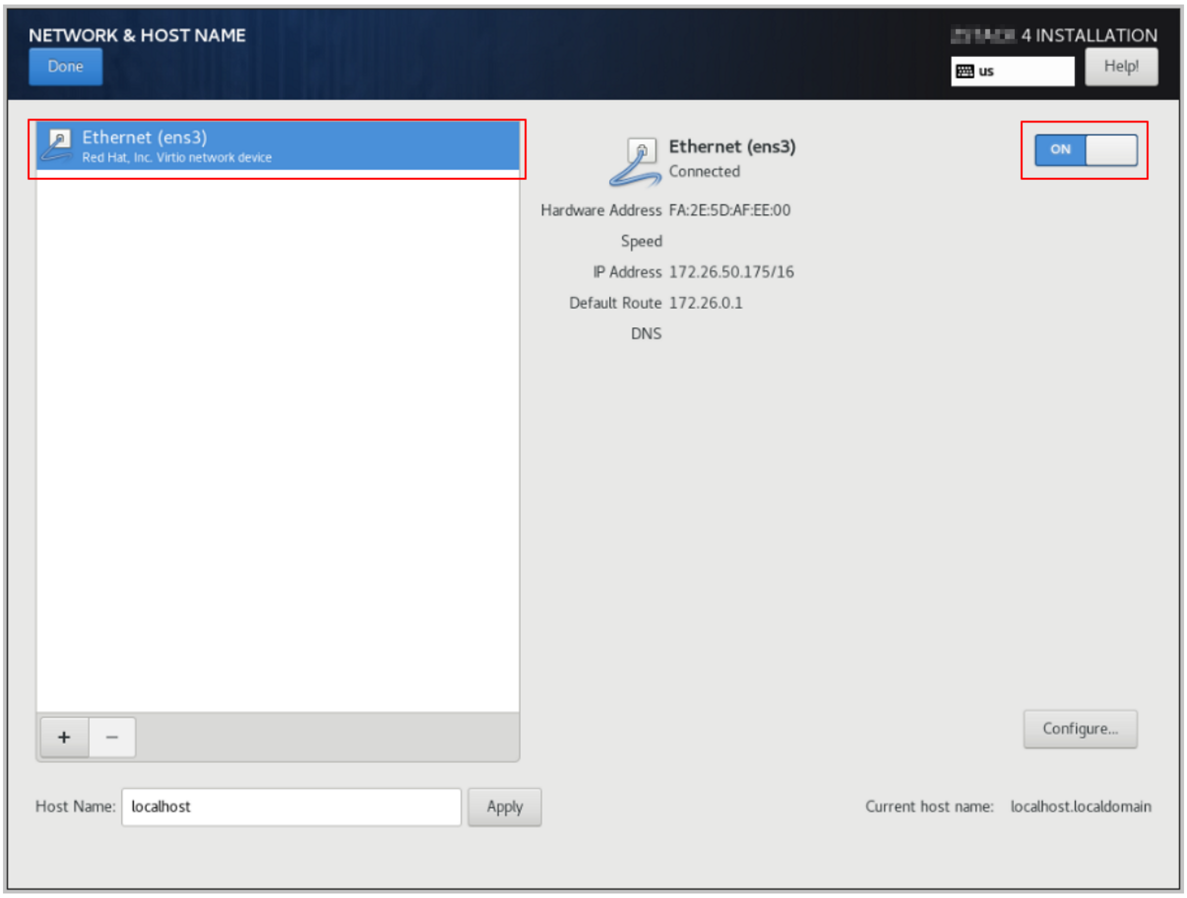
Metered connection: Automatic

8. Complete the NIC configuration.

   a) Return to the **NETWORK & HOST NAME** page, and confirm that you have selected the correct NIC and that the NIC status is **ON**.

   b) Click **Done** to return the **INSTALLATION SUMMARY** page.

Figure 1-27: Check NIC Configuration



Ethernet (ens3)
Red Hat, Inc. Virtio network device

Ethernet (ens3)
Connected

Hardware Address FA:2E:5D:AF:EE:00
Speed
IP Address 172.26.50.175/16
Default Route 172.26.0.1
DNS

Host Name: localhost

Current host name: localhost.localdomain

9. On the **INSTALLATION SUMMARY** page, click **Root Password** to set the root password for the operating system.

10. On the **INSTALLATION SUMMARY** page, click **Begin Installation** to begin installing the operating system.

1.3.2 Set Up Management Node HA

1.3.2.1 Through GUI

Prerequisites

- You must install management node services on the selected two servers. For installation instructions, see *Install Management Node*.
- Ensure both management nodes have gateway addresses on the same network segment and have consistent NIC names.
- Ensure both management nodes are running the same version.

- Ensure the operating system type and architecture are supported and both management nodes run compatible operating system types.
- Ensure both management nodes use the same license type.

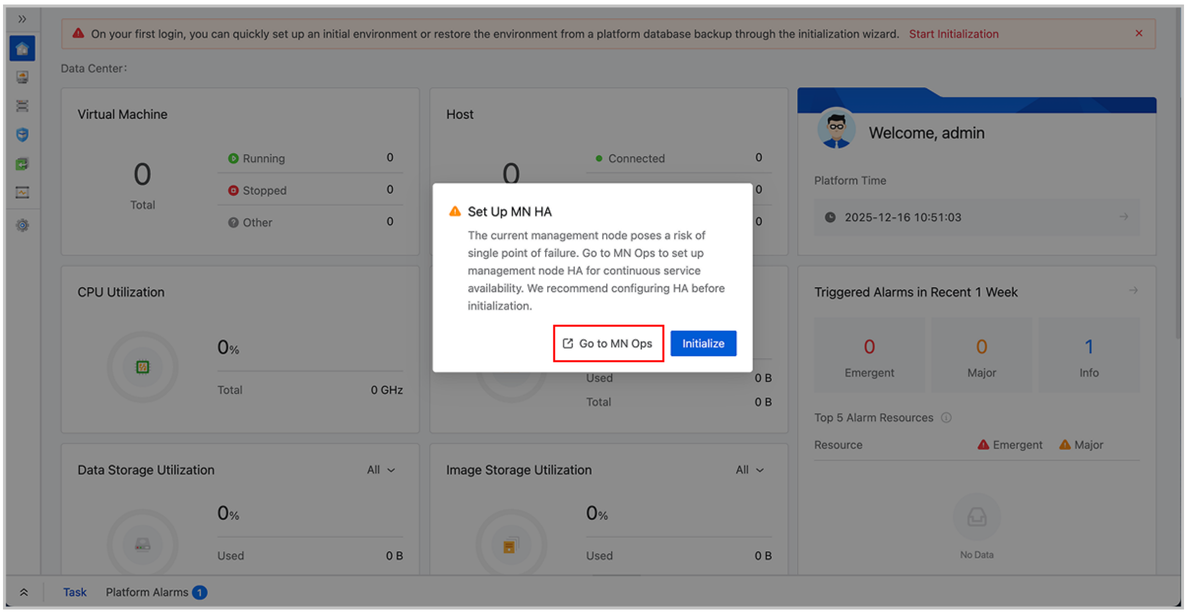
Procedure

1. Log in to the UI management interface of either management node.

   For a new environment that has not been initialized:

   1. In the **Welcome to Initialization Wizard** dialog, click **Next**. The system automatically detects the management node HA status.
   2. In the **Set Up MN HA** dialog, click **Go to MN Ops**.
   3. A new browser tab opens displaying the MN Ops page.

   Figure 1-28: Go to MN Ops from the Initialization Page



On your first login, you can quickly set up an initial environment or restore the environment from a platform database backup through the initialization wizard. Start Initialization

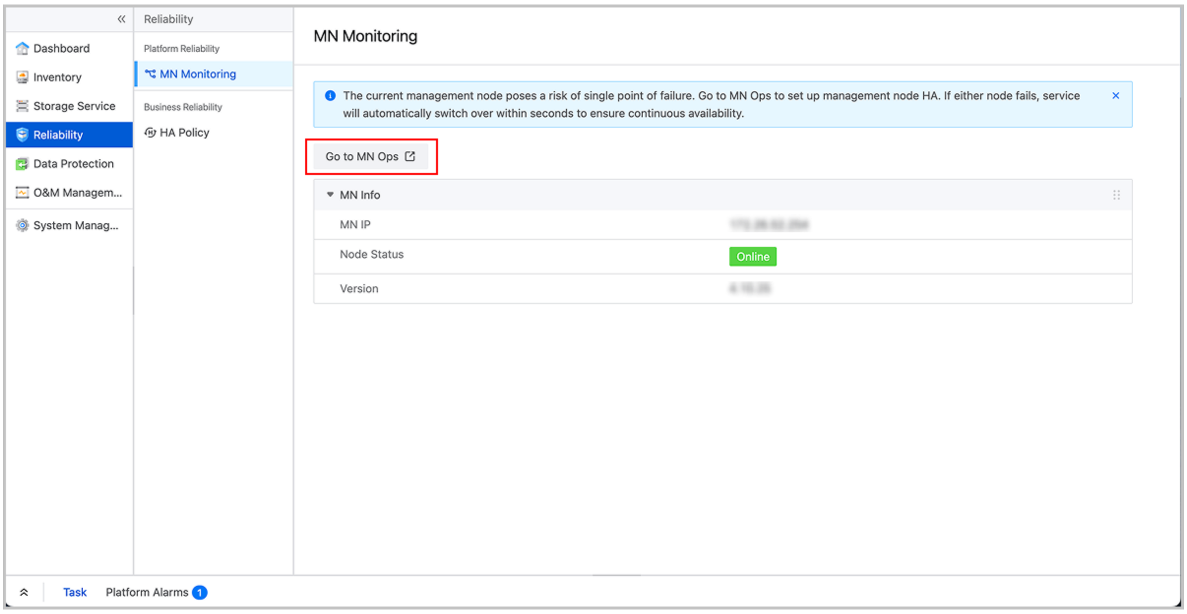
Set Up MN HA

The current management node poses a risk of single point of failure. Go to MN Ops to set up management node HA for continuous service availability. We recommend configuring HA before initialization.

   For an existing environment:

   1. In the navigation pane, choose **Reliability** > **MN Monitoring**.
   2. On the **MN Monitoring** page, click **Go to MN Ops**.
   3. A new browser tab opens displaying the MN Ops page.

Figure 1-29: Go to MN Ops from the MN Monitoring Page

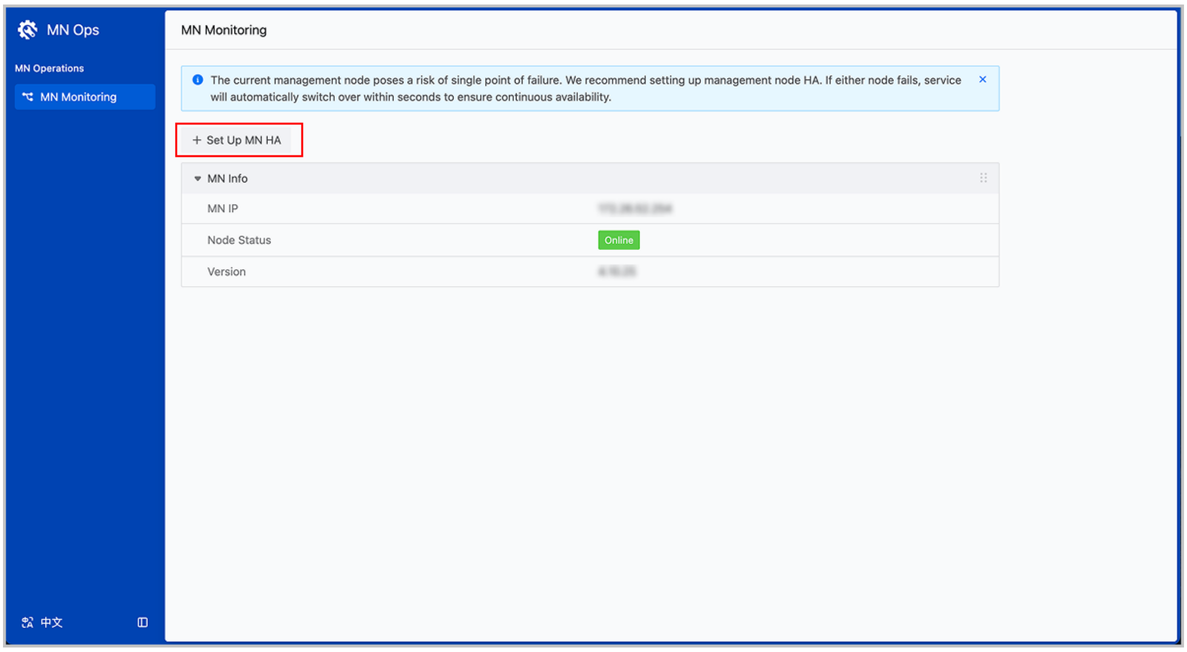


The current management node poses a risk of single point of failure. Go to MN Ops to set up management node HA. If either node fails, service will automatically switch over within seconds to ensure continuous availability.

MN Info	
MN IP	[redacted]
Node Status	Online
Version	[redacted]

2. On the **MN Monitoring** page in MN Ops, click **Set Up MN HA**.

Figure 1-30: MN Monitoring



The current management node poses a risk of single point of failure. We recommend setting up management node HA. If either node fails, service will automatically switch over within seconds to ensure continuous availability.

MN Info	
MN IP	[redacted]
Node Status	Online
Version	[redacted]

3. In the **Set Up MN HA** dialog, complete configuring MN, reviewing configuration, and setting up MN HA.

   a) For **Configure MN**, set the following parameters:

- **VIP**: Configure the VIP for accessing the management interface of the management node environment.

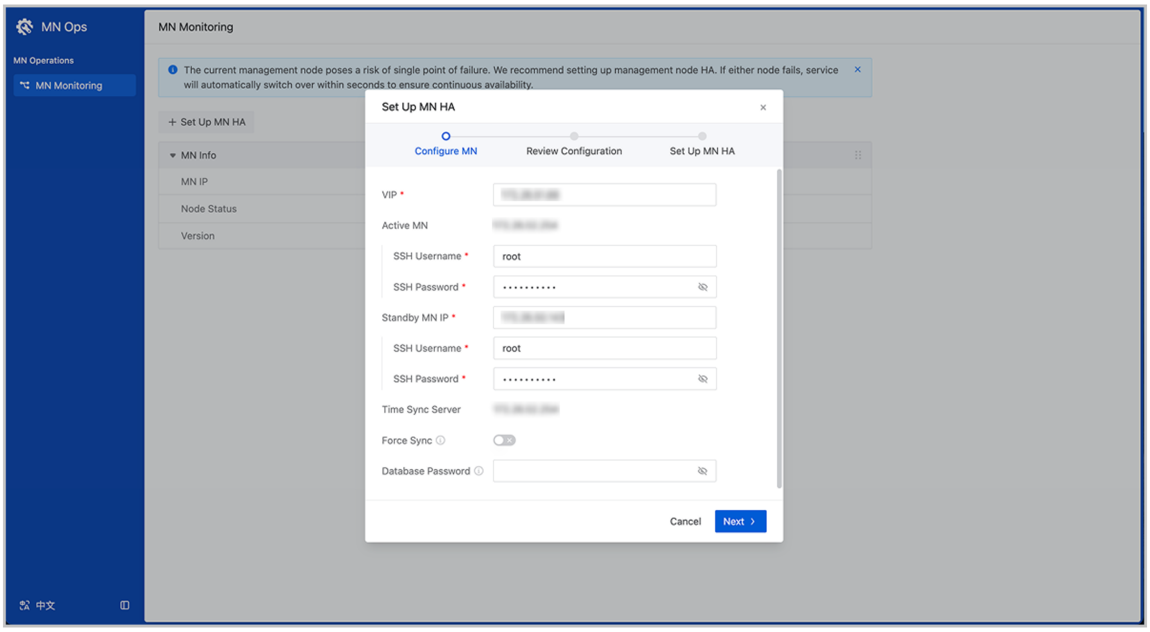
  > **Note:**
  >
  > Ensure the VIP is in the same network segment as the active management node IP.

- **Active MN IP**: Display the IP address of the active management node. Specify the SSH username and password for the active management node.
- **Standby MN IP**: Specify the IP address, SSH username, and SSH password for the standby management node.

  > **Note:**
  >
  > - Ensure the standby management node IP is in the same network segment as the active management node IP.
  > - When setting up management node HA, the management node password can contain English letters, numbers, and these special characters: `` -=[];,./~!@#$%^&*()_+|{}:<>?` ``. If your password does not meet this rule, update it before setting up management node HA.

- **Time Sync Server**: Uses the active management node IP as the time synchronization server by default.
- **Force Sync**: Disabled by default. If the databases between active and standby management nodes cannot synchronize automatically, run the zsha2 installation command forcibly on the active management node.
- **Database Password**: If left blank, the initial database password will be used by default. If the password has been changed, enter the new password here.

Figure 1-31: Configure MN



MN Ops

MN Operations

MN Monitoring

MN Monitoring

The current management node poses a risk of single point of failure. We recommend setting up management node HA. If either node fails, service will automatically switch over within seconds to ensure continuous availability.

+ Set Up MN HA

MN Info

MN IP

Node Status

Version

Set Up MN HA

Configure MN — Review Configuration — Set Up MN HA

VIP * [redacted]

Active MN [redacted]

SSH Username * root

SSH Password * ••••••••••

Standby MN IP * [redacted]

SSH Username * root

SSH Password * ••••••••••

Time Sync Server [redacted]

Force Sync

Database Password

Cancel | Next

中文

b) Click **Next**.

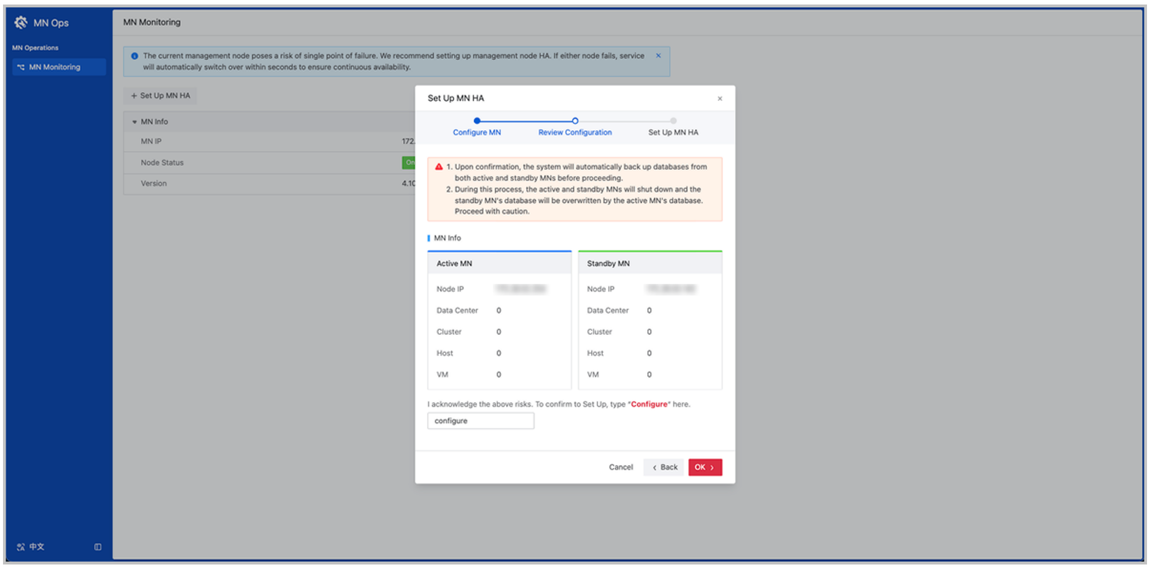
The system automatically checks if the requirements for addition are met.

c) In the **Review Configuration** step, check the resource information of both active and standby management nodes.

Note:

1. Upon confirmation, the system will automatically back up databases from active and standby management nodes before proceeding.
2. During this process, the active and standby MNs will shut down and the standby MN's database will be overwritten by the active MN's database. Proceed with caution.
3. If you find that the standby management node contains more resources during the resource comparison, and you want to preserve these resources, we recommend that you select the **Switch Active/Standby MNs** checkbox. When selected, this option switches the roles of active and standby management nodes, using the resource-rich standby management node as the active management node to set up management node HA.

Figure 1-32: Review Configuration



The current management node poses a risk of single point of failure. We recommend setting up management node HA. If either node fails, service will automatically switch over within seconds to ensure continuous availability.

Set Up MN HA

1. Upon confirmation, the system will automatically back up databases from both active and standby MNs before proceeding.
2. During this process, the active and standby MNs will shut down and the standby MN's database will be overwritten by the active MN's database. Proceed with caution.

MN Info

Active MN		Standby MN	
Node IP	[redacted]	Node IP	[redacted]
Data Center	0	Data Center	0
Cluster	0	Cluster	0
Host	0	Host	0
VM	0	VM	0

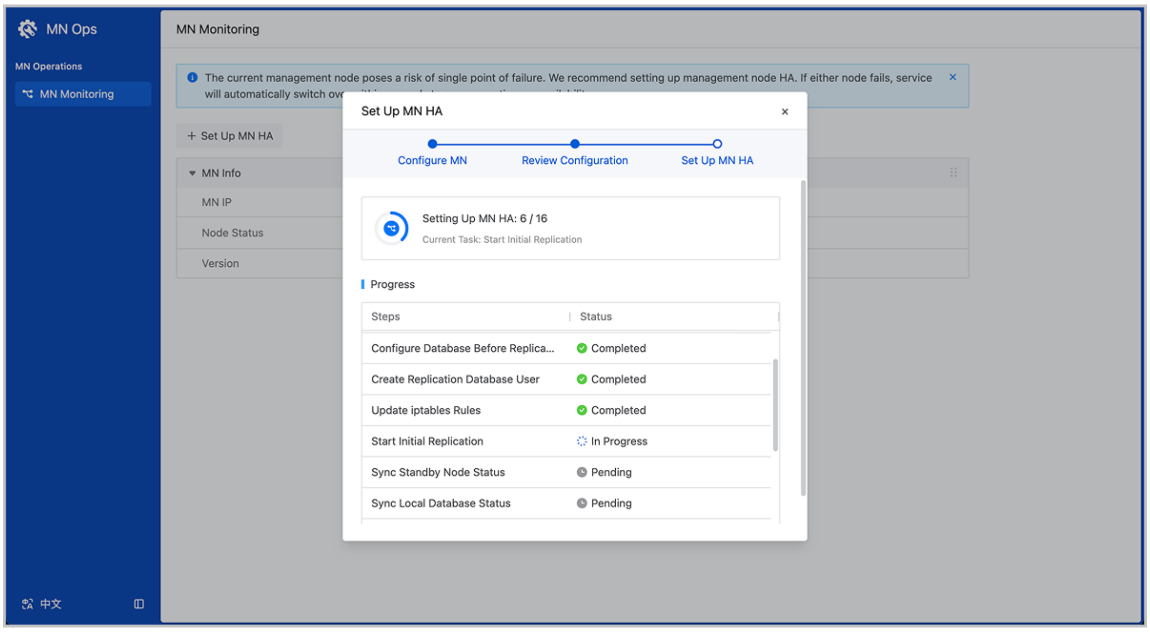
I acknowledge the above risks. To confirm to Set Up, type "**Configure**" here.

configure

d) Enter the confirmation information. Then, click **OK**.

e) In the **Set Up MN HA** step, view the addition progress and task results.

Figure 1-33: Set Up MN HA



Set Up MN HA

Setting Up MN HA: 6 / 16

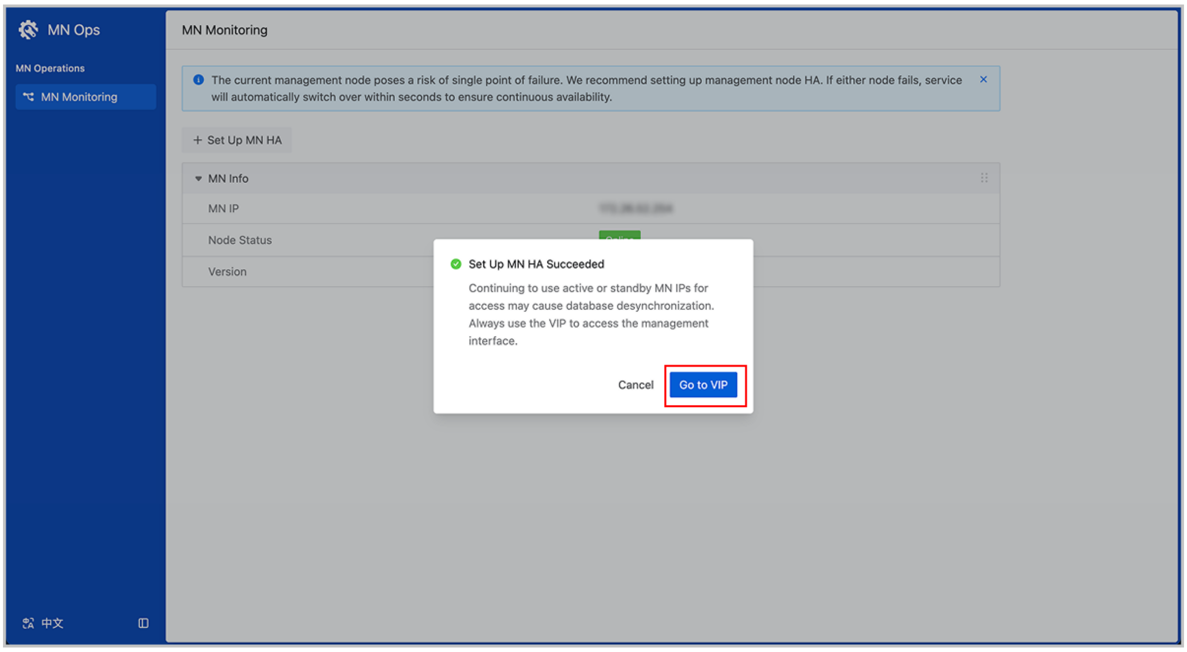
Current Task: Start Initial Replication

Progress

Steps	Status
Configure Database Before Replica...	Completed
Create Replication Database User	Completed
Update iptables Rules	Completed
Start Initial Replication	In Progress
Sync Standby Node Status	Pending
Sync Local Database Status	Pending

4. After the addition completes successfully, click **Go to VIP** to access the platform management interface through the VIP.

Figure 1-34: Go to VIP


MN Ops

MN Operations

MN Monitoring

MN Monitoring

The current management node poses a risk of single point of failure. We recommend setting up management node HA. If either node fails, service will automatically switch over within seconds to ensure continuous availability.

+ Set Up MN HA

MN Info

MN IP [redacted]

Node Status

Version

Set Up MN HA Succeeded

Continuing to use active or standby MN IPs for access may cause database desynchronization. Always use the VIP to access the management interface.

Cancel

Go to VIP

中文

1.3.2.2 Through CLI

1.3.2.2.1 Step 1: Install Operating System

In this scenario, you need to install the management node mode on both selected servers.

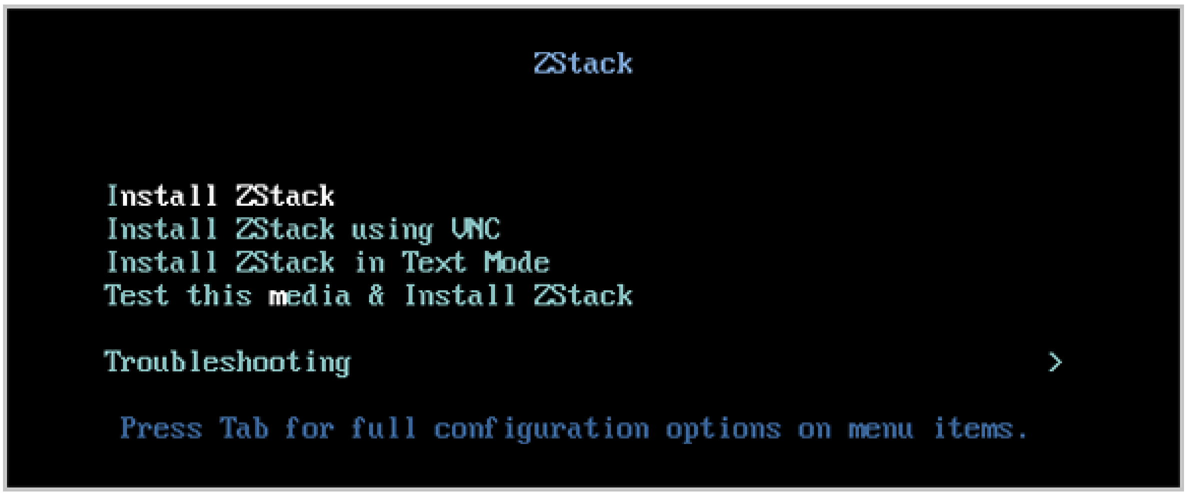
Procedure

1. Select the boot option.

   Enter the ISO boot interface and choose the default option to start the operating system installation. You can select based on your actual situation, but we recommend using the graphical user interface (GUI) for installation. If the server does not have a VGA port and only supports serial connections, you can use either VNC or text mode installation methods.

   - GUI method
   - VNC method
   - Text mode method

Figure 1-35: System Boot



ZStack

Install ZStack
Install ZStack using VNC
Install ZStack in Text Mode
Test this media & Install ZStack

Troubleshooting >

Press Tab for full configuration options on menu items.

2. Select the installation mode.

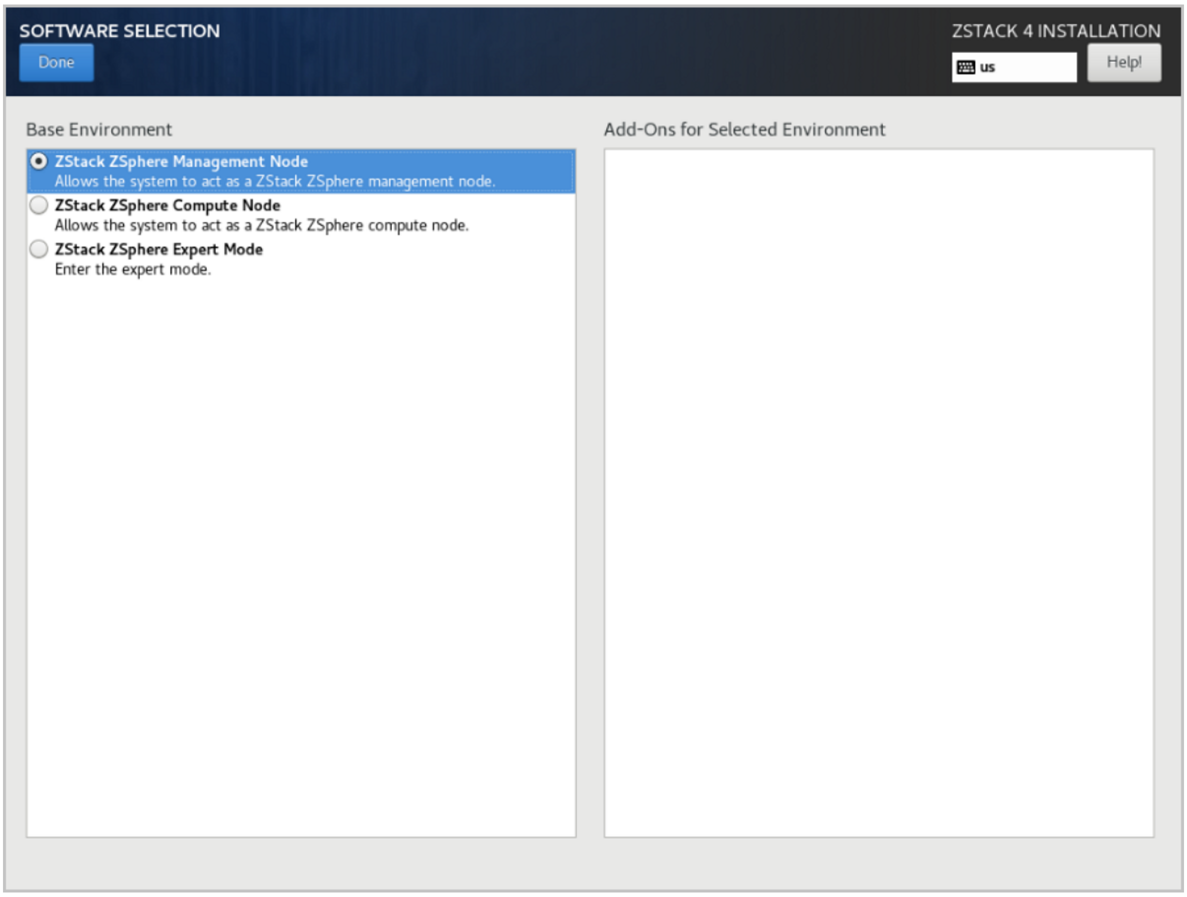
   a) On the **INSTALLATION SUMMARY** page, click **Software Selection**.

   b) On the **SOFTWARE SELECTION** page, choose the installation mode.

      Set the servers for management nodes to **ZStack ZSphere Management Node** mode. Set the other servers to **ZStack ZSphere Compute Node** mode.

   c) After selecting the installation mode, click **Done**.

Figure 1-36: Select Installation Mode



Base Environment

- ● ZStack ZSphere Management Node
  Allows the system to act as a ZStack ZSphere management node.
- ○ ZStack ZSphere Compute Node
  Allows the system to act as a ZStack ZSphere compute node.
- ○ ZStack ZSphere Expert Mode
  Enter the expert mode.

Add-Ons for Selected Environment

3. Configure the disk partitions.

a) On the **INSTALLATION SUMMARY** page, click **Installation Destination** to enter the **INSTALLATION DESTINATION** page.

b) For **Device Selection**, we recommend that you only configure the system disk. After the system is installed, you can configure other disks.

c) For **Storage Configuration**, we recommend selecting **Automatic** to automatically configure the disk partitions.

If you need to manually configure disk partitions, refer to the following guidelines based on the BIOS boot mode:

- UEFI Mode:
  - `/boot`: This directory stores the core files needed for Linux boot. We recommend allocating 1 GB of space.
  - `/boot/efi`: This directory stores the UEFI boot files. We recommend allocating 500 MB.

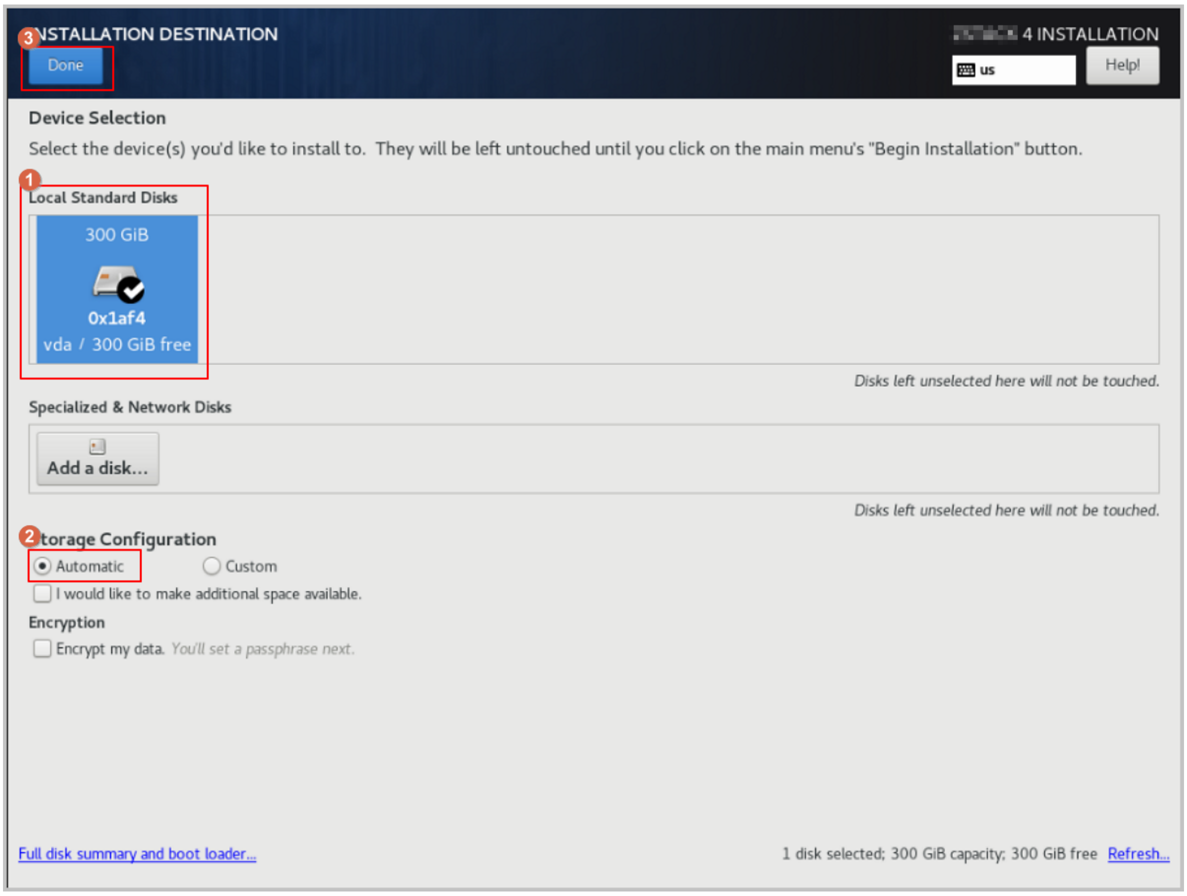
    - `swap`: This is the swap area. We recommend allocating 32 GB.
    - `/`: This is the root directory for the Linux system. We recommend allocating all remaining space.
- Legacy Mode:
    - `/boot`: This directory stores the core files needed for Linux boot. We recommend allocating 1 GB of space.
    - `swap`: This is the swap area. We recommend allocating 32 GB.
    - `/`: This is the root directory for the Linux system. We recommend allocating all remaining space.

Note:

- The above values represent the recommended partition sizes for ZStack ZSphere (total disk capacity should be greater than 300 GB).
- In Legacy mode, if the system disk capacity exceeds 2 TB, you need to configure a BIOS boot partition to support GPT partitioning. UEFI mode does not have this limitation and supports GPT partitioning.

d) Review the configuration and click **Done**.

Figure 1-37: Configure Disk Partitions


3
INSTALLATION DESTINATION
Done
[redacted] 4 INSTALLATION
us
Help!
1
2
Add a disk...
Full disk summary and boot loader...
Refresh...

Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

300 GiB
0x1af4
vda / 300 GiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

Disks left unselected here will not be touched.

Storage Configuration

● Automatic ○ Custom

□ I would like to make additional space available.

Encryption

□ Encrypt my data. *You'll set a passphrase next.*

1 disk selected; 300 GiB capacity; 300 GiB free

4. On the **INSTALLATION SUMMARY** page, click **Root Password** to set the root password for the operating system.
5. On the **INSTALLATION SUMMARY** page, click **Begin Installation** to begin installing the operating system.

1.3.2.2.2 Step 2: Configure Management Network

About this task

The following tables list the network information for the management nodes and the VIP settings for Keepalived communication in this scenario.

Table 1-1: Management Network

Server	NIC 1	NIC 2	Bond	Bridge	IP Address	Netmask	Gateway
MN 1	eth0	eth1	bond0	br_bond0	*192.168.195.200*	*255.255.0.0*	*192.168.0.1*

Server	NIC 1	NIC 2	Bond	Bridge	IP Address	Netmask	Gateway
MN 2	eth0	eth1	bond0	br_bond0	*192.168.196.125*	*255.255.0.0*	*192.168.0.1*

Table 1-2: VIP

-	IP Address	Netmask
VIP	*192.168.199.151*	*255.255.0.0*

Note:

- The VIP is used to log in to the UI of the management node. Avoid using the VIP for SSH logins to the management nodes.
- The above data is for example only. You need to modify it based on your actual deployment environment.
- The gateway must be provided by physical network devices and will also serve as **network status arbitration detection**.

Procedure

1. Log in to the **MN 1** operating system and run the following commands.

```
# Create the bonded NIC bond0
[root@localhost ~]# zs-bond-lacp -c bond0

# Add NICs eth0 and eth1 to bond0
[root@localhost ~]# zs-nic-to-bond -a bond0 eth0
[root@localhost ~]# zs-nic-to-bond -a bond0 eth1

# After configuring the link aggregation, you need to set up LACP
aggregation on the corresponding switch ports.

# Create the bridge br_bond0 and specify network IP, netmask, and
gateway
[root@localhost ~]# zs-network-setting -b bond0 192.168.195.200 255.
255.0.0 192.168.0.1

# Check if the aggregated port bond0 was created successfully
[root@localhost ~]# zs-show-network
...
------------------------------------------------------------------------------
| Bond Name   | SLAVE(s)          | BONDING_OPTS
              |
------------------------------------------------------------------------------
| bond0       | eth0              | miimon=100 mode=4 xmit_hash_policy=
layer2+3        |
|             | eth1              |
                |
-------------------------------------------------------------------------------
```

2. Log in to the **MN 2** operating system and run the similar configuration commands.

Note:

- After adding eth0 and eth1 to bond0, you need to configure LACP aggregation on the corresponding switch ports. Otherwise, network communication will be disrupted.
- After creating the bridge through bond0, the bridge will be named as br_bond0 to provide management network services.
- You need to configure the bridge's IP address, netmask, and gateway according to your actual network environment.
- Once you complete the management network configuration, use the `ping` command to test it. If configured correctly, the management network IP addresses of the two management nodes should be able to `ping` each other.
- A 10 Gigabit or higher bandwidth is recommended for the management network. A 1 Gigabit bandwidth is acceptable if the network is deployed independently.

1.3.2.2.3 Step 3: Configure Business Network

About this task

The following table lists the configuration for the business network in this scenario.

Table 1-3: Business Network

Server	NIC 1	NIC 2	Bond	Bridge	IP Address	Netmask	Gateway
MN 1	em1	em2	bond1	-	-	-	-
MN 2	em1	em2	bond1	-	-	-	-

Procedure

1. Log in to the **MN 1** operating system and run the following commands.

```
# Create the bonded NIC bond1
[root@localhost ~]# zs-bond-lacp -c bond1

# Add NICs em1 and em2 to bond1
[root@localhost ~]# zs-nic-to-bond -a bond1 em1
[root@localhost ~]# zs-nic-to-bond -a bond1 em2

# After configuring the link aggregation, you need to set up LACP
aggregation on the corresponding switch ports.
```

```
# You do not need to create a bridge for business network

# Check if the aggregated port bond1 was created successfully
[root@localhost ~]# zs-show-network
...
------------------------------------------------------------------------------
| Bond Name   | SLAVE(s)        | BONDING_OPTS
              |
------------------------------------------------------------------------------
| bond1       | em1            | miimon=100 mode=4 xmit_hash_policy=
layer2+3        |
|             | em2            |
               |
------------------------------------------------------------------------------
```

2. Log in to the **MN 2** operating system and run the similar configuration commands.

Note:

After adding em1 and em2 to bond1, you need to configure LACP aggregation on the corresponding switch ports. Otherwise, network communication will be disrupted.

1.3.2.2.4 Step 4: Install HA Suite

This section introduces two methods for installing the high availability (HA) suite:

- *Install Through CLI*
- *Install Through Configuration File*

Note:

When installing the HA suite with the same configuration, the CLI method takes precedence over the configuration file method.

1.3.2.2.4.1 Install Through CLI

In this scenario, you have installed both servers as the ZStack ZSphere management nodes. To enable high availability for both nodes, you only need to install the **HA suite** on one of the nodes. If you install the HA suite on **MN 1**, MN 1 becomes the active management node and MN 2 becomes the standby management node.

Procedure

1. Import the HA suite.

   Log in to the **MN 1** operating system. Import the HA suite to MN 1 and unzip the HA suite.

```
# Use scp to import HA suite to MN 1
[root@localhost ~]# ls
ZStack-ZSphere-Multinode-HA-Suite.tar.gz
```

```
# Unzip the suite to get two executable files: zsha2 and zstack-
hamon
[root@localhost ~]# tar zxvf ZStack-ZSphere-Multinode-HA-
Suite.tar.gz
zsha2 //Installation and management program for management node high
 availability
zstack-hamon //Monitoring program for management node high
 availability
```

2. Initialize HA.

   Run the following command to install the HA suite on **MN 1**:

```
[root@localhost ~]# chmod +x zsha2 zstack-hamon
[root@localhost ~]# ./zsha2 install-ha -nic br_bond0 -gateway 192.
168.0.1 -slave "root:password@192.168.196.125" \
-vip 192.168.199.151 -myip 192.168.195.200 -db-root-pw zstack.mysql.
password -time-server 192.168.196.125 -cidr 192.168.0.0/16 -yes
```

Note:

- After executing the installation command, the system will automatically back up the databases of the active and standby management nodes before proceeding with the installation.
- To install the high availability suite, ensure that **zsha2** and **zstack-hamon** are in the same directory. During the installation, **zsha2** will automatically deploy **zstack-hamon** and the related configuration files.

3. Check the management nodes status.

   After initializing the HA suite, run the following command to check the status of the management nodes:

```
# Check the status of Management Node 1
[root@localhost ~]# zsha2 status
Status report from 192.168.195.200
=================================
Owns virtual address:            yes  // MN 1 has acquired the VIP.
Only one management node can acquire the VIP at any given time.
Self 192.168.195.200 reachable:   yes // MN1 is reachable.
Gateway 192.168.0.1 reachable:    yes // Current gateway is
reachable.
VIP 192.168.199.151 reachable:    yes // VIP is reachable.
Peer 192.168.196.125 reachable:   yes // MN 2 is reachable.
Keepalived status:               active // Keepalived service is
active.
ZStack HA Monitor:               active // HA monitoring service is
active.
MySQL status:                    mysqld is alive // Database is
functioning normally.
MN status: Running [PID:6500] // Management node is operating
normally.
UI status: Running [PID:9785] https://192.168.195.200:443 // UI is
functioning normally.
```

```
Slave Status:
-------------
             Slave_IO_Running: Yes // Slave IO is running normally.
            Slave_SQL_Running: Yes // Slave SQL is running normally.
                   Last_Error:
        Seconds_Behind_Master: 0
                Last_IO_Error:
               Last_SQL_Error:

Warning: Permanently added '192.168.196.125' (ECDSA) to the list of
known hosts.
Status report from 192.168.196.125 // Check the status of Management
 Node 2
================================
Owns virtual address:            no
Self 192.168.196.125 reachable:    yes
Gateway 192.168.0.1 reachable:    yes
VIP 192.168.199.151 reachable:     yes
Peer 192.168.195.200 reachable:   yes
Keepalived status:               active
ZStack HA Monitor:               active
MySQL status:                    mysqld is alive

Slave Status:
-------------
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
                   Last_Error:
        Seconds_Behind_Master: 0
                Last_IO_Error:
               Last_SQL_Error:

Note: visit ZStack UI with https://192.168.199.151:443
```

Note:

During the installation of the HA suite, SSH password-free login has been automatically configured for both management nodes.

1.3.2.2.4.2 Install Through Configuration File

In this scenario, you have installed both servers as the ZStack ZSphere management nodes.

To enable high availability for both nodes, you only need to install the **HA suite** on one of the nodes. If you install the HA suite on **MN 1**, MN 1 becomes the active management node and MN 2 becomes the standby management node.

Procedure

1. Import the HA suite.

   Log in to the **MN 1** operating system. Import the HA suite to MN 1 and unzip the HA suite.

```
# Use scp to import HA suite to MN 1
[root@localhost ~]# ls
ZStack-ZSphere-Multinode-HA-Suite.tar.gz
```

```
# Unzip the suite to get two executable files: zsha2 and zstack-
hamon
[root@localhost ~]# tar zxvf ZStack-ZSphere-Multinode-HA-
Suite.tar.gz
zsha2 //Installation and management program for management node high
 availability
zstack-hamon //Monitoring program for management node high
 availability
```

2. Create the configuration fie.

   Run the following commands to create the initialization configuration file for the HA suite:

```
[root@localhost ~]# chmod +x zsha2 zstack-hamon
[root@localhost ~]# ./zsha2 sample-config > zs-install.config
[root@localhost ~]# cat zs-install.config
{
  "gateway": "192.168.0.1", // Arbiter gateway for active and
standby management nodes
  "virtualIp": "192.168.199.151", // The VIP for Keepalived
communication
  "myIp": "192.168.195.200", // Specify the local IP
  "peerIp": "192.168.196.125", // Specify the Peer management node
IP
  "peerSshUser": "root", // Specify the SSH username for the Peer
management node
  "peerSshPass": "password", // Specify the SSH password for the
Peer management node
  "peerSshPort": 22, // Specify the SSH port for the Peer management
 node
  "dbRootPass": "zstack.mysql.password", // Specify the root
password for the database on both management nodes (must be the same
)
  "interface": "br_bond0", //Name of the physical device for
configuring the VIP. Typically a management network bridge in
production environments
  "timeServer": "192.168.196.125" //Specify the time synchronization
 server for unified time synchronization
}
```

3. Initialize HA.

   Run the following command to install the HA suite:

```
[root@localhost ~]# ./zsha2 install-ha -config zs-install.config
```

Note:

- After executing the installation command, the system will automatically back up the databases of the active and standby management nodes before proceeding with the installation.

- To install the high availability suite, ensure that **zsha2** and **zstack-hamon** are in the same directory. During the installation, **zsha2** will automatically deploy **zstack-hamon** and the related configuration files.

4. Check the management nodes status.

After initializing the HA suite, run the following command to check the status of the management nodes:

```
# Check the status of Management Node 1
[root@localhost ~]# zsha2 status
Status report from 192.168.195.200
=================================
Owns virtual address:            yes  // MN 1 has acquired the VIP.
Only one management node can acquire the VIP at any given time.
Self 192.168.195.200 reachable:   yes // MN1 is reachable.
Gateway 192.168.0.1 reachable:    yes // Current gateway is
reachable.
VIP 192.168.199.151 reachable:    yes // VIP is reachable.
Peer 192.168.196.125 reachable:   yes // MN 2 is reachable.
Keepalived status:               active // Keepalived service is
active.
ZStack HA Monitor:               active // HA monitoring service is
active.
MySQL status:                    mysqld is alive // Database is
functioning normally.
MN status: Running [PID:6500] // Management node is operating
normally.
UI status: Running [PID:9785] https://192.168.195.200:443 // UI is
functioning normally.

Slave Status:
-------------
             Slave_IO_Running: Yes // Slave IO is running normally.
            Slave_SQL_Running: Yes // Slave SQL is running normally.
                   Last_Error:
        Seconds_Behind_Master: 0
                Last_IO_Error:
               Last_SQL_Error:

Warning: Permanently added '192.168.196.125' (ECDSA) to the list of
known hosts.
Status report from 192.168.196.125 // Check the status of Management
 Node 2
================================
Owns virtual address:            no
Self 192.168.196.125 reachable:    yes
Gateway 192.168.0.1 reachable:    yes
VIP 192.168.199.151 reachable:     yes
Peer 192.168.195.200 reachable:   yes
Keepalived status:               active
ZStack HA Monitor:               active
MySQL status:                    mysqld is alive

Slave Status:
-------------
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
                   Last_Error:
```

```
        Seconds_Behind_Master: 0
                Last_IO_Error:
               Last_SQL_Error:

Note: visit ZStack UI with https://192.168.199.151:443
```

Note:

During the installation of the HA suite, SSH password-free login has been automatically configured for both management nodes.

1.4 Manage ZStack ZSphere Service

Check MN Service Status

You can use the `zstack-ctl status` command to check the running status of the services related to the ZStack ZSphere management node.

```
[root@localhost ~]# zstack-ctl status
ZSTACK_HOME: /usr/local/zstack/apache-tomcat/webapps/zstack
zstack.properties: /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-
INF/classes/zstack.properties
log4j2.xml: /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/
classes/log4j2.xml
PID file: /usr/local/zstack/management-server.pid
log file: /usr/local/zstack/apache-tomcat/logs/management-server.log
version: 4.10.25 (ZStack-enterprise 4.10.25)
MN status: Running [PID:123135]
UI status: Running [PID:795] https://10.0.0.254:443
```

You can also use the `zstack-ctl ui_status` command to check the status of the Web UI separately.

```
[root@localhost ~]# zstack-ctl ui_status
```

```
UI status: Running [PID:8459] https://10.0.0.254:443
```

Change MN Service Status

If you need to restart the management node service without restarting the Web UI service during use, run the following command:

```
zstack-ctl restart_node
```

It is not recommended to stop and restart all services at once during use. If you must restart all services, you can run the following command:

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

If the management node stops services due to maintenance or other issues, you need to start the services manually. To start the ZStack ZSphere service, run the following command:

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

Check Service Status of MN HA

You can run the `zsha2 status` command to check if the zsha2 service is running normally.

Export Log of MN HA

You can run the following commands to collect logs related to zsha2 service:

```
[root@localhost ~]# zsha2 collect-log
Collecting logs ...
Collected log: zsha2-log-2018-09-17T154358+0800.tgz

# Unpack the log archive
[root@localhost ~]# tar zxvf zsha2-log-2021-01-17T154358+0800.tgz
tmp/zsha2-log588815976/
tmp/zsha2-log588815976/zsha2-status.log
tmp/zsha2-log588815976/zstack-ha.log
tmp/zsha2-log588815976/keepalived.data
tmp/zsha2-log588815976/zs-vip-192.168.199.151.log
tmp/zsha2-log588815976/keepalived_status.log
```

2 ZStack ZSphere Upgrade

2.1 Upgrade Management Node

This section uses H84r as an example to introduce a step-by-step guide for upgrading a single management node environment.

Procedure

1. Check the current environment version and the operating system version.

   ```
   [root@localhost ~]# zstack-ctl status
   [root@localhost ~]# cat /etc/readhat-release
   ```

2. Obtain the upgrade packages.

   Download the zstack-upgrade script, ISO software package, upgrade packages, and the HA suite for management node as needed.

3. Disable the HA policy.

   Before the upgrade, you need to disable the global switch for virtual machine high availability to avoid triggering it accidentally, which could affect the upgrade. After the upgrade is complete, manually enable the HA policy.

   a) Log in to ZStack ZSphere.

   b) Click **Business Reliability** > **HA Policy** to enter the **HA Policy** page.

   c) Disable the HA policy switch.

4. Back up the database and upgrade script.

   Log in to the management node system and then run the following commands to back up the database and upgrade script for emergency recovery:

   ```
   # Back up the database to the /var/lib/zstack/mysql-backup/
    directory
   [root@localhost ~]# zstack-ctl dump_mysql --file-name zstack-db-
   backup

   # Back up the upgrade script to the /root/ directory
   [root@localhost ~]# cp /usr/local/bin/zstack-upgrade /root/zstack-
   upgrade-bk
   ```

5. Upgrade ZStack ZSphere.

   ```
   # Two offline upgrade methods are supported. The first method is
    recommended.
   # Method 1: Upgrade the local repository and management services
   [root@zstack-1 opt]# zstack-upgrade ZStack-ZSphere-x86_64-
   DVD-4.10.25-H84r.iso
   ```

```
# Method 2: First upgrade the local repository and then upgrade the
 management services
[root@zstack-1 opt]# zstack-upgrade -r ZStack-ZSphere-x86_64-
DVD-4.10.25-H84r.iso
[root@zstack-1 opt]# bash ZStack-ZSphere-installer-4.10.25.bin -u -P
 MYSQL_ROOT_PASSWORD
```

Note:

- If the database root password uses the system default password **zstack.mysql.password**, you can omit the `-P MYSQL_ROOT_PASSWORD` parameter.
- Before executing the `zstack-upgrade` command, ensure that the prepared ISO is based on version H84r to avoid using other ISOs that may overwrite the local source.

6. Clear the browser cache.

   To ensure that the new features work properly, it is recommended that after the upgrade is complete, you log in to the UI management interface and manually clear the browser cache by pressing `Ctrl+F5` or `Ctrl+Shift+R`.

7. Enable the HA policy.

2.2 Upgrade MN HA Environment

This section uses H84r as an example to introduce a step-by-step guide for upgrading a management node environment that has HA configured.

Procedure

1. Check the current environment version and the operating system version.

```
[root@localhost ~]# zstack-ctl status
[root@localhost ~]# cat /etc/readhat-release
```

2. Obtain the upgrade packages.

   Download the zstack-upgrade script, ISO software package, upgrade packages, and the HA suite for management node as needed.

3. Disable the HA policy.

   Before the upgrade, you need to disable the global switch for virtual machine high availability to avoid triggering it accidentally, which could affect the upgrade. After the upgrade is complete, manually enable the HA policy.

   a) Log in to ZStack ZSphere.

   b) Click **Business Reliability** > **HA Policy** to enter the **HA Policy** page.

   c) Disable the HA policy switch.

4. **4.** Back up the database and upgrade script.

   Log in to the management node system and then run the following commands to back up the database and upgrade script for emergency recovery:

   ```
   # Back up the database to the /var/lib/zstack/mysql-backup/
    directory
   [root@localhost ~]# zstack-ctl dump_mysql --file-name zstack-db-
   backup

   # Back up the upgrade script to the /root/ directory
   [root@localhost ~]# cp /usr/local/bin/zstack-upgrade /root/zstack-
   upgrade-bk
   ```

5. Obtain the IP address of the management node where the VIP is located.

   Run the following command to obtain the IP address of the management node where the VIP is located. The node with VIP marked as yes in the returned results is the management node where the VIP is located:

   ```
   [root@localhost ~]# zsha2 status
   ```

6. Unpack the HA suite and grant executable permission.

   On the management node where the VIP is located, run the following commands in sequence to unpack the HA suite and grant executable permissions to the `zsha2` and `zstack-hamon` files:

   ```
   # Unpack the HA suite
   [root@localhost ~]# tar zxvf ZStack-ZSphere-Multinode-HA-
   Suite.tar.gz

   # Grant executable permissions
   [root@localhost ~]# chmod +x zsha2 zstack-hamon
   ```

7. Upgrade the HA suite.

   On the management node where the VIP is located, run the following command to upgrade the HA suite:

   ```
   [root@localhost ~]# ./zsha2 upgrade-ha
   ```

8. Run the `zsha2 version` command to check if the `commit id` matches the one in the latest version package.

9. Upgrade ZStack-ZSphere.

On the management node where the VIP is located, run the following command to upgrade the virtualization platform:

```
zsha2 upgrade-mn -peerpass password ZStack-ZSphere-x86_64-
DVD-4.10.25-H84r.iso
```

Note:

`-peerpass` is optional and can be set to the SSH login password for the peer management node.

10. Clear the browser cache.

    To ensure that the new features work properly, it is recommended that after the upgrade is complete, you log in to the UI management interface and manually clear the browser cache by pressing `Ctrl+F5` or `Ctrl+Shift+R`.

11. Enable the HA policy.