NexaSphere

Installation and Initialization

Version: V2.1.1

Issue: V2.1.1

Nexavm Technologies AG

NEXAVM

Copyright Statement

Copyright © 2026 Nexavm Technologies AG. All rights reserved.

No part of this document may be excerpted, reproduced, or distributed in any form without prior written permission from Nexavm Technologies AG.

Trademark Notice

NexaSphere and other trademarks of Nexavm Technologies AG are trademarks of Nexavm Technologies AG.

All other trademarks or registered trademarks mentioned in this document are the property of their respective owners.

Notice

The products, services, and features you purchase are governed by the applicable commercial contracts and terms of Nexavm Technologies AG. Some products, services, or features described in this document might not be included in your purchase or available for your use. Unless otherwise agreed in the applicable contract, Nexavm Technologies AG makes no express or implied representations or warranties regarding the contents of this document.

This document might be updated from time to time due to product version upgrades or other reasons. Unless otherwise agreed, this document is provided for guidance only. The statements , information, and recommendations in this document do not constitute any express or implied warranty.

Contents

Copyright Statement..... I
Installation and Initialization..... 1
1.1 Overview..... 1
1.2 Planning and Preparation..... 2
1.2.1 Hardware Requirements..... 2
1.2.2 Network Planning..... 3
1.2.3 Prepare Software Packages..... 4
1.2.4 Create Installation Media..... 5
1.2.4.1 Create a USB Drive with Rufus..... 5
1.2.4.2 Create a USB Drive with Fedora Media Writer..... 9
1.2.5 Configure Servers..... 9
1.3 Install the Management Node..... 10
1.3.1 Bonded NIC Deployment..... 10
1.3.2 Single NIC Deployment..... 23
1.3.3 Install with TUI..... 30
1.4 Set Up Management Node HA..... 34
1.4.1 Set Up with the UI..... 35
1.5 Log in to NexaSphere..... 40
1.6 Initialize NexaSphere..... 41
1.6.1 Initialize Manually..... 41
1.6.2 Restore from Backup Data..... 44
Glossary..... 46

1 Installation and Initialization

1.1 Overview

About This Guide

This guide describes how to complete pre-deployment preparation, management node installation, management node HA setup, basic service checks, first login, and environment initialization for NexaSphere.

Intended Audience

This guide is intended for administrators, implementation engineers, and O&M engineers who are responsible for deploying and initializing NexaSphere. Readers should be familiar with server hardware, basic networking, operating system installation, and virtualization infrastructure deployment.

Installation Modes

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

Installation Mode	Installed Content	Applicable Scenario
Management Node Mode	• Base operating system • Dependencies such as `MariaDB` and `CloudBus` message bus	Suitable for installing a management node for the virtualization platform.
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 Preparation

Before installing NexaSphere, complete hardware, network, software package, and server configuration preparation to ensure that the servers can boot from the installation media and meet the deployment requirements for management nodes, compute nodes, and subsequent business resources.

This chapter describes the basic conditions that must be confirmed before deployment, including hardware requirements, network planning, software package preparation, installation media creation, and server configuration. After completing these preparations, you can start installing the management node.

1.2.1 Hardware Requirements

Basic Hardware Requirements

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

- Basic demonstration environment: The server must have at least 4 CPU cores and 8 GB of memory.
- Production environment:
  - Management node configuration: In 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 lists the recommended server hardware configuration for both basic demonstration environments 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.

Device		Configuration
	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

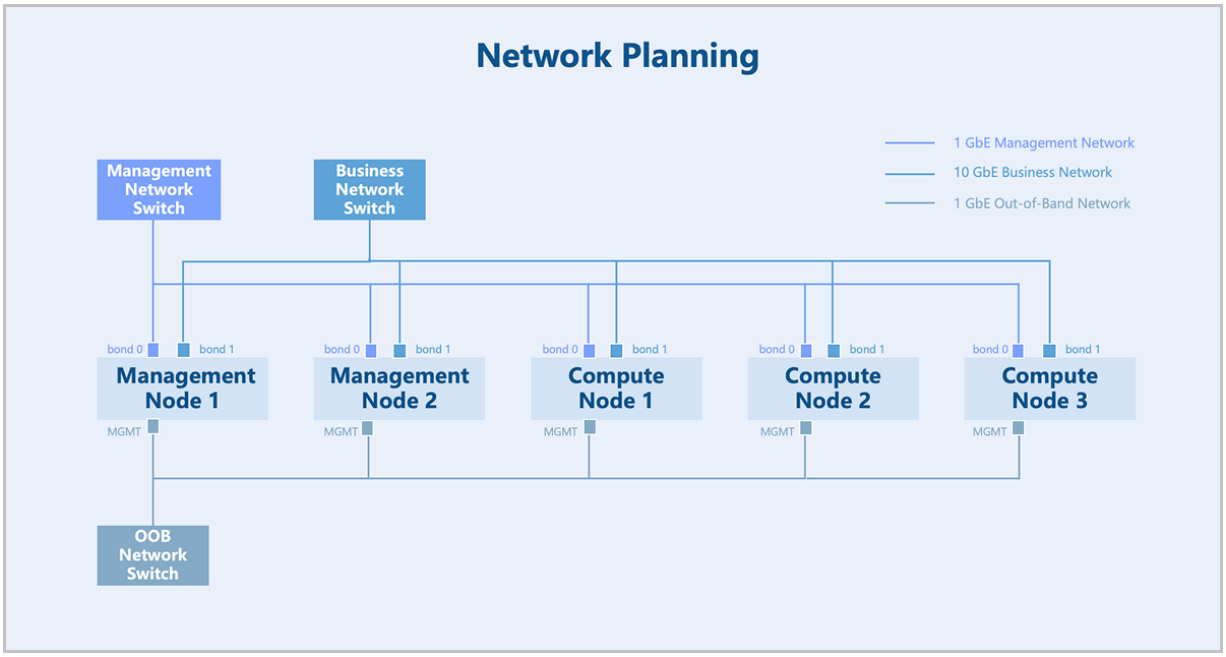
You need to plan your server resources according to your production needs. In a large data center with sufficient resources, we recommend deploying two servers as management nodes to control the entire virtualization platform. These two management nodes provide high availability. If one management node 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

A typical data center consists of several servers with different functions and two independent network environments.

Figure 1-1: 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.
- NexaSphere 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 Software Packages

Software Package Description

NexaSphere ISO is built on Helix, a self-developed virtualization kernel that runs between the infrastructure layer and upper-layer guest operating systems. Helix integrates hardware drivers,

macro kernel components, virtual agents, and other required components. When guest operating systems access underlying hardware resources, Helix masks differences across heterogeneous hardware, removes the dependency on physical hardware drivers, and improves hardware compatibility, reliability, availability, scalability, and performance in the virtualization environment.

Installing NexaSphere does not require Internet access or a yum repository. The installation can be completed offline.

Software Package List

The following table lists the software packages used to install NexaSphere:

Server Architecture	Software Package Name
x86	NexaSphere-x86_64-DVD-2.1.1-H84r.iso
	NexaSphere-x86_64-DVD-2.1.1-KylinV10SP3.iso
ARM	NexaSphere-aarch64-DVD-2.1.1-H22e.iso
	NexaSphere-aarch64-DVD-2.1.1-KylinV10SP3.iso

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

1.2.4 Create Installation Media

After obtaining the NexaSphere ISO image file, write the ISO image to a USB drive so that the physical server can boot the installer from the USB drive.

You can create the installation media with Rufus or Fedora Media Writer based on your local operating system and tool preference. After the installation media is created, set the USB drive as the boot media in the server BIOS or boot menu.

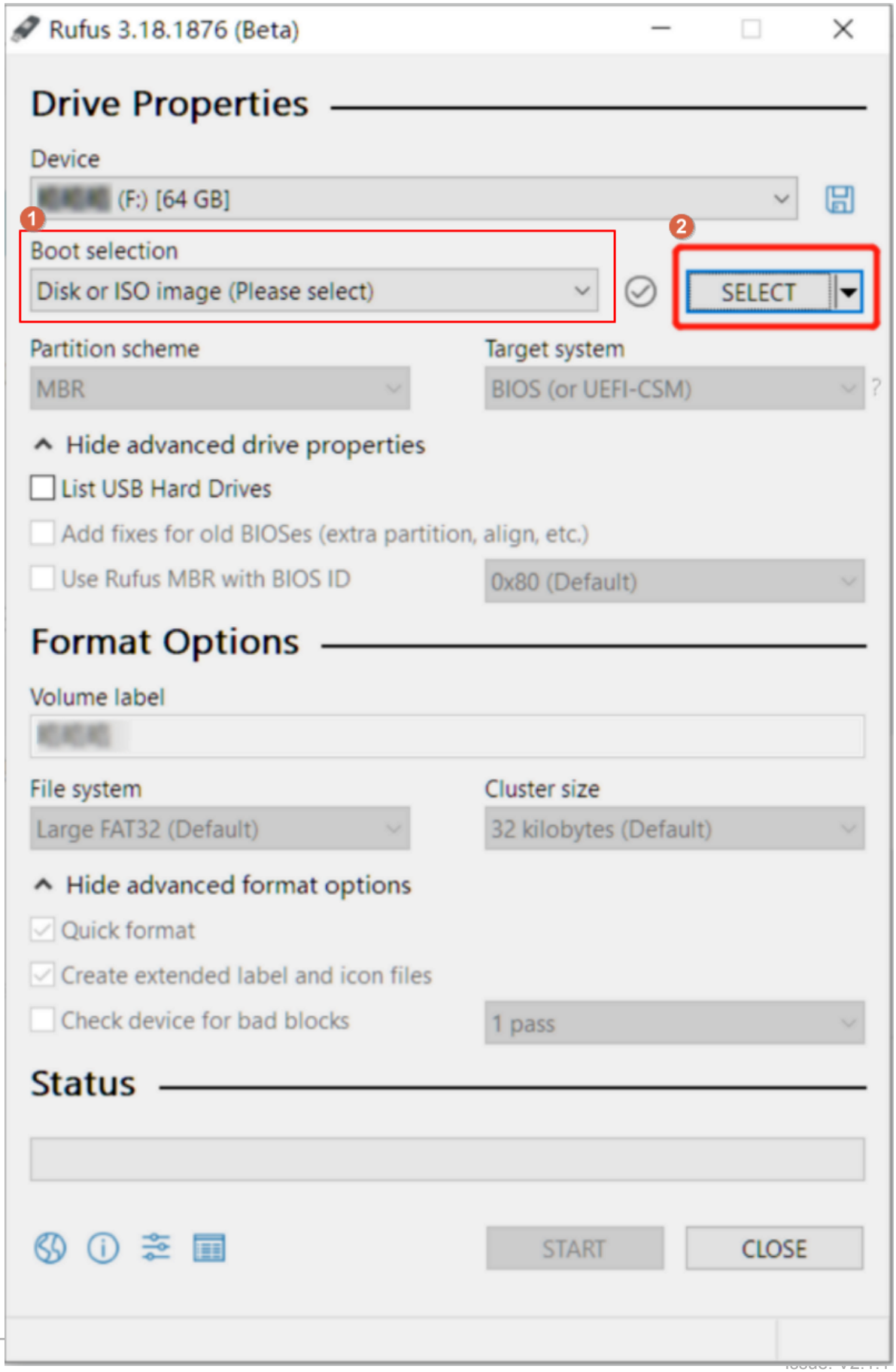
1.2.4.1 Create a USB Drive with Rufus

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 1-2: Select ISO Image



2. Burn the image.

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

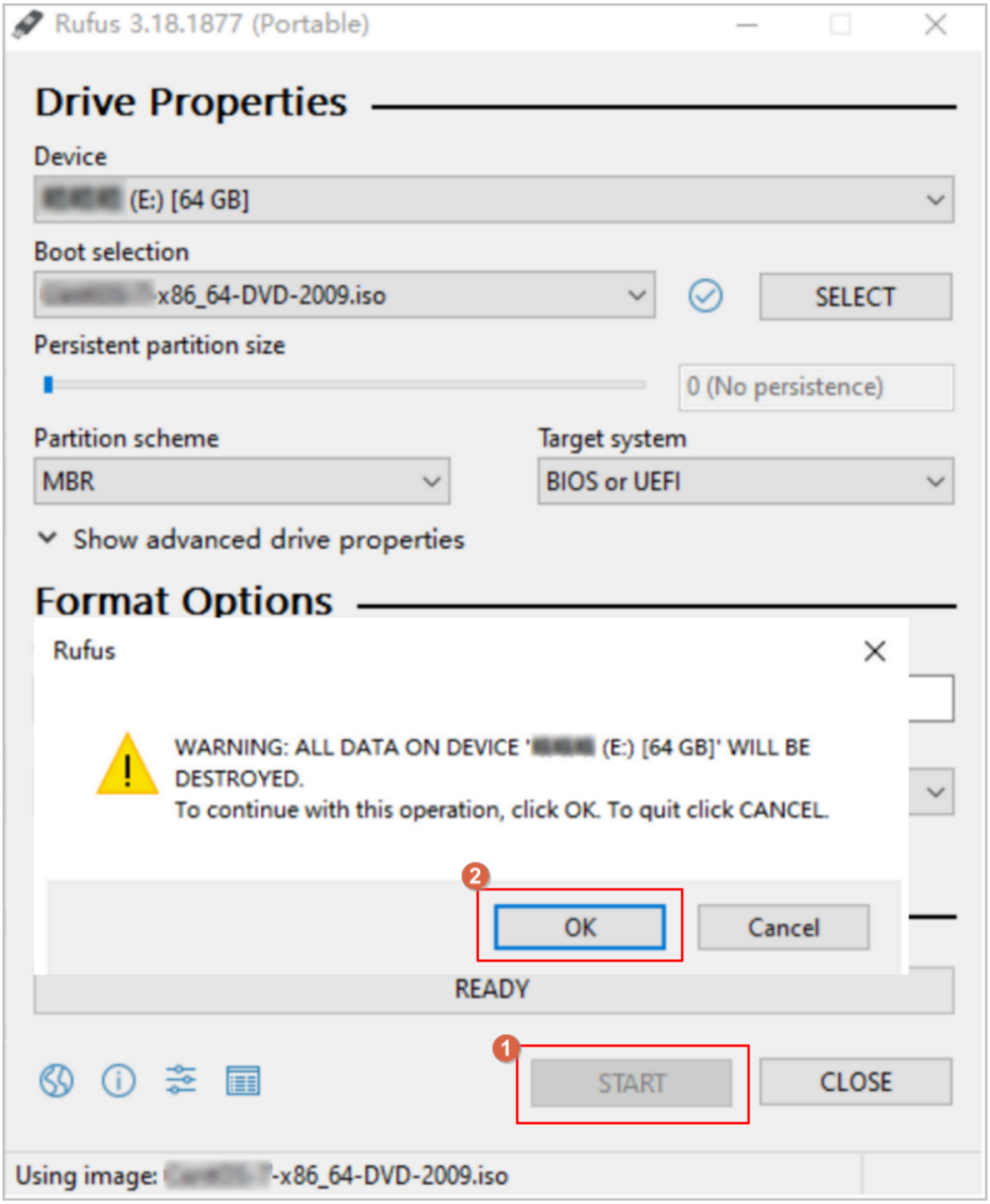
   b) Confirm the warning message.

   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 1-3: Burn the Image



What's next

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

1.2.4.2 Create a USB Drive with 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.
   a) Connect your USB drive and open Fedora Media Writer.
   b) Click **Custom Image** to open the ISO image file that you obtained.
2. Burn the image.
   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's next

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

1.2.5 Configure Servers

Server Configuration Check

Based on your actual network planning, rack, cable, and power on the servers and network equipment. Then, start the servers, enter BIOS, and 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 the Management Node

The management node hosts NexaSphere management services, Web UI, and basic control services. It is the entry point for completing platform deployment and managing resources after deployment.

Select an installation method based on your network planning and deployment scenario. In production environments, bonded NIC deployment is typically used to improve management network reliability. In simple verification scenarios or single-NIC environments, you can use single NIC deployment. If you need to configure the management node from a text interface after installation, use the TUI installation path.

After installation, check the NexaSphere service status and determine whether to set up management node HA based on business continuity requirements.

1.3.1 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

2. Review the installation configuration summary.

   This page displays the system installation configuration. You can modify the configuration as needed. By default, NexaSphere 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.

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 **Management Node** mode. Set the other servers to **Compute Node** mode.

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

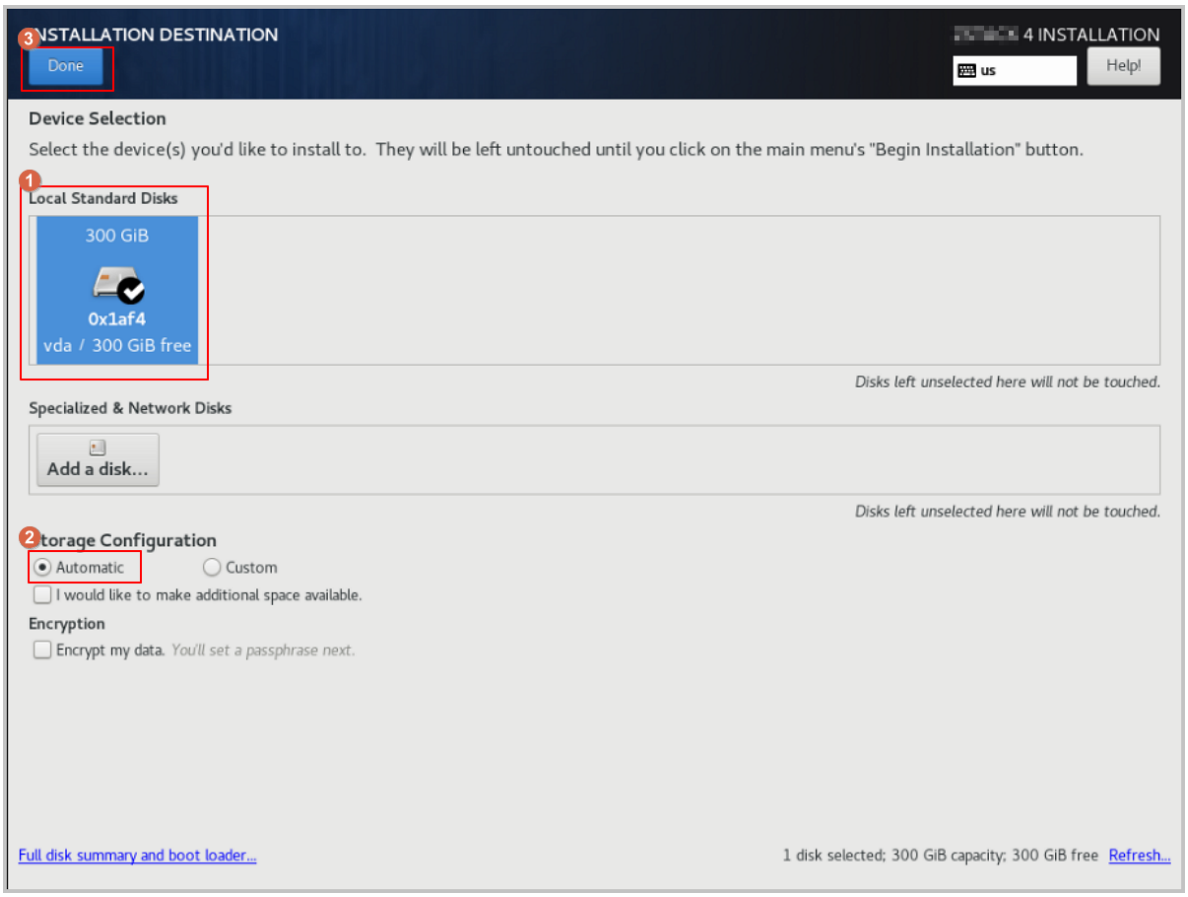
      - UEFI Mode:
        - `/boot`: This directory stores the core files needed for Linux boot. We recommend allocating 1 GB of space.
        - `/boot/efi`: This directory stores the UEFI boot files. We recommend allocating 500 MB.
        - *swap*: This is the swap area. We recommend allocating 32 GB.
        - `/`: 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 NexaSphere (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 1-4: Configure Disk Partitions

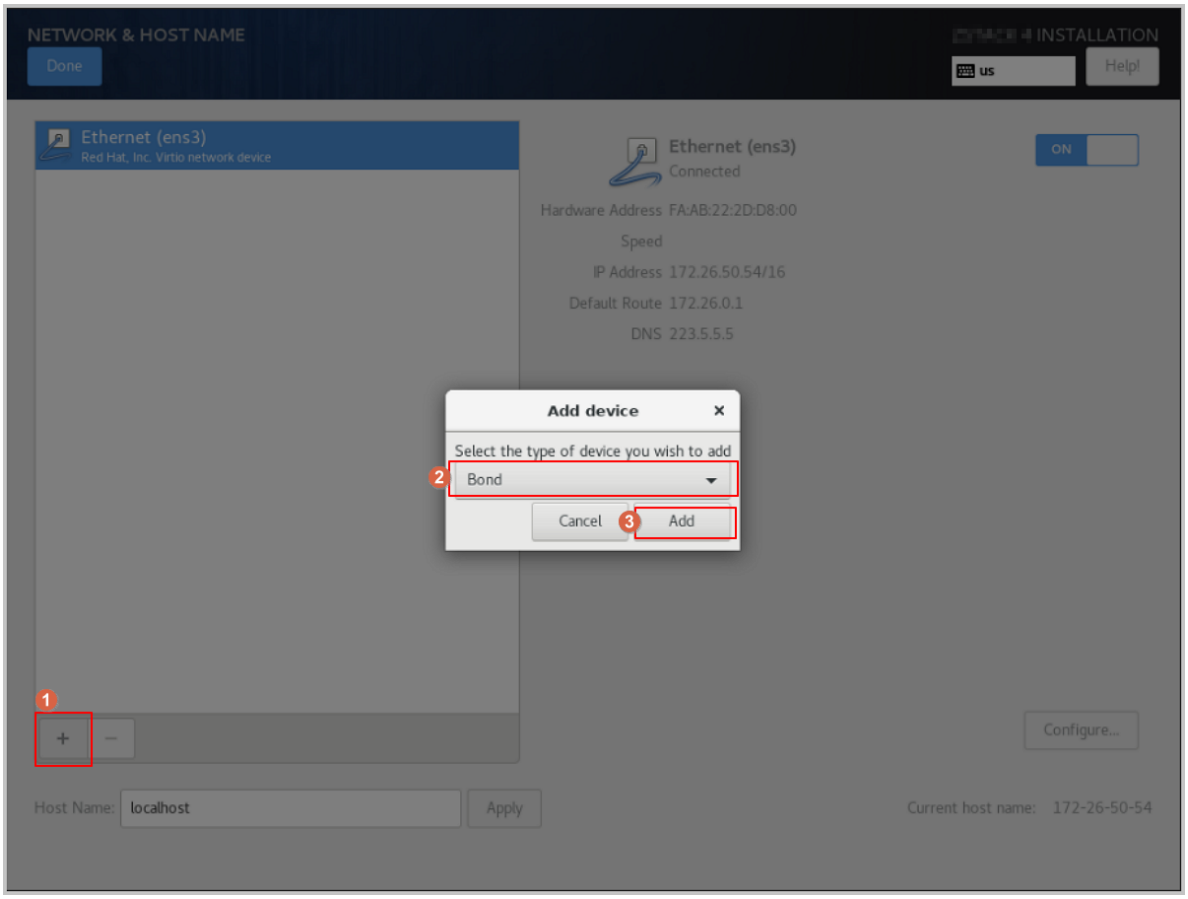


5. Add a bond device.

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 1-5: Add Bond Device

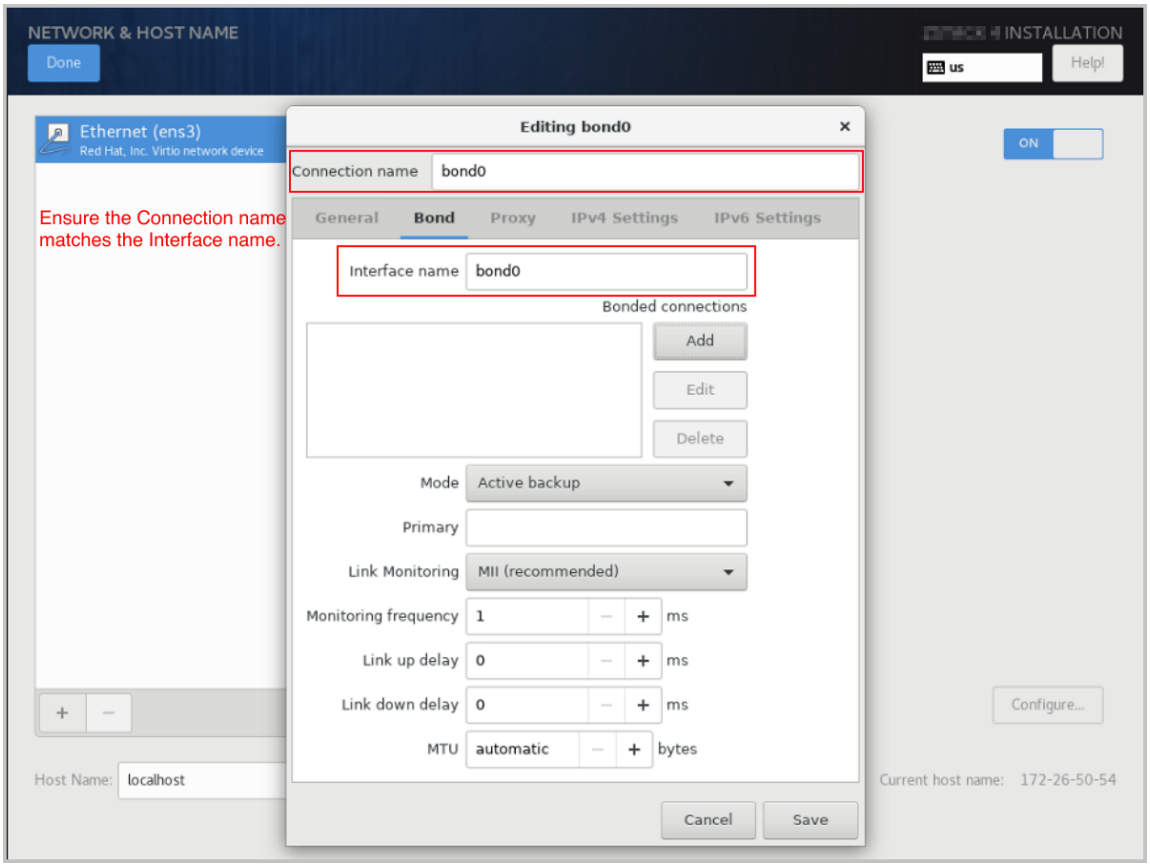


6. Add a Bond Slave.

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

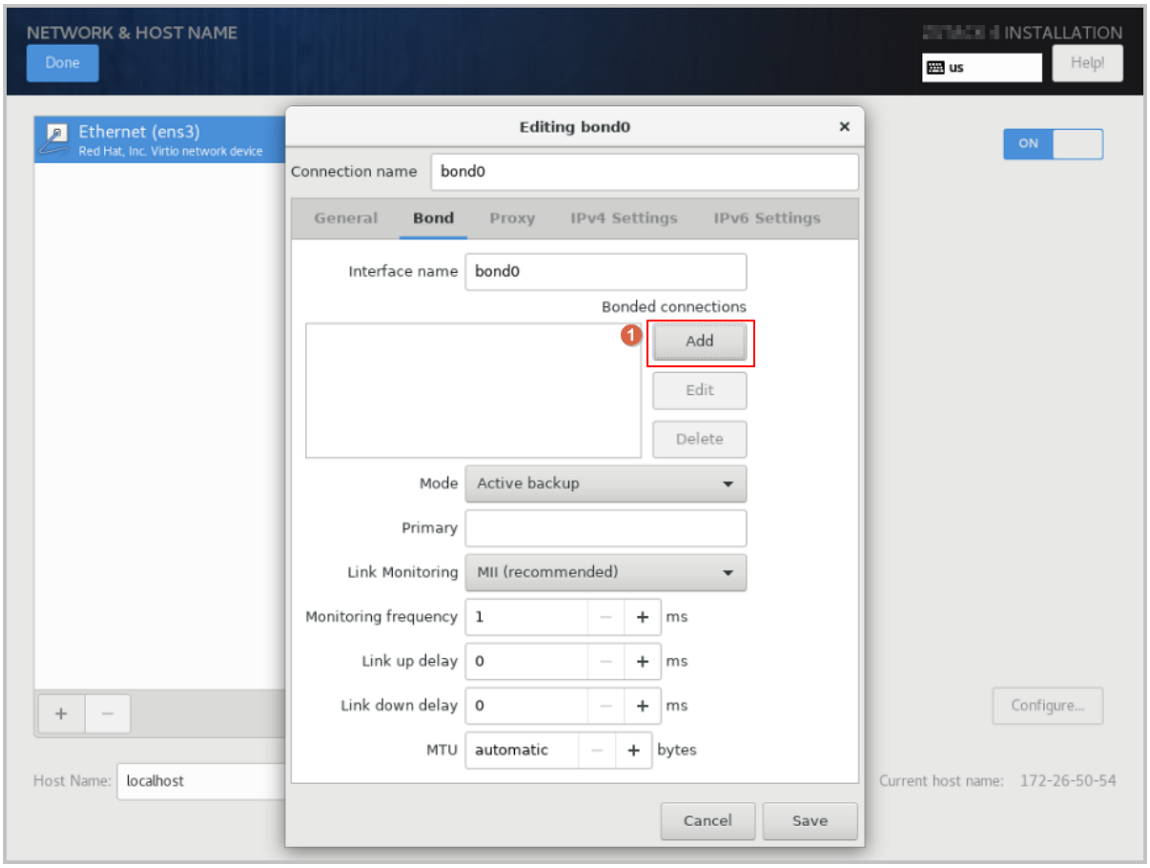
> **Note:**
>
> **Make sure the Connection name matches the Interface name.**

Figure 1-6: Adjust Connection Name



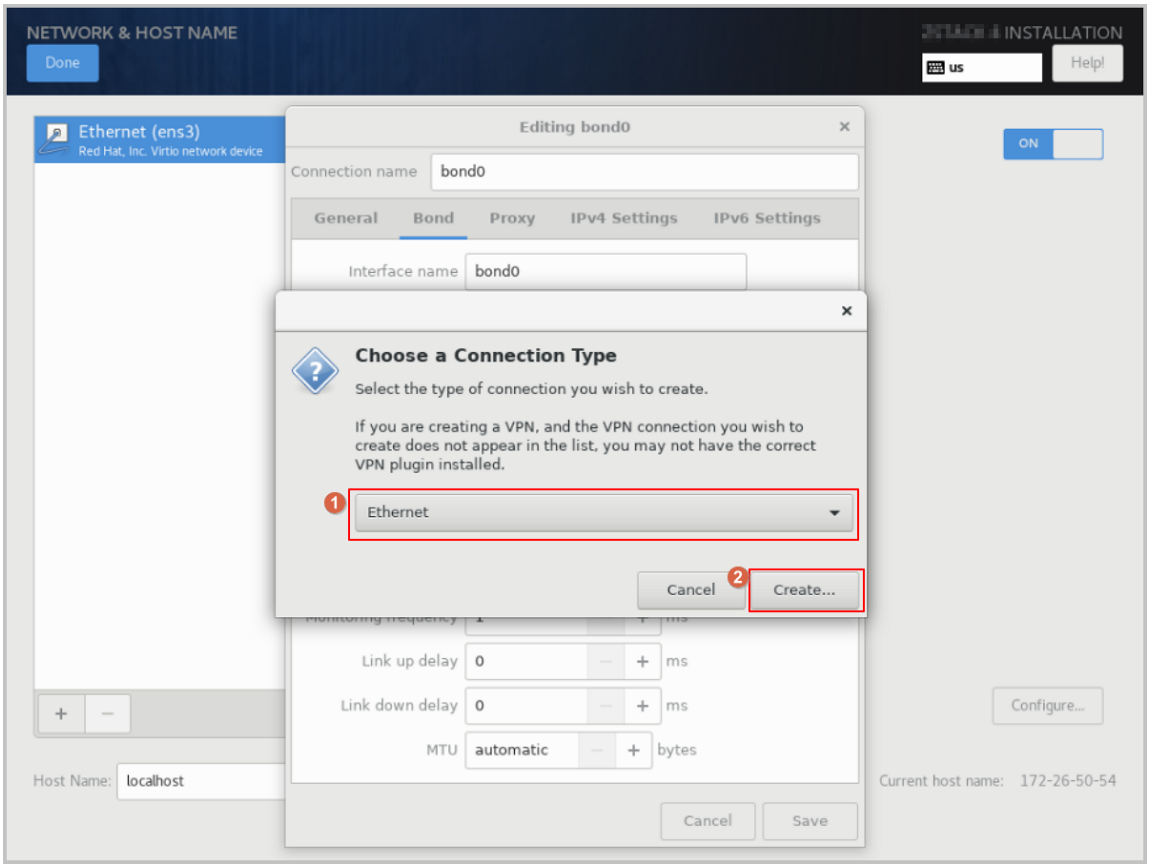
b) On the Bond configuration window, click **Add** to add a bond slave.

Figure 1-7: Add Bond Slave



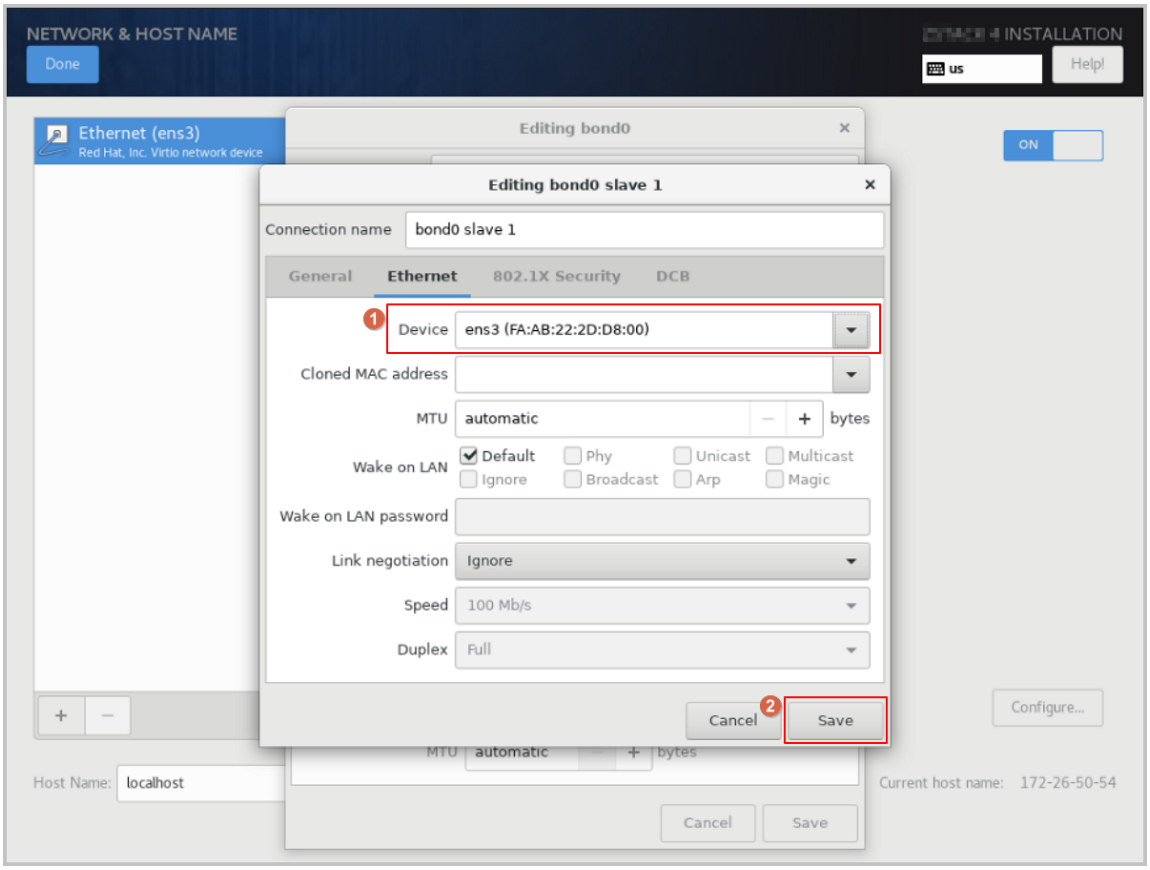
c) In the **Choose a Connection Type** dialog, choose a connection type from the drop-down list, such as **Ethernet**, and then click **Create...**.

Figure 1-8: Select Bond Slave Connection Type



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**.

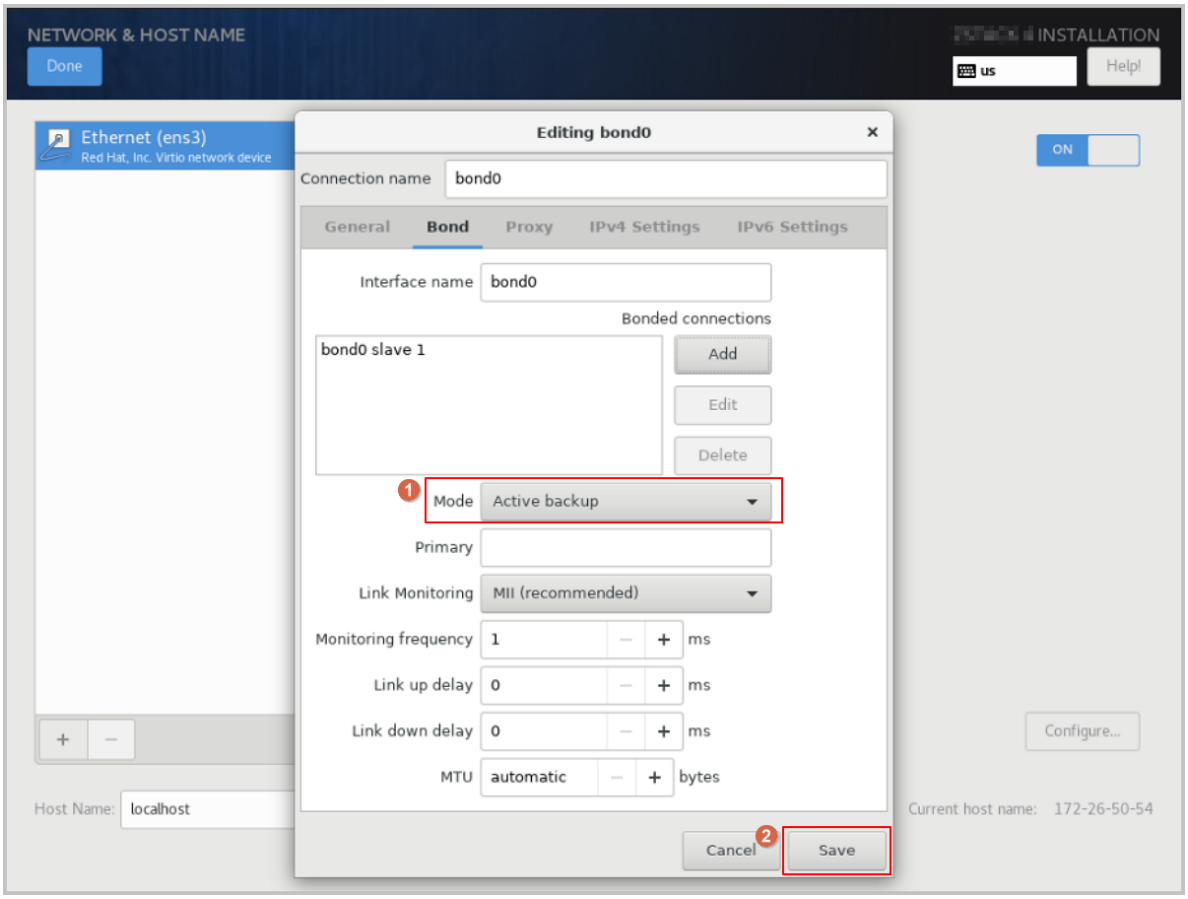
Figure 1-9: Select Bond Slave Device



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**.

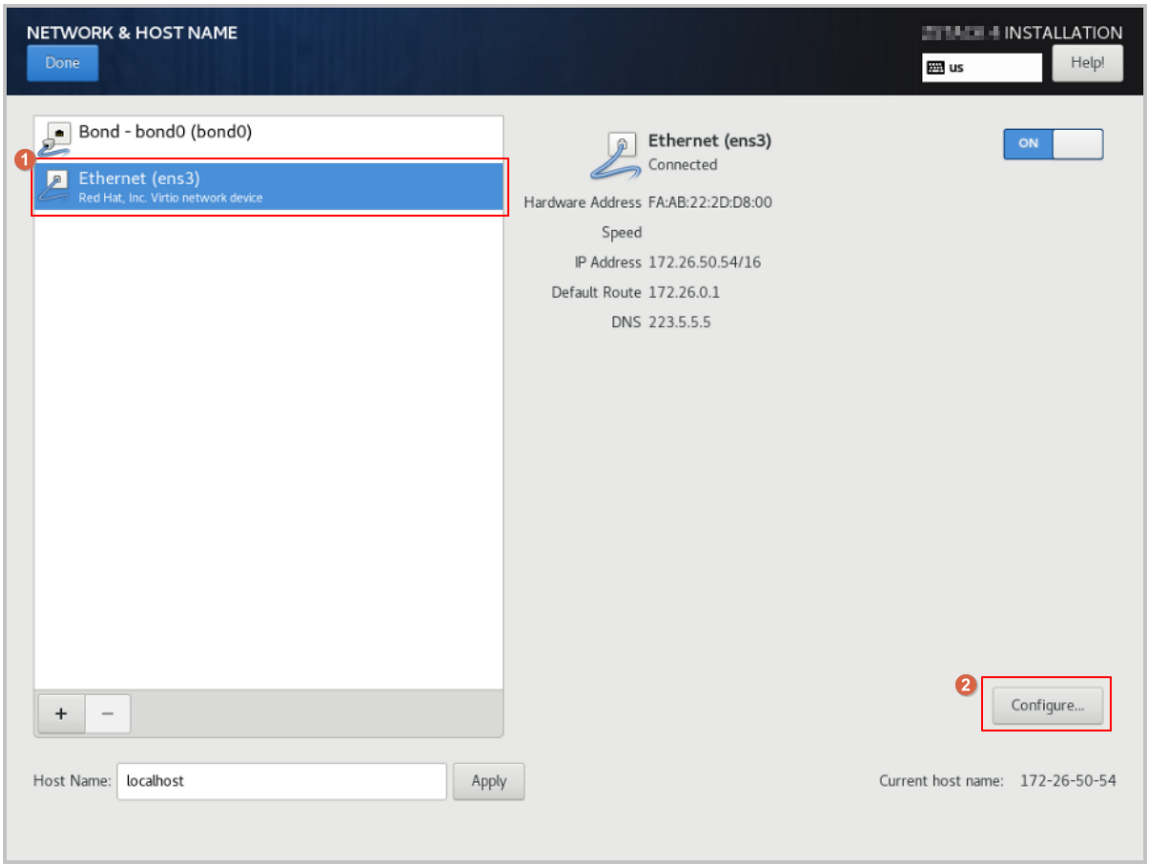
Figure 1-10: Select Bond Mode



8. Disable IPv4 on the original NIC.

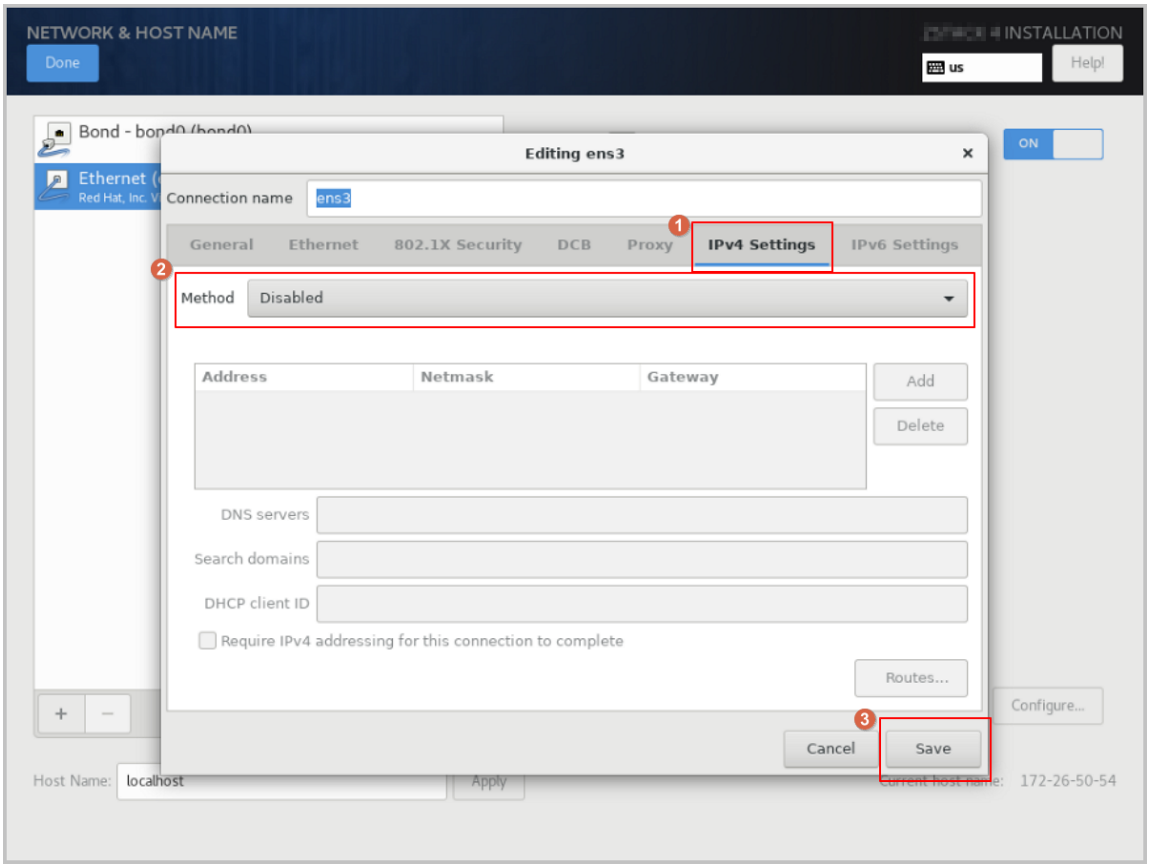
   a) Select the original NIC, such as **Ethernet (ens3)**, and click **Configure**.

Figure 1-11: Configure Original NIC



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 1-12: Disable IPv4



9. Configure a static IP address for Bond.

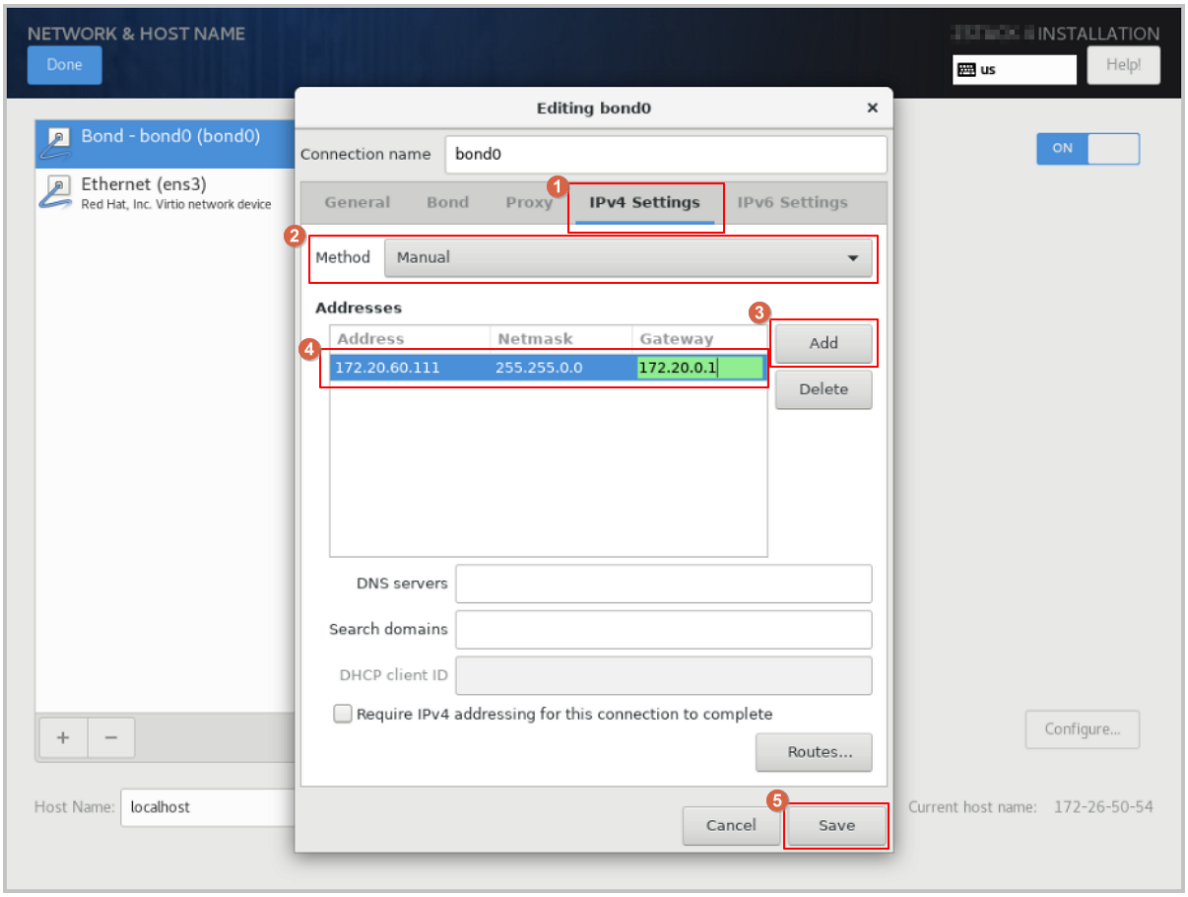
   a) On the **NETWORK & HOST NAME** page, choose the bond device, such as **Bond (bond0)**, and then click **Configure**.

   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.

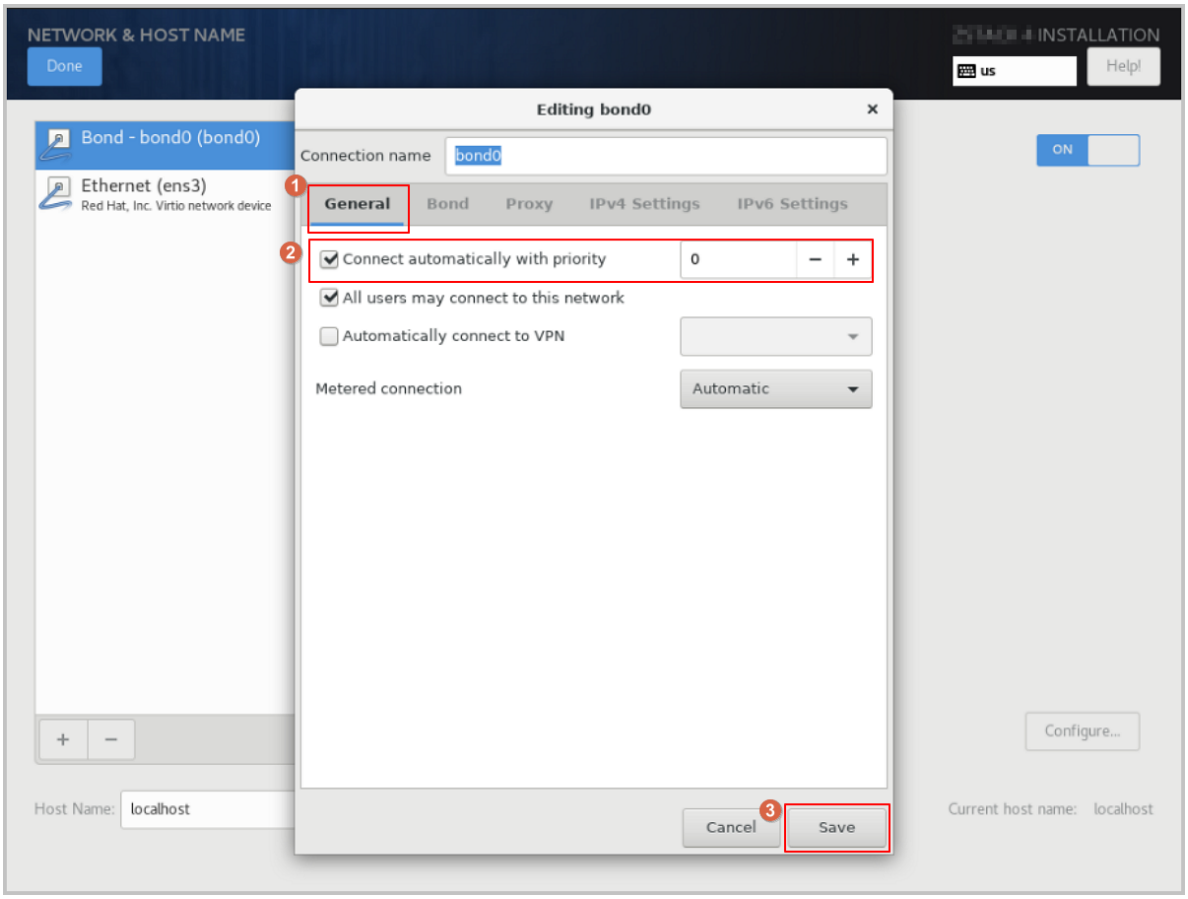
Figure 1-13: Configure Bond Static IP Address



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 1-14: Configure NIC to Activate Automatically

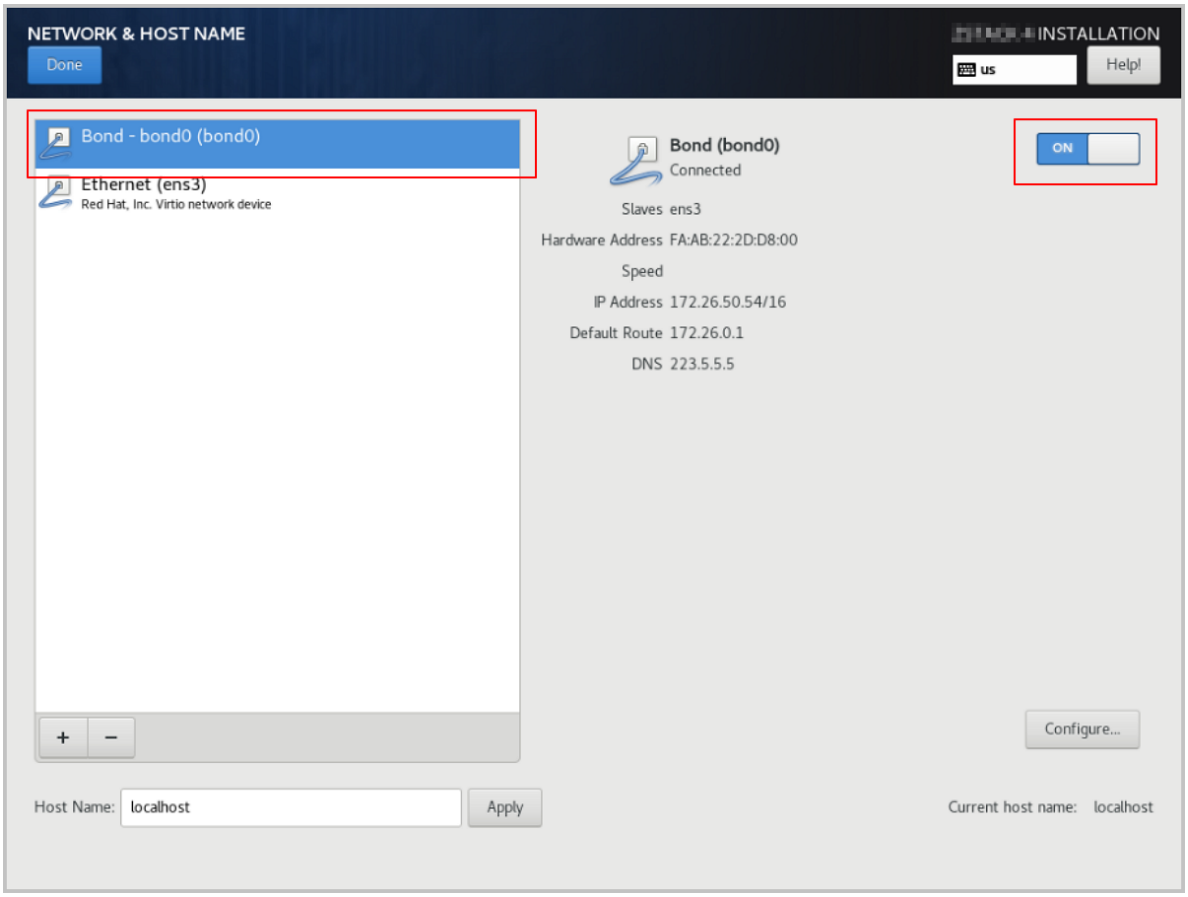


11. Complete the Bond configuration.

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, NexaSphere will not be installed properly.

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

Figure 1-15: Check Bond Configuration



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.

1.3.2 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

2. Review the installation configuration summary.

   This page displays the system installation configuration. You can modify the configuration as needed. By default, NexaSphere 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.

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 **Management Node** mode. Set the other servers to **Compute Node** mode.

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

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.

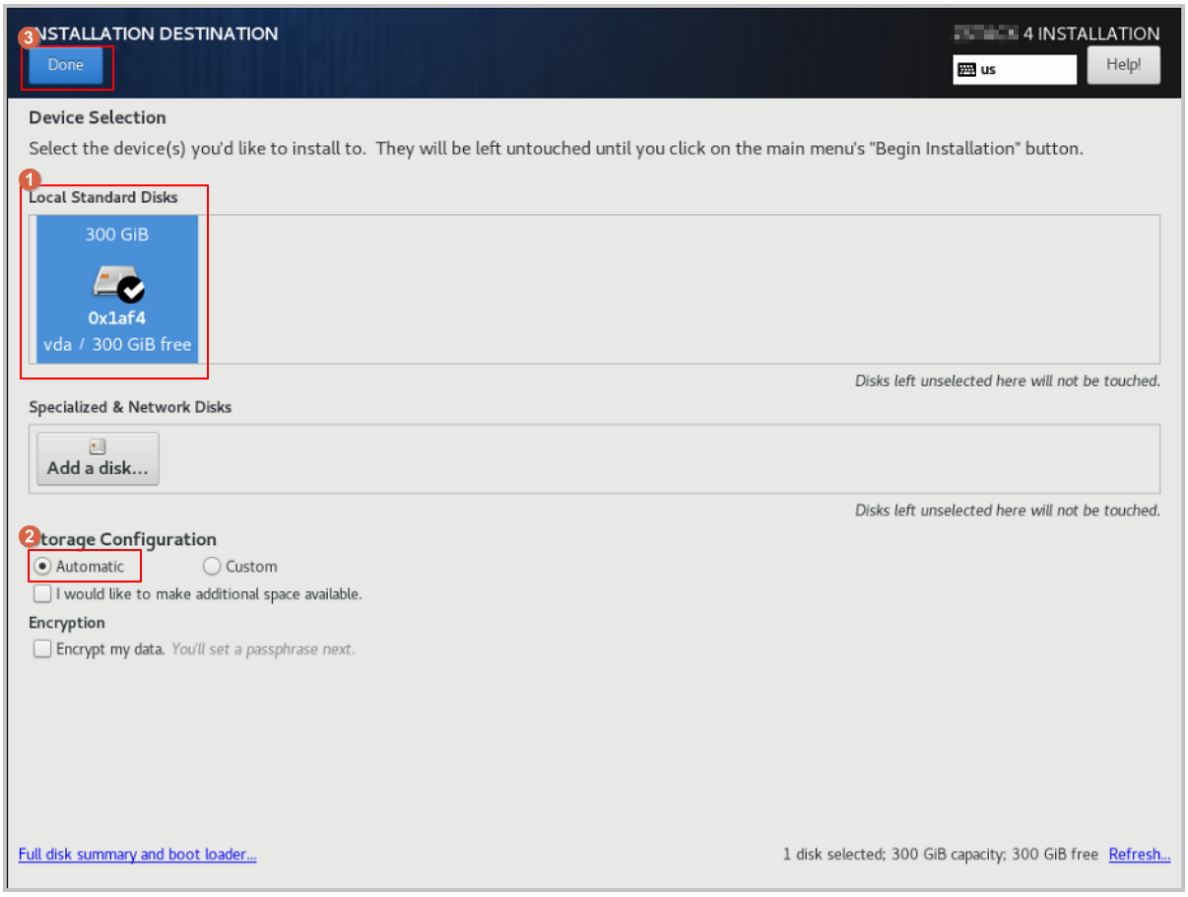
- Legacy Mode:
  - /boot: This directory stores the core files needed for Linux boot. We recommend allocating 1 GB of space.
  - swap: This is the swap area. We recommend allocating 32 GB.
  - /: This is the root directory for the Linux system. We recommend allocating all remaining space.

Note:

- The above values represent the recommended partition sizes for NexaSphere (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 1-16: Configure Disk Partitions



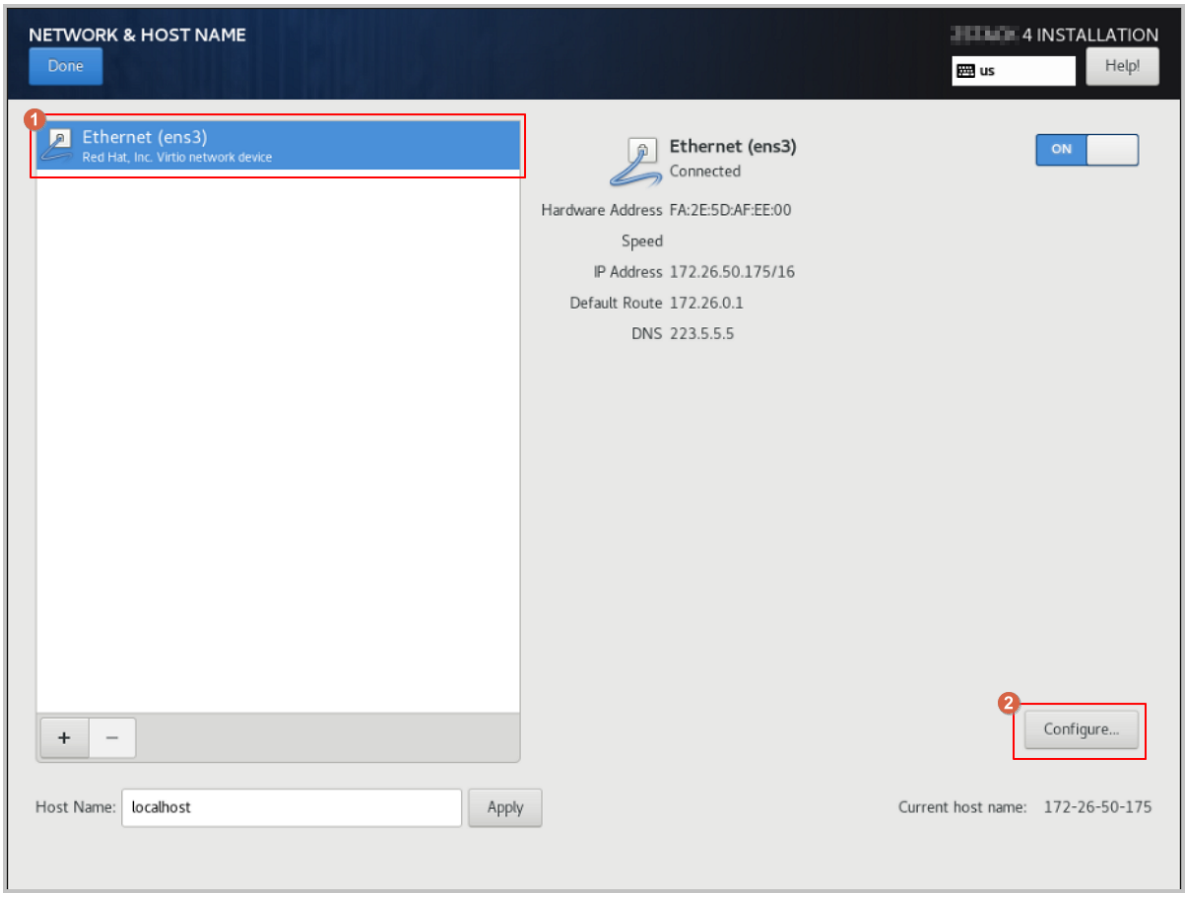
5. Start configuring the NIC.

   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 1-17: Configure NIC



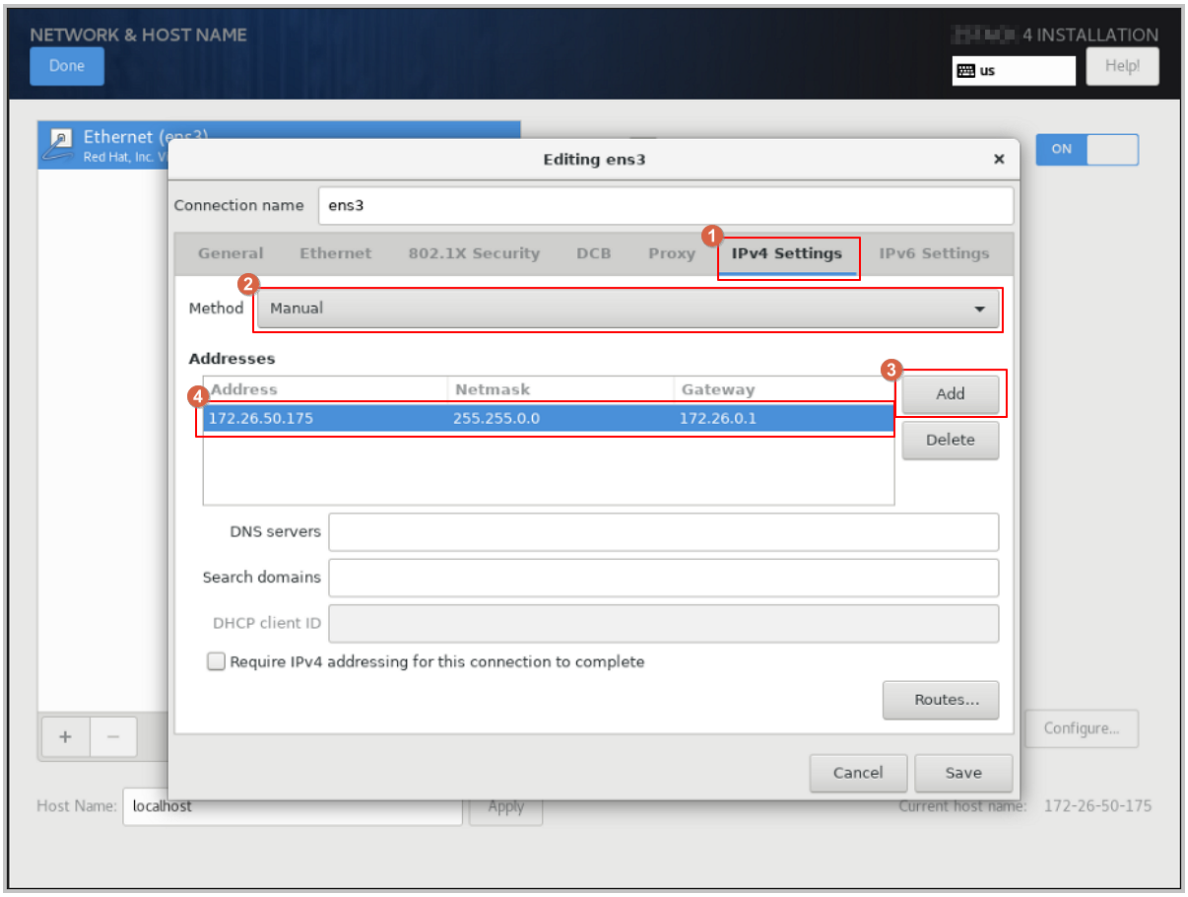
6. Configure a static IP address for the NIC.

   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 1-18: Configure Static IP Address

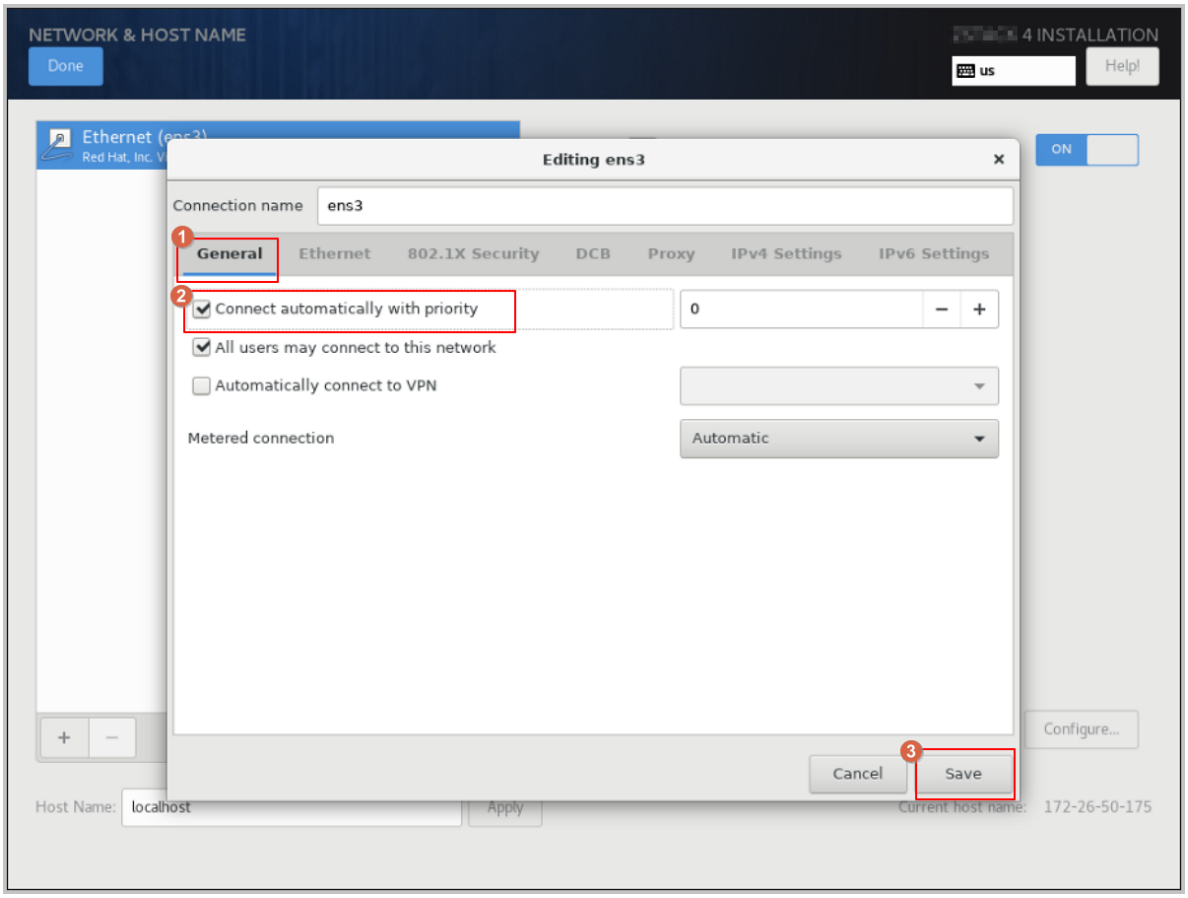


7. Configure the NIC to activate automatically.

   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 1-19: Configure NIC to Activate Automatically

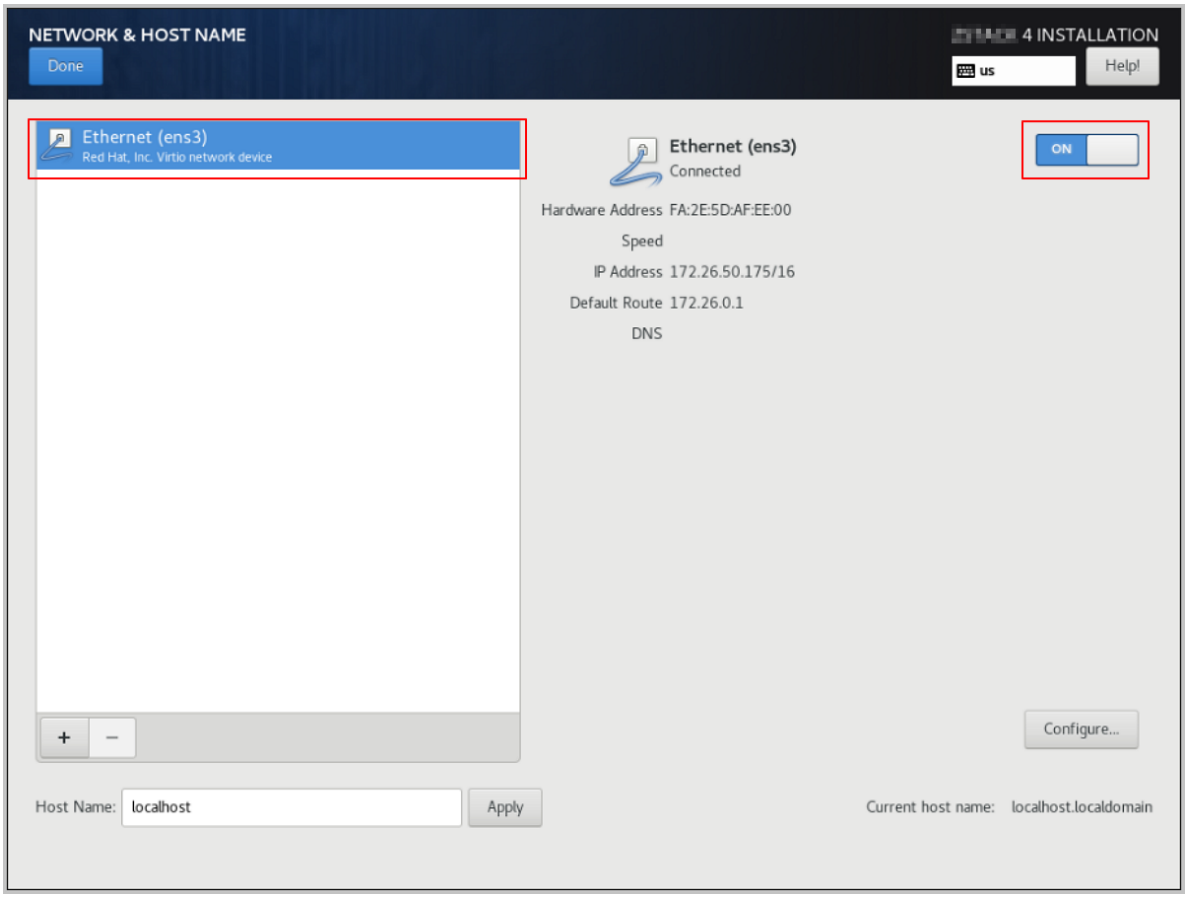


8. Complete the NIC configuration.

   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 1-20: Check NIC Configuration



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.

1.3.3 Install with TUI

This chapter describes the complete procedure for deploying a Compute Node from an ISO, configuring the management network as a bond in the TUI, and installing the management node on that compute node.

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

2. Enter the INSTALLATION SUMMARY wizard.

   After the installation boot screen loads automatically, the **INSTALLATION SUMMARY** page appears. On this page, focus on the following three configuration items: **Installation Destination**, **Software Selection**, and **Root Password**.

3. Configure Installation Destination.

   a) Click **Installation Destination**.

   b) Under **Local Standard Disks**, select a disk to use as the system disk.

   c) Keep **Storage Configuration** set to the default **Automatic**.

   d) Click **Done** in the upper-left corner to return.

4. Configure Software Selection.

   a) Click **Software Selection**.

   b) Under **Base Environment**, select **Compute Node** for the compute node mode.

   c) Click **Done** in the upper-left corner to return.

5. Configure the Root Password.

   a) Click **Root Password**.

   b) Enter and confirm the root password.

      The password must meet the strength requirements indicated by the prompt.

   c) Click **Done** to return.

6. Start the installation and wait for it to finish.

   Verify that all items marked with red boxes are configured (no yellow warning bars remain), and click **Begin Installation** in the lower-right corner to start the installation.

   The installation completes automatically and requires no manual intervention. After the installati on finishes, the system reboots and the TUI appears.

7. Enter the TUI main screen and complete root authentication.

   The TUI is divided into four information areas:

   - **NODE INFO**: Node uptime, load, CPU, and memory usage.
   - **DISK INFO**: Disk mount points and capacity.

- **NIC INFO**: NIC names and IP addresses. The default NIC, such as ens3, is displayed at first boot.
- **VM INFO**: List of virtual machines on the current node.

The shortcut keys are shown at the bottom of the screen:

- **<F2> System Configuration**: Enter system configuration.
- **<F12> Reboot/Poweroff**: Reboot or shut down the system.

a) Press **F2** to enter system configuration. The **ROOT PASSWORD** authentication dialog box appears.

b) Enter the root password and press **Enter** to confirm.

8. Open the Configure Networks settings.

After authentication, the **System Configuration** menu appears.

a) Use the arrow keys to select **Configure Networks**, and then press **Enter**.

b) In the **CONFIGURE NETWORKS** dialog box that appears, select the physical NIC to configure (for example, ens3).

c) Switch the keyboard to **uppercase**.

d) Press the **A** key to trigger the **Link <A>ggregation** operation.



Note:

Make sure the keyboard is in **uppercase** mode. Otherwise, pressing **A** will not start the bond creation process.

9. Select the bond mode.

a) In the **CONFIGURE BOND** dialog box that appears, select a bond mode.

b) This chapter uses **Active-Backup** as an example. Press **Enter** to confirm.

10. Name the bond and select slave NICs.

The **CONFIGURE BOND SLAVE** dialog box appears. Configure the following settings.

a) In **BOND NAME**, enter a name for the bond, for example, bond0.

b) In **Select SLAVES**, use the arrow keys to navigate to the target NIC and press **Space** to select it.

A selected NIC is marked with `[X]`.

c) After selecting all required NICs, press **Enter** to confirm.

11. Confirm the bond configuration.

The **CONFIGURE BOND NETWORK CONFIRM** warning dialog box appears with the following message:

```
Be careful! Changing the network configuration may cause failure!
If you know what you are doing, then enter 'Y' to continue!
```

a) Switch the keyboard to **uppercase**.

b) Press the **Y** key to confirm the configuration.

c) When the operation is successful, the **SUCCESS** dialog box appears with the message `Network configuration is changed successfully!`. Press **Enter** to close it.

12. Select the bond to configure its IP.

You return to the **Configure Networks** dialog box.

a) In the NIC list, select the bond created in the previous step (for example, bond0).

b) Press **Enter** to enter the IP configuration.

13. Configure the management network IP address.

a) In the **CONFIGURE NETWORK** dialog box, enter the following fields as shown in the example:

- **VLAN ID**: Enter the VLAN ID of the management network. Leave it empty if no VLAN is used.
- **IP ADDR**: Enter the management network IP address, for example, *172.26.215.195*.
- **NETMASK**: Enter the subnet mask, for example, *255.255.0.0*.
- **GATEWAY(DEF)**: Enter the default gateway, for example, *172.26.0.1*.

b) Press **Enter** to confirm.

14. Confirm the IP configuration.

a) Press **Enter** to submit. The **CONFIGURE NETWORK CONFIRM** confirmation dialog box appears.

b) Switch the keyboard to **uppercase**.

c) Press the **Y** key to confirm.

d) The **SUCCESS** dialog box appears. Press **Enter** to close it.

15. Open the Install Nologo option.

a) Press **Esc** to return to the **System Configuration** menu.

b) Use the arrow keys to select **Install Nologo**.

c) Press **Enter**.

16. Confirm the management node installation.

The **INSTALL Nologo** warning dialog box appears with the following message:

```
This process will install a brand new Nologo, please confirm
```

a) Type the full string `install nologo`.

b) Press **Enter** to confirm.

17. Wait for the management node installation to complete.

The screen enters a waiting state and displays the message `Please wait...`. Wait for the installation to complete.

18. After the installation is complete, view the TUI main screen.

After the management node installation completes, the information on the TUI main screen changes as follows:

- **DISK INFO**: New mount points such as */var/lib* and */usr/local* are added.
- **NIC INFO**: A new `docker0` interface (related to the management service) is displayed, along with the configured `bond0` and its IP address (for example, *172.26.215.195*).

19. Verify the management node status from the command line.

a) Press **Ctrl + Alt + F2** to switch to the command line login screen.

b) Log in as the root user.

c) Run the following command to query the management node status:

```
[root@localhost ~]# cloud-ctl status
```

When the management node is running, the expected output is as follows:

```
MN status: Running
UI status: Running
```

1.4 Set Up Management Node HA

Management node HA improves the availability of the NexaSphere management plane. After management node HA is configured, if the active management node becomes unavailable, the standby management node can continue to provide management services.

Before setting up management node HA, prepare two servers on which the management node service has been installed, and plan the management network, business network, and VIP in advance. You can complete the setup from the user interface, or follow the CLI workflow to install the operating system, configure networks, and install the HA suite in sequence.

1.4.1 Set Up with the UI

Prerequisites

- You must install management node services on the selected two servers. For installation instructions, see *Install the 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.

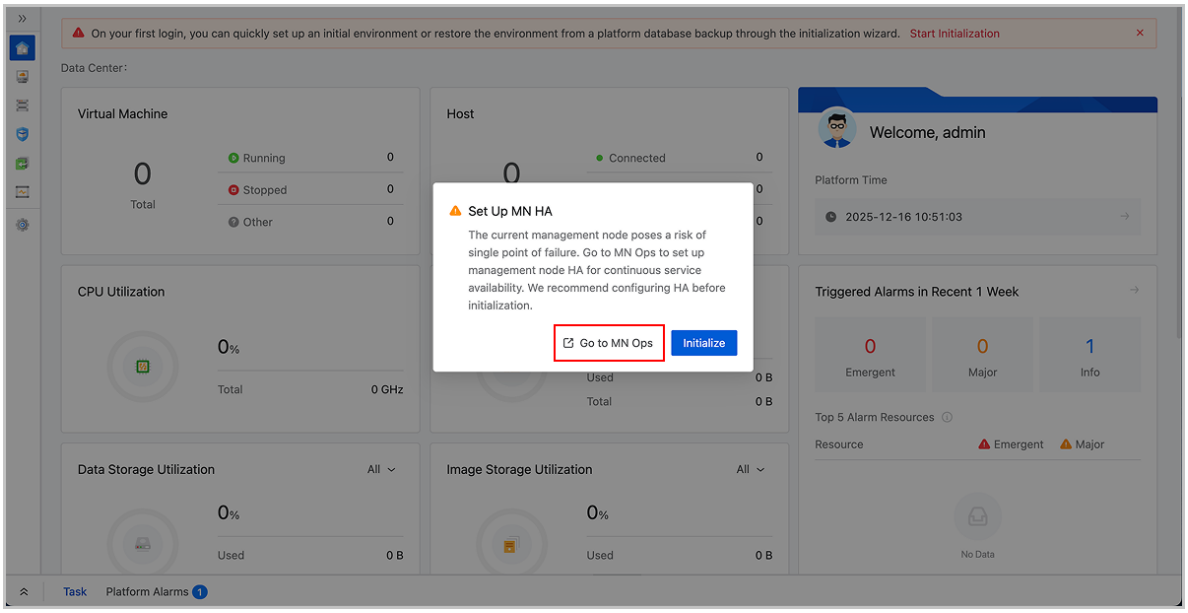
Procedure

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.

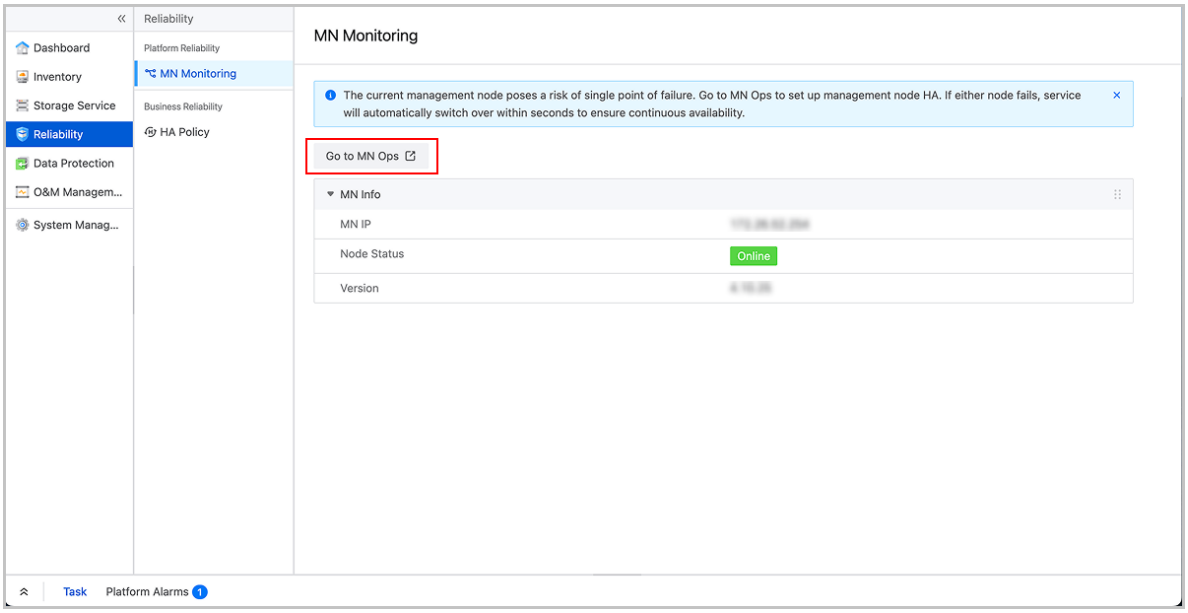
   Figure 1-21: Go to MN Ops from the Initialization Page



   For an existing environment:

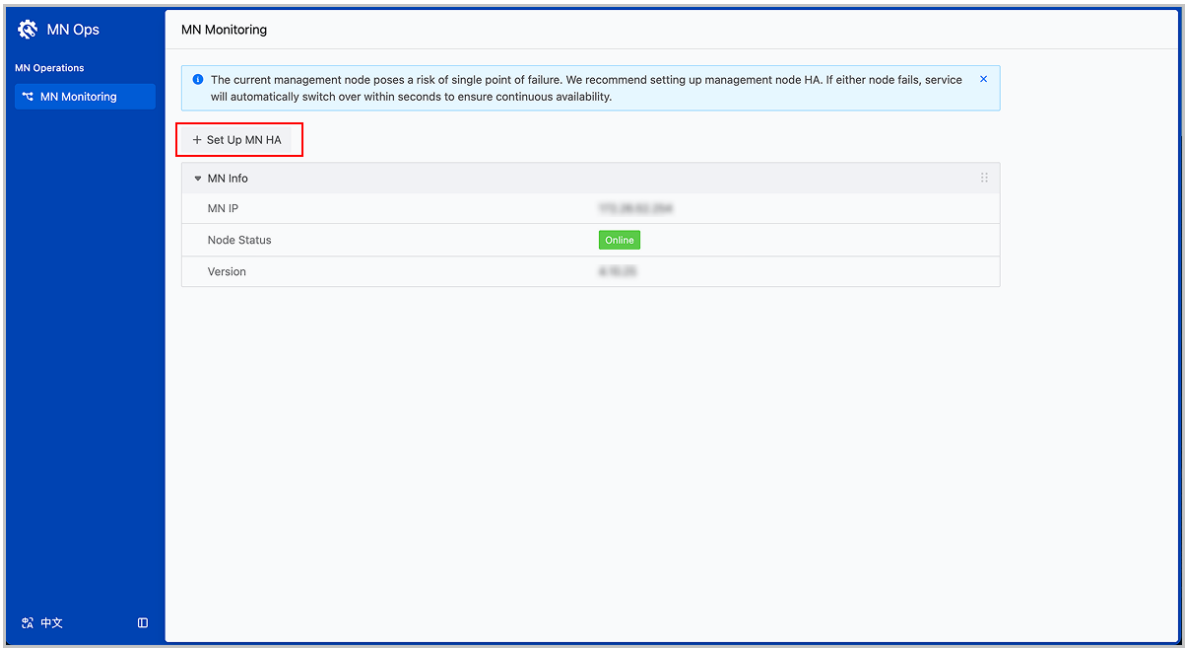
1. In the navigation pane, choose **Reliability** > **MN Monitoring**.
2. On the **MN Monitoring** page, click **Go to MN Ops**.
3. A new browser tab opens displaying the MN Ops page.

Figure 1-22: Go to MN Ops from the MN Monitoring Page



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

Figure 1-23: MN Monitoring



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.

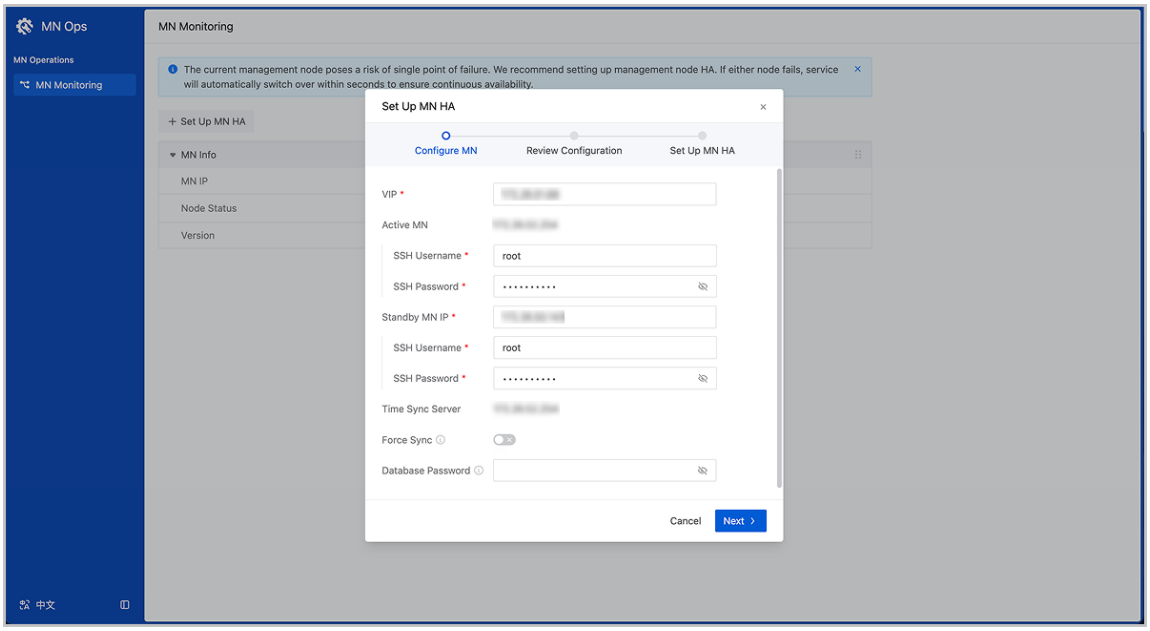
   - **Active MN IP**: Display the IP address of the active management node. Specify the SSH username and password for the active management node.
   - **Standby MN IP**: Specify the IP address, SSH username, and SSH password for the standby management node.

     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 1-24: Configure MN



b) Click **Next**.

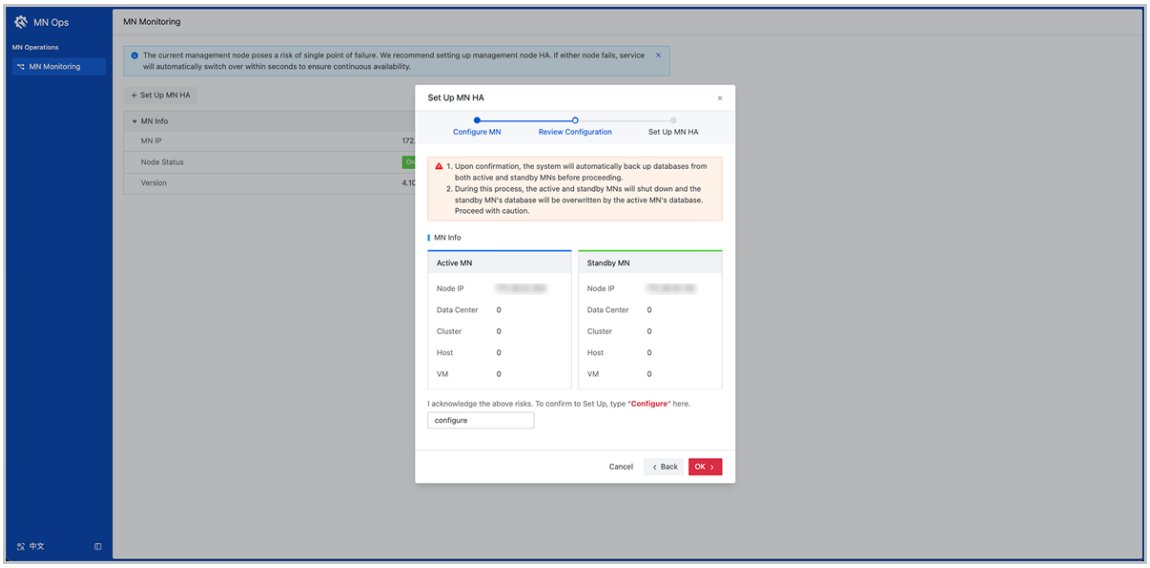
The system automatically checks if the requirements for addition are met.

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.

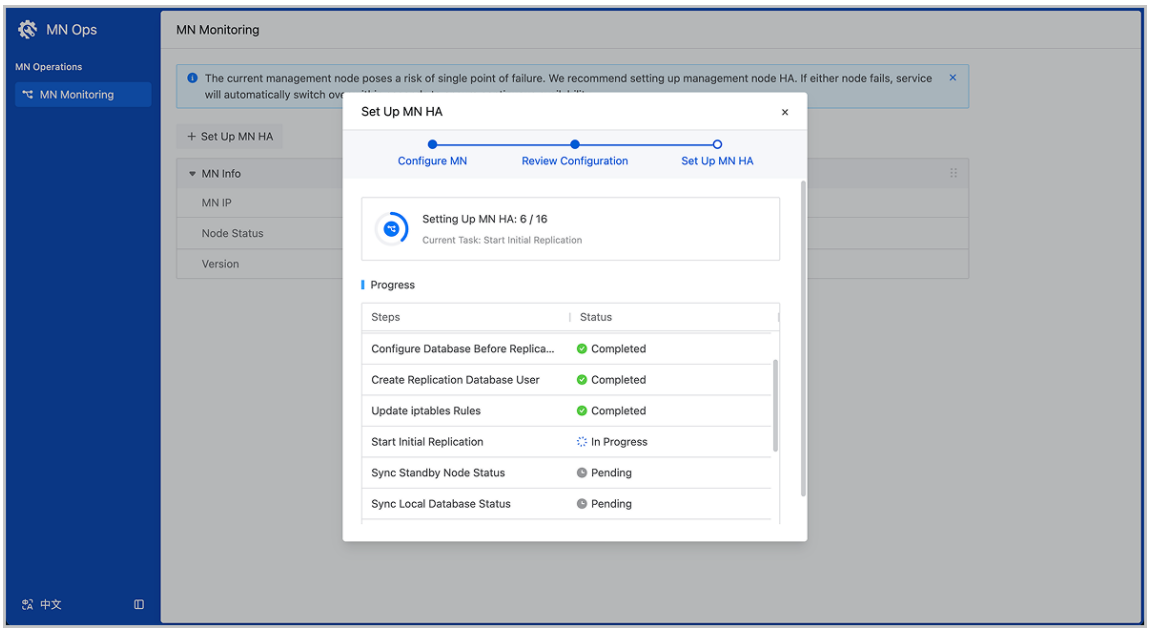
Figure 1-25: Review Configuration



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

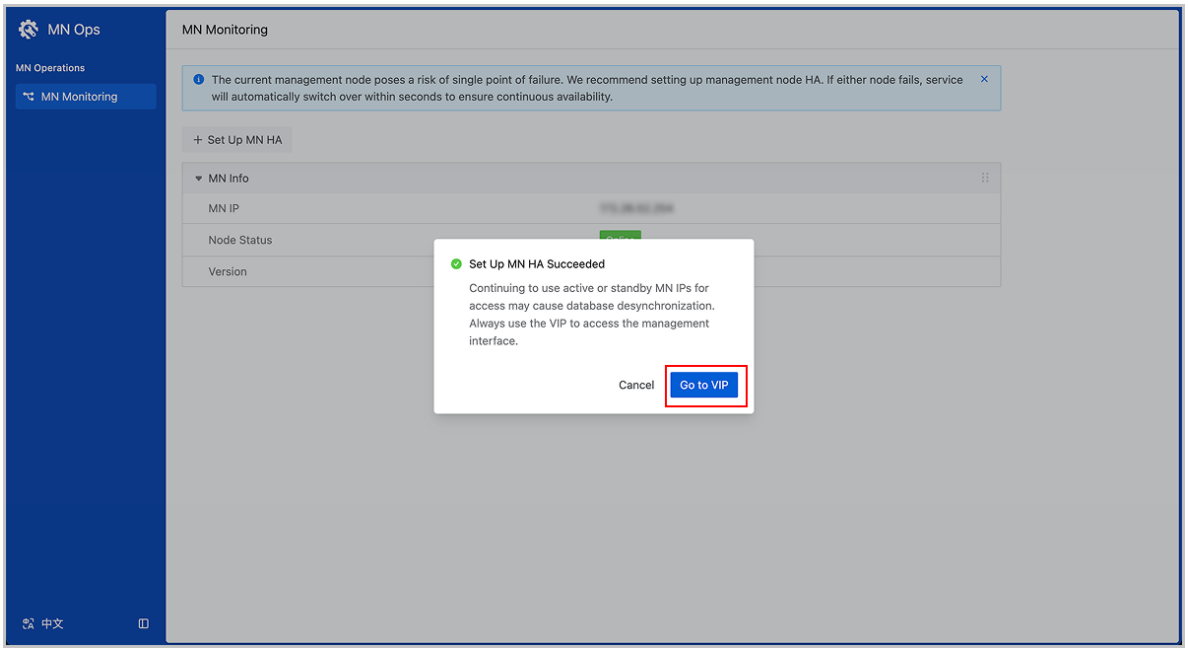
e) In the **Set Up MN HA** step, view the addition progress and task results.

Figure 1-26: Set Up MN HA



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

Figure 1-27: Go to VIP



1.5 Log in to NexaSphere

The platform uses HTTPS protocol by default and automatically redirects to port 443. You can simply enter the management node IP address in your browser to access the UI.

Prerequisites

- For a better experience, we recommend using Chrome 67 or later version with minimum screen resolution of 1280 × 900 px.
- If the web page fails to load, check whether both the management node and UI service are running properly.

Procedure

1. In a browser, enter the management node IP address in this format: *https://management_node_ip*.

   For a dual management node environment, use the VIP to access the UI.

2. Enter your username and password.

   On your first login, the default username is **admin** and the initial default password is **password**.

3. Click **Log In**.

What's next

- For more information about login policies, HTTPS/HTTP access, unified authentication, and certificates, see *Security*.
- After the first login, continue to initialize NexaSphere based on your deployment objective.

1.6 Initialize NexaSphere

After you log in to NexaSphere for the first time, you can use the initialization wizard to create basic resources so that the environment is ready for adding hosts, configuring storage, and creating virtual machines.

You can initialize the environment through the following methods:

- Initialize manually
- Restore from backup data

Notes during the initialization:

- If you exit the Wizard midway, **you will not be able to enter the Wizard again**.
- If no resources are created during the initialization, you can initialize the environment again from the Dashboard page.
- If you accidentally exit the Wizard, you can delete the data center and re-enter the initialization wizard from the Dashboard page.



Note:

Deleting a data center will delete clusters, hosts, networks, and data storage resources, along with all subordinate resources of each resource. Proceed with caution.

1.6.1 Initialize Manually

You can follow the wizard to initiate a new environment by creating necessary resources, including data center, cluster, host, data storage, image storage, image and distributed port group.

Procedure

1. In the **Welcome to Initialization Wizard** dialog, choose **Initialize Manually**.
2. Click **Next**.
3. On the **Initialize Manually** page, create a data center.
   a) Enter a name and description for the data center.
   b) Click **OK**.
4. Create a cluster.

a) Enter a name for the cluster.

b) Select a CPU architecture for the cluster. Options include x86_64 and aarch64.

c) Click **OK**.

5. Add a host.

a) Enter a name for the host.

b) Enter the host IP address, SSH port, SSH username, and SSH password.

> **Note:**
> The host architecture must match the cluster's CPU architecture, otherwise host addition to the cluster will fail.

c) Click **OK**.

The addition process may take several minutes to complete.

6. Add a data storage.

a) Enter a name for the data storage.

b) Select a data storage type. Options include local storage, nSDS distributed storage, and ZHPS distributed storage.

- Local storage: Set mount path and host disk configurations.

  > **Note:**
  > - Avoid system directories such as */*, */dev/*, */proc/*, */sys/*, */usr/bin*, and */bin* for mount path. Using system directories might cause the hosts unable to work properly.
  > - Host disk configuration will format the selected disks and completely erase all partitions, file systems, and data on the disk.

- nSDS distributed storage: Set whether to enable key authentication, add monitoring node, and specify image cache pool, storage pool, and storage network.

  > **Note:**
  > Make sure the key authentication configuration is consistent with the platform configuration. Otherwise, virtual machine creation may fail.

- ZHPS distributed storage: Enter IP address, port, username, and password. Add a storage pool.
- ZBS distributed storage: Add MDS nodes and Enter the pool name of the storage pool.

c) Click **OK**.

7. Add an image storage.

a) Enter a name for the image storage.

b) Select the image storage type. Options include standalone image storage and distributed image storage.

- Standalone image storage: Enter the image storage IP address, SSH port, username, and password. Complete the disk configurations, including addition method, mount path, whether to retrieve existing image, image sync network, and data network.



Note:

- If you select free disk for addition method, this configuration will format the selected disks and completely erase all partitions, file systems, and data on the disk.
- Avoid system directories such as `/`, `/dev/`, `/proc/`, `/sys/`, `/usr/bin`, and `/bin` for mount path. Using system directories might cause the image storage unable to work properly.

- Distributed image storage: Configure the monitoring node, including monitoring node IP address, SSH port, username, and password. Specify an image storage pool UUID as needed. If not specified, the platform creates one automatically.

c) Click **OK**.

8. Add an image.

a) Select the image path. Options include URL and local file.

b) Enter a name for the image.

c) Select the image type. Options include system image and disk image.

d) Select the image format. Options include qcow2, iso, vmdk, and raw.

e) Click **OK**.

9. Create a distributed port group.

a) Enter a name for the distributed port group.

b) Select the distributed switch for the distributed port group. Options include default switch and new switch.

- Default switch: Automatically created based on host configuration when adding the first host to a cluster. Primarily used for host management network. You can reuse this switch for both management network and business networks.

- New switch: To realize network separation between management network and business network, you can create a distributed switch as needed. This option is recommended for production environment. If you select this option, you need to configure aggregated interface configuration, uplink name, bond mode, hash policy, and host NC.

c) Select the VLAN type. Options include none and standard VLAN.

You need to specify a VLAN ID when selecting standard VLAN.

d) Choose whether to enable the DHCP service.

When enabled, you need to configure the network range method (IP range or CIDR), gateway, IP allocation policy, and DHCP IP.

e) Enter a DNS.

f) Click **OK**.

10. The **Manual Initialization Complete** dialog appears. Click **OK**.

You have completed the necessary resource creations for environment initialization. You may now start using the platform.

1.6.2 Restore from Backup Data

In the event of a disaster in the local data center, you can rely on the platform's database backup data to rebuild the data center and restore business. You can quickly restore the whole environment from an existing platform database backup using the initialization wizard.

Prerequisites

You have at least one valid platform backup.

Procedure

1. In the **Welcome to Initialization Wizard** dialog, choose **Restore from Backup Data**.
2. Click **Next**.
3. In the **Restore from Backup Data** dialog, set the following parameters to complete server configurations:

Parameter	Description
Backup Storage IP	Enter the IP address of the backup storage that stores the platform backup data.
URL	URL of the backup storage.
SSH Port	SSH port of the backup storage. Default is 22.

Parameter	Description
Username	Username of the backup storage.
Password	Password of the backup storage.

4. Click **Test Connection** to validate network connectivity to the backup storage.
5. After successful connection, set the following parameters to complete backup data configurations:

Parameter	Description
Database Backup	Select platform backup data.  **Note:** To avoid management node start failure due to insufficient licensed quota, select the appropriate data to restore. You can click **Update License** to renew your licensed quota.

6. Review the configuration and click **OK**.
7. In the **Restore Platform Database** dialog, enter the database root password and click **OK**.

 **Note:**
Restoring the platform database requires a management node restart, during which the management interface will be unavailable. This process takes a few minutes and does not affect your resources.

8. After the platform database is successfully restored, click **Log in Again**.

What's next

After platform database recovery, all resources on the platform will be recovered to the state at which the backup is created. Click **Scan Backup Data** in the local backup storage to obtain real-time backup data.

Glossary

2.1.1.1 Glossary

Data Center
A data center is the largest resource namespace within a virtualization platform, including resources such as clusters, hosts, data storage, distributed switches, and distributed port groups.

Cluster
A logical collection of a group of hosts (compute nodes).

Host
A host is an x86 or ARM physical server running a KVM virtualization hypervisor, providing resources such as computing, networking, and storage to virtual machines.

Virtual Machine Group
A logical grouping of virtual machines based on business needs.

Virtual Machine
A virtual machine is a virtualized host running on a physical host, capable of running an operation system and applications just like a physical host.

Disk
A disk provides storage space for a virtual machine. Disks are categorized into system disks and data disks.

System Disk
A system disk provides support for the system operations of a virtual machine.

Data Disk
A data disk provides extended storage space for a virtual machine.

Image
An image is a template file used by virtual machines or disks. Images are categorized into system images and disk images.

Image Storage
An image storage is a virtualized resource that provides storage space for image template files used by virtual machines or disks. An image storage can be categorized into standalone image storage and distributed image storage.

Standalone Image Storage
A standalone image storage stores image files through image slices and support incremental storage.

Distributed Image Storage
A distributed image storage stores image files through distributed block storage.

Data Storage
A data storage is a virtualized resource that provides storage space for virtual machines and their application data. A data storage can be categorized into local storage and network shared storage .

Local Storage
A local storage is storage resource constructed using the physical storage space of one or more hosts.

Netowrk Shared Storage
A storage system used for remote storage of virtual machines and their application data, accessible concurrently by hosts over a network.

Distributed Switch
A virtual switching device that provides unified virtual network management and monitoring for virtual machines within a cluster.

Distributed Port Group
A logical grouping of ports on a distributed switch, used for port configuration.

vNUMA Configuration

vNUMA uses CPU pinning to passthrough the topology of associated host physical NUMA (pNUMA) nodes to a virtual machine, generating a topology of virtual NUMA (vNUMA) nodes for the virtual machine. This topology enables a vCPU on a vNUMA node to primarily access the local memory and thus improves VM performance.

NUMA (Non-Uniform Memory Access)

Non-uniform memory access (NUMA) is a computer memory design where the memory access time depends on the memory location relative to the CPU. Under NUMA, a processor can access its own local memory faster than non-local memory and thus improves VM performance.

pNUMA Node (physical NUMA Node)

A pNUMA node (physical NUMA node) is a host NUMA node predefined based on the host NUMA architecture. It is used to manage the CPUs and memory of the host.

pNUMA Topology (physical NUMA Topology)

A pNUMA topology (physical NUMA topology) is the topology of the host NUMA nodes predefined by the CPU vendor based on the host NUMA architecture.

vNUMA Node (virtual NUMA Node)

A vNUMA node (virtual NUMA node) is generated by passing-through associated pNUMA nodes via CPU pinning. It is used to manage the CPUs and memory of a virtual machine.

vNUMA Topology (virtual NUMA Topology)

A vNUMA topology (virtual NUMA topology) is the topology of VM NUMA nodes generated by passing-through associated pNUMA nodes via CPU pinning.

Local Memory

Local memory is the memory that a CPU (pCPU or vCPU) accesses through the Uncore iMC (Integrated Memory Controller) of the same NUMA (pNUMA or vNUMA) node. Compared with accessing non-local memory, accessing local memory has lower latencies.

CPU Pinning

CPU pinning assigns the virtual CPUs (vCPUs) of a virtual machine to specific physical CPUs (pCPUs) of the host, which improves VM performance.

EmulatorPin Configuration

EmulatorPin assigns all other threads than virtual CPU (vCPU) threads and IO threads of a virtual machine to physical CPUs (pCPUs) of the host so that these threads run on assigned pCPUs.

Snapshot

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

VM Scheduling Policy

A VM scheduling policy is a resource orchestration policy based on which virtual machines are assigned to hosts to achieve the high performance and high availability of businesses.

Management Node

A physical host where the system is installed, providing UI management and virtualization platform deployment capabilities.

Compute Node

Also known as a host, it is a physical server that provides computing, networking, and storage resources for virtual machines.

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 SAN storage or passthrough the block to a virtual machine.

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 SAN storage or passthrough the block to a virtual machine.

NVMe Storage

A type of storage implemented via the NVMe-oF (NVMe over fabrics) protocol. You can add a block device configured from an NVMe storage as SAN storage.

Management Network

A management network is used to manage physical resources in the platform. For example, you can create a management network to manage access to hosts, data storage, and image storage.

Security Group

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

MN Monitoring

Management Node (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 and event alarm.

Message Template

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

Endpoint

An endpoint is a method that users obtain subscribed messages.

Alarm Message

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

Operation Task

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

HA Task

HA task logs generated when the platform executes high availability procedures in accordance with the enabled HA policy.

Scheduling Task

Scheduling task logs generated when the platform executes dynamic resource scheduling operations after the cluster DRS is enabled.

Event

Event monitors and records all activities on the platform. You can use this feature to implement operation tracking, security analysis, troubleshooting, and automatic O&M.

Backup Plan

You can create a backup plan to back up local virtual machines or platform databases to a specified backup storage on a regular basis.

Local Backup Data

Local backup data of virtual machines or platform 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 the a remote data center and is used to store remote backup data.

Tag

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

Custom Attribute

Custom attributes are user-defined key-value pairs in the platform that extend the resource tagging and management capabilities.

Single Sign-On

The Single Sign-On service supports seamless access to SSO systems. Through the service, related users can directly log in to the platform and manage resources.

Console Proxy

Console proxy allows you to log in to a virtual machine 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 platform. AccessKey pairs shall be kept confidential.

IP Blocklist/Allowlist

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

User Management

A user can be created by the admin or synchronized from an authentication system. A user is managed by the admin. Resources created by a user are managed by the user.

Theme and Appearance

You can customize the theme and appearance of the platform.

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 receives management node logs or platform operation logs sent from the virtualiza tion platform for centralized retention, search, and analysis.

System Parameters

System parameters allow you to configure settings that take effect on the whole platform.

HA Policy

HA Policy is a mechanism that ensures sustained and stable running of the business if virtual machine are unexpectedly stopped or are errored because of errors occurring to compute, network, or storage resources associated with the virtual machines. By enabling this feature, you can customize VM HA policies to ensure your business continuity and stability.

Bare Metal Template

With bare metal templates, preconfigured files can be quickly generated to achieve unattended bulk OS installation for bare metal instances.

Bare Metal Cluster

A bare metal cluster consists of bare metal chassis.

Deployment Server

An independent server used for providing PXE services and console proxies for bare metal chassis.

Bare Metal Chassis

Bare metal chassis is used to create bare metal instances and can be universally identified by the BMC interface and IPMI configuration.

Bare Metal Instance

A virtualized instance of bare metal chassis.