nCSSV Installation Guide

Clustering with HA and virtualized nSAN storage

Contents

1 Overview

This document describes how to install **nCSSV**.

This installation guide focuses on **practical implementation** rather than serving as an exhaustive technical reference. The objective is to provide administrators and engineers with clear, step-by-step instructions that can be followed in real deployment scenarios.

The guide covers the most common **clustering configurations**, including setups with **High Availability (HA)** and **virtualized storage with nSAN**. It assumes the use of **standard hardware resources** and typical network environments, so that the procedures described can be reproduced in most datacenter or lab contexts without requiring custom adaptations.

Advanced tuning, troubleshooting, and edge-case scenarios are outside the scope of this document.

The guide provides:

- Step-by-step installation procedures for nCSSV
- Essential hardware and network configuration requirements
- Basic post-installation setup through both CLI and web interface

> **Note**
>
> A functional nCSSV cluster requires either a setup of two nodes plus a witness, or a configuration of three or more nodes. The specific differences between these deployment options will be detailed in the following sections of this guide.

2 Install nCSSV and Perform Initialization

2.1 Hardware Requirements

Device Configuration Requirements

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

Note

The nCSSV operating system must be installed on solid-state storage.

2.2 Create Bootable USB Drive

To begin the installation, you need to create a bootable USB drive with the nCSSV ISO image:

- Download the nCSSV ISO image from the official repository
- Use a tool like Rufus to write the ISO to a USB drive
- Ensure the USB drive has at least 8GB of capacity
- Insert the bootable USB drive into the target server
- Configure the server BIOS/UEFI to boot from the USB device

The system will boot from the USB drive and start the nCSSV installation process.

2.3 Installation

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.

2.4 Installation Summary Page

This page displays the system installation configuration. You can modify the configuration as needed.

Remember to insert your custom root password, it will be used for settings later.

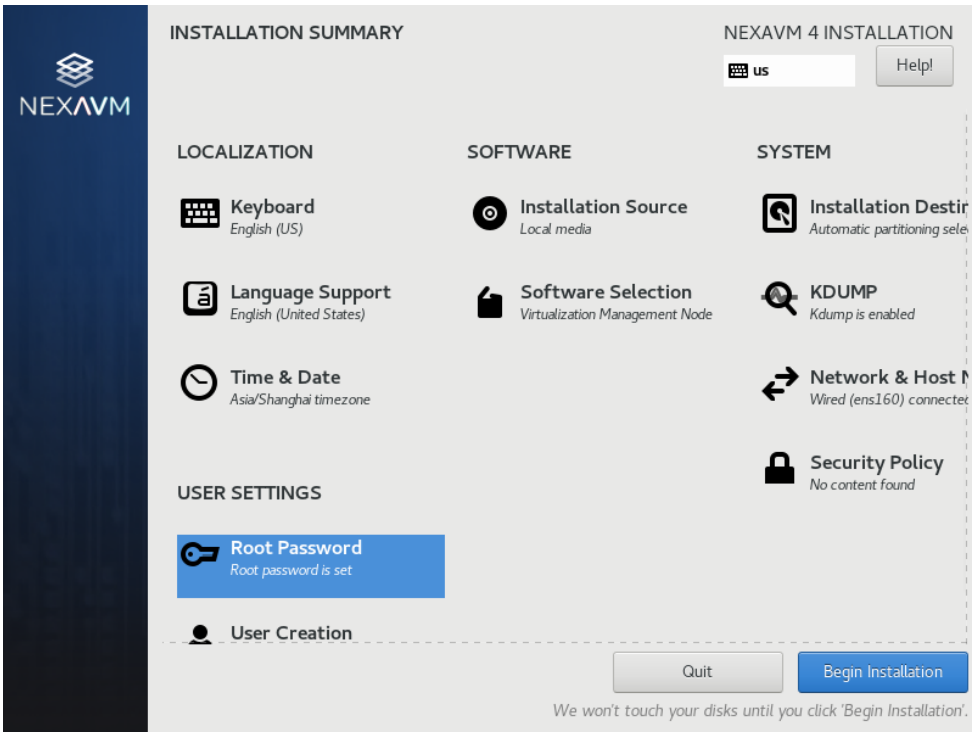

Figure 1: Installation Summary

2.5 Select Installation Mode

On the *Installation Summary* page, click *Software Selection*.

On the *Software Selection* page, choose the installation mode based on the intended role of the node within the cluster:

- *Enterprise Management Node* — select this option if the current server will act as a **management node**. This node will host the nCSSV management services and, in High Availability (HA) deployments, will synchronize with a peer management node.
- *Compute Node* — select this option if the current server will serve as a **compute node** (or **witness node**) within the cluster. Compute nodes provide virtualization and processing resources, while witness nodes are required in two-node HA configurations to ensure proper arbitration and quorum for nSAN storage.

> Note
>
> In HA setups with virtualized storage (**nSAN**), at least two management nodes plus one witness are required. Select *NexaVM Compute Node* for the witness node installation.

After selecting the appropriate installation mode, click **Done** to return to the Installation Summary page.

2.6 Configure Disk Partitions

On the *Installation Summary* page, click *Installation Destination* to enter the *Installation Destination* page.

Note

We recommend that you only configure the system disk on the page. After the system is installed, you can configure other disks.

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

If the selected disk does not have enough available space, click *Reclaim Space* and *Delete All*.

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 1GB of space.
- `/boot/efi`: This directory stores the UEFI boot files. We recommend allocating 500MB.
- `/`: 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 1GB of space.
- `/`: 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 nCSSV (total disk capacity should be greater than 300GB).
- In Legacy mode, if the system disk capacity exceeds 2TB, you need to configure a BIOS boot partition to support GPT partitioning. UEFI mode does not have this limitation and supports GPT partitioning.

Review the configuration and click *Done*.

2.7 Configure Network Interfaces

On the *Installation Summary* page, click *Network & Host Name* to configure the network interfaces.

- Select the network interface cards (NICs) you want to use
- For each NIC you wish to configure, follow these steps:
    1. Click on the NIC from the list in the left panel

2. Click the **Configure** button in the bottom-right corner
3. In the configuration window, select **IPv4 Settings** from the menu
4. From the **Method** dropdown menu, select **Disabled**
5. Select **IPv6 Settings** from the menu
6. From the **Method** dropdown menu, select **Disabled**
7. Click **Save** to apply the configuration

- Repeat this process for each NIC you want to configure
- After configuring all NICs, click **Done** to return to the main installation screen

This configuration ensures that the network interfaces are properly set up before proceeding with the installation.

Begin The Installation Process

Once all required configurations have been completed, click **Begin Installation** in the bottom-right corner of the Installation Summary page.

Wait for the first part of the installation to complete. When the screen turns black and the server begins to reboot, **remove the USB drive** to prevent the system from booting from it again.

The system will now complete the installation and reboot. After the reboot, we will continue with the backend configuration manually through the command line interface.

3 Post-Installation Network Configuration

3.1 Login and Initial Setup

After the system reboots, log in using the credentials created during the installation process.

3.2 Post-Installation Network Configuration

General Rules

- Replace interface names (e.g., eth0, eth1, eth2, eth3) with the real ones from your system.
- For trunk mode, replace VLAN IDs (100, 200) with your actual VLAN IDs.
- Use the provided IPs, masks, and gateways only as examples.
- Typically, only the management network requires a gateway.

3.3 Network Configuration Commands

The following procedure describes how to configure a bond interface. These steps (`create bond` → `attach NICs` → `optional VLAN` → `bridge and IP configuration`) must be repeated for each bond that the system requires. At a minimum, one bond should be created for **management** and one for **storage**. Additional bonds may be configured as needed for **business traffic**, **backup**, or **migration**.

Create a virtual link aggregation interface in active-backup mode:

```
zs-bond-ab -c [BOND_NAME]
```

Attach a physical NIC to the bond interface:

```
zs-nic-to-bond -a [BOND_NAME] [NIC_NAME]
```

Create a network bridge and configure its IP address:

```
zs-network-setting -b [BOND_NAME] [IP_ADDRESS] [NETMASK] [GATEWAY]
```

(Optional) If required create a VLAN interface, add it to the selected bond, and configure the network:

```
zs-vlan -c [BOND_NAME] [VLAN_ID]
```

```
zs-network-setting -b [BOND_NAME].[VLAN_ID] [IP_ADDRESS] [NETMASK] [
    GATEWAY]
```

Verify the current network configuration:

```
zs-show-network
```

3.4 Removing Incorrect Configurations

If a bond or bridge was configured incorrectly:

```
# Stop the created bridge
ip link set [BRIDGE_NAME] down
```

```
# Delete the bridge
brctl delbr [BRIDGE_NAME]
```

```
# Delete the bridge configuration file
rm -f /etc/sysconfig/network-scripts/ifcfg-[BRIDGE_NAME]
```

Delete VLAN configuration:

```
zs-vlan -d [BOND_NAME] [VLAN_ID]
```

Delete bond:

```
zs-bond-ab -d [BOND_NAME]
```

Check that bonds are active and IPs are correctly assigned. Then continue with the remaining nCSSV configuration steps.

4 Install nCSSV Management Service

After configuring the network, run the following command **only on the management nodes** to manually install the nCSSV management service:

```
bash /opt/zstack-installer.bin
```

5 High Availability and Storage Installation

To enable cluster High Availability (HA) and Distributed Storage, the corresponding packages must be installed on **only one** of the management nodes (for example, Node A). After installation, the services will automatically synchronize with the peer management node.

5.1 Install the High-Availability Suite

Prepare and extract the HA installation package on the first management node:

```
tar zxvf NexaVM-Multinode-HA-Suite.tar.gz
```

```
chmod +x zsha2
```

Generate and edit the HA configuration file:

```
./zsha2 sample-config > zs-install.config
```

```
vim zs-install.config
```

Configuration example:

```
{
  "gateway": "[GATEWAY_IP]",           # Arbitration gateway
  "datalink": "",                      # Leave default
  "virtualIp": "[VIP_ADDRESS]",        # VIP for keepalived
     communication
  "myIp": "[LOCAL_NODE_IP]",           # This management node IP
  "peerIp": "[PEER_NODE_IP]",          # Peer management node IP
  "peerSshUser": "root",               # SSH username for peer
  "peerSshPass": "[PEER_PASSWORD]",    # SSH password for peer
  "peerSshPort": 22,                   # SSH port
  "dbRootPass": "[MYSQL_ROOT_PASSWORD]",# Database root password (same
      on both nodes)
  "interface": "[INTERFACE]",          # Device/bridge used for VIP
  "timeServer": "[NTP_SERVER_IP]"      # Time synchronization server
}
```

Start the installation:

```
./zsha2 install-ha -config zs-install.config
```

Check the HA status:

```
zsha2 status
```

5.2 Install the Distributed Storage Service (nSAN)

Create a working directory and extract the installation package:

```
mkdir nSAN-installer
```

```
tar -zxvf NexaVM-nSAN-installer-[VERSION].tar.gz -C nSAN-installer
```

```
cd nSAN-installer
```

Edit the configuration file for distributed storage installation:

```
cd zstone-installer/
```

```
vim install.conf
```

Configuration example:

```
# Storage cluster management VIP (same as Cloud VIP in dual management
    setup)
zstone_vip=[VIP_ADDRESS]

# Management nodes (comma-separated for dual-node setup)
zstone_managerment_host_ip=[MGMT_NODE1_IP],[MGMT_NODE2_IP]
zstone_managerment_host_rootpw=["PASSWORD"]

# MySQL configuration
zstone_db=zstone
zstone_db_user=root
zstone_db_port=3306
zstone_db_password=[MYSQL_PASSWORD]

# PostgreSQL
zstone_temporal_db_port=5432

# ZStone account
zstone_account_name=admin
zstone_account_password=password

# Enable ZBS installation
zbs_install=true
```

Run the installation script:

```
bash install.sh
```

After completion, the storage service will automatically synchronize with the second management node, ensuring high availability and consistency.

6 Cluster Storage Configuration via Web Interface

Once the High Availability and Distributed Storage packages have been installed and synchronized between the management nodes, the next step is to configure the cluster virtual storage.

Open a web browser and connect to the cluster management interface using the Virtual IP (VIP) specified in the previous configuration file:

```
http://[VIP_ADDRESS]:4000
```

Use the default credentials `admin` / `password` to log in.

6.1 Cluster Initialization Wizard

After logging in for the first time, the initialization wizard will automatically appear on the screen. To begin, click on the **Initialize** button and carefully follow the guided procedure. Each step of the wizard will require entering basic configuration parameters; complete them sequentially until the initial cluster setup is finalized.

6.2 Adding the Servers to the Cluster

Once the wizard is completed, proceed to register the servers that will be part of the cluster. From the menu on the left, navigate to:

- **Hardware → Server → Add Server**

Servers must be added one at a time. After clicking **Add Server**, the *Basic Configurations* section will appear, where the server's role within the cluster must be defined. The configuration varies depending on the deployment scenario:

- **Two management nodes + witness**:
  - For both management nodes, select the roles *Management* and *Monitor*.
  - For the witness node, select only the *Monitor* role.
  - This configuration ensures proper metadata control and guarantees correct communication and data distribution between the two main nodes.
- **Three or more nodes**:
  - For each server, select both the *Management* and *Monitor* roles.

In all scenarios, make sure to **deselect the "Block Storage Gateway" option** if it is enabled by default.

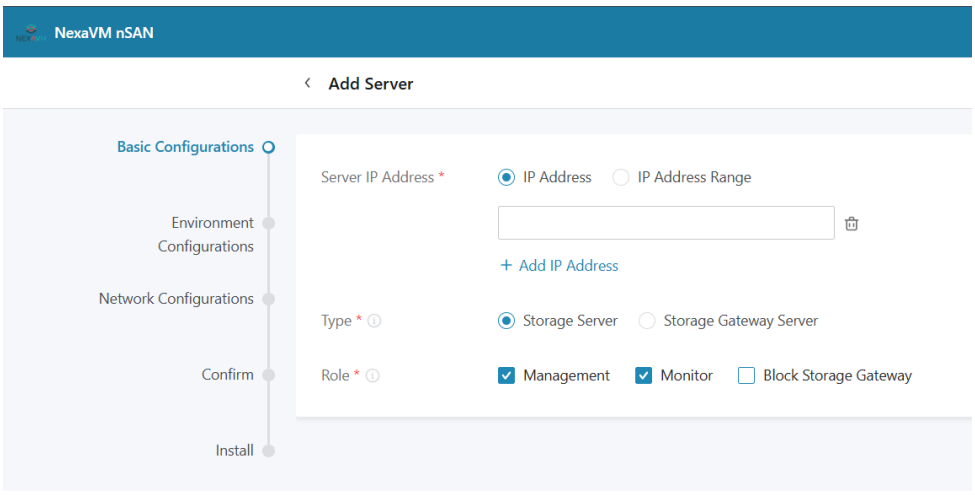

Figure 2: Roles

In the following configuration section, continue by entering the required data. It is essential to ensure that the option **Password-Free Login** is enabled, as shown in the reference screenshot.

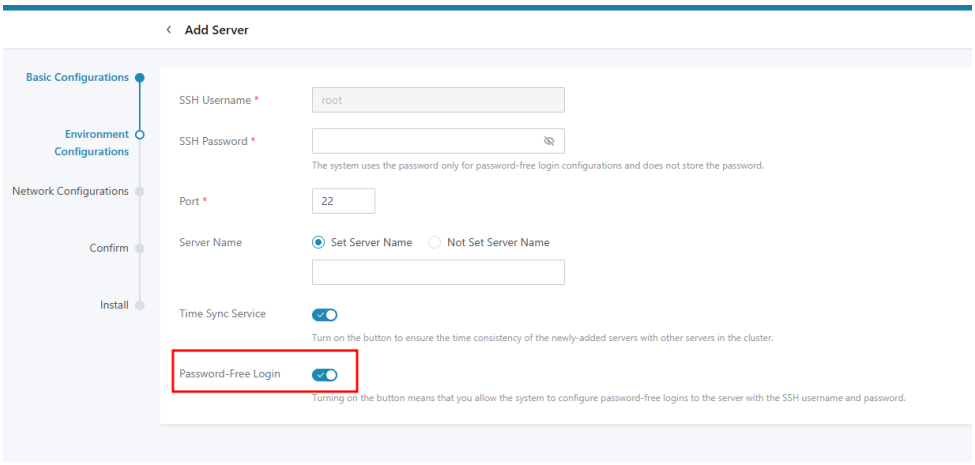

Figure 3: Password-Free Setup

This procedure (**Add Server** → configuration) must be repeated for each server that will take part in the cluster.

6.3 Creating the Topology

The next step is to create the physical topology of your environment. From the left-hand menu, navigate to:

- **Hardware** → **Topology**

In this section, use the **drag-and-drop** feature from the left-hand panel to recreate the actual physical topology of your infrastructure, following the example shown in the reference screenshot.

Start by adding the following hierarchical structure:

1. **Datacenter** — This represents the top-level element of the infrastructure.
2. **Room** — Place it inside the Datacenter.
3. **Rack** — Place it inside the Room.
4. **Nodes** — Add the physical nodes inside the Rack.

Depending on your deployment scenario:

- **Two-node + Witness scenario:** Add only the two data nodes inside the Rack.
- **Three or more node scenario:** Add all nodes that participate in the creation of the virtual storage, ensuring their physical location is accurately represented.

Make sure the topology accurately reflects your actual hardware layout before proceeding to the next step.

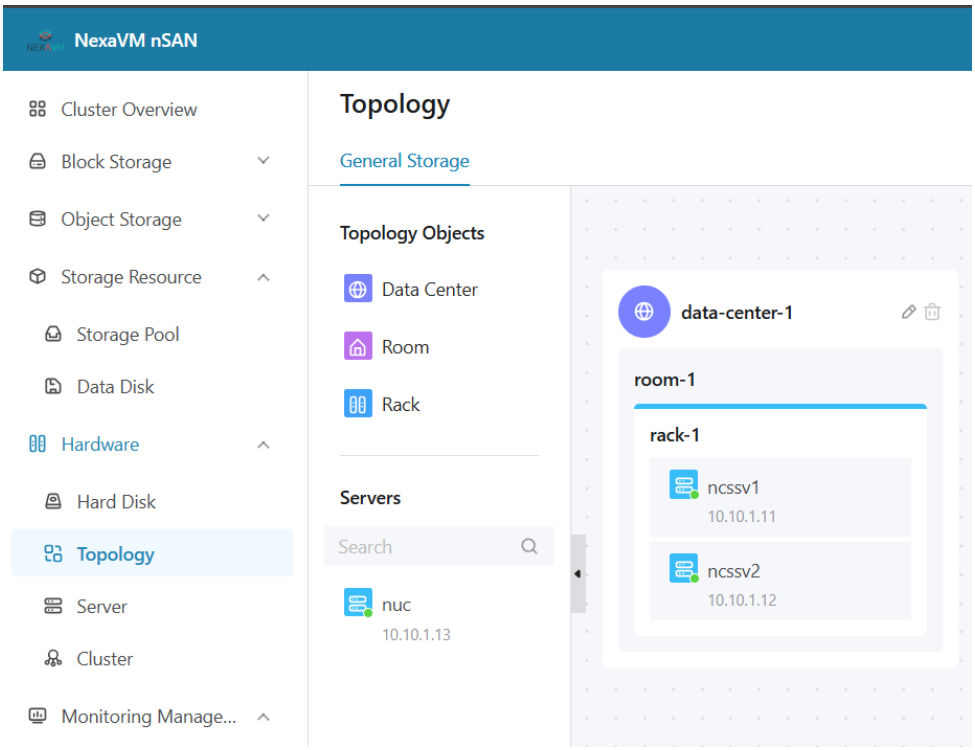

Figure 4: Topology Example

6.4 Creating the Data Disks

Once all servers have been successfully added, the next step is to configure the data disks. From the left-hand menu, navigate to:

- **Storage Resources** → **Data Disk** → **Create Data Disk**

Add the physical or virtual disks that will later be used to create the storage pool.

6.5 Creating the Storage Pool

With the data disks available, proceed to create the storage pool. From the left-hand menu, select:

- **Storage Resources** → **Storage Pool** → **Add Storage Pool**

Fill in the requested fields and, most importantly, assign the previously created data disks to the *Data Disk* section at the bottom of the form.

Once this procedure is completed, the storage pool will be created. At this point, it is essential to note the **UUID** of the newly created storage pool.

To obtain this information, simply click on the storage pool entry in the list and copy the *Storage Pool UUID*, as shown in the screenshot. This value will be required later when configuring the nCSSV environment.

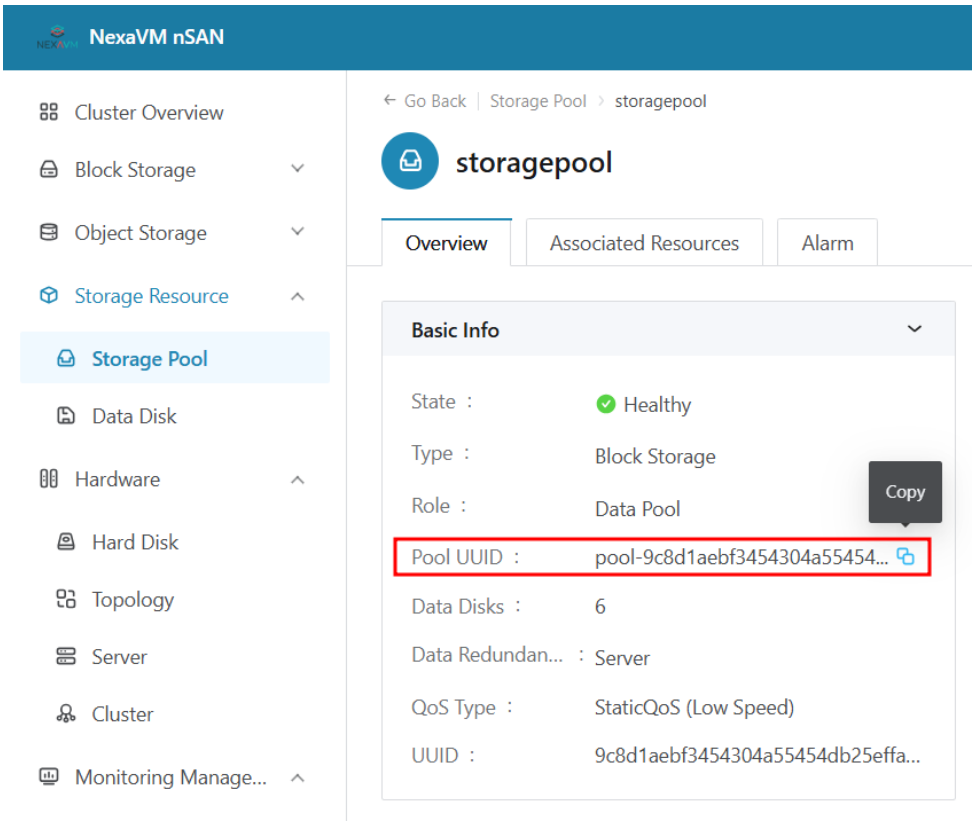

Figure 5: UUID-Location

7 Cluster Configuration via Web Interface (nCSSV)

After completing the cluster setup at port `4000`, the next step is to configure the nCSSV environment.

Open a web browser and connect to the cluster interface using the same Virtual IP (VIP) defined earlier, but on port `5000`:

```
http://[VIP_ADDRESS]:5000
```

Use the default credentials `admin` / `password` to log in. After logging in with the default credentials, the initialization wizard will automatically appear. Click on **Initialize** to start the guided procedure and complete each step by entering the required configuration data.

Follow the wizard until you reach the section **Add Primary Storage**. At this stage, be sure to:

- Select **Ceph** as the storage *Type*.
- Fill in the configuration fields as shown in the example screenshot.
- Insert the previously saved **UUIDs** into the highlighted fields corresponding to:
  - **Root Volume Pool**
  - **Data Volume Pool**
  - **Image Cache Pool**

Correctly configuring this section ensures that the primary storage is properly linked to the nCSSV environment.

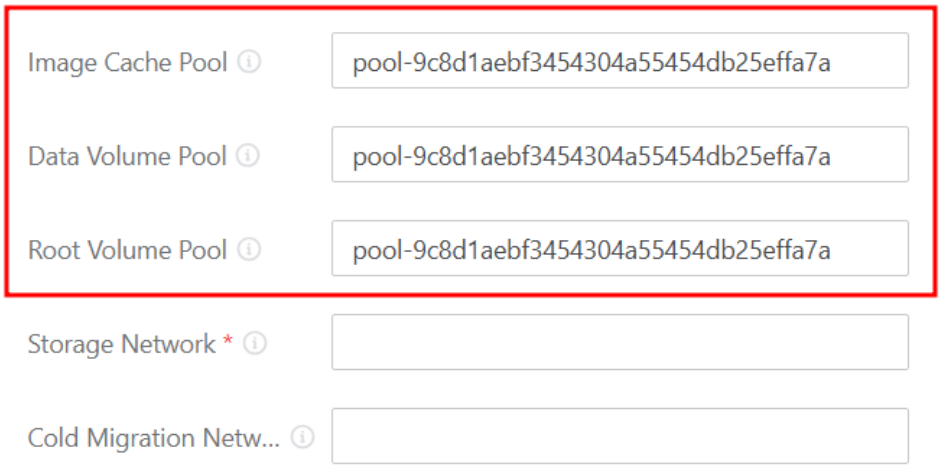

Figure 6: Ceph UUID Field (example)

7.1 License Creation and Activation

Once all configurations in the installation wizard have been completed, it will be necessary to generate and activate the product license. This can be done directly from the management GUI:

1. After logging into the GUI, click on the **Admin** menu in the top right corner.
2. Select **License Management**.
3. Download the system key file provided in this section.
4. Share the downloaded file with your sales or pre-sales contact, who will generate and return the license file.
5. Once received, upload the license file in the same **License Management** section to complete the activation.

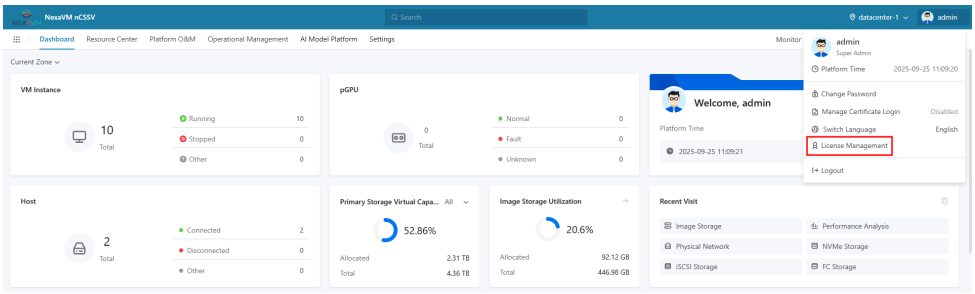

Figure 7: License Management Menu

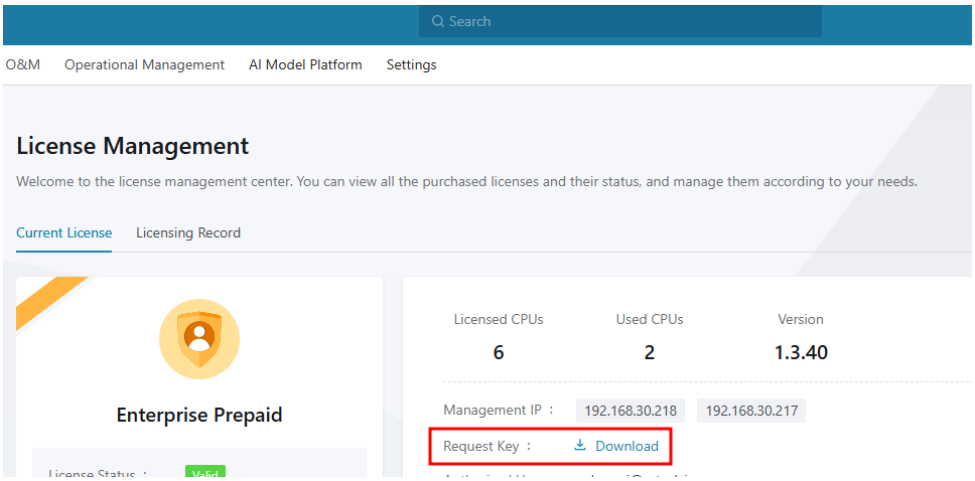

Figure 8: System Key Download

7.2 Adding a Monitoring Node

After uploading the license, the next step is to add an additional monitoring node to the previously created primary storage.

To perform this operation from the GUI, navigate to:

- **Resource Center** → **Hardware** → **Primary Storage**

Click on the primary storage that was created earlier. In the detailed view, locate the **Monitoring Node** section (as shown in the example screenshot), and then click on **Add Mon Node**.

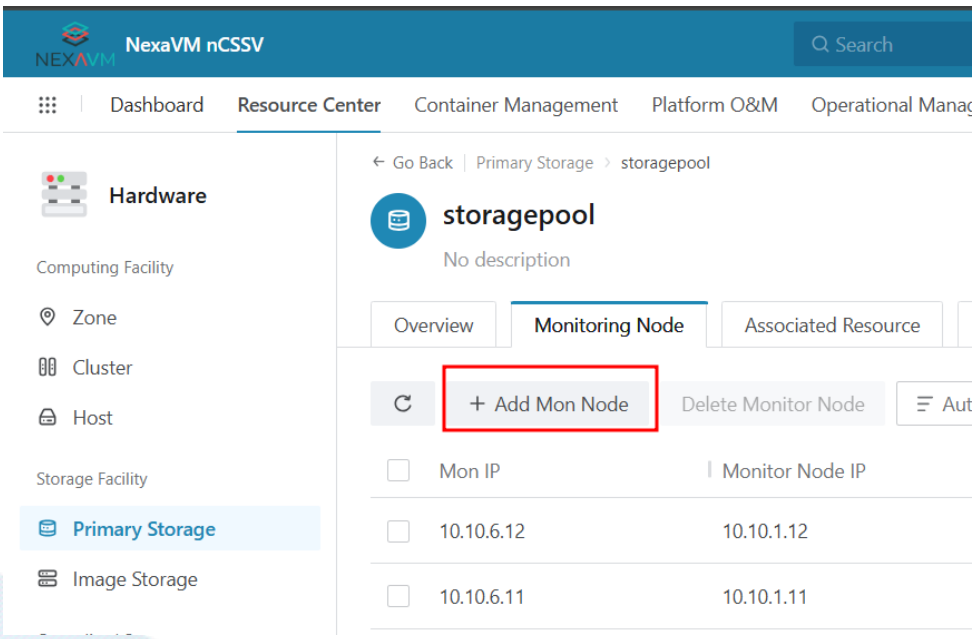

Figure 9: System Key Download

8 Conclusion of the Installation

At this point, all essential steps for the initial installation of the nCSSV platform have been successfully completed. The procedure has guided you through the following phases:

- Installation and synchronization of High Availability and Distributed Storage packages.
- Access to the management interface and execution of the initialization wizard.
- Addition of cluster servers with the appropriate roles depending on the deployment scenario.
- Creation of Data Disks and assembly of the Storage Pool.
- Retrieval and registration of the Storage Pool UUID.
- Configuration of the Primary Storage and association with the nCSSV environment.
- License generation and activation.

The system is now operational and ready for use. From this stage onward, administrators can proceed with:

- Deploying and configuring virtual machines.
- Setting up advanced networking features according to infrastructure requirements.
- Integrating monitoring and backup solutions for production environments.
- Applying security policies and best practices to ensure system protection.

Dynamic Expansion: The nCSSV platform has been designed to be flexible and scalable. Even after completing the installation described in this guide, it is possible to expand the infrastructure by:

- Adding new compute nodes to increase capacity.
- Integrating additional storage resources into existing storage pools.
- Connecting external storage systems for heterogeneous environments.
- Extending networking features to adapt to future needs.

This completes the base installation procedure. The environment is now ready to be customized and expanded according to the specific requirements of each deployment scenario.