



# nSSV Upgrade Guide

# Contents

1	Upgrade Overview . . . . .	2
1.1	Configuration Information . . . . .	2
1.2	Change Principles and Scope . . . . .	2
2	Upgrade Procedure . . . . .	2
2.1	Platform Upgrade Check . . . . .	2
2.2	Pre-Change Environment Handling . . . . .	3
2.3	Upgrade Execution . . . . .	4
2.4	Platform Risk Assessment . . . . .	6
3	Virtualization Component Upgrade . . . . .	6
3.1	Detailed Upgrade Steps . . . . .	6

# 1 Upgrade Overview

This document describes the maintenance and upgrade procedure for the nSSV platform.

The change covers the cloud management layer as well as the virtualization components (QEMU and libvirt). All operations are designed so that no impact is introduced to running production workloads.

## 1.1 Configuration Information

### Environment:

- Dual or Single Management Node (x86)

## 1.2 Change Principles and Scope

The upgrade procedure:

- Does not modify business workloads.
- Only affects the cloud management platform and virtualization components.
- Does not introduce architectural changes.

# 2 Upgrade Procedure

## 2.1 Platform Upgrade Check

Before upgrading, review the platform conditions and perform several validation tasks.

### General Checks

```
zstack-ctl status
```

```
cat /etc/*-release
```

```
uname -a
```

```
rpm -qa | grep -i qemu
```

```
rpm -qa | grep -i glib2
```

```
rpm -qa | grep -i libvirt
```

```
zsha2 status
```

## Pre-upgrade Validation Tools

Extract and execute the environment inspection tool as required.

To verify the consistency between the master and slave management nodes, extract and run the `zsmap` tool. In the following command, replace:

- **[MANAGEMENT\_NODE\_IP]** with the IP address of the management node to be checked
- **admin / password** with the corresponding login credentials

```
tar -zxvf zsmap-v2.3.tar.gz
```

```
cd zsmap/
```

```
bash check.sh [MANAGEMENT_NODE_IP] admin password
```

## 2.2 Pre-Change Environment Handling

1. Disable global HA:

- **Business Reliability → HA Policy**

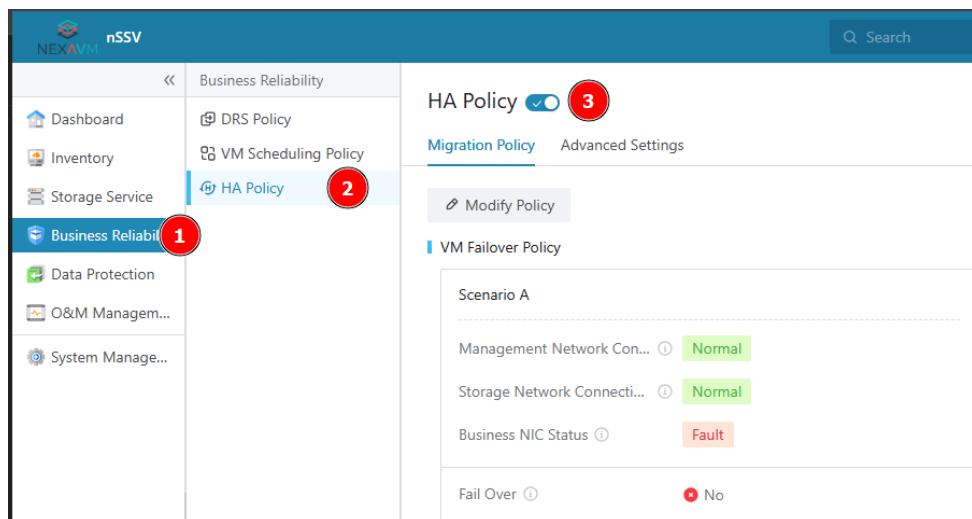


Figure 1: HA Policy

2. Prepare and upload all required upgrade packages.

Before starting the upgrade, it is essential to ensure that all necessary installation files are available on the management nodes. The exact set of required packages depends on whether the platform is deployed with a **single management node** or a **dual management node (HA)** configuration.

### Single Management Node Deployment:

For a standalone management node, upload the following packages to the server:

- **nSSV ISO** of the target version (used to update the local repository)
- **nSSV installer bin** of the target version

These two components are sufficient to complete the upgrade procedure on a single-node environment.

### Dual Management Node Deployment (HA):

For environments using dual management nodes, the following packages must be uploaded to **both management nodes**:

- **nSSV ISO** of the target version (to update the repository sources on each node)
- **nSSV installer bin** of the target version (used during the management service upgrade stage)
- **High-Availability Suite Package** (required to upgrade the HA framework before updating the management service)

Ensure that all files are transferred to each node and that their integrity is confirmed via MD5 checksum validation before proceeding.

### 3. Backup the database:

- Dual MN:

```
zstack-ctl dump_mysql --file-name zstack-db-backup-master
```

```
zstack-ctl dump_mysql --file-name zstack-db-backup-slave
```

- Single MN:

```
zstack-ctl dump_mysql --file-name zstack-db-backup
```

### 4. Backup the upgrade script:

```
cp /usr/local/bin/zstack-upgrade /root/zstack-upgrade-bk
```

## 2.3 Upgrade Execution

Choose the appropriate procedure depending on your management node topology.

### Dual Management Node

#### 1. Update source on both MNs:

```
bash /root/zstack-upgrade -r nexavm-nssv-x86_64-dvd-1.10.18-h84r.iso
```

2. Check VIP node:

```
zsha2 status
```

3. Extract HA suite on VIP node:

```
tar zxvf nexavm-nssv-multinode-ha-suite.tar.gz
```

```
chmod +x zsha2 zstack-hamon
```

4. Upgrade HA:

```
./zsha2 upgrade-ha -gencfg=true
```

5. Stop MN services on both nodes:

```
zsha2 stop-node
```

6. Upgrade cloud platform on VIP node (the UI will be inaccessible during the time):

```
zsha2 upgrade-mn nexavm-nssv-installer-1.10.18.bin
```

7. Check the status of the nodes and version after upgrading:

```
zstack-ctl status
```

```
zsha2 status
```

8. Log in to the web UI, check the status of inventory, storage service, clusters, etc.
9. Select physical hosts running non-critical business for priority UI manual reconnection. After a successful reconnection, check the kvmagent status and the running/business status of the VM instance. At this time, the upgrade status should display "Upgraded."
10. After the physical host reconnects successfully, check the specific storage according to the recorded data.
11. Check the VM status, log in to the console, and use ping to verify whether the network is normal. Ensure that business operations are not affected.

## Single Management Node

1. Upgrade repository and platform:

```
zstack-upgrade -r nexavm-nssv-x86_64-dvd-1.10.18-h84r.iso
```

```
bash nexavm-nssv-installer-1.10.18.bin -u
```

2. Validate upgrade:

```
zstack-ctl status
```

## 2.4 Platform Risk Assessment

- VM services remain unaffected during the upgrade.
- Perform the upgrade during off-peak hours.
- MN services will be temporarily unavailable.
- UI may require cache clearing due to framework updates.
- In case of unexpected issues, the process can be repeated or rolled back following the rollback plan.

## 3 Virtualization Component Upgrade

### 3.1 Detailed Upgrade Steps

1. Check current versions:

```
rpm -qa | grep qemu
```

```
rpm -qa | grep libvirt
```

```
rpm -qa | grep glib2
```

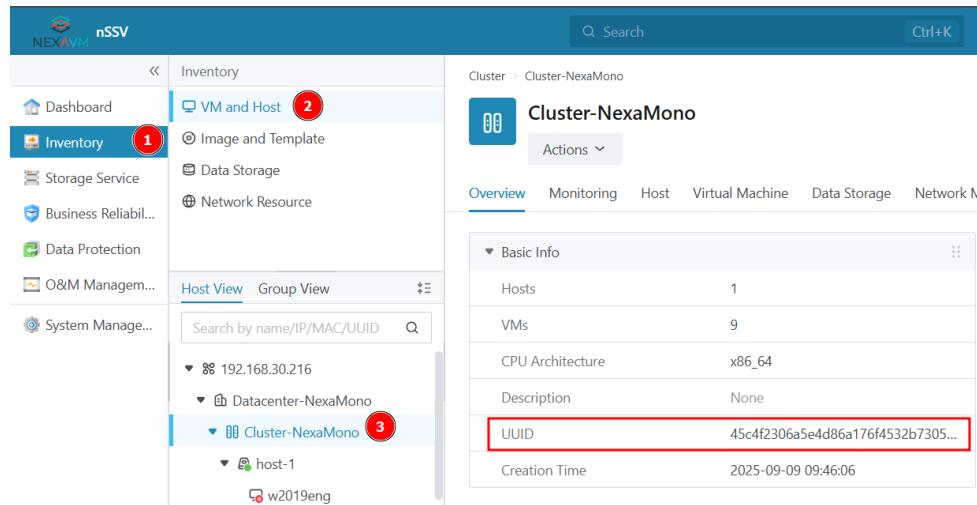
2. Retrieve platform UUID:

```
zstack-cli
```

```
>>> LogInByAccount accountName=admin password=password
```

3. Upgrade components using `UpdateClusterOS` commands: Before upgrading the virtualization components, it is necessary to retrieve the identifiers of both the cluster and the individual hosts on which the upgrade will be performed.

**Retrieve the Cluster UUID:** From the cloud platform interface, navigate to the Cluster details page and copy the **Cluster UUID**.

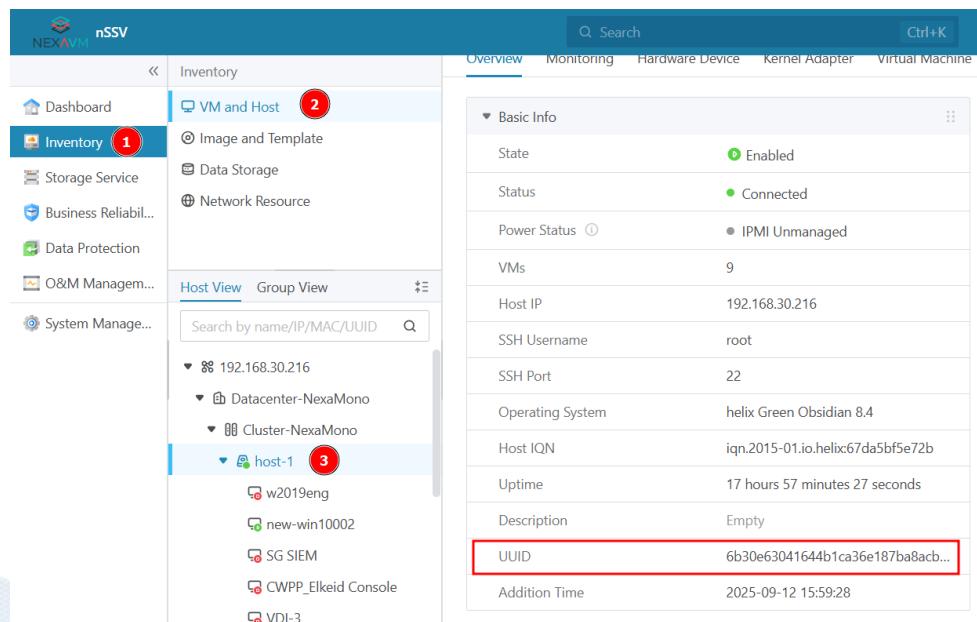


The screenshot shows the nSSV interface. The left sidebar has a red circle with '1' over the 'Inventory' button. The main navigation bar has a red circle with '2' over 'VM and Host'. The 'VM and Host' section is expanded, showing 'Image and Template', 'Data Storage', and 'Network Resource'. The 'Host View' tab is selected. A search bar shows '192.168.30.216'. Below it, 'Datacenter-NexaMono' is expanded, showing 'Cluster-NexaMono' with a red circle with '3' over it. Under 'Cluster-NexaMono', 'host-1' is expanded, showing 'w2019eng'. The right panel shows the 'Cluster-NexaMono' details. The 'Basic Info' table includes:

Hosts	1
VMs	9
CPU Architecture	x86_64
Description	None
<b>UUID</b>	45c4f2306a5e4d86a176f4532b7305...
Creation Time	2025-09-09 09:46:06

Figure 2: Cluster UUID Location

**Retrieve the Host UUID:** Open the details page of the target physical host and copy the **Host UUID**. This UUID will be required when upgrading components on a specific node.



The screenshot shows the nSSV interface. The left sidebar has a red circle with '1' over the 'Inventory' button. The main navigation bar has a red circle with '2' over 'VM and Host'. The 'VM and Host' section is expanded, showing 'Image and Template', 'Data Storage', and 'Network Resource'. The 'Host View' tab is selected. A search bar shows '192.168.30.216'. Below it, 'Datacenter-NexaMono' is expanded, showing 'Cluster-NexaMono' with a red circle with '3' over it. Under 'Cluster-NexaMono', 'host-1' is expanded, showing 'w2019eng', 'new-win10002', 'SG SIEM', 'CWPP\_Elkid Console', and 'VDI-3'. The right panel shows the 'host-1' details. The 'Basic Info' table includes:

State	Enabled
Status	Connected
Power Status	IPMI Unmanaged
VMs	9
Host IP	192.168.30.216
SSH Username	root
SSH Port	22
Operating System	helix Green Obsidian 8.4
Host IQN	iqn.2015-01.io.helix:67da5bf5e72b
Uptime	17 hours 57 minutes 27 seconds
Description	Empty
<b>UUID</b>	6b30e63041644b1ca36e187ba8acb...
Addition Time	2025-09-12 15:59:28

Figure 3: Host UUID Location

Once both values have been retrieved, proceed with the component upgrade commands shown below. In each command, replace:

- **[CLUSTER\_UUID]** → with the actual Cluster UUID

- **[HOST\_UUID]** → with the actual Host UUID of the node being upgraded

#### Upgrade qemu-storage-daemon on a specific host:

```
>>> UpdateClusterOS uuid=[CLUSTER_UUID] excludePackages=python2-  
crypto updatePackages=qemu-storage-daemon hostUuid=[HOST_UUID]
```

#### Upgrade qemu-kvm on a specific host:

```
>>> UpdateClusterOS uuid=[CLUSTER_UUID] excludePackages=python2-  
crypto updatePackages=qemu-kvm hostUuid=[HOST_UUID]
```

#### Upgrade glib2 on a specific host:

```
>>> UpdateClusterOS uuid=[CLUSTER_UUID] updatePackages=glib2  
hostUuid=[HOST_UUID]
```

#### Upgrade libvirt on a specific host:

```
>>> UpdateClusterOS uuid=[CLUSTER_UUID] excludePackages=python2-  
crypto updatePackages=libvirt hostUuid=[HOST_UUID]
```

#### 4. Validate upgraded versions:

```
rpm -qa | grep qemu
```

```
rpm -qa | grep libvirt
```

```
rpm -qa | grep glib2
```

#### 5. Migrate VMs to activate new QEMU version.

Before verifying the QEMU version of a running virtual machine, obtain the **VM UUID** from the VM details page in the management interface.

The screenshot shows the NexaVM nSSV interface. The left sidebar has a 'Inventory' section with a red circle containing the number '1'. The 'VM and Host' section is selected, indicated by a red circle containing the number '2'. The main content area shows a 'Basic Info' table for a VM named 'w2019eng'. The table includes fields like Status (Shut Down), OS (WindowsServer 2019), IPv4 Address(1) (192.168.30.221), and UUID (63a4ec8ecbf34fd09c3c1b183e6255dc). A red box highlights the 'UUID' row. The 'Host View' section on the left shows a tree structure with '192.168.30.216', 'Datacenter-NexaMono', 'Cluster-NexaMono', and 'host-1'. The 'w2019eng' VM is selected, indicated by a red circle containing the number '3'.

Basic Info	
Status	Shut Down
OS	WindowsServer 2019
IPv4 Address(1)	192.168.30.221
IPv6 Address	None
Uptime	-
High Availability	Disabled
Console Address	None
Owner	admin
Group	Default
Sharing Mode	Not Share
Description	Empty
UUID	63a4ec8ecbf34fd09c3c1b183e6255dc
Creation Time	2025-11-17 22:50:25

Figure 4: VM UUID Location

Once the VM UUID has been retrieved, run the following command on the physical host where the VM is currently running. Replace:

- **[VM\_UUID]** → with the actual UUID of the virtual machine

```
virsh qemu-monitor-command [VM_UUID] --hmp info version
```

6. Re-enable global HA.