HITACHI
Inspire the Next

Hitachi Virtual SMU Installation and Upgrade Guide

VSP N series

Hitachi NAS Platform

Release 14.9 or higher

MK-92HNAS074
January 2024

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Contents

Preface

This guide provides information about how to install and configure and upgrade a virtual System Management Unit (SMU).

Related Documentation

Release Notes provide the most up-to-date information about the system, including new feature summaries, upgrade instructions, and fixed and known defects.

Command Line References

The Command Line Reference provides information on the commands used to manage your system, and includes relevant information on the operation of your hardware and software. Depending on the model of your server or cluster node, refer to the Command Line Reference that is appropriate for your system.

- *NAS Module Server Command Line Reference*
- *Command Line Reference for models 4060, 4080, and 4100*
- *Command Line Reference for models 5200 and 5300*

Administration Guides

- *System Access Guide* (MK-92HNAS014)—Explains how to log in to the system, provides information about accessing the NAS server/cluster CLI and the SMU CLI, and provides information about the documentation, help, and search capabilities available in the system.
- *Server and Cluster Administration Guide* (MK-92HNAS010)—Provides information about administering servers, clusters, and server farms. Includes information about licensing, name spaces, upgrading software, monitoring servers and clusters, and backing up and restoring configurations.
- *Storage System User Administration Guide* (MK-92HNAS013)—Explains user management, including the different types of system administrator, their roles, and how to create and manage these users.
- *Network Administration Guide* (MK-92HNAS008)—Provides information about the server's network usage, and explains how to configure network interfaces, IP addressing, name and directory services.
- *File Services Administration Guide* (MK-92HNAS006)—Explains about file system formats, and provides information about creating and managing file systems, and enabling and configuring file services (file service protocols).
- *Data Migrator Administration Guide* (MK-92HNAS005) —Provides information about the Data Migrator feature, including how to set up migration policies and schedules.
- *Storage Subsystem Administration Guide* (MK-92HNAS012)—Provides information about managing the supported storage subsystems (RAID arrays) attached to the server/cluster. Includes information about tiered storage, storage pools, system drives (SDs), SD groups, and other storage device related configuration and management features and functions.
- *Snapshot Administration Guide* (MK-92HNAS011)—Provides information about configuring the server to take and manage snapshots.
- *Replication and Disaster Recovery Administration Guide* (MK-92HNAS009)—Provides information about replicating data using file-based replication and object-based replication, provides information on setting up replication policies and schedules, and using replication features for disaster recovery purposes.
- *Antivirus Administration Guide* (MK-92HNAS004)—Describes the supported antivirus engines, provides information about how to enable them, and how to configure the system to use them.
- *Backup Administration Guide* (MK-92HNAS007)—Provides information about configuring the server to work with NDMP, and making and managing NDMP backups.

Note: For a complete list of Hitachi NAS open source software copyrights and licenses, see the *System Access Guide*.

Hardware References

- *Hitachi NAS Platform and Hitachi Unified Storage Series 4000 Hardware Reference* (MK-92HNAS030)—Provides an overview of the Hitachi NAS Platform Series 4000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components
- *Hitachi NAS 5000 Series Hardware Reference* MK-92HNAS089—Provides an overview of the Hitachi NAS Platform Series 5000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components.
- *Hitachi NAS Platform System Manager Unit (SMU) Hardware Reference* (MK-92HNAS065)—This document describes the usage and replacement instructions for the SMU 300/400.

Best Practices

- *Hitachi NAS Platform Best Practices Guide for NFS with VMware vSphere* (MK-92HNAS028)—This document covers best practices specific to using VMware vSphere with the Hitachi NAS platform.
- *Hitachi NAS Platform Deduplication Best Practice* (MK-92HNAS031)—This document provides best practices and guidelines for using deduplication.
- *Hitachi NAS Platform Best Practices for Tiered File Systems* (MK-92HNAS038)—This document describes the Hitachi NAS Platform feature that automatically and intelligently separates data and metadata onto different Tiers of storage called Tiered File Systems (TFS).
- *Hitachi NAS Platform Data Migrator to Cloud Best Practices Guide* (MK-92HNAS045)—Data Migrator to Cloud allows files hosted on the HNAS server to be transparently migrated to cloud storage, providing the benefits associated with both local and cloud storage.
- *Best Practices for Hitachi NAS Universal Migrator* (MK-92HNAS047)—The Hitachi NAS Universal Migrator (UM) feature provides customers with a convenient and minimally disruptive method to migrate from their existing NAS system to the Hitachi NAS Platform. The practices and recommendations outlined in this document describe how to best use this feature.
- *Hitachi Data Systems SU 12.x Network File System (NFS) Version 4 Feature Description* (MK-92HNAS056)—This document describes the features of Network File System (NFS) Version 4.
- *Hitachi NAS HDP Best Practices* (MK-92HNAS057)—This document lists frequently asked questions regarding the use of Hitachi Dynamic Provisioning.
- *Hitachi Multi-tenancy Implementation and Best Practice Guide* (MK-92HNAS059)—This document details the best practices for configuring and using Multi-Tenancy and related features, and EVS security.
- *Hitachi NAS Platform HDP Best Practices* (MK-92HNAS063)—This document details the best practices for configuring and using storage pools, related features, and Hitachi Dynamic Provisioning (HDP).
- *Hitachi NAS Platform System Manager Unit (SMU) Hardware Reference* (MK-92HNAS065)—This document describes the usage and replacement instructions for the SMU 300/400.

- *NAS Platform ICC with Cisco Nexus Reference Guide* (MK-92HNAS085)—This document describes how to configure Cisco Nexus series switches for use as an ICC (intra-cluster communication) switch.
- *File System Snapshots Operational Best Practice* (MK-92HNAS068)—This document provides operational guidance on file system snapshots.
- *Virtual Infrastructure Integrator for Hitachi Storage Platforms Operational Best Practice* (MK-92HNAS069)—This document provides operational guidance on Hitachi Virtual Infrastructure Integrator for the HNAS platform.
- *Hitachi NAS Platform Replication Best Practices Guide* (MK-92HNAS070)—This document details the best practices for configuring and using HNAS Replication and related features.
- *Hitachi NAS Platform to Hitachi Virtual Storage Platform Unified Gx00 Models Migration Guide* (MK-92HNAS075)—This best practice guide describes how to perform a data-in-place migration of the Hitachi NAS Platform and Virtual Storage Platform (VSP) Gx00 File solution to the VSP Gx00 platform.

Accessing product documentation

Product user documentation is available on the Hitachi Support Website: https://knowledge.hitachivantara.com/Documents. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

The Hitachi Support Website is the destination for technical support of products and solutions sold by Hitachi. To contact technical support, log on to the Hitachi Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Community is a global online community for Hitachi customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send comments to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi.

Thank you!

Chapter 1: System requirements

Installation requirements

Before you install the virtual System Management Unit (SMU), check that your system meets all of the requirements for new installations.

The minimum virtual SMU resource requirements are stated below. The physical hardware should exceed these minimum requirements so that the host has resources beyond those allocated to the virtual SMU. In particular, the host should have more physical RAM than is allocated to the virtual SMU.

> **Note:** The vSMU OVA is not supported for deployment on any other type of virtualization product except as defined herein. Deployment of CentOS on a bare metal server and then placing the SMU application on that server is strictly unsupported. The CentOS version used in the OVA is purposely hardened to Hitachi Vantara standards and the SMU application applies CVE patches as required.

- Minimum virtual SMU specifications:
  - 64-bit CPU with at least 2 CPU cores (1 CPU core per managed server or cluster recommended).
  - 4GiB minimum for CentOS Stream 8 (or 1 GiB per managed server or cluster, if higher).
  - 100 GiB hard drive space.
  - 1 GigE network adapter.
- IP addresses for access to a hypervisor installation, if applicable, and for connecting to the SMU.

  > **Note:** Each SMU virtual machine (VM) you deploy requires at least one IP address for management UI access.
- An SMU OS install package.
- An SMU software install image.

If you have any questions, please contact your support organizations for assistance with these products.

Considerations when using a virtual SMU

Before you install and configure the virtual SMU, consider the following:

- A minimum amount of resources must be available for each VM if the hypervisor is configured to enforce minimum reservations. For more information, see Memory and CPU resource allocations (on page 10).
- The following SMU software versions support up to 10 managed servers or clusters:
  - VMware vSphere® (ESXi): Version 12.5.4038.04 or later.
  - Hyper-V: Version 12.7.4221.xx or later.

  Earlier SMU software versions support up to two managed servers or clusters.
- Open virtual appliance/application (OVA) is the standard distribution format of a virtual SMU OS for VMware. An OVA is a compressed archive (tarball) of Open Virtualization Format (OVF) files, including configuration and sparse disk image files.

  A zip file containing a Virtual Hard Disk (VHDX) file is the standard distribution format of a virtual SMU OS for Hyper-V.

Browser support

Use one of the following browsers to run NAS Manager, the web-based graphical user interface (GUI) of the system management unit (SMU):

- Microsoft Edge: any version released in 2020 or later.
- Mozilla Firefox: any version released in 2015 or later
- Google Chrome: any version released in 2015 or later.

> **Note:** The SMU uses cookies and sessions to remember user selections on various pages. Therefore, open only one web browser window or tab to the SMU per workstation or computer. If multiple tabs or windows are opened from the same workstation or computer, changes made in one tab or window might affect the other tabs or windows.

Memory and CPU resource allocations

A minimum amount of resources must be available for each VM if the hypervisor is configured to enforce minimum reservations.

In SMU software version 12.5.4038.04 or later for VMware, and version 12.7.411.xx or later for Hyper-V, the virtual SMU supports up to 10 managed servers or clusters.

The virtual SMU should be allocated 1 GiB RAM and 1 CPU core per managed server or cluster, regardless of the number of nodes in a cluster. For example, to manage four HNAS clusters, the virtual SMU should be allocated 4 GiB RAM and 4 CPU cores. The virtual SMU's minimum requirement is 4 GiB RAM for CentOS Stream 8, and 2 CPU cores, which is the default when it is deployed.

Note: If a server or cluster has more than 128 filesystems, the minimum requirements are 4 GiB RAM and a minimum of 2 CPU cores allocated to the virtual SMU with a maximum of two clusters per virtual SMU.

Sufficient memory and CPU resources allocated to the virtual SMU ensure that:

- The SMU's quorum device has enough priority on an oversubscribed host to maintain real-time communication with an HNAS cluster.
- Sufficient resources are available for background monitoring, which the SMU performs for each managed server cluster.

Important: The quorum device must respond to cluster heartbeats (over UDP) within five seconds to prevent the possibility of dependent and degraded HNAS clusters rebooting. Make sure that the SMU VM always has sufficient resources so that the quorum device is not paused or unresponsive for more than five seconds.

Resource reservations are less important when the SMU is not used as a quorum device.

Note: The NAS module in VSP models uses a different mechanism to control High Availability, so it does not use the SMU's quorum device.

Support for a virtual SMU running CentOS Stream 8

SMU versions 13.9.6918.04 or later can also be installed on a later version of the operating system, CentOS Stream 8.

In order to install a virtual SMU that runs on CentOS Stream 8 with VMware vSphere ESXi, follow the procedure documented in Chapter 2, ensuring that you deploy the OS template version SMU OVA 3.0 or later.

Starting with the vSMU CentOS Stream 8 release, the vSMU can be deployed in Azure.

Note: If you want to install SMU in Azure, refer to *Microsoft Azure – Installing and configuring a virtual SMU User Guide (MK-92HNAS079)* for details.

In order to install a virtual SMU that runs on CentOS Stream 8 with Hyper-V, follow the procedure documented in Chapter 3, ensuring that you deploy the OS template version SMU-OS-HYPERV-3.0.zip or later.

Note: HDRS versions 4.3 and 6.1 are only supported on CentOS Stream 8.

See Chapter 4 for instructions on how to upgrade an existing CentOS 6 SMU to one running CentOS Stream 8.

Chapter 2: VMware vSphere ESXi– Installing and configuring a virtual SMU

Installing the vSphere ESXi host and client

If the vSphere ESXi™ host is not already installed and operational, install the vSphere ESXi host onto the bare-metal host machine for your VM.

Note: For SMU-OS-3.0.ova, the vSphere ESXi host must be version 6.5 (Update 3) or later.

Use a Web browser to access the vSphere Client which manages the vSphere ESXi host, and operates its virtual machines.

Deploying the SMU OS

Deploy and map the pre-configured SMU OS template.

Procedure

1. Using a Web browser, log into the vSphere Client.
2. Right-click in the required location in the left-hand task bar and select **Deploy OVF template**.
3. Browse to the location of the SMU OS OVA file. Click **Next**.
4. Specify a unique virtual machine name and target location. Click **Next**.
5. Select the destination computer resource (host). Click **Next**.
6. Review the details and click **Next**.
7. Select the following virtual disk format: **Thin Provision**.
8. Select the storage (data store) and click **Next**.
9. Select the destination network (network card). Click **Next**.
10. Click **Finish**. The virtual image is deployed.

Increasing memory and CPU resource allocations

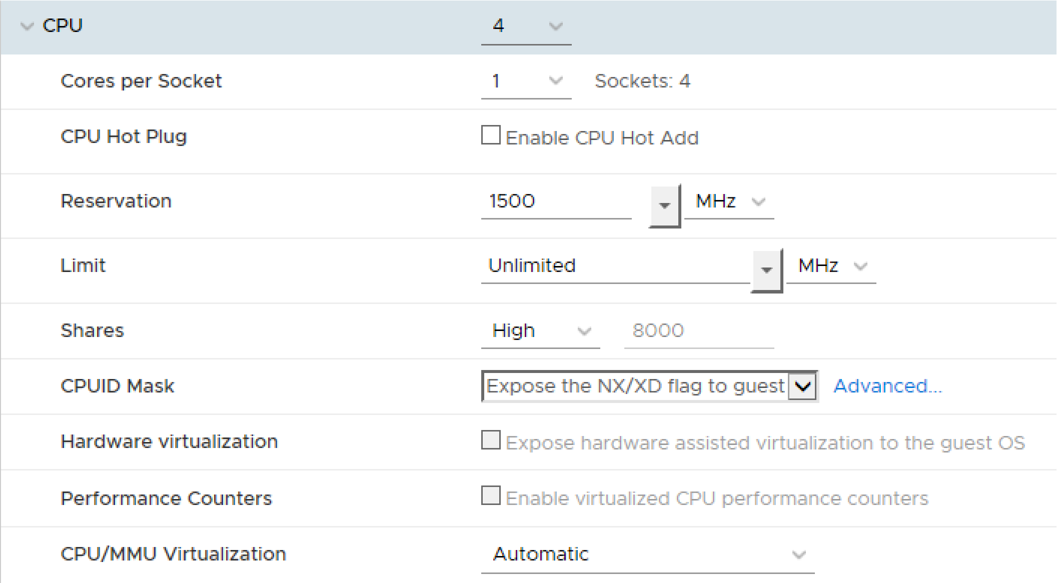
Before you add extra managed servers or clusters to the virtual SMU, increase the memory and the CPU resource allocations to reserve sufficient resources for each VM.

> **Note:** The exact user interface may differ from the screenshots shown below, depending on the version of the vSphere client in use.

The following example is for four managed servers.

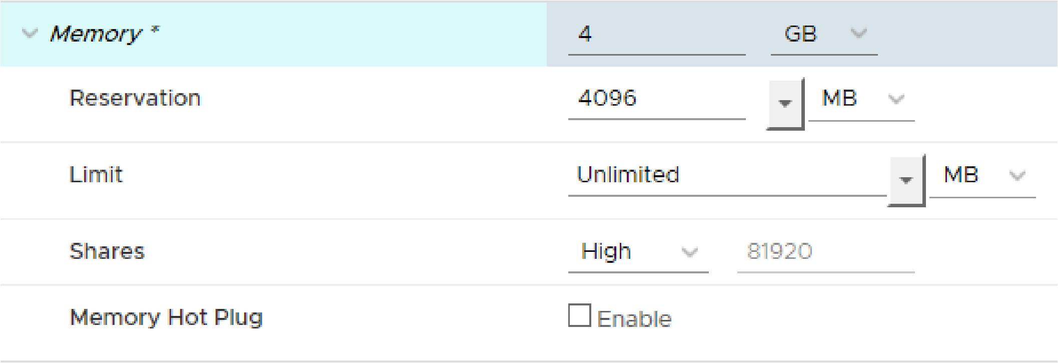
Procedure

1. Power off the VM.
2. In the vSphere Client, right-click the VM and select **Edit Settings** to open the Virtual Machine properties dialog box.
3. Under Virtual Hardware, select **CPU**:
    a. Either set the **CPU** option to four or set the **Cores per Socket** option to two to make a total of four sockets.
    b. (Optional) Although CPU reservation is not required, you should increase the CPU reservation if the host supports it.
    c. (Optional) If other VMs on the host can starve the virtual SMU of resources, you can set **Shares** for **CPU** (and Hard Disk) to **High**. This prioritizes the virtual SMU over VMs with a **Normal** or **Low** setting.



CPU	4	
Cores per Socket	1	Sockets: 4
CPU Hot Plug	□ Enable CPU Hot Add	
Reservation	1500	MHz
Limit	Unlimited	MHz
Shares	High	8000
CPUID Mask	Expose the NX/XD flag to guest	Advanced...
Hardware virtualization	□ Expose hardware assisted virtualization to the guest OS	
Performance Counters	□ Enable virtualized CPU performance counters	
CPU/MMU Virtualization	Automatic	

4. Under Virtual Hardware, select **Memory**:
    a. Increase the memory value to 4GB.
    b. (Optional Best Practice*) Set the reservation to 4096GB.
    c. (Optional) If other VMs on the host can starve the virtual SMU of resources, you can set **Shares** for **Memory** to **High**.



*Memory **	4	GB
Reservation	4096	MB
Limit	Unlimited	MB
Shares	High	81920
Memory Hot Plug	□ Enable	

5. Click **OK** to save your changes, and then close the dialog box.
6. Right-click the VM and select **Edit Settings** again to verify that your memory and CPU settings are correct.

***Best Practice**

Although resource reservations are not required, it is best to reserve a portion of the host's physical RAM to guarantee the responsiveness of the virtual SMU and its quorum device. Ultimately, if you oversubscribe the host, do so responsibly to ensure that the virtual SMU is not starved of resources.

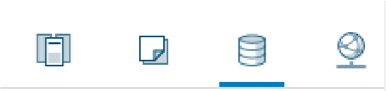
The critical virtual SMU requirement is that the quorum device must respond to cluster heartbeats (over UDP) within five seconds to prevent the possibility of dependent and degraded HNAS clusters rebooting. Resource reservations are just one way of achieving this requirement. VMware also provides other mechanisms to ensure VM responsiveness and to protect against resource starvation.

Installing the SMU software

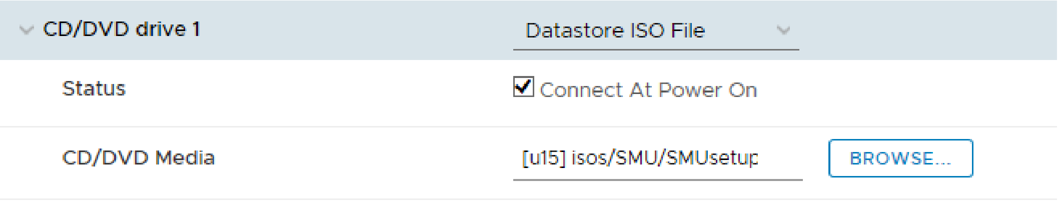
The SMU software is a virtual solution that runs on the vSphere ESXi server. After you install the SMU OS template, set up and connect the SMU software image to the newly created guest virtual machine.

Procedure

1. Click on the **datastore** icon in the left-hand task bar.



2. Select a datastore which is visible to the new SMU VM and click on the **Files** tab.
3. Upload the SMU software ISO file.
4. Right-click the new SMU VM and select **Edit Settings** to open the Virtual Machine properties dialog box.
   a. Under **Virtual Hardware**, select the **CD/DVD drive**.
   b. Select **Datastore ISO File**, and then click **Browse**.
   c. Select the recently uploaded SMU software ISO file, and then click **Open**.
   d. Verify that the **Connect At Power On** check box is selected, and then click **OK**.



CD/DVD drive 1 — Datastore ISO File

Status — ☑ Connect At Power On

CD/DVD Media — [u15] isos/SMU/SMUsetup

5. Power on the new SMU VM. and then launch a console.
6. Log in as `User: root` and `Password: passwd123!`

> **Note:** The default password for root used by the CentOS Stream 8 template differs from that previously used by the CentOS 6 template.

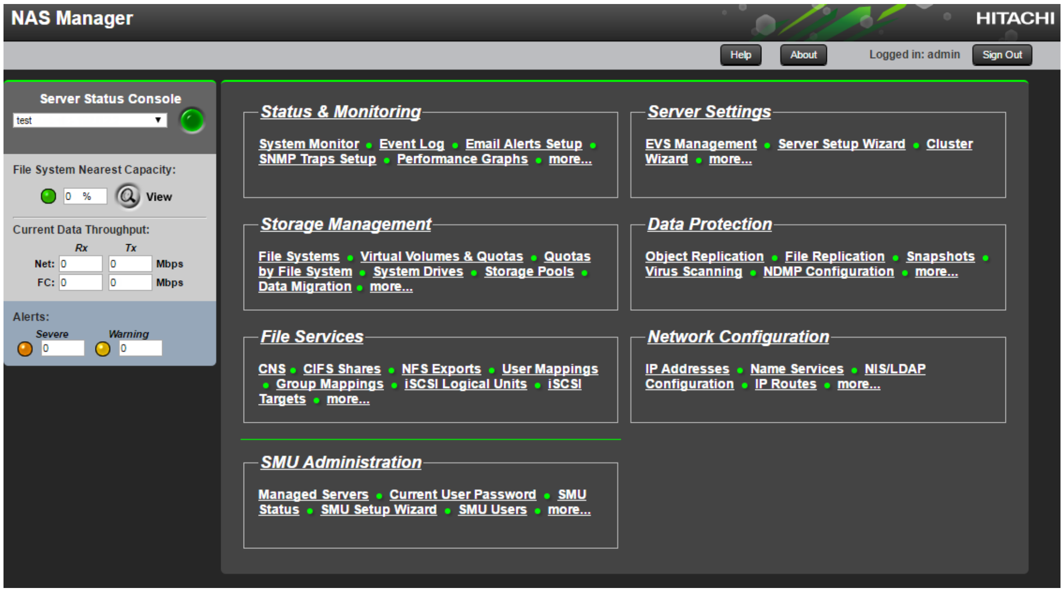
7. Run `mount /media/cdrom`.
8. Run `/media/cdrom/autorun` to start the installation. Note that the installation may take a few minutes to complete, after which the system reboots.

Configuring the SMU software

After you have installed the virtual SMU software, configure the virtual SMU network settings.

Procedure

1. In the console, log in as `User: root` and `Password: passwd123!`
2. Run `smu-config`, and then follow the prompts to configure the network.
3. Review all of the settings, and then type `Y` to confirm.
   The script sets up the network interfaces and the default properties, and then the SMU reboots.
4. On your laptop or desktop, open a web browser and point it to one of the SMU IP addresses.
5. Log in to NAS Manager as **`admin`**.
   The NAS Manager GUI opens.



NAS Manager HITACHI

Help About Logged in: admin Sign Out

Server Status Console

test

File System Nearest Capacity:

0 % View

Current Data Throughput:

	Rx	Tx	
Net:	0	0	Mbps
FC:	0	0	Mbps

Alerts:

Severe 0 Warning 0

Status & Monitoring

System Monitor • Event Log • Email Alerts Setup • SNMP Traps Setup • Performance Graphs • more...

Server Settings

EVS Management • Server Setup Wizard • Cluster Wizard • more...

Storage Management

File Systems • Virtual Volumes & Quotas • Quotas by File System • System Drives • Storage Pools • Data Migration • more...

Data Protection

Object Replication • File Replication • Snapshots • Virus Scanning • NDMP Configuration • more...

File Services

CNS • CIFS Shares • NFS Exports • User Mappings • Group Mappings • iSCSI Logical Units • iSCSI Targets • more...

Network Configuration

IP Addresses • Name Services • NIS/LDAP Configuration • IP Routes • more...

SMU Administration

Managed Servers • Current User Password • SMU Status • SMU Setup Wizard • SMU Users • more...

6. Before you set up the server, navigate to **Home** > **SMU Administration** > **SMU Setup Wizard** to configure the SMU settings.

   Note:

   For more information about using the SMU Setup Wizard, see the *Server and Cluster Administration Guide*.

Installing VMware Tools

VMware Tools™ is an optional package that provides useful tools for managing the virtual SMU. The main benefit of VMware Tools is its ability to shut down or restart the VM cleanly.

Without VMware tools installed, the hard Power Off option is equivalent to removing the power cords from the outlet. However, with VMware Tools installed, Power Off provides a cleaner shutdown.

Tip: For an alternative cleaner shutdown, either enter the `shutdown -h` command from a console session, or in NAS Manager, navigate to Home > SMU Administration > SMU Shutdown / Restart, and then click shut down.

Note: You may need to reinstall VMware Tools each time the SMU software is updated.

Procedure

1. Power on the VM.
2. Right-click on the SMU VM and select **Guest OS > Install VMware Tools**....
3. Read the text and then click **Mount**.
4. Launch the console.
5. Log in as `User: root` and `Password: passwd123!`

6. Run `mount /media/cdrom`.
7. To change to the `/tmp` directory and then extract the contents of the tar file into a new directory called `vmware-tools-distrib`, run:

   ```
   cd /tmp;
   ```

   ```
   tar -zxpf /media/cdrom/VMwareTools*.tar.gz.
   ```
8. To change the directory to `vmware-tools-distrib` and then start the installer, run:

   ```
   cd vmware-tools-distrib;
   ```

   ```
   ./vmware-install.pl
   ```
9. Follow the prompts and confirm the default settings.
10. When the script is complete, type `reboot`.
11. To confirm that VMware Tools has installed, click the VM **Summary** tab.

Adding an optional eth1

> **Note:** This optional eth1 port is only necessary if implementing a Private Management Network to segment Management and Quorum away from the Customer Management Network.

You can add an optional eth1 in addition to the default single eth0.

In general, SMUs need only a single Network Interface Card (NIC). Add a second NIC only if there a clear requirement for it.

Before you begin, make sure that a separate distributed virtual switch is configured.

Procedure

1. Power off the VM.
2. In the vSphere Client, right-click the VM and select **Edit Settings** to open the virtual machine properties dialog box.
3. On the **Virtual Hardware** tab, click **Add New Device**.
4. Select **Network Adapter**.
5. Select the name of the separate distributed virtual switch from the drop-down list.
6. Under **Adapter Type**, from the drop-down list, select **E1000**.
7. Click **OK**.

   After restarting the SMU VM, login to NAS Manager and configure an IP address for the eth1 port under **Home > SMU Administration > SMU Network Configuration.** The recommended IP is 192.0.2.1 (or 192.0.2.253 for a standby SMU)

   > **Note:** You should always explicitly assign a static IP address to the port. Although an address may have been assigned by DHCP, you should not rely on that as the SMU will not be correctly configured to use DHCP assigned addresses.

Chapter 3: Hyper-V – Installing and configuring a virtual SMU

Downloading the SMU OS files

Download the Hyper-V SMU zip file from which you can install the SMU OS.

Before you begin

Verify that you have a suitable Microsoft Hyper-V environment installed and ready to use, such as Microsoft Windows Server 2019 with the Hyper-V role added.

Procedure

1. Copy the Hyper-V SMU zip file, for example `SMU-OS-HYPERV-3.0.zip` file to the windows server.
2. Extract the contents of the zip file to a location that is easy to find, such as `C:\VSMU`.

Deploying the SMU OS

Deploy the pre-configured SMU OS template.

The SMU-OS-HYPERV-3.0 template is version 9 that can be deployed on a Windows Server 2019 Hyper-V host and above. To deploy on earlier Windows Server versions, instead of importing the VM from the extracted template, you need to create a new VM and then chose an existing VHDX (from the template) during its creation.

Before you begin

- Create a unique folder in which to store the VM files. The following example uses `C:\vSMU\smu1\`.

> **Note:** Each virtual SMU that you create needs its own unique ID and its own unique folder.

Procedure

1. In Hyper-V Manager, in the **Actions** pane, select **Import Virtual Machine**.
2. In the **Import Virtual Machine** dialog box, click **Next**.

3. Click **Browse**, and then locate the folder that contains the contents of the Hyper-V SMU zip file (`C:\vSMU`).
4. Click **Select Folder**, and then click **Next**.
5. Select the SMU OS file, and then click **Next**.
6. Select **Copy the virtual machine (create a new unique ID)**, and then click **Next**.
7. Select **Store the virtual machine in a different location**.
   a. In the **Virtual Machine configuration folder**, **Checkpoint store**, and **Smart Paging folder** boxes, enter your folder path (`C:\vSMU\smu1\`), and then click **Next**.
8. In the **Location** box, again enter your folder path, and then click **Next**.
9. On the **Connect Network** page, an error may indicate that the configuration “Could not find the External Virtual Switch” (a switch that connects through a physical network adapter to a physical network). The template file looks for a virtual switch with a specific name, but it needs only a virtual switch with an external connection type. Either:
   - Select an existing virtual switch with an external connection type from the **Connection** list.
   - Create a new virtual switch with the **Virtual Switch Manager** in the **Actions** pane.
10. Click **Next**, review the settings on the **Summary** tab, and then click **Finish**.
    A progress bar appears while the system sets up the virtual SMU.

Renaming the virtual SMU VM

Give the virtual SMU VM a unique name.

> **Note:** Hyper-V allows more than one VM to have the same name, so give each VM a unique name to avoid any confusion.

Procedure

1. In Hyper-V Manager, under **Virtual Machines**, right-click the new VM and select **Rename**.
2. Give the VM a unique name.

Modify the SMU VM resource and network settings

Before you add extra managed servers or clusters to the virtual SMU, increase the memory and the CPU resource allocations to reserve sufficient resources for each VM.

The following example is for four managed servers.

Procedure

1. In Hyper-V Manager, under **Virtual Machines**, right-click the VM and select **Turn Off**.
2. Right-click the VM again and select **Settings**.
3. (Best practice*) In the left pane, under **Hardware**, select **Memory**.

a. Change the **Startup RAM** to **4096 MB**.
b. Select **Enable Dynamic Memory**. This ensures that Hyper-V receives accurate information about the memory architecture of the host when the VM starts.
c. Change the **Minimum RAM** to **4096 MB**.

4. Under **Hardware**, select **Processor**.
   a. Change the **Number of Virtual Processors** to **4**.
   b. Click **Apply**, and then click **OK**.
5. Under **Settings Network Adaptor** configure the adaptor to use a static MAC address. If not using System Center Virtual Machine Manager (SCVMM), assign a static MAC address outside all assigned dynamic ranges of all nodes in the cluster. If using SCVMM, assign a static MAC address from the appropriate pool.
6. Right-click the VM and select **Start**.
7. At the bottom of the **Hyper-V Manager** dialog box, click the **Memory** tab and check that all of your settings are correct.

***Best practice**

Although resource reservations are not required, it is best to reserve a portion of the host's physical RAM to guarantee the responsiveness of the virtual SMU and its quorum device. Ultimately, if you over provision the host, do so responsibly so that the virtual SMU is not starved of resources.

The critical virtual SMU requirement is that the quorum device must respond to cluster heartbeats (over UDP) within five seconds to prevent the possibility of dependent and degraded HNAS clusters rebooting.

Installing the SMU software

The SMU software is a virtual solution that runs on the Hyper-V server. After you install the SMU OS template, set up and connect the SMU software image to the newly created guest virtual machine.

Procedure

1. In Hyper-V Manager, under **Virtual Machines**, right-click the VM and select **Settings**.
   a. In the left pane, under **Hardware**, select **DVD drive**.
   b. Under **Media**, select **Image File**.
   c. Click **Browse**, and then locate the folder that contains the contents of the Hyper-V zip file.
   d. Select the SMU setup ISO file, and then click **Open**.
   e. Click **Apply**, and then click **OK**.
2. Under **Virtual Machines**, right-click the VM, and then select **Connect**.
3. On the toolbar, click the **Start** button ⏻ to start the VM console.
4. Log in as `User: root` and `Password: passwd123!`

> **Note:** The default password for **root** used by the CentOS Stream 8 template differs from that previously used by the CentOS 6 template.

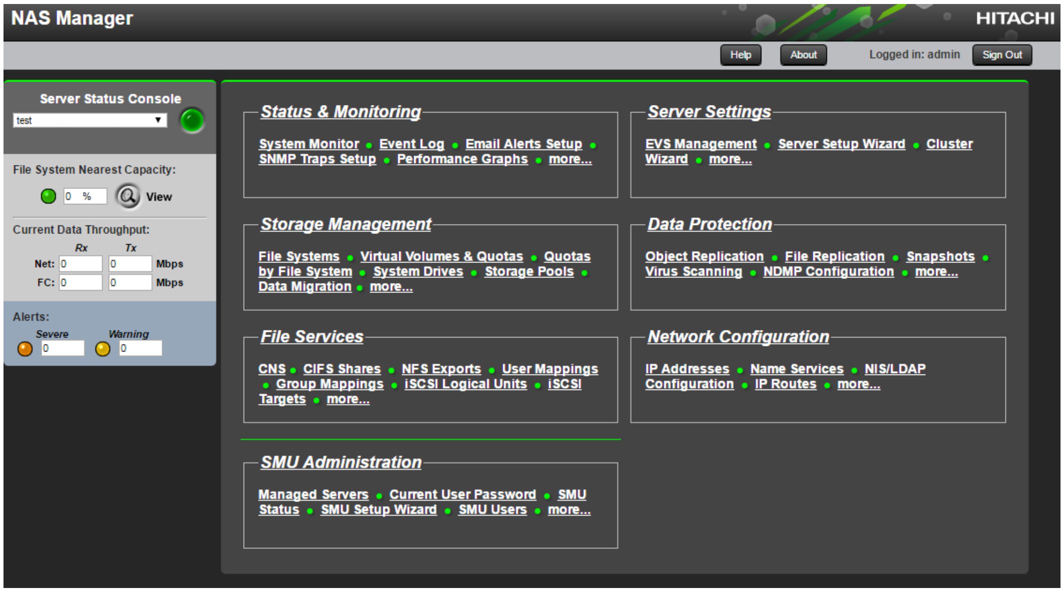
5. Run `mount /media/cdrom`.
6. Run `/media/cdrom/autorun` to start the installation. Note that the installation may take a few minutes to complete, after which the system reboots.

Configuring the SMU software

After you have installed the virtual SMU software, configure the virtual SMU network settings.

Procedure

1. In Hyper-V Manager, under **Virtual Machines**, Right-click the VM and select **Connect**.
2. On the toolbar, click the **Start** button ⏻ to start the VM console.
3. Log in as `User: root` and `Password: passwd123!`
4. Run `smu-config`, and then follow the prompts to configure the network.
5. Review all of the settings, and then type `Y` to confirm.
   The script sets up the network interfaces and the default properties, and then the SMU reboots.
6. On your laptop or desktop, open a web browser and point it to one of the SMU IP addresses.
7. Log in to NAS Manager with the `admin` user.
   The NAS Manager GUI opens.


NAS Manager
HITACHI
Help
About
Logged in: admin
Sign Out
Server Status Console
test
File System Nearest Capacity:
0 %
View
Current Data Throughput:
Rx
Tx
Net: 0 0 Mbps
FC: 0 0 Mbps
Alerts:
Severe
Warning
0
0
Status & Monitoring
System Monitor • Event Log • Email Alerts Setup • SNMP Traps Setup • Performance Graphs • more...
Server Settings
EVS Management • Server Setup Wizard • Cluster Wizard • more...
Storage Management
File Systems • Virtual Volumes & Quotas • Quotas by File System • System Drives • Storage Pools • Data Migration • more...
Data Protection
Object Replication • File Replication • Snapshots • Virus Scanning • NDMP Configuration • more...
File Services
CNS • CIFS Shares • NFS Exports • User Mappings • Group Mappings • iSCSI Logical Units • iSCSI Targets • more...
Network Configuration
IP Addresses • Name Services • NIS/LDAP Configuration • IP Routes • more...
SMU Administration
Managed Servers • Current User Password • SMU Status • SMU Setup Wizard • SMU Users • more...

8. Before you set up the server, navigate to **Home** > **SMU Administration** > **SMU Setup Wizard** to configure the SMU settings.

Note:

For more information about using the SMU Setup Wizard, see the *Server and Cluster Administration Guide*.

Guidelines and requirements

Follow these guidelines when you use Hyper-V to ensure that your system operates correctly.

- Do not manually install or change Linux Integration Services (LIS) on the virtual SMU. Red Hat LIS is set up automatically in software version 12.7.411.xx or later.
- Avoid using checkpoints (formerly snapshots), as doing so will affect the virtual SMU's performance.
- The virtual SMU is a generation 1 VM. The SMU OS does not support generation 2 VMs.
- The virtual SMU has not been tested with a System Center Virtual Machine Manager (SCVMM) or a VMM guest agent. Use these options at your own risk.
- Avoid using Dynamic HW MAC Addresses. If not using SCVMM, assign a static MAC Address outside all assigned dynamic ranges of all nodes in the cluster. If using SCVMM, assign a static MAC Address from the appropriate pool.

Chapter 4: Upgrading Firmware on a NAS Virtual SMU

This chapter shows the steps to upgrade firmware on a NAS Virtual SMU.

Before you begin

Download or stage the SMUsetup firmware:

1. Download the latest SMU GA version from a Hitachi Vantara resource.

   Note: Check the MD5 checksum for the firmware.

2. Stage the firmware on the final destination server or workstation where the SMU GUI will run.
3. To generate a MD5 for the file on the final destination, use the following command:

   ```
   certutil -hashfile <file> MD5
   ```

   Example: `certutil -hashfile SMUsetup_deer_7322.05_hds.iso MD5 MD5 hash of SMUsetup_deer_7322.05_hds.iso: c9ab6f627bf700443389c99768f78c19 CertUtil: -hashfile command completed successfully.`

Open a browser session to the SMU:

1. Log in to the SMU as admin.

Backup the External SMU configuration:

1. Navigate to Home > SMU Administration > SMU Backup and Restore.
2. Click Backup.
3. Repeat the above steps until you have two backup files of the same size.
4. Verify that the archive file opens.
5. Take a Snapshot of the VMware instance.

Collect Diagnostics from the system:

1. Navigate to Home > Status & Monitoring > Download Diagnostics.
2. In the Managed Server section, click Include Only the Currently Managed Server.
3. Ensure the Storage and FC Switches checkboxes are checked.
4. In the SMU section, uncheck Include archived diagnostics.
5. Click Download and save locally on your computer.

Stop all Replications:

1. Navigate to Home > Data Protection > File Replication.

2. In the Schedules section, abort any running replication jobs.
3. On the Details page, set any jobs scheduled to run during the upgrade period to INACTIVE.
4. Navigate to Home > Data Protection > Object Replication
5. In the Schedules section, abort any running replication jobs.
6. On the Details page, set any jobs scheduled to run during the upgrade period to INACTIVE.

To upgrade the SMU, do the following:

Procedure

1. Navigate to **Home** > **SMU Administration** > **SMU Upgrade**.
2. Browse to the location of `SMUsetup_<version>_hds.iso` file.
3. Click **Apply**.
4. Click **OK** to confirm.

   > ❗ **Important:** Do not interrupt the process; doing so might corrupt the PostgreSQL database, and the only recovery will be a rebuild or recovery of the vSMU.

Result

The virtual SMU automatically reboots and successfully completes the upgrade.

Next steps

1. From the vSMU Home screen, click About to check the virtual SMU version and verify the successful upgrade of the virtual SMU.
2. Check that the administrators have access to the Primary and/or Standby SMU

Restart all Replications:

1. Navigate to Home > Data Protection > File Replication.
2. In the Schedules section, restart File Replication schedules.
3. Verify that File Replication jobs start successfully.
4. Navigate to Home > Data Protection > Object Replication
5. In the Schedules section, restart Object Replication schedules.
6. Verify that Object Replication jobs start successfully.

Collect Diagnostics from the system:

1. Navigate to Home > Status & Monitoring > Download Diagnostics.
2. In the Managed Server section, click Include Only the Currently Managed Server.
3. Ensure the Storage and FC Switches checkboxes are checked.
4. In the SMU section, uncheck Include archived diagnostics.
5. Click Download and save locally on your computer.

External Program checks:

1. Hitachi recommends to upgrade the Remote Ops (Hi-Track) Monitor to the latest GA release of HTM.

2. Ensure that the HNAS System is configured and reporting in Remote Ops (Hi-Track) Monitor.

Chapter 5: Migrating an existing virtual SMU from CentOS 6 to CentOS Stream 8

A standard upgrade of an earlier virtual SMU to version 13.9.6918.04 or later will not upgrade the operating system version. If you want to upgrade an existing CentOS 6 SMU to run on CentOS Stream 8, while preserving the existing network address, it is necessary to deploy a new virtual SMU and migrate the settings from the existing SMU to the new one by performing a backup and restore.

Note: The SMU will be temporarily unavailable while following this procedure.

Configuring the SMU Software

Before you begin

Backup the HNAS registry and SMU Configuration:

1. Log in to the SMU as admin.
2. Navigate to Home > SMU Administration > SMU Backup and Restore.
3. Click Backup.
4. Save the registry files locally on your computer.
5. Verify that the archive file opens.

Backup the External SMU configuration:

1. Navigate to Home > SMU Administration > SMU Backup and Restore.
2. Click Backup.
3. Save the configuration files locally on your computer.
4. Repeat the above steps until you have two backup files of the same size.
5. Verify that the archive file opens.

Collect Diagnostics from the system:

1. Navigate to Home > Status & Monitoring > Download Diagnostics.
2. In the Managed Server section, click Include Only the Currently Managed Server.
3. Ensure the Storage and FC Switches checkboxes are checked.
4. In the SMU section, uncheck Include archived diagnostics.
5. Click Download and save locally on your computer.

Stop all Replications:

1. Navigate to Home > Data Protection > File Replication.
2. In the Schedules section, abort any running replication jobs.
3. On the Details page, set any jobs scheduled to run during the upgrade period to INACTIVE.

   Note: Note the schedule values so they can be reset after the procedure.

4. Navigate to Home > Data Protection > Object Replication
5. In the Schedules section, abort any running replication jobs.
6. On the Details page, set any jobs scheduled to run during the upgrade period to INACTIVE.

   Note: Note the schedule values so they can be reset after the procedure.

Verify the status of the Cluster:

1. Navigate to Home > Server Settings > Cluster Configuration.
2. Verify that the Cluster Health is Robust.

Deploy and install the CentOS Stream 8 SMU VM

To deploy and install a new virtual SMU that runs on CentOS Stream 8 using VMware vSphere ESXi, follow the procedure documented in the sections Deploying the SMU OS (on page 12) to Installing the SMU software (on page 14).

Ensure that you deploy the OS template version SMU OVA 3.0 or later.

To deploy and install a new virtual SMU that runs on CentOS Stream 8 with Hyper-V, follow the procedure documented in the sections Deploying the SMU OS (on page 18) and Installing the SMU software (on page 20). Ensure that you deploy the OS template version SMU-OS-HYPERV-3.0.zip or later.

Procedure

1. Start the console for the new VM from ESXi or Hyper-V Manager and login as `User: root` and `Password: passwd123!`
2. Run smu-config and follow the prompts to configure the passwords and network. Enter the same IP address and host name and domain that were used by the virtual SMU that you are upgrading from.
3. Review all of the settings, and then type **Y** to confirm.
4. The script sets up the network interfaces and default properties, and then the SMU reboots.

Next steps

Restoring the SMU Configuration to the new Stream 8 SMU:

1. Open a web browser and log in to NAS Manager with the `admin` user.
2. Navigate to Home > SMU Administration > SMU Backup and Restore.
3. Hit Choose File to select the backup file that you downloaded from the existing SMU and then select Restore.

4. NAS Manager will restart and will then be configured in the same way as the virtual SMU from which the backup was taken.

   Note: The passwords for all users including `root` and `manager` are restored from the backup and will overwrite those supplied to smu-config if different.

Chapter 6: Migrating a Physical SMU to a Virtual SMU

This task describes the steps to migrate a physical SMU to a virtual SMU.

Prerequisites

Hitachi Supplied Software/Documentation for a Virtual SMU (vSMU)

Note: Contact the local CS&S Support Personnel for the following files and documentation.

1. SMU CentOS Stream 8 (`SMU-OS-3.0.iso`).
2. SMU Application version 14.5.7413.01 or later (i.e. `SMUsetup_deer_7413.01_hds.iso`).
3. *Hitachi Virtual Installation and Upgrade Guide (MK-92HNAS074)*.

Customer Supplies Information

Important: A customer physical presence will be required on-site to manipulate cables on the nodes.

1. Obtain the passwords for the supervisor, admin, manager, and root users of the HNAS Cluster.
2. Obtain the passwords for the root, and manager users of the Physical SMU 400.
3. VLANS: If using VLANs, verify that the network ports on the Customer Ethernet Management Switch for HNAS Management and Quorum are all in the same VLAN so that the Management Stations can get to this VLAN.
4. Enough Ethernet drops run to the HNAS rack from the Customer Ethernet Management Switch.
   a. SMU - (eth0) (**this should already exist in the SMU**).
   b. A drop for eth1 on ALL Nodes in the Cluster, unless one already exists on eth0 of the Node.
5. IP addresses

   Note: All IP addresses are from the customer IP address pool.

   - **a.** SMU: Physical SMU - One **permanent** IP address (eth0) (this should already exist in the SMU).
   - **b.** Cluster Nodes, if possible, use consecutive IP Addresses:
      - **i.** AdminEVS: One **permanent** IP address (eth1).
      - **ii.** Cluster Nodes: One permanent IP address (eth1) for each Node in the Cluster.

6. vSMU setup information:
   - **a.** One temporary IP address (eth0).
   - **b.** Customer Netmask (use the one from the Hardware SMU).
   - **c.** Customer Default Gateway (use the one from the Hardware SMU).
   - **d.** Customer Fully Qualified Domain Name (use the one from the Hardware SMU).
   - **e.** SMU Host Name (use the one from the Hardware SMU).
   - **f.** If doing the complete SMU Setup Wizard.

Prep Work

Backup the HNAS registry and SMU Configuration

1. Open a browser session to the SMU.
2. Log in as admin; enter the current password when prompted.
3. Back up the Server registry:
   - **a.** Navigate to Home > Server Settings > Configuration Backup & Restore.
   - **b.** Click the <Backup> button.
   - **c.** Save the registry file to a location on your computer.
   - **d.** Verify that the archive file opens.
4. Backup the SMU Configuration:
   - **a.** In the GUI, navigate to SMU Administration > SMU Backup and Restore.
   - **b.** Click the Backup SMU: <Backup> button.
   - **c.** Save the configuration file to a location on your computer.
   - **d.** Repeat steps i. and ii. until you have two backup files of the same size.
   - **e.** Verify that the archive file open.

Collect System Diagnostics

1. Collect Diagnostics from the system:
   - **a.** Navigate to Home > Status & Monitoring > Download Diagnostics.
   - **b.** Select Include Only the Currently Managed Server in the Managed Server section.
   - **c.** Leave the Storage, and FC Switches check boxes selected.
   - **d.** In the SMU section, uncheck Include archived diagnostics.
   - **e.** Click Download.
   - **f.** Save to a location on your computer.

Stop All Replications

1. Open a browser session to the SMU GUI at the SMU IP Address.
2. Stop all File Replication Jobs:
   a. Navigate to Home > Data Protection > File Replication
   b. In the Schedules section, abort any running file replication jobs
   c. On the details page, set any jobs scheduled to run during the upgrade period to INACTIVE.

   > **Note:** Note the schedule values so they can be reset after the procedure.

3. Stop all Object Replication Jobs:
   a. Navigate to Home > Data Protection > Object Replication.
   b. In the Schedules section, abort any running object replication jobs.
   c. On the details page, set any jobs scheduled to run during the procedure to INACTIVE.

   > **Note:** Note the schedule values so they can be reset after the procedure.

Verify the Status of the Cluster

1. Navigate to Home > Server Settings > Cluster Configuration.
2. Verify that the Cluster Health is Robust.

> **Note:** If the Cluster is not Robust, resolve all issues before performing the Reconfiguration Procedure.

Migration of a Private Management Network to a Customer Management Network

Reconfiguration of the Management and Quorum Network

Verify/Relocate the location of the adminEVS

1. Verify and Relocate, as necessary, the location of the adminEVS:
   a. Navigate to Home > Server Settings > EVS Management.
   b. Take note of the name of the adminEVS.
   c. Verify the location of the adminEVS.
   d. If the adminEVS is NOT assigned to Node 1, perform the following steps:
      i. Navigate to Home > Server Settings > EVS Migration
      ii. In the EVS Migration section, select Migrate EVS.
      iii. In the dropdown, select the adminEVS name.

iv. In the next dropdown, select Node 1.

v. Click <Migrate>.

vi. When the adminEVS migration to Node 1 has been completed successfully, proceed to the next step.

Additional adminEVS IP addresses on eth1

1. Navigate to Home > Network Configuration > IP Addresses.
2. Remove all IP addresses except 192.0.2.x on the eth1 port of the nodes.

Reconfigure IP addresses on the cluster nodes

1. From the IP Addresses screen, click Add.
2. In the following screen, enter the new adminEVS IP address and netmask.
    a. Port: eth1
    b. IPv4: IP Address
    c. IPv4: Netmask (select the appropriate netmask from the dropdown)
    d. Click OK.
3. From the IP Addresses screen, click Details for the Node 1 node address (typically 192.0.2.200).
4. In the following screen, enter the new cluster node IP address and netmask.
    a. IPv4: IP Address
    b. IPv4: Netmask (select the appropriate netmask from the dropdown)
    c. Click OK.
5. Click Details for the Node 2 node address (typically 192.0.2.201)
6. In the following screen, enter the new cluster node IP address and netmask.
    a. IPv4: IP Address
    b. IPv4: Netmask (select the appropriate netmask from the dropdown)
    c. Click OK.
7. Repeat the previous step for each of the remaining nodes in the Cluster.

Reconfigure Ethernet Cabling

1. Disconnect all cables from the SMU and Nodes to the Private Management Switch.
2. Connect the Physical SMU eth0 to the Customer Management Network (this should already be in place)
3. Connect each of the Nodes to the Customer Management Network:
    a. If a customer network drop exists on eth0 of the Node, move the cable to eth1 on each Node.
    b. If a customer network drop does NOT exist on eth0 of the Node, then connect a new customer network drop to eth1 on each Node.

Change the Cluster Managed Server IP Address

1. Navigate to Home > SMU Administration > Managed Servers

2. Click on Details for the Cluster that was just changed. (typically 192.0.2.2)
3. Change the Server IP Address from 192.0.2.x to the new adminEVS IP address
4. The Server Username should be `supervisor`.
5. Unless changed, the Server Password should be `supervisor`.
6. Click OK

The Managed Servers screen should reappear and the Cluster should now show the new adminEVS IP address and Green status.

Remove adminEVS IP addresses on eth0 of the Nodes

1. From the IP Addresses screen, delete all IP addresses on the eth0 port of the nodes.

> **Note:** All external communication with applications or users will now be accomplished via the customer network on the eth1 port.

Remove Private Management Node IP addresses on eth1 of the Nodes

1. From the IP Addresses screen, delete all IP addresses on the eth1 port of the nodes.

> **Note:** All management and quorum communication between the SMU and the Cluster will now be accomplished via the customer network on the eth1 port.

Reconfigure the Cluster Management and Quorum

1. Switch to the browser session on the External SMU.
2. Navigate to Home > Server Settings > Cluster Configuration.
3. Verify that the SMU can see the Cluster Nodes.
4. In the Quorum Device section, click Remove to delete the old 192.0.2.1 quorum device.
5. Click Add.
6. A new screen with the SMU Quorum with the latest customer-facing IP address should appear.
7. Select the new SMU Quorum device and click OK
8. The Cluster should now show a Robust Health.

Reconfiguration of the SMU (if necessary)

Perform the steps below to change the eth0 settings on the SMU

1. Switch to the browser session on the External SMU.
2. Navigate to Home > SMU Administration > Network Configuration.
3. Change the IP address on eth0 to the desired value.
4. Change the Subnet mask on eth0 to the desired value.
5. Change the Gateway on eth0 to the desired value.
6. Click <Apply>.
7. The SMU will now reboot to make the appropriate network configuration changes.

8. When the SMU has rebooted, open a browser session to the SMU.
9. Log in as `admin`; Enter the current password.

Verify that the SMU can contact the nodes across the network connections

1. Open a PUTTy session to the SMU.
2. Log in as `manager`; Enter the manager password when prompted.
3. Ping each of the Node's new IP addresses from the SMU.

Migration of Physical SMU 400 to a Virtual SMU Stream 8

Physical SMU

Connect to the SMU

1. Open a web browser to the Physical SMU
2. Log in as `admin`; Enter the current password when prompted

Check the SMU code version installed on the Hardware SMU

1. Verify the SMU code version:
   a. Click the <About> button in the upper right corner of the screen.

      The next screen will display the SMU Code version.
   b. If the version is not the Latest GA Release of SMU Code, proceed to the Upgrade the Hardware SMU (if the code version is below 13.x) (on page 34) and upgrade the SMU code version to the Latest GA Release.
   c. If the version is the Latest GA Release of SMU Code, skip the Upgrade the Hardware SMU (if the code version is below 13.x) (on page 34) and proceed to Backup the SMU configuration (on page 34).

Upgrade the Hardware SMU (if the code version is below 13.x)

> **Note:** Always upgrade the Hardware SMU to the latest GA Release of SMU code.

1. Navigate to Home > SMU Administration > SMU Upgrade.
2. Browse to the file `SMUsetup_<latest-ga-code-version>_hds.iso`.
3. Click <apply>.

   Wait for the upgrade to complete and the SMU to reboot.

Backup the SMU configuration

1. Open a browser session to the SMU.
2. Log in as `admin`; Enter the current password when prompted.
3. In the GUI, navigate to SMU Administration > SMU Backup and Restore.

4. Click the Backup SMU: <Backup> button.
5. Save the configuration file to a location on your computer.
6. Repeat the steps until you have two backup files of the same size.
7. Verify that the archive file opens.

Shutdown the Original SMU

> **Note:**
>
> 1. Because the vSMU is on the Customer Network, the Hardware SMU cannot be powered on during the SMU restore to the vSMU; at the end of the restore, there would be a conflict of IP addresses and cluster quorum.
> 2. Verify that no power outages or maintenance are scheduled during this procedure.

1. Open a browser session to the Hardware SMU.
2. Navigate to Home > SMU Administration > SMU Shutdown / Restart
3. Click <shutdown>
4. Wait for the Hardware SMU to power off (if after 10 minutes it has not shut down, remove the power cords)

Virtual SMU (vSMU)

Virtual SMU (vSMU) Installation

Follow the installation instructions in VMware vSphere ESXi– Installing and configuring a virtual SMU (on page 12) or Hyper-V – Installing and configuring a virtual SMU (on page 18) to install a new Virtual SMU using CentOS Stream 8 on VMware or Hyper-V.

Restore the SMU configuration from the latest backup of the Physical SMU

1. Open a browser to the vSMU
2. Navigate to Home > SMU Administration > SMU Backup and Restore
3. In the Manually Saved SMU Backup section, click <Browse> and browse to the location where the Physical SMU backup file was saved.
4. Click <restore>; the restore process will begin.

   > **Note:** The smu-restore process can take 45 minutes to 2 hours. Do not interrupt the process.

5. Once the SMU has rebooted, the logon ID displayed should be that of the old SMU, and all settings and configurations are as they were on the Physical SMU.

Perform a sanity check on the new vSMU

1. Open a browser to the vSMU.
2. Navigate to Home.
3. Check in the Upper Left Corner that the Cluster shows a Green Dot.

4. Click the About button in the upper right.

   The version should be the latest GA release of the SMU software.

5. Click <back>.
6. Navigate to Home > SMU Administration > SMU Network Configuration.
7. eth0 should show the original customer IP address.
8. The Host Name should show the original SMU name.
9. The Domain should match the customer's Domain.
10. Navigate to Home > Server Settings > Cluster Configuration.
11. The Cluster Health should be Robust.
12. The Node Health should be Green for each Node.
13. The Cluster Quorum IP Address should be the vSMU.
14. The Cluster Quorum Status should be Configured.

End of Migration Procedures

After the successful completion of migration

Start All Replications

1. Open a browser session to the SMU GUI at the SMU IP Address.
2. Start all File Replication Jobs:

   a. Navigate to Home > Data Protection > File Replication.
   b. In the Schedules section, click <details> for any of the INACTIVE file replication jobs.
   c. Click <restart> for any of the aborted file replication jobs.
   d. Change the schedule values back to the previous values.

3. Start all Object Replication Jobs:

   a. Navigate to Home > Data Protection > File Replication.
   b. In the Schedules section, click <details> for any of the INACTIVE file replication jobs.
   c. Click <restart> for any of the aborted object replication jobs.
   d. Enable any jobs disabled during the procedure.

Perform End Of Procedure Checks

1. Check that the clients have access to their data
2. Check SMTP Server:

   a. Navigate to Home > Status & Monitoring > Email Alerts Setup
   b. If the SMTP Server IP/Name is still configured for the old SMU IP Address, change the IP/Name to point to the new SMU IP/Name
   c. Click <apply>.
   d. Click the Shortcut: <Configure Email Forwarding> (in the lower left of the screen)
   e. Verify the SMTP Server is still correct

   f. If changed; Click <apply>

3. Verify Quorum Device:

   a. If the Quorum Device Status does not show: Configured, Navigate to Home > Server Settings > Cluster Configuration.
   b. Click <remove>.
   c. Click <add>.
   d. Select a new Quorum Device.
   e. Click <OK>.

4. Check EVS location

   a. Navigate to Home > Server Settings > EVS Migration
   b. Check that the EVSs are assigned to the preferred nodes; if they are not on the preferred nodes, click the Set all to preferred link.

5. Collect Diagnostics from the system

   a. Navigate to Home > Status & Monitoring > Download Diagnostics
   b. In the Managed Server section, select Include Only the Currently Managed Server.
   c. Leave the Storage, and FC Switches check boxes selected.
   d. In the SMU section, uncheck Include archived diagnostics.
   e. Click <download>.
   f. Save to a location on your computer.

6. If an adminEVS is required on an aggregation, refer to the earlier notes and re-add the adminEVS.

   a. Navigate to Home > Network Configuration > IP Addresses.
   b. Click <add>.
   c. Select Admin-EVS-x – admin services in the dropdown.
   d. Select the Port:.
   e. Click <OK>.

Chapter 7: Installing and Configuring a Standby Virtual SMU

Before you begin

Deploy and install the CentOS Stream 8 SMU VM

To deploy and install a new virtual SMU that runs on CentOS Stream 8 using VMware vSphere ESXi, follow the procedure documented in the sections Deploying the SMU OS (on page 12) to Installing the SMU software (on page 14).

Ensure that you deploy the OS template version SMU OVA 3.0 or later.

To deploy and install a new virtual SMU that runs on CentOS Stream 8 with Hyper-V, follow the procedure documented in the sections Deploying the SMU OS (on page 18) and Installing the SMU software (on page 20). Ensure that you deploy the OS template version SMU-OS-HYPERV-3.0.zip or later.

Configure the Standby vSMU

Procedure

1. From the ESXi Console tab, Login as Username: `root` Password: `<current root password>`
2. Configure the SMU by Run the following command:

   ```
   smu-config
   ```

   > **Note:** The script will prompt for the following (if an item is incorrect, the script can be re-run until you save it).

   a. root password - (entered twice - ignore the warning about a dictionary word).
   b. manager password - (entered twice - ignore the warning about a dictionary word).
   c. IPv4 address to assign to eth0 (public network) – **Customer IP Address**.
   d. IPv4 netmask to assign to eth0 (public network) – **Customer Netmask**.
   e. Default IPv4 gateway – **Customer Gateway**.
   f. Enter the (optional) SMU Private IP Address (eth1) - **<Enter>** (Leave it unconfigured, can be added later in the GUI if necessary).
   g. Configure IPv6 address [y/n] - answer **n** at this time.
   h. Fully qualified domain name (without the hostname) – **Customer Domain Name**.
   i. Host name (without the fully qualified domain name) – **Customer Host Name**.
   j. Confirm that all settings are correct; answer **y**.

Result

The SMU will reboot after you save the configuration.

Next steps

Configure the Primary vSMU

1. Open a browser and connect to the Primary vSMU.
2. Log in as Username: `admin` Password: `(Current admin password).`
3. Navigate to Home > SMU Administration > Standby SMU.
4. Enter the hostname or IP address of the Standby SMU in the **Public Name/IP of the Standby SMU** field.
5. Click Apply.
6. Click on the Backup and Restore Link at the bottom of the page.
7. Click the Backup.
8. Save the file on your locally on your computer.

> **Note:** In the Auto Saved SMU backup, an entry will be tagged as remote. This is the Standby SMU.

Verification of the configuration on the Standby vSMU

1. Establish an ssh (putty) session to the Standby SMU.
2. Log in as Username: **`manager`** Password: `(Current manager password).`
3. Enter **q** to quit to the bash shell on the SMU.
4. Navigate to `/var/opt/smu/archive/smu-backup/<Primary SMU ip address>`
5. In this directory, you will find the Primary SMU configuration files (these files will be time-stamped to facilitate which backup configuration to use in a later procedure).
6. Type **exit** to close out of the ssh (putty) session.

Connect the Standby vSMU eth0 port to the Customer Management Network

1. Connect the SMU customer management network drop to the vSMU eth0 port.
2. Verify that the customer has access to the vSMU.

Appendix A: Advanced features

⚠ **Caution:** Before you use any advanced features, verify that the system is configured correctly and that it can operate with advanced features installed.

vSphere High Availability features

VMware High Availability (HA) monitors all virtualized servers and detects physical server and operating system failures. HA can improve the availability of the virtual SMU and make HNAS deployments more robust.

vSphere Fault Tolerance (FT) provides continuous availability for applications if a server fails.

The main HA and FT configuration options when used with virtual SMUs are as follows:

- **vSphere vMotion® and Storage vMotion®:** Provide Manual and automatic migration of compute and storage without service interruption. The three vMotion scenarios are:

  - **Host-only migration (with shared storage):** Moves VM execution from one host to another.
  - **Storage-only migration (single host access to two storage pools):** Moves a VM's disk image from one storage pool to another storage pool.
  - **Host and storage migration:** A combination of both host and storage migration.

  Risk of losing quorum: none to minimal. However, vMotion does not protect against an ESXi host loss.

- **Cold standby SMU:** In an ESXi HA cluster, if the ESXi host running the primary virtual SMU fails, a new instance of the primary virtual SMU starts on another ESXi host. The new instance uses the last updated disk image from the shared storage. Although recovery is fast, it requires starting the VM, which is not fast enough to prevent a quorum loss. If the HNAS cluster is healthy, an SMU HA failover does not affect its availability, but it does prevent access to NAS Manager and the CLI while the new instance of the SMU starts.

  Risk of losing quorum: high to certain.

- **Hot standby SMU:** With FT on, a secondary virtual SMU (on a different ESXi host) takes over immediately from a primary virtual SMU if the primary SMU fails. This requires a 10 Gbps FT logging network in addition to the normal network that connects the ESXi hosts and the HNAS nodes. If the SMU serves as a quorum device, the failover should be within the five-second requirement before a quorum loss occurs. In this case, an SMU HA failover can occur without affecting the HNAS cluster, even if one of the HNAS nodes is down.

  Risk of losing quorum: none to minimal.

In summary, HA provides a highly available virtual SMU, but failovers will cause a short-term loss of quorum. FT provides a highly available virtual SMU with a negligible chance of losing quorum.

Guidelines and requirements

Follow these guidelines when you use vSphere High Availability (HA) or Fault Tolerance (FT) to ensure that the system operates correctly.

- Verify that VMware Tools is installed.
- Test that vSphere vMotion, HA, or FT configurations are robust and operate correctly.
- Do not host the virtual SMU on the same HNAS cluster for which the SMU is providing quorum to avoid creating a circular dependency. A quorum loss could prevent access to the SMU's disk image
- Follow guidelines for CPU and memory allocations. Make sure that the SMU VM always has sufficient resources so that the quorum device is not paused or unresponsive for more than five seconds.
- Use 10 Gbps for the FT logging network. Do not use 1 Gbps for the FT logging network as doing so will affect the virtual SMU's performance.
- Use a larger ESXi license when required rather than limit the number of virtual CPUs. FT configurations allow a maximum of two or four virtual CPUs, depending on the ESXi license installed. If you have more than two or four managed entities, verify that operation is sufficient with less than one virtual CPU per managed entity.
- Set up HA or FT configurations with the vSphere Web Client to receive more informative error messages.

For more information about vSphere High Availability, including features, license options, and pricing, visit: www.vmware.com.

Hitachi

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact